Security and Usability of Authentication by Challenge Questions in Online Examination

Abrar Ullah

School of Computer Science
University of Hertfordshire

Thesis submitted to the University of Hertfordshire in partial fulfilment of the requirements of the degree of Doctor of Philosophy (PhD)

December, 2016

Declaration

I certify that the work submitted is my own and that any material derived or quoted from the published or unpublished work of other persons has been duly acknowledged.

Student Full Name: Abrar Ullah

Student Registration Number: 10281203

____

Date: 14th Dec, 2016

Abstract

Online examinations are an integral component of many online learning environments and a high-stake process for students, teachers and educational institutions. They are the target of many security threats, including intrusion by hackers and collusion. Collusion happens when a student invites a third party to impersonate him/her in an online test, or to abet with the exam questions. This research proposed a profile-based challenge question approach to create and consolidate a student's profile during the learning process, to be used for authentication in the examination process. The proposed method was investigated in six research studies using a usability test method and a risk-based security assessment method, in order to investigate usability attributes and security threats.

The findings of the studies revealed that text-based questions are prone to usability issues such as ambiguity, syntactic variation, and spelling mistakes. The results of a usability analysis suggested that image-based questions are more usable than text-based questions ($p < 0.01$). The findings identified that dynamic profile questions are more efficient and effective than text-based and image-based questions ($p < 0.01$). Since text-based questions are associated with an individual's personal information, they are prone to being shared with impersonators. An increase in the numbers of challenge questions being shared showed a significant linear trend ($p < 0.01$) and increased the success of an impersonation attack. An increase in the database size decreased the success of an impersonation attack with a significant linear trend ($p < 0.01$). The security analysis of dynamic profile questions revealed that an impersonation attack was not successful when a student shared credentials using email asynchronously. However, a similar attack was successful when a student and impersonator shared information in real time using mobile phones. The response time in this attack was significantly different when a genuine student responded to his challenge questions ($p < 0.01$). The security analysis revealed that the use of dynamic profile questions in a proctored exam can influence impersonation and abetting. This view was supported by online programme tutors in a focus group study.

Acknowledgement

This research represents a considerable amount of my personal commitment, family support and guidance from my supervision team. I am grateful to the University of Hertfordshire and Professor Bruce Christianson, School of Computer Science for this opportunity.

I am short of words to thank my parents for their love, support, and encouragement to follow my dreams. Without their support, I doubt, I would be submitting this thesis.

This would have never been completed without the unwavering support of my wife Salma. I am grateful for her presence, continuous support and looking after the young family, when I have been away for research in the library most of the evenings for six long years.

My supervision team –Dr. Hannan Xiao, Dr Trevor Barker and Dr. Mariana Liley– have been outstanding. Their input has been invaluable. As my Principal Supervisor, Hannan helped me throughout this research to turn ideas into reality with encouragement and timely advice. Mariana has helped me in realizing the potential use of learning activities for authentication. I would like to extend a very special thanks to Dr. Trevor Barker for helping me through the difficult stage of statistical analysis, reasoning and thesis writing.

Finally, I would like to acknowledge that this research was partly funded by the Wales Deanery, Cardiff University. I wish to offer my sincere thanks to Paul Kirk and Maggie Kirk for their support and precious advice. Paul being Manager of the Business Systems Support Unit, Wales Deanery Cardiff University, has been very flexible in work and research activities. He was very instrumental in funding this research.

Table of Contents

List of Tables

List of Figures

1 Introduction

Online learning – delivering teaching and learning through the Internet – has attracted increased interest in the past 15 years, and continues to offer more opportunities (Levy and Ramim, 2007). It is used in education today with a positive influence on the learning experience and teaching alike (Barker et al., 2007). Some of the benefits of online learning include accessibility, quality of teaching and learning, a knowledge-based approach, re-usability of learning resources, use of interactive media, cost effectiveness, enhanced time management and remote access (Strother, 2002, Ruiz et al., 2006).

Besides the anticipated benefits, online learning has some limitations, including the security of online examinations, one of the major concerns. It is an important and integral component of online learning. With the increasing use of technology and the Internet, human interaction has been reduced and substituted with computers, tablets, mobile phones and software. The lack of face-to-face proctoring and the use of remote authentication approaches create security threats to high-stake examinations. The issues of security and authentication have been discussed in many research studies (McMurtry, 2001, Olt, 2002, Chan et al., 2003, Colwell and Jenks, 2005, Vician et al., 2006, Wielicki, 2006, Jung and Yeom, 2009). Some studies (Agulla et al., 2008, Harmon et al., 2010) suggest that unethical conduct has intensified in online learning due to an uncontrolled environment, as a result of the use of technology and the Internet. These studies indicate that remote and weak authentication approaches cause many threats, and also create opportunities for academic dishonesty. These threats may come from intruders or legitimate students. Students collude with third parties, who may impersonate them in their online tests, or accept help from abettors to answer their test questions.

This thesis investigates the usability and security of authentication in online examinations. The study reports on multi-method empirical research to use a profile-based challenge question approach and to understand the usability attributes and their influence on security in online examinations.

1.1 Research Background

1.1.1 Online Learning

The term ‘online learning’ has been discussed in the literature with multiple definitions. Researchers and practitioners have referred to distance learning, e-learning and online learning interchangeably (Lowenthal and Wilson, 2010, Volery and Lord, 2000, Moore et al., 2011). The context and use of these classifications is different based on their objectives, target audience, access method and type of content (Moore et al., 2011). Distance education is a common reference used for distance learning, which refers to providing education to geographically distant learners. With the introduction of computers and software in delivery of education, this term is used for teaching and learning using both print and electronic media. The history of distance learning goes back to the 19th century, when Isaac Pitman taught shorthand in Great Britain via correspondence through postal services in the 1840s (Kearsley and Moore, 2005).

Society has embraced new forms of teaching and learning through the years. One such form is referred to as online learning, which was introduced in the 1980s with the advent of the World Wide Web (Harasim, 2000, Moore et al., 2011). Another similar form is known as e-learning. It is the use of electronic media and associated tools for teaching and learning, which covers web-based training (WBT), computer-based instructions (CBI), computer-based training (CBT), Internet-based training (IBT) and virtual learning delivered via the Internet, intranet, mobiles, satellite broadcasts and interactive TV (Moore et al., 2011).

Online learning is described as a modern version of distance learning, where teaching and learning is performed remotely with the use of technology and the Internet (Carliner, 2004, Benson, 2002). In recent years, it has become an important tool for teaching and learning. Kolowich (2014) states that approximately 5.5 million students in the US participated in at least one online learning course till 2012. There has been an increase in the acceptance of online learning: a report published by Ambient Insight Research (2012) identified that the worldwide market for online learning products was $32.1 billion in 2010 and it was forecasted to rise to $49.9 billion by 2015. In a similar report by Global Industry Analysts (2012), the online learning market is projected to reach $168.8 billion by 2018. The above studies indicate a rising trend in the adoption of online learning.

1.1.2 Online Examinations

The term ‘examination’ in the context of education means testing and measuring a student’s knowledge and skills acquired during a learning period on a course. It drives the learning process and evaluates learning outcomes. The UK Quality Assurance Agency (QAA) code of practice (Agency, 2006) describes the purpose of examination as i) promoting the learning process by evaluating a student’s feedback, ii) evaluating a student's skills and knowledge against the learning goals and iii) providing marks or grades based on evaluation that enable a student's performance to be established. With the development of learning techniques, examination has also evolved and become an integral part of many learning environments (Joosten-ten Brinke et al., 2007). Depending on the intended purpose and outcome, examinations are classified into two main categories: summative and formative assessments, which are used in both traditional and remote settings.

- *Summative Assessment or Examination*: evaluates the outcome of learning and measures a student's skills against learning goals using a set of assessment techniques. The outcome is recorded in a grade book and accumulated in the final score. Apampa et al. (2010a) suggest that summative assessments are taken towards the end of a learning event and the outcome is counted in a mark sheet for the final award. It is a high-stake process, which confirms a student's qualification for the award as a result of attaining the required abilities and skills in a specific domain.
- *Formative Assessment or Examination*: teachers and educational supervisors use formative assessment to review and provide feedback on students' performance (Birenbaum, 1996). Xiang and Ye (2008) suggest that tutors use formative assessment in multiple iterative phases during the learning process. This enables them to reflect on learning feedback and manage teaching and learning processes. The outcome of this type of assessment does not count towards the final award.

Several methods have been implemented to conduct examinations. These methods have evolved due to intensive research work and ongoing student and teacher experiences (Moreno-Ger et al., 2008). Commonly used methods include questionnaires, assignments, projects, peer reviews, essays, quizzes, self-assessments and portfolios (Gaytan and McEwen, 2007, Joosten-ten Brinke et al., 2007).

1.1.3 Research Context

In typical online learning environments, examinations are often conducted remotely (Apampa et al., 2009, Ullah et al., 2014a). This poses many security threats. With the increasing demand for online learning, there is a rising concern about the integrity of such examinations (Watson and Sottile, 2010). According to Phillips and Lowe (2003), verifying the identity of students is a major security issue. Karvonen (1999) indicates that students' interaction with an online learning environment is performed remotely, and building confidence and trust is essential for the credibility of remote examinations.

The high-stake process relies upon remote authentication approaches for the identification of test takers. These features are performed using human factors, which are classified into three categories: knowledge-based, object- or token-based and biometrics. Examples of the knowledge-based method are user-identifiers and passwords, challenge questions, and graphical passwords. The object- or token-based method includes swipe cards and magnetic chip cards. Biometric features include fingerprint recognition, signature recognition, audio recognition and video recognition. These approaches provide different security assurances against different threats.

Usability is an important quality of systems. It is a measure of useful interactions between a system and target users in a specified context. This is important for the implementation of secure systems. Sasse et al. (2001) state that security techniques are only effective when usable. Security and usability experts suggest that authentication can only provide adequate security when usable (Sasse et al., 2001). Hence, it is essential to investigate the influence of usability on the security of authentication approaches in online examinations.

The research work presented in this thesis investigates security threats to online examinations. These threats include intrusion and non-intrusion attacks which are performed by both hackers and genuine students. It is anticipated that students are likely to have higher stakes in the online examination process compared to hackers. Therefore, this research focuses on non-intrusion threats posed by genuine students. These include collusion and non-collusion (plagiarism) threats, which are major security concerns. For example, some universities in the UK deliver their online courses remotely, whereas the high-stake examinations are conducted in supervised, invigilated locations (Cardiff, 2007, Queen Mary, 2011). Similarly, a number of market-leading licence and certificate providers including Microsoft (Adelman, 2000), IBM (Reinschmidt and Francoise, 2000), Apple and Cisco (Lammle, 2011) conduct several courses online and use the Prometric (1990) service for face-to-face invigilated examinations before the final award. This service is a subsidiary of the Educational Testing Service (ETS), which administers tests over 10,000 manned supervised sites in 160 countries. This indicates a lack of trust in the use of the remote online examination process and a desire to enhance security using a traditional supervised approach for further reassurance of students' identities.

The rise in collusion is a challenge to the security and credibility of online examinations (Dick et al., 2002, Pillsbury, 2004). In such attacks, a student invites a third party to help with an online test in different ways. Collusion is classified into impersonation and abetting threats. In impersonation, a student shares access credentials with a third party, who impersonates them and takes the online test. In abetting, a student takes the test while a third party helps, sitting close by or in a remote location.

Keeping in view the above research problems, the aim and objectives of this thesis are described below.

1.2 Research Aim and Objectives

The main aim of this PhD thesis is:

> “To design and analyse an authentication approach, understand the essential usability attributes of the proposed approach and its impact on security threats in remote online examinations”

In order to achieve the above aim, a list of objectives was generated to:

Objective 1) Investigate security threats to online examinations.

Objective 2) Investigate and design an authentication approach, and understand its influence on the potential security threats to online examinations.

Objective 3) Evaluate the usability and its influence on the security of the proposed authentication method.

Objective 4) Evaluate the security of the proposed method.

The first objective of this research is to investigate security threats to online examinations. These threats are documented in various pieces of literature. Learning and examinations are delivered online in web-based environments, which are open to a wide number of security threats (Kritzinger, 2006). The lack of security is identified in a number of research studies (Percoco and SpiderLabs, 2014, Apampa et al., 2009, Levy and Ramim, 2007). The security of high-stake online examinations is based on authentication and the assurances that only a legitimate student can gain access to an online test.

Conventional authentication approaches provide a different level of security assurances, cost effectiveness and usability. These are implemented to determine whether someone is who they claim to be (Marcel and Del Millan, 2007). Burr et al.

(2006) indicate that authentication verifies the identification of users. However, some of these methods may not ensure identification in certain threat scenarios. For example, a password feature cannot identify an attacker who logs into a system as a legitimate user with a stolen password (Chun-Li et al., 2001). Similarly, it is challenging to counter identification theft and masquerading, which is likely to help students in collusion attacks. Hence, the second objective of this research is to design an authentication approach and understand its impact on security threats.

Usability is essential in the design of secure authentication methods. It is the extent to which a system can be used by specified users efficiently and effectively in a given context (Jokela et al., 2003). It is important for the implementation of secure systems. Hence, the third objective of this research is to investigate the usability attributes associated with the proposed authentication method.

Security evaluation is essential for understanding how the authentication methods achieve the intended goals. Hence, the fourth and final objective of this research is to investigate the security of the proposed method in order to understand its impact on various types of attacks.

1.3 Research Questions

In an attempt to achieve the research objectives, this thesis aims to answer the following research questions and sub-questions:

RQ 1) What are the potential security threats to online examinations?

a. What are the potential collusion and non-collusion threats to online examinations?

RQ 2) What method can be used to support secure authentication of students in online examinations?

a. How can the challenge question approach be used for authentication of students in online examinations?

RQ 3) How does the usability of the proposed authentication method influence the security?

a. How does the usability of text-based questions influence the security of the challenge question approach in online examinations?
b. How does the usability of image-based questions influence the security of the challenge question approach in online examinations?
c. How does the usability of dynamic profile questions influence the security of the challenge question approach in online examinations?

RQ 4) How does the proposed authentication method influence security threats?

a. How does the use of text-based questions influence collusion threats in online examinations?

b. How does the use of dynamic profile questions influence collusion threats in online examinations?

1.4 Structure of the Thesis

This thesis is organised into 12 chapters. Chapter 1 provides an overview of the research background, objectives, context and original contribution to knowledge. The structure of the chapters is given below.

Chapter 2 (Literature Review) presents a literature review on information security, authentication, and usability of authentication methods, which provides a rationale and basis for this thesis. This chapter explores information security with particular interest in identifying system assets and threats to inform security goals, in order to protect assets. It also explores the information security of online learning and examination with a focus on threats to online examinations. The literature review provides evaluation of authentication in online learning with a focus on challenge questions authentication. The chapter describes the need for usability relating to information security and usability attributes that constitute usability in software systems. In addition, it also describes the influence of usability on security of authentication approaches. The literature review leads to the next chapter, which describes an overview of the research problems.

Chapter 3 (An Overview of Research Problems) explores various types of security threats to online examinations, in order to substantiate a theoretical underpinning for this thesis. The purpose of this chapter is to locate evidence of threats in the literature and also identify new evolving threats using abuse cases. The chapter presents a threat classification tree and factors that motivate students and intruders to attack online examinations. The collusion threats are classified into impersonation and abetting attacks. In impersonation, a student shares access credentials with a third party, who impersonates the student in an online test. In abetting, a student takes an online test; however, a third party helps the student to answer the test questions. This chapter provides the justification and need for this research. In response to the research problems, the next chapter will propose a challenge questions authentication approach.

Chapter 4 (Profile-based Authentication) proposes a challenge question approach for the authentication of students in online examinations. This chapter presents the overview and structure of the proposed method. It describes the text-based challenge question type and explains the architecture, design and development of an initial prototype, and integration with the MOODLE learning management system. In order to evaluate the proposed method, research methods and methodology are presented in the next chapter.

Chapter 5 (Research Methods and Methodology) presents research methods and methodology used to approach the research problems. This chapter presents a background of quantitative and qualitative methods associated with research studies. Furthermore, it provides justification for using empirical enquiries for security and usability evaluation. A risk-based security assessment method is described, along with the manner in which this method will approach specific parts of this research. This chapter also describes the need for a focus group to be utilised in this research and the overall security threats and empirical evaluation. The usability test method and questionnaire are presented, as well as examining how it will evaluate the usability attributes associated with this research. To evaluate the proposed challenge questions method developed in chapter 4, the first empirical study is presented in the next chapter using research methods described in this chapter.

Chapter 6 (Text-based Challenge Questions) presents the first empirical study involving an initial prototype of the proposed approach using text-based challenge questions. This chapter presents an exploratory simulation study to collect the benchmark data for the evaluation of usability attributes. The chapter presents study hypotheses, method, details of participants, empirical study phases and results. The initial findings show some usability issues as a result of syntactic variation, ambiguity, spacing and spelling errors. To address these issues, design of the text-based questions is revised in the next chapter. In addition, image-based questions are presented for improved usability.

Chapter 7 (Image-based and Text-based Challenge Questions) proposes image-based questions and presents an empirical study to investigate the usability of text-based and image-based challenge questions in a real online course. In response to usability issues reported in the previous chapter, this chapter implements image-based and revised text-based questions. Additionally, this chapter presents the purpose of the study, research questions, a relevant hypothesis, study method and phases, and, finally, reports the findings of efficiency and effectiveness analysis associated with text-based and image-based questions. Text-based questions are associated with an individual's personal information which can be shared with a third party impersonator for impersonation attacks. The next chapter presents a simulation study to evaluate students' ability to share text-based questions with a third party impersonator.

Chapter 8 (Impersonation and Text-based Challenge Questions) presents a third study to investigate impersonation attacks when pre-defined text-based challenge questions are implemented. This study examines the influence of sharing text-based questions with a third party impersonator. It investigates how the number of questions shared and database size affect the success of an impersonation attack. This chapter is detailed with the purpose, research questions and relevant hypotheses, impersonation abuse case scenarios, study method, details of participants, and study phases. Finally, it reports the findings of an impersonation abuse case scenario to test the study hypotheses. Text-based questions are associated with an individual's personal information and students are required to register their answers during the learning process. This introduces an additional process and also provides an opportunity for students to memorise or store these questions for sharing with a third party impersonator. In order to address this, the next chapter introduces non-intrusive dynamic profile questions.

Chapter 9 (Impersonation and Dynamic Profile Questions) presents study four, which proposes dynamic profile questions. These questions are non-intrusive and dynamically created during the learning process, which does not require students to register their answers. This chapter investigates impersonation attacks via email and phone when dynamic profile questions are implemented. It reports the usability findings and the outcome of impersonation abuse case scenarios via phone and email. Dynamic profile questions influence impersonation via email or phone during an online examination where the response time factor is implemented.

The previous studies were conducted in simulated and real online courses, inviting students to be stakeholders in the process. However, it is important to involve online programme tutors as significant stakeholders. The next study will investigate a focus group study, inviting online programme tutors to provide feedback on the research problems and the proposed solution.

Chapter 10 (Focus Group with Online Programme Tutors) reports feedback obtained from a focus group session with online programme tutors as the experts. Given their expertise in online learning, teaching and assessment, online programme tutors have a central role in an online learning and examination context;

therefore, it is important to understand their views on threats and prevention methods. They were invited to provide their views on potential threats, authentication methods, usability and applicability of the proposed challenge question approach against identified threats with a focus on collusion attacks, and remote proctors and secure examination browsers.

The online programme tutors agreed to the use of dynamic profile questions and remote proctoring for the reduction of impersonation and abetting attacks. However, it is anticipated that students may still be able to share information related to dynamic profile questions with a third party impersonator before an online examination session. The next chapter will report an impersonation abuse case scenario in a proctored exam.

Chapter 11 (Dynamic Profile Questions and Proctoring) presents study six, which implements content-based dynamic profile questions in an online course and simulates an impersonation abuse case scenario, where a student shares the learning experience with a third party impersonator before an online test by means of email, phone, instant messaging or face-to-face meeting. The third party attempts to impersonate a student in the presence of a live proctor.

This chapter concludes the research work investigated in this thesis. The next chapter reports the summary of conclusions developed from the research work conducted in this thesis.

Chapter 12 (Conclusion) presents the conclusions which reflect the objectives introduced in chapter 1 and answers the subsequent research questions. Additionally, this chapter summarises the main contributions of the work, and addresses the future outlook of securing online learning and examination environments.

1.5 Summary

This chapter provided an introduction to this work. The terms ‘online learning’ and ‘examinations’ were introduced in the context of this research. Online learning is a modern version of distance learning, where teaching and learning are performed remotely with the use of technology and the Internet. In the context of this work, online examinations are assessments which are performed remotely in and out of classroom settings with no face-to-face interaction. The aims and objectives of this research were identified. Four research questions were created in order to achieve the research aims and objectives.

In order to provide the rationale for this research, a relevant literature survey is conducted, which is presented in the following chapter.

2 Literature Review

This chapter presents a literature review on information security, authentication, and usability of authentication methods, which provides the rationale and basis for this thesis. This includes a literature review of information security with particular interest in identifying system assets and threats in order to inform security goals and, consequently, protect assets. The chapter also explores the security of online learning, focusing on threats to online examinations. Moreover, it provides a review of authentication in online learning with a focus on the challenge question approach. Finally, it addresses the need for usability relating to information security, describing usability attributes that constitute usability in software systems. In addition, the final section describes the influence of usability on security of authentication approaches.

2.1 Security

Computer security is a process of protecting computer software, hardware and networks against harm (Schechter, 2004). In this context, harm implies a loss of desired system properties such as confidentially, integrity and availability. The application of computer security has a wider scope, including hardware, software and network security. The focus of this research is application-level security, which falls into the information security context described in the following section.

2.1.1 Information Security

"Information security is the protection of information and systems from unauthorised access and use, disclosure, disruption, modification, perusal, inspection, recording or destruction, in order to meet the information security principle" (Khalfan, 2004). The concept of information security is formed from the recognition that "information" is valuable and that it requires protection (Tajuddin et al., 2015). According to ISO/IEC 27002 (2008), it is the protection of information from a wide range of threats that ensures business continuity and minimises business risks. The concept of business can be applied in any commercial or non-commercial context, such as online learning. Stallings (2007) defines it as "a collection of related components: assets, threats, goals and preventive measures designed to protect a system." Stallings' definition is helpful in identifying assets in a business context, describing and detailing various types of threats, and evaluating security goals to propose countermeasures against any potential threats.

Gollman (2010) states that security is the protection of assets against unauthorised access. Pfleeger and Pfleeger (2002) define assets as software, hardware and human resources that support the operational aspects of a system. Gollman (2010) indicates that the identification of assets is relatively easier than their valuation, which is closely related to a business context. According to ISO/IEC 27001 (2005), an asset is anything that has value for an organisation. A common view from the above discussion indicates that assets can be classified into tangible (i.e. hardware, human resources and infrastructure) and non-tangible assets (i.e. software, skills, reputation, data and information). It is vital for an organisation to protect tangible and non-tangible assets against all threats. These “assets” have value not only for an organisation but also for attackers (p. 10, Faily, 2011). Stakes for attackers may vary depending on their nature. In the context of online learning, course content and examinations are identified as valuable assets. Any breach of security properties, i.e. confidentiality, integrity and access, may cause harm to learning and examinations.

According to ISO/IEC 27002 (2005), protection of assets from all possible threats is unattainable; therefore, security requirements, i.e. confidentiality, integrity and accessibility, are often derived by assessing their risks. Risk is the probability of a particular adverse event during a stated period of time, or resulting from a particular challenge (p. 2,Warner, 1992). A Royal Society Study Group report (1983) classified risk into objective and perceived risks. Hansson (2010) states that objective risk is the probability of harm occurring which can be measured and described scientifically; perceived risk is based on subjective assumptions about future events. Risk comprises a combination of assets, threats and vulnerabilities (ISO/IEC TR 13335-1, 1996, p.5-10), and it is essential to identify threats and vulnerabilities (Jung et al., 1999). The above discussion suggests that risk is indicative of a threat, danger or hazard, and provides an estimation of the likelihood of a threat exploiting vulnerability and compromising assets.

Threat and vulnerability are closely related with the concept of risk. According to ISO/IEC 27002 (2005), a threat is a potential cause of an unwanted incident; a vulnerability is a weakness of assets that can be exploited by threats. To protect a system’s assets, it is important to understand its threats. Assets of an information system may attract a number of threats, which may target the security. The security goals are commonly referred to as Confidentiality, Integrity and Availability (CIA), which ensure that assets are not compromised by threats (Gollmann, 2010). The BS7799/ISO17799 (1999) standards describe CIA as:

1. **Confidentiality**: ensures that assets are restricted to authorised users only.

2. **Integrity**: ensures that assets are only altered by authorised users.
3. **Availability**: ensures that the system is available and operational.

A compromise in the CIA security goals may compromise secure assets. A threat is the potential for misuse or abuse that will cause harm or abuse assets (Haley et al., 2004). In security taxonomy, threats that exploit vulnerabilities of assets are: interception, modification, interruption and fabrication (Apampa et al., 2010b), which are described below:

1. **Interception:** An attack on confidentiality, when an unauthorised user gains access to an asset.
2. **Modification**: An attack on the integrity of assets, when an unauthorised user gains access and alters an asset.
3. **Interruption**: An asset of the system is attacked and made unavailable to render service.
4. **Fabrication:** An attack on authenticity, occurring when an unauthorised user creates a counterfeit asset.

Authentication is an addition to the three primary security goals; it may or may not be included in the taxonomy (Stallings, 2007). It has been a widely researched area and seen as the main challenge for online examinations. Apampa (2010b) states that the security of online examinations faces two challenges, i.e. identity management and authentication. In an online test, a student is required to prove that "he is who he claims to be". Identity management and authentication are closely interrelated and embedded in many approaches (Schultz et al., 2001). The authentication goal is to verify the claimed identity of a user. It has a central role in prevention against identification attacks.

2.1.2 Security in Online Examinations

The growth in the use of online learning in higher education has been documented and reported in many studies (Buzzetto-More, 2008, Eshet-Alkalai and Geri, 2007, Allen and Seaman, 2007, Koohang et al., 2009, Analysts, 2012). It has attracted a considerable level of research focus on developing and delivering secure, efficient and effective online learning systems. However, researchers have also raised concerns about the security of online learning environments. Watson and Sottile (2010) indicate that there is an increasing demand for online learning, but with it there are rising concerns for the integrity of the online examination process.

Security is about the protection of assets (Gollmann, 2010) and the online examination is an important asset in the context of online learning. In a recent study, Miguel et al. (2015b) state that among the learning activities developed in most educational institutions, online examination is an essential component of a course, which enables educators to assess online students. The lack of security in such examinations is reported in a number of research studies (Percoco and SpiderLabs, 2014, Apampa et al., 2009, Levy and Ramim, 2007). Due to the high-stake nature of examination, security is based on the assurance that only a legitimate student can gain access to an online test. However, remote access and the absence of proctoring provide extra freedom to students when taking their online exams. Hence, the security goals are an essential factor in terms of countering security threats.

Based on the definition of assets above (see section 2.1.1), online examination is an important asset, and a security threat compromising an online learning system may cause potential harm (Apampa et al., 2009). This threat may come from intruders motivated for various reasons or a legitimate student with valid credentials. Harm from a legitimate student is seen differently than harm from an attacker with malicious intentions. A student is motivated by various factors to boost his grades without causing any harm to the online examination. However, the fair process of assessment is compromised, which is also an asset as discussed earlier. The information security literature review in the previous sections described security goals as confidentiality, integrity and availability, and ensuring that assets are not compromised by threats. In the context of this study, the CIA relationship may be written as follows:

- Online examinations to be accessed by authorised users *(Confidentiality).*
- Online examinations to be modified by authorised users (*Integrity)*.
- Authorised students may access online examinations in a timely manner (*Availability)*.

To contextualise security goals to the current research, an impersonation attack is “unauthorised access” and “modification by unauthorised users”. The following scenario describes how the violation of security goals occurs when such attacks are perpetrated:

> *A student shares his/her login and password with a friend to help with an online quiz which is part of the summative assessment. The friend logs in using the shared credentials to impersonate the student at a scheduled time and takes the online quiz.*

If the above chain of events occurs, the security is breached and the threat scenario outlined is realised. To understand the potential harm a security breach may cause, it is important to understand the likelihood and nature of a threat. Identifying threat scenarios may help us understand what can go wrong if a scenario occurs.

Kritzinger (2006) states that various online learning activities are open to abuse and security threats. These include unauthorised access and alteration to course content, fake content submission to students, unauthorised access and copying of submitted assignments, unauthorised changes or removal of submitted assignments, changes or removal of course grades, unauthorised access to online exams, unauthorised changes or removal of online exams, collusion and receiving help during online exams, destruction of online course or database, denial of service attack (DDoS) on the online learning server, and stealing and misuse of a student's online authentication information (Kritzinger et al., 2006). McGee (2013) identifies intrusion, collusion, deception and plagiarism as major information security threats. The observations of Kritzinger et al. and McGee are valid; however, the description of collusion can be explored in more detail. With the advent of technology such as the evolution of smart phones, and availability of 3rd and 4th generation Internet, chat applications and instant messaging on smart phones can be used by students to exploit holes in security. In collusion attacks, students may involve third parties to assist with their online examination in various ways, which are described in the next chapter (see Chapter 3). Such attacks are motivated by students' desire to perform well and obtain high grades, as well as peer and social pressure. After identifying assets and potential threats, the security goals are formed to prevent:

- an incorrect or illegal student from taking an online examination
- abuse of authentication details
- denial of service attacks against online examinations

The security goals described above ensure that only the correct student takes an online test. Within the context of this thesis, the goal of information security is to investigate threats to online examinations and understand the influence of authentication methods to counter these threats.

2.2 Authentication

Authentication is a widely used first line of defence in the security of information systems (Furnell et al., 2000). It is a component of security taxonomy that confirms the identity of remote users. Many authentication methods are implemented to determine whether someone is who they claim to be (Marcel and Del Millan, 2007). Burr et al. (2006) state that it is a process of establishing confidence in user identities presented to an information system. Researchers share a common view that authentication implements the identification of users. The problem with this view is that some methods are unlikely to ensure identification in certain threat scenarios. As an example, a password method cannot identify an attacker who logs into a system as a legitimate user with a stolen password (Chun-Li et al., 2001). This observation is helpful in understanding that some approaches cannot prevent identification theft and masquerading.

The National Institute of Standards and Technology (NIST) guidelines suggest that authentication is a challenging issue for network applications, including the Internet and web-based systems, when the process involves remote users (Burr et al., 2006). The security model for authentication has evolved and been reviewed in the light of an evolving threat model over time (Anderson, 2010). However, certain threats are unreported or under-represented in this model, which is exploited by attackers. Schneier (2011) argues that security threats are always the same whereas security tools are just not as effective as they were in the past when initially developed. Overall, the literature review suggests growing threats to remote authentication in online environments and recommends a continuous evaluation of security goals and threats.

Many authentication features have been developed to secure online learning and examinations, which are discussed in the following section.

2.2.1 Authentication in Online Learning and Examinations

Authentication has an important security role in online learning and examinations, particularly in the absence of visual identification. Conole and Oliver (2006) state that a lack of face-to-face interaction with students increases the challenge of knowing that “they are who they say they are”. Alwi and Fan (2010) studied a threat analysis of online learning systems, which is helpful in analysing information security threats. They identified authentication of students as a leading challenge. Moini and Madni (2009) consider this to be a major security concern for stakeholders, which is a reason why many educational institutions prefer supervised examinations over the use of a remote online examination. The consequences of weak and vulnerable authentication approaches can raise the concerns of stakeholders. The prevailing views of researchers indicate this as a reason for potential threats to the high-stake online examination process.

Learning and examinations are delivered online in a web-based environment, which is open to a high number of security threats (Kritzinger, 2006). Collusion, plagiarism and intrusion were identified as major concerns. Kritzinger proposed identification and authentication as an information security goal to prevent these threats. Paullet et al. (2014) state that online learning and examinations provide many benefits to educators, administrators and students, which sometimes overshadow the need to enforce student identities and academic integrity. Paullet et al. argue that this could potentially introduce the risk of collusion, where another student impersonates the one registered for the course and completes assignments in their place. This view is insightful because the identification and presence of students in online environments is often reliant upon authentication mechanisms. Absence of visual identification is a common cause for concern.

The literature review also suggests that some risks are associated with incentives for the attacker. For example, stakes for a user of an online examination are different than an online bank, i.e. *"it is unlikely for a user to share login identifier and password for his online bank account due to a higher risk, however, a student may be willing to share login details for his online course with another student to complete his assignment due to a relatively lower risk"* (Bailie and Jortberg, 2009).

The traditional authentication methods are implemented using human factors based on "*what you know*" (Huiping, 2010),*"what you have"* (Deo et al., 1998) and *"what you are"* (Moini and Madni, 2009). These methods are discussed below:

1. **Knowledge-Based Authentication (KBA)**: This method is based on the concept of *"what you know"*. These features employ the method of verifying users by matching one or more secrets supplied by an individual against data associated with the same individual (Chen and Liginlal, 2008). It is a widely accepted approach because of its simplicity, availability and accessibility on a wide range of platforms. It is a low-cost and preferred authentication method implemented in the majority of secure systems due to simple administration requirements (Hafiz et al., 2008).

   The KBA method implements both secret and shared knowledge. Secret knowledge is only known to a user, such as PIN numbers, pass phrases and passwords. Shared knowledge relates to an individual's personal information, which may potentially exist in the public/friends domain; for example, personal questions related to date of birth, place of birth, best friend, academic qualification and last school attended. The login-identifier, password and challenge question methods are commonly known as knowledge-based features.

2. **Object-Based Authentication (OBA)**: This method is based on the concept of *"what you have"*. This approach verifies users' identification based on the possession of physical objects such as a smart card (Sandhu and Samarati, 1996). In day-to-day life, physical objects are often used as proof of identification, e.g. ID cards, staff card, passport and driver's licence. The OBA feature utilises an electronic chip and embedded magnetic strip, which are programmed. This approach implements various types of token-based technologies, e.g. smart card (Smart Card, 2003), magnetic strip card (Brown and Chatelain, 2007) and proximity card (Mandel et al., 2004). Special purpose card-reading devices are required for the implementation of this method.

3. **Biometrics Authentication:** This method is based on the concept of *"what you are"* or *"what you do"* (Ortega-Garcia et al., 2004). It performs authentication and identification using an individual's physical or behavioural characteristics (Asha and Chellappan, 2008). It frees users from remembering passwords and carrying cards, as the user is the key for identification (Gil et al., 2010). These features are based on an individual's physical characteristics, e.g. fingerprints, video authentication, face recognition and audio recognition. Some biometric features are based on behavioural characteristics such as keystroke dynamics, mouse-use characteristics and signature recognition (Gamboa and Fred, 2004).

The authentication features above provide different levels of security assurance, cost effectiveness, usability, accessibility and prevention against threats to online examinations. This research investigates the use of a challenge question approach for authentication of students in online examinations, which is described below.

2.2.2 Challenge Questions Authentication

Challenge questions represent a knowledge-based feature, which is widely seen as a credential recovery technique (Just and Aspinall, 2009a). This is a knowledge-based feature and relies upon personal information associated with individuals, e.g. mother's maiden name, favourite holiday destination, best friend's surname, etc. The conventional challenge questions use information which could be a "*shared secret"*. This approach has developed and evolved over the years. Ozsoyoglu and Chin (1982) proposed a question-and-answer-based system for the security of a statistical database in the early 1980s. Zviran and Haga (1991, 1990) identified question-and-answer-based cognitive or associative passwords that were memorable and difficult to guess. However, this method became popular when used by leading email providers such as Yahoo, Google, Microsoft and AOL (Schechter et al., 2009). These service providers use it for authentication when a user needs to reset or retrieve lost credentials.

Challenge questions is a cost-effective method, which minimises the administration cost when a user needs to recover his/her lost credentials (Just, 2004). However, some studies have reported usability and security associated issues with this method. Just and Aspinall (2009a) studied a usability and security analysis of this method using 73 participants. The authors reported that, of the 117 questions asked in their study, 88 (75%) answers were recalled exactly, while 21 (18%) had different punctuation/capitalisation (typically performed when registering answers). 8 (7%) of the answers were completely different, citing a memorability issue in a span of 28 days. The authors identified that the memorability issue of 8 (7%) was higher than the password memorability of 4.28% reported by Florencio and Herley (2007). In the security evaluation, participants believed that 88% of the questions would be “somewhat difficult” for a stranger to answer; however, this reduced to 46% when considering the case of a friend or family member. To address the memorability, Renaud and Just (2010) proposed associative picture-based cues with multiple choice answers. The authors of the study reported a 13% increase in memorability. Schechter et al. (2009) evaluated the security of challenge questions used by four mail service providers – Google, Yahoo, AOL and Microsoft. The authors of the study reported that acquaintances of participants were able to guess 10% of their answers and 13% of answers could be guessed within five attempts. The authors state that participants forgot 20% of their own answers within six months.

The security and usability of the challenge question approach is reliant upon the quality of question design. In their study, Griffith and Jakobsson (2005) attributed security and usability issues to weak question design, including memorability, availability of information on the Internet or among close acquaintances, and lack of clarity. Rabkin (2008) discovered that a significant number of questions were either insecure or difficult when he analysed administratively chosen challenge questions. Schechter et al. (2009) reference Sarah Palin (the Republican vice-presidential candidate in the 2008 US election), whose Yahoo email account was compromised, as the answer to her secret question had been figured out (Bridis, 2008). The user of a password tends to memorise the password for later use; however, challenge questions are based on information a user would already know. This information relating to certain questions may consist of “shared secrets” and be known to family and friends. Such questions have weak security and may be vulnerable to guessing attacks, as in the case of Palin. There is a common view among researchers relating to guessing and memorability of questions with design flaws. For example, “date of birth” is common knowledge in a family and friends domain, and could also be found from social media websites such as Facebook. This discussion is helpful in understanding that some challenge questions may be weak against guessing attacks by family, friends and acquaintances.

Several banks utilise a dual text credential using the challenge question approach (Just and Aspinall, 2012). This method is implemented by many banking websites in verifying a customer’s identity. Rabkin (2008) investigated 15 online banks that implemented this approach of customer verification. He identified that questions used by these 15 institutions were classified into three categories. Six institutions used personal challenge questions, coupled with a username or “Social Security” number and email verification. Four institutions used both personal challenge questions and account details, such as account number or credit card number and a PIN number. Two institutions relied only on account numbers and PINs. Rabkin inferred that these questions were difficult to guess and may not be easy for an attacker to learn. The majority of financial institutions implement challenge questions as a second factor used alongside another option in order to deter any guessing attacks. Bruce (2007) states that challenge questions are adopted as a low-cost method by many financial institutions. Bruce proposed using a structured approach to the design of challenge questions with a focus on usability, uniqueness, integrity, affordability and accuracy. He also suggested that asking multiple questions during the authentication process can improve overall security, but some residual risk will remain.

2.2.2.1 Challenge Questions in Online Examinations

The challenge question approach in an online examination context was initially proposed by Jortberg and Baile (2009). They suggested the use of questions from a US consumer database for the identification of online students. A prototype involving students from the National University of America and Acxiom Corporation, acting as a third party database, was piloted (Jortberg, 2009). The data of 183 identity verification instances was reported, where an average of 8% either failed or aborted the verification process. Barker and Lee implemented video identification and chat verification from a student information database for identity verification (Barker and Lee, 2007). The main objective of their research was preventing impersonators from logging into an online examination.

This was a usable approach. However, the implementation of challenge questions from a third party database has other issues, i.e. integration, data protection, accessibility, bandwidth usage and tariff. With the rapid growth of the Internet and increasing popularity of online learning, it has been used by students from all over the world. One of the key challenges of using a US consumer database is the wider implementation for students outside the US consumer market.

This thesis will explore the idea of using a challenge question approach with no reliance on a US consumer database. Discussion in the previous section suggests that this approach faces many usability issues. The following section describes the importance of usability and how it applies to this research.

2.3 Usability

Usability is an important quality of software systems. It is a measure of useful interactions between a system and target users in a specified context. The word usability emerged to replace the term “user-friendly” in the mid-1980s and was adopted by the software industry in 1990 (Bevan, 1995). The body of knowledge is large and includes various perspectives, from usability engineering (Nielsen and Hackos, 1993) to more context-oriented approaches (Beyer and Holtzblatt, 1997). The literature review suggests a consensus regarding the definition; however, there are different approaches to measure usability. Multiple definitions for usability have been developed in numerous influential studies (Shackel, 1991, Nielsen and Hackos, 1993, Hix and Hartson, 1993, Preece et al., 1994, Wixon and Wilson, 1997, ISO9241-11, 1998, Shneiderman and Ben, 1998, Constantine and Lockwood, 1999, Seffah et al., 2001). The authors in these studies tried to define usability attributes that can be measured to compose usability. These attributes are described in the following section.

2.3.1 Usability Attributes

Usability is not a single component, but multiple attributes applied to a system in a specified context. Table 2-1 shows a selection of such attributes defined by researchers over time to measure usability. Description of these definitions and attributes is given below.

Table 2-1 Overview of Usability Attributes (Pedersen, 2010)

ISO 9241-11 (1998)	Nielsen and Hackos (1993)	Quesenbery (2010)
Efficiency	Efficiency of use	Efficient
	Learnability	Ease to Learn
Effectiveness	Memorability	Effective
	Errors	Error Tolerant
Satisfaction	Satisfaction	Engaging

Nielsen is one of the first authors to define usability measurement scales. Besides designing 10 heuristics, he identified the following attributes (1993):

- **Learnability:** measured by how easily a system can be learned and utilised, so users can start using it in a minimal amount of time.
- **Efficiency:** another attribute that measures the time a user needs to accomplish tasks after he or she has learned how to utilise a system.
- **Memorability:** measured by how easily a user can remember a system or process if they use it again after leaving it for an extended period of time.
- **Errors:** an attribute that measures the rate of errors that users make during their use of a system. These errors, if they exist, must be minimal and easy to recover from.
- **Satisfaction:** measures users' satisfaction.

Quenesbery (2010) defined the following usability attributes, also known as the 5 Es:

- **Effective**: how complete and accurate the work is.
- **Efficient**: how quickly the work can be completed.
- **Engaging**: how pleasant and satisfying the product interface is to use.
- **Error tolerant**: how effective the product is in preventing errors and how it can help the user to recover from mistakes.
- **Easy to learn**: how well the product supports learning throughout its lifetime of use.

According to ISO/9241-11 (2003), usability is *"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"*.

- **Efficiency:** a measure of completion time for each separate task and sub-task (Seffah et al., 2001). A system is considered efficient if users are able to complete tasks in a reasonable time.
- **Accuracy:** an important usability factor that indicates a degree of completeness with which users achieve a specified task in a certain context (Seffah et al., 2001).
- **Satisfaction:** reflects the desirability of a product. It determines the extent to which a user finds a product to be effective and efficient.

Jacko (2012) states that usability is closely related to a system's context of use. The ISO/9241-11 definition above encapsulates this contextual nature. Table 2-2 further describes the ISO/9241-11 standard. Figure 2-1 shows a relationship between different usability measures.

Table 2-2 ISO 9241 Usability definition

Concept	Description
Product	Equipment i.e. hardware, software and material for which usability is to be evaluated
User	Person who interacts with the product
Goal	Intended outcome
Effectiveness	Accuracy and completeness with which user achieves specified goals
Efficiency	Completion time in which user achieves specified goals
Satisfaction	Positive attitude towards the use of a product
Context of use	Users, tasks, product, i.e. hardware, software and materials, and the physical and social environments in which a product is used.

The figure represents a "Work System", described in the ISO standard, i.e. a system consisting of users, equipment, tasks, and a physical and social environment, for the purpose of achieving particular goals (ISO/ISO9241-11, 1998).

The following sections review the user-centred design approach according to this definition, and problems that arise when considering security and usability.

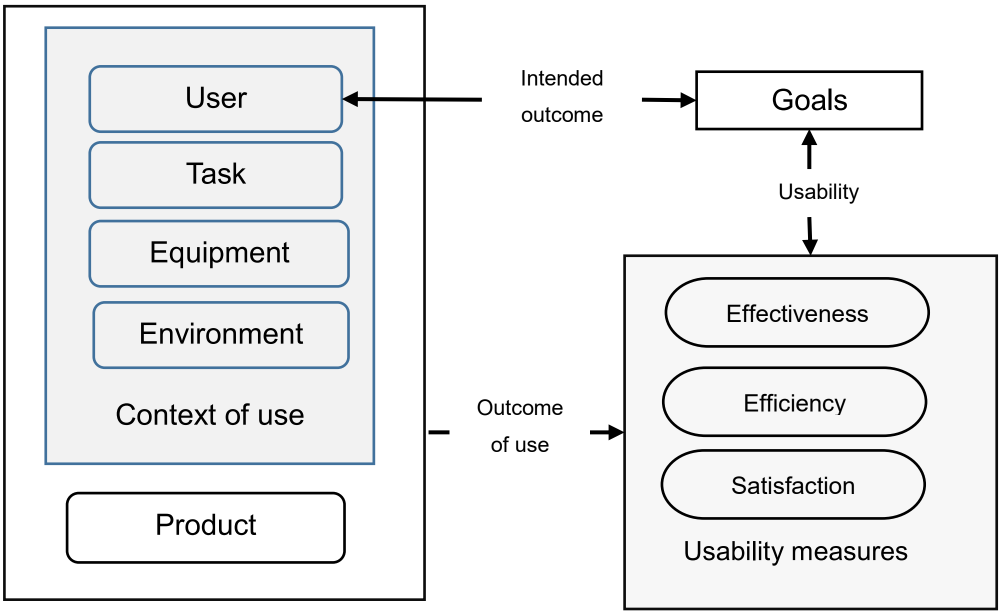


Figure 2-1 ISO 9241-11 Usability Framework

User-Centred Design

The design principle adopted by most usability professionals is known as User-Centred Design (UCD). The term was first used by Donald Norman (2013), who designed this as *"a philosophy based on the needs and interests of the user, with an emphasis on making products usable and understandable"*. The UCD is a prevalent usability paradigm for many systems including software. The principles of UCD place increased focus on users when developing products, in order to ensure that they are useful and usable (Shackel, 1991, Gould and Lewis, 1985, Dumas and Redish, 1999, Eason, 2005). Gould and Lewis recommended three design principles:

- **Early focus on users and tasks:** encourage designers to directly contact users. The authors encourage designers to “interview”, “review” and “verify” design with users.
- **Empirical measurement:** emphasises empirical evaluation of actual behavioural usability.
- **Iterative design:** a cycle of design, test, measure and redesign should be carried out and repeated as necessary.

The principles proposed by Gould and Lewis are similar to Human-Centred Design, described by ISO/IEC 13407 (Jokela et al., 2003):

- the active involvement of users and a clear understanding of user and task requirements
- an appropriate allocation of function between users and technology
- the iteration of design solutions; and
- multi-disciplinary design.

2.3.2 Usability of Authentication Methods

Many researchers argue that secure systems are compromised through human errors and that "ease of use" is essential in order for users to behave securely (Adams and Sasse, 1999, Yee, 2002, Poulsen, 2000). Sasee et al. (2001) state that security techniques are only effective when implemented correctly. They suggest that security designers should understand user behaviour in order to build usable and secure systems. Sasee and Flachais (2005) argue that usability and security mechanisms can only offer the intended protection if used correctly. They stressed the importance of usable systems for the implementation of adequate security: *"when users fail to comply with the behaviour required by a secure system, security will not work as intended."* Braz and Roberts (2006) state that the usability of security systems has become a major issue in the research on efficiency and user acceptance. They expressed their concerns regarding a trade-off between security and usability when both are essential in the authentication process.

One possible solution in the implementation of usability is security awareness and training of users; however, this could not be a substitute for a usable authentication method to fill the gap between a secure system and a user's behaviour (Krug, 2005). Krug suggests that security training and advice require additional resources, and this is infeasible in an online context. Herley (2009) identifies that users tend to ignore security advice and prefer an alternative security approach with minimal requirements.

Schultz et al. (2001) state that the key security controls that exist today apply to identification and authentication of a user. Braz and Robert (2006) state that usability is essential in the design of authentication methods. They argue that these methods may fail to protect digital assets if users are unable to use them correctly.

As an example, a strong password or a challenge question may be more secure but less usable as it may be difficult to memorise.

There is increased demand for a secure and usable authentication method. Designing a secure authentication mechanism that is usable enough to be effective is a specialised problem, and interface design strategies that are effective for other software will not be sufficient to solve this problem (Whitten and Tygar, 1998). Authentication provides a gateway to many secure systems and, therefore, it is successful when security and usability are aligned. Di Raimondo and Gennaro (2005) state that authentication is the main goal when security is implemented, whereas usability is the main goal of the system's implementation. Both are the main drivers to user acceptance of a system. According to Braz and Robert (2006):

> *"Usability becomes a strategic issue in the establishment of user authentication methods."*

Many research studies (Cranor and Garfinkel, 2005, Dustin et al., 2002, Just and Aspinall, 2009c, Braz and Robert, 2006) identified security and usability as major success factors for authentication approaches. Therefore, usability evaluation is an important aspect of designing a secure authentication method.

2.4 Summary

This chapter provided a literature review of information security, threats to online examinations, authentication, usability and the challenge question approach. Information security is a collection of related components: assets, threats, goals and preventive measures designed to protect a system where assets are considered to be anything that has value for an organisation. Security is about protection of assets. The online examination is an important component of the learning model and a valuable asset. However, this faces the numerous security threats reported in the literature. Collusion is identified as one of the major security threats, where students are assisted by third parties in completing their online tests. Remote authentication and lack of visual identification of students are some of the reasons for collusion attacks.

Jortberg and Bailie (2009) proposed challenge questions from a US consumer database for the authentication of students in online examinations to influence collusion attacks. Their approach is not feasible for students who are not registered in the US consumer database, including international students. Moreover, some research studies reported usability and security issues such as memorability, and guessing by friends and families when using the challenge questions. Many online banks and email service providers still prefer challenge questions for recovery of users' lost or forgotten credentials in order to reduce additional administration costs. In the literature review, many studies suggested the usability evaluation of authentication methods and considered this as an integral part of the security paradigm. The ISO/9241-11 standard identified efficiency and effectiveness as the main attributes that constitute a usable authentication method.

The review of information security suggests that a detailed description of all threats is important for the design of a secure authentication method. Different forms of security threats to online examinations are described in the following chapter.

3 An Overview of the Research Problem

The previous chapter identified weak authentication as one of the reasons behind security threats to online examinations. This chapter explores different types of security threats in order to substantiate a theoretical underpinning for this thesis. The purpose of this chapter is to locate evidence of threats in the literature and also identify new, evolving threats using abuse case scenarios. This includes an overview of the factors that motivate students and intruders to attack online examinations. It provides a review on intrusion and non-intrusion attacks, including collusion of various types. Finally, it provides the justification and need for this research in light of the literature review.

3.1 Threats to Online Examinations

A threat represents the potential for misuse or abuse that will cause harm or exploit assets (Haley et al., 2004). In security taxonomy, threats which exploit vulnerabilities of assets are interruption, interception, modification and fabrication (Apampa et al., 2010b). Based on the definition of assets described in Chapter 2, an online examination is considered a critical asset in the context of online learning. It is delivered in a remote web-based environment, which is open to a wide number of threats (Kritzinger, 2006). In an attempt to mitigate them, it is essential to understand and identify the nature and details of all threats. Miguel et al. (2015a) state that security threats in online examinations can be approached in two stages, i.e. threats are analysed, and then recommendations are introduced and discussed in order to cope with the detected threats.

Security threats may come from different sources including intruders and genuine students, which are motivated by a variety of objectives. It is anticipated that stakes for intruders in online examinations are potentially not as high as online banks with deposit transfer capabilities. However, stakes for students in such examinations are high. Therefore, this work focuses on security threats sourced from students. These threats are motivated by varying objectives. Many studies agree that cheating contributes to a large number of them. It is reported by researchers in all forms of education (Aggarwal et al., 2002, Bowers, 1964). Research on cheating dates back to the 1930s (Strang, 1937). More work was published and reported regarding cheating in the 1960s and 1970s (Wrightsman Jr, 1959, Bushway and Nash, 1977). Bowers (1964) identified the involvement in cheating activities of 75% of students from 99 colleges and universities in the US. Thirty years later, McCabe and Pavela

(1997) repeated the study and reported the involvement of 70% of students in cheating. McGee (2013) states that although cheating is a priority in all environments, it is a particular concern for courses offered in remote online learning environments.

For example, numerous studies (Vician et al., 2006, Olt, 2002, Colwell and Jenks, 2005, Wielicki, 2006, Jung and Yeom, 2009, McMurtry, 2001) have reported that online learning offers more opportunities for cheating than traditional face-to-face examinations. Chiesel (p.330, 2009) reported that 64% of university professors perceived cheating in online examinations to be easier. In another study, King (2009) reported that 73.6% of students perceived that cheating in online examinations is easier compared to traditional face-to-face exams. Pillsbury and Harmon (2004, 2010), in their studies, indicated that unethical conduct has intensified in online learning platforms, due to more opportunities for cheating as a result of the use of technology and the Internet. The lack of physical interaction or monitoring during learning and examinations is a security risk which increases opportunities for cheating.

However, some researchers indicate that there is no difference in cheating as a direct result of the type of examination environment (McNabb and Olmstead, 2009, Spaulding, 2009). McNabb surveyed faculty members regarding their perception of cheating in both online and face-to-face examinations. The majority of faculty members did not believe that there was a difference in cheating between the two environments. Spaulding (2009) presented a similar literature survey, reporting no difference in cheating between the two environments. McGee (2013) argues that much of the research about cheating is based on self-reports or students' perceptions of academic dishonesty. Spaulding (2009) states that it is difficult to capture comprehensive rates of cheating in either environment.

Students often cheat in online examinations to qualify or enhance their grades. This motivates a number of unique security threats, which may be classified into multiple categories including non-intrusion and intrusion. Non-intrusion threats are further classified into collusion and non-collusion threats. Collusion attacks happen when students invite third party impersonators or abettors to help with online examinations. Intrusion attacks are performed by cyber attackers, cybercriminals and hackers. In general, all the above threats are open-ended and widespread due to access on the Internet, and a weak authentication mechanism. An overview of potential application-level threats to online examinations are shown in Figure 3.1 and described below. The threat classification does not cover network or server/database side attacks:

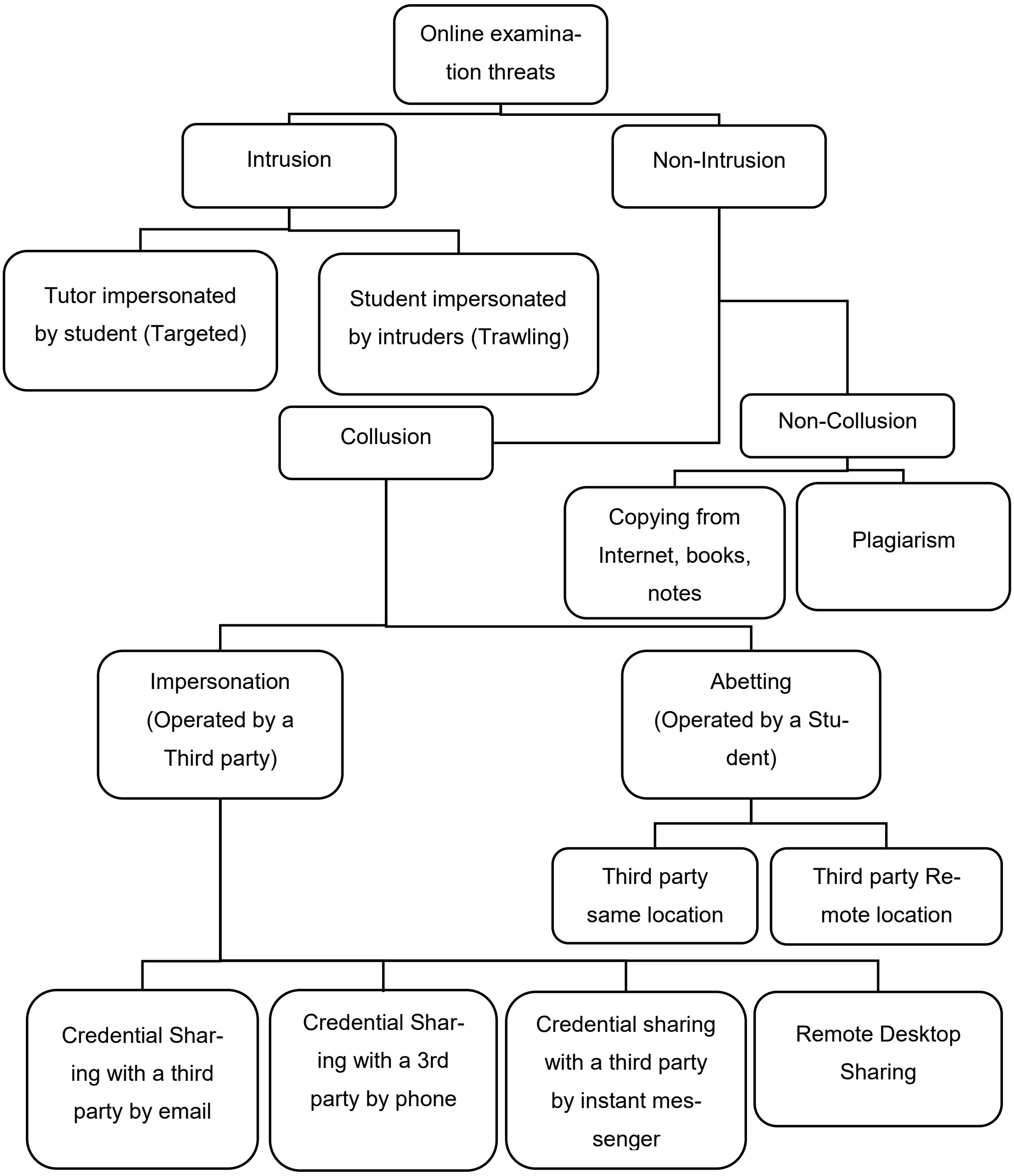

Online examination threats
Intrusion
Non-Intrusion
Tutor impersonated by student (Targeted)
Student impersonated by intruders (Trawling)
Collusion
Non-Collusion
Copying from Internet, books, notes
Plagiarism
Impersonation (Operated by a Third party)
Abetting (Operated by a Student)
Third party same location
Third party Remote location
Credential Sharing with a third party by email
Credential Sharing with a 3rd party by phone
Credential sharing with a third party by instant messenger
Remote Desktop Sharing

Figure 3-1 Overview of Threats to Online Examinations

3.1.1 Intrusion

Unlike an online bank with deposit transfer capabilities, a university with an online programme is normally not a target for an attacker looking to gain access for the purpose of financial gain. However, there are still concerns regarding intrusion in online examinations (Bailie and Jortberg, 2009). Intrusion attacks are carried out with malicious intentions and classified as i) targeted and ii) trawling attacks (Bonneau et al., 2010). In a targeted attack, the attacker possesses information about the user of the targeted account. For example, a student attacking the account of an online tutor would be interested in collecting information about the tutor in order to penetrate his account using different attack methods. These methods include eavesdropping or sniffing (Mir et al., 2011), key loggers (Cordes, 2005), clickjacking (Rydstedt et al., 2010), malware (Christodorescu et al., 2005), dictionary attacks (Pinkas and Sander, 2002) and brute force, i.e. an exhaustive pattern search attack on cryptographic credentials (Schneier, 1999). Other social engineering methods include token theft and surveillance (Perković et al., 2011). By contrast, a trawling attack is performed without any prior information about a user. Intrusion attacks may come from fellow students, friends and cyber criminals using the above methods. Different types of intrusion attacks are described below.

3.1.1.1 Student Impersonated by Intruders (Trawling)

In this type of attack, an attacker impersonates a student in an online examination without his or her knowledge (Kumar et al., 2011). Such attacks are deliberate and may come from cybercriminals with the intention of revealing confidential information about an online course and examinations (Barik and Karforma, 2012). Hugerat et al. (2013) state that such attacks are carried out to exploit information in an online learning course and examinations without causing any harm to the online learning system. Although the attacker may not destroy data in an online course, this causes distrust and affects the credibility of an online system. Ramim and Levy (2006) conducted a case study on the Knowledgeville University, which experienced a cyberattack in 2002 that resulted in shutting down the server hosting online courses in the middle of the semester. This thwarted the academic work of students and faculty members on the courses. These attacks may come from fellow students, hackers and individuals who sell exam secrets on the Internet to potential students undertaking online courses. A scenario of this type of attack is described below:

> *"A hacker stages an attack by intercepting a student's password. The hacker impersonates the student and gains access to an online examination. The hacker retrieves test questions and sells it online"*

With the advent of new technologies, students are adopting new methods of cheating (McGee, 2013). For example, Krsak (2007) reported a method of cheating where a student starts an online test in order to retrieve all the questions. The student stores the exam questions, aborts the test in order to search for answers and then re-attempts the test. Students or attackers may share or sell exam questions to students on the same course or on the Internet. As an example, a professor of Indiana State University found her test questions for sale on eBay (Hill, 2010). Research studies have reported a new method of cheating known as “braindump”, which is a service that maintains a bank of questions and answers stolen from many online examinations (Paullet et al., 2015, Hill, 2010, Howell et al., 2010). Hackers may attack online examinations to access questions in order to sell or share them with online users and potential buyers such as braindump services. Braindump is an online business that provides students with studying services and often guarantees passing scores. For example, Cramster, Koofers, Study Blue and Course Hero are famous braindump sites, which are considered tutoring websites, where students can review past exams, assignments and projects used in their current courses.

3.1.1.2 Tutor Impersonated by Intruders/Students (Targeted)

Rowe (2004) has shown that students can attempt to log in as online tutors in order to reveal answers to exam questions. He identified that most online tests are protected by short passwords. For example, Blackboard allows passwords as few as eight characters to protect online assessments. Such passwords are relatively simple to circumvent using systematic "cracker" software. Rowe explains that even if the password guessing fails, the student can still use "social engineering" methods that have been successfully used to scam people into revealing their passwords. As an example, "emergency" calls from alleged programming staff or "please change your password temporarily for system testing" requests (Mitnick, 2002). Since few online tutors are security experts, they can potentially fall for many of these scams. A scenario of this type of attack is described below:

> *“A student stages an attack by intercepting an online tutor’s password. The hacker impersonates the tutor and gains access to all questions and answers on an online examination. The student uses questions and answers to complete an online test.”*

Students and hackers can use different methods to gain access to online examinations. For example, password protection can be circumvented by using a key logger (Cordes, 2005), sniffing, clickjacking (Rydstedt et al., 2010), dictionary attacks, token theft, user surveillance, malware (Christodorescu et al., 2005) and brute force login. For example, *sniffer* could decipher message packets of a local-area network used by fellow students or the instructor and thereby read their answers or passwords (McClure et al., 2009). In another example, Rowe (2004) states that students could use spyware to sneak a look at the activities of a person preparing electronic files for an online test.

However, a number of security measures could be implemented to deter intrusion attacks. For example, use of secure authentication, anti-virus, anti-spyware, anti-malware, anti-phishing and security socket layers (SSL certificates) can mitigate many intrusion attacks (Kirda et al., 2006).

3.1.2 Non-Intrusion

Non-intrusion attacks may come from a legitimate student acting individually or inviting a third party collaborator. There are a number of reasons that influence cheating behaviour of students in general. Evans and Craig (1990) identified numerous common reasons including desire for better grades, fear of failure, pressure from parents to do well, unclear instructional objectives and being graded on a curve. Chiesel (p.329, 2009) identified more reasons, including "everyone else is doing it", "it helps me get better grades, a good job, or admitted to graduate school", no fear of being caught, and no fear of punishment if caught. Other studies provided similar reasons, including pressure to succeed, to gain high grades, getting away with something, lack of organisational skills, and fear of failing a course (Faucher and Caves, 2009, Simkin and McLeod, 2010, Heyneman, 2015). Other reasons that students report include a desire to help others, procrastination, need to pass, course difficulty, "it doesn't matter if I cheat", or cheating being easy (Christie, 2003, Owunwanne et al., 2010). Irrespective of the factors that motivate students, there is a common consensus that collusion and plagiarism are major threats to online examinations.

Non-intrusion is classified into two categories, namely collusion and non-collusion. These threats are also identified in the code of practice for the Assurance of Academic Quality and Standards in Higher Education (QAA) for the UK. The QAA identified plagiarism, collusion, impersonation and use of inadmissible material as academic misconduct in online examinations (Quality Assurance Agency, 2006). Such attacks can be carried out in several ways, which are described below.

3.1.2.1 Non-Collusion

A non-collusion attack is a form of cheating which is different from collusion, as it does not involve a third party collaborator. Such attacks happen when a student breaks regulations about what can be used to complete course assignments or exams (McGee, 2013). Some research studies suggest that students in online environments feel "distant" from others, and are more likely to engage in deceptive behaviour (Burgoon et al., 2003, George and Carlson, 1999, Rowe, 2004). This view is incomplete, as regardless of the learning environment, non-collusion threats may be a cause for concern in different modes of assessment. In both face-to-face and online learning environments, students can write assignments, dissertations and course work in their own time.

Bunn, Caudill and Gropper (1992) identified non-collusion as planned cheating which involves copying from books, notes and plagiarising. This is classified further into the following categories:

- **Copying from the Internet, Books and Notes**

  While writing assignments and online tests, students can search for answers from the Internet, books and notes. Such attacks are known as panic cheating, when a student is at loss for answers during an online test. However, planned cheating is more common than panic cheating due to the nature of the online environment (Grijalva, 2006). Underwood and Szabo (2003) reported students using concealed notes to cheat on tests, exchanging work with other students and using the Internet.

  These threats depend upon the type of assessment and examination. In many remote assessments a tutor may not be particularly concerned about students using a book or other source of information. These tests are designed carefully and may need to be completed in an allocated time, which may discourage students from accessing books or the Internet.

- **Plagiarism**

  Plagiarism is copying someone else's ideas and material, from any source, and claiming it as your own work (Dietz-Uhler and Hurn, 2011). The growth of the Internet makes it appealing to copy and paste the writing of others without having to exert oneself. It has been defined in many ways, including theft, deception and misunderstanding (Sutherland-Smith, 2010, Vander Schaaf, 2005).

  Use of the Internet and technology has increased a student's ability to plagiarise written assignments (Scanlon, 2003). Plagiarism has been reported in both online and face-to-face courses. However, with the increasing availability of information online, some researchers believe that it is more prevalent in online courses (Ackerman and White, 2008, Gilmore et al., 2010). Turnitin is a widely used originality software to determine the origin of written work (Turnitin, 2014). It is used by more than 3,000 institutions in the US alone, with 55 million documents submitted for plagiarism checking. However, plagiarism still poses a threat to online examinations.

3.1.2.2 Collusion

A collusion attack is an organised form of cheating which involves collaboration between a student and a third party to solve examination problems. It is a consensual and pre-planned cheating attack by a student. It is an ongoing issue, which has been reported in a number of recent studies (Apampa et al., 2010b, Ayodele et al., 2011, Sonhera et al., 2012). The threat level of collusion in an online examination can be different from other online applications such as banking, where implicit collusion is unlikely to happen as the stakes are different (Rabkin, 2008). This type of threat involves legitimate students and may be challenging to circumvent. However, it can be made harder for an attacker to reach their goal. Schechter (2005) states that the greater the incentive, the more likely it is for an adversary to attack a system. If a student stages an attack on an online test, the incentives are high, i.e. passing an exam, getting a degree or certificate, boosting grades. Wheeler et al. (2003) reported collusion in different disciplines, including medicine. As reported by Carter et al. (2003), collusion is a security risk which can bring into question the validity and credibility of online examinations. In another study, Laubscher et al. (2005) suggest that collusion is one of the major security threats to remote assessment, and proposed remote proctoring to detect impersonation. Howell et al. (2010) reported online services such as *Wetakeyourclass* (2016), *Boostmygrades* (2016) and *UnemployedProfesssors* (2016), in which students pay a fee for someone to take their online classes and exams. It is anticipated that students would be sharing their credentials with these websites, in order that someone else could take their online tests. There are two types of collusion attacks, i.e. impersonation and abetting, which are described in the following sections.

3.1.2.2.1 Impersonation

In an impersonation attack, a student shares his or her access credentials with a third party impersonator, who impersonates and takes the online test. It is difficult to detect impersonation once an online test is completed (Kerka and Wonacott, 2000). These attacks are pre-planned and consensual, involving legitimate students with valid access credentials. Moini and Madni (2009) state that impersonation and illegal sharing or disclosure of authentication secrets is challenging to defend against in a remote online setting. They identified that students invite third parties to take their online tests for extra benefit. Such attacks are evolving with the advent of new communication technology. A number of scenarios are presented below to describe the potential impersonation attacks.

- **Credential Sharing with a Third Party via Email (Non-Real Time)**

  The conventional login-identifier and password is a widely used approach for the authentication of students in online tests. This method may provide adequate security in many online applications. However, it is vulnerable to attacks when students invite third parties to take their examinations. A student is able to share his or her access credentials prior to the test via email, phone and instant message. Rowe (2004) states that individuals share credentials with collaborators, who take the online test on behalf of the intended test taker. Email is a widely used communication method and students may share access credentials via this method. An abuse case scenario for such an attack is described below.

  Consider that an online test authenticates students using a login and password. A scenario of collusion via email is described below:

  "Alex is a registered student on an online course 'PRG-1 programming languages'. He is due to write his final semester online test on a scheduled date. Alex wants to boost his grades but he has not prepared for the test. He finds a professional helper, John, to assist with his test. John has agreed to impersonate him in the test for an agreed amount of money. Alex emailed his online test details and password to John before the test date. On the test day, John satisfies authentication by providing the shared login and password. He writes the answers and completes the online test on behalf of Alex."

- **Credential Sharing with a Third Party via Phone (Real Time)**

  The mobile phone has become an increasingly used communication technology and an essential personal accessory. McGee (2013) identified that students may use smartphones for information exchange during online examinations. Howell et al. (2010) reported that students exchange answers to questions using their phones and take photographs of exams and transmit them to others. Paullet et al. (2015) identified phone use as a new method of cheating. They argue that the use of browser-locking techniques may become irrelevant if a student has access to a smartphone during their exam. There are two possible scenarios where a smart phone may be used to cheat in an online test, i.e. sharing answers to questions, and sharing access credentials for impersonation. It may be argued that access credentials could be shared before an online test, but if a challenge questions method (Bailie and Jortberg, 2009) or a random PIN code is implemented, where questions or PIN code are generated randomly, students will not know their credentials before an online test. Thus, in this case, students must use smartphones to share access credentials during the test with a third party. This provides a real-time interaction between a student and an impersonator. In a recent study, Paullet et al. (2014) identified the use of mobile phones as a rising concern, which is a challenging issue to combat. An abuse case scenario for such attacks is described below.

Consider that an online test is only available in a secure browser, which prevents unwanted applications, e.g. remote desktop, instant messaging applications. Students are authenticated using two factors: login identifier and password, and a randomly generated PIN code emailed to the student upon completing the password authentication. A scenario of collusion using a smartphone is described below:

"Joe is a registered student on an online course 'OS-1 Operating Systems'. He is due to write his final semester online test on a scheduled date. Joe feels that he might not be able to pass his final test. He discusses this with a close friend, Daniel, who has already completed the same course. Daniel is willing to help Joe and agreed to impersonate him in the test on the scheduled date. Joe shared his online test details and password with Daniel before the test. However, the online test requires students to provide a randomly generated PIN code, sent to their phone at the time of the test, in order to authenticate their identity. On the scheduled date, Daniel satisfies the initial login using the shared password; however, the PIN code is sent to Joe's phone, as he is the registered user. Joe collects the PIN code and forwards it to Daniel on his phone, who satisfies the authentication. Daniel writes the test answers and completes the online test."

- **Credential Sharing with a Third Party via Instant Messaging (IM)**

Instant Messaging (IM) is another potential method to communicate during an online examination session. The growth of IM services is a global phenomenon, which is rapidly changing the way people interact. IM applications are easily available on mobile phones, tablets and computers for little or no cost. Ease of access makes it a potential tool for cheating in an online examination. Examples of instant messaging applications include Skype, Viber, WhatsApp, and Phone

(Church and de Oliveira, 2013). The prevalence and free availability of these applications means they are gradually replacing short messaging service (SMS) communication (Oghuma et al., 2015). As of 2016, chat service WhatsApp has reached 1 billion registered users (McCarthy, 2016). Technology has been a useful tool for advanced learning; however, it may also be used by people in promoting their personal objectives, including cheating. McGee (2013) stated that technology is the most commonly used strategy to cheat in online examinations. Many research studies reported that students with access to phones and computers use instant messages during online examinations (Dee and Jacob, 2012, Rogers, 2006). IMs may be used for communication with a third party for help with exam questions as well as impersonation attacks. A student and a third party impersonator may exchange access credentials using IMs in order that the third party can access an online examination. An abuse case scenario for such an attack is described below.

Consider that an online test is only available in a secure browser, which mitigates unwanted applications, e.g. remote desktop, instant messaging applications. Students are authenticated using two factors: login identifier and password, and a randomly generated PIN code sent to the student's phone upon completing the password authentication. A scenario of collusion using IM is described below:

"Joe is a registered student on an online course 'PRG-1 programming languages'. He is due to complete his final semester online test on a scheduled date. Joe wants to pass his test in the final semester, but he has not studied, and therefore is not confident in taking the test. He discusses this with his close friend Daniel, who has already completed and passed the same course. Daniel is willing to help Joe and agreed to impersonate him in the online test. Joe shares his online test details and password with Daniel before the test. However, the online test requires students to provide a randomly generated PIN code sent to their phone in order to authenticate their identity. On the test day, Daniel satisfies the initial login using the shared password; however, the PIN code was sent to Joe's phone, as he is the registered user. Daniel chats with Joe using Skype instant messaging on a smartphone, collects the PIN code instantly and satisfies the authentication process. He writes the test answers and completes the online test on behalf of Joe."

- **Remote Desktop Sharing**

  Using remote desktop sharing applications, a remote user can access and control a desktop with permission to all programs (Manion et al., 2014). By combining remote desktop sharing and an online examination session, a student may login and invite a third party to impersonate him in an online test. Desktop sharing is reported as one of the ten most inventive cheating attempts in eCampus News (Barbour, 2014). Heussner (2012) state that it could be tempting to accept help from a friend or helper remotely using technology including remote desktop sharing. This enables a third party in the next room, or even in a different city, country and time zone, to impersonate a test taker. This type of attack is pre-planned and the student and attacker agree a time to perform the test.

  Consider that there is no protection against remote desktop sharing during an online examination. A scenario of collusion using remote desktop sharing is described below:

  "Joe is a registered student on an online course 'RD-1 relational databases'. He is due to sit his final semester online test on Saturday but has not prepared for the test. Joe makes contact with William, who is an experienced programmer and helps students with their tests for money. William agreed to impersonate him and sit his online test for an agreed amount. Joe sent a remote desktop login to William before the test time on Saturday. On the test day, William logs in to Joe's computer using a remote desktop application. Joe logs in to his online test and hands over the test to William, who completes the answers and finishes the test."

  A secure browser is one possible solution to prevent remote desktop sharing during an online examination session. For example, a safe exam browser is an application to prevent the running of undesirable applications during an online examination session (Frank, 2010). Respondus Lockdown Browser (Respondus, 2016) is an example of a secure browser application.

The security of the online examination is breached in the above scenarios. It is challenging to detect these types of collusion attacks.

3.1.2.2.2 Abetting

In abetting attacks, a legitimate student takes an online examination with the help of a third party abettor (Dietz-Uhler and Hurn, 2011). This is also described as “panic cheating”, when a student is struggling to answer a question during the test. Stuber-McEwen et al. (2009) state that aiding and abetting is a common practice in both online and classroom cheating. Regardless of whether students were online or physically in classes, aiding and abetting with exams was the most frequently reported form of cheating (Dietz-Uhler and Hurn, 2011). Dietz-Uhler and Hurn state that panic cheating occurs during a test when a student finds himself at a loss for an answer. The absence of monitoring or proctoring allows students to invite third parties to assist with their online examinations. The potential abetting threats are described below:

- **Third Party – Same Location**

  A fellow student or a third party collaborator sitting next to a student can help him/her in an online test (2004). In the absence of a live invigilation or remote monitoring, it may be a challenge to prevent the presence of helpers and abettors during an online test. McGee (2013) identified that in a test-taking situation, a student and a third party may be physically located in the same place. Rowe (2004) stated that the issue of authentication has been widely researched in order to ensure that a genuine student is present, but not to ensure that he or she is alone, which requires different methods. The presence of a third party with a test taker is a challenging issue.

- **Third Party – Remote Location**

  Students may get help from a third party collaborator based in a remote location during an online exam. Some research studies reported that students use their phones to receive help with the exam questions, and take photographs of questions to transmit them to others (Howell et al., 2010). As discussed in the previous section, a student may use a smartphone, instant messaging and emails to gain assistance from third parties remotely. Paullet et al. (2015) identified that the phone has been increasingly used for cheating in online examinations. This view is helpful to establish that students may use all possible means in a panic situation when they need help with exam questions.

3.2 Countermeasures

While deterrence of all types of threats to online examinations is a priority, based on a review of threats it is observed that collusion is a particular concern, due to the involvement of students and third parties (Hernandez et al., 2008, Apampa et al., 2009, McGee, 2013). As pointed out in numerous studies (Wisher et al., 2005, Levy and Ramim, 2007, McGee, 2013, Bailie and Jortberg, 2009), a major threat when conducting a remote online examination is the inability to know whether the correct student is taking the test or someone else has taken over the test on their behalf. This threat translates into impersonation, as described in the preceding sections. In this type of attack, a student and a third party collude, with the latter impersonating the registered student in an online test. This is considered to be a major concern and perceived as a great risk by the academic community (Kerka and Wonacott, 2000).

3.2.1 Existing Authentication Approaches

The existing authentication satisfies identity and authentication to ensure that the correct student has access to an online test. However, based on the literature review and evaluation of potential threats above, it has been identified that an authenticated student is sometimes not the expected student, or an expected student may start a test but does not complete it. Hence, the existing mechanisms are not sufficient to ensure that the correct student takes the online test.

Table 3-1 shows an overview of the existing methods in the context of impersonation threats. In the majority of features, students may be able to share access credentials with an impersonator. For example, students reveal their passwords to third parties for impersonation (Weippl, 2005). Apampa et al. (2010b) state that an impersonator could produce correct login details on behalf of a student during authentication, which raises the question “is the student really who he/she claims to be?” As discussed in Chapter 2 above, authentication methods are implemented to achieve identity and authentication security goals. However, each method provides a different level of security assurances, reliability and deterrence to impersonation threats. According to guidelines for authentication in online examination, the proposed method needs to:

- support, not prevent or disrupt, learning (usable)
- be integrated in the learning process (secure)
- be simple and flexible to deploy (usable)

- be secure, non-invasive and not diminish privacy (secure and usable)
- be low-cost (feasible).

  (Jortberg, 2009)

Table 3-1 Authentication Methods to Mitigate Impersonation Threats

Authentication methods	**Impersonation**
Knowledge-based Authentication (KBA)	
Login identifier and password	Can be shared with a third party
Personal challenge questions	Can be shared with a third party
Object-based Authentication (OBA)	
Smartcard, or magnetic card	Can be shared with a third party
Biometrics	
Fingerprint recognition	Cannot be shared with a third party
Face recognition	Cannot be shared with a third party
Signature recognition	Cannot be shared with a third party
Web video recording	Cannot be shared with a third party
Human invigilation	
Face-to-face invigilation	Cannot impersonate with identity verification
Remote monitoring (Web cam)	Cannot impersonate with identity verification

KBA is the simplest technique to fulfil the security requirements. This is an easy to use method, and expected to provide secure authentication in online examinations. This is a low-cost, accessible, widely acceptable and preferred authentication method (Hafiz et al., 2008). However, a review of KBA methods suggests impersonation attacks are inevitable. Using both challenge questions based on personal information, and login-identifier and password, students may be able to share credentials with third party impersonators using phone, IMs, remote desktop and email.

OBA method utilises physical objects such as smart cards and magnetic strip cards for authentication (Deo et al., 1998). This method is widely used in the banking, transport and hospitality sectors with a purpose-built infrastructure. Implementation of these features requires special purpose input devices and infrastructure, which incurs additional costs and human resources. Smart cards can be shared in person or by post with impersonators before online tests, meaning the method is fallible, and vulnerable to impersonation attacks. Furthermore, implementation of the OBA method may be challenging to implement in dispersed geographical locations with students needing to access online learning and examinations from their homes and offices.

Biometric features such as fingerprint and face recognition methods are suggested to enhance security in online examinations (Agulla et al., 2008). Thus, it is anticipated that only the correct student can authenticate, due to unique physical attributes associated with individuals. Ko and Cheng (2004) proposed the use of video recording of an online examination session, which may countermeasure impersonation attacks. These features are reported to be more reliable than KBA and OBA. However, some studies identified issues with the use of biometrics. Balie and Jortber (2009) state that biometrics require proprietary software, special purpose hardware and broadband Internet to transmit the required input. Unlike KBA, biometric features are associated with an individual's physical or behavioural characteristics, which cannot be updated if compromised. For example, some studies indicated that an individual's fingerprint can be lifted from the surfaces of objects without one's knowledge and used for replay attacks (Moini and Madni, 2009, Derakhshani et al., 2003). False Reject Rate (FRR) and False Accept Rate (FAR) are widely known issues with these features: Ratha et al. (2000) stated that fingerprint matching faces two common and competing errors, these being FRR and FAR. The same issues were reported in other biometric features, including face recognition. In a recent study, Sahoo and Choubisa (2012) identified the performance issues of algorithms used in biometric features, which include FAR, FRR, Equal Error Rate (ERR), Failure to Enrol Rate (FER), Failure to Capture Rate (FCR) and Template Capacity (TC) issues. The video recording feature may enhance security, but it will require post-assessment monitoring of exam sessions for all students, which incurs additional resources and demands extra effort (Ko and Cheng, 2004). This discussion implies that biometrics is more reliable in terms of identification; however, they are unreasonably intrusive, expensive and may cause difficulties in wider implementation where students are situated in dispersed geographical locations.

A human invigilator is an example of a secondary authentication method which can be used to ensure the presence of the correct student. This includes face-to-face proctoring and remote monitoring via a web cam. Face-to-face proctoring requires test centres and human invigilators in all locations (different cities worldwide) where students are enrolled on an online course. In addition, each test centre requires a review by academic staff to ensure proctor quality and compliance with the institution's test centre standards (Bailie and Jortberg, 2009). Student authentication that relies upon a human invigilator will require extra human resources, costs and allocated test centres. Remote monitoring via webcam may be a feasible alternative to physical invigilation. A dedicated proctor is assigned to authenticate identity and monitor an online test (Mahmood, 2010). Students can access their tests from the home or office without needing to go to an allocated test centre. This approach may be cost-efficient compared to face-to-face invigilation, but there is a cost attached to remote proctoring (Mahmood, 2010). This approach requires one-to-one monitoring and, therefore, would be expensive and challenging in testing a large number of students in dispersed geographical locations.

3.2.2 Exploratory Study with Online Programme Tutors

Xiao et al. (Xiao et al., 2011) conducted an exploratory survey with the academic staff from the University Hertfordshire. The participants of the study were teaching in online programmes offered by School of Computer Science.

The questionnaire was aimed to investigate the types of assessments used in online programmes, and to collect information on participants' awareness of possible student cheatings in online examinations. The participants had adequate experience of online teaching with 33% teaching on more than 3 online modules and 67% teaching on more than 2 modules across different levels of BSc and MSc programmes.

The results showed that individual coursework is favoured as the main assessment method (92%) compared to in-class-test (42%) and examination (17%). Group coursework was not adopted due to the lack of face-to-face communication among students. Online programme tutors showed concern about students' cheating in online examinations. Although only being asked to tick the most concerned type of cheating, many of them showed their concern on all types of cheating including plagiarism, impersonation, and abetting.

This study was a driver and motivated further research conducted in this thesis. The findings of this study and discussion in the previous sections suggest a need for an authentication approach which is accessible, usable, cost effective, and prevents collusion attacks in online examinations.

3.3 Summary

This chapter provided a review of threats to online examinations in general, and a detailed analysis of collusion. Collusion is further classified into impersonation and abetting threats. Impersonation occurs when a student works with a third party, who impersonates him or her in an online test. Abetting occurs when a student takes an online test aided by a third party either based in the same location or with remote access. Collusion is identified as a major challenge when conducting online examinations. In this chapter, it is suggested that weak authentication methods make online examinations fallible to these threats. The need for an authentication method was identified to satisfy the security goals, in order to ensure that the correct person is taking the online examination and that the student undertaking the test is the same one that completed the online course. In order to address this and answer research question two, a challenge questions authentication method is proposed in the next chapter.

4 Profile-Based Authentication

The previous chapter described threats to online examinations in general and collusion attacks in more detail. Discussions in the previous chapter emphasised the need for an authentication approach which is usable and may prevent collusion attacks. This chapter proposes the profile-based method, which utilises challenge questions for the authentication of students in online examinations. The following sections present an overview and structure of the proposed method. Details are provided for the design and development of an initial prototype. Finally, the architecture of the MOODLE learning management system is described to demonstrate the integration of the proposed approach.

4.1 Proposed Solution

In an attempt to address the research problems and answer the research questions, this thesis proposes that learning, examination and authentication should be integrated to achieve the security goals. The conventional authentication methods may disregard the learning process to confirm that the person who is taking the test is the same one that completed the learning. The proposed solution attempts to ensure that a student who is authenticated is the same one that completed the course.

This thesis proposes a challenge question approach to collect and consolidate a student’s information during the learning process and randomly use a subset of the collected information for authentication during an online test. This attempts to ensure that i) a student who is taking an online test is the same one that completed the coursework and ii) a student is deterred from sharing information with a third party impersonator during or before an online test. The design, development and implementation of the proposed approach are described in the following sections.

4.2 Profile-Based Authentication

To implement the proposed solution described above, a profile-based challenge questions authentication method is presented here. Figure 4-1 shows an overview of the proposed method. This is a knowledge-based approach, designed for secure and usable authentication in online examinations (Ullah et al., 2012a). Using this method, information about a student is collected in the form of questions and answers during the learning process to build and consolidate a profile, which is used for authentication in examinations.

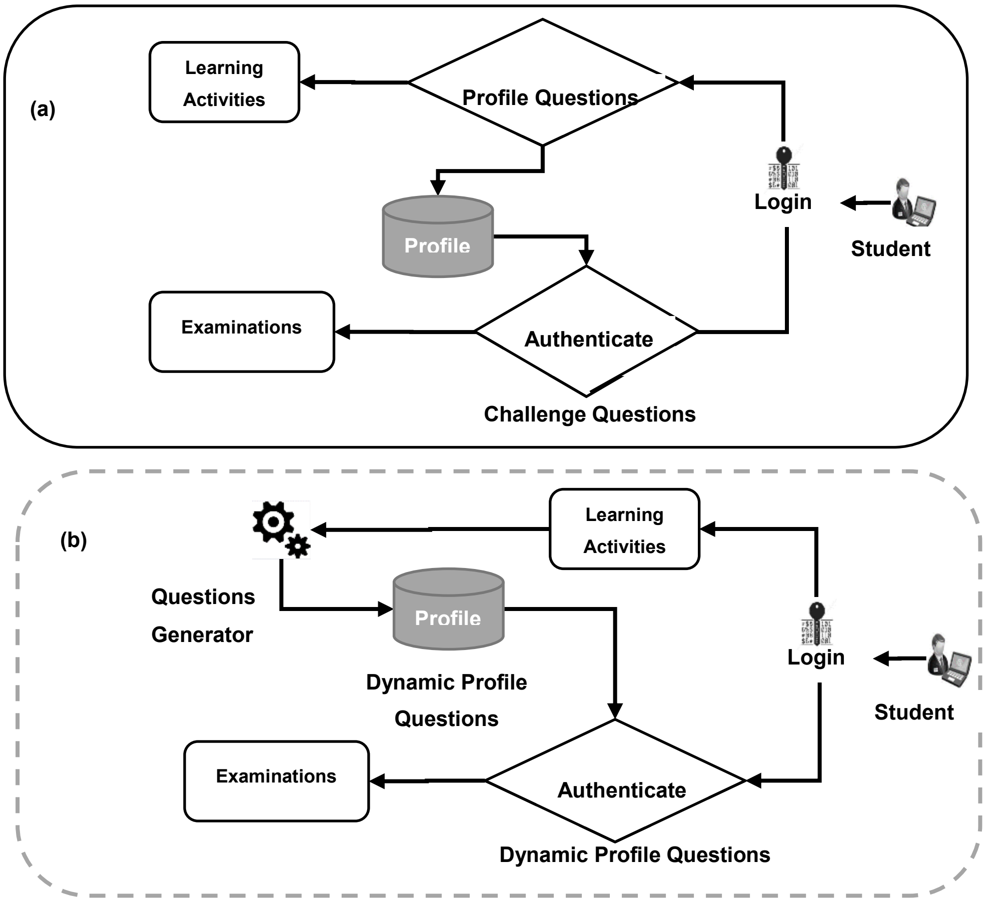


Figure 4-1 Profile-Based Authentication

As shown in Figure 4-1, this method can be implemented using two types of questions, i.e. *pre-defined* or *dynamic non-intrusive* questions, which are described below.

Figure 4-1 (a) shows a design of the proposed method implementing pre-defined challenge questions. Using this type, an administrator creates and sets questions at the start. A student is required to provide answers to these questions, referred to as *profile questions*, in order to access learning activities. These answers are used to build and consolidate a student's *profile*. In order to access an online examination, the student is presented with a subset of random *challenge questions* extracted from his or her profile. A student registers *n* profile questions and is presented with $t \leq n$ challenge questions upon authentication.

Figure 4-1 (b) shows a design of the proposed method implementing non-intrusive dynamic questions. Using this type, a student's *profile* is built and consolidated non-intrusively in the background during the learning process based on his or her interactions with learning activities. Features of the challenge question method are described below:

- *Profile:* The information associated with an individual student is stored in the database and referred to as the *profile*. Based on a question type, it represents a student's description or an individual's learning profile. The data in a profile is a collection of questions and answers associated with a student. Profiles are created for all students participating in learning activities.
- *Profile Questions:* These are registered during the learning process to build and consolidate a student's profile. Answers to profile questions are registered by students or created dynamically in the background. The learning is anticipated to be a continuous process, and therefore, answers to profile questions are collected recurrently when a student performs learning activities.
- *Challenge Questions:* These are randomly extracted from an individual's *profile* for authentication. As discussed above, a student registers *n* profile questions and is presented with *t* challenge questions upon authentication, where $t \leq n$ (Just and Aspinall, 2009c, Ullah et al., 2012b). Profile and challenge questions are the same entities used in different contexts, i.e. learning and examination. To an individual student, $r = t$ challenge questions must be answered correctly in order to access an online examination.
- *Traffic Light Access Control:* This is an optional feature, which could be implemented to relax the authentication constraints based on the number of correct answers to challenge questions. If a student registers *n* profile questions and is presented with *t* challenge questions upon authentication, it is sufficient to answer $r \leq t$ challenge questions correctly in order to access an online examination. The outcome of this method is classified into three categories described below, which are based on the number of correct answers:
    - *Red:* If the number of correct answers is *t1* out of *n (n = total questions presented)*, deny access.
    - *Orange:* If the number of correct answers is *t2* out of *n*, present more questions for re-authentication.
    - *Green:* If the number of correct answers is *t3* out of *n*, grant access.

The proposed method has a number of benefits and limitations. Recall Chapter 2, which described the use of a challenge questions method to mitigate impersonation attacks, citing advantages over other approaches (Bailie and Jortberg, 2009). In their work, Bailie and Jortberg proposed challenge questions based on a US consumer database to prevent impersonation attacks. The method presented in this thesis is adaptable and based on a student's learning activities. The key benefits of using a knowledge-based approach include wider accessibility on standard input devices, Internet speed and a lower cost compared to biometrics and object-based approaches (Ullah et al., 2014b). Furthermore, this method attempts to link learning and examinations to deter security threats. It is anticipated that the process of collecting information over a period of time in the learning process may deter a student from sharing it with a third party impersonator.

There are also some limitations to the use of the challenge questions method. Several studies reported usability as a major issue for challenge questions (Just and Aspinall, 2012, Schechter et al., 2009). These issues include usability attributes such as efficiency and effectiveness. This approach introduces additional steps in learning and examination processes, which will cause distraction for students. Guessing has been reported as a security concern for questions associated with personal information (Just and Aspinall, 2009c).

This research work will examine the proposed method for relevant usability attributes and to understand its influence on collusion attacks in an online examination context. The initial prototype was designed for use with the conventional text-based challenge questions, which are discussed below.

4.3 Question Types

4.3.1 Text-Based Questions

This is a widely used question type implemented by leading email service providers (Just and Aspinall, 2009a). These are associated with an individual’s personal and professional information, which is further classified into fixed and open questions, as described below (Just, 2003):

- *Fixed Questions*: Presented to users from a pool of pre-defined questions (Just, 2005). A user is required to register answers to pre-set questions presented “as is” at registration, e.g. “what is your mother’s maiden name?” With this type of question, a user is not provided with the ability to modify the question text. This provides the ability to a question designer to create secure and usable questions. Some websites provide a list of pre-defined fixed questions for users to select during registration (Schechter et al., 2009).
- *Open Questions*: Open to users, who can create their own questions in a free text area during registration (Just, 2004). This is a user-driven type of question, with users having full control over choosing questions and answers. Most often, questions and answers are received in a free text format.

The initial prototype implemented *fixed type questions* and the course administrator was required to create and upload pre-defined questions. Similar to question type, there are different answer types including free text, multiple choice and fixed set answers, which are described below:

- *Free Text Answers:* This is the most commonly used answer type. Users can provide their answers in a free text format. Using this type, answers of different data types, i.e. date, numeric, alpha-numeric and string, can be implemented. The initial prototype implemented free text answers.

- *Multiple Choice Answers:* Users are presented with multiple choice answers and must choose the correct answer. There is always a correct answer in the list of choices.

- *Fixed Set of Answers:* These are similar to multiple choice answers. Users are presented with a list of options to select a correct choice. The most common interface used for fixed set answers is a drop down list.

4.3.2 Image-Based Questions

The concept of image authentication has been implemented as image-based questions. They are pre-defined questions and an administrator is required to upload multiple choice image questions at the start. Students register their answers during the learning process. These questions are further classified into recall and recognition-based image questions, which are described in further detail in Chapter 7.

4.3.3 Dynamic Profile Questions

Figure 4-1 (b) shows the design of the proposed method with dynamic profile questions. These questions are adaptable and created dynamically. Questions are created non-intrusively and non-distractingly in the background during the learning process to build a student's profile. These questions are extracted from a student's learning activities, content submissions, grades, lessons, and forum posts in order to build and consolidate a student's profile. These questions are described in more detail in Chapter 9.

4.4 Initial Prototype

In order to evaluate the challenge questions method, an initial prototype was developed based on the design shown in Figure 4-1 (a) above. It was developed using

PHP (Hypertext Pre-processor) scripting language and a MySQL database. It was integrated in MOODLE (Modular Object Oriented Dynamic Learning Environment) Learning Management System (LMS) as a proof of concept for evaluation.

4.4.1 What is MOODLE?

MOODLE is free source online learning software known by multiple definitions, such as Learning Management System (LMS), Course Management System (CMS) and Virtual Learning Environment (VLE) (Dougiamas and Taylor, 2003). It is a popular system, used by a large number of institutions across the world. As of December 2012, MOODLE had 72,087 registered sites in 223 countries with 63,955,527 users (Dougiamas, 2012). Reasons for choosing MOODLE are described below.

4.4.1.1 Reasons for Choosing MOODLE

MOODLE has a number of features, and the important reasons for choosing it for the current research are listed below (Williams, 2005, Al-Ajlan and Zedan, 2007, Dougiamas, 2012):

- A free source environment available to end users for development, distribution, copying, studying and modifications, which makes it feasible for use in this research.
- A wide range of open source community developers for help and support with development and design queries.
- A widely used and acceptable LMS.
- Highly extendable and customisable.
- Students and tutors familiar with the concept of online learning in the majority of educational institutions are familiar with MOODLE.
- Detailed documentation and online community support available 24/7, which is a useful resource for developing prototypes, extending the functionality and promoting the research work.
- MOODLE is developed in PHP scripting language, compatible with a range of database software including MySQL, PostgreSQL, Oracle, SQL Server databases in the backend. PHP and MySQL are popular open source development environments that can be used to develop, deploy and distribute the initial prototype of the challenge question approach, without any licence restrictions.

4.4.2 MOODLE Architecture

Figure 4-2 shows three-tier MOODLE architecture. It is a structured modular object-oriented application and a highly customisable and expandable learning management system (Al-Ajlan and Zedan, 2007). The three-tier architecture comprises a user interface or presentation layer, business logic layer and data layer.

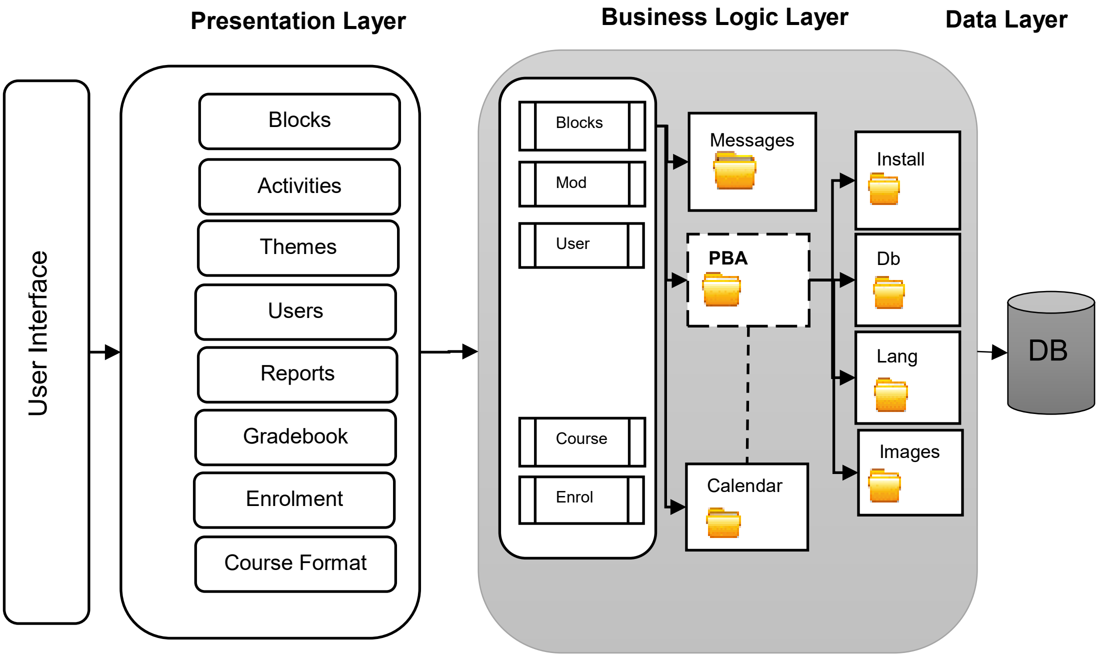


Figure 4-2 MOODLE Architecture

As shown in Figure 4-2, the core is surrounded by a number of independently customisable plug-ins at site and course levels. The basic authentication, access control (roles), learning and examination activities, and grades are delivered with the core application. The MOODLE core constructs the basic infrastructure necessary to build the LMS component and implements the key concepts with which all the different plug-ins will need to work (Dougiamas, 2012). The three-tier MOODLE architecture is described in the following sections.

4.4.2.1 Presentation Layer

The presentation layer is responsible for rendering the user interface. It can be seen in Figure 4-2 that a combination of plug-ins is linked with the core. The user interface for all plug-ins is defined in the respective interface folder. Each plug-in inherits the presentation (view) objects from the core and implements the inherited or customised view. The global theme plug-in is responsible for the overall style of a user interface. The following is a list of important plug-in types.

- Blocks: responsible for small building blocks and delivers a range of functions. Blocks are rendered and positioned in customisable left and right columns of the page. Examples of blocks include blog menu, settings, recent activity, comments, messages, main menu, online users, etc. The profile-based challenge questions method was developed and implemented as a block.

- Activities: responsible for delivery of teaching and learning components. Activities create learning content and deliver online assessments such as quizzes, assignments, forums, lessons, chat, long questions, etc.
- Themes: responsible for the look and feel of the entire website. The overall style of a MOODLE website, specific course and categories can be customised using the theme plug-in.
- Users: responsible for managing site and course users.
- Reports: responsible for reporting various outcomes to site administrators, teachers and students.
- Gradebook: manages and reports the outcome of formative and summative assessments. It provides a flexible interface for parameterised gradebook rendering.
- Course Format: MOODLE offers a number of different course formats, including topics, weekly and daily, which are defined in the course format. This component is responsible for rendering a chosen course format.
- Enrolment: responsible for access control, such as contexts, roles, capabilities and permissions.

4.4.2.2 Business Logic Layer

The business logic layer is a combination of PHP and HTML script files. System and user inputs are processed and serviced by this layer. The MOODLE core is responsible for holding the core objects, which interact with the expandable plug-ins. Each plug-in is responsible for processing its functionality together with the core. As shown in Figure 4-2, presentation, functional logic, deployment and database logic is defined and processed by the business logic layer. Code for all blocks is located in the “Blocks” folder. Similarly, resources and activities are stored in the “mod” folder. MOODLE is expandable and therefore, new blocks, activities, resources and themes can be added. A customisable block can be added with the knowledge of MOODLE programming and coding conventions.

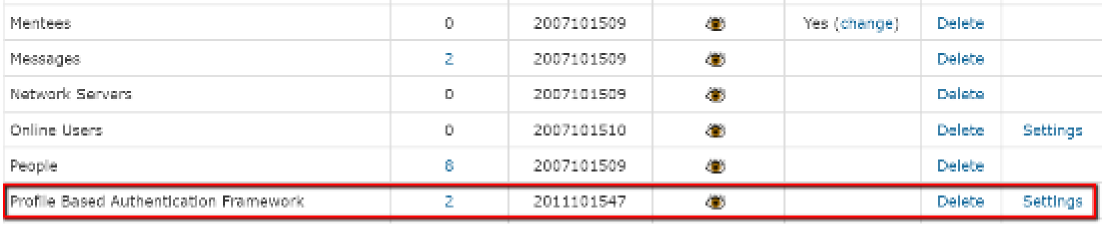
The profile-based challenge questions method was developed and implemented as a new block. The codebase for this block was stored using the MOODLE coding approach in “install”, “db”, “lang” and “images” folders located inside “Blocks”. MOODLE automatically detects new installations and deploys the core to install and configure a new block plug-in into the database, which is available for configuration from the administrator interface.

4.4.2.3 Data Layer

The data layer is responsible for the storage of data in the database. The MOODLE database comprises more than 200 tables. It is a combination of core and other associated tables to hold information about configurations, installations, users, courses, activities, resources, grades, plug-ins, etc. The number of tables may therefore increase with the deployment of more plug-ins.

4.4.3 Development and Integration of the Challenge Questions

The profile-based challenge questions method was integrated as a MOODLE block deployed with a configurable interface. After integration, it was set up and linked with all the available resources (online examinations components) such as quizzes, Forums, databases and assignments for authentication purposes. Figure 4-3 shows the profile-based challenge questions block configuration interface.



Mentees	0	2007101509	👁	Yes (change)	Delete	
Messages	2	2007101509	👁		Delete	
Network Servers	0	2007101509	👁		Delete	
Online Users	0	2007101510	👁		Delete	Settings
People	8	2007101509	👁		Delete	
Profile Based Authentication Framework	2	2011101547	👁		Delete	Settings

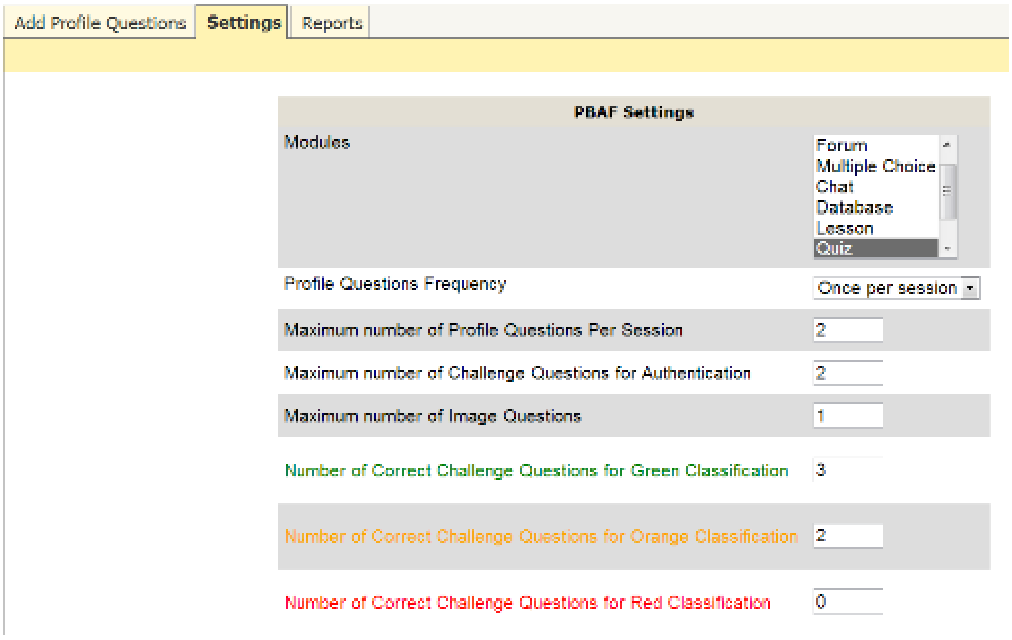
Figure 4-3 Challenge Questions Settings

4.4.4 Configuration of the Challenge Questions (Course Administrator)

In order to implement the profile-based challenge question approach , configurations of different settings are described in this section. A user with an *administrator* role is required to enable the block in an online course. This is followed by a number of configurations, which include setting up authentication variables, adding questions and monitoring reports, which are described below:

4.4.4.1 Authentication Setup

Authentication variables are configured to determine the functionality of the challenge questions method. Figure 4-4 shows the configuration interface implemented in a MOODLE block.



PBAF Settings

Modules	Forum Multiple Choice Chat Database Lesson Quiz
Profile Questions Frequency	Once per session
Maximum number of Profile Questions Per Session	2
Maximum number of Challenge Questions for Authentication	2
Maximum number of Image Questions	1
Number of Correct Challenge Questions for Green Classification	3
Number of Correct Challenge Questions for Orange Classification	2
Number of Correct Challenge Questions for Red Classification	0

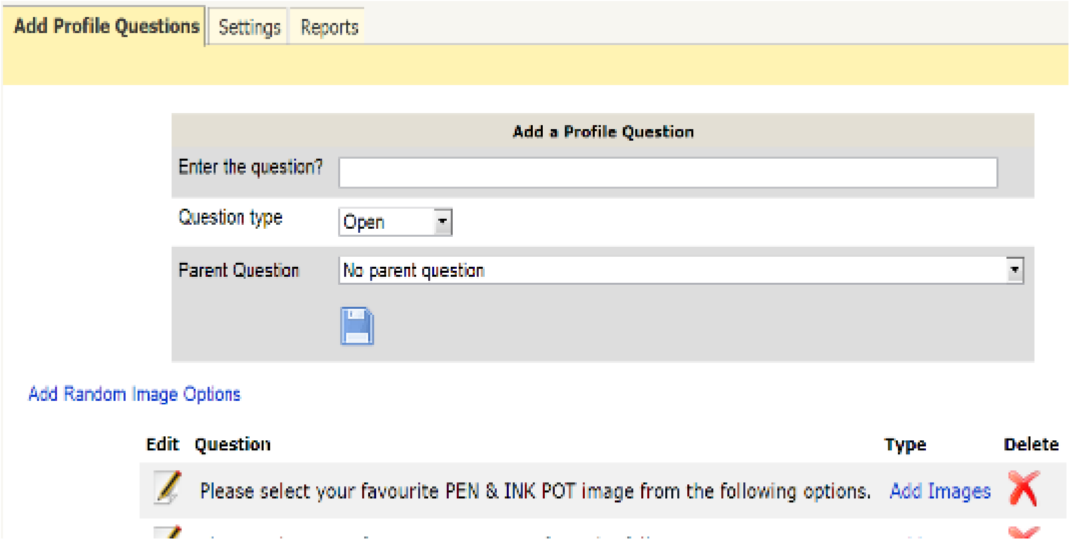
Figure 4-4 Authentication Configuration

Descriptions of all variables shown in Figure 4-4 are given below:

1) *Modules:* This links examination modules with the challenge questions. All assessment modules in MOODLE are available in the multiple select list, i.e. MCQs, Quiz, Lesson, Database, Chat and Forum discussions. Outcomes of the assessment modules are reported in the gradebook; therefore, users attempting to access these modules are authenticated using the profile-based challenge questions method. For the purpose of this study, MOODLE quiz was the main assessment module.
2) *Profile Questions Frequency:* In the initial prototype, students were required to register their answers to profile questions at the learning stage. A student was required to provide answers to profile questions in order to access course content. The frequency of these questions was made configurable to enforce collection of answers once per “login session” or “day”.
3) *Maximum Number of Profile Questions:* This variable determines the number of profile questions presented to a student in order to register their answers. The default value of this variable was 3.
4) *Maximum Number of Challenge Questions for Authentication:* This variable determines the number of challenge questions presented to a student to au-

thenticate their identity, in order that they can access an online examination (quiz). The default value of this variable was 3.

5) *Maximum Number of Image Questions:* This variable determines the number of image-based profile and challenge questions presented to a student to register answers and authenticate their identity.
6) *Number of Correct Challenge Questions for Green Classification:* This variable determines the number of correct answers needed to authenticate a student based on a traffic light access control system. For example, a student is authenticated if the number of correct answers is 2 out of 3 challenge questions.
7) *Number of Correct Challenge Questions for Orange Classification:* This variable determines the number of correct answers to *re-authenticate* (present more questions to) a student based on a traffic light access control system. For example, present more questions to a student (to re-authenticate) if the number of correct answers is 1 out of 3 challenge questions.
8) *Number of Correct Challenge Questions for Red Classification*: This variable determines the number of incorrect answers to penalise a student based on a traffic light access control and disable access. For example, disable a student's account if the number of correct answers is 0 out of 3 challenge questions.



Add a Profile Question

Enter the question?	
Question type	Open
Parent Question	No parent question

Add Random Image Options

Edit	Question	Type	Delete
	Please select your favourite PEN & INK POT image from the following options.	Add Images	✗

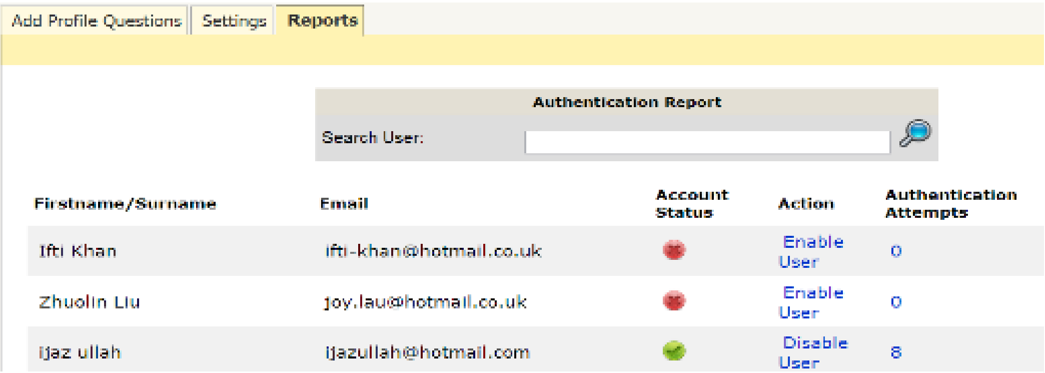
Figure 4-5 Initial Configuration: Add Questions

4.4.4.2 Adding Questions

The profile-based challenge questions method is a questions-driven approach and pre-defined text-based questions were utilised in the initial prototype. A set of pre-defined questions can be uploaded via a configurable interface. Figure 4-5 shows the user interface for adding questions. Different types of questions can be added, updated and deleted through this interface.

4.4.4.3 Authentication Reports

A reporting interface is built for an administrator to monitor and audit students' authentication outcomes. A student account can be activated or deactivated from this interface. Similarly, a student failing the challenge questions authentication in an online assessment module is locked out from further access to any assessments.



Authentication Report

Search User:

Firstname/Surname	Email	Account Status	Action	Authentication Attempts
Ifti Khan	ifti-khan@hotmail.co.uk	🔴	Enable User	0
Zhuolin Liu	joy.lau@hotmail.co.uk	🔴	Enable User	0
Ijaz ullah	ijazullah@hotmail.com	🟢	Disable User	8

Figure 4-6 Challenge Questions: Authentication Report

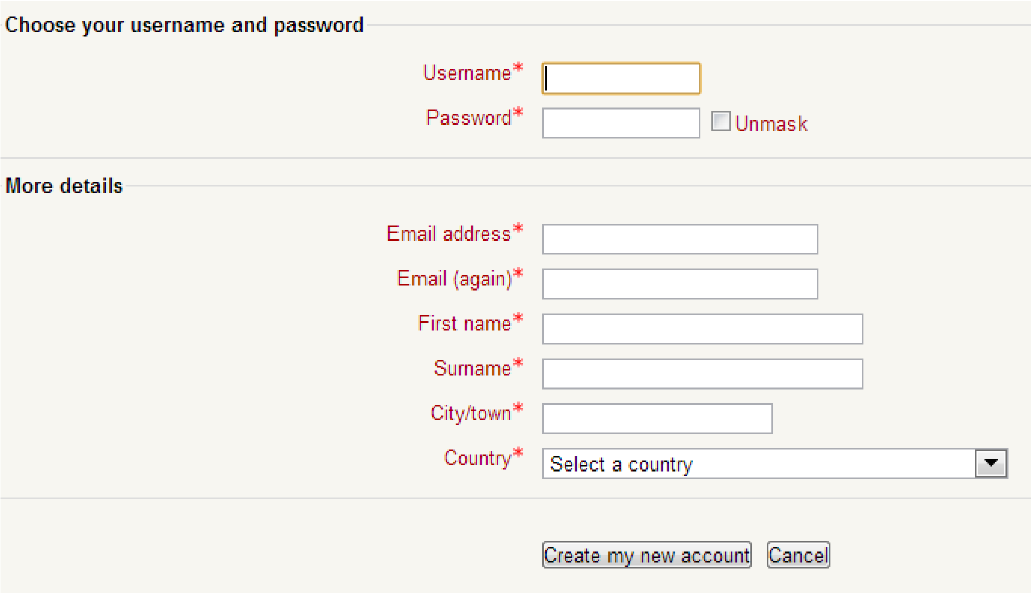
This allows the course administrator to verify the identity of an individual student and take appropriate action.

4.4.5 Registration and Challenge Questions Authentication (Student)

This section describes students' interaction with an online course, examinations and challenge questions authentication. A student is required to sign up before gaining access to an online course; therefore, registration is an essential process for each student.

4.4.5.1 Registration

MOODLE allows multiple ways to register students, i.e. self-registration, bulk upload and individual user registration by an administrator. Figure 4-7 shows a standard MOODLE registration form, where (*) denotes mandatory fields to register a user. In order to register a student, information in the registration form is filled and submitted online. This triggers and sends an email to the user account with a confirmation link. The registered student can access the online course with a username and password, selected during the registration process.



Choose your username and password

Username*

Password* □ Unmask

More details

Email address*

Email (again)*

First name*

Surname*

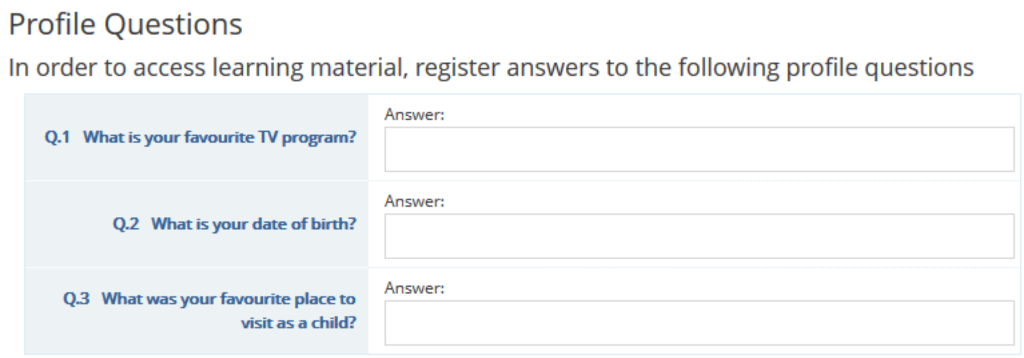
City/town*

Country* Select a country

Figure 4-7 Moodle: Registration

4.4.5.2 Profile Questions

Profile questions are randomly presented from the questions uploaded by an administrator as described above (see section 4.4.4.2). Students are required to register their answers to profile questions. As shown in Figure 4-8, this is a mandatory process and students can only proceed to view learning resources when answers to profile questions are registered. As described above (see section 4.4.4.1), the number of questions presented is configurable. Answers to profile questions are used to build and consolidate an individual's profile, which is used for authentication, as described in the following section.



Profile Questions

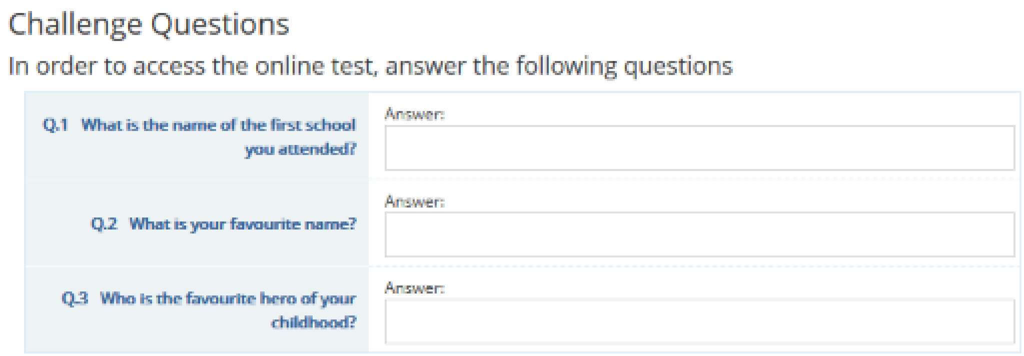
In order to access learning material, register answers to the following profile questions

Q.1 What is your favourite TV program?	Answer:
Q.2 What is your date of birth?	Answer:
Q.3 What was your favourite place to visit as a child?	Answer:

Figure 4-8 Learning: Profile Questions

4.4.5.3 Challenge Questions

Challenge questions are randomly presented from an individual student's profile for authentication, as shown in Figure 4-9. In order to access an online quiz, students are required to authenticate their identity and provide correct answers to their challenge questions. Answers to these questions were initially registered by students during the learning process described above (see section 4.4.5.2). The number of questions presented is configurable, as described above (see section 4.4.4.1). Students can be asked to answer challenge questions in multiple attempts if the traffic light access control system is enabled.



Challenge Questions

In order to access the online test, answer the following questions

Q.1 What is the name of the first school you attended?	Answer:
Q.2 What is your favourite name?	Answer:
Q.3 Who is the favourite hero of your childhood?	Answer:

Figure 4-9 Authentication: Challenge Questions

4.5 Summary

In this chapter, the design of the proposed challenge question approach was developed and implemented. Question design associated with the initial prototype was described, i.e. pre-defined text-based questions. The proposed method was implemented using MOODLE Learning Management System, which is a free source learning management software. It is customisable, expandable and feasible for evaluating the challenge question approach. The system architecture of MOODLE was presented to describe the user interface, business logic layer and data layer. The challenge question approach was integrated as a MOODLE block, which is accessible and configurable from a user interface.

In order to evaluate the proposed approach, research methods and methodology are presented in the next chapter.

5 Research Methods and Methodology

The previous chapter described the design and development of the profile-based challenge questions authentication method. This chapter presents research methods and methodologies to approach the research problems and evaluate the proposed method for usability and security. The background of quantitative and qualitative methods associated with research studies conducted in this thesis are explained. The chapter provides the justification for using empirical enquiries for security and usability evaluation. A risk-based security method is presented along with the manner in which it will approach specific parts of this research. The chapter presents a focus group method and how it is applied to this research. The usability test method, questionnaire and usability attributes associated with this work are justified. Finally, titles of the empirical studies and associated ethical considerations are presented.

5.1 Quantitative Research

Quantitative methods are applied on numerical and quantifiable data to draw meaningful results (Creswell and Clark, 2007). This method is classified into inferential, experimental and simulation methods. Inferential statistics allow an opportunity to draw inferences using characteristics or relationships of a population from the data (Cohen et al., 2013). This approach usually utilises surveys and questionnaires, where a sample of the population is studied to determine its characteristics in order to draw interpretations.

The experimental method is also known as the empirical method, which gives the researcher greater control over the research environment using variables wherein manipulation of variables is observed (Creswell and Clark, 2007). Using this method, the researcher can get facts (data) first-hand. This is a data-driven method, which produces a conclusion. In this approach, the researcher must set up hypotheses to approve or disprove on the basis of data analysis. This method is based on an experimental design to manipulate processes and participants in order to investigate the hypothesis. Kothari (2004) states that empirical research is appropriate when evidence is sought that certain variables affect other variables in some way. Kothari identified that evidence gathered through empirical studies is considered to be the most powerful support possible for a given hypothesis.

5.2 Qualitative Research

The qualitative approach is associated with subjective assessment of attitudes, opinions and behaviours (Berg and Lune, 2004). This approach generates results of non-quantitative form. In some instances the research outcome is not subjected to rigorous quantitative analysis. Qualitative methods include focus groups and interviews. This research method is concerned with phenomena relating to or involving quality; as an example, research investigating the reasons for human behaviour (i.e. people's opinions and responses to certain things). Motivation research is an important type of qualitative research, which aims to discover the motives and desires of participants by using detailed interviews. Other such techniques are word association tests, sentence completion tests, story completion tests and similar projective techniques (Gibbs, 1997). The following sections describe different qualitative and quantitative methods to evaluate security and usability of the proposed method.

5.3 Security

The methodology and research approach for security and usability design in computer science has been a widely discussed area. Many authors reported the benefits and limitations of various research approaches. Studies involving security analysis are logistically challenging in terms of accessing the actual resource assets for research and evaluation. Empirical studies are identified as useful techniques to evaluate security and usability of artefacts. Perry et al. (2000) state that an empirical study has a fundamental role in scientific research in software development, helping us understand how and why things work. However, Fléchais (2005) warns that real-world empirical research in security design can be difficult logistically. This view is insightful, as those responsible for a real-world system would be reluctant to disclose their system security model and data for empirical evaluation. Nevertheless, empirical validation is essential to evaluate the security design of information systems.

As discussed in the Chapter 2 literature review, security taxonomy covers areas including confidentiality, authentication and authorisation. The premise of this research is, however, focused on authentication. Recall Chapter 3, which described security threats to online examinations. Chapter 4 introduced and developed the proposed method, and to validate the research work in this thesis, a relevant research method is proposed to evaluate the security. Potter and McGraw (2004) proposed a "Risk-Based Security Test Approach" for risks and security evaluation.

They created use cases, listed normative security requirements and performed security risk analysis.

5.3.1 Risk-Based Security Test Approach

There are two methods to approach security testing: i) testing of functionality with standard security testing techniques, and ii) a risk-based security approach based on the threats, risk analysis and abuse cases. The risk-based security approach is a quantitative method, which provides rapid quantification of security-level risks associated with processes (Ni et al., 2003). This method focuses on the testing of features and functions of artefacts based on the risk of their failure (McGraw, 2004). Some authors suggest that the risk model evaluates the importance of functions and the impact of their failure (Gerrard and Thompson, 2002, Bach, 2003). This view is helpful in understanding the impact of threats and security failures in the context of a system. Risk-based security testing identifies if the risks have been mitigated. The important risks are identified from architectural risk analysis, abuse cases, attack patterns and threat analysis. Based on the identified risks, tests are performed in three steps, i.e. plan, test and mitigate risks. Standard security techniques may not reveal all possible security issues; therefore, the risk-based security approach is used to evaluate the proposed challenge question approach to mitigate the identified threats discussed in Chapter 3. The three steps of the risk-based security assessment method are described below.

5.3.1.1 Plan

A security test should be planned in a structured way to identify and mitigate potential threats. A test plan is organised, which combines multiple steps in order to identify the functions, risks and threats, and create abuse case scenarios. Descriptions of the planning steps are presented below.

- **Identify Functions and Features**: A conventional system translates business processes into functions and features based on a system design. At the outset, features and functions directly responsible for security are identified. The impact of these features on the secure assets is assessed. Users of the identified functions and features are listed.

  In the context of this research the proposed challenge question approach was designed and developed (see Chapter 4). Online learning and examinations are identified as important assets, and activities associated with them are essential features and functions. Students, teachers and course administrators are identified as main users.

- **Identify Risks and Threats**: Identification of risks and threats is a critical aspect of security testing. According to ISO, risk is a "probability of occurrence of harm and its effect on objectives" (Purdy, 2010). As discussed earlier in Chapter 2, risk comprises a combination of assets, threats and vulnerabilities (ISO/IEC TR 13335-1, 1996, p.5-10). In an attempt to mitigate threats, it is essential to identify them in detail (Jung et al., 1999). The threat analysis presented in Chapter 3 identified potential threats which risk the security of online examinations. This described a number of threats including intrusion, non-intrusion, collusion and non-collusion. This research will focus on collusion attacks and evaluate the security by creating abuse case scenarios in the context of online examinations.
- **Creating Security Abuse Use Cases:** McGraw (2004) states that thinking like an attacker is essential to identify and analyse security threats. This informs the creation of abuse case scenarios or abuse use cases, which are created for identified risks and vulnerabilities. A *use case* is a user interaction with a system, and an *abuse use case* is staging a scenario by simulating attacks. A user role is played by an actor in a simulation scenario or a user himself in a real empirical study. It involves users interacting with system features and functions with a focus on identified threats. The abuse case scenarios do not work in isolation, and involve multiple users and interdependent functions. These scenarios are executed and the impact is recorded to mitigate risks. This is an important aspect of research methodology, which provides a basis for the empirical studies discussed later in this thesis.

5.3.1.2 Security Test

The test plan identifies features and threats, and describes abuse cases. A security test is executed based on the abuse case scenarios created at the planning stage. It can be executed involving actors (users) performing the abuse case scenarios in a simulation or a real situation. Actors are provided guidance and a task execution plan before the actual test. The data from security tests is traced and recorded for evaluation purposes. Security analysis is performed on the data collected from the execution of abuse case scenarios in an attempt to investigate the impact of threats and vulnerabilities identified in *risks and threats analysis*.

Table 5-1 shows an overview of the risk-based security test. It will attempt to evalulate the challenge question approach against the collusion threats, identified in Chapter 3, in an online learning enviornment.

Table 5-1 Overview of the Risk-Based Security Test

Actors	Features and Functions	Threats	Abuse case scenarios
Students Tutor Administrator	Online learning (lessons, course content, assignments) Online examintions i.e. Quiz	Collusion (identified in Chapter 3)	Attack scenarios in online examinations (identified in Chapter 3)

5.3.1.3 Mitigate Risks

In response to the security analysis of the test (which was based on the abuse case scenarios), the security is reviewed. Threats uncovered in security analysis are mitigated and risks are reviewed. Adequate security controls are implemented to mitigate risks (Jones and Rastogi, 2004). This is an iterative process, and in order to confirm that risks are mitigated, another iteration of the security test is planned.

5.3.2 Focus Group

Research designed to investigate people’s opinions, attitudes, or what individuals or groups think about a particular subject or institution is also qualitative research. This approach is particularly important in a situation where the aim is to discover the underlying motives of human behaviour. This thesis adopted the focus group qualitative research technique. Several definitions for focus groups are available in the literature, i.e. collective activity (Powell and Single, 1996), organised discussion (Kitzinger, 1995), and social events and interaction (Goss and Leinbach, 1996).

According to Powell et al. (1996), a group of representative individuals are chosen and gathered by researchers to discuss their personal experience and comment on the topic under research. This is a form of group interview performed collectively, at the same time, with a focus on questions and responses between researchers, moderators and participants. However, it relies upon interaction with the group on the subject under research. The primary objective of a focus group is to draw upon respondents’ behaviour, beliefs, feelings, experiences and reactions in such a way that would not be feasible using other research techniques. Individuals in a group may have partially independent opinions, attitudes, feelings and beliefs; however, these are likely to be revealed via the social gathering and the interaction which being in a focus group entails.

The focus group has been used to collect data, views and opinions of online programme tutors on various threats to online examinations, and the proposed challenge question approach, which is discussed later in this thesis.

5.4 Usability

The importance of usability for secure systems is discussed in Chapter 2. Usability is essential in the design of authentication methods (Braz and Robert, 2006). Authentication mechanisms may fail to protect digital assets if users are unable to use them correctly. This research will approach usability in the context of authentication and online examination systems.

The discussion in Chapter 2 (literature review) suggests that usability and security are important and inter-related. Security experts emphasise the use of secure methods, whereas usability experts suggest "easy to use" methods. A *Usability test* and system usability questionnaire is selected for evaluating the usability of the proposed challenge questions method. These approaches are described in the following sections.

5.4.1 Usability Testing Approach

The literature review in Chapter 2 established the importance of usability for a secure authentication method. An effective means of ensuring usability of a secure system is periodic usability testing and evaluation. It is a method of usability inspection, which tends to focus on the interaction between humans and computers (Corry et al., 1997). Using this approach, usability goals are set at the design stage and evaluated with the involvement of active evaluators and system users. The representative users work on typical tasks using the system or a prototype. This approach allows testing of the attributes of prototypes and the final product, even if it is not ready yet. The evaluators use the results to see how the system supports users to perform their tasks.

Dumas and Redish (1999) described the following characteristics of usability testing:

1) Improve usability: The primary goal of usability testing is to improve the usability of a system. Another goal is to improve the process of product design.

For each test you have specific goals which might be different from other tests.

2) Real users: The participants performing the usability testing should represent real users in various roles.
3) Real tasks: The participants performing the usability testing should undertake real tasks.
4) Record Data: The evaluator records and observes the test activities.
5) The evaluator analyses the data, diagnoses the issues, recommends changes and applies fixes.

In the context of this research, the usability test characteristics described above are translated into the following:

1) The usability test goals, in the context of this research, are to evaluate usability attributes, efficiency and effectiveness of the proposed challenge questions method.
2) User roles associated with the proposed challenge questions method are student, tutor and course administrator.
3) The system tasks are user interactions with challenge questions during learning and examination processes.
4) The data associated with users' activities and challenge questions is recorded in a database. The researcher records data and observes the usability test.
5) The data collected from the usability testing is analysed towards the end of each empirical study.

The usability attributes associated with this research are based on ISO/9241-11 (2003), which includes efficiency and effectiveness.

5.4.2 Usability Evaluation Scale

According to Molich et al. (2004), the effectiveness of a usability test is dependent upon the chosen tasks, the methodology and the people in charge of the test. Sauro and Kindlund (2005) state that customers or users of processes define what is an acceptable level of quality for any measure of a process. They state that acceptable levels of usability goals are relative and may change for different systems. As an example, the state of being 99% error free is not good enough for critical functions such as nuclear plants. However, based on the literature review discussed in Chapter 3, designers of text-based challenge questions may anticipate errors. It is important to determine the acceptable level of usability for the proposed method. Bang et al. (2009), using the standard letter grade scale, proposed that products that scored in the 90s, 80s and 70s were exceptional, good and acceptable, respectively. Anything below a 70 had usability issues that were a cause for concern. This scale is adopted for evaluation of usability attributes later in this thesis.

5.4.3 Questionnaire

The survey is a widely used method to collect representative user feedback and performance associated with a prototype system (Preece et al., 2002, Gable, 1994). The questionnaire is one of the most effective survey techniques used for data collection and feedback. In this research, online web questionnaires are used to collect participants' feedback on different aspects of the challenge question approach.

Online questionnaire survey tools are becoming increasingly popular for research in various fields. These are interactive and offer cost-effective, validated and fast results. The questionnaire's scales, adopted for this research, are commonly used and recommended by researchers for usability analysis, as discussed later in this thesis.

5.5 Empirical Evaluation

Six studies were conducted to build up the knowledge necessary for this research. These studies include five empirical enquiries and a focus group session listed below:

- Empirical Study 1 (Text-Based Questions)
- Empirical Study 2 (Text-Based and Image-Based Questions)
- Empirical Study 3 (Impersonation and Text-Based Questions)
- Empirical Study 4 (Impersonation and Dynamic Profile Questions)
- Study 5 (Focus Group with Online Programme Tutors)
- Empirical Study 6 (Dynamic Profile Questions and Remote Proctoring)

5.6 Ethical Considerations

According to the University of Hertfordshire Policy and Regulations (UPR RE01), all empirical studies involving human subjects require ethical approval from the relevant ethics committee before the studies are undertaken. The policy describes the need for ethical approval and identifies the Ethics Committee with Delegated Authority

(ECDA). The respective designated committee for ethics considers requests in the relevant disciplinary area. The committee requires complete information, including empirical study design, number of participants, information sought, data capture details and survey questionnaires (if required).

In relation to this research, ethical approvals were sought from the Ethical Committee for the Faculty of Science, Technology and Creative Arts. The approved protocols and pertinent studies are listed below in Table 5-2.

Table 5-2 Research Studies Ethical Approvals

Research Study	Protocol Ref	Date
Empirical Study 1	1112/63	01/03/2012
Empirical Study 2	1213/05	30/10/2012
Empirical Study 3	COM/PGR/UH/02006	22/10/2015
Empirical Study 4	COM/PG/UH/00041	14/11/2013
Study 5 Focus Session	COM/PG/UH/00059	06/08/2014
Empirical Study 6	COM/PGR/UH/02006	22/10/2015

5.7 Summary

This chapter described the research methods and methodology used to approach the research problems. Both quantitative and qualitative research methods are used in this thesis. The justification and description of a risk-based research method is provided, along with how the abuse case scenarios are used to investigate security of the proposed challenge questions method. The usability test method is described, as well as how it will approach the usability analysis of the proposed method.

An initial prototype of the proposed method was developed to conduct the first empirical study in order to investigate usability attributes. The next chapter will report the study, which was conducted using research methods described in the current chapter.

6 Study 1 – Text-Based Challenge Questions

This chapter presents the first empirical study using an initial prototype of the proposed challenge question approach . The study aims to collect the benchmark data from evaluation of the usability and security of text-based questions in a simulation environment. The chapter describes the purpose, research questions, hypothesis and research method. The following sections explain participants' recruitment, design of a simulation online course and quiz, and study phases to describe how the problem was approached. This includes an abuse case scenario, in which a friend or colleague attempts to impersonate a student by guessing answers to his text-based challenge questions. Finally, the chapter reports usability and security results.

6.1 Purpose

This is an exploratory study which aims to investigate the usability and security of text-based challenge questions. As described in Chapter 4, text-based questions are associated with individual personal information, contact and academic details. Some earlier studies (Just and Aspinall, 2009c, Just, 2004) identified usability as one of the major issues with the use of challenge questions. As discussed in Chapter 2, usability analysis is important in evaluating how effectively security measures can be implemented. The common attributes defined by the International Organization for Standards (ISO) (ISO9241-11, 1998) which contribute to usability include efficiency and effectiveness. Efficiency is a usability metric, which can be evaluated by measuring the completion time of each task and sub-task separately (Seffah et al., 2001). Effectiveness is considered to be the degree of accuracy of participants' responses.

Previous research suggests that challenge questions can be vulnerable to guessing attacks by adversaries, acquaintances, friends and colleagues (Schechter et al., 2009, Just and Aspinall, 2009b). Just and Aspinall (2009c) described guessing in three categories: blind guessing, focused guessing and observation. Schechter (2009) investigated guessing attacks by acquaintances and statistical guessing in the context of credential recovery to evaluate the security of challenge questions. Therefore, this study investigates the security of challenge questions when a friend or colleague attempts to impersonate a student using a guessing attack. The purpose of this study was:

1. To analyse the usability attributes, i.e. efficiency and effectiveness, of text-based challenge quesitons.

2. To analyse impersonation by friends and colleagues using a guessing abuse case scenario.

6.2 Research Questions and Hypotheses

The research questions identified in Chapter 1 are cascaded into more questions associated with the usability of text-based challenge questions. The research question RQ 3) is associated with the usability attributes of efficiency and effectiveness of the proposed method. The research question RQ 4) is associated with the security of the proposed method. This study attempted to answer the following research questions, which were derived from RQ 3a) and RQ 4a):

RQ 6.1) How efficient are text-based challenge questions when implemented for the authentication of students in online examinations?

RQ 6.2) How effective are text-based challenge questions when implemented for the authentication of students in online examinations?

RQ 6.3) How can the text-based challenge questions mitigate impersonation by friends and colleagues using guessing attacks in online examinations?

The following hypotheses were framed to answer the above research questions. Each hypothesis is mapped to a corresponding research question:

H 6.1) Text-based challenge questions are efficient when implemented for the authentication of students in online examinations.

H 6.2) Text-based challenge questions are effective when implemented for the authentication of students in online examinations.

H 6.3) Text-based challenge questions mitigate impersonation by friends and colleagues using guessing attacks in online examinations.

6.3 Study Method and Design

The usability test and risk-based security assessment methods described in Chapter 5 were implemented to evaluate usability attributes and guessing attacks in a simulation online course. The usability test is a usability inspection method, which tends to focus on the interaction between humans and computers (Corry et al., 1997). Using this method, the representative users (i.e. students) interact with online learning and examinations using text-based challenge questions for authentication. The user's response time to challenge questions was used to evaluate efficiency. The usability evaluation scale described in Chapter 5 (see section 5.2.1) was used to translate the effectiveness analysis. This scale translates the usability of products in the 90s as exceptional, 80s as good, 70s as acceptable and anything below 70s indicates issues that are a cause for concern (Bangor et al., 2009).

The risk-based security assessment approach focuses on the test of features and functions of artefacts based on the risk of their failure using abuse case scenarios (McGraw, 2004). An abuse case scenario was simulated to analyse whether friends or colleagues could impersonate students by guessing their text-based challenge questions.

The structure of text-based challenge questions, online course, examination and study phases are described in the following sections.

6.3.1 Text-Based Questions Design

A total of 20 text-based questions were created for this study, which are presented later in the results section. The study implemented fixed type questions and free text answers, as described in Chapter 4. These questions were classified into five different themes, i.e. academic, personal, favourite, contact, and date. Questions in the academic and contact themes were based on the University of Hertfordshire undergraduate admission form. Questions in the personal and favourite themes were copied from security questions used by Google, Microsoft, AOL and Yahoo (Schechter et al., 2009).

6.3.2 Simulating Study Phases

The study was organised into multiple phases, including participant recruitment, initial configuration, registration, learning, examination, traffic light access control system and performing a guessing abuse case scenario. These phases are described in more detail below:

- **Simulation Online Course**: A simulation online course was created and deployed in MOODLE Learning Management System (LMS). Since this was a simulation course, only guidance notes were presented as course content. A simulation quiz was also created.
- **Participants Recruitment:** A total of 23 participants were recruited from the University of Hertfordshire in Hatfield, UK, and the Institute of Management Sciences in Peshawar, Pakistan. They were already enrolled in undergraduate and postgraduate programmes in their respective institutions. Correspondence with participants was performed via email. They were provided with a design and guidance notes describing the aims and objectives of the study. To motivate par-

ticipants, they were invited to attend a free “PHP & MySQL” online course subject to completion of the simulation.

- **Initial Configuration:** An initial setup was required to assign values to configurable variables of the challenge questions method. A total of 20 text-based questions, described above, were uploaded to MOODLE. The number of profile questions presented during the learning process was set to 3 in order to collect more data for analysis without causing fatigue in participants. Similarly, the number of challenge questions presented during the examination process was set to 3. Bruce (2007) recommended that asking multiple challenge questions for authentication improves security. A traffic light access control system was implemented to determine authentication on the basis of total number of correct answers to challenge questions. This was implemented to relax the authentication constraints. The following traffic light configuration was defined:

  1. *Condition-1 Red*: If the number of correct answers to challenge questions was 0 out of 3, the participant was locked out and access to the online examination was denied. This condition was classified as *red*.
  2. *Condition-2 Amber*: If the number of correct answers to challenge questions was 1 out of 3, the participant was presented with more challenge questions to re-authenticate iteratively. This condition was classified as *amber*.
  3. *Condition-3 Green*: If the number of correct answers to challenge questions was 2 or 3 out of 3, the participant was authenticated and access to the online examination granted. This condition was classified as *green*.

- **Registration:** The study started from the registration phase, followed by learning and examination phases, which are described later. The registration was a standard MOODLE sign-up process, which was essential to create login credentials to access the simulation online course. Upon successful registration, participants received their login-identifier and password. The course was available to registered users only.

- **Online Learning:** In a practical scenario, it is anticipated that a student will access an online course multiple times in order to complete the course work. To simulate the learning process, participants were required to access the course for a period of one month with a minimum three-day gap between each visit. The following steps were performed in the online learning phase:

  1. Participants accessed the online course using their login-identifier and password.

2. On each visit, participants were required to provide answers to three profile questions in order to access the simulation course. This helped to collect sufficient data for the preliminary analysis.
3. Profile questions and their answers were stored in the database to build and consolidate participants' profiles.

- **Online Examination:** On completion of the learning phase, participants were emailed and advised to access the simulation quiz. There was an intervening period of 30 days between learning and examination phases. The following steps were simulated in the online examination phase:

  1. Participants accessed the course using their login-identifier and password, and attempted to access the simulation quiz.
  2. In order to access the quiz, participants were required to authenticate their identity and provide answers to three challenge questions randomly presented from their profiles.

- **Using the Traffic Light Access Control System:** Authentication was performed using the equality algorithm, i.e. a string-to-string comparison of answers (Schechter et al., 2009). To compare the data of the authentication process using the traffic light access control, it was disabled in the first authentication attempt. Participants were granted access to the quiz when answers to all their three challenge questions were correct. In all subsequent visits, the traffic light access control was enabled, as described above in the *initial configuration*.

- **Security Abuse Case:** A follow-up study was conducted for security assessment. An abuse case scenario was performed to examine the challenge question approach when a friend or colleague attempts impersonation using guessing attacks. The following steps were performed to simulate the abuse case scenario:

  1. Participants were asked to identify their friends and colleagues who participated in the previous phases of the study. Of the total 23 participants, 6 identified their friends and colleagues.
  2. Participants were paired up with their friends and colleagues in order to impersonate a friend's account.
  3. Fictitious passwords were created for all 6 participants in the abuse case scenario. The login-identifiers and passwords of friends and colleagues were amended for privacy reasons and shared with their pairs for impersonation.

4. Participants accessed the simulation course, each using their pair's login-identifier and password.
5. In an attempt to impersonate, participants were required to answer challenge questions on behalf of their pair. Participants were encouraged to guess answers to challenge questions. Results of authentication attempts were not revealed to participants and stored in the database for security analysis. The traffic light access control was enabled using the conditions outlined above in the *initial configuration*.

6.4 Usability Results

A total of 23 participants completed the initial registration. 18 participants completed the learning phase and answered 274 profile questions. A total of 13 participants answered 66 challenge questions during authentication in the online examination phase.

The usability results presented here are extracted from the data collected during participants' interactions with the online learning and examination phases discussed above. Participants submitted 38 (58%) correct answers in authentication, whereas 28 (42%) were incorrect due to various usability issues discussed below. The efficiency and effectiveness analyses are presented below.

6.4.1 Efficiency

Efficiency was analysed using data collected from participants' answers to profile questions in the learning phase. To examine the efficiency of the challenge question approach, the "completion time" and "answer length" of answers to profile questions were measured. Table 6-1 shows the mean score and standard deviation (SD) of the completion time and answer length variables. The correlation analysis of the two variables was measured to analyse any relation between a user's response and answer length. A Pearson Correlation was computed to examine the relationship between the "completion time" and the "answer length". The Pearson r = 0.152; p = 0.01 indicates a significant correlation between the two variables for n = 274. The small value of r = 0.152 suggests that there were other intervening variables affecting the completion time, however, these are not covered in this study. The efficiency of questions classified in various themes is discussed below.

Table 6-1 Usability Analysis: Efficiency of Text-Based Questions

Question Themes	Completion Time (seconds)		Answer Length (characters)	
Academic Questions	**Mean**	**SD**	**Mean**	**SD**
Find out about this course	14.14	7.98	7.0	6.11
Student number	14.55	8.52	3.0	2.9
Name of last school attended	14.60	6.67	14.86	9.38
Grades in highest qualification	15.14	6.29	2.0	2.47
Year of highest qualification	15.20	7.16	4.0	0
Month started the current course	15.61	8.06	5.0	2.03
Year started the current course	16.18	8.98	4.29	1.07
Highest qualification	16.93	6.80	9.40	8.47
Personal Questions				
Father's surname	13.55	8.76	4.71	1.26
Country of birth	13.78	7.25	7.20	1.37
Best friend's surname	14.47	6.95	5.79	2.57
Dream job as a child	18.03	8.65	9.85	5.24
Favourite Questions				
Hero of your childhood	14.70	5.94	11.71	5.31
Tutor	15.06	8.13	8	3.48
Module on this course	18.34	9.8	7.5	5
Contact Questions				
Home tel. no. with country code	15.73	8.78	10.60	3
Home address town	16.83	9.36	15	13.75
House name or number	17.18	7.8	19.58	18.55
Mobile number with country code	17.43	8.98	11.69	1.43
Date Questions				
Date of birth	16.42	6.75	6.36	3.91

Academic Questions: The relevance of questions to individuals is an important factor to inform efficiency. The completion time for academic questions that were relevant to users was short. For example, the completion time of answers to profile questions "*Where did you find out about this course*", "*Student number*" and "*Last school attended*" was the shortest in the academic theme with a mean completion time of 14.14, 14.55 and 14.60 seconds, respectively, which indicates that relevance of questions has an influence on efficiency.

Providing hints and examples has been a useful and standard practice to enhance usability. *Answer hint* is another factor which may contribute to enhanced efficiency. The findings indicate that questions with embedded answer hints were answered in a short time. For example, the profile question "*Where did you find out about this course*" was answered in the shortest completion time, i.e. 14.4 seconds. It was presented with an answer hint, i.e. "Friend, Internet", to help participants understand the context of the question. Although the completion time was efficient, detailed analysis of data revealed that 78% of the answers were identical and selected from the answer hint "Friend, Internet", which can be usable, but may lead to security risks.

The use of both abbreviations and long descriptions in answers can translate into usability challenges. It was noted that in spite of efficient completion time, i.e. 14.60 seconds, the length of answers to the question "*Name of last school attended*" was the largest for any question in the academic theme. To account for the length, further exploration revealed that 44% of the answers were abbreviations and 56% full school names; long school names resulted in increased answer length. Questions inviting long descriptive answers may have a longer completion time. This may also trigger memorability issues at a later stage during authentication.

Question clarity is another important factor which influences efficiency. Ambiguous and unclear questions may take extra time to answer and also frustrate users. As an example, answers to the profile question "*Grades in highest qualification*" were completed in 15.14 seconds. This was the longest completion time for the shortest answer length, i.e. a mean 2 characters. Such questions may also stimulate the thinking process to recall the correct grades. The question did not explicitly describe the grade type, which resulted in variations in answers. Detailed sorting of answers revealed that participants submitted different grade types (letters, percentage and description). 64% of answers contained letters, e.g. "A, A*, A+", 22% contained percentages (%) and 14% contained descriptive text.

As discussed above, question context and relevance to individuals is also an important factor for usability. For example, the profile question "*In which month did you start the current course*" was completed in 15.61 seconds. Detailed analysis of answers revealed that participants in this study were originally enrolled on different courses and programmes at their respective institutions. The question in the context of this study using a *simulation course* needed further clarity and participants were not clear that the "*current course*" referred to the simulation course, which contributed to a longer response time. Of the total answers to this question, 50% were incorrect. A similar response was noted to the profile question "*Year started current* *course*", with a mean completion time of 16.18 seconds. Detailed analysis of answers revealed 28% *"incorrect year"* or unrealistic answers.

Personal Questions: Questions in this theme were associated with an individual's personal information. These questions are widely used and researched by AOL, Yahoo, Google and Microsoft (Schechter et al., 2009). Given the increased use of personal questions, this was anticipated to be more usable than other themes. The findings indicate shorter completion time, which shows better efficiency. For example, the mean completion times of answers to the profile questions "*Father's surname*", "*Country of birth*" and "*Best friend's surname*" were 13.55, 13.78 and 14.47 seconds, respectively, with answer length of 4.71, 7.20 and 5.79 characters.

Personal questions requesting subjective information from the past resulted in a longer completion time. As an example, the profile question "*Dream job as child*" resulted in a longer completion time and answer length – 18.03 seconds and 9.85 characters. Mean completion time of all questions in the personal theme was 14.89 seconds.

Favourite Questions: Questions in this theme have been widely used for credential recovery (Schechter et al., 2009). The majority of favourite questions collect subjective information, which may change over time. For example, a student may have more than one favourite tutor. These questions need careful consideration at the design stage. Questions in this theme resulted in better response times. The completion times of the questions "*Hero of childhood*" and "*Tutor*" were 14.70 and 15.06 seconds, respectively.

Findings in this theme reinforce the argument discussed in the previous section regarding the influence of a question's context and relevance on usability. The mean completion time of answers to the question "*Favourite module on this course*" was 18.03 seconds. The simulation course was not modular and the question lacked clarity. The analysis of data revealed that 47% of answers contained unrealistic answers, i.e. "NA, Nil and Unknown". However, this question was incorrect in this context.

Contact Questions: Questions regarding contact information were created in a more generic way, in order to cover addresses for a wide range of participants in different geographic locations. However, this led to clarity issues. The mean completion times of answers to "*Telephone number including country code*" and "*Address town"* were 15.73 and 16.83 seconds respectively, with answer lengths of 10.60 and 15 characters. Detailed analysis of answers to "*Address town*" revealed that 33%

contained “full address” and 67% “address town” or “city name”. The variation in answers indicates ambiguity in the question, which may be difficult to recall during authentication.

The mean completion time of answers to “*House name or number*” was 17.18 seconds with the largest mean answer length of 19.58 characters. Analysis of the answers revealed that the generalisation of the question created ambiguity and answer lengths contained large variations. Answers contained 42% “full home address”, 25% “house number”, 17% “home phone number”, 8% “house name” and 8% “city name”.

Findings revealed ambiguity in the questions designed in this theme, which may also influence effectiveness negatively – to be discussed later in this chapter.

Date Questions: Date is often presented and stored in varied formats. Without specifying a format, users may submit their answers in different formats, which can influence usability. Detailed analysis of answers to *“Date of birth”* revealed that open and varied “date” formats were used by participants, i.e. “dd/mm/yyyy”, “dd-mm-yyyy“, and descriptive month name, e.g. “October 2012”. Using a standard date format can enhance the efficiency of date type questions.

Summary of Efficiency: In summary, participants’ understanding of questions and their ability to answer realistically has an influence on efficiency. Questions with design flaws may result in distraction and trigger a longer response time, which negatively influences the overall efficiency of the challenge questions method. This may lead to usability issues at a later stage during online examinations, which is discussed below. Questions providing answer hints for more clarity resulted in efficient completion time; however, this approach can create security risks, as will be discussed later. The results suggest that question design should consider clarity, ambiguity, syntax and relevance. The potential intervening factors that can negatively influence completion time include typing speed, phone calls, question relevance to an individual, question ambiguity, personal breaks, Internet connection speed, system shutdown, power outages, privacy concerns, etc. The mean completion time of all questions was 15.7 seconds per question. A participant was required to read a question and enter a text reply. This is considered to be a reasonable time, and a user could answer three questions within a mean time of 47.1 seconds (just under a minute). Based on the findings discussed above, the following hypothesis was accepted.

H 6.1) *Text-based challenge questions are efficient when implemented for the authentication of students in online examination.* ***Accepted***

6.4.2 Effectiveness

Effectiveness is considered to be the degree of accuracy of participants' responses. In the context of this study, it means that participants were able to submit correct answers during authentication effectively with a low error rate. It was analysed using data collected from participants' answers during the online examination phase. The questions were divided into five common themes: academic, personal, contact, favourites and date. As discussed earlier, the equality algorithm was implemented for the comparison of answers. Results were also analysed to understand the impact on effectiveness of a more relaxed algorithm being implemented.

The results of the relaxed algorithm were derived from the data collected in the online examination, disregarding capitalisation, white-spaces and minor spelling errors using a combination of substring and distance algorithms as described in an earlier study (Schechter et al., 2009). Table 6-2 shows analysis of data using the equality and relaxed algorithms. Data in columns 5 and 6 presented in boldface shows an increase in effectiveness when results were computed using the relaxed algorithm. In order to test the significance of any differences in the means of correct answers between different themes, a one-way ANOVA test of significance was performed on data shown in Table 6-2. The results of this analysis showed that there were no significant differences in the means F = 1.93, p = 0.15 ($p > 0.05$), eta-squared $\eta^2 = 0.32$. Post hoc comparisons of the groupings yielded no significant results. Answers were submitted by all participants during authentication prior to accessing to the online examination. Challenge questions were presented randomly to participants to simulate a real authentication scenario. Therefore, the sample distribution was not uniform. The effectiveness of challenge questions in different themes is discussed below.

Academic Questions: In a string-to-string comparison, reproducing the exact answer is important. Syntax of questions can be an important factor to reproduce answers when a user is authenticated. As discussed in the preceding section, it was anticipated that questions with an answer hint would be easy to recall during authentication. The challenge question "*Where did you find out about this course*" received 2 (67%) correct answers. Detailed analysis of answers revealed that 1 (33%) answer was penalised for syntactic variation.

Table 6-2 Usability Analysis: Effectiveness of Text-Based Questions

Question Themes	**Effectiveness**				
Academic Questions	**N[2]**	**Equality Algorithm**		**Relaxed Algorithm[1]**	
		Correct	**Incorrect**	**Correct**	**Incorrect**
Student number	1	1(100%)	0(0%)	1(100%)	0(0%)
Year started the current course	3	3(100%)	0(0%)	3(100%)	0(0%)
Year of highest qualification	4	3(75%)	1(25%)	3(75%)	1(25%)
Highest qualification	4	3(75%)	1(25%)	**4(100%)**	**0(0%)**
Find out about this course	3	2(67%)	1(33%)	2(67%)	1(33%)
Name of last school attended	5	3(60%)	2(40%)	**4(80%)**	**1(20%)**
Grades in highest qualification	2	0(0%)	2(100%)	0(0%)	2(100%)
Month started the current course	1	0(0%)	1(100%)	**1(100%)**	**0(0%)**
Total		*15(65%)*	*8(35%)*	*18(78%)*	*5(22%)*
Personal Questions					
Best friend's surname	6	6(100%)	0(0%)	6(100%)	0(0%)
Country of birth	4	4(100%)	0(0%)	4(100%)	0(0%)
Father's surname	3	2(67%)	1(33%)	**3(100%)**	**0(0%)**
Dream job as a child	2	1(50%)	1(50%)	**2(100%)**	**0(0%)**
Total		*13(87%)*	*2(13%)*	*15(100%)*	*0(0%)*
Favourite Questions					
Tutor	6	1(17%)	5(83%)	**5(83%)**	**1(17%)**
Hero of your childhood	3	3(100%)	0(0%)	3(100%)	0(0%)
Module on this course	3	0(0%)	3(100%)	0(0%)	3(100%)
Total		*4(33%)*	*8(67%)*	*8(67%)*	*4(33%)*
Contact Questions					
Home Tel no with country code	2	1(50%)	1(50%)	1(50%)	1(50%)
Home address town	4	1(25%)	3(75%)	**2(50%)**	**2(50%)**
House name or number	4	0(0%)	4(100%)	**1(25%)**	**3(75%)**
Mobile no. with country code	1	0(0%)	1(100%)	0(0%)	1(100%)
Total		*2(18%)*	*9(82%)*	*4(36%)*	*7(64%)*
Date Questions					
Date of birth	5	4(80%)	1(20%)	**5(100%)**	**0(0%)**
Grand Total	**66**	**38(58%)**	**28(42%)**	**50(76%)**	**16(24%)**

[1] Disregard capitalisation, whitespace and minor spelling errors

[2] Number of Challenge Questions

Question clarity, reported in the previous section, also has an impact on recall, when a user is required to reproduce the same answer during authentication. The challenge question "*Month started current course*" received 2 (100%) incorrect answers.

As reported in the efficiency results, the question was not relevant in the context of a simulation course, which led to usability issues. Questions reported with clarity issues in the efficiency analysis translated into poor effectiveness.

Using the equality algorithm, challenge questions in the academic theme received 15 (65%) correct answers. However, there is potential to further improve this by addressing the issues reported here.

The number of correct answers may improve if issues such as syntactic variation and capitalisation are addressed using a relaxed algorithm for answer comparison. Analysis of data revealed that a more relaxed algorithm increased the effectiveness of questions in the academic theme by 13%. Of the incorrect answers, 3 were penalised for capitalisation, spelling mistakes and spacing, factors which could be addressed by using a relaxed algorithm. Implementation of a relaxed algorithm decreased error rate and increased effectiveness to 18 (75%).

Personal Questions: Questions regarding personal information are more memorable and therefore widely used for credential recovery (Schechter et al., 2009). Some challenge questions in the personal theme are reported with better effectiveness. The challenge questions "*Best friend's surname*" and "*Country of birth*" received 100% correct answers during authentication.

Syntactic variations including capitalisation, spacing, spellings and writing syntax can affect the usability of challenge questions. Answers with syntactic variation were lexicographically correct; however, in using a string-to-string comparison such answers were penalised during authentication.

Using the equality algorithm, the challenge questions in the personal theme received 13 (87%) correct answers. The use of the relaxed algorithm increased effectiveness in the personal theme by 13%. Manual sorting of the data revealed that 2 answers were penalised for capitalisation and spacing, which could be addressed by using a relaxed algorithm. Implementation of the relaxed algorithm decreased the error rate and increased the effectiveness to 15 (100%).

Favourite Questions: Questions in the favourite theme are a subset of personal questions, which are associated with an individual's favourites. Some questions pertaining to favourites can be easy to recall. For example, the challenge question "*(Favourite) hero of childhood*" received 3 (100%) correct answers. This was also reported as efficient in the previous section.

As discussed earlier, syntactic variation can increase the usability challenges. The question "*(Favourite) tutor*" received 1 (17%) correct answer. The analysis revealed that 80% of answers were lexicographically correct; however, they were penalised for syntactic variations as described above. Similarly, the challenge question "*(Favourite) module on this course*" was also reported with 0 (0%) correct answers. The analysis revealed that participants produced entirely different answers from those registered in the learning phase. This was due to clarity issues described in the efficiency analysis, and the difficulty for participants to recall and reproduce the registered answers.

Using the equality algorithm, challenge questions in the favourite theme received 4 (33%) correct answers. The relaxed algorithm increased effectiveness by 32%. Manual sorting of the data revealed that 2 answers were penalised for capitalisation, which could be addressed by using the relaxed algorithm. The implementation of the relaxed algorithm decreased the error rate and increased effectiveness to 8 (66%).

Contact Questions: The ambiguous questions identified in the efficiency analysis had a knock-on effect and negatively influenced effectiveness. The challenge questions "*Address town*" and "*House name or number*" received 1 (25%) and 0 (0%) correct answers, respectively. The syntactic variation presented in the efficiency analysis increased the difficulty for participants to reproduce the exact answers in the authentication phase.

Using the equality algorithm, the challenge questions in the contact theme received 2 (18%) correct answers. Questions in the contact theme were also reported to have efficiency issues in the preceding section, which negatively influenced effectiveness. The use of a relaxed algorithm increased the effectiveness of questions in the contact theme by 18%. Manual sorting of the data revealed that 2 answers were penalised for spelling mistakes, which could be addressed by using a relaxed algorithm. The implementation of the relaxed algorithm decreased error rate and increased the overall effectiveness in the contact theme to 4 (36%).

Date Questions: The challenge question "*Date of birth*" received 4 (80%) correct answers during authentication. Syntactic variation in the date format was reported in the efficiency analysis. There was 1 incorrect answer as a result of syntactic variation in the date format.

Using the equality algorithm, challenge questions in the date theme received 80% correct answers; however, it increased to 100% using a relaxed algorithm.

Summary of Effectiveness: In summary, the mean of correct responses to all questions was 58% using the equality algorithm. This increased to 76% using the relaxed algorithm. In an earlier study conducted by Schechter (2009) and sponsored by the Microsoft corporation, participants answered 76% of their challenge questions in a laboratory-based environment with 24% incorrect answers. In another study, Just and Aspinall (2009b) reported 18% incorrect answers in the space of 23 days. Research indicates that challenge questions are fraught with memorability issues and users cannot reproduce 100% exact answers to all their questions.

Results of this empirical study also revealed 42% incorrect answers citing usability issues. The results showed that the questions with more clarity were effective. Questions with low clarity, ambiguity and format issues had poor efficiency, which negatively influenced the effectiveness in the authentication phase. The effectiveness of questions increased from 38 (58%) to 50 (76%) when using the relaxed algorithm to compensate for capitalisation, spacing and spelling mistakes. A paired-sample t-test was performed to compare the mean of correct answers using equality and relaxed algorithms. There was a significant difference in correct answers between the equality algorithm (M = 53.3, SD = 39.2) and relaxed algorithm (M = 71.5, SD = 37.5) conditions; t (19) = -2.9, *p* = 0.007 (*p* < 0.01).

According to the usability scale presented in Chapter 5 (section 5.2.1) and letter grades (i.e. 70-79% acceptable, 80-89% good, +90% exceptional) described by (Bangor et al., 2009), 76% correct answers using a relaxed algorithm is acceptable effectiveness for text-based challenge questions. Similarly, the use of the equality algorithm shows usability issues. Based on the above findings, the following hypothesis was rejected when the equality algorithm (a string-to-string comparison) was implemented. However, it was accepted when a relaxed algorithm was implemented.

H 6.2) *Text-based challenge questions are effective when implemented for the authentication of students in online examination.*

Accepted – relaxed algorithm; Rejected – equality algorithm

In concluding this section, it is noted that question design needs particular consideration to address clarity, ambiguity and relevance. Question design has an important role in the usability of challenge questions.

6.4.2.1 Usability and Traffic Light System

To address the usability challenges posed by the question design, a traffic light access control system was implemented. It was based on the criteria outlined in the “initial configuration" above (section 6.3.2). The data presented in Table 6-4 was collected from the implementation of the challenge questions method, with and without the traffic light access control system. Each participant was presented with 3 challenge questions in a single authentication attempt. The findings revealed that, before using the traffic light system, 23% of the participants submitted correct answers to all their 3 challenge questions and were authenticated successfully. Another 38% participants provided correct answers to 2 out of 3, and 31% to 1 out of 3 challenge questions. However, 8% provided no correct answers to any of their challenge questions in the online examination phase. The reasons for providing incorrect answers were discussed in the preceding section. Before using the traffic light system, the participants who failed to provide correct answers to all of their 3 challenge questions were locked out. The participants who provided correct answers to 1 or 2 of their 3 challenge questions (i.e. 31% + 38% = 69%) were also penalised before implementation of the traffic light access control.

Table 6-3 Results of Traffic Light Access Control System

Authentication Before Traffic Light System				
Attempt	**0/3 Correct**	**1/3 Correct**	**2/3 Correct**	**3/ 3 Correct**
1	1(8%)	4(31%)	5(38%)	3(23%)
Authentication After Traffic Light System				
	Red	**Amber**	**Green**	
	0/3 Correct	**1/3 Correct**	**2/3 Correct or**	**3/3 Correct**
1	1(8%)	4(31%)		8(61%)
2	0(0%)	2(12%)		3(19%)
3	0(0%)	0(0%)		2(12%)

Authentication results were changed after implementation of the traffic light access control. This method compensated for usability issues and improved authentication success rate. A summary of data collected ‘before’ and ‘after’ the traffic light implementation is presented in Table 6-3. The number of correct answers is presented against the number of authentication attempts. Overall, effectiveness has increased from 23% to 92% (61% + 19% + 12%).

The traffic light access control improved the effectiveness of the challenge question approach. However, it is important to consider the security implications when allowing multiple attempts to users providing incorrect answers.

6.5 Security Results

In a follow-up security abuse case test, 6 participants submitted answers to 24 challenge questions in an attempt to impersonate their friends and colleagues. The security analysis presented here is based on the data from the security abuse case scenario described above in the study method.

6.5.1 Impersonation and Guessing by Friends

Tables 6-4 and 6-5 show an analysis of the impersonation and guessing abuse case scenario. A total of 6 participants made 9 attempts to impersonate their friends and colleagues, and guessed answers to challenge questions. They were allowed to perform multiple attempts using the traffic light access control criteria described above.

Table 6-4 Abuse Case Scenario: Traffic Light system

Participants	Attempt	Correct	Incorrect	Authentication
P1	1st	0	3	Failed (Red)
P2	1st	0	3	Failed (Red)
P3	1st	0	3	Failed (Red)
P4	1st	1	2	Repeat (Amber)
P5	1st	1	2	Repeat (Amber)
P6	1st	1	2	Repeat (Amber)
P4	2nd	0	3	Failed (Red)
P5	2nd	0	3	Failed (Red)

Table 6-4 shows analysis of the abuse case scenario in terms of participants' attempts with traffic light access control using the equality algorithm. Of the 6 participants, 3 (50%) failed to guess correct answers to any of their challenge questions on the 1st attempt and were classified as *red*. The remaining 3 (50%) participants guessed correct answers to 1 out of 3 challenge questions and were classified as *amber*. Of the 3 participants' classified *amber*, 1 abandoned the process and the remaining 2 completed the abuse case scenario. In the second attempt, 2 participants were presented with more challenge questions. They failed to guess correct answers to any of these questions.

Table 6-5 Security Analysis: Guessing Abuse Case Scenario

Question Themes	**Security Abuse Case**				
	N	**Equality Algorithm**		**Relaxed Algorithm**	
Academic Questions		**Correct**	**Incorrect**	**Correct**	**Incorrect**
Student number	1	0(0%)	1(100%)	0(0%)	1(100%)
Year started the current course	3	0(0%)	3(100%)	**2(75%)**	**1(25%)**
Year of highest qualification	1	1(100%)	0(0%)	**1(100%)**	**0(0%)**
Highest qualification	2	0(0%)	2(100%)	0(0%)	2(100%)
Find out about this course	0	*NA	*NA	*NA	*NA
Name of last school attended	2	0(0%)	2(100%)	0(0%)	2(100%)
Grades in highest qualification	2	0(0%)	2(100%)	0(0%)	2(100%)
Month started the current course	2	0(0%)	2(100%)	0(0%)	2(100%)
Total		*1(8%)*	*12(92%)*	*3(23%)*	*10(77%)*
Personal Questions					
Best friend's surname	1	0(0%)	1(100%)	0(0%)	1(100%)
Country of birth	2	1(50%)	1(50%)	**2(100%)**	**0(0%)**
Father's surname	1	0(0%)	1(100%)	**1(100%)**	**0(0%)**
Dream job as a child	0	*NA	*NA	*NA	*NA
Total		*1(25%)*	*3(75%)*	*3(75%)*	*1(25%)*
Favourite Questions					
Tutor	1	0(0%)	1(100%)	0(0%)	1(100%)
Hero of your childhood	0	*NA	*NA	*NA	*NA
Module on this course	1	0(0%)	1(100%)	0(0%)	1(100%)
Total		*0(0%)*	*2(100%)*	*0(0%)*	*2(100%)*
Contact Questions					
Home tel. no. with country code	1	0(0%)	1(100%)	0(0%)	1(100%)
Home address town	1	0(0%)	1(100%)	0(0%)	1(100%)
House name or number	1	0(0%)	1(100%)	0(0%)	1(100%)
Mobile number including country code	1	1(100%)	0(0%)	1(100%)	0(0%)
Total		*1(25%)*	*3(75%)*	*1(25%)*	*3(75%)*
Date Questions					
Date of birth	1	0(0%)	1(100%)	0(0%)	1(100%)
Grand Total	**24**	**3(12%)**	**21(88%)**	**7(29%)**	**17(71%)**

Table 6-5 shows the crosstab analysis of the abuse case scenario using the equality and relaxed algorithms. Data presented in boldface in columns 5 and 6 show changes to security level when results were computed using the relaxed algorithm.

Participants were presented 24 challenge questions randomly on behalf of their friends and colleagues. Using the equality algorithm, answers to 3 (13%) questions were successfully guessed by participants, whereas 21 (88%) answers were incorrect. The use of a relaxed algorithm increased the number of correct answers to 7 (29%). The abuse case scenario is discussed below to examine challenge questions in different themes.

Academic Questions: Participants submitted answers to 13 challenge questions in the academic theme and correctly guessed 1 (8%). It was anticipated that academic information would be known to friends and colleagues. However, findings of the abuse case test show that a large number of answers were incorrect. Answers to questions associated with the *current course* were anticipated to be the same for all participants. However, the questions "*Year started current course"* and *"Month started current course*" were guessed incorrectly in all attempts.

The analysis shows an increase in correct answers to 3 (23%) when a relaxed algorithm was used. This indicates that certain questions may be guessed by friends and colleagues in multiple attempts. A review of the academic questions is recommended to mitigate any risks.

Personal Questions: It was anticipated that answers to some personal questions would be correctly guessed by friends and colleagues. Schechter et al. (2009) indicate that personal information can be found on many social media websites. Of the 4 challenge questions, participants guessed 1 (25%) answer correctly. However, the detailed sorting of answers revealed that some were penalised for capitalisation and spaces. The use of a relaxed algorithm increased correct answers to 3 (75%). Furthermore, the analysis of registered answers to *"Father's surname"* in the learning phase revealed that 64% of participants had the same surname as their fathers, which may be easily guessed by friends and colleagues.

Favourite Questions: Participants submitted a total of 2 answers to challenge questions in the favourite theme. The number of questions presented in this theme was small due to randomisation.

A review of security analysis for challenge questions in the favourite theme is recommended in future studies.

Contact Questions: Participants submitted a total of 4 answers to challenge questions in the contact theme; 1 (25%) was guessed correctly.

It is likely that challenge questions relating to home address, phone or mobile numbers, and town can be easily guessed by friends and colleagues. The analysis of data in the contact theme shows that there was no change in results when a more relaxed algorithm was implemented.

Date Questions: Participants submitted one answer to challenge questions in the date theme. Although "*date of birth*" is likely to be known to friends and colleagues, participants failed to guess a correct answer.

The analysis of data in the date theme shows that there was no change in results when a more relaxed algorithm was implemented.

Summary of Security Analysis: In summary, some questions in the personal and academic themes were correctly guessed. 3 (12%) answers were correctly guessed when the equality algorithm was used. This increased to 7 (29%) when a relaxed algorithm was used. The use of a traffic light access control system can increase usability; however, it may provide multiple opportunities to an attacker in a real scenario. Implementation of the traffic light access control system shows a usability and security trade-off. A guessing attack with 71% error rate will alert the course administrator or trigger a process to block access to an attacker. To conclude this section, informed guessing by friends and colleagues was not highly successful; however, security analysis is warranted on a larger sample size. Also, questions in the domains of the public, friends and colleagues may be vulnerable to guessing. Based on the above discussion, the following hypothesis was accepted.

H 6.3) *Text-based challenge questions can mitigate impersonation by friends and colleagues using a guessing attack in online examinations.* ***Accepted***

6.6 Summary

The findings reported in this chapter suggest that challenge question-based authentication in online examinations can be an effective feature to prevent the attacks of adversaries. However, usability and security issues were reported due to flaws in question design. Questions reported to have clarity, ambiguity, relevance and format issues negatively influenced the efficiency and effectiveness results. Participants failed to provide correct answers to challenge questions in the favourite and contact themes due to clarity issues reported earlier. Implementation of the relaxed algorithm to compensate for capitalisation, spelling mistakes and spacing improved usability. The findings suggest that participants were unable to provide correct answers to all of their 3 challenge questions in a single attempt, due to usability issues such as syntactic variation and memorability. Implementation of a traffic light system improved the authentication outcome from 23% to 92%, by allowing multiple chances. However, during the abuse case scenario, the traffic light access control granted 2 out of 6 attackers a second chance to answer more challenge questions in order to re-authenticate. Multiple attempts may encourage attackers to repeat the attack pattern, which needs to be addressed.

The security analysis showed that participants guessed correct answers to some questions on behalf of their friends and colleagues because of poor question design. The findings revealed that answers to questions known to friends, colleagues and in common public knowledge can be a security risk. The overall results showed the potential of using challenge questions for the authentication of students in online examinations. However, secure and usable implementation of the challenge questions method relies upon the quality of question design.

The study was conducted as a proof of concept on a small sample size, conducted in a simulation environment to collect the benchmark data. Virzi's empirical study (1992) on the number of subjects for usability identification indicates that as few as 5 users can identify 80% of the usability issues. However, conclusions cannot be drawn reliably for challenge questions in security analysis due to a small number of participants and, therefore, it is imperative to verify the security results in a real educational context on a larger sample size. In the next study, question design will be revised to address the issues identified in the current study. The next chapter will report an empirical study to investigate the usability attributes of text-based and image-based questions in a real online course on a larger sample size.

7 Study 2 – Image-Based and Text-Based Challenge Questions

The previous chapter described the first empirical study using an initial prototype, which identified a number of issues, including questions ambiguity, relevance, syntactic variation, spellings and spacing. These issues negatively influenced the usability of text-based questions. In order to address these issues, an image-based challenge question approach is proposed and evaluated using a real online course. This chapter presents an empirical study to investigate the usability of text-based and image-based challenge questions. Furthermore, the chapter describes the purpose, research questions, hypotheses and research method. The following sections explain participants' recruitment, the design of an online course, and study phases, in order to describe how the problem was approached and the online course conducted. The study involved remote online students from nine countries. Finally, the chapter reports the efficiency and effectiveness analysis of text-based and image-based questions.

7.1 Purpose

The previous study described in Chapter 6 indicated usability and security issues in the use of text-based challenge questions due to weak question design (Ullah et al., 2014a). The study evaluated the usability attributes of efficiency and effectiveness. These are common attributes defined by the ISO, which contribute to usability (ISO9241-11, 1998).

In response to the risks and usability issues indicated in Chapter 6, the design of text-based questions was revised and multiple-choice image-based questions introduced for use in this study. Research indicates that humans are better at remembering images than text (Shepard, 1967). Image-based authentication has been adopted for a number of online services. For example, the Bank of America utilises a site key image combined with text-based challenge questions to authenticate users (Youll, 2006). Renaud and Just (Renaud and Just, 2010) reported enhanced usability while using association-based image questions for authentication purposes. This study will investigate the following:

1. The usability attributes, i.e. efficiency and effectiveness of text-based and image-based questions in an online examination context.

7.2 Research Questions and Hypotheses

The research questions identified in Chapter 1 are cascaded into more questions associated with the usability attributes of efficiency and effectiveness using text-based and image-based questions. The research question RQ 3) is associated with the usability attributes of the proposed method. This study attempts to answer the following research questions, which are derived from RQ 3a) and RQ 3b):

RQ 7.1) How does an increase in the interaction with text-based and image-based questions influence efficiency when implemented in an online learning and examinations context?

RQ 7.2) How effective are text-based challenge questions when implemented for authentication in online examinations?

RQ 7.3) How effective are multiple-choice image-based challenge questions when implemented for authentication in online examinations?

The following hypotheses were framed to answer the above research questions. Each hypothesis maps to a corresponding research question:

H 7.1) An increase in interaction with text-based and image-based questions increases efficiency when implemented for authentication in online examinations.

H 7.2) Text-based challenge questions are effective when implemented for authentication of students in online examinations.

H 7.3) Image-based challenge questions are effective when implemented for authentication of students in online examinations.

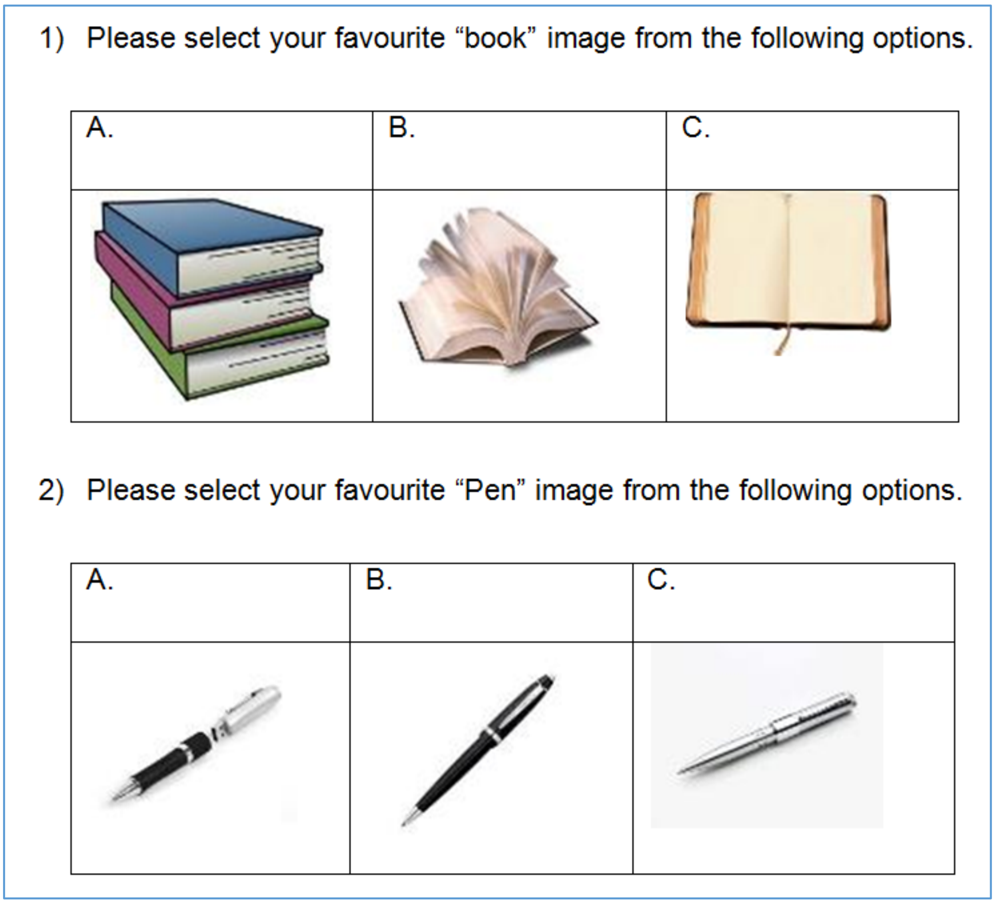
7.3 Study Method and Design

The usability test method described in Chapter 5 was used to evaluate the usability attributes of efficiency and effectiveness. It is a usability inspection method, which tends to focus on the interaction between humans and computers (Corry et al., 1997). Using this method, the representative users (i.e. students) interact with online learning and examinations using text-based and image-based challenge questions for authentication. The usability evaluation scale described in Chapter 5 (section 5.2.1) was used for the effectiveness analysis. This scale translates usability of products in the 90s as exceptional, 80s as good, 70s as acceptable and anything below 70s indicates issues that are a cause for concern (Bangor et al., 2009).

The study design and methodology was approved by the University of Hertfordshire research ethics committee. The design of an online course, text-based questions, image-based questions and study phases are described below.

7.3.1 Text-Based and Image-Based Questions Design

In order to address the usability issues indicated in the first study, text-based questions were revised and replaced with alternatives giving careful design consideration to mitigate ambiguity and clarity issues (Ullah et al., 2014a). 31 text-based questions were designed and classified into 4 themes: academic, favourite, personal, and date as shown in Appendix A-I and presented in Table 7-2 below.



1) Please select your favourite “book” image from the following options.

A.	B.	C.

2) Please select your favourite “Pen” image from the following options.

A.	B.	C.

Figure 7-1 Example of Image-based Questions

Image-based questions were introduced, as shown in Appendix A-II and Table 7-3 below. Figure 7-1 shows example of image-based questions. The use of image authentication has been adopted for a number of reasons. Renaud and Just (2010) identified enhanced usability while using association-based image questions. Humans are better at memorising pictures than words (Wiedenbeck et al., 2005, Chiasson et al., 2007). De Angeli et al. (2005) state that pictures substitute the need to memorise and recall text-based tokens. They indicated that image authentication may overcome issues related with text-based authentication. The security is related with the difficulty of sharing or recording images to promote insecure practices (Weinshall and Kirkpatrick, 2004). Given the anticipated benefits, this study implemented multiple-choice image-based challenge questions. These questions were designed using the following two types:

- *Recall Image-Based Questions:* Recall is the ability to remember something learned or experienced. Shephard (Shepard, 1967) indicates that humans are better at recalling images than words, which is driven by the “picture superiority effect”. The recall image-based method requires a user to recall and select their previously chosen images. For example, a user is initially required to register a choice from multiple images. Later, the user is presented with multiple images again to recall and identify his selection (Wiedenbeck et al., 2005).
- *Recognition Image-Based Questions:* These rely upon an individual’s ability to judge whether he/she has seen or selected an image before (Hayashi et al., 2011). The correct image is presented with a set of distraction images and the user is asked to recognise a previously viewed or chosen image.

A total of 13 image-based questions were designed for this study, as shown in Appendix A-II and Table 7-3 below. These images were randomly searched from Google using “teaching”, “learning”, ”assessment”, “nature”, “birds” and “animals” keywords. These were selected using the following guidelines:

- Images of the same type were selected for each multiple choice question as shown in Figure 7-1.
- Images of the same type were chosen with different colours, and orientation.
- Images with rich and contrasting colours were chosen for nature, birds and animals.

7.3.2 Conducting the Study and Online Course

The study was organised in multiple phases to provide learning opportunities to students and achieve the research objectives. Study phases are described below:

- **PHP & MySQL Course Design**: An online course in PHP and MySQL was set up and deployed in the MOODLE Learning Management System (LMS) on a remote web server. The course contents were released on a daily basis to engage participants and increase their interest and number of visits. A weekly online multiple-choice question (MCQ) quiz was set up as a summative online examination. Participants were recommended to invest 10 hours' weekly learning effort for 25 days over a span of 5 weeks.

- **Participants Recruitment:** In order to motivate and recruit participants, the course was offered free of charge on the University of Hertfordshire online portal. Participants were required to have basic programming knowledge in order to enrol. A total of 70 students were recruited. The distribution of participants was not uniform across countries and cities, but there was a good level of representation from a diverse group of students from 9 countries. Of the 70 students, 50 (71%) were from the United Kingdom. 11 (16%) students were from Pakistan, 2 (4%) from Malta and Nigeria, plus 1 (1%) each from Ireland, Greece, India, Trinidad and Tobago, and Togo. There was no repeated attendance of participants from the previous study presented in Chapter 6.
- **Student Registration**: Guidance notes and an enrolment key for registration were emailed to all participating students. The course was only available to registered users. Registration was a standard MOODLE sign-up process, which was essential to create login credentials to access the online course. Upon successful registration, participants received their login-identifier and password. The course was launched and made available to students after registration.
- **Online Coursework:** The course was presented over a period of 5 weeks. To collect data for the evaluation of usability and security, the transactional information, including completion time of profile questions and challenge questions authentication results, were stored in a database. Answers to profile questions were collected during the coursework to build and consolidate an individual student's profile.
- **Weekly Quizzes:** The course contained 5 quizzes, which were released on a weekly basis, one by one, towards the end of each week on completion of the weekly coursework. The weekly course content was released to those participants who completed their weekly quizzes, e.g. week 2 content was released to participants who completed the week 1 quiz. Participants were authenticated using challenge questions stored in their individual profiles and recorded during the coursework. A total of three challenge questions were randomly presented during the authentication process.

7.4 Usability Results

A total of 70 participants answered 2315 profile questions during the course. The weekly quizzes were attempted by 48 participants, who answered 1347 challenge questions. A usability test analysis was performed to evaluate the usability attributes of efficiency and effectiveness, which are discussed below.

7.4.1 Efficiency of Text- and Image-Based Questions

Efficiency was analysed by computing the completion times of students answering their profile questions. The total number of profile questions collected was higher than the number of challenge questions posed for authentication. A student needed to access the course work recurrently and the completion time of profile questions presented during the course would be expected to relate to efficiency. Table 7-1 shows mean and standard deviation scores of the completion time variable.

Table 7-1 Usability Analysis: Efficiency

	Completion Time in seconds		
Visit No.	**Mean**	**SD**	**N = Visitors**
1	74.87	59.48	70
2	62.28	61.77	60
3	53.22	63.52	54
4	43.26	47.92	50
5	32.07	15.13	44
6	45.18	41.37	40
7	43.05	38.15	38
8	44.42	41.98	38
9	46.11	34.20	35
10	47.32	38.84	34
11	37.93	23.43	29
12	43.50	30.18	24
13	42.50	67.65	23
14	40.57	31.08	19
	49.59	**47.13**	**558**

A decrease can be seen in completion time of profile questions from 74.87 to 40.57 seconds, which indicates increased efficiency with an increase in the number of visits. In order to test the significance of any trend in the data presented in Table 7-1, a one-way ANOVA was performed with linear contrasts. A significant trend was confirmed for completion time in multiple visits F = 8.39, *p* = 0.004, eta-squared η^2 =

0.02. A Pearson correlation was performed to assess the direction of the trend on each subsequent visit (r = -0.171, n= 558, *p* = 0.00). The findings indicate a decrease in completion time with an increasing number of visits. Figure 7-2 shows a graphical representation of analysis, which shows a linear and decreasing trend.

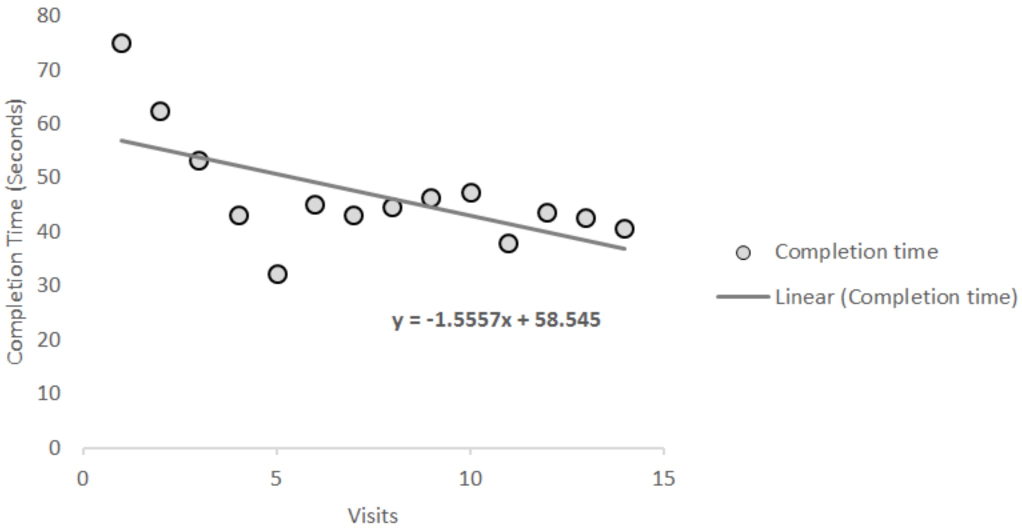


Figure 7-2 Trend Graph – Completion Time

A learning curve can be observed and participants were familiarised with the process in subsequent visits. Based on the above discussion, the following hypothesis was accepted.

H 7.1) *An increase in interaction with text-based and image-based questions increases efficiency when implemented for authentication in online examinations.* ***Accepted***

7.4.2 Effectiveness of Text- and Image-Based Questions

A total of 890 text-based and 457 image-based questions were answered by participants to authenticate their identity in five weekly quizzes. Findings of the effectiveness analysis are discussed in the following sections.

7.4.2.1 Text-Based Questions

To examine the effectiveness of text-based challenge questions, an analysis of correct answers during the weekly quizzes was performed. Capitalisation and spaces were treated programmatically and the equality algorithm (string-to-string comparison) was implemented for authentication purposes (Ullah et al., 2014a, Schechter et al., 2009). Results in Table 7-2 show that, of the 890 text-based challenge questions

Table 7-2 Usability Analysis: Effectiveness of Text-Based Questions

Questions Theme	**Equality Algorithm**	**Failure Reason**		**Relaxed Algorithm**
	Correct / In Correct *N (%)*	**Syntactic Variation**	**Recall**	**Correct / In Correct *N (%)***
Academic				
Student number	29 (81%)/ 7 (19%)	0(0%)	7(100%)	29 (81%) / 7 (19%)
First school attended	21 (75%)/ 7 (25%)	4(57%)	3(43%)	25 (89%) / 3 (11%)
Level achieved best grades	18 (69%)/ 8 (31%)	1(12%)	7(88%)	19 (73%) / 7 (27%)
Grades in highest qualification	13 (65%)/ 7 (35%)	2(29%)	5(71%)	15 (75%) / 5 (25%)
Last school attended	15 (50%)/ 15 (50%)	8(53%)	7(47%)	21 (70%) / 9 (30%)
Year of graduation	21 (48%)/ 23 (52%)	0(0%)	23(100%)	21 (48%) / 23 (52%)
Total	**117(64%)/67 (36%)**	**15 (22%)**	**52 (78%)**	**130 (71%) / 54(29%)**
Favourite				
Colour	26 (84%)/ 5 (16%)	1(20%)	4(80%)	27 (87%) / 4 (13%)
TV programme	22 (79%)/ 6 (21%)	1(17%)	5(83%)	23 (82%) / 5 (18%)
Website URL	16 (73%)/ 6 (27%)	1(17%)	5(83%)	17 (77%) / 5 (23%)
Car Colour	13 (72%)/ 5 (28%)	3(60%)	2(40%)	15 (83%) / 3 (17%)
Cousin name-3 letters	21 (72%)/ 8 (28%)	0(0%)	8(100%)	21 (72%) / 8 (28%)
Bird	29 (71%)/ 12 (29%)	2(17%)	10(83%)	31 (76%) / 10 (24%)
Animal	16 (70%)/ 7 (30%)	0(0%)	7(100%)	16 (70%) / 7 (30%)
Car	20 (69%)/ 9 (31%)	4(44%)	5(56%)	22 (76%) / 7 (24%)
Childhood place to visit	17 (65%)/ 9 (35%)	2(22%)	7(78%)	17 (65%) / 9 (35%)
Academic course	20 (65%)/ 11 (35%)	5(36%)	6(55%)	21 (68%) / 10 (32%)
Tutor	19 (63%)/11 (37%)	2(18%)	9(82%)	21 (70%) / 9 (30%)
Movie	12 (63%)/ 7 (37%)	3(43%)	4(57%)	15 (79%) / 4 (21%)
Holiday destination	19 (58%)/ 14 (42%)	1(7%)	13(93%)	19 (58%) / 14 (42%)
Childhood hero	21 (58%)/ 15 (42%)	2(13%)	13(87%)	23 (64%) / 13 (36%)
Food	21 (53%)/ 19 (47%)	0(0%)	19(100%)	21 (53%) / 19 (47%)
Book	9 (33%)/ 18 (67%)	4(22%)	14(78%)	12 (44%) / 15 (56%)
Total	**301(65%)/ 162(35%)**	**31(19%)**	**131(81%)**	**321(69%) /142(31%)**
Personal				
Country of dream vacation	29 (83%)/ 6 (17%)	2(33%)	4(67%)	31 (89%) / 4 (11%)
Grandfather's surname	31 (74%)/ 11 (26%)	1(9%)	10(91%)	22 (67%) / 11 (33%)
Best friend's surname	14 (64%)/ 8 (36%)	1(13%)	7(88%)	15 (68%) / 7 (32%)
Dream job as a child	19 (58%)/ 14 (42%)	6(43%)	8(57%)	24 (73%) / 9 (27%)
Best childhood friend	16 (48%)/ 17 (52%)	7(41%)	10(59%)	36 (86%) / 6 (14%)
Total	**109 (66%)/ 56 (34%)**	**17 (30%)**	**39 (70%)**	**128 (78%) /37 (22%)**
Date				
Date of birth	10 (50%)/ 10 (50%)	10(100%)	0(0%)	20 (100%) / 0 (0%)
Year of birth	13 (87%)/ 2 (13%)	1(50%)	1(50%)	26 (100%) / 0 (0%)
Day of birth	22 (85%)/ 4 (15%)	4(100%)	0(0%)	17 (100%) / 0 (0%)
Month of birth	11 (65%)/ 6 (35%)	6(100%)	0(0%)	14 (93%) / 1 (7%)
Total	**56 (72%)/ 22 (28%)**	**21 (96%)**	**1(4%)**	**77 (99%) / 1 (1%)**
Grand Total	**583(66%)/307(34%)**	**84(27%)**	**223(73%)**	**656 (74%)/234(26%)**

randomly presented to students, 583 (66%) were answered correctly during the authentication process.

Students submitted incorrect answers to 307 (34%) questions due to recall and syntactic variation, which is discussed later.

The text-based challenge questions were analysed into four themes. In order to test the significance of any differences in the means of correct responses to questions shown in Table 7-2, a one-way ANOVA test of significance was performed. The results of this analysis showed that there was no significant difference in the means of correct answers between different themes ($p > 0.05$). The mean effectiveness of text-based questions was 66%, which increased to 74% when the data was analysed using a relaxed algorithm to compensate for spelling mistakes and syntactic variation.

According to the usability scale presented in Chapter 5 (section 5.2.1) and letter grades (i.e. 70-79% acceptable, 80-89% good, +90% exceptional) described by (Bangor et al., 2009), 66% correct answers using the equality algorithm indicates usability issues, whereas 74% correct answers using the relaxed algorithm is an acceptable level of effectiveness. Based on the above discussion, the following hypothesis was rejected using the equality algorithm and accepted using the relaxed algorithm.

H 7.2) *Text-based challenge questions are effective when implemented for authentication of students in online examinations.*

Rejected – equality algorithm; Accepted – relaxed algorithm

The findings are encouraging; however, the number of incorrect answers was 26% even if a more relaxed algorithm was implemented to compensate for spelling mistakes and incorrect syntax. This indicates memorability issues with some text-based questions.

7.4.2.2 Effectiveness of Image-Based Questions

The effectiveness analysis of both “Recall” and “Recognition” image-based challenge questions is shown in Table 7-3. Image-based questions used in this study are shown in Appendix A-II. As discussed earlier, the “Recognition” image questions were derived non-intrusively in the background while students answered their multiple-choice image-based questions. A student’s answer was used with a random subset of distraction images. These distraction images were not shown to participants previously. They were required to recognise their previously chosen image from a set of distraction images.

Of the total of 457 image-based challenge questions, 389 (85%) were answered correctly during authentication. The effectiveness result for the text-based questions described above was 66% using the equality algorithm and 74% using the relaxed algorithm. Implementation of multiple-choice questions addressed the issue of syntactic variation, capitalisation, formatting and spelling mistakes, which increased effectiveness. Results in Table 7-3 show that "Recall" and "Recognition" image-based questions received 192 (80%) and 197 (90%) correct answers, respectively.

Table 7-3 Usability Analysis: Effectiveness of Image-Based Questions

Question Description	**Type**	**Correct / Incorrect** ***n (%)*** ***n = number of answers***
Recall-based image questions		
Pen	Object	15 (79%) / 4 (21%)
Book	Object	7 (70%) / 3 (30%)
Pen & Inkpot	Object	10 (63%) / 6 (38%)
Examination	Logo	15 (100%) / 0 (0%)
Science	Logo	18 (100%) / 0 (0%)
Online Learning	Logo	16 (94%) / 1 (6%)
Graduation	Logo	24 (73%) / 9 (27%)
Internet Security	Logo	10 (53%) / 9 (47%)
Peace	Logo	17 (89%) / 2 (11 %)
Fish	Nature	20 (100%) / 0 (0%)
Flower	Nature	12 (86%) / 2 (14%)
Deer	Nature	20 (77%) / 6 (23%)
Bird	Nature	8 (62%) / 5 (38%)
Total		**192(80%)/47(20%)**
Recognition-based image questions		
Recognise image you have chosen before	Mixed	197 (90%) / 21 (10%)
Total		**197 (90%) / 21 (10%)**
Grand Total		**389 (85%) / 68 (15%)**

The “recognition” image-based questions received 10% more correct answers than the “recall” questions. A participant was presented a previously chosen (seen) image with a set of distraction images. These distraction images were randomly extracted from a pool of 50 images, which were not seen by the participant before. This is likely to have enhanced the implicit recall. Research in psychology suggests that implicit learning and memory of visual context can guide spatial attention (Chun and Jiang, 1998). Implicit memory is unintentional retrieval of previously acquired information (Roediger, 1990, Schacter, 2016). The above results indicate that this phenomenon may be a factor which helped participants to provide an increased number of correct answers to “recognition” image-based questions, which enhanced the effectiveness.

The following section presents a comparative analysis of text-based and image-based questions.

7.4.2.3 Comparison of Text-Based and Image-Based Questions

The effectiveness of image-based questions was significantly better than that of the text-based challenge questions ($p < 0.01$). An independent sample t-test was performed on the data shown in Tables 7-2 and 7-3 to compare the mean of correct answers between text- and image-based questions. There was a significant difference in effectiveness between text- (M=66.12, SD=12.6) and image-based questions (M=81.92, SD=13.95) conditions t (42) =-3.67; $p = 0.001$ ($p < 0.01$). The use of image-based questions resulted in greater effectiveness by minimising usability problems such as syntactic variation, spacing, capitalisation, spelling mistakes and memorability.

In order to test the significance of any differences in the means of correct answers between text and image questions, shown in Table 7-2 and 7-3 according to the *equality* and *relaxed* algorithms, a one-way ANOVA test of significance was performed. The results of this analysis showed that there were significant differences in the means F = 6.11, $p = 0.004$ ($p < 0.01$), eta-squared $\eta^2 = 0.14$. Post hoc comparisons of the groupings yielded the following significant results.

Text-based (equality algorithm) x Image-based, mean difference (MD) = -14.33, Standard Error (SE) = 4.94, $p = 0.028$ ($p < 0.01$) Text-based (equality algorithm) x Text-based (relaxed algorithm), MD = -9.2, SE = 3.39, $p = 0.026$ ($p < 0.01$). No other significant differences were found in the post hoc comparisons. The findings indicate that the use of image-based questions increased effectiveness by addressing the issues related with syntax, spellings, spacing and formatting. However, the use of a relaxed algorithm also increased effectiveness, which compensated the stated issues. There was no significant difference in effectiveness between image-based questions and text-based questions using a relaxed algorithm.

The use of image-based questions is encouraging for better usability. In an earlier study, Renaud and Just (2010) reported a 13% increase in memorability while using association-based pictures in authentication. Multiple-choice image-based questions indicate more potential and increased answer recall. According to the usability scale described in Chapter 5 (section 5.2.1), 82% correct answers indicates a good level of effectiveness. Based on the above findings the following hypothesis was supported.

H 7.3) *The image-based challenge questions are effective when implemented for authentication of students in online examinations.* ***Accepted***

7.4.2.4 Recall and Syntactic Variation

This section discusses the proposed reasons, of recall and syntactic variation, for incorrect answers during the authentication process. Answer recall or memorability has been an ongoing issue with challenge questions (Schechter et al., 2009). Manual sorting of the answers revealed that memorability was not the only reason for incorrect results. For the purpose of this analysis, recall and syntactic variation was identified based on manual sorting of answers. If a participant's answers to profile and challenge questions were different, it was considered a result of recall. If a participant's answers to profile and challenge questions had a variation in syntax (e.g. "http://google.com" and "www.google.com") or spelling mistakes, it was considered a result of syntactic variation. Results of this analysis are presented in Table 7-2 for text-based questions only. Image-based questions were multiple-choice and therefore, the syntactic variation was not applicable.

Of the total incorrect answers to text-based questions, 223 (70%) were a result of recall and 94 (30%) syntactic variation. 68 (100%) incorrect answers to image-based questions shown in Table 7-3 were attributed to answer recall.

Answers to subjective questions such as individual favourites in the "Favourite" theme received 81% incorrect answers due to recall.

Formatted answers were prone to syntactic variation. Of all the incorrect answers in the "Date" theme, 95% were a result of variation in date syntax. Students were advised to submit their answers to date questions in a British date format, i.e. "dd/mm/yyyy". This indicates that formatted answers should be validated for better usability. A standard syntax such as a calendar/date picker could be enforced from the user interface to counter this issue

The use of the equality algorithm (string-to-string comparison) penalised answers with syntactic variation and spelling mistakes, which would otherwise be considered correct if a more relaxed algorithm was used. Data in Table 7-2 columns 2 and 3 show the results of the equality algorithm. Similarly, data in Table 7-2 column 4 shows the results of a more relaxed algorithm. This was compiled using a substring and distance algorithms (Schechter et al., 2009). It compensates for syntax variation such as date format and spelling mistakes. A paired-sample t-test showed a significant difference in effectiveness between the equality (M = 66.12, SD = 12.6) and relaxed (M = 75.35, SD = 14.09) algorithm conditions t (30) = -4.33; *p* = 0.00 (*p* < 0.01). This indicates that addressing issues relating to syntax, spellings and capitalisation can significantly enhance usability.

7.5 Summary

This chapter reported a comparative analysis of the usability attributes of both text-based and image-based challenge questions in the context of online examinations. Text-based questions were reported to have syntactic variation and recall issues in a study reported in Chapter 6 with 38 (58%) correct answers. Questions reported to have ambiguity and usability issues were revised and the number of correct answers in this study was enhanced to 583 (66%) using the equality algorithm and 74% using the relaxed algorithm. The use of a relaxed algorithm improved usability of text-based questions significantly (p < 0.01). Introduction of image-based questions further increased the usability results. There was a significant difference (p < 0.01) in the effectiveness between recognition image questions 197 (90%), recall image questions 192 (80%) and text-based questions 583 (66%).

While the usability findings are positive, it is important to investigate how the challenge question approach influences impersonation attacks. Text-based questions are associated with an individual's personal information and students may be able to share the answers with third party impersonators in impersonation attacks. The next chapter will present a study to investigate these attacks using a risk-based security assessment method.

8 Study 3 – Impersonation and Text-based Challenge Questions

Text-based challenge questions are associated with an individual’s personal information. It is anticipated that students may be able to share this information with a third party impersonator to perform an impersonation attack. This chapter presents study three, which examines impersonation attacks using pre-defined text-based challenge questions. This study explores the influence of sharing questions with a third party impersonator. It investigates how the number of questions shared and the size of the database affect the success of an impersonation attack. This chapter provides the purpose, research questions, hypotheses and research method. The following sections explain the participants’ recruitment, the design of the challenge questions, and the study phases. This includes a description of an abuse case scenario using a simulation web application to investigate impersonation attacks. The study involved sharing challenge questions with the participants, who simulated impersonation using different numbers of shared questions and database sizes. Finally, the chapter reports the findings of the impersonation abuse case scenario.

8.1 Purpose

This study investigates how the proposed challenge question method influences impersonation attacks. The description of these attacks is provided in Chapter 3 – they could happen in two phases, if a challenge question approach were implemented. Firstly, a student would need to share his or her questions and answers with a third-party impersonator. Secondly, the third party impersonator would use the shared information to answer the challenge questions in order to impersonate the student and take the online test. Therefore, a successful attack would rely upon a student’s ability to share as many challenge questions with a third party as possible. Further, it would rely upon the impersonator’s ability to memorise or search and locate the correct answer from the shared information, in order to authenticate and impersonate a student. This study investigates the following:

1. The influence of *sharing* challenge questions and *database size* on impersonation attacks in a simulation abuse case scenario.

The attacker may search and locate correct answers from the shared information using a printed or electronic copy. However, if an online examination process is monitored or if the authentication process is timed, the attacker would need to memorise the shared challenge questions and answers. This study also investigates the following:

2. The influence of using a printed or electronic source and memory, when answering the challenge questions during the impersonation attack.

8.2 Research Questions and Hypotheses

The research question RQ 4) associated with collusion threats (see Chapter 1) is cascaded into further questions associated with impersonation attacks using text-based challenge questions. This study attempts to answer the following research questions, which are derived from RQ 4a):

RQ 8.1) How does an increase in the number of shared challenge questions influence the success of an impersonation?

RQ 8.2) How does the size of a database influence the success of an impersonation attack?

RQ 8.3) How does a response of an impersonator influence the success of an impersonation attack, when challenge questions are memorised or copied for impersonation?

The following hypotheses were framed in order to answer the above research questions. Each hypothesis maps to a corresponding question:

H 8.1) The larger the number of challenge questions shared, the more successful an impersonation attack will be.

H 8.2) The larger the database size, the less successful an impersonation attack will be.

H 8.3) There is a measure difference in the success of an impersonation attack, when challenge questions are memorised or searched and copied for impersonation.

8.3 Study Method

The study was conducted in a controlled simulation environment. The risk-based security assessment method described in Chapter 5 was adopted to perform impersonation attacks. This method focuses on testing the features and functions of artefacts based on the risk of their failure using abuse case scenarios (McGraw, 2004). An abuse case scenario was designed and simulated using a web-based application to analyse the influence of sharing the number of questions and the database size.

The study was organised in the following phases: designing challenge questions, creating an online database, recruiting participants and finally simulating an abuse case scenario.

- **Designing Challenge Questions**: A total of 50 text-based challenge questions were created as shown in Appendix B (I). Only pre-defined text-based questions were implemented in order to simulate the impersonation abuse case scenario. A subset of these questions was used in study two, described in Chapter 7. The questions were associated with personal, academic, and favourite themes.
- **Online Simulation Databases**: An online challenge question database and web-based application was set up to simulate impersonation. Fifty challenge questions and answers designed for this study (see Appendix B (I)), were uploaded to the web-based application. The application implemented three different database sizes, i.e. 20, 30, and 50, which were hosted on a web server. The answers to the questions in these databases were uploaded from the profiles of three different students who participated in study three, described in Chapter 7 above.
- **Participants Recruitment:** A total of 15 participants from the University of Hertfordshire, Southampton University, Cardiff University, the University of South Wales and the Institute of Management Sciences Pakistan volunteered to participate in the simulation abuse case tests. The majority of participants were researchers and programmers collaborating on different research projects. There was no repeated attendance of participants from the previous studies presented in Chapter 6 and 7.

8.3.1 Simulating Impersonation Abuse Case Scenarios

The following collusion abuse case scenario was simulated sharing different numbers of questions and database sizes:

> *A student is registered on an online course. The course uses the challenge question approach for authentication of students in online examinations. The student is due to write his final semester online test. He or she wants to boost his/his grades and recruit a third party to impersonate and take the test. However, to satisfy the challenge questions authentication, the student is required to share his/her challenge questions and answers with the third party helper in order to help with the impersonation. The third party helper*

would use the shared information to answer the randomly presented challenge questions for authentication.

Given the above scenario, this study simulated the following sharing on database containing 20, 30, and 50 questions. Different numbers of profile questions and answers were shared as shown in Table 8-1 below:

Table 8-1 Impersonation Abuse Case: Sharing Questions

Database size 50	
1) 0 or no sharing:	A student is unable to share any questions with a third-party helper. In an attempt to impersonate and access the online examination, the third party uses random guessing to answer the challenge questions. This attack was simulated on the largest database size (50).
Database size 20	
2) Share 8	A student shares 8 answers of his database size 20 with a third party helper.
3) Share 12	A student shares 12 answers of his database size 20 with a third party helper.
4) Share 20	A student shares 20 answers of his database size 20 with a third party helper.
Database size 30	
5) Share 12	A student shares 12 answers of his database size 30 with a third party helper.
6) Share 18	A student shares 18 answers of his database size 30 with a third party helper.
7) Share 30	A student shares 30 answers of his database size 30 with a third party helper.
Database size 50	
8) Share 20	A student shares 20 answers of his database size 50 with a third party helper.

9) Share 30	A student shares 30 answers of his database size 50 with a third party helper.
10) Share 50	A student shares 50 answers of his database size 50 with a third party helper.

The simulation process is described below starting from the guessing attack with no answers shared:

1) A participant was asked to access the application and randomly guess answers to 50 challenge questions as shown in Table 8-1.

To understand the influence of sharing using different database sizes, different sharing conditions were tested for all three database sizes (20, 30 and 50 respectively) in a sequence shown in Table 8-1 and described below.

2) A total of 8 challenge questions and answers were shared with a participant via email to simulate impersonation (see Table 8-1).

3) The participant accessed the database and answered 5 challenge questions randomly presented from database size 20 using the shared questions and answers.

4) The number of shared questions was then increased to 12 and 20 respectively.

5) The above steps were repeated for databases size 30 and 50 and the number of questions shared.

Of the total 15 participants simulating the above scenarios, 10 participants answered the challenge questions using an *electronic or printed copy* shared through email. The other 5 participants answered the challenge questions by memorising the answers from the shared email. The participants were not allowed to copy or see the shared email while answering the questions from memory. Data from the study was stored in the respective database, which is analysed in the following section.

8.4 Security Results

This section presents the security analysis extracted from the simulation attacks. Tables 8-2 and 8-3 show the security analysis of the impersonation abuse case performed by 15 participants using three different database sizes. The results of the 10 participants who answered challenge questions from an electronic or printed copy are presented in Table 8-2. The results of the 5 participants who memorised the answers before responding the challenge questions are presented in Table 8-3. Detailed security analysis on the data is presented below:

Table 8-2 Sharing: Answers Copied for Impersonation

Database Size 50		**Database Size 20**			**Database Size 30**			**Database Size 50**		
P#	**0** *n = 50*	**8** *n = 5*	**12** *n = 5*	**20** *n = 5*	**12** *n=5*	**18** *n = 5*	**30** *n = 5*	**20** *n = 5*	**30** *n = 5*	**50** *n = 5*
Answers Copied for Impersonation										
1	3(6%)	2(40%)	5(100%)	5(100%)	1(20%)	3(60%)	5(100%)	2(40%)	2(40%)	5(100%)
2	1(2%)	1(20%)	5(100%)	5(100%)	2(40%)	4(80%)	5(100%)	2(40%)	2(40%)	5(100%)
3	1(2%)	3(60%)	4(80%)	5(100%)	1(20%)	2(40%)	5(100%)	1(20%)	3(60%)	5(100%)
4	2(4%)	2(40%)	2(40%)	5(100%)	2(40%)	2(40%)	5(100%)	1(20%)	1(20%)	5(100%)
5	1(2%)	2(40%)	4(80%)	5(100%)	2(40%)	3(60%)	5(100%)	0(0%)	2(40%)	5(100%)
6	1(2%)	2(40%)	3(60%)	5(100%)	3(60%)	2(40%)	5(100%)	2(40%)	3(60%)	5(100%)
7	3(6%)	2(40%)	2(40%)	5(100%)	1(20%)	2(40%)	5(100%)	2(40%)	2(40%)	5(100%)
8	1(2%)	3(60%)	3(60%)	5(100%)	2(40%)	3(60%)	5(100%)	2(40%)	2(40%)	5(100%)
9	3(6%)	2(40%)	3(60%)	5(100%)	2(40%)	2(40%)	5(100%)	1(20%)	2(40%)	5(100%)
10	1(2%)	2(40%)	2(40%)	5(100%)	2(40%)	2(40%)	5(100%)	2(40%)	3(60%)	5(100%)
	17(3%)	**21(42%)**	**33(66%)**	**50(100%)**	**18(36%)**	**25(50%)**	**50(100%)**	**15(30%)**	**22(44%)**	**50(100%)**

Table 8-3 Sharing: Answers Memorised for Impersonation

Database Size 50		**Database Size 20**			**Database Size 30**			**Database Size 50**		
P#	**0** *n = 50*	**8** *n = 5*	**12** *n = 5*	**20** *n = 5*	**12** *n=5*	**18** *n = 5*	**30** *n = 5*	**20** *n = 5*	**30** *n = 5*	**50** *n = 5*
1	1(2%)	2(40%)	3(60%)	2(40%)	2(40%)	0(0%)	4(80%)	1(20%)	1(20%)	3(60%)
2	1(2%)	2(40%)	2(40%)	1(20%)	1(20%)	1(20%)	2(40%)	2(40%)	2(40%)	1(20%)
3	0(0%)	1(20%)	2(40%)	3(60%)	1(20%)	3(60%)	2(40%)	2(40%)	3(60%)	3(60%)
4	2(4%)	2(40%)	1(20%)	1(20%)	2(40%)	1(20%)	2(40%)	2(40%)	2(40%)	2(40%)
5	3(6%)	2(40%)	3(60%)	2(40%)	1(20%)	4(80%)	2(40%)	2(40%)	3(60%)	3(60%)
	7(2.8%)	**9(36%)**	**11(44%)**	**9(36%)**	**7(28%)**	**9(36%)**	**12(48%)**	**9(36%)**	**11(44%)**	**12(48%)**

8.4.1 The Effect of “Number of Questions Shared” for Impersonation

This section provides an analysis with a focus on the “number of questions shared” by a student with a third party impersonator and how this affects the success of an impersonation attack.

In order to test the significance of any trend in the data presented in Table 8-2 using four sharing conditions in an impersonation attack using database sizes of 20, 30 and 50, a one-way ANOVA was performed with linear contrasts. A linear trend was found for all sharing conditions on database size 20, F = 293.8, p = 0.00 (p < 0.01), eta-squared η^2 = 0.88 database size 30, F = 507.6, p = 0.00 (p < 0.01), eta-squared η^2 = 0.89, and database size 50, F = 507.67, p = 0.00 (p < 0.01), eta-squared η^2 = 0.87. A Pearson correlation was performed on the data presented in Table 8-3 to test the direction of the trend for all sharing conditions on database size 20, r = 0.94, n = 40, p = 0.00, database size 30, r = 0.94, n = 40, p = 0.00 and database size 50, r = 0.93, n = 40, p = 0.00.

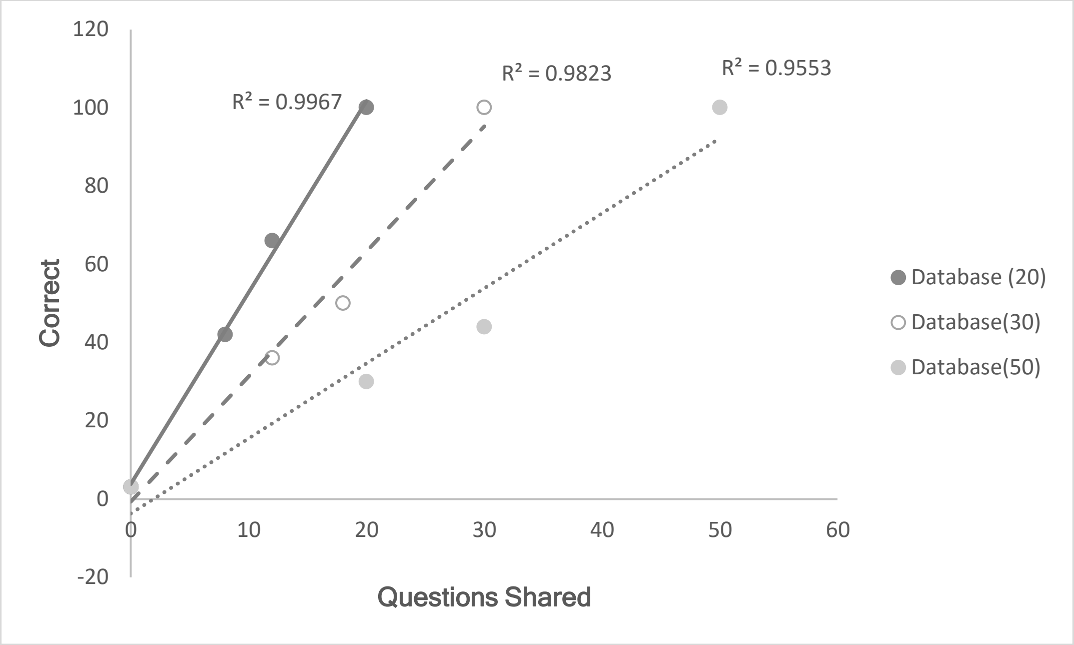


Figure 8-1 Trend Graph: Sharing Vs Correct Answers Using Database Sizes

The above results show that an increase in the number of shared questions increases the number of correct answers in an impersonation abuse case. Figure 8-1 shows a strong linear trend for all sharing conditions using all database sizes.

The findings revealed that an impersonation attack is more successful if a student is able to share a large number of questions with a third party impersonator. In the absence of monitoring or timing the user response, an impersonator can answer challenge questions by copying from a printed or electronic source shared by a student in order to authenticate. In the abuse case simulation, challenge questions were randomised; however, the impersonator was able to search and copy the correct answers from the shared information. Figure 8-1 shows that an increase in sharing resulted in an increase in correct answers for all three database sizes (20, 30, and 50). This shows that the impersonator may circumvent the challenge question approach, irrespective of the size of database, if an online examination is not monitored or if students are not restricted to answer the questions in a limited time. Based on the above findings, the following hypothesis was accepted:

H 8.1) *The larger, the number of challenge questions shared, the more successful an impersonation attack will be.* ***Accepted***

Table 8-4 Database Size: Answers Copied for Impersonation

P#	Database 20	Database 30	Database 50
Answers Copied for Impersonation			
1	12(80%)	9(60%)	9(60%)
2	11(73%)	11(73%)	9(60%)
3	12(80%)	8(53%)	9(60%)
4	9(60%)	9(60%)	7(47%)
5	11(73%)	10(67%)	7(47%)
6	10(67%)	10(67%)	10(67%)
7	9(60%)	8(53%)	9(60%)
8	11(73%)	10(67%)	9(60%)
9	10(67%)	9(60%)	8(53%)
10	9(60%)	9(60%)	10(67%)
	104(69%)	**93(62%)**	**87(58%)**

Table 8-5 Database Size: Answers Memorised for Impersonation

P#	Database 20	Database 30	Database 50
1	7(47%)	6(40%)	5(33%)
2	5(33%)	4(27%)	5(33%)
3	6(40%)	6(40%)	8(53%)
4	4(27%)	5(33%)	6(40%)
5	7(47%)	7(47%)	8(53%)
Total	**29(39%)**	**28(37%)**	**32(43%)**

8.4.2 The Effect of “Database size” on Impersonation Attacks

This section provides an analysis of the database size and how this affects the success of an impersonation attack. In order to test the significance of any trend in the data presented in Tables 8-4 using database sizes 20, 30 and 50, a one-way ANOVA was performed with linear contrasts. A trend was found for all database sizes: 20, 30 and 50 F = 11.45, p = 0.045 (p < 0.01) , eta-squared η^2 = 0.31. A Pearson correlation was performed on the data presented in Table 8-4 to test the direction of the trend on all database sizes for r = -0.559, n = 30, p = 0.041 (p < 0.01).

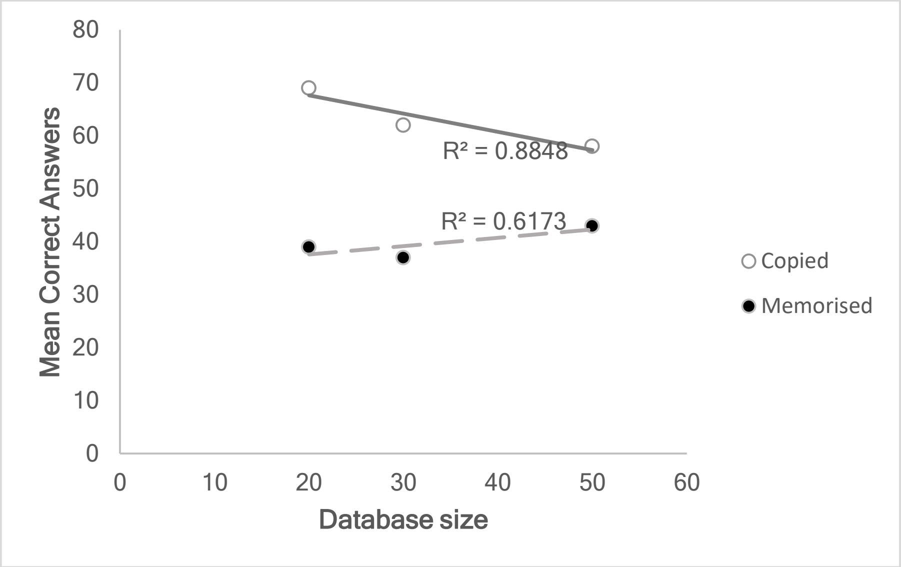


Figure 8-2 Trend graph: Database Sizes

The above findings revealed that an impersonation attack was less successful with an increase in the database size. The trend line in Figure 8-2 for all sharing conditions shows a decrease in the number of correct answers with an increase in the database size. Also, an increase in the database size decreases the probability of randomly having the same subset of questions shared by a student for impersonation. It is anticipated that an increase in the database size would mitigate a student from being able to share all of the answers with a third party impersonator. Based on the above discussion, the following hypothesis is accepted:

H 8.2) *The larger the database size, the less successful an impersonation attack will be, when attempted from written or printed source.* ***Accepted***

If answers to challenge questions are timed or monitored, this would increase the difficulty, and make it harder for an impersonator to search for the correct answers from a shared source, especially with an increase in the database size. As shown in Figure 8-2, the impersonation attack was less successful when the participants had to memorise and answer the challenge questions. This is discussed in more detail in the following section.

8.4.3 The Effect of Answering Challenge Questions from Memory

In a practical situation, it is anticipated that students would answer challenge questions in a limited time. In the above scenario, the participants were allowed to search for the shared information in order to answer the questions with no time constraints. However, if answers to challenge questions are timed or if the authentication process is monitored, an impersonator would be required to memorise the shared information. In order to test the significance of any trend in the data presented in Table 8-3 for four sharing conditions in an impersonation attack using database sizes 20, 30 and 50, a one-way ANOVA was performed with linear contrasts. A linear trend was found for all sharing conditions on database size 20, F = 17.8, $p = 0.001$ ($p < 0.01$), eta-squared $\eta^2 = 0.31$, database size 30, F = 13.5, $p = 0.002$ ($p < 0.01$), eta-squared $\eta^2 = 0.44$, and database size 50, F = 30.09, $p = 0.00$ ($p < 0.01$), eta-squared $\eta^2 = 0.56$. A

Pearson correlation was performed on the data presented in Table 8-3 to test the direction of the trend for all sharing conditions on database size 20, r = 0.61, n = 20, $p = 0.004$ ($p < 0.01$), database size 30, r = 0.66, n = 20, $p = 0.001$ ($p < 0.01$) and database size 50, r = 0.75, n = 20, p = 0.00 ($p < 0.01$).

The above findings show an increasing trend in correct answers with an increase in the number of shared answers for impersonation. However, the number of correct answers decreased when the impersonator answered the questions from memory. Figures 8-3, 8-4 and 8-5 show a difference in the correct answers for all sharing conditions using different database sizes and the way that the impersonator answered these questions. It shows that for all sharing conditions and database sizes, answers were less successful when attempted from memory. In order to test the significance of any differences in the means of correct answers between “Answers copied” and “Answers Memorised”, a one-way ANOVA test of significance was performed on the data shown in Table 8-4 and 8-5. The results of this analysis showed that there were significant differences in the means for database size 20 conditions F = 47.4; $p = 0.00$ ($p < 0.01$), eta-squared $\eta^2 = 0.78$ database size 30 conditions F = 43.18; $p = 0.00$ ($p < 0.01$), eta-squared $\eta^2 = 0.76$, and database size 50 conditions F = 12.47; $p = 0.004$ ($p < 0.01$), eta-squared $\eta^2 = 0.49$. This indicates that if answers to challenge questions are timed or if an online examination process is monitored, it will discourage the impersonator from searching a printed or electronic source for answers and will require them to memorise the shared challenge questions.

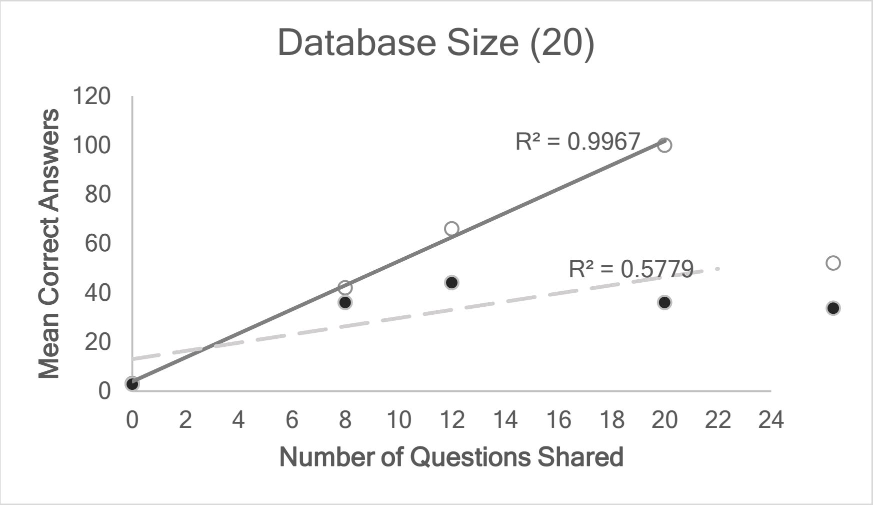


Figure 8-5 Database 20: Electronic or Printed Source Vs Memory

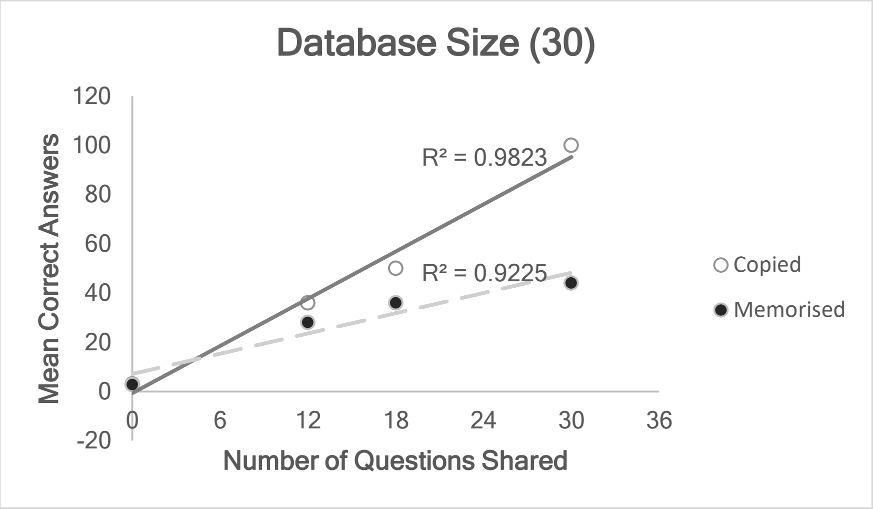


Figure 8-5 Database 30: Electronic or Printed Source Vs Memory

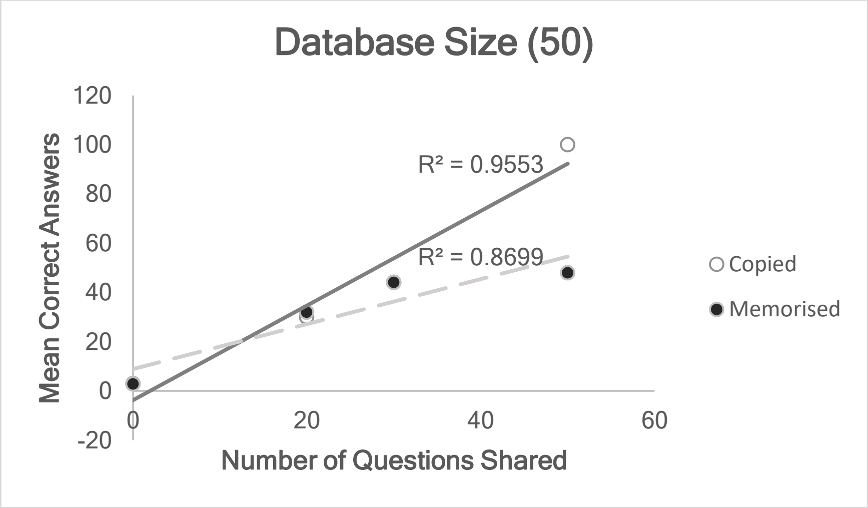


Figure 8-5 Database 50: Electronic or Printed Source Vs Memory

The above findings show that the success of a collusion attack was different when the participants answered questions from an electronic or printed source and memory. Based on the above findings, the following hypothesis was accepted.

H 8.3) *There is a measure difference in the success of an impersonation attack, when challenge questions are memorised or searched and copied for impersonation.* ***Accepted***

8.5 Summary

The study described in this chapter was based on a collusion abuse scenario testing different sharing conditions and database sizes. The findings revealed that an increase in the number of shared questions for impersonation increases the success of an impersonation attack. There was a significant linear trend, when impersonators answered their challenge questions from a printed or electronic copy of the shared questions. The number of correct answers decreased when impersonators memorised and answered the challenge questions. The study also revealed that an increase in the database size decreases the number of correct answers during a collusion attack. This indicates that an increase in the database size increases the difficulty of finding correct answers from shared information. It also increases the randomness of challenge questions extracted from a larger database.

The above findings indicate that the success of an impersonation attack depends upon a student's ability to share challenge questions. While text and image-based challenge questions are usable, students are required to register their answers to pre-defined questions. This enables them to store or memorise these questions for sharing with a third party impersonator. It may be challenging to discourage students from storing or memorising pre-defined challenge questions with the intention of inviting impersonators.

In order to address the above issue and to deter students from sharing questions, the next chapter will propose a dynamic profile question approach.

9 Study 4 –Impersonation and Dynamic Profile Questions

The previous study in Chapter 8 reported an impersonation abuse case scenario, when a student shares different numbers of challenge questions with an impersonator using different database sizes. The results of the study indicated that an increase in the number of shared questions increases the success of an impersonation attack. To discourage students from sharing their pre-defined text-based challenge questions with third party impersonators, this chapter presents study four, which proposes dynamic profile questions. The chapter presents the purpose, research questions, hypothesis and method. The following sections explain the participants' recruitment and the design of the online course. This includes impersonation abuse case scenarios, which investigate attacks when students and impersonators communicate asynchronously (via email) and in real time (through mobile phones). Finally, the chapter reports the effectiveness analysis and outcome of phone and email driven impersonation attacks.

9.1 Purpose

This study proposes dynamic profile questions, which are created when a student performs learning activities. Using this method, a student's profile is built and consolidated non-intrusively, non-distractively, in the background during the learning process. Dynamic profile questions are associated with students' learning activities. This implies that students are not aware of which questions will be asked for authentication. As discussed in the previous chapters, the usability analysis is important for evaluating how effectively security measures can be implemented. The effectiveness is a usability metric, which is considered to be the degree of accuracy of the participants' responses. In the context of a challenge question approach, it means that users are able to provide correct answers to their questions effectively with a low error rate.

The traditional text-based questions are associated with personal information and students can share these with a third party for impersonation in an online examination. The proposed dynamic profile questions attempt to discourage a student from sharing the questions with impersonators. The threats classification presented in Chapter 3 suggests that students can share their challenge questions with an impersonator via email or mobile. Dynamic profile questions attempt to influence such attacks. This study will investigate the following:

1. The usability attributes of the proposed dynamic profile question approach.
2. Whether a student could share dynamic profile questions with a third party impersonator using asynchronous and real-time communication methods (i.e. email and mobile phone) and successfully perform impersonation.

9.2 Research Questions and Hypotheses

The research questions RQ 3) and RQ 4) described in Chapter 1 are cascaded into more research questions with a focus on usability attributes and impersonation attacks via email and phone. The reseach question RQ 3c) is associated with the usability attributes of the dynamic profile questions. Similarly, the research question RQ 4b) is associated with the use of dynamic profile questions and their influence on collusion attacks. This study attempts to answer the following research questions, which are derived from RQ 3c) and RQ 4b):

RQ 9.1) How effective are dynamic profile questions for authentication in online examinations?

RQ 9.2) How can dynamic profile questions influence impersonation attacks using asynchronous sharing (email) in online examinations?

RQ 9.3) How can dynamic profile questions influence impersonation attacks using real-time sharing (mobile phone) in online examinations?

RQ 9.4) What is the measured difference in response time between a genuine student and a third party impersonator during impersonation attacks (phone/email), when dynamic profile questions are implemented?

RQ 9.5) Can the response rate of dynamic profile questions be used to indicate impersonation?

The following hypotheses were framed to answer the above research questions. Each hypothesis maps to a corresponding research question:

H 9.1) Dynamic profile questions provide effective authentication in online examinations.

H 9.2) Dynamic profile questions can positively influence impersonation attacks, when a student shares access credentials with a third party impersonator using asynchronous sharing through email.

H 9.3) Dynamic profile questions can positively influence impersonation attacks, when a student shares access credentials with a third party impersonator in real time using instant messaging on a mobile phone.

H 9.4) The measured differences in the security performance of dynamic profile questions in impersonation attacks (phone/email) are due to an attacker *taking extra time to retrieve answers from shared information sources, compared to a genuine student.*

H 9.5) The response rate to dynamic profile questions will be quicker "when there is no impersonation" than "when there is impersonation".

9.3 Study Method and Design

The usability test and risk-based security assessment methods described in Chapter 5 were adopted to evaluate the dynamic profile questions. As discussed in the previous chapters, the usability test is a usability inspection method, which tends to focus on the interaction between humans and computers (Corry et al., 1997). Using this method, the representative users, i.e. students, interact with online learning and examinations using dynamic profile question authentication in a real online course, which is described later in this chapter. The usability evaluation scale described in Chapter 5 (section 5.2.1) was used to translate the effectiveness analysis (Bangor et al., 2009).

The risk-based security assessment approach focuses on the test of features and functions of artefacts based on the risk of their failure using abuse case scenarios (McGraw, 2004). An abuse case scenario was simulated to analyse impersonation attacks when students and impersonators communicated asynchronously (via email) and in real time (via a mobile phone) to share dynamic profile questions. The study was conducted in multiple phases, which are described in the following sections.

9.3.1 Dynamic Profile Questions

This section provides a background and description of the dynamic profile questions. Babic et al. (2009) proposed a theoretical approach for activity-based security questions, which programmatically generates a security profile based on an individual's network and search activities. Babic et al. proposed this for authentication of users in web applications. In another study, Jortberg and Baile (2009) implemented challenge questions from a US consumer database for identification of online students in online examinations. However, the database is limited to the US consumers' market and does not hold information about prospective students from across the world.

Dynamic profile questions are an adaptable method. A student profile is created dynamically based on learning activities. Questions are created non-intrusively and non-distractingly in the background during the learning process. These questions are extracted from a student's learning activities, content submissions, grades, lessons, and forum posts in order to build and consolidate a student's profile. In order to access an online examination, the student is required to answer a subset of questions randomly presented from his or her profile. This study implemented multiple choice questions using a combination of distractors and correct answers. A total of 18 dynamic profile questions were utilised in this study as shown in Appendix C (II).

9.3.2 Online Course Design and Study Phases

An online course was conducted in multiple phases to provide learning opportunities to students and achieve the research objectives. The study phases are described below:

- **Designing PHP & MySQL Course**: Online course design plays an important role in setting up learning goals and assessment for students. The dynamic profile question approach utilised a student's learning interactions during the course work to create and consolidate a profile; therefore, the course design was highly relevant. A remote "PHP and MySQL" online course was organised in five weekly modules, which included lessons, forum submissions, assignments and students' reflections at the end of each week. The course was set up and deployed in the MOODLE Learning Management System (LMS) on a remote web server accessible on the Internet. The course content was released on a daily basis to maximise participants' engagement and learning interactions. A total of five weekly quizzes were set up for summative assessment. The participants were recommended to invest 10 hours weekly learning effort over a span of five weeks. A detailed course outline is given in Appendix C (I).
- **Participants Recruitment**: In order to motivate and recruit participants, the course was offered free of charge and advertised on the University of Hertfordshire online portal (StudyNet). A total of 31 students were enrolled onto the course; however, only 21 completed the five-week course. Of the 21 students, the majority (n =17, 80%) were students from United Kingdom and 1(5%) each were from Slovakia, Kenya, Malta, and Trinidad and Tobago. They were already enrolled in different programmes at the University of Hertfordshire as distance learners. This was helpful for the participants' engagement due to their existing knowledge of using a remote online learning environment. There was no repeated attendance of participants from the previous studies presented in Chapters 6, 7 and 8.

- **Registration**: The students were required to email a short introduction before registration. Guidance notes on the registration process and an enrolment key were emailed to all participants as shown in Appendix C (III). It was a standard MOODLE sign up process, which was essential to create login credentials to access the learning material. Upon successful registration, the participants received a confirmation email to access the course. The course was only available to registered users.
- **Online Coursework:** An instructor-led course was taught over a period of five weeks. To collect pertinent data for the evaluation of usability and security, authentication results were stored in the database. Participants were required to submit their weekly assignments in order to access their weekly quizzes. Each assignment was associated with the weekly course content.
- **Creating Dynamic Profile Questions**: Dynamic profile questions were created manually for each individual student and uploaded to the database in their profiles via the user interface in MOODLE. These questions were created on a daily basis for each participant after access to course content and lessons, assignment submissions, assignment grades, quiz completions, feedback and reflection, and forum discussions.
- **Weekly Quizzes:** The participants were required to complete a quiz at the end of each week. The course content of the following weeks were conditionally released to those participants who completed their quizzes – e.g. week 2 content was released to participants who completed the week 1 quiz. The conditional release was implemented to encourage participants to complete their coursework and assessments in order to generate dynamic profile questions. In order to access the weekly quizzes, the participants were authenticated using the dynamic profile questions stored in individual profiles created during the coursework.

9.3.3 Simulating Abuse Case Scenarios

The following collusion abuse case scenario was simulated towards the end of week five in order to evaluate impersonation attacks using email and phone:

> *A student is registered on a PHP & MySQL programming course, which is delivered in an online learning environment. The course uses dynamic profile questions for the authentication of students in summative assessments, which are accessible on a secure browser with no access to unwanted software e.g. Internet browser, chat sessions, etc. The student is due to write*

his/her final semester online test. He or she wants to boost his/her grades and recruits a third party impersonator to help him to take his test. However, to satisfy the authentication, the student needs to share his/her dynamic profile questions and answers (access credentials) with the impersonator. The impersonator would use the shared information to answer the randomly presented dynamic profile challenge questions during authentication in order to access the online test.

Given the above scenario, this study simulated two types of collusion attacks: i) a student shares dynamic profile questions with a third party impersonator through email *before* an online examination session; and ii) a student shares dynamic profile questions with a third party impersonator in real time through the mobile phone *during* an online examination session. Before simulating the abuse case scenarios:

- Two impersonators were recruited to attempt to impersonate students in an online examination session.
- Each impersonator was assigned a group of 10 students to simulate the abuse cases in allocated time slots.
- Skype accounts and email addresses for each impersonator were shared with his/her allocated students.
- Each impersonator was required to access a simulation quiz (online examination) created on the "PHP & MySQL" on behalf of each allocated student in the scheduled time slot.
- Each impersonator was required to answer all 18 dynamic profile questions associated with each of his/her allocated students in order to complete the simulation.

9.3.3.1 Credential Sharing with an Impersonator Asynchronously via Email

When students are discouraged from sharing information and communication during an online examination session, they may attempt to share questions and answers with a third party impersonator before an online examination session via email. This type of attack was simulated as described below:

1) Students were asked to share their dynamic profile questions using a template shown in Appendix C (V).
2) Students emailed their dynamic profile questions and login details to their allocated impersonator.

3) The impersonator accessed the online course using the allocated student's login details.

4) In order to access the online quiz on behalf of a student, the impersonator was randomly presented with three dynamic profile questions.

5) The impersonator answered the dynamic profile questions using the shared information. The impersonator was required to search and locate the correct answer from the shared information and to guess answers to questions if they were not shared. The authentication results were stored in the database for analysis.

6) Steps 4 to 5 were repeated until all of the 18 dynamic profile questions were answered by the impersonator.

9.3.3.2 Credential Sharing With an Impersonator Using Real-time Communication Via Phone

A student may share answers to his dynamic profile questions with a third party impersonator in real time during an online examination session using *Skype* on a smart phone. The participants were emailed the guidance notes on impersonation using Skype as shown in Appendix C (VI). The impersonator was taking the test on a PC computer and communicated with the student using Skype messenger installed on a smart phone. The attack was simulated as described below:

1) At a scheduled time, an impersonator and a student started a chat session on the phone using the Skype instant messaging service.

2) A student shared his login details with the impersonator to enable him/her to access the online course.

3) The impersonator accessed the online course on a PC using the shared login details.

4) In order to access the simulation online quiz, the impersonator was randomly presented with three dynamic profile questions on behalf of the student.

5) The impersonator shared these questions and multiple choice options with the student on a mobile phone using Skype in real time to collect the correct answers.

6) The student identified and shared a correct answer on Skype. The impersonator answered the questions and the authentication results were stored in the database for analysis.

7) Steps 5 to 6 were repeated until all of the 18 dynamic profile questions were answered by the impersonator.

9.4 Usability Results

This section presents the usability analysis of dynamic profile questions in the context of online learning and examinations. A total of 21 participants answered 378 questions for authentication in five weekly quizzes. The response time to questions was not recorded as they were created non-intrusively, non-distractingly in the background. This shows an increased efficiency compared to pre-defined text-based and image-based questions which require students to register their answers. The effectiveness analysis is presented in the following section.

9.4.1 Effectiveness of Dynamic Profile Questions

The effectiveness is considered to be the degree of accuracy of the participants' responses. In the context of this study, it means that participants were able to submit correct answers to dynamic profile questions effectively with a low error rate. This was analysed from the data collected from the participants' answers to dynamic profile questions during weekly quizzes. Table 9-1 shows the analysis of dynamic profile questions and the mean correct and incorrect answers. The results show that a large number of answers were correct. Out of 378 questions answered by 21 participants, 376 (99.5 %) were correct, which shows an increased effectiveness.

Table 9-1 Usability analysis: Effectiveness of Dynamic Profile Questions

Questions		**Correct**	**Incorrect**
1	Course objectives 1	21(100%)	0(0%)
2	Course objectives 2	21(100%)	0(0%)
3	Course objectives 3	21(100%)	0(0%)
4	Assignment 1	21(100%)	0(0%)
5	Assignment 2	21(100%)	0(0%)
6	Assignment 3	21(100%)	0(0%)
7	Assignment 4	21(100%)	0(0%)
8	Assignment 5	20(95.2%)	1(4.8%)
9	Forum Post 1	21(100%)	0(0%)
10	Forum Post 2	21(100%)	0(0%)
11	Forum Post 3	21(100%)	0(0%)
12	Assignment content 1	20(95.2%)	1(4.8%)
13	Assignment content 2	21(100%)	0(0%)
14	Assignment content 3	21(100%)	0(0%)
15	Assignment content 4	21(100%)	0(0%)
16	Student Reflection	21(100%)	0(0%)
17	Grades 1	21(100%)	0(0%)
18	Grades 2	21(100%)	0(0%)
Total		**376(99.5%)**	**2(0.5%)**

As shown in Table 9-1, the dynamic profile questions were based on the introduction and objectives, assignment submissions, forum discussions, assignment content, student reflection and grades. Each question was presented with five multiple choice options i.e. four distraction and a correct answer. For example:

Which one of the following statements below were written by you as a course objective?

1. Distraction statement
2. Distraction statement
3. Distraction statement
4. **Correct Answer**
5. None of the above

The participants were required to recognise the correct answer amongst the multiple choice options in order to authenticate. The multiple choice options provided cues to the participants in order to identify their answers, which resulted in 99.5% correct answers. We recall that in Chapter 7 (section 7.4.2.2), 90% of the recognition-based image questions were correct, which was significantly ($p < 0.01$) different to the predefined text-based questions. The current results for dynamic profile questions show further improvement on image-based questions. This was a result of using multiple choice options and creating questions associated with the students' learning activities.

According to the usability scale presented in Chapter 5 (section 5.2.1) and letter grades (i.e. 70%-79% acceptable, 80%-89% good, more than 90% exceptional) described by (Bangor et al., 2009), 99.5% correct answers to dynamic profile questions is an exceptional effectiveness. Based on the above findings, the following hypothesis was accepted.

H 9.1) *Dynamic profile questions provide effective authentication in online examinations.* ***Accepted***

9.5 Security Results

This section reports the security analysis of dynamic profile questions to evaluate impersonation attacks when students and impersonators communicate through email and mobile phone. The analysis was performed on the data collected from simulation abuse case scenarios. In total, 21 participants performed email and phone collusion attacks with two impersonators. The findings of impersonation using email resulted in 29 (8%) correct answers. The findings of impersonation using a mobile phone (Skype) resulted in 351 (93%) correct answers. A detailed discussion on the findings of the abuse case scenarios is presented below:

9.5.1 Impersonation Using Asynchronous Sharing via Email

The security analysis of an impersonation attack in this section is based on the number of correct answers received when third party impersonators answered dynamic profile questions on behalf of allocated students and the information was shared asynchronously through email. Table 9-2 shows the list of participants and the mean of correct and incorrect answers submitted by an impersonator. The email attack was performed before the phone attack to evaluate participants' ability to recall and share their dynamic profile questions, which would help a third party to impersonate them in an online examination.

Dynamic profile questions implemented five multiple choice options and the probability of a correct answer by chance would be $1/5^{th}$ or 20%. In the abuse case scenario, the impersonators answered 29 (8%) challenge questions correctly. This was largely based on information shared via email and guessing by the impersonators.

Table 9-2 Security analysis: Impersonation via Email/Phone

Participants	Email Impersonation		Phone Impersonation	
	Correct	Incorrect	Correct	Incorrect
1	9(50%)	9(50%)	18(100%)	0(0%)
2	0(0%)	18(100%)	12(67%)	6(33%)
3	0(0%)	18(100%)	13(72%)	5(28%)
4	1(6%)	17(94%)	18(100%)	0(0%)
5	0(0%)	18(100%)	18(100%)	0(0%)
6	1(6%)	17(94%)	14(78%)	4(22%)
7	0(0%)	18(100%)	16(89%)	2(11%)
8	0(0%)	18(100%)	18(100%)	0(0%)
9	0(0%)	18(100%)	18(100%)	0(0%)
10	5(28%)	13(72%)	16(89%)	2(11%)
11	0(0%)	18(100%)	18(100%)	0(0%)
12	0(0%)	18(100%)	18(100%)	0(0%)
13	0(0%)	18(100%)	17(94%)	1(6%)
14	0(0%)	18(100%)	16(89%)	2(11%)
15	5(28%)	13(72%)	16(89%)	2(11%)
16	1(6%)	17(94%)	18(100%)	0(0%)
17	0(0%)	18(100%)	17(94%)	1(6%)
18	0(0%)	18(100%)	16(89%)	2(11%)
19	0(0%)	18(100%)	18(100%)	0(0%)
20	0(0%)	18(100%)	18(100%)	0(0%)
21	7(39%)	11(61%)	18(100%)	0(0%)
Total	**29 (8%)**	**349 (92%)**	**351(93%)**	**27 (7%)**

Of the 21 participants, only 7 were able to share at least one correct question and answer with a third party impersonator. In order to test the significance of any differences in the means of correct answers between students (during authentication) and third party impersonators in an email abuse case scenario on the data shown in Table 9-1 and 9-2, a paired-sample t-test was performed. There was a significant difference in the correct answers by students (M = 99.5, SD = 2.4) and impersonators in email abuse case attack (M = 7.8, SD = 14.9) conditions t (20) = 28.41, *p* = 0.00 (*p* < 0.01). This indicates that students were unable to share their dynamic profile questions with a third party impersonator; however, they recognised their correct answers when presented with multiple choice options during weekly quizzes reported in the effectiveness analysis (see section 9.4.1). Based on the above findings, the following hypothesis was accepted.

H 9.2) *Dynamic profile questions can positively influence impersonation attacks, when a student shares access credentials with a third party impersonator using asynchronous sharing via email.* ***Accepted***

9.5.2 Impersonation Using Real-time Sharing via Phone

The security analysis of an impersonation attack in this section is based on the number of correct answers received when third party impersonators answered dynamic profile questions on behalf of allocated students and the information was shared in real time through a mobile phone. Table 9-3 shows the analysis of the dynamic profile questions and the mean correct and incorrect answers.

Table 9-3 Security Analysis: Impersonation Abuse Case via Mobile Phone

Question#	**Content Type**	**Authentication**	
		Correct	**Incorrect**
1	Course objectives 1	20(95%)	1(5%)
2	Course objectives 2	20(95%)	1(5%)
3	Course objectives 3	21(100%)	0(0%)
4	Assignment 1	20(95%)	1(5%)
5	Assignment 2	20(95%)	1(5%)
6	Assignment 3	20(95%)	1(5%)
7	Assignment 4	21(100%)	0(0%)
8	Assignment 5	19(90%)	2(10%)
9	Forum Post 1	18(86%)	3(14%)
10	Forum Post 2	20(95%)	1(5%)
11	Forum Post 3	21(100%)	0(0%)
12	Assignment content 1	17(81%)	4(19%)
13	Assignment content 2	18(86%)	3(14%)
14	Assignment content 3	20(95%)	1(5%)
15	Assignment content 4	19(90%)	2(10%)
16	Student Reflection	18(86%)	3(14%)
17	Grades 1 (Assignment)	21(100%)	0(0%)
18	Grades 2 (Quiz)	18(86%)	3(14%)
Total		**351(93%)**	**27(7%)**

The findings revealed that a third party impersonator answered 351 (93%) questions correctly. This shows a 93% success as a percent of total answers. Students were able to recognise correct answers from the multiple choice options when asked on the mobile phone in real time. In order test the significance of any difference between correct answers submitted by students (during authentication) in weekly quizzes and third party impersonators using mobile phone, a paired-sample t-test was performed on the data shown in Table 9-1 and Table 9-3. There was a significant difference in the correct answers by students (M=99.47, SD=2.4) and impersonators by phone (M=92.8, SD=10) conditions t (20) = 3.49, p = 0.002 (p < 0.001). However, the mean of correct answers by phone (M=92.8) indicates a high percentage of the total answers. This identified a vulnerability of the dynamic profile questions when a student interacts with a third party impersonator via mobile phones in real time. A student can circumvent this approach if an online examination process is not monitored or the response to questions during authentication is not timed. Based on the above findings the following hypothesis was rejected:

H 9.3) *Dynamic profile questions can positively influence impersonation attacks, when a student shares access credentials with a third party impersonator using real-time sharing via instant messaging on a mobile phone.* ***Rejected***

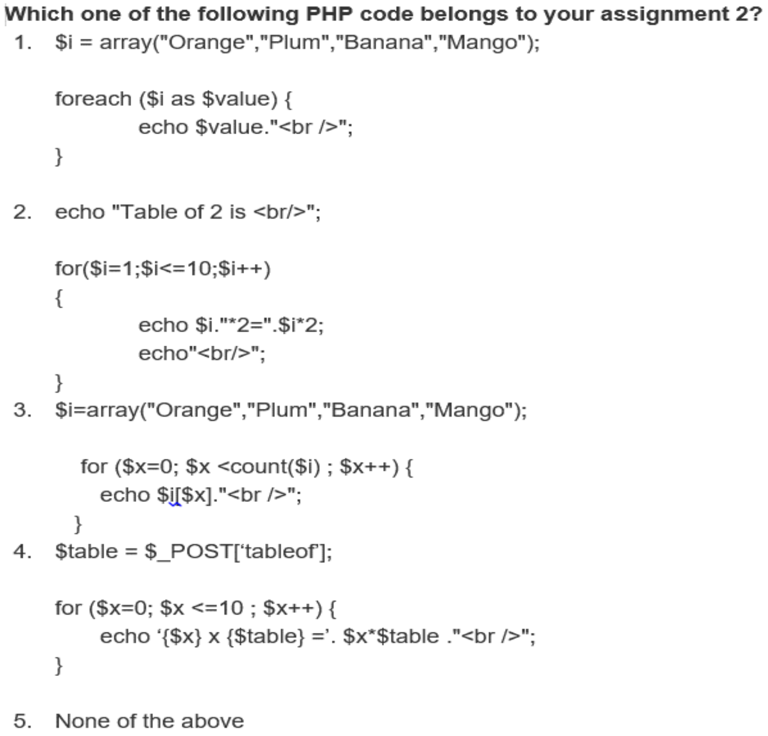
9.5.3 Security Performance and Response-time Factor

Traditional online examinations are often required to be completed in an allocated time. Students are expected to authenticate and complete their online tests on or before the allocated time. In a practical situation, when a third party impersonator communicates with a student to share answers to dynamic profile questions using a mobile phone or email, the response time may change. It is anticipated that the response time of a genuine student and an impersonator may be different when answering these questions.

In order to test the significance of any differences in the mean response time to dynamic profile questions between a genuine student and a third party impersonator, a paired-sample t-test was performed on the data shown in Tables 9-1 and 9-3. There was a significant difference in the scores for the response time of a genuine student during authentication (M=39.69, SD=104.07) and a third party during impersonation by phone (M=290.47, SD=90.39) conditions t (377) = -35.55, p = 0.00 (p < 0.01). Based on the above findings, the following hypothesis was accepted:

H 9.4) *The measured differences in the security performance of student's dynamic profile questions in impersonation attacks (Skype/email) are due to an attacker taking extra response time to retrieve answers from shared information sources compared to a genuine student.* ***Accepted***

The impersonation abuse case scenario via phone was simulated using Skype instant messaging. It is anticipated that verbal communication via phone may be quicker than texting. However, reading a question with 5 multiple choice options may still require extra time for an impersonator, compared to a genuine student who could choose a correct answer in a shorter time. Furthermore, dependent upon the question design, some questions may be challenging to describe verbally such as:



Which one of the following PHP code belongs to your assignment 2?

```
1.  $i = array("Orange","Plum","Banana","Mango");

    foreach ($i as $value) {
            echo $value."<br />";
    }

2.  echo "Table of 2 is <br/>";

    for($i=1;$i<=10;$i++)
    {
            echo $i."*2=".$i*2;
            echo"<br/>";
    }
3.  $i=array("Orange","Plum","Banana","Mango");

      for ($x=0; $x <count($i) ; $x++) {
        echo $i[$x]."<br />";
      }
4.  $table = $_POST['tableof'];

    for ($x=0; $x <=10 ; $x++) {
        echo '{$x} x {$table} ='. $x*$table ."<br />";
    }

5.  None of the above
```

In order to test the significance of any trend in the response time on the data presented in Table 9-1 and Table 9-3, a one-way ANOVA was performed with linear contrasts. A trend was found for response time by students and a third party impersonator F = 1250.96, *p* = 0.00 ($p < 0.01$), eta-squared $\eta^2 = 0.62$. A Pearson correlation was performed on the data presented in Table 9-1 and Table 9-3 to test the direction of the trend in response time by a student and a third party r = 0.79, n = 756, p = 0.00 ($p < 0.01$). This indicates an increasing trend with r = 0.79. The above findings show that the response time of a genuine student is shorter than that of a third party impersonator. Based on the above findings, the following hypothesis was supported.

H 9.5) *The response rate of dynamic profile questions will be quicker "when there is no impersonation" than "when there is impersonation".* ***Accepted***

9.6 Summary

The study reported in this chapter implemented dynamic profile questions in a real online course. These questions were created non-intrusively and non-distractingly in the background during a student's learning period. This increased the efficiency compared to text-based and image-based questions. The findings revealed a significantly increased effectiveness, i.e. 99.5% correct answers. These questions are usable and positively influence impersonation when a student and impersonator communicate asynchronously via email. The security analysis revealed that dynamic profile questions may negatively influence impersonation attacks when a student and an impersonator use a smart phone to communicate in real time during the exam session. However, there was a significant difference ($p < 0.01$) in response time between a genuine student and a third party impersonator. This may be implemented as an additional factor on which to base reports of impersonation attacks. The response time factor can discourage students from sharing access credentials with impersonators in real time to perform collusion attacks.

The current study involved online students as an important user group. However, it is essential to collect feedback from other important stakeholders such as online programme tutors on security threats, usability, and the proposed dynamic profile question approach. The following chapter will present a focus group study involving online programme tutors.

10 Study 5: Focus Group with Online Programme Tutors

Students, online programme tutors, and educational institutions are the key stakeholders in online learning programmes. With teaching and assessment responsibilities, online programme tutors have a central role in an online learning and examination context, and it is important to understand their views on security threats and the proposed methods to counter them. Previous chapters indicated the usability and security of the challenge question approach involving students. This chapter presents feedback obtained from a focus group of online programme tutors, who were chosen as experts in this field. They were invited to provide their views on potential threats, authentication methods, usability and applicability of the proposed challenge question approach against identified threats with a focus on collusion attacks, remote proctor, and secure examination browsers.

The following sections explain the process before, during, and after expert review. This includes how the questions were developed and piloted, characteristics of the experts and why they were chosen, how the process was conducted and the feedback received, how the data were analysed, and the findings.

10.1 Purpose

An online examination is a high-stake process, which faces many security threats. These threats are classified into two main categories: intruder and non-intruder attacks, as described in the threats classification presented in Chapter 3. Non-intruder threats include collusion and non-collusion threats. Collusion is further classified into impersonation and abetting categories. Impersonation threats are difficult to identify and mitigate, because such threats involve legitimate students inviting third parties to impersonate them in their online tests. This research developed and empirically evaluated a challenge question approach for deterrence of this type of collusion threat. Five empirical studies were conducted in simulation, as well as real online courses involving both online and on-campus students. To understand the perspective of online programme tutors as important stakeholders, a focus group study was conducted. The purpose of this study was to:

1. Explore the views of online programme tutors around collusion threats to remote online examinations.

2. Explore the views of online programme tutors around the usability and security of dynamic profile questions in order to mitigate collusion attacks.
3. Explore the views of online programme tutors around a secure browser, remote proctoring, and dynamic profile questions to influence collusion in online examinations.

10.2 Study Method and Design

This study adopted a mixed methods approach, comprising a focus group (qualitative research technique) and a questionnaire (quantitative technique). Several definitions for a focus group are available in the literature review, including collective activity (Powell and Single, 1996), organised discussion (Kitzinger, 1995), and social events and interaction (Goss and Leinbach, 1996). According to Powell et al. (1996), a group of representative individuals are chosen and gathered by researchers to discuss their personal experience and comment on the topic under research. This is a form of group interview performed collectively with a focus on questions and responses between researchers, moderators and participants. However, it relies upon interaction with the group on the subject under research. The primary objective of the focus group was to determine participants' perceptions of security threats, including collusion, authentication methods, usability, and security of the proposed challenge questions method. Data from this study were collected on video from a moderator-led discussion and a paper-based questionnaire. The focus group discussion was analysed using a content analysis approach. The study was performed in multiple phases, which are described below.

Table 10-1 Focus Group: Participant characteristics

Categories	Focus Group (n=9)
Gender	Male: 5 (55%) Female: 4 (45%)
Role	Online Programme Tutors
Summary of background	Online programme tutors with expert level experience in course design, teaching online and face-to-face courses, proctoring, supervision, and assessment. Participants were also expert in usability, security, HCI, and research.

10.2.1 Format of the Focus Group Sessions

The focus group study was conducted over two sessions. In the first session, participants were given a presentation to provide them with an overview of the research problems and proposed solutions. After the presentation, participants were asked for their feedback on a paper-based questionnaire. In the second session, a moderator-led discussion was conducted. Participants' feedback was recorded on a video for analysis. The duration of the session was two hours. The structure of the study is described below:

- **Participants Recruitment**: In this study, a group of online programme tutors from the University of Hertfordshire was invited. A total of nine participants attended the study. They were highly experienced and experts in the area of online teaching, face-to-face teaching, course design, examinations design, invigilation, research supervision, Human-Computer Interaction (HCI), usability, security, and assessment of students. The session was also attended by authors, research supervisors, and the moderator. The characteristics of the focus group participants are presented in Table 10-1 above. Online programme tutors are key stakeholders in the online examination process and therefore, interested in research related to security threats, usability and authentication approaches to mitigate threats. There was no repeated attendance of participants from the previous studies presented in Chapters 6, 7, 8 and 9.
- **Presentation on Threats and Challenge Question approach**: Before the group discussion, participants were given a power point presentation (see Appendix D (I)) on remote online examinations, authentication, collusion attacks, and the challenge question approach. Findings of the empirical studies using pre-defined text-based, image-based, and dynamic profile questions were also presented to provide a background to an online examination context, threats, and mitigation methods. At the end of the presentation, participants were handed the paper-based questionnaire for their feedback, as described in the following section.
- **Questionnaire:** As shown in Appendix D (II), a 19-question paper-based questionnaire was produced to collect participants' feedback on security threats and collusion, usability of authentication methods, effectiveness of question types, and overall usability and security of the challenge question approach. 5- and 10-point scales were used for all questions. The questionnaire was distributed to participants after the first presentation described

above. They were asked for feedback based on their experience associated with the information provided in the first presentation. The questionnaire was filled in and returned by all participants after the focus group discussion.

- **Presentation on Remote Proctor and Secure Browser:** Participants were given a second presentation on the use of a secure browser and remote proctoring tool, ProctorU (Eisenberg, 2013), to deter collusion attacks. This method has been offered by a number of service providers to conduct proctor-led examinations remotely. This approach was presented as a potential candidate for mitigation of abetting attacks.
- **Focus Group Discussion**: After the presentations, seats were arranged in a circle to facilitate group discussion. The moderator welcomed all participants and asked for their consent to record the session on a video. After setting up video cameras, the moderator gave a brief introduction about the research aim and problems. He started the discussion by describing a scenario followed by probes, shown in Appendix D (III). He posed relevant probes one by one and steered the discussion. Participants responded to each probe in a group discussion, which is analysed later in this chapter.

10.3 Questionnaire Analysis

In this section, the results and discussion from the data analysis are presented. The analysis is derived mainly from three sources to ensure triangulation and validity (Creswell, 2012). One source is participants' feedback to questionnaires, as shown in Table 10-2, and the second source is findings from the empirical enquiries presented in Chapters 6, 7, 8 and 9. The third source is analysis of the focus group discussion shown in Table 10-3.

The following sections present an analysis of the feedback about security threats and collusion, usability of authentication approaches, usability of the different question types, i.e. text-based, image-based, and dynamic profile questions, and usability and security of the challenge question approach in an online examination context.

Security Threats and Collusion: The threat of collusion in online examinations has been a rising concern for educational institutions and tutors. There is a prevailing view that online examinations pose a higher threat than face-to-face examinations. Numerous studies (Vician et al., 2006, Olt, 2002, Colwell and Jenks, 2005, Wielicki, 2006, Jung and Yeom, 2009, McMurtry, 2001) report that online learning offers more opportunities for cheating. Chiesel (p.330, 2009) identifies that 64% of university professors perceive cheating in online examinations to be easier. Table 10-2 shows an analysis of the questionnaire regarding security threats, including collusion attacks, in the section "*Security Threats and Collusion*". Online programme tutors have been actively involved in designing and conducting examinations for both on-campus and online students. They were asked about their concerns regarding threats and authentication approaches in online examinations. As shown in Table 10-2, in response to Q1 and Q2 regarding *"Online examinations"* and *"Authentication approaches"*, the majority of participants reported their concern and scored M = 4 and M = 3.7 respectively (1 – No concern at all; 5 – Strong concern). In response to Q3 and Q4, participants felt that it is less difficult to cheat in online examinations (M = 2.1) compared to face-to-face examinations (M = 3.6). While cheating in an online examination has been reported as a risk, collusion is seen as a main concern. Participants were requested for feedback in Q5-8 regarding different types of collusion attacks including "copying from books and other resources", "copying from the Internet", "abetting" and "impersonation". In response to these questions, the majority of participants reported high concern regarding impersonation and abetting, which scored M = 4.1 and M = 4.2 respectively.

Table 10-2 Focus Group Analysis: Survey Questionnaire

	Questions	**M**	**Med**	**SD**
	Security Threats and Collusion			
1	How concerned are you about the security of a remote online examination?	4	4	0.7
2	How concerned are you about the authentication methods implemented for the security of a remote online examination?	3.7	4	1.1
3	In your view, how difficult is it for a student to cheat in a remote online examination?	2.1	2	1
4	In your view, how difficult is it for a student to cheat in face-to-face invigilated examination?	3.6	4	1.3
5	Consider the threat of a student copying answers from a book or other course material. Please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation.	3.8	4	0.8
6	Consider the threat of a student copying answers	3.8	4	0.8

	from the Internet. Please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation.			
7	Abetting – Consider the threat of a student getting help from someone else, based in the same location. Please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation.	4.2	4	0.6
8	Impersonation – Consider the threat of a student getting help from a third party, based in a remote location. Please rate the seriousness of this threat in a remote online examination where there is a remote student authentication but no invigilation.	4.1	4	0.7
	Existing Authentication Methods			
9	Login Identifier and Password Authentication	3.4	3	0.8
10	Graphical Password Authentication	3.4	3	0.8
11	Security/Challenge Questions Authentication	3.6	4	1.1
	Effectiveness of Different Question Types			
12	How effective would the challenge question approach be to mitigate impersonation attacks?	3.3	3	0.7
13	Pre-defined Text-Based Questions	3.0	3	0.5
14	Pre-defined Image-Based Questions	3.4	3	0.5
15	Dynamic Profile Questions	3.8	4	0.8
	Overall Usability and Security of Challenge Questions			
16	How usable is the challenge question approach?	3.6	4	0.8
17	How secure is the challenge question approach in terms of non-collusion based intruder attacks?	3.6	3	0.7
18	How secure is the challenge question approach in terms of collusion attacks?	2.9	3	0.6
19	Given that security and usability may be considered to be a trade-off, on a scale of 1 to 10, please indicate where you think the best option should be.	3.6	3	1.9

Knowledge-based authentication approaches: The knowledge-based approach is the simplest technique employed to fulfil the security requirements. This is an easy to use method, and expected to provide secure authentication. It is a low-cost, accessible, widely acceptable and preferred authentication method (Hafiz et al., 2008).

Participants were asked for their feedback on the usefulness of existing knowledge-based authentication approaches in the context of online examinations. These approaches include ‘Login Identifier and Password’, ‘Graphical Passwords’ and ‘Challenge Questions’. Participants rated the ‘Challenge Questions’ approach as M = 3.6 (1 - Not useful at all to 5 - Very useful).

Usability of Challenge Questions: Braz and Roberts (2006) state that the usability of security systems has become a major issue in research on efficiency and user acceptance. It is important to investigate usability attributes, i.e. the efficiency and effectiveness of the proposed challenge question approach. This method implemented text-based, image-based and dynamic profile questions. In the empirical studies reported in Chapters 6, 7, and 9, the effectiveness of different question types was analysed by computing correct answers during authentication. Dynamic profile questions were the most usable of all question types, with 99.5% correct answers. Unlike other question types, this was the most efficient method as questions and answers were generated dynamically in the background during the learning process to build profiles, and students were not required to register their answers.

In response to survey questions 13, 14 and 15, participants rated the effectiveness of text-based, image-based and dynamic profile questions as 3, 3.4, and 3.7 respectively (1 - Not useful – 5 - very useful). A one-way ANOVA was performed on the data shown in Table 10-2: questions 13, 14, and 15, with linear contrasts to find a difference in participants’ responses to the usability of different question types. A significant trend was found in participants’ responses to the usability of different question types (F = 6.64, *p* = 0.016, eta-squared $\eta^2 = 0.22$). A Pearson correlation was performed on participants’ feedback to questions regarding the usability of question types to test the direction of the trend. The result of the test shows a significant correlation p = 0.014, and r = 0.46 indicates a positive trend in the usability of questions from text-based, image-based, and dynamic profile questions. Figure 10-1 shows a linear graph of different question types, which indicates an increasing trend. It is important to consider that, a one-way ANOVA on a small sample size may not have sufficient power. The power depends on the error variance, the selected significance (alpha-) level of the test, and the sample size. However, findings of the test here yielded significant value.

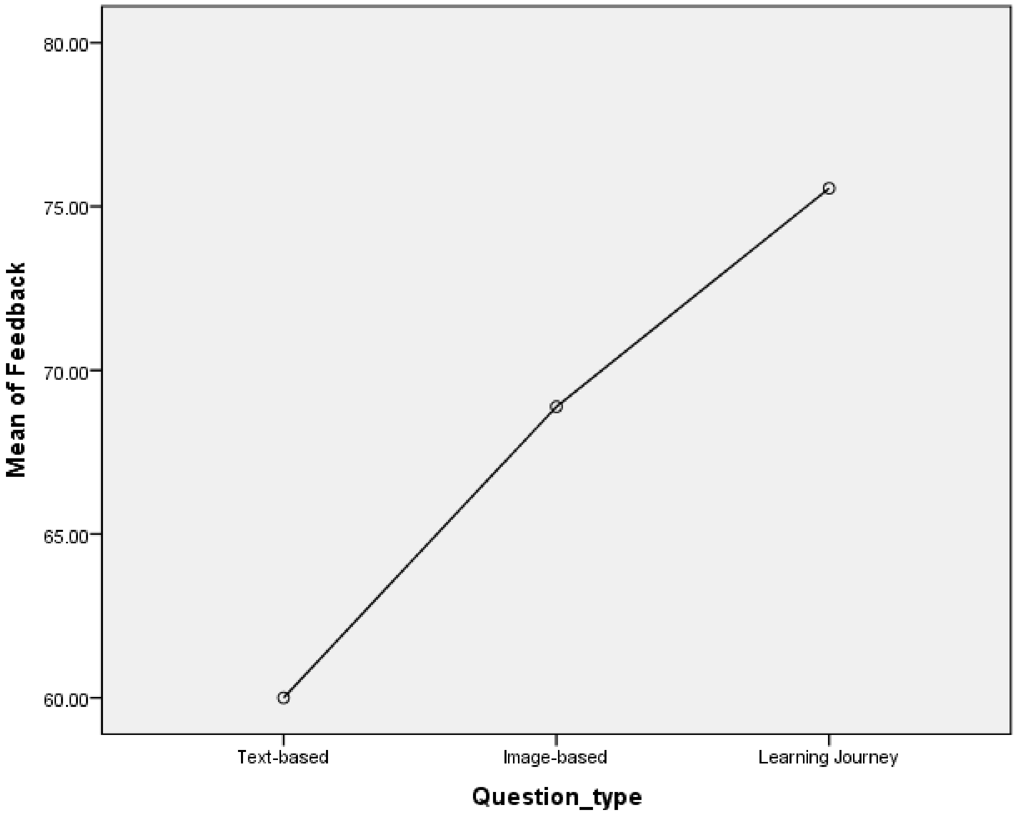


Figure 10-1Usability – Trend Graph

Security of Challenge Questions: Mitigation from all types of threat is a priority; however, based on the feedback to questions associated with threats, collusion is reported as a rising concern for online examinations. Participants were requested for feedback on the security of the proposed method to mitigate non-collusion and collusion attacks. There was an agreement on the security of challenge question approach to influence non-collusion threats. However, some participants reported concerns when this approach is implemented to mitigate collusion attacks. Question 18, regarding the security of challenge question approach to mitigate collusion attacks, scored M = 2.9.

In summary, participants felt that impersonation and abetting are challenging threats to online examinations. The proposed method is usable when dynamic profile questions are implemented. There was an agreement that this method could influence impersonation attacks; however, some participants showed concern about abetting attacks, which are discussed in the focus group analysis.

10.4 Focus Group Analysis

The data analysis of the focus group was performed using a qualitative content analysis approach (Berg and Lune, 2004). It is a systematic and reliable technique for compressing many words of text into fewer content categories based on explicit rules of coding (Berelson, 1952). The recording from the focus group discussion was transcribed for detailed analysis. Categories of the main themes associated with this research were identified in the transcription. Phrase analysis was carried out and data were organised into subcategories for further analysis.

Table 10-3 Content Analysis: Focus Group Discussion

	Raters		Score
Categories	**1**	**2**	**Mean**
Collusion Threats			
A user will share access credentials with a third party for a bank account	1.25	1.5	1.4
A user will share access credentials with a third party for an online examination	3.3	3.3	3.3
[1] The risk of sharing bank credentials for a user is…	5.0	5.0	5.0
[1] The risk of sharing online examination credentials for a student is…	2.0	2.3	2.2
[1] The risk of Mobile/Instant Messaging/SMS is…	5.0	5.0	5.0
[1] The risk of Desktop Sharing is…	5.0	4.0	4.5
[1] The risk of inviting third party to exam location is…	5.0	5.0	5.0
Challenge questions method using dynamic profile questions			
Secure against collusion	3.3	3.3	3.3
It can make it hard to collude	4.5	5.0	4.8
As a programme tutor, I will use the dynamic profile question approach in an online exam for my students	4.5	4.4	4.5
Mitigates mobile collusion when answers are timed	4.0	3.5	3.8
[1] Risk of using time factor to penalise students	3.0	2.6	2.8
Timing answers make it hard to collude	5.0	4.0	4.5
Course Design to Prevent Collusion via Mobile SMS	5.0	4.3	4.7
Secure browser and remote proctoring (ProctorU)			
Secure against collusion	4.0	4.5	4.3
Secure against screen sharing	4.3	4.3	4.3
It can make it hard to collude	4.0	3.5	3.8
As a programme tutor, I will use ProctorU in an online exam for my students	4.5	4.7	4.6

[1] 1-Very Low Risk to 5-Very High Risk

The data collected during the study were rated by two independent raters on a scale of 1-5 (1 - Strongly Disagree – 5 - Strongly Agree) and (1 - Very Low Risk – 5 - Very High Risk) as shown in Table 10-3. The data were evaluated for inter-rater reliability using Cohen's kappa test. The kappa value of 0.583 shows moderate agreement between the raters. The results are discussed in the following section.

10.4.1 Participants' Perception of Collusion Threats

To understand the perception of online tutors regarding collusion attacks, it was made a central point of the focus group discussion. While there has been ongoing debate around threats to online examinations and face-to-face invigilated exams, there is agreement that collusion is a potential threat and it is challenging to verify that a student signed up for the course is the same person who is taking the online examination. There was a good discussion on the difference of stakes in online examinations and other web-based applications like online banking. It was discussed that collusion attacks are unique and pose a threat to remote online examinations as well as face-to-face invigilated exams. A participant reported that:

Participant 4:

> *"There have been occasions when students have colluded and impersonated in the invigilated exams, where both parties were from the university"*

Collusion is classified in different types and each type poses a different threat level in an online examination context. A student copying answers from a book or the Internet is not considered collusion because a third party is not involved. Discussion on collusion and types of collusion threats are discussed below.

10.4.1.1 Impersonation in Online Examinations Vs Online Banking

Impersonation is seen as a larger threat to the security of an online examination compared to online banking. There was collective agreement that impersonation poses a different threat to both because of the difference in stakes. As a user of an online bank account, an individual is less likely to share their login credentials or associated information with a third party as it may expose their monetary assets to risk. There was strong disagreement from participants, if they were asked to share their credential for an online banking system, where stakes are different. As shown in Table 10-3, participants perceived sharing of access credentials in online banking as a high security risk for the account holder and scored M = 5. According to a participant:

Participant 2:

> *"The potential risk you are exposing yourself to by giving people your banking details is enormous"*

Unlike online banking, users of an online examination would share their access credentials with third party impersonators. These users have different stakes than in online banking, and individuals may be tempted to collude in order to boost their grades or qualify a test. The absence of invigilation or monitoring creates more opportunities and students are not challenged. According to many participants, there is a lower risk for a student to collude and share credentials for his online examination with a third party M = 2.2 (1 - Low Risk to 5 - Very High Risk). According to some participants:

Participant 1:

> *"If you are trying to collude, you would be interested to share your information"*

Participant 2:

> *"Whereas if you giving your detail to some person who can impersonate, the risk is, I suppose is potentially quite large, but essentially it is not as large as giving out your bank details*"

In summary, there was an agreement that students in online examinations are more likely to collude with third parties and share their access credentials, which is discussed in the following section.

10.4.1.2 Impersonation

Students employing someone else to take their test instead of them would willingly share their credentials with impersonators, regardless of any rules or regulations (Frank, 2010). Recall in Chapter 3, the collusion between a student and a third party impersonator can happen using different communication approaches. A student may share credentials with a third party in real-time or asynchronously before an examination session using email, mobile phone for SMS (Short Messaging Service), or Instant Messaging. Access credentials can be shared using an email before a test, if the authentication method uses simple credentials which are easy to share. Also, a student may use email if an online examination is monitored or proctored remotely. For example, password for logging into an online examination and answer to memorable challenge questions can be shared through email before the test session. However, authentication approaches which implement dynamic and interactive mechanisms may discourage sharing access credentials beforehand. Results from the empirical study reported in Chapter 9 show that students may find it difficult to share dynamic profile questions though email. These questions are non-intrusive and created dynamically based on individuals' learning activities, and students would not know the questions beforehand. Another example is a dynamically-created security code sent to a mobile phone through SMS. However, the study reported in Chapter 9 indicated that students may share information via mobile phones in real-time. Participants in the focus group discussion identified that mobile phones pose a potential threat to share access credentials or answers to exam questions in real time. According to participants:

Participant 5:

> *"If I want to share a code, I would use my mobile phone"*
>
> *"If I have a mobile phone I can receive text with the answers"*

As shown in Table 10-3, participants in the focus group perceived sharing of access credentials using a mobile phone during an examination as a high security risk and scored M = 5.

Another potential threat is when a student colludes with a third party using remote desktop sharing. As in (Frank, 2010), remote desktop sharing software can be used to share the screen with someone remotely to impersonate and take the test. In an online examination scenario, where there is no invigilation, a student may share a screen or access credentials with a third party for impersonation. This was perceived as a serious threat and scored M = 4.5 (1 - Not serious at all – 5 - Very serious). According to a participant in the focus group:

Participant 5:

> *"I can easily share my screen with someone sitting somewhere else,*
> *who can see the same screen as I do"*

There was agreement that a student may share access credentials via email, phone, instant messaging, and remote desktop with an impersonator to cheat in an online examination. The potential solution to this will be discussed later in the thesis.

10.4.1.3 Abetting

In a non-proctored exam, students may receive help from a third party to answer the test questions. In their study, Tindell et al. (2012) surveyed 269 students, with 10% admitting to the use of mobile phone for abetting during exams. Absence of remote proctoring or monitoring creates opportunities for students to ask third parties for help. As outlined in Chapter 3, this type of collusion was classified as abetting. A student and a third party could collaborate and answer the test questions based in the same location or communicate remotely. Participants of the focus group perceived this as a serious threat as there is always a possibility that a student may get someone to sit close by, or in a remote online examination, who is an expert. According to a participant:

Participant 9:

> *"I would imagine the trick would be to prevent people sitting next to you and doing the test with, and I think that is the biggest problem"*

The content analysis in Table 10-3 shows that participants perceived this a high risk and scored M = 5, if a student invites a third party to the exam location for abetting. The potential solution to this will be discussed later in the thesis.

10.4.2 Security Analysis and Discussion

While it is established that collusion is a rising concern in remote online examinations, authentication approaches alone may not provide adequate security to mitigate both impersonation and abetting threats. Different types of collusion threat may need different deterrence approaches.

A challenge question approach, as well as ProctorU (secure browser and proctoring tool), were proposed to influence impersonation and abetting attacks. The focus group discussion on the proposed methods is presented in the following sections.

10.4.2.1 Dynamic Profile Questions to Influence Impersonation

The dynamic profile question approach was proposed as a solution to positively influence impersonation attacks in the first presentation. In order to explore participants' perception of the use of dynamic profile questions, the moderator asked whether they would use this approach in an online examination for their students. The majority of participants agreed and understood that it would make an impact on impersonation. The content analysis in Table 10-3 on the use of dynamic profile questions for mitigation of impersonation shows participants' agreement and scored M = 3.8. According to participants in the focus group:

Participant 6:

> *"Yes, I agree!"*

Participant 7:

> *"Yes, it is better than what we do now"*

Participant 8:

> *"Yes, it is that extra level of security"*

Participant 5:

> *"Yes!"*

Dynamic profile questions may influence impersonation attacks using phone and email. The empirical study reported in Chapter 9 shows that these questions can positively influence impersonation via email. The study also revealed that impersonation attacks using mobile phones were successful; however response times could be implemented to discourage such attacks. The study reported a significant difference ($p < 0.01$) in the response time of a third party impersonator using a mobile phone and a genuine student during an online examination. Students are often expected to complete their tests in an allocated time and this can be used as a factor to positively influence the use of mobile phones in online examinations. Participants in the focus group provided positive feedback on the use of a response time factor for use against impersonation. The content analysis in Table 10-3 shows participants' perception that timing answers may impact impersonation using a mobile phone, which scored M = 3.8. There was agreement that timing answers will deter students from colluding (M = 4.5). According to some participants:

Participant 1:

> *"If the answers are coming slowly, slower than what you would expect, or in some strange way, we can just say that we are not accepting this, because there is a problem"*

Participant 4:

> *"It makes it very hard for somebody who pretends to be you or collude"*

In a practical situation, if a student is taking noticeable time to respond to authentication and questions in an online examination, it could be noticed by the course administrator/tutor. According to some participants, response time could be used as a factor for assessing test questions as well.

Participant 4:

> *"If they cannot get through the test in time. Time can be used as a factor to minimise the looking"*

Course and online examination design is another important factor to discourage students from taking help. As an example, if an online test consists of multiple choice questions, an expected response time can be easily determined. However, for an open text descriptive question, this may vary. A participant suggested that course and examination design may discourage students from searching the Internet.

Participant 8:

> *"That's what we have done on the JAVA module. Because some student came and said, I can just search the answer on the Internet and can find the correct answer. I replied, if you do, you won't get enough time to finish the majority of the questions. Basically, those questions cost the time"*

However, there are risks associated with the implementation of response time factor for reduction of collusion. This may be challenging to prove a slow response time as the only evidence of a collusion attack. Some participants raised their concerns about using a response time factor to penalise students:

Participant 6:

> *"I think it is a bit of a hassle to try and prove whether a student has colluded or cheated"*

In a practical scenario, students may challenge a decision if they were penalised due to a longer response time, and ask to redo their test. Another participant raised concerns for penalising students based on a response time factor:

Participant 1:

> *“What if the student wants to protest? If you say, well, I don’t accept this answer, and the student says, why not, I dint do anything wrong”*

However, the majority of participants agreed to implement additional security factors, including response time, to deter collusion.

Participant 4:

> *“If we are confident that someone has cheated, we know that the test in invalid, we ask the student to go back and do it again”*

10.4.2.2 Secure Browser and Proctoring (ProctorU) to Influence Abetting

The majority of traditional authentication approaches may not detect abetting attacks to ensure that a student is taking an online test without getting help from someone sitting close by or in a remote location. Live invigilation or monitoring may mitigate abetting and discourage a student from communicating with a third party during an online examination session. Participants in the focus group agreed that remote proctoring may positively influence abetting. According to a participant:

Participant 8:

> *“I think the remote proctoring possibility sorts out the person sitting next to you to some extent anyway”*

A remote proctor and secure browser can be implemented to prevent the use of unwanted software e.g. Skype, remote desktop sharing, Internet browser and invigilate an online examination session. One such example is ProctorU, a remote proctoring system for online tests. Trained invigilators at ProctorU watch test-takers by using screen sharing and webcam feeds at offices in Alabama and California (Eisenberg, 2013). An invigilator verifies the identity of an online student and monitors the examination process. This may be an expensive approach for online tests with a large number of students. In order to explore their feedback on using ProctorU, participants were asked if they would use this approach in an online examination for their students. A large number agreed and understood that it would impact collusion.

Participants suggested that the use of dynamic profile questions and ProctorU together would enhance the security of online examinations to mitigate impersonation and abetting.

Participant 9:

> *“And by making it harder with challenge questions could have another additional layer. Ok! The name did match, and the photo looks all right, however, how come this part (dynamic profile question) of the authentication did not occur”*

10.5 Summary

The study investigated a group of experienced online programme tutors from the University of Hertfordshire. Based on their feedback, impersonation using mobile phone, email, remote desktop sharing, and abetting were identified as common cause for concern. The empirical results in previous studies and feedback from the focus group suggest that dynamic profile questions are more usable than text-based and image-based questions. This method may positively influence impersonation attacks using email and mobile phones if an additional factor, such as response time, is also considered. However, dynamic profile questions may not detect abetting attacks, when a third party helps a student sitting close by or remotely during an online examination session. A secure browser and remote proctoring tool (ProctorU) may countermeasure abetting attacks to monitor the location of a test taker.

There has been an increase in the use of online learning and examinations across the world. Many course providers use 100% coursework in remote online environments, and rely upon online examinations for assessment purposes. This increases the importance of a secure examinations environment. This study recommends the use of challenge questions (dynamic profile questions) and remote proctoring with a secure browser that will improve the situation. It was agreed by the online programme tutors that the use of these proposed methods could influence and discourage students from perpetrating impersonation and abetting attacks.

The implementation of dynamic profile questions and proctoring tools will make it more difficult for students to use mobile phones or chat services on a computer for real-time information sharing. However, students may attempt to share answers to dynamic profile questions, learning experience with a third party impersonator *before* an online examination session through email, phone, or a face-to-face meeting to circumvent the proposed method and impersonate. To investigate students’ ability to share dynamic profile questions with a third party offline, before an examination session, the following chapter will report the final study.

11 Study 6: Dynamic Profile Questions and Proctoring

In the focus group study described in the previous chapter, online programme tutors recommended the use of dynamic profile questions, remote proctoring (Mahmood, 2010), and a secure browser to influence impersonation and abetting attacks. However, students may still attempt to circumvent this approach. A student may share information about their learning experience and activities with a third party impersonator before an online test via email, phone, instant messaging, or face-to-face meeting. This chapter presents Study 6, which simulates an impersonation abuse case scenario, when a student shares information about his learning experience with another individual who attempts impersonation in the presence of live proctoring.

The chapter describes the purpose, research questions, hypotheses, and research method. The following sections explain participants' recruitment and their characteristics, design of an online course, and study phases. This includes a description of an abuse case scenario using a three-week online course to investigate impersonation attacks. The study involved campus students for pairing and simulating the abuse case in a controlled lab based environment. Finally, the chapter reports the effectiveness and outcomes of the impersonation abuse case. Feedback from a post-study questionnaire is also reported to conclude the chapter.

11.1 Purpose

The focus group study presented in Chapter 10 indicates that the use of dynamic profile questions with a secure browser and proctoring (ProctorU) (Mahmood, 2010) can positively influence collusion attacks. As described in Chapter 9, dynamic profile questions are created non-intrusively and non-distractingly in the background when a student performs learning activities. Using this method, a student's profile is built and consolidated in the background during the learning process. Students are not aware of which questions will be asked for authentication. This attempts to verify that the person who is taking the online test is the same individual who completed the coursework. The use of a secure browser and proctoring monitors an online examination, and attempts to ensure that a student is not taking help from the Internet or an abettor sitting close by or remotely. However, a student may still circumvent the system and share access credentials with an impersonator *before* the test session.

As discussed in the previous studies, effectiveness is an important attribute defined by the ISO which contributes to the usability (ISO9241-11, 1998). In the context of this study, effectiveness means that participants were able to answer dynamic profile questions correctly with a low error rate. This study will investigate the following:

1. The effectiveness of dynamic profile questions in a proctored examination.
2. Whether a student can share information about learning activities and experience with a third party impersonator using email, instant messaging, phone, or face-to-face meeting before an online test session, and how successful the impersonator is in answering the dynamic profile questions.

11.2 Research Questions and Hypotheses

The research questions RQ 3) and RQ 4) identified in Chapter 1 are cascaded into more questions associated with usability and collusion, in order to approach the research problems. The research question RQ 3c) is associated with the usability attributes of dynamic profile questions. Similarly, the research question RQ 4b) is associated with the use of the dynamic profile question approach and its influence on collusion threats. This study attempts to answer the following research questions, which are derived from RQ 3c) and RQ 4b) :

RQ 11.1) How effective are the dynamic profile questions for authentication in a proctored online examination?

RQ 11.2) How can authentication based on dynamic profile questions influence a third party impersonation attack in a proctored online examination?

The following hypotheses were framed to answer the above research questions. Each hypothesis maps to the corresponding research question:

H 11.1) Dynamic profile questions are effective when implemented for authentication in a proctored online examination.

H 11.2) Dynamic profile questions can positively influence impersonation attacks in a proctored online examination, when a student shares dynamic profile questions with a third party before an online examination session.

11.3 Study Method and Design

This study was conducted in a real online course and a controlled laboratory-based simulation environment. The usability test and risk-based security assessment methods described in Chapter 5 were adopted to evaluate the usability and security of dynamic profile questions. The usability test method is a usability inspection, which tends to focus on the interaction between humans and computers (Corry et al., 1997). Using this method, the representative users – i.e. students – work on typical system tasks on an online course and examination, which implements dynamic profile questions in a proctored test. In this study, the system tasks were simulated in a laboratory-based environment. The usability evaluation scale described in Chapter 5 (section 5.2.1) was used to translate the effectiveness analysis. This scale describes the usability of products in the 90s as exceptional, 80s as good, 70s as acceptable, and anything below 70 indicates usability issues that are cause for concern (Bangor et al., 2009).

As discussed earlier, the risk-based security assessment approach provides rapid quantification of security level risks associated with processes (Ni et al., 2003). This method focuses on the test of features and functions of artefacts based on the risk of their failure using abuse case scenarios (McGraw, 2004). An abuse case scenario was simulated to investigate impersonation attacks, when dynamic profile questions are implemented for authentication of students in a proctored examination.

This study was conducted in a remote online learning environment and face-to-face sessions involving on-campus students. It was organised into two phases: Phase I - online course and Phase II - abuse case simulation. Study phases are described below.

11.3.1 Phase I – Online Course and Student Pairing

In Phase I of the study, an online course was conducted to provide learning opportunities for students and facilitate the collusion abuse case scenario. The structure of Phase-I is described below.

- **PHP & MySQL Course Design:** A ‘PHP and MySQL’ online course was organised with three weekly modules, which included lessons, forum discussions, assignments, quizzes, grades and student reflection at the end of each week. The course was set up and deployed in the MOODLE Learning Management System (LMS) on a remote web server accessible on the Internet. Students were required to invest 10 hours weekly learning effort for 15 days in a span of three weeks. A detailed course outline is given in Appendix E (I).
- **Participants Recruitment:** On-campus students from the School of Computer Science, University of Hertfordshire, were recruited to participate in the study and the online course. The course was advertised on the StudyNet. To motivate

students the course was offered free of charge. Participants were selected on the basis that they knew each other already. They were also required to have basic programming knowledge in order to enrol. A total of 12 students were enrolled and completed the three-week course. There were 7 (58%) male and 5 (42%) female participants. They were also enrolled in BSc/MSc programmes which were helpful in setting up face-to-face meetings to present the study structure and research objectives, and perform the abuse case scenario in a laboratory. There was no repeated attendance of participants from the previous studies presented in Chapters 6, 7, 8, 9, and 10.

- **Presentation and Students Registration**: Participants were required to attend a face-to-face 15 minute presentation (see Appendix E (II)) on the course structure and research objectives, before registration. They were also provided detailed information on an impersonation abuse case scenario. It was essential for participants to understand the purpose of the research and how to perform impersonation attacks. They were provided an enrolment key and the course was made available to registered users. After the presentation, all participants signed the consent forms mandated by the University ethics regulations.
- **Pairing up of Participants for Impersonation**: In order to perform the impersonation, each participant was paired up with a fellow student (classmate), where both participants confirmed that they were familiar already. All participants consented to share learning experience and activities with their pairs. They were informed about the format of an impersonation abuse case scenario, which was conducted towards the end of the course.
- **Online Course Work:** The instructor-led course was conducted over a period of three weeks. Participants were required to submit their weekly assignments in order to access their weekly quizzes. Each assignment was based on the weekly course content, which ensured participants' engagement. It was mandatory for each participant to take their weekly quizzes and provide a 'reflection feedback' towards the end of each week.
- **Creating Dynamic Profile Questions**: Dynamic profile questions were created manually during the course for each individual student and stored in a Microsoft Word file in a secure location. These questions were created on a daily basis for each participant after access to course content including lessons, assignment submission, assignment grades, quiz completion, feedback and reflection, and forum discussion. This helped with creating and consolidating a profile for each

participant. A total of 28 dynamic profile questions were created for each participant, which were based on questions shown in Appendix E (III). Dynamic profile questions created during the coursework were not shown to any participant during the online course until the abuse case scenario described in the following section.

11.3.2 Phase II – Impersonation Abuse Case Scenario

In Phase II, the following impersonation abuse case scenario was simulated towards the end of a three-week course described above in order to evaluate impersonation attacks:

> *"A student is registered on an online course. The course utilises dynamic profile questions, a remote proctor and a secure browsing tool for authentication of students in online examinations. The student is due to write his/her final online test. He or she wants to boost his/her grades and recruits a third party impersonator to take his test. The online test is monitored by a proctor remotely on a live web cam. In order to satisfy the dynamic profile questions authentication, the student needs to share his/her learning experience, learning activities and cues with the impersonator before the online test. The impersonator uses the shared information to answer the randomly presented dynamic profile questions for authentication in presence of a live proctor"*

Given the above scenario, this study simulated an impersonation abuse case scenario described below:

1. Participants were paired up before registration as described above in Phase I (section 11.3.1).
2. Dynamic profile questions for each participant were manually created and stored in their respective profiles. These questions were extracted from student activities on a daily basis, as described above in Phase I (section 11.3.1).
3. Participants were asked to share their learning experience, learning activities, and cues with their pairs during the course. They were allowed to share this information using any communication means, e.g. email, phone, WhatsApp, Skype, face-to-face meeting, Facebook, Facetime, SMS, printed paper, etc. They were required to memorise the shared information for simulating impersonation in a proctored examination.

4. At the end of week three, participants attended a laboratory-based simulation session.
5. Participants were informed about the format of simulating the laboratory-based proctored session. They were required to answer the questionnaire from memory and were not allowed to use an electronic or printed copy of the information shared by their pairs for impersonation. Also, they were not allowed to communicate or share information when answering the two questionnaires in the following order:
    a. **Questionnaire 1 (Effectiveness):** Participants were asked to answer paper-based Questionnaire 1 with a total of 10 dynamic profile questions randomly extracted from their profiles created during the course work in Phase I (section 11.3.1).
    b. **Questionnaire 2 (Impersonation):** After answering Questionnaire 1, the participants were asked to answer a paper-based Questionnaire 2 with a total of 5 dynamic profile questions randomly extracted from their pair's profile to simulate impersonation.

11.4 Results

The usability analysis of dynamic profile questions was initially performed and reported in Chapter 9. This section aims to evaluate the usability of dynamic profile questions in the presence of a live proctor. At the end of week three, 12 participants answered 120 dynamic profile questions which were created during the course. Results of the abuse case scenario is also analysed to determine the outcome of an impersonation attack.

11.4.1 Effectiveness

The effectiveness is considered to be the degree of accuracy of participants' responses. It is an important usability factor which indicates a degree of completeness with which users achieve a specified task in a certain context (Seffah et al., 2001). In the context of this study, it means that participants were able to provide correct answers to their dynamic profile questions correctly with a low error rate. It was analysed on the data collected from participants' answers on paper-based questionnaire 1 in a laboratory-based session. Table 11-1 shows the mean of correct answers to dynamic profile questions in order to analyse effectiveness. The findings show 114 (95%) correct answers, which indicates better effectiveness compared to text-based and image-based questions reported in Chapters 6 and 7.

Table 11-1 Usability Analysis: Effectiveness

Participants	Correct
1	10 (100%)
2	10 (100%)
3	9 (90%)
4	9 (90%)
5	10 (100%)
6	9 (90%)
7	10 (100%)
8	9 (90%)
9	9 (90%)
10	9 (90%)
11	10 (100%)
12	10 (100%)
Total	**114 (95%)**

According to the usability scale presented in Chapter 5 (section 5.2.1) and letter grades (70%-79% acceptable, 80%-89% good, more than 90% exceptional) described by (Bangor et al., 2009), 95% correct answers is an exceptional effectiveness. Based on the above discussion, the following hypothesis was accepted.

H 11.1) *Dynamic profile questions are effective when implemented for authentication in a proctored online examination.* ***Accepted***

11.4.2 Impersonation in Presence of Live Proctoring

The abuse case scenario was performed to decide if dynamic profile questions can mitigate impersonation in a proctored exam. In a laboratory-based session, participants answered paper-based Questionnaire 2 consisting of five dynamic profile questions on behalf of their pairs. They memorised the shared information during pairing and answered the questionnaire from memory. These questions implemented five multiple choice options and the probability of a correct answer to a random guessing would be 1/5th or 20%. In the impersonation abuse case scenario, participants answered 26 (22%) of the questions correctly on behalf of their pairs. These questions were not shown to any participant during the online course and presented at the final stage of the study to evaluate their ability to circumvent the dynamic profile question approach and impersonate students in the presence of a live proctor.

The findings in Table 11-2 show that the sharing of information associated with individuals' learning experience led to correct answers just above 1/5th of the total questions.

Table 11-2 Security Analysis: Answers by Impersonator

Participants	Correct
1	2 (20%)
2	1 (10%)
3	3 (30%)
4	3 (30%)
5	2 (20%)
6	1 (10%)
7	2 (20%)
8	2 (20%)
9	3 (30%)
10	2 (20%)
11	2 (20%)
12	3 (30%)
Total	**26 (22%)**

To determine the significance of difference in the means of correct answers to dynamic profile questions by a student and a third party impersonator, a one-way ANOVA was performed on the data shown in Tables 11-1 and 11-2, which shows a significant difference F = 596; p = 0.00 ($p < 0.01$); eta-squared $\eta^2 = 0.97$. An ANOVA test on a small sample size may not produce significant values due to insufficient power. However, findings of the test here yielded significant value.

In a practical situation, this may fail the authentication and alert the proctor or invigilator. This shows that students were able to answer their own challenge questions presented in the previous section (see section 11.4.1); however, collusion between students and impersonators was not successful. Based on the above findings, the following hypothesis was accepted.

H 11.2) *Dynamic profile questions can positively influence an impersonation attack in a proctored test, when a student shares dynamic profile questions with a third party before an online examination session.* ***Accepted***

The data shared by participants with their pairs for impersonation could not be recorded for analysis. However, to collect information about data sharing, a post-study questionnaire was developed and is discussed below.

11.4.3 Information Sharing Frequency and Method

In a post-study survey, participants were asked for feedback on the communication method, frequency, and type of information shared during the abuse case simulation. Table 11-3 shows a summary of feedback received, which is discussed in the

Table 11-3 Information Sharing: Frequency, Type and Method of Sharing

Question	Options	Feedback
Q.1 How did you share information with your pair during collusion?		
	Email	10 (66.7%)
	WhatsApp	3 (20%)
	Skype	0 (0%)
	Facetime	0 (0%)
	Facebook	0 (0%)
	Face-to-face meeting	2 (13.3%)
	SMS	0 (0%)
	Printed Paper	0 (0%)
	Other	0 (0%)
Q.2 How many times did you share information in the three weeks?		
	On a daily basis	0 (0%)
	On completion of each session	4 (33.3%)
	On a weekly basis	2 (16.7%)
	Once through the entire course	2 (16.7%)
	Twice through the entire course	3 (25%)
	Towards the end of the course	1 (8.3%)
Q.3 What kind of information did you share with your pair during the collusion?		
	Titles of the completed course sessions	11 (42.3%)
	Details of the completed course sessions	3 (11.5%)
	Assignment score	4 (15.4%)
	Assignment questions completed	5 (19.2%)
	Quiz score	1 (3.8%)
	Reflection Information	1 (3.8)
	Email Information	1 (3.8%)

following sections.

Communication during Collusion: To understand a preferred communication method, participants were asked for their feedback to Q.1 shown in Table 11-3. It was anticipated that phones and face-to-face meetings would be the preferred communication methods to share information. However, the majority of participants 10 (66.7%) used email for information sharing. Face-to-face meetings were held by 2 (13.3%) participants and another 3 (20%) used mobile chatting application ‘WhatsApp’. The above results indicate that email was a preferred and convenient method of communication for students to share information.

Frequency of Information Sharing: Frequency of communication in a timely manner is important to share relevant information for the success of an impersonation attack. In order to understand how frequently students communicated to share information, participants were asked for their feedback to Q.2 shown in Table 11-3. The online course contained multiple daily and weekly learning sessions, and participants shared information on completion of their relevant learning activities. A large number of participants (4: 33.3%) shared information about their learning experience with a partner at the end of “each session”. The majority of participants shared information at least once, twice or three times a week. As shown in Table 11-3, 2 (16.7%) communicated “once through the entire course” and 1 (8.3%) “towards the end of the course” which implies that 2 (16.7%) + 1 (8.3%) = 3 (25%) communicated only once through the entire course duration. A total of 3 (25%) communicated twice. The above results indicate that the frequency of communication for sharing learning experience and information about learning activities was at least once a week during a three-week course. This may enable a student to share learning activities performed in the week.

Type of Information Sharing: In order to understand what type of information was shared for impersonation, participants were asked for their feedback to Q.3 shown in Table 11-3. A large number of participants (11: 42.3%) shared “titles of the lessons” completed. Results of the impersonation attack discussed in the previous section indicated that “titles of the lessons” was not helpful to inform answers to the dynamic profile questions. These questions were extracted from the content and associated with individuals’ submissions. 5 (19.2%) participants shared assignment questions and 4 (15.4%) shared assignment scores, which were associated with the actual dynamic profile questions and resulted in 22% correct answers in the impersonation abuse case reported in the previous section (see section 11.4.2). The findings indicate that sharing relevant information increases the success of an impersonation attack.

11.5 Summary

This study examined the use of dynamic profile questions in a proctored examination. Participants shared information using mobile phones, emails, chat, and face-to-face meetings at their own convenience before an online examination in pairs. They memorised the shared information and answered the questionnaire on dynamic profile questions on behalf of their pairs in the presence of a proctor. The results show that dynamic profile questions decreases impersonation attacks when implemented with live proctoring. Participants' sharing helped the impersonators to provide 26 (22%) correct answers in the impersonation attack, which is just above 20%, which is the percentage of correct answers by chance. There was a significant difference ($p < 0.01$) in the correct answers between a student (114: 95%) and an impersonator (26: 22%). In participants' feedback taken from the post-study online questionnaire, email was reported as the preferred way of sharing information with a third party impersonator. Students were able to share titles of the learning activities, which was not enough for impersonators to answer all their dynamic profile questions. Although, the frequency of sharing was at least once a week during a three-week course, the information shared was not relevant to the actual questions. This implies that sharing of relevant information increases the success of an impersonation attack. Furthermore, dynamic profile questions extracted from course content and submissions makes sharing harder for students.

The above findings indicate the use of dynamic profile questions and proctoring tools recommended in the focus group study can positively influence impersonation and abetting in online examinations.

12 Conclusion and Future Work

This chapter summarises the findings and conclusions of this research work. The following sections represent the summary of the work, and the research outcomes. It provides a summary of the main contributions and the future outlook of this research.

12.1 Summary of Research

This research focused on the security and usability of authentication by challenge questions in online examinations. In this work, I undertook the following research studies.

This research work investigated security threats and proposed a profile-based challenge question authentication approach to mitigate them. The first empirical study described in Chapter 6 was organised to examine the usability attributes: the efficiency and effectiveness of the proposed challenge question approach. This study implemented pre-defined text-based questions, which are associated with individuals' personal information. It was anticipated that a friend or colleague may be able to guess correct answers on behalf of the user. Therefore, this study also performed a security investigation using a guessing abuse case scenario. The first study was performed using an initial prototype for the collection of benchmark data.

Based on the findings of the first study, pre-defined text-based and image-based questions were implemented in the second study presented in Chapter 7. This study investigated usability attributes: the efficiency and effectiveness of text-based and image-based questions in a real educational context using an online course.

The third study presented in Chapter 8 investigated impersonation attacks using pre-defined text-based challenge questions. The study examined the influence of sharing different numbers of questions with a third party impersonator. It investigated how the number of questions shared and the size of the database affects the success of a collusion attack.

Based on the findings of the third study, dynamic profile questions were proposed. The fourth study presented in Chapter 9 investigated usability attributes: the effectiveness of dynamic profile questions in an online course. The study examined impersonation attacks, when a student and a third party impersonator share access credentials using an email (asynchronously) or a mobile phone (real time).

The fifth study presented in Chapter 10 invited online programme tutors as important stake holders to participate in a focus group session. Participants in the study were security and assessment experts, scientists, tutors, and examinations designers. They were asked for their feedback on security threats including collusion, the proposed solution and relevant usability attributes.

The sixth and final study presented in Chapter 11 investigated the usability and security of dynamic profile questions in a proctored online examination. The study simulated an impersonation attack in an online course and face-to-face laboratory-based sessions.

The above studies were conducted to achieve the following aims and objectives. This thesis aimed to design and analyse an authentication approach, understand the essential usability attributes and impact of the proposed method on collusion attacks in a remote online examination. In order to achieve the above aim, a list of the following research objectives was generated to:

Objective 1) Investigate security threats to online examinations.

Objective 2) Investigate and design an authentication approach, and understand its influence on the potential security threats to online examinations.

Objective 3) Evaluate usability and its influence on the security of the proposed authentication method.

Objective 4) Evaluate the security of the proposed method.

To achieve the above objectives, this research attempted to answer the following research questions and sub-questions:

RQ 1) What are the potential security threats to online examinations?

a. What are the potential collusion and non-collusion threats to online examinations?

RQ 2) What method can be used to support the secure authentication of students in online examinations?

a. How can the challenge question approach be used for the authentication of students in online examinations?

RQ 3) How does the usability of the proposed authentication method influence the security?

a. How does the usability of text-based questions influence the security of the challenge question approach in online examinations?

b. How does the usability of image-based questions influence the security of the challenge question approach in online examinations?

c. How does the usability of dynamic profile questions influence the security of the challenge question approach in online examinations?

RQ 4) How does the proposed authentication method influence security threats?

a. How does the use of text-based questions influence the collusion threats in online examinations?

b. How does the use of dynamic profile questions influence the collusion threats in online examinations?

12.2 Summary of Research Outcomes

The research problems were approached with a focus on the research questions, which were derived from the research objectives. In order to achieve this, the research work was organised into two phases. In the first phase, the research problems and a proposed solution were identified. In the second phase, the empirical evaluation of the proposed solution was performed in multiple studies. These studies were conducted in simulation and real educational contexts using a combination of quantitative and qualitative methods. These two phases aimed to answer the four research questions and sub-questions identified in Chapter 1, which were further cascaded into more research questions as the work progressed. These questions were answered in the following manner.

RQ 1) What are the potential security threats to online examinations?

The first research question focused on determining the weaknesses and vulnerabilities that create potential threats to online examinations. A threat is the potential for misuse or abuse that will cause harm or exploit online examinations (assets) (Haley et al., 2004). Weak authentication and the absence of face-to-face interaction create numerous threats to the high-stake examination process. To understand the potential harm that a security breach may cause, it is important to recognise the likelihood and description of a threat (Miguel et al., 2015a). Identifying potential threat scenarios may help us to understand what can go wrong if a threat scenario occurs. To achieve this, multiple abuse case scenarios were created using the risk-based assessment method presented in Chapter 5.

Threats to online examinations were identified from the literature review and experience. The threat classification presented in Chapter 3 provided a description of potential threats, which include intrusion and non-intrusion attacks. Intrusion attacks are performed by cyber attackers, criminals and hackers (Hugerat et al., 2013). These attacks are carried out to exploit information without causing any harm to the online learning and examination system (Hugerat et al., 2013). The attacker may not destroy data in an online course; however, this causes distrust and affects the credibility of an online system.

RQ 1a) What are the potential collusion and non-collusion threats to online examinations?

The sub-question RQ 1a) was related to collusion and non-collusion attacks. These attacks may come from a legitimate student individually or in collusion with a third party. There are a number of factors that influence the cheating behaviour of students in general. They often cheat to qualify or to enhance their grades. This stimulates many threats that may be further classified in two categories: collusion and non-collusion. In general, these threats are open-ended and widespread due to the fact that students access learning and examinations on the Internet, and there are weak authentication mechanisms. Collusion was further classified into impersonation and abetting threats. Impersonation happens when a student willingly shares access credentials with a third party to impersonate him in an online examination (McGee, 2013). These attacks are pre-planned and consensual, involving legitimate students with valid access credentials. It is difficult to detect such attacks once an online test is completed (Kerka and Wonacott, 2000). These are evolving with the increasing use of new communication technologies. The potential impersonation scenarios include: impersonation using mobile phone, email, remote desktop sharing, and instant messaging. In abetting, a legitimate student takes an online test; however, he or she obtains help from a third party. This is described as panic cheating, when a student is struggling to answer a question during the test. Stuber-McEwen et al. (2009) state that aiding and abetting is a common practice in both online and classroom cheating. Regardless of whether students were online or in on-ground classes, aiding and abetting with exams were the most frequently reported forms of cheating (Dietz-Uhler and Hurn, 2011). In the absence of proctoring, live invigilation or remote monitoring, it may be challenging to ensure that the test taker is not getting help from someone sitting next to them or in a remote location.

While the literature review provided an understanding of the threats, experts were asked for their perception of the identified threats in a focus group study. The study described in Chapter 11 presented feedback from online programme tutors, who were experts in course design, examinations, assessment design, invigilation, teaching and scientific research. A paper-based questionnaire and a focus group discussion were used for the collection of feedback in two phases (see Table 12-1).

Table 12-1 Evidence: Threats Classification

Items	Method	Section	Outcome
1.	Questionnaire	10.3	Online programme tutors participated in a focus group study. They identified impersonation and abetting as serious threats.
2.	Focus Group	10.4	Online programme tutors agreed that collusion is a major threat and that the use of technology creates more opportunities for impersonation and abetting.

In the first phase, the experts provided their feedback on the questionnaire (see Table 12-1 item 1). They showed strong concern regarding the security threats to online examinations. The majority of the participants were concerned about *"Online examinations" and "Authentication approaches"*, and their feedback scored M = 4 and M = 3.7 respectively (1 = no concern at all and 5 = strong concern). There was an agreement that cheating in online examinations is less difficult than in a face-to-face invigilated exam. They expressed high concern for security threats including *"impersonation"* and *"abetting",* which scored M = 4.1 and M = 4.2 respectively (1 = no concern at all and 5 = strong concern).

In the second phase, the focus group discussion was held (see Table 12-1 item 2). The participants agreed that the absence of invigilation or monitoring creates more opportunities for cheating, and that students' actions are difficult to monitor in a remote environment. There was an agreement that collusion is a major threat and the use of technology (mobile phones, email, instant messaging, and remote desktop sharing) creates more opportunities for impersonation and abetting attacks. The majority expressed concern that *"it is challenging to verify that a student signed up for a course is the same person who is taking the online examination".*

In response to these threats, an authentication method was needed, which could countermeasure impersonation and abetting attacks in online examinations. It was followed up in the next research question below.

RQ 2) What method can be used to support secure authentication for online examinations?

The existing authentication features are not sufficient to ensure that the correct student takes an online examination. These features provide different levels of security assurances and usability. Their cost of implementation and accessibility in dispersed geographical locations vary. Many of the existing features may have varying issues including costs of implementation, infrastructure constraints, accessibility, usability and security.

RQ 2a) How can the challenge question approach be used for the authentication of students in online examinations?

In order to answer the second research question and sub-question, a profile-based authentication was proposed (Ullah et al., 2012a). The proposed method was described in Chapter 4; it utilises challenge questions for the authentication of students in online examinations (see Table 12-2). Using this method, a student profile is built and consolidated during the learning process. Information in a student profile is stored in the form of questions and answers. A subset of these questions is used for authentication. A student registers *n* profile questions, and presented with *t* challenge questions upon authentication, where $t \leq n$. To an individual $r = t$ or $r \leq t$ questions must be answered correctly in order to authenticate (r = number of correct answers). This approach aimed to discourage students from sharing their access credentials with third party impersonators. It attempts to help ensure that the student taking an online test is the same one who completed the course work. The initial prototype of the proposed method was designed in PHP and implemented in a MOODLE learning management system. The architecture of the proposed design, including a presentation layer, business logic layer and data layer, were presented (see Table 12-2 items 1-2). This is a knowledge-based feature, which is accessible

Table 12-2 Evidence: Proposed Authentication Approach

Items	Method	Section	Outcome
1.	Design	4.2	A conceptual design of the proposed profile-based authentication system.
2.	Architecture	4.4.2	A three-tier architecture design of MOODLE and integration of the proposed profile-based authentication method.

on standard input devices. Unlike biometrics and object-based features, this method does not require dedicated input devices or infrastructure.

The traditional challenge questions feature an important fall back and credential recovery approach (Just and Aspinall, 2009a). The security and usability of this method are reliant upon the quality of the question design. Therefore, this thesis proposed and examined different types of questions, including text-based, image-based and dynamic profile questions. The proposed method was evaluated for usability and security in six studies using different question types. The outcomes of the usability investigations are presented in the following section.

RQ 3) How does the usability of the proposed method influence the security?

Usability is an important quality of software systems. It is a measure of useful interactions between a system and target users in a specified context. It is not a single component but multiple attributes applied to systems in different contexts. Many researchers argue that secure systems are compromised through human errors and that “ease of use” is essential in order to make users behave securely (Adams and Sasse, 1999, Yee, 2002, Poulsen, 2000). Security techniques are only effective when usable (Sasse et al., 2001). It is essential for security designers to understand the user behaviour in order to build usable and secure systems. Authentication provides access to many secure systems and it is successful when security and usability are aligned. Di Raimondo and Gennaro (2005) state that authentication is a main goal when security is implemented, whereas usability is the main goal of system implementation. Therefore, this research investigated the usability attributes of the proposed challenge question approach in multiple studies.

In order to answer the third research question, a review of the literature associated with methodologies to evaluate usability attributes was undertaken. The usability test method described in Chapter 5 was implemented to examine usability attributes: efficiency and effectiveness recommended by ISO/9241-11 (Jokela et al., 2003). The efficiency is a usability attribute, which can be evaluated by measuring the completion time of each task and sub-tasks separately (Seffah et al., 2001). A system is considered efficient if users are able to complete tasks in a reasonable time. The effectiveness is considered to be the degree of accuracy of the participants’ responses. In the context of a challenge question approach, it means that the participants were able to provide answers to their questions correctly with a low error rate. The effectiveness was evaluated using a scale defined by Bang et al.

(2009) based on the standard letter grade scale. This scale provides an adjective description of the effectiveness, i.e. products that scored in the 90s were exceptional, those that scored in the 80s were good, and those that scored in the 70s were acceptable. The usability attributes were investigated for text-based, image-based and dynamic profile questions in empirical studies presented in Chapters 6, 7, 9, 10 and 11.

Table 12-3 Evidence: Usability Investigations

Items	Method	Section	Outcome
1.	Simulation	6.4	The effectiveness was 58% using an equality algorithm and 76% using a relaxed algorithm. The mean completion time was 15.7 seconds per response.
2.	Simulation	6.4.2.1	The effectiveness increased using a traffic light access control system. This allowed multiple authentication attempts.
3.	Statistical Analysis	7.4.1	The efficiency increased with an increase in the number of visits.
4.	Statistical Analysis	7.4.2	The effectiveness of image-based questions (85%) was better than text-based questions
5.	Statistical Analysis	9.4.1	The effectiveness of dynamic profile questions was 99.5%
6.	Questionnaire	10.3	Participants' feedback ranked questions effectiveness as 1) dynamic profile 2) image-based and 3) text-based questions. (1 most effective)

RQ 3a) How does the usability of text-based questions influence the security of the challenge question approach in online examinations?

The first empirical study is presented in Chapter 6, which examined the usability attributes: efficiency and effectiveness using an initial prototype of the challenge question method. A total of 20 text-based questions were implemented in the first study. These questions were organised into different themes: academic, contact, personal, date and favourite. These are traditional personal security questions, which are utilised by many email service providers, websites and online banks (Just and Aspinall, 2012, Schechter et al., 2009). The study was conducted in a simulation online learning and examination environment. The initial findings revealed some usability challenges (see Table 12-3 items 1-2). The mean completion time of all questions was 15.7 seconds, which implies that a user could answer three questions within a minute. There was a significant correlation between answer length and response time ($p < 0.01$). The use of challenge questions creates an interruption in the normal learning process. The mean correct responses to all questions were 58% using a string-to-string comparison or equality algorithm (see Table 12-3 item 1). Questions with clarity, ambiguity and format issues had poor efficiency, which influenced the effectiveness during authentication. This algorithm penalised answers with syntactic variation, spacing, capitalisation and spelling mistakes, which led to incorrect answers. The use of a relaxed algorithm (Schechter et al., 2009) compensated for these issues and increased the correct per cent to 76%. There was a significant difference in the correct answers between equality and relaxed algorithms ($p < 0.01$). To compensate for the identified usability issues, a traffic light access control system was also implemented. This allowed multiple attempts to users, who provided correct answers to some questions out of the total presented on pre-set criteria. This increased the success rate of authentication from 23% to 92%.

RQ 3b) How does the usability of image-based questions influence the security of the challenge question approach in online examinations?

To address the usability issues identified in Chapter 6, image-based questions were implemented. The second empirical study presented in Chapter 7 utilised image-based and text-based questions. This study examined the usability attributes: efficiency and effectiveness. Image-based authentication substitutes the need to memorise and recall text-based tokens (2005). A five-week online course was organised involving remote students from nine countries interacting with the learning and examination processes. The findings of the study showed an increase in the usability (see Table 12-3 items 3-4). The efficiency analysis showed a significant linear trend ($p < 0.01$) in the completion time of the challenge questions with an increase in the number of visits by the participants. The direction of the trend was negative, which showed that completion time decreased with an increasing number of visits. The mean correct answers to determine effectiveness of text-based questions was 66%, which increased to 74% using a relaxed algorithm to compensate for spelling mistakes and syntax variation. The mean correct answers to image-based questions were 85% (see Table 12-3 item 4). This showed that the use of image-based questions increased the effectiveness and that there was a significant difference in the mean correct answers between text-based and image-based questions ($p < 0.01$). The implementation of the multiple choice image-based questions addressed the usability issues reported with the text-based questions, which resulted in better effectiveness. The use of multiple choice options provided clues to the participants in order to recall the correct answers and they also addressed usability issues: capitalisation, spacing, spellings and syntax variation.

RQ 3c) How does the usability of dynamic profile questions influence the security of the challenge question approach in online examinations?

The fourth empirical study presented in Chapter 9 implemented dynamic profile questions and examined the usability attributes: efficiency and effectiveness. In order to implement these questions, a five-week online course was used, involving remote students from five countries interacting with the learning and examination processes. The findings of the study showed an increase in the usability (see Table 12-3 item 5). Unlike pre-defined text-based and image-based questions, which required students to register their answers, dynamic profile questions were created non-intrusively and non-distractively in the background, which resulted in better efficiency. Information was extracted from the students' learning activities, the content of submissions, grades, lessons and forum posts in order to build and consolidate his or her profile. These questions implemented five multiple options using correct and distraction choices. The mean correct answers during the authentication process were 99.5% (see Table 12-3 item 5). This was significantly different than both text-based and image-based questions ($p < 0.01$).

Online programme tutors are important stakeholders in the online learning and examinations process. The focus group study presented in Chapter 10 was organised with experienced online programme tutors to provide their views on different points for discussion, including the usability and applicability of the proposed challenge question approach. The participants of the focus group also provided their feedback on the usability of the proposed challenge question method (see Table 12-3 items 6-7). In response to the survey questions regarding the effectiveness of text-based, image-based and dynamic profile questions, the participants rated them as 3, 3.4, and 3.7 respectively (1 = not useful, 5 = very useful). There was a significant linear trend ($p < 0.01$) in their responses to questions associated with the usability of the three question types. Their feedback supported the findings of the empirical studies on effectiveness.

While usability is important, security is critical to maintain the confidentiality, integrity and availability of systems. A security analysis of the challenge question approach is presented in the following section.

RQ 4) How does the proposed authentication method influence security threats?

The risk-based assessment method described in Chapter 5 was adopted to evaluate the security of the proposed challenge question approach in order to answer the fourth and final research question. It is a quantitative method that provides rapid quantification of security level risks associated with processes (Ni et al., 2003). It focuses on the testing of features and functions of artefacts based on the risk of their failure (McGraw, 2004). Using this method, i) functions and features are identified; ii) threats and risks are identified; and iii) an abuse case scenario is created. Multiple abuse case scenarios were created to evaluate the collusion attacks of different types using text-based and dynamic profile questions in five studies presented in Chapters 6, 8, 9, 10 and 11.

Table 12-4 Evidence: Security Investigations

Items	Method	Section	Outcome
1.	Simulation	6.5.1	The guessing attack was not successful.
2.	Statistical Analysis	8.4.1	An increase in the number of shared questions increased the success of an impersonation attack.
3.	Statistical Analysis	8.4.3	There was a difference in the number of correct answers when answered from a printed source or memory.
4.	Statistical Analysis	8.4.2	An increase in the database size decreased the success of an impersonation attack.
5.	Simulation / Statis-	9.5.1	The findings of sharing using email

	tical Analysis		asynchronously showed that impersonator was not successful
6.	Simulation / Statistical Analysis	9.5.2	The findings of sharing using a phone in real time showed that the impersonator was successful
7.	Simulation / Statistical Analysis	9.5.3	The response time of students to dynamic profile questions was quicker “when there was no impersonation” compared to “when there was impersonation”
8.	Focus Group	10.4.2.1 10.4.2.2	The response time factor can be used for mitigation of impersonation when the challenge question approach is implemented
9.	Focus Group	10.4.2.2	Dynamic profile questions, a secure browser and remote proctoring can be used to mitigate collusion attacks
10.	Simulation / Statistical Analysis	11.4.2	The impersonation attack was not successful when dynamic profile questions were implemented in a proctored exam.

RQ 4a) How does the use of text-based questions influence collusion threats in online examinations?

Text-based challenge questions are associated with an individual’s personal information which can be vulnerable to blind, focused and informed guessing attacks by adversaries, acquaintances, friends and colleagues (Schechter et al., 2009, Just and Aspinall, 2009b). The study presented in Chapter 6 investigated the security of text-based challenge questions when a friend or colleague attempts to impersonate a student using a guessing attack. The findings of the study showed that the guessing may not succeed in a practical situation (see Table 12-4 item 1). The mean correct answers in a guessing abuse case scenario were 13% using an equality algorithm. This increased to 29% if a relaxed algorithm was implemented. In a practical situation, 71% incorrect answers would alert the course administrator and the guessing attack may not be successful. The difference in the number of correct answers using equality and relaxed algorithms showed usability and security trade-off.

Since text-based questions are associated with an individual's personal information, students may be able to share them with third parties for impersonation. The third empirical study presented in Chapter 8 investigated the influence of sharing different numbers of challenge questions for impersonation using varying database sizes. The study was simulated sharing different numbers of questions using three different databases of size 20, 30 and 50. The results showed that an increase in the number of shared questions increased the number of correct answers with a significant linear trend ($p < 0.01$) (see Table 12-4 item 2). In the simulation attack, the challenge questions were randomised; however, the impersonators were able to search and copy the correct answers from an electronic or printed source of the shared information. The mean correct answers decreased when the impersonators were required to memorise and answer the challenge questions. There was a significant difference in the mean correct answers when impersonators copied answers from printed information and memorised information ($p < 0.01$) (see Table 12-4 item 3). This implies that an impersonator can circumvent the text-based challenge questions irrespective of the size of the database, if an online examination is not monitored or the students are not restricted to answering their challenge questions in a limited time. Also, an increase in the database size decreased the success of an impersonation attack. A significant linear trend with a negative direction was found for all database sizes ($p < 0.01$) (see Table 12-4 item 4). This showed that the larger the database size, the less successful the impersonation attack. An increase in the database size also increased the randomisation of questions, the difficulty of memorising a large number of shared questions and answers, and the difficulty of searching for answers in a shared source.

The threat classification described in Chapter 5 identified impersonation as a serious threat. Students invited third parties to take their online tests for extra benefit. Rowe (2004) stated that individuals share credentials with impersonators, who take the online test on behalf of the intended test taker. Based on the findings of the study presented in Chapter 8, it was appropriate to mitigate the issue of credential (questions) sharing. To achieve this, a dynamic profile question method was proposed and implemented.

RQ 4b) How does the use of dynamic profile questions influence the collusion threats in online examinations?

The fourth empirical study presented in Chapter 9 used dynamic profile questions in a five-week online course. Students can make use of modern technology and share these questions using email asynchronously or with a mobile phone in real time. To evaluate the effect of these threats, the study investigated impersonation abuse case scenarios using email and mobile phones. The findings of impersonation using email showed that the impersonator was not successful. In this study, dynamic profile questions implemented five multiple choice options and the probability of a correct answer by chance would be 1/5th or 20%. In the impersonation using email, the impersonator answered 8% of challenge questions correctly (see Table 12-4 item 5). In a practical situation this may not be sufficient to impersonate a student. In the second abuse case scenario, when a student and an impersonator shared information using a mobile phone in real time, the impersonator answered 92% of challenge questions correctly (see Table 12-4 item 6). This is an increased number of correct answers and indicates that an impersonator can succeed if they communicate with a student in real time. There was a significant difference ($p < 0.01$) in the mean correct answers between an email and a mobile phone attack. However, there was a significant difference ($p < 0.01$) in the response time between a genuine student and a third party impersonator (see Table 12-4 item 7). This indicated that the response time factor can be used to discourage students from sharing their access credentials with impersonators in real time.

The focus group study described in Chapter 10 presented the feedback of online programme tutors. The majority of the participants recommended a response time factor for mitigation of real-time impersonation attacks ($M = 3.8$) (see Table 12-4 item 8). There was an agreement that dynamic profile questions can influence impersonation attacks ($M = 3.8$). However, they recommended proctoring or monitoring of the online examination process to mitigate abetting attacks (see Table 12-4 item 9). However, students may still attempt to circumvent the system by sharing login details and dynamic profile questions with an impersonator *before* an online examination session.

In order to evaluate the security of dynamic profile questions and live proctoring, an abuse case scenario was simulated in a real online course and a face-to-face laboratory-based session. The final empirical study presented in Chapter 11 investigated an impersonation attack, when a student shares their learning experience, access credentials and associated information with a third party impersonator *before* an online examination session. Students were paired at the beginning to share information with their partner for impersonation towards the end of the study. The participants were allowed to reveal their credentials and dynamic profile questions with their pairs face-to-face or through any convenient communication method. The findings of the study showed that impersonation was not successful in a proctored exam. In this study, dynamic profile questions implemented five multiple choice options and the probability of a correct answer by chance would be 1/5th or 20%. Impersonators answered 22% of the questions correctly in a proctored exam (see Table 12-4 item 10). In a practical situation, 78% incorrect answers would alert a proctor and it is unlikely that an impersonator would succeed.

To conclude, the use of dynamic profile questions, a secure browser and proctoring can influence impersonation and abetting attacks.

12.3 Summary of Contributions

This work is a continuation of previous research in the field of the authentication and identity verification of students in online examinations. The contributions of this research will add to the existing body of research. It provides an understanding of threats, usability, mitigation methods and the profile-based challenge question approach in the context of online examinations. This research has made the following contributions:

12.3.1 Understanding of Threats

Identifying potential threats may help us to understand what can go wrong if a threat occurs. Threats to online examinations have been identified in numerous research studies. The threats classification presented in this thesis provides a better understanding of weaknesses in a clear hierarchical structure. It has attempted to describe a distinction between intrusion and non-intrusion attacks. Threats in these two categories originate from different sources with varying motivations. Most importantly, there are different security approaches to provide different levels of deterrence against these threats. Intrusions are traditional threats to many web-based systems, including online learning and examinations. There are many security approaches to deter them; however, security approaches that mitigate intrusion attacks may not influence non-intrusion attacks.

Non-intrusion attacks are posed by genuine students, and they include collusion and non-collusion threats. Collusion is categorised on the basis of a person taking an online test, to distinguish between abetting and impersonation, which require different security approaches. A detail description of these threats was provided in Chapter 3.

The threat classification may help the experts, practitioners, tutors and educational institutions to align their security models in line with the potential threat model.

12.3.2 Usability Evaluation

Usability is essential in the design of authentication methods (Braz and Robert, 2006). These methods may fail to protect critical information if users are unable to use them correctly. This research approached usability in the context of authentication and online examination systems. Many research studies have previously examined the usability of the challenge question approach. This thesis added to the existing body of knowledge and contributed a usability investigation of text-based, image-based and dynamic profile-based challenge questions. The analysis was performed on the data collected from simulation and real online learning and examinations contexts. The results of the usability analysis revealed usability issues with text-based questions, such as ambiguity, syntax variation, and spelling mistakes. Image-based questions compensated for these issues and were more usable than text-based questions. Dynamic profile questions were the most usable of all question types, providing minimal distraction to students during the learning process.

12.3.3 Usability and Security Trade-off

A trade-off between security and usability has been an issue; both are important for the authentication process (Braz and Robert, 2006). The usability and security analysis of challenge questions also indicated a trade-off. The findings described in Chapter 6 showed that the use of a relaxed algorithm increased the effectiveness of questions compared to the equality algorithm. However, this had security implications in a guessing attack. The use of a relaxed algorithm increased the success of a guessing attack from 13% to 29%. Similarly, the usability of image-based and dynamic profile questions reported in Chapters 7 and 8 was significantly better than text-based questions. Besides other factors, one of the important reasons for increased usability was the implementation of multiple choice answers. However, this has security implications. The probability of a successful guess using multiple choice questions is $^{1}/_{n}$ (n = number of choices). Both image-based and dynamic profile-based questions implemented 5 multiple choice options and the probability of a successful guess was 1/5 or 20%.

The design of a usable and secure system is challenging when it comes to aligning these two competing and essential factors. This is more important in the context of online examinations and collusion, where a more usable system may be circumvented by a student and a third party impersonator. Designing challenge questions that are difficult to guess, may be less usable for users due to recall. Similarly, the use of strict security parameters may be less usable, such as the use of an equality algorithm. This adds to the existing knowledge, which may be useful for security and usability experts.

12.3.4 Security Evaluation

In studies involving security analysis it is logistically challenging to access the actual resource assets for research and evaluation. Empirical evaluation is a useful method to evaluate the security of artefacts. It has a fundamental role in scientific research to help us understand how and why things work (Perry et al., 2000). However, real-world empirical research in security design can be difficult logistically (Fléchais, 2005). Security experts responsible for a real-world system may not be willing to disclose their secret system security model and data for empirical evaluation.

While security has always been a challenge for researchers and practitioners, this thesis has attempted to answer questions associated with security issues. This work created both simulation and real online learning contexts to examine the identified security threats with a focus on collusion. Impersonation abuse case scenarios were simulated involving students. Online programme tutors were invited for their feedback on the research problems and the proposed solutions. Impersonation abuse case scenarios were organised with remote online students as well as in face-to-face laboratory sessions. The results showed that dynamic profile questions can influence impersonation attacks. The use of a secure browser and proctoring can impact abetting attacks. This contribution may be useful for educational institutions, students, tutors, practitioners and the security experts.

12.3.5 Profile-based Challenge Question Authentication

The existing authentication provides adequate security to deter intrusion attacks in online examinations. However, it is essential to address collusion attacks. The work in this thesis contributed knowledge and the practical application of using a profile-based challenge question method. This method has a practical advantage over the use of conventional authentication methods in remote online settings, where students can use it in varying time zones and dispersed geographical locations. The integration of learning and examination processes provides an additional factor to influence security threats.

12.3.6 Dynamic Profile Questions

One of the key security challenges of online examinations is to ensure that the person taking an online test is the same who completed the learning. The majority of existing methods rely upon a code of honour and the assumption that a genuine student is taking the test. However, research studies discussed in Chapter 3 indicated that impersonation is on the rise.

It is important that the use of technology does not interrupt or distract a student from learning. Thus, the dynamic profile question approach was designed. This is a more adaptable method, as it creates a student's profile based on his/her learning activities and content submissions. Unlike text-based and image-based questions, dynamic profile questions are created non-intrusively in the background when a student performs his/her course work. These questions are based on students' learning activities e.g. assignments, submissions, lessons, forum interactions, forum postings, reflections, grades, quizzes and interaction with other learning resources. They are not aware of which questions will be asked for authentication. This approach implements multiple choice answers and students are required to recognise a correct answer from the given choices, which results in increased usability compared to the traditional text-based questions. Results from the experiments presented in Chapters 9, 10 and 11 showed that the use of dynamic profile questions increased the relevant usability attributes and influenced the success of impersonation attacks.

12.4 Discussion

Collusion is one of the key challenges to online examinations today. Approaching this problem, providing an understanding of the influence of such attacks on online examinations, discussing the problems and motivating factors, and the proposed solutions are important. Evaluating the solution involving students and tutors in research studies contributes to key areas in security and usability in the online examinations context.

This research provided a detailed understanding of the threats to online examinations. In response to these threats a profile-based challenge question authentication method was designed. The usability findings of the three different question types showed that dynamic profile questions were more usable. The security analysis provided an increased understanding of security issues and countermeasures. It showed that the use of these questions provides an additional security factor. To circumvent the proposed method, a student was required to share dynamic profile questions with an impersonator in an impersonation attack. The successful attack was reliant upon the number of questions shared. Unlike text-based and image-based questions, dynamic profile questions were created in the background and asynchronous sharing of these questions with third party impersonators was not successful. Also, sharing of these questions in real time may be difficult if the user response is timed.

The findings of this research will benefit tutors, students and research communities. In the focus group session, online programme tutors provided positive feedback, highlighting the important security threats including collusion and investigating potential countermeasures. The use of a secure learning environment may help with organising a fair learning and examination process. The research findings will help the research community by promoting further work on providing a usable and secure environment in order to improve the online learning experience.

This research work has a potential social impact described below:

- *Cost Effective*: Due to increasing cost of traditional universities, online courses have become increasingly attractive for learners (Christensen and Eyring, 2011). The use of online learning and examinations reduces the cost of travelling, infrastructure, and resources. Students can learn on demand from any location in their own time. This research work investigated a knowledge-based approach, which is likely to be cost effective compared to biometrics and object-based approaches.

- *Accessibility*: The rapid growth and expansion of the Internet and technology increased the use of online learning and examinations internationally. This also appealed to those learners who are unable to access traditional education. This mode of teaching and learning offers more convenient access to all students including people with limited access. This research contributed a knowledge-based method to reduce the accessibility challenges.

- *Academic institutions*: As described in chapter 3, security of online examinations has been a common issue for academic institutions. There are a number of open-ended threats to such exams. Collusion is identified as a major concern for stake holders including academic institution (McGee, 2013). This research work highlighted those concerns and investigated potential threats in more detail. This work investigated and proposed potential solutions to mitigate these threats in order to enhance the creditability of online learning and examinations, which will enhance the trust of academic institutions.

- *Availability*: The learners are able to access the online resource at any time that suit them due to availability on the Internet (Arkorful and Abaidoo, 2015). Online learning environments can be accessed from dispersed geographical locations, which enables the access of less privileged communities' to education. This research helps the use of secure and usable approaches to such environments.

This work contributed to the literature, which may help researchers who wish to further investigate the evolving threats to online examinations and propose countermeasures.

12.5 Future Work

This research concluded that the use of dynamic profile questions and remote proctoring may positively influence security threats including collusion attacks. Suggestions to extend this work and its application in other contexts are described in the following sections.

12.5.1 Empirical Evaluation of Secure Browser and Proctoring

The current research proposed dynamic profile questions, a secure browser and a proctoring approach to deter impersonation and abetting in online examinations. The challenge question method was evaluated in multiple empirical studies. The secure browsing and remote proctoring method was simulated using a laboratory-based experiment with a small group of students. Future work is warranted to investigate this in a real scenario using a larger sample size.

Remote proctoring could be an expensive option when implemented for a large number of students. According to Eisenberg (2013), the cost of remote proctoring per student is $60 to $90. Eisenberg states that trained proctors at computers can monitor faraway students via webcams. A multi-student proctoring method may potentially reduce the cost of monitoring online tests. Using this method, a proctor will schedule online tests with multiple students simultaneously.

There is a potential for designing an automated proctoring method for use with dynamic profile questions. Using this method, a student will attend a scheduled online examination session which is recorded remotely using a web cam. A special purpose system will implement a secure browser, dynamic profile questions, and record the exam session. Furthermore, the use of a 360° web cam will further enhance the security of online examinations to mitigate abetting attacks.

12.5.2 Continuous Authentication

User authentication is often performed as a one-off process during the initial interaction with a system. However, one time validation of users' is becoming insufficient. Using continuous authentication, a user is required to validate their identity continuously. This type of authentication is often implemented by smartphones (Xu et al., 2014). Some studies (Moini and Madni, 2009, Flior and Kowalski, 2010, Monaco et al., 2013) suggest the use of continuous authentication in online examinations. These studies proposed biometrics such as face-recognition and keystroke analysis.

The current research evaluated the use of challenge question approach as a single sign on authentication method to access online examinations. This implies that once a student is in, someone else can take over and complete the online test. To mitigate such threats, a continuous authentication is necessary. A user will be asked to answer challenge questions in order to access examinations and intermittently during the exam session. This will enhance the security. However, this will create usability issues and increase interruptions.

Further research is necessary in the future to implement continuous authentication using the challenge question approach, in order to understand its impact on usability and security.

12.5.3 Implementation as an Assessment Component

Assessment is a core component of teaching and learning. With the development of learning techniques, assessment or examination has also evolved and become an integral part of many learning environments (Joosten-ten Brinke et al., 2007). According to Hargreaves (2008), assessment measures students' learning at the end of an instructional unit, end of a course, or after some defined period. Challis (2005) states that it aims to ascertain that the desired learning goals have been met or certifying that the required levels of competence have been achieved. In general, summative assessment includes scoring for the purposes of awarding a grade or other forms of accreditation. Online assessment has reconceptualised the pedagogy in order to achieve the assessment goals effectively. In their study, Gikandi et al. (2011) recommended the integration of teaching and learning in order to support learners to develop deep knowledge and understanding. This can be implemented using the course and assessment design.

The proposed challenge questions approach may support the integration of learning and examinations. The profile-based authentication method implements dynamic profile questions, which collects information about students' learning activities to build their profile. The profile represents a student's learning description, built and consolidated over a period of time. This information could potentially be implemented as an assessment component. Furthermore, a student's learning profile could be reconciled with the outcomes of assessment activities, in order to verify that a genuine student has undertaken the learning and examination activities. Further work is needed to investigate the use of dynamic profile questions as an assessment component with the outcomes recorded in the gradebook.

12.5.4 Research Impact on Other Applications

The profile-based challenge questions could be implemented in many traditional web-based applications for the deterrence of attacks:

- **Online Banking:** Banking is a fast growing business, which utilizes the Internet for marketing and delivery of services. Rapid growth and advances in information technology have increased user acceptance of technology driven methods of handing daily banking affairs (Pikkarainen et al., 2004). One such method is online banking. Many banks offer a wide range of retail services over the Internet. Beside the anticipated benefits, these banks are a target of many security threats. According to Aladwani (2001), authentication is one of the key security features to deter these threats.

  Many banks implement strong password authentication. However, users tend to forget strong passwords. To address this, banks couple strong passwords with challenge questions. The use of challenge questions in online banking has been identified in many research studies recently. Rabkin (2008) investigated 15 online banks using challenge questions, which were implemented for customer verification. Rabkin identified that answers to roughly 12% of the challenge questions were available on social media websites. The stakes for the users of online banking are higher than students in online examination environments. The traditional challenge questions approach, which utilizes pre-defined text-based questions, is prone to many threats. In his study, Smyth (2010) identified security vulnerabilities in the text-based questions used by Bank of Scotland and Halifax, Natwest, and Royal Bank of Scotland and Ulster. Smyth revealed that information required for an adversary to commit fraud in these banks, may likely be available in public domain.

The dynamic profile questions could be implemented to build and consolidate a customer's profile during their interactions with an online bank account. Information in the profile will be used for authentication in many ways e.g. when the customer requests a transfer of funds through online banking, a customer requests to retrieve password etc. For example, "which of the following transaction was made by you in the last two weeks?" This will likely increase the security. As discussed earlier, using the conventional text-based questions, adversaries can learn, guess or retrieve answers from different sources (Rabkin, 2008). However, the dynamic profile questions are associated with individual's activities, transactions and profile which may likely be known to the genuine customer. This will address the issues related with the text-based challenge questions. More work is warranted to investigate this in the future.

- **Email Service Providers:** Challenge questions became a popular fall back authentication method when used by leading email providers such as Yahoo, Google, Microsoft and AOL (Schechter et al., 2009). These service providers use it for authentication when a user needs to reset or retrieve lost credentials. It is identified as a cost-effective method, which minimises the administration cost when a user needs to recover his/her lost credentials (Just, 2004). However, some studies have reported usability and security issues associated with this method. Just and Aspinall (2009a) reported usability issues with the challenge questions. They stated that, of the 117 questions asked in their study, 88 (75%) answers were recalled exactly, while 21 (18%) had different punctuation/capitalisation (typically performed when registering answers). 8 (7%) of the answers were completely different, citing a memorability issue in a span of 28 days. In the security evaluation, participants believed that 88% of the questions would be "somewhat difficult" for a stranger to answer; however, this reduced to 46% when considering the case of a friend or family member. To address the memorability, Renaud and Just (2010) proposed associative picture-based cues with multiple choice answers. The authors of the study reported a 13% increase in memorability. Schechter et al. (2009) evaluated the security of challenge questions used by four mail service providers – Google, Yahoo, AOL and Microsoft. The authors of the study reported that acquaintances of participants were able to guess 10% of their answers and 13% of answers could be guessed within five attempts. The authors state that participants forgot 20% of their own answers within six months. Rabkin (2008) discovered that a significant number of questions were either insecure or difficult when he analysed administratively chosen challenge questions. Schechter et al. (2009) reference Sarah Palin (the Republican vice-presidential candidate in the 2008 US election), whose Yahoo email account was compromised, as the answer to her secret question had been figured out (Bridis, 2008).

The use of dynamic profile questions approach will potentially address the usability and security issues reported in the above studies. The usability findings reported in chapters 9 and 11 showed 95% and 99% effectiveness. Using the approach a user profile is built in background during interactions with emails e.g. “which of the following email subject was sent by you?” As identified in the online examination context, the usability and security of the dynamic profile questions improved significantly compared to conventional text-based questions. However, further work is needed to investigate this in an “email service” experimental or real context.

- **Social Media:** The use of social media websites has been growing fast. For example Facebook is a famous social media site that has 1.59 billion users as of September, 2015 (Kohen, 2016). Similarly, Instagram has 400 million, Twitter 300 million and Google+ 300 million active users. With the large number of users, the security of these websites is critical as it stores personal information for millions of users. Passwords are the most widely used method for authentication of users in the majority web applications including social media (Hafiz et al., 2008). However, when users forget passwords, fall back authentication are used to help users regain access. A commonly used method for fall back authentication is the email-based password reset. When a user requests a new password, a reset link is sent to the user’s email address. This approach is reported with issues such as single point of failure, out of date email address, and email interception (Garfinkel, 2003). The challenge question is another popular fall back method by social media websites. Given the security and usability issues with the use of text-based challenge questions, Hang (2015) proposed location based security questions. These questions utilize personal information and associate it with a location e.g. “where did you first meet your girlfriend?” Users are asked to pick up a location on a map to answer the question. The study reported issues such as answer precision, and answer distance issues.

The dynamic profile-based challenge question approach could be used to build a user’s profile during day to day interactions with a social media website e.g. Facebook, Twitter or Instagram. The profile information will be used to authenticate users when a password change is requested. For example, “which of the following comments did you like?” or “which of the following message did you post on your timeline?” This will potentially increase the security and mitigate adversary attacks. Further work is needed to investigate the security and usability impact of this approach.

REFERENCES

Ackerman, C. D. & White, J. T. (2008). A descriptive study of the ethical practices of students in both traditional and online environments at a university in Missouri. In *Journal of Legal, Ethical and Regulatory Issues,* 11**,** 109.

Adams, A. & Sasse, M. A. (1999). Users are not the enemy. In *Communications of the ACM,* 42**,** 40-46.

Adelman, C. (2000). A parallel universe: Certification in the information technology guild. In *Change: The Magazine of Higher Learning,* 32**,** 20-29.

Agency, Q. A. (2006). Code of practice for the assurance of academic quality and standards in higher education. *Assessment of students (Second edition).*

Aggarwal, R., Bates, I., Davies, G. & Khan, I. (2002). A study of academic dishonesty among students at two pharmacy schools. In *Pharmaceutical journal,* 269**,** 529-533.

Agulla, E. G., Rifón, L. A., Castro, J. L. A. & Mateo, C. G. (2008). Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments. In: *Eighth IEEE International Conference on Advanced Learning Technologies*, 2008. IEEE, 551-553.

Al-Ajlan, A. & Zedan, H. (2007). E-learning (Moodle) based on service oriented architecture. In: *Proceedings of the EADTU's 20th Anniversary Conference, Lisbon, Portugal*, 2007. 62-70.

Aladwani, A. M. (2001). Online banking: a field study of drivers, development challenges, and expectations. In *International Journal of Information Management,* 21**,** 213-225.

Allen, I. E. & Seaman, J. (2007). Online Nation. In *Five Years of Growth in Online learning. Needham, Mass.: Sloan Consortium*.

Alwi, N. H. M. & Fan, I. S. (2010). Threats analysis for e-learning. In *International Journal of Technology Enhanced Learning,* 2**,** 358-371.

Analysts, G. I. (2012). e-Learning A Global Strategic Business Report.

Anderson, R. J. (2010). *Security Engineering: A guide to building dependable distributed systems,* New York, Wiley Computer Publishing.

Apampa, K. M., Wills, G. & Argles, D. (2009). Towards security goals in summative e-assessment security. In: *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 2009. IEEE, 1-5.

Apampa, K. M., Wills, G. & Argles, D. (2010a). An approach to presence verification in summative e-assessment security. In: *International Conference on Information Society (i-Society 2010)*, 2010a. IEEE, 647-651.

Apampa, K. M., Wills, G. & Argles, D. (2010b). User security issues in summative e-assessment security. In *International Journal of Digital Society (IJDS),* 1**,** 1-13.

Arkorful, V. & Abaidoo, N. (2015). The role of e-learning, advantages and disadvantages of its adoption in higher education. In *International Journal of Instructional Technology and Distance Learning,* 12**,** 29-42.

Asha, S. & Chellappan, C. (2008). Authentication of e-learners using multimodal biometric technology. In: *International Symposium on Biometrics and Security Technologies* 2008. IEEE, 1-6.

Ayodele, T., Shoniregun, C. & Akmayeva, G. (2011). Towards e-learning security: A machine learning approach. In: *Information Society (i-Society), 2011 International Conference on*, 2011. IEEE, 490-492.

Babic, A., Xiong, H., Yao, D. & Iftode, L. (2009). Building robust authentication systems with activity-based personal questions. In: *Proceedings of the 2nd ACM workshop on Assurable and usable security configuration*, 2009. ACM, 19-24.

Bach, J. (2003). Exploratory testing explained. In *Online: http://www. satisfice. com/articles/et-article. pdf.*

Bailie, J. L. & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online users. In *Bulletin-board postings,* 547**,** 17.

Bangor, A., Kortum, P. & Miller, J. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. In *Journal of usability studies,* 4**,** 114-123.

Barbour, A. (2014). The 10 most inventive cheating attempts on online exams. p.30/12/2015.

Barik, N. & Karforma, S. (2012). Risks and remedies in e-learning system. In *arXiv preprint arXiv:1205.2711*.

Barker, T. & Lee, S. (2007). The verification of identity in online assessment: A comparison of methods. In: *Proceedings of 11th CAA International Computer Assisted Conference*, 2007.

Barker, T., Lee, S. & Hewitt, J. (2007). The development and testing of a video system for online authentication of assessment. *Second International Blended Learning Conference.*

Benson, A. D. (2002). Using Online Learning To Meet Workforce Demand: A Case Study of Stakeholder Influence. In *Quarterly Review of Distance Education,* 3**,** 443-52.

Berelson, B. (1952). *Content analysis in communication research,* Glencoe, IL, Free Press.

Berg, B. L. & Lune, H. (2004). *Qualitative research methods for the social sciences*, Pearson Boston, MA.

Bevan, N. (1995). Usability is quality of use. In *Advances in Human Factors/Ergonomics,* 20**,** 349-354.

Beyer, H. & Holtzblatt, K. (1997). *Contextual Design: A Customer-Centered Approach to Systems Designs (Morgan Kaufmann Series in Interactive Technologies)*, Morgan Kaufmann.

Birenbaum, M. (1996). Assessment 2000: Towards a pluralistic approach to assessment. In *Alternatives in assessment of achievements, learning processes and prior knowledge***,** 3-29.

Bonneau, J., Just, M. & Matthews, G. (2010). What's in a Name? In: Sion, R. (ed.) Financial Cryptography and Data Security.FC 2010 Lecture Notes in Computer Science. vol. 5628. (98-113): Springer, Berlin, Heidelberg.

Boostmygrade. (2016). *Boost my grade* [Online]. Available: www.boostmygrade.com [Accessed 30/3/2016 2016].

Bowers, W. J. (1964). *Student dishonesty and its control in college,* New York, Bureau of Applied Social Research, Columbia University.

Braz, C. & Robert, J.-M. (2006). Security and usability: the case of the user authentication methods. In: *Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine*, 2006. ACM, 199-203.

Bridis, T. (2008). Hacker impersonated Palin, stole e-mail password, Sept. 18, 2008. *The Huffington Post*.

Brown, K. D. & Chatelain, D. (2007). *Pin-secyred dynamic magnetic stripe payment card*. U.S patent application 11/676,285.

Bruce, K. M. (2007). Tips for Avoiding Bad Authentication Challenge Questions. Security Professional Services, Inc.

Bunn, D. N., Caudill, S. B. & Gropper, D. M. (1992). Crime in the classroom: An economic analysis of undergraduate student cheating behavior. In *The Journal of Economic Education,* 23**,** 197-207.

Burgoon, J. K., Stoner, G. M., Bonito, J. & Dunbar, N. E. (2003). Trust and deception in mediated communication. In: *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, 2003 Hawaii, USA. IEEE, 44-56.

Burr, W. E., Dodson, D. F. & Polk, W. T. (2006). Electronic Authentication Guidelines. *Information Security* [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

Bushway, A. & Nash, W. R. (1977). School cheating behavior. In *Review of Educational Research*, 623-632.

Buzzetto-More, N. (2008). Student perceptions of various e-learning components. In *Interdisciplinary Journal of E-Learning and Learning Objects,* 4**,** 113-135.

Cardiff, U. (2007). *Diploma in Practical Dermatology Examination* [Online]. Cardiff: Cardiff University. Available: http://www.dermatology.org.uk/courses/dpd/dpd-overview.html [Accessed 03/07/2011 2011].

Carliner, S. (2004). *An overview of online learning,* Armherst, MA, Human Resource Development.

Carter, J., Ala-Mutka, K., Fuller, U., Dick, M., English, J., Fone, W. & Sheard, J. (2003). How shall we assess this? In: *ACM SIGCSE Bulletin*, 2003. ACM, 107-123.

Challis, D. (2005). Committing to quality learning through adaptive online assessment. In *Assessment & Evaluation in Higher Education,* 30**,** 519-527.

Chan, Y. Y., Leung, C. H. & Liu, J. K. (2003). Evaluation on Security and Privacy of Web-Based Learning Systems. In: *The 3rd IEEE International Conference on Advanced Learning Technologies*, 2003.

Chen, Y. & Liginlal, D. (2008). A maximum entropy approach to feature selection in knowledge-based authentication. In *Decision Support Systems,* 46**,** 388-398.

Chiasson, S., Van Oorschot, P. C. & Biddle, R. (2007). Graphical password authentication using cued click points. In: Biskup, J. & López, J. (eds.) Computer Security – ESORICS 2007. ESORICS 2007. Lecture Notes in Computer Science,. vol. 4734. (359-374): Springer, Berlin, Heidelberg.

Chiesel, N. (2009). Pragmatic methods to reduce dishonesty in web-based courses. In *A. Orellana***,** 327-399.

Christensen, C. M. & Eyring, H. J. (2011). *The innovative university: Changing the DNA of higher education from the inside out*, John Wiley & Sons.

Christie, B. (2003). Designing Online Courses to Discourage Dishonesty: Incorporate a Multilayered Approach to Promote Honest Student Learning. In *Educause Quarterly,* 11**,** 54-58.

Christodorescu, M., Jha, S., Seshia, S. A., Song, D. & Bryant, R. E. (2005). Semantics-aware malware detection. In: *Security and Privacy, 2005 IEEE Symposium on*, 2005. IEEE, 32-46.

Chun-Li, L., Hung-Min, S. & Hwang, T. (2001). Attacks and solutions on strong-password authentication. In *IEICE transactions on communications,* 84**,** 2622-2627.

Chun, M. M. & Jiang, Y. (1998). Contextual cueing: Implicit learning and memory of visual context guides spatial attention. In *Cognitive psychology,* 36**,** 28-71.

Church, K. & De Oliveira, R. (2013). What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS. In: *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, 2013. ACM, 352-361.

Cohen, L., Manion, L. & Morrison, K. (2013). *Research methods in education*, Routledge Taylor and Francis Group.

Colwell, J. L. & Jenks, C. F. (2005). Student Ethics in Online Courses. In: *35th Annual Conference Frontiers in Education (FIE '05)* 2005 IN, USA. IEEE, T2D-17-T2D-19.

Commission, I. O. F. S. I. E. (2005). ISO/IEC 27001: Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO Copyright Office: Geneva, Switzerland.

Conole, G. & Oliver, M. (2006). *Contemporary perspectives in e-learning research: themes, methods and impact on practice,* Abingdon, Routledge Taylor and Fracis Group.

Constantine, L. L. & Lockwood, L. A. (1999). *Software for use: a practical guide to the models and methods of usage-centered design*, Pearson Education.

Cordes, C. S. (2005). Monsters in the closet: Spyware awareness and prevention. In *Educause Quarterly,* 28**,** 53-56.

Corry, M. D., Frick, T. W. & Hansen, L. (1997). User-centered design and usability testing of a web site: An illustrative case study. In *Educational Technology Research and Development,* 45**,** 65-76.

Cranor, L. F. & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use,* Sebastopol, CA, O'Reilly Media.

Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches,* Thousand Oaks, CA, Sage Publications.

Creswell, J. W. & Clark, V. L. P. (2007). *Designing and conducting mixed methods research*, SAGE Publications.

De Angeli, A., Coventry, L., Johnson, G. & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. In *International journal of human-computer studies,* 63**,** 128-152.

Dee, T. S. & Jacob, B. A. (2012). Rational ignorance in education: A field experiment in student plagiarism. In *Journal of Human Resources,* 47**,** 397-434.

Deo, V., Seidensticker, R. B. & Simon, D. R. (1998). *Authentication system and method for smart card transactions*. US patent application.

Derakhshani, R., Schuckers, S. a. C., Hornak, L. A. & O'gorman, L. (2003). Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. In *Pattern Recognition,* 36**,** 383-396.

Di Raimondo, M. & Gennaro, R. (2005). New approaches for deniable authentication. In: *Proceedings of the 12th ACM conference on Computer and communications security*, 2005. ACM, 112-121.

Dick, M., Sheard, J., Bareiss, C., Carter, J., Joyce, D., Harding, T. & Laxer, C. (2002). Addressing student cheating: definitions and solutions. In: *ITiCSE-WGR '02 Working group reports from ITiCSE on Innovation and technology in computer science education*, 2002. ACM, 172-184.

Dietz-Uhler, B. & Hurn, J. (2011). Academic dishonesty in online courses. In: *44th Annual Conference June 12-16, 2011*, 2011. 71.

Dougiamas, M. (2012). *MOODLE Statistics* [Online]. Moodle. Available: https://moodle.org/stats [Accessed 28/12/2012 2012].

Dougiamas, M. & Taylor, P. (2003). Moodle: Using learning communities to create an open source course management system. In: *World conference on educational multimedia, hypermedia and telecommunications*, 2003. 171-178.

Dumas, J. S. & Redish, J. (1999). *A practical guide to usability testing,* Portland, OR, Intellect Books.

Dustin, E., Rashka, J. & Mcdiarmid, D. (2002). *Quality web systems: performance, security, and usability*, Addison-Wesley Longman Publishing Co., Inc.

Eason, K. D. (2005). *Information technology and organisational change*, CRC Press.

Eisenberg, A. (2013). Keeping an eye on online test-takers. *New York Times*.

Eshet-Alkalai, Y. & Geri, N. (2007). Does the medium affect the message? The influence of text representation format on critical thinking. In *Human Systems Management,* 26**,** 269.

Evans, E. D. & Craig, D. (1990). Teacher and student perceptions of academic cheating in middle and senior high schools. In *The Journal of Educational Research,* 84**,** 44-53.

Faily, S. (2011). *A framework for usable and secure system design.* University of Oxford.

Faucher, D. & Caves, S. (2009). Academic dishonesty: Innovative cheating techniques and the detection and prevention of them. In *Teaching and Learning in Nursing,* 4**,** 37-41.

Fléchais, I. (2005). *Thesis:Designing Secure and Usable Systems.* Doctor of Philosphy, University College London.

Flior, E. & Kowalski, K. (2010). Continuous biometric user authentication in online examinations. In: *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, 2010. IEEE, 488-492.

Florencio, D. & Herley, C. (2007). A large-scale study of web password habits. In: *Proceedings of the 16th international conference on World Wide Web*, 2007. ACM, 657-666.

Frank, A. J. (2010). Dependable distributed testing: Can the online proctor be reliably computerized? In: *e-Business (ICE-B), Proceedings of the 2010 International Conference on*, 2010. IEEE, 1-10.

Furnell, S. M., Dowland, P., Illingworth, H. & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. In *Computers & Security,* 19**,** 529-539.

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. In *European Journal of Information Systems,* 3**,** 112-126.

Gamboa, H. & Fred, A. (2004). A behavioral biometric system based on human-computer interaction. In: *Defense and Security*, 2004. International Society for Optics and Photonics, 381-392.

Garfinkel, S. L. (2003). Email-based identification and authentication: An alternative to PKI? In *IEEE security & privacy,* 99**,** 20-26.

Gaytan, J. & Mcewen, B. C. (2007). Effective online instructional and assessment strategies. In *The American Journal of Distance Education,* 21**,** 117-132.

George, J. F. & Carlson, J. R. (1999). Group support systems and deceptive communication. In: *Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on*, 1999. IEEE, 10 pp.

Gerrard, P. & Thompson, N. (2002). *Risk-based e-business testing*, Artech House Publishers.

Gibbs, A. (1997). Focus groups. In *Social research update,* 19**,** 1-8.

Gikandi, J. W., Morrow, D. & Davis, N. E. (2011). Online formative assessment in higher education: A review of the literature. In *Computers & Education,* 57**,** 2333-2351.

Gil, C., Castro, M. & Wyne, M. (2010). Identification in web evaluation in learning management system by fingerprint identification system. In: *Frontiers in Education Conference (FIE)*, 2010 Washington DC, USA. IEEE, T4D-1-T4D-6.

Gilmore, J., Strickland, D., Timmerman, B., Maher, M. & Feldon, D. (2010). Weeds in the flower garden: An exploration of plagiarism in graduate students' research proposals and its connection to enculturation, ESL, and contextual factors. In *International Journal for Educational Integrity,* 6.

Gollmann, D. (2010). Computer security. In *Wiley Interdisciplinary Reviews: Computational Statistics,* 2**,** 544-554.

Goss, J. D. & Leinbach, T. R. (1996). Focus groups as alternative research practice: experience with transmigrants in Indonesia. In *Area***,** 115-123.

Gould, J. D. & Lewis, C. (1985). Designing for usability: key principles and what designers think. In *Communications of the ACM,* 28**,** 300-311.

Griffith, V. & Jakobsson, M. (2005). Messin'with Texas Deriving Mother's Maiden Names Using Public Records. In: Ioannidis, J., Keromytis, A. & Yung, M. (eds.) Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science,. vol. 3531. (91-103): Springer, Berlin, Heidelberg.

Grijalva, T. C. (2006). *Academic honesty and online courses.* Department of Economics, Weber State University.

Hafiz, M. D., Abdullah, A. H., Ithnin, N. & Mammi, H. K. (2008). Towards identifying usability and security features of graphical password in knowledge based authentication technique. In: *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, 2008. IEEE, 396-403.

Haga, W. J. & Zviran, M. (1991). Question-and-answer passwords: an empirical evaluation. In *Information systems,* 16**,** 335-343.

Haley, C. B., Laney, R. C. & Nuseibeh, B. (2004). Deriving security requirements from crosscutting threat descriptions. In: *Proceedings of the 3rd international conference on Aspect-oriented software development*, 2004. ACM, 112-121.

Hang, A., De Luca, A., Smith, M., Richter, M. & Hussmann, H. (2015). Where have you been? using location-based security questions for fallback authentication. In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015. USENIX Association, 169-183.

Hansson, S. O. (2010). Risk: objective or subjective, facts or values. In *Journal of Risk Research,* 13**,** 231-238.

Harasim, L. (2000). Shift happens: Online education as a new paradigm in learning. In *The Internet and Higher Education,* 3**,** 41-61.

Hargreaves, E. (2008). *The Routledge international encyclopedia of education,* New York, Routledge.

Harmon, O. R., Lambrinos, J. & Buffolino, J. (2010). Assessment design and cheating risk in online instruction. In *Online Journal of Distance Learning Administration,* 13.

Hayashi, E., Hong, J. & Christin, N. (2011). Security through a different kind of obscurity: Evaluating Distortion in Graphical Authentication Schemes. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011. ACM, 2055-2064.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. In: *Proceedings of the 2009 workshop on New security paradigms workshop*, 2009. ACM, 133-144.

Hernandez, J., Andaverde, J. & Burlak, G. (2008). Biometrics in online assessments: A study case in high school students. In: *Electronics, Communications and Computers, 2008. CONIELECOMP 2008, 18th International Conference on*, 2008. IEEE, 111-116.

Heussner., K. M. (2012). 5 ways online education can keep its students honest. *GIGAM Research* [Online]. Available: https://gigaom.com/2012/11/17/5-ways-online-education-can-keep-its-students-honest/ [Accessed 30/12/2015].

Heyneman, S. (2015). The corruption of ethics in higher education. In *International Higher Education*.

Hill, C. (2010). Student Authentication:What Are Your Duties Under the HEA Reauthorization. In *Madison, Wisconsin, US: Magna Publications, Inc. Retrieved December,* 18**,** 10-11.

Hix, D. & Hartson, H. R. (1993). *Developing user interfaces: ensuring usability through product & process*, John Wiley & Sons, Inc.

Howell, S., Sorenson, D. & Tippets, H. (2010). The news about cheating for distance educators. *Faculty Focus Specialty Report* [Online]. Available: http://www.facultyfocus.com/wp-content/uploads/images/promoting-academic-integrity-in-online-edu1.pdf.

Hugerat, M., Odeh, S., Saker, S. & Agbaria, A. (2013). Vulnerabilities and Attacks on Information Systems in E-learning Environments in Higher Education. In *A US-China Education Review,* 3**,** 615-622.

Huiping, J. (2010). Strong password authentication protocols. In: *4th International Conference on Distance Learning and Education (ICDLE)*, 2010 San Juan, Puerto Rico. IEEE, 50-52.

Insight's, A. (2012). Learning Technology Research Taxonomy. *Research methodology, buyer segmentation, product definitions, and licensing model.* Monroe, WA.

Iso9241-11 (1998). Ergonomic Requirements for Office Work with Visual Dispaly Terminals, Part 11: Guidance on Usability. *ISO 9241-11.* Geneva.

Iso/Iec Tr 13335-1 (1996). Information technology Guidelines for the management of IT Security *Part 1: concepts and models for IT Security.* 1st ed.: Switzerland.

Jacko, J. A. (2012). Designing for user interface plasticity. Human Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications. vol. (1107-1125): CRC press.

Jokela, T., Iivari, N., Matero, J. & Karukka, M. (2003). The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11. In: *Proceedings of the Latin American conference on Human-computer interaction*, 2003. ACM, 53-60.

Jones, R. L. & Rastogi, A. (2004). Secure coding: building security into the software development life cycle. In *Information Systems Security,* 13**,** 29-39.

Joosten-Ten Brinke, D., Van Bruggen, J., Hermans, H., Burgers, J., Giesbers, B., Koper, R. & Latour, I. (2007). Modeling assessment for re-use of traditional and new types of assessment. In *Computers in Human Behavior,* 23**,** 2721-2741.

Jortberg, M. A. (2009). *Methods to verify the identity of distance learning students* [Online]. Acxiom. Available: http://u.cs.biu.ac.il/~ariel/download/de666/resources/dependable_distributed_testing/verify_students.pdf [Accessed 01/04/2011 2011].

Jung, C., Han, I. & Suh, B. (1999). Risk analysis for electronic commerce using case-based reasoning. In *International Journal of Intelligent Systems in Accounting, Finance & Management,* 8**,** 61-73.

Jung, I. Y. & Yeom, H. Y. (2009). Enhanced security for online exams using group cryptography. In *IEEE Transactions on Education,* 52**,** 340-349.

Just, M. (2003). Designing Secure Yet Usable Credential Recovery Systems with Challenge Questions. In: *CHI 2003 Workshop on Human-Computer Interaction and Security Systems*, 2003. Florada, USA: Citeseer, 1-6.

Just, M. (2004). Designing and evaluating challenge-question systems. In *Security & Privacy, IEEE,* 2**,** 32-39.

Just, M. (2005). Designing authentication systems with challenge questions. In *Security and Usability: Designing Secure Systems That People Can Use***,** 143-155.

Just, M. & Aspinall, D. (2009a). Challenging challenge questions. In: *Socio-Economic Strand*, 2009a. Oxford University UK, 6–8.

Just, M. & Aspinall, D. (2009b). Choosing Better Challenge Questions. In: *Symposium on Usable Privacy and Security (SOUPS)*, 2009b CA, USA. ACM.

Just, M. & Aspinall, D. (2009c). Personal choice and challenge questions: a security and usability assessment. In: *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009c CA,USA. ACM, 8.

Just, M. & Aspinall, D. (2012). On the security and usability of dual credential authentication in UK online banking. In: *Internet Technology And Secured Transactions, 2012 International Conferece For*, 2012. IEEE, 259-264.

Karvonen, K. (1999). Creating trust. In: *In Proceedings of the Fourth Nordic Workshop on Secure IT Systems*, 1999. Citeseer, 21–36.

Kearsley, G. & Moore, M. (2005). *A System View,* Belmount, CA.

Kerka, S. & Wonacott, M. E. (2000). Assessing Learners Online. Practitioner File. *ERIC Cleaninghouse on adult,career and vocational education.* Washington DC.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. In *International Journal of Information Management,* 24**,** 29-42.

King, C. G., Guyette Jr, R. W. & Piotrowski, C. (2009). Online Exams and Cheating: An Empirical Analysis of Business Students' Views. In *Journal of Educators Online,* 6**,** n1.

Kirda, E., Kruegel, C., Banks, G., Vigna, G. & Kemmerer, R. (2006). Behavior-based Spyware Detection. In: *Usenix Security*, 2006.

Kitzinger, J. (1995). Qualitative research. Introducing focus groups. In *BMJ: British Medical Journal,* 311**,** 299.

Ko, C. C. & Cheng, C. D. (2004). Secure Internet examination system based on video monitoring. In *Internet Research,* 14**,** 48-61.

Kohen, D. (2016). Everything you need to know about Facebook's Q4 and Full Year 2015 Results. *Adweek*, 26.01.2016.

Kolowich, S. (2014). Exactly how many students take online courses. In *Chronicle of Higher Education*.

Koohang, A., Riley, L., Smith, T. & Schreurs, J. (2009). E-learning and constructivism: From theory to application. In *Interdisciplinary Journal of E-Learning and Learning Objects,* 5**,** 91-109.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*, New Age International.

Kritzinger, E. (2006). Information Security in an E-learning Environment. In: Kumar, D. & Turner, J. (eds.) Education for the 21st Century—Impact of ICT and Digital Resources. IFIP International Federation for Information Processing,. vol. 210. (345-349): Springer, Boston, MA.

Kritzinger, E., Von Solms, S. & Johannesburg, S. (2006). Incorporating Information Security Governance. In *Issues in Informing Science and Information Technology,* 3.

Krsak, A. (2007). Curbing academic dishonesty in online courses. In: *TCC Worldwide Online Conference*, 2007. 159-170.

Krug, S. (2005). *Don't make me think: A common sense approach to web usability*, Pearson Education India.

Kumar, S., Gankotiya, A. K. & Dutta, K. (2011). A comparative study of moodle with other e-learning systems. In: *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, 2011. IEEE, 414-418.

Lammle, T. (2011). *CCNA Cisco Certified Network Associate Deluxe Study Guide*, John Wiley & Sons.

Laubscher, R., Olivier, M. S., Venter, H. S., Eloff, J. H. P. & Rabe, D. J. (2005). The role of key loggers in computer-based assessment forensics. In: *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, 2005. South African Institute for Computer Scientists and Information Technologists, 123-130.

Levy, Y. & Ramim, M. M. (2007). A Theoretical Approach For Biometrics Authentication of E-Exams. In: *International Journal of Digital Society (IJDS)*, 2007.

Lowenthal, P. & Wilson, B. G. (2010). Labels do matter! A critique of AECT's redefinition of the field. In *TechTrends,* 54**,** 38-46.

Mahmood, N. (2010). *Remote Proctoring Software Means Students Can Now Take Exams From Home* [Online]. Technological News Portal. Available: http://thetechjournal.com/science/remote-proctoring-software-means-students-can-now-take-exams-from-home.xhtml [Accessed 13/07/2011 2011].

Mandel, J., Roach, A. & Winstein, K. (2004). MIT Proximity card vulnerabilities. Massachusetts Tech. rep., Massachusetts Institute of Technology.

Manion, T. R., Kim, R. Y. & Patiejunas, K. (2014). *Remote desktop access*.

Marcel, S. & Del Millan, J. R. (2007). Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. In *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* 29**,** 743-752.

Mccabe, D. L. & Pavela, G. (1997). Ten Principles of Academic Integrity for Faculty. In *The Journal of College and University Law,* 24**,** 117-118.

Mccarthy, N. (2016). *Whatsapp Reaches One Billion Users* [Online]. New Jersey: Forbes LLC. Available: http://www.forbes.com/sites/niallmccarthy/2016/02/02/whatsapp-reaches-one-billion-users-infographic/#14158bb0520b [Accessed 03/02/2016 2016].

Mcclure, S., Scambray, J., Kurtz, G. & Kurtz (2009). *Hacking exposed: network security secrets and solutions,* Berkley, CA, McGraw-Hill.

Mcgee, P. (2013). Supporting Academic Honesty in Online Courses. In *Journal of Educators Online,* 10**,** n1.

Mcgraw, G. (2004). Software security. In *Security & Privacy, IEEE,* 2**,** 80-83.

Mcmurtry, K. (2001). E-Cheating: Combating a 21st Century Challenge. In *THE journal*.

Mcnabb, L. & Olmstead, A. (2009). Communities of integrity in online courses: Faculty member beliefs and strategies. In *Journal of Online Learning and Teaching,* 5**,** 208-23.

Miguel, J., Caballé, S., Xhafa, F. & Prieto, J. (2015a). A massive data processing approach for effective trustworthiness in online learning groups. In *Concurrency and Computation: Practice and Experience,* 27**,** 1988-2003.

Miguel, J., Caballé, S., Xhafa, F. & Snasel, V. (2015b). A Data Visualization Approach for Trustworthiness in Social Networks for On-line Learning. *IEEE 29th International Conference on Advanced Information Networking and Applications.* Gwangju, Korea: IEEE.

Mir, S. Q., Mehraj-Ud-Din Dar, S. & Beig, B. M. (2011). Information Availability: Components, Threats and Protection Mechanisms. In *Journal of Global Research in Computer Science,* 2.

Mitnick, K. (2002). *The art of deception,* New York, CyberAge books.

Moini, A. & Madni, A. M. (2009). Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective. In *IEEE Systems Journal,* 3**,** 469-476.

Molich, R., Ede, M. R., Kaasgaard, K. & Karyukin, B. (2004). Comparative usability evaluation. In *Behaviour & Information Technology,* 23**,** 65-74.

Monaco, J. V., Stewart, J. C., Cha, S.-H. & Tappert, C. C. (2013). Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works. In: *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*, 2013. IEEE, 1-8.

Moore, J. L., Dickson-Deane, C. & Galyen, K. (2011). e-Learning, online learning, and distance learning environments: Are they the same? In *The Internet and Higher Education,* 14**,** 129-135.

Moreno-Ger, P., Burgos, D., Martínez-Ortiz, I., Sierra, J. L. & Fernández-Manjón, B. (2008). Educational game design for online education. In *Computers in Human Behavior,* 24**,** 2530-2540.

Ni, M., Mccalley, J. D., Vittal, V. & Tayyib, T. (2003). Online risk-based security assessment. In *Power Systems, IEEE Transactions on,* 18**,** 258-265.

Nielsen, J. & Hackos, J. T. (1993). *Usability engineering*, Academic press San Diego.

Norman, D. A. (2013). *The design of everyday things: Revised and expanded edition*, Basic books.

Oghuma, A. P., Chang, Y., Libaque-Saenz, C. F., Park, M.-C. & Rho, J. J. (2015). Benefit-confirmation model for post-adoption behavior of mobile instant messaging applications: A comparative analysis of KakaoTalk and Joyn in Korea. In *Telecommunications Policy,* 39**,** 658-677.

Olt, M. R. (2002). Ethics and distance education: Strategies for minimizing academic dishonesty in online assessment. In *Online Journal of Distance Learning Administration,* 5.

Ortega-Garcia, J., Bigun, J., Reynolds, D. & Gonzalez-Rodriguez, J. (2004). Authentication gets personal with biometrics. In *Signal Processing Magazine, IEEE,* 21**,** 50-62.

Owunwanne, D., Rustagi, N. & Dada, R. (2010). Students' perceptions of cheating and plagiarism in higher institutions. In *Journal of College Teaching & Learning (TLC),* 7.

Ozsoyoglu, G. & Chin, F. Y. (1982). Enhancing the security of statistical databases with a question-answering system and a kernel design. In *IEEE Transactions on Software Engineering***,** 223-234.

Paullet, K., Chawdhry, A. A., Douglas, D. M. & Pinchot, J. (2015). Assessing Faculty Perceptions and Techniques to Combat Academic Dishonesty in Online Courses. In: *Proceedings of the EDSIG Conference*, 2015. n3433.

Paullet, K., Douglas, D. M. & Chawdhry, A. (2014). Verifying user identities in distance learning courses: Do we know who is sitting and submitting behind the screen? In *Issues in Information Systems,* 15.

Pedersen, A. B. (2010). Usability of authentication in web applications–a literature review. In *July,* 8**,** 31.

Percoco, N. J. & Spiderlabs, T. (2014). Global security report 2014 analysis of investigations and penetration tests. Tech. rep., SpiderLabs.

Perković, T., Li, S., Mumtaz, A., Khayam, S. A., Javed, Y. & Čagalj, M. (2011). Breaking undercover: Exploiting design flaws and nonuniform human behavior. In: *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011. ACM, 5.

Perry, D. E., Porter, A. A. & Votta, L. G. (2000). Empirical studies of software engineering: a roadmap. In: *Proceedings of the conference on The future of Software engineering*, 2000. ACM, 345-355.

Pfleeger, C. P. & Pfleeger, S. L. (2002). *Security in computing*, Prentice Hall Professional Technical Reference.

Phillips, R. & Lowe, K. (2003). Issues associated with the equivalence of traditional and online assessment. In: *Proceedings of the 20th Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education*, 2003. ascilite.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. In *Internet Research,* 14**,** 224-235.

Pillsbury, C. (2004). Reflections of academic misconduct: An investigating officer's experiences and ethics supplements. In *Journal of American Academy of Business,* 5**,** 446-454.

Pinkas, B. & Sander, T. (2002). Securing passwords against dictionary attacks. In: *Proceedings of the 9th ACM conference on Computer and communications security*, 2002. ACM, 161-170.

Potter, B. & Mcgraw, G. (2004). Software security testing. In *Security & Privacy, IEEE,* 2**,** 81-85.

Poulsen, K. (2000). Mitnick to lawmakers: People, phones and weakest links. In *Available fro m www. politechbot. com/p-00969. html.*

Powell, R. A. & Single, H. M. (1996). Focus groups. In *International journal for quality in health care,* 8**,** 499-504.

Powell, R. A., Single, H. M. & Lloyd, K. R. (1996). Focus groups in mental health research: enhancing the validity of user and provider questionnaires. In *International Journal of Social Psychiatry,* 42**,** 193-206.

Preece, J., Rogers, Y. & Sharp, H. (2002). Interaction design: beyond human-computer interaction. 2002. In *NY: John Wiley & Son.*

Preece, J., Rogers, Y., Sharp, H., Benyon, D., Holland, S. & Carey, T. (1994). *Human-computer interaction*, Addison-Wesley Longman Ltd.

Prometric. (1990). *Prometric: Trusted Test Development and Delivery Provider* [Online]. Education Testing Services. Available: https://www.prometric.com/ [Accessed 25/12/2012 2012].

Purdy, G. (2010). ISO 31000: 2009—setting a new standard for risk management. In *Risk analysis,* 30**,** 881-886.

Queen Mary, U. O. L. (2011). *Postgraduate Diploma in Clinical Dermatology* [Online]. London: Barts and London School of Dentistry. Available: http://www.londondermatology.org/courseint/index.html [Accessed 13/07/2011 2011].

Quesenbery, W. & Brooks, K. (2010). *Storytelling for user experience: Crafting stories for better design*, Rosenfeld Media.

Rabkin, A. (2008). Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In: *In SOUPS 2008: Proceedings of the 4th Symposium on Usable Privacy and Security*, 2008 23, New York, NY, USA. ACM, 13-23.

Ramim, M. & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. In *Journal of Cases on Information Technology (JCIT),* 8**,** 24-34.

Ratha, N. K., Bolle, R. M., Pandit, V. D. & Vaish, V. (2000). Robust fingerprint authentication using local structural similarity. In: *Applications of Computer Vision, 2000, Fifth IEEE Workshop on.*, 2000. IEEE, 29-34.

Reinschmidt, J. & Francoise, A. (2000). Business intelligence certification guide. In *IBM International Technical Support Organisation*.

Renaud, K. & Just, M. (2010). Pictures or questions?: examining user responses to association-based authentication. In: *Proceedings of the 24th BCS Interaction Specialist Group Conference*, 2010. British Computer Society, 98-107.

Respondus. (2016). *Respondus Assessment Tools for Learning Systems* [Online]. Redmond, WA. Available: https://www.respondus.com/products/lockdown-browser/ [Accessed 01/04/2016.

Roediger, H. L. (1990). Implicit memory: Retention without remembering. In *American psychologist,* 45**,** 1043.

Rogers, C. F. (2006). Faculty perceptions about e-cheating during online testing. In *Journal of Computing Sciences in Colleges,* 22**,** 206-212.

Rowe, N. C. (2004). Cheating in online student assessment: Beyond plagiarism. In *Online Journal of Distance Learning Administration,* 7.

Ruiz, J. G., Mintzer, M. J. & Leipzig, R. M. (2006). The impact of e-learning in medical education. In *Academic medicine,* 81**,** 207.

Rydstedt, G., Bursztein, E., Boneh, D. & Jackson, C. (2010). Busting frame busting: a study of clickjacking vulnerabilities at popular sites. In *IEEE Oakland Web,* 2.

Sahibudin, S., Sharifi, M. & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In: *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, 2008. IEEE, 749-753.

Sahoo, S. K. & Choubisa, T. (2012). Multimodal Biometric Person Authentication: A Review. In *IETE Technical Review,* 29**,** 54.

Sandhu, R. & Samarati, P. (1996). Authentication, access control, and audit. In *ACM Computing Surveys (CSUR),* 28**,** 241-243.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. In *BT technology journal,* 19**,** 122-131.

Sasse, M. A. & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? Usable security. vol. (13-30) London.

Sauro, J. & Kindlund, E. (2005). Making sense of usability metrics: usability and six sigma. In: *Proc. 14th Annual Conf. Usability Professionals Association*, 2005.

Scanlon, P. M. (2003). Student online plagiarism: how do we respond? In *College Teaching,* 51**,** 161-165.

Schacter, D. L. (2016). 31 Memory: Beyond Remembering. Scientists Making a Difference: One Hundred Eminent Behavioral and Brain Scientists Talk about Their Most Important Contributions. vol. (148) New York, USA: Cambridge University Press.

Schechter, S., Brush, A. J. B. & Egelman, S. (2009). It's No Secret. Measuring the Security and Reliability of Authentication via 'secret' questions. In: *30th IEEE Symposium on Security and Privacy*, 2009. IEEE, 375-390.

Schechter, S. E. (2004). *Computer security strength & risk: A quantitative approach.* Harvard University Cambridge, Massachusetts.

Schechter, S. E. (2005). Toward econometric models of the security risk from remote attack. In *IEEE security & privacy***,** 40-44.

Schneier, B. (1999). Attack trees. In *Dr. Dobb's journal,* 24**,** 21-29.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*, John Wiley & Sons.

Schultz, E. E., Proctor, R. W., Lien, M.-C. & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. In *Computers & Security,* 20**,** 620-634.

Seffah, A., Kececi, N. & Donyaee, M. (2001). QUIM: A Framework for Quantifying Usability Metrics in Software Quality Models. In: *Quality Software, 2001. Proceedings. Second Asia-Pacific Conference on*, 2001. IEEE, 311-318.

Shackel, B. (1991). Usability-context, framework, definition, design and evaluation. In *Human factors for informatics usability***,** 21-37.

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. In *Journal of verbal Learning and verbal Behavior,* 6**,** 156-163.

Shneiderman, B. & Ben, S. (1998). *Designing the user interface*, Pearson Education India.

Simkin, M. G. & Mcleod, A. (2010). Why do college students cheat? In *Journal of Business Ethics,* 94**,** 441-453.

Smart Card, A. (2003). *HIPAA compliance and smart cards: Solutions to privacy and security requirements* [Online]. Available: http://www.smartcardalliance.org/resources/lib/HIPAA_and_Smart_Cards_Report.pdf.

Smyth, B. (2010). Forgotten your responsibilities? How password recovery threatens banking security. *Technical Report CSR-10-13.* Birmingham: School of Computer Science.

Sonhera, N., Kritzinger, E. & Loock, M. (2012). A proposed cyber threat incident handling framework for schools in South Africa. In: *Proceedings of the South African Institute for Computer Scientists and Information Technologists Conference*, 2012. ACM, 374-383.

Spaulding, M. (2009). Perceptions of academic honesty in online vs. face-to-face classrooms. In *Journal of interactive online learning,* 8**,** 183-198.

Stallings, W. (2007). *Data and computer communications,* New Jersey, Pearson/Prentice Hall.

Standard, B. (1999). Information security management—Part 1: Code of practice for information security management. In *British Standard BS7799-1,* 1999.

Standards, O. F. I. (2005). ISO/IEC 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management. ISO/IEC.

Strang, R. (1937). *Behavior and Background of Studentsin College and Secondary Schools,* New York, Harper and Brothers.

Strother, J. B. (2002). An assessment of the effectiveness of e-learning in corporate training programs. In *The International Review of Research in Open and Distance Learning,* 3**,** Article 3.1. 2.

Stuber-Mcewen, D., Wiseley, P. & Hoggatt, S. (2009). Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom. In *Online Journal of Distance Learning Administration,* 12.

Sutherland-Smith, W. (2010). Retribution, deterrence and reform: the dilemmas of plagiarism management in universities. In *Journal of Higher Education Policy and Management,* 32**,** 5-16.

Tajuddin, S., Olphert, W. & Doherty, N. (2015). Relationship between stakeholders' information value perception and information security behaviour. In: *International Conference on Integrated Information (IC-ININFO 2014): Proceedings of the 4th International Conference on Integrated Information*, 2015. AIP Publishing, 69-77.

Tindell, D. R. & Bohlander, R. W. (2012). The use and abuse of cell phones and text messaging in the classroom: A survey of college students. In *College Teaching,* 60**,** 1-9.

Turnitin (2014). The effectiveness of Turnitin. Oakland, CA: iParadigm.

Ullah, A., Xiao, H. & Barker, T. (2015). Usability of Activity-Based and Image-Based Challenge Questions in Online Student Authentication. In: Tryfonas, T. & Askoxylakis, I. (eds.) Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science. vol. 9190. (131-140): Springer, Cham.

Ullah, A., Xiao, H., Barker, T. & Lilley, M. (2014a). Evaluating security and usability of profile based challenge questions authentication in online examinations. In *Journal of Internet Services and Applications,* 5**,** 2.

Ullah, A., Xiao, H., Barker, T. & Lilley, M. (2014b). Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations. In: *The 9th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2014b London, UK. IEEE.

Ullah, A., Xiao, H. & Lilley, M. (2012a). Profile Based Student Authentication in Online Examination. In: *International Conference on Information Society* 2012a London, UK. IEEE, 118-122.

Ullah, A., Xiao, H., Lilley, M. & Barker, T. (2012b). Usability of Profile Based Student Authentication and Traffic Light System in Online Examination. In: *The 7th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2012b London, UK. IEEE, 220-225.

Ullah, A., Xiao, H., Lilley, M. & Barker, T. (2012c). Using Challenge Questions for Student Authentication in Online Examination. In *International Journal for Infonomics (IJI)* 5**,** 9.

Ullah, A., Xiao, H., Lilley, M. & Barker, T. (2013). Design, privacy and authentication of challenge questions in online examinations. In: *IEEE Conference on e-Learning, e-Managementand and e-Services (IC3e)*, 2013 Malaysia. IEEE, 46-50.

Ullah, A., Xiao, H., Lilley, M. & Barker, T. (2014c). Privacy and Usability of Image and Text Based Challenge Questions Authentication in Online Examination. In: *The International Conference on Education Technologies and Computers (ICETC2014)*, 2014c Lodz, Poland. IEEE, 24-29.

Underwood, J. & Szabo, A. (2003). Academic offences and e-learning: individual propensities in cheating. In *British Journal of Educational Technology,* 34**,** 467-477.

Unemployedprofessors. (2016). *Unemployed Professors* [Online]. Available: http://unemployedprofessors.com/ [Accessed 30/03/2016 2016].

Vander Schaaf, A. (2005). *Plagiarism: A Philosophical Analysis of Aspects of Property, Theft, and Deception.* University of Guelph.

Vician, C., Charlesworth, D. D. & Charlesworth, P. (2006). Students' Perspectives of the Influence of Web-Enhanced Coursework on Incidences of Cheating. In *Journal of Chemical Education,* 83**,** 1368.

Virzi, R. A. (1992). Refining the test phase of usability evaluation: how many subjects is enough? In *Human Factors: The Journal of the Human Factors and Ergonomics Society,* 34**,** 457-468.

Volery, T. & Lord, D. (2000). Critical success factors in online education. In *International Journal of Educational Management,* 14**,** 216-223.

Warner, F. (1983). Risk assessment: report of a Royal Society study group. London: British Royal Society.

Warner, F. (1992). Risk: Analysis, Perception and Management, Report of a Royal Society Study Group. London: The British Royal Society.

Watson, G. & Sottile, J. (2010). Cheating in the Digital Age: Do Students Cheat More in Online Courses? In *Online Journal of Distance Learning Administration,* 13**,** n1.

Weinshall, D. & Kirkpatrick, S. (2004). Passwords you'll never forget, but can't recall. In: *CHI'04 extended abstracts on Human factors in computing systems*, 2004. ACM, 1399-1402.

Weippl, E. R. (2005). Security in e-learning. In *eLearn Magazine,* 2005**,** 3.

Wetakeyourclass. (2016). *Take my online class* [Online]. Wetakeyourclass. Available: https://www.takeyourclass.com/ [Accessed 30/03/2016 2016].

Wheeler, D., Whittlestone, K., Smith, H., Gupta, A. & Menon, D. (2003). A web-based system for teaching, assessment and examination of the undergraduate peri-operative medicine curriculum. In *Anaesthesia,* 58**,** 1079-1086.

Whitten, A. & Tygar, J. (1998). Usability of security: A case study. PA: Department of Computer Science, Carnegie-Mellon University Pittsburgh PA.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. & Memon, N. (2005). Authentication using graphical passwords: effects of tolerance and image choice. In: *Proceedings of the 2005 symposium on Usable privacy and security*, 2005. ACM, 1-12.

Wielicki, T. (2006). Integrity of online testing in e-learning: Empirical study. In: *Fourth IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, 2006. IEEE, 5 pp.-210.

Williams, B. C. (2005). MOODLE for Teachers, Trainers and Administrators. In *Consultado el,* 13.

Wisher, R., Curnow, C. & Belanich, J. (2005). Verifying the learner in distance learning. In: *18th Annual Conference on Distance Teaching and Learning*, 2005.

Wixon, D. & Wilson, C. (1997). The usability engineering framework for product design and evaluation. In *Handbook of human-computer interaction,* 2**,** 653-68.

Wrightsman Jr, L. S. (1959). Cheating—A research area in need of resuscitation. In *Peabody Journal of Education,* 37**,** 145-149.

Xiang, J. & Ye, L. (2008). Thought and Tentative Idea of Reform in Formative Assessment. In: *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*, 2008. IEEE, 2376-2380.

Xiao, H., Ji, W. & Ullah, A. (2011). Authentication of Students and Students' Work in E-Learning. *Report for the Development Bid of Academic Year 2010/11.* University of Hertfordshire.

Xu, H., Zhou, Y. & Lyu, M. R. (2014). Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In: *Symposium On Usable Privacy and Security, SOUPS*, 2014. 187-198.

Yee, K.-P. (2002). User interaction design for secure systems. In: Deng, R., Bao, F., Zhou, J. & Qing, S. (eds.) Information and Communications Security. ICICS 2002. Lecture Notes in Computer Science,. vol. 2513. (278-290): Springer, Berlin, Heidelberg.

Youll, J. (2006). Fraud vulnerabilities in sitekey security at bank of america. In *Available: www. cr-labs. com/publications/SiteKey-20060718. pdf.*

Zviran, M. & Haga, W. J. (1990). User authentication by cognitive passwords: an empirical assessment. In: *Information Technology, 1990.'Next Decade in Information Technology', Proceedings of the 5th Jerusalem Conference on (Cat. No. 90TH0326-9)*, 1990. IEEE, 137-144.

Appendix A – Text and Image-based Questions

A –I Text-based questions

Text-based questions designed study 2 usability analysis reported in chapter 7.

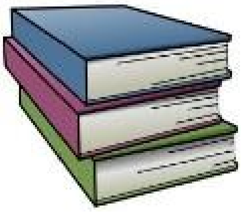
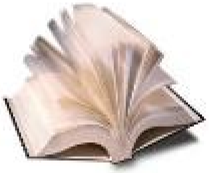
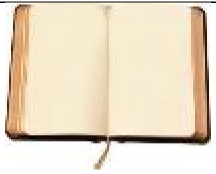
No.	**Academic**
1	What is your student number?
2	What is the name of your first school attended
3	In which class/level you achieved the best grades?
4	What were your grades in the highest qualification before this course?
5	What is the name of your last school attended?
6	What year did you graduate from high school?
	Favourite
7	What is your favourite colour?
8	What is your favourite TV program?
9	What is your favourite website URL?
10	What is your favourite “colour car”?
11	Write the first three letters of your favourite cousin’s name?
12	What is your favourite bird?
13	What is your favourite animal?
14	What is your favourite car?
15	What is your favourite place to visit as a child?
16	What is your favourite academic course?
17	What is the first name of your favourite tutor?
18	What is your favourite movie?
19	What is your favourite holiday destination?
20	Who is your favourite childhood hero?
21	What is your favourite food?
22	What is your favourite book?
	Personal
23	What is the country of dream vacations?
24	What is your grandfather's surname?
25	What is your best friend's surname?
26	What was your dream job as a child?
27	What is the name of your best childhood friend?
	Date
28	What is your date of birth?
29	What is your year of birth?
30	What is your “Day” of birth?
31	What is your “Month” of birth?

A –II Image-based questions

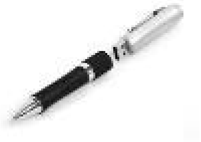
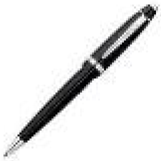
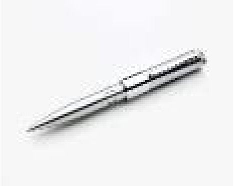
Image based questions designed for study 2 usability analysis reported in chapter 7.

1) Please select your favourite “book” image from the following options.

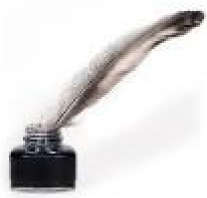
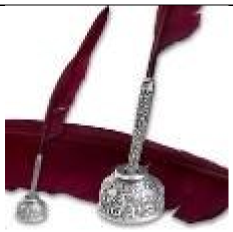
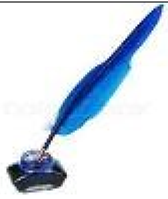
A.	B.	C.

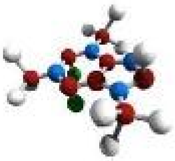
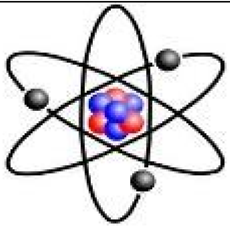
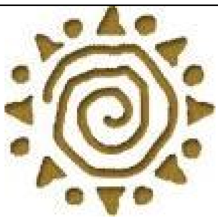
2) Please select your favourite "Pen" image from the following options.

A.	B.	C.
		

3) Please select your favourite "Pen & ink pot" image from the following options.

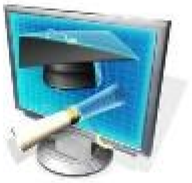
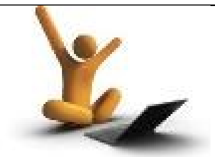
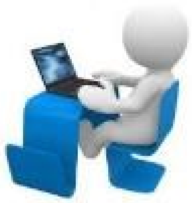
A.	B.	C.
		

4) What is your choice of a logo representing "Science"?

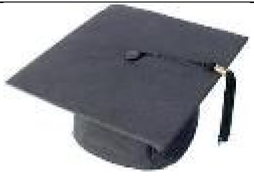
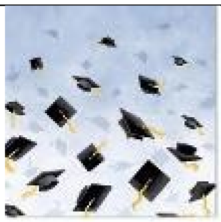
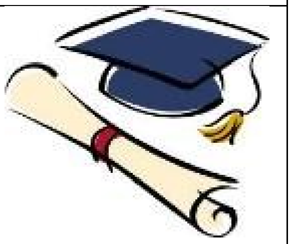
A.	B.	C.
		

5) What is your choice of a logo representing "online learning"?

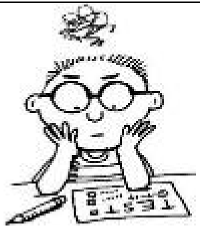
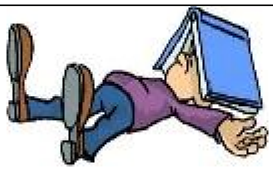
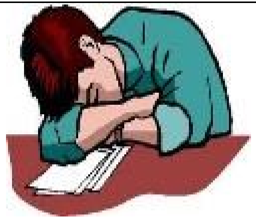
A.	B.	C.

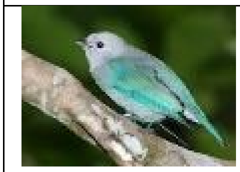
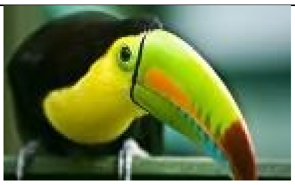
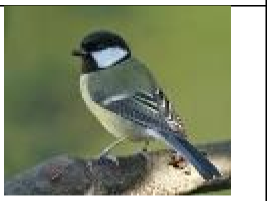
6) What is your choice of a logo representing “graduation”?

A.	B.	C.
		

7) What is your choice of a logo representing “examination”?

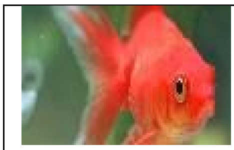
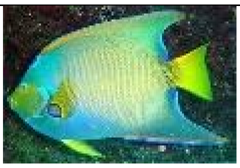
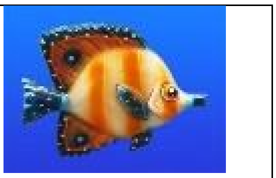
A.	B.	C.
		

8) Which one of the following is your favourite “bird”?

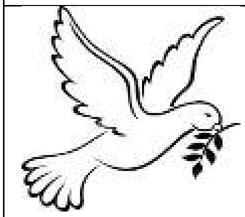
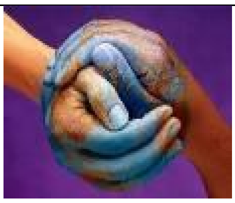
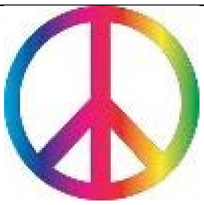
A.	B.	C.
		

9) Which one of the following is your favourite “fish”?

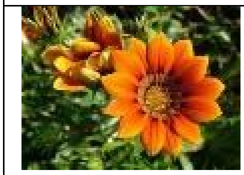
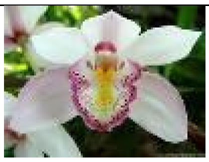
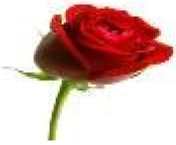
A.	B.	C.

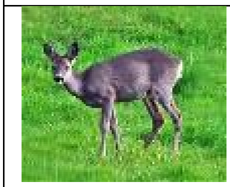
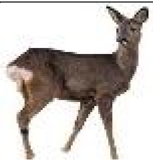
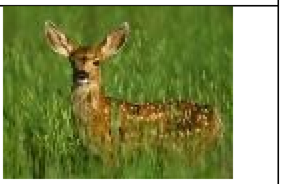
10) Which one of the following is your choice of a logo representing “peace”?

A.	B.	C.
		

11) Which one of the following is your favourite “flower”?

A.	B.	C.
		

12) Which one of the following is your favourite “deer”?

A.	B.	C.
		

13) Which one of the following is your choice of a logo representing "internet security”?

A.	B.	C.

Appendix B – Text-based Questions and Impersonation

B –I Text Based questions

Text-based questions designed for collusion and guessing abuse case scenarios reported in study 3 chapter 8.

No.	Questions
1	Which town were you born in?
2	What is your favourite food?
3	What was the name of your favourite teacher in primary school?
4	What is your favourite holiday destination?
5	What is the name of your last school attended?
6	What is your best friend's surname?
7	What is your favourite academic course subject?
8	Write the first three letters of your favourite cousin?
9	What year did you graduate from High School?
10	Who is the favourite hero of your childhood?
11	What is the name of the first school you attended?
12	What is the make of your phone set?
13	What is your favourite TV program?
14	What was your favourite place to visit as a child?
15	What is your favourite name?
16	What is the title of your favourite book?
17	What is your date of birth?
18	What is your favourite politician of all times?
19	What is your favourite colour?
20	What is your favourite restaurant?
21	Who is your favourite singer?
22	What is your favourite fruit or vegetable?
23	What is your favourite town?
24	What is your favourite sports?
25	What is your favourite FLOWER?
26	What is the name of your best childhood friend?
27	What is your favourite colour car?
28	Where did you go on your first train journey?
29	What is your student number?
30	What is your favourite website url?
31	Where is your favourite shopping place?
32	What is your father's year of birth?
33	What is your favourite University?
34	In which class or level you achieved your best grades ever?
35	What is your favourite animal?
36	What is your first line of your doctor's address?
37	What is your favourite car?

38 What is your favourite bird?
39 What is your favourite number?
40 Where was your most memorable holiday?
41 What is your favourite movie?
42 What shop do you prefer to buy cloths in?
43 What is your favourite pet's name?
44 What is your favourite pet?
45 What is the country of your ultimate dream vacation?
46 What is your favourite sports player?
47 What is your favourite pastime activity?
48 What are the last four digits of your mobile number?
49 When you were young, what did you want to be when you grew up?
50 What is the name of your favourite world leader (current/past)?

Appendix C – Course Design & Dynamic Profile Questions

C –I An Overview of Online Course

The course outline used for study 3 using dynamic profile question reported in chapter 9.

Week 1

- Let us know about you
- Introduction Resource
- PHP Installation (XAMPP Installation) Resource
- My first PHP page Resource
- PHP variables Resource
- Strings and Variables Resource
- PHP Operators Resource
- PHP Introduction Lesson
- Project Assignment Week 1 (Write one of the following PHP short programs)
    1) Write a PHP program to assign your name to $myname and qualification to $qualification variables and display the output on page with on two separate lines.
    2) Write a PHP program to assign any two numbers to two variables and display their sum on screen.
    3) Write a PHP program to assign any number to a variable and display the value using pre-increment operator (++). Check PHP operators for help.
- Student Reflection –What have I learned about PHP variables, strings and lessons?
- Week 1 Quiz

Week 2

- Conditional statements Resource
- PHP switch statement Resource
- PHP Arrays Resource
- Conditional Flow Lesson
- Project Assignment Week 2 (Write one of the following PHP short programs)
    - Write a PHP program to display your favourite fruit from the given choices Mango, Orange, Apple, Plum, and Cherry using a Switch statement.
    - Write a PHP program to Input three numbers n1, n2, and n3 and display the largest on screen?
    - Write a PHP program using an indexed array to store name of cars i.e. Honda, BMW, and Fiat and print them on screen.
    - Write a PHP program using associate array to store student's score i.e. student 1 20%, student 2 40%, student 3 87%, student 4 90% and display them on screen.
- Student Reflection –What have I learned about PHP condition statements in week 2?

- Week 2 Quiz

Week 3

- PHP Looping -While Loop Resource
- PHP Looping -for Loop Resource
- PHP functions Resource
- PHP Looping Lesson
- Project Assignment Week 3 (Write one of the following PHP short programs)
    - Write a PHP program using compute and display table of 2 e.g. 2 x 1 =2 to the count of 10 using any of the Looping statements.
    - Using any of the PHP Looping, write a program to display 1-10 even numbers
    - Using a PHP for loop, display values of an array $i=array(“BMW”, ”Honda”,”Ford”, “Mini”);
- Student Reflection –What have I learned about PHP Looping in week 3?
- Week 3 Quiz

Week 4

- PHP & HTML Forms Resource
- $_GET method Resource
- $_POST method Resource
- HTML Forms Lesson
- Student Reflection –What have I learned about PHP HTML forms in week 4
- Week 4 Quiz

Week 5

- MySQL Resource
- PHP MySQL Database connection & insert form data Resource
- Create database connection and get data from Db Resource
- Practice lesson -Select and display data from database Resource
- Where clause, update, delete from database Resource
- Student Reflection –What have I learned about MySQL database functions in week 5
- Week 5 Quiz –Final

C –II Dynamic Profile Questions

Below is the 18 dynamic profile questions implemented in study 3 reported in chapter 9.

Q.1 which one of the following statement below were written by you?

- I am currently in second year of Economics Degree
- I have a degree in Chemistry from Trinity College Dublin, Ireland and pursued a part-time research MSc in Computational Chemistry with Trinity College. 3 publications.
- I used SQL during the second year of my course a few years ago, along with Java (JDBC)

- Currently I’m enrolled at the MSc Computer Science course, previously I studied BSC (Hons) in Computers and Electronics at the Northampton University.
- None of the above

Q.2 which one of the following statement below were written by you as a course objective

- I have over seven year experience in the IT sector, I’m currently working as database administrator/programmer
- I am doing this course as part of my CPD required in my workplace
- I would like to pursue this course in order to learn more for my field of work and have more knowledge for advancement.
- I want to do this course because i can work as a freelancer after doing php as i have seen so many projects in Freelancer, Odesk and Elance and i already have some experience of Sql.
- None of the above

Q.3 which of the following statement were written in your introduction email?

- For networking I need to know some of scripting languages and so I want to learn php.
- I work in a non-IT related field- I am a cook.
- Have already got the basics in HND for PHP and MySQL but thought this would be a good opportunity to refresh memory and expand on this
- Recently my employer have introduced software products and web pages written in PHP and using MySQL databases so it will be highly beneficial for my career to familiarise myself with this technologies.
- None of the above

Q.4 which one of the following discussion posts were made by you?

- I just completed the week 1 quiz and all the contents of week 1. I can’t access to week 2, Am I too late for it, or is there any specific reason for it?
- When I run the page that should execute Hello World. I'm getting an error saying the URL was not found on the server
- I've tried the following: Test after starting of Apache (and MySQL), go to the address http://localhost/ or http://127.0.0.1/ in your browser and examine all of the XAMPP examples and tools. but all I get is a HTTP 404 not found page

- Did you save the example1.php in your xampp folder correctly? (i.e. make a new folder called myproject in the htdocs folder)
- None of the above

Q.5 which one of the following discussion posts were made by you?

- I have now completed week 1 assignment. Can I have access to week 1 quiz?
- I have managed to install XAMPP but I cannot connect to MySQL module. I have tried to uninstall and reinstall but nothing is working. I had installed MYSQL database previously.
- Thanks Mr Abrar but I do not think that is going to be necessary. I have managed to install XAMPP on another computer.
- Hi Evens, It works for me but it is not is English. AND. Many thanks Chelsea, not a great start but you cracked it.
- None of the above

Q.6 which one of the following discussion posts were made by you?

- I found this too. Googling it, as I understand it what is happening is when the script first runs the $i variable is not initialised, effectively resulting in a null being passed in to the switch statement
- You have stated that the second example is the same as the first one. So how come you have used quotation marks for the second example?
- Normally port 443 is used for secure host and accessible using https
- You nailed it. Perfect. Actually if the port is used by another service, apache won't start as the port is already taken.
- None of the above

Q.7 your score for the week 1 quiz was:

- Within the 60%-69% range
- Within the 80%-100% range
- Within the 40% -59% Range
- Within the 70%-79% range
- Less than 40%

Q.8 which one of the following assignments have you submitted in week 1?

- Write a PHP program to assign your name to $myname and qualification to $qualification variables and display the output on page with on two separate lines.
- List examples of logical operators and provide evidence with php programs?
- Write a php function to compute standard deviation of data array?
- Write a php program to connect to database using PDO and retrieve data using select statement?
- None of the above

Q.9 which one of the following assignments have you submitted in week 1?

- Write a php program to demonstrate difference between static, private and public class?
- Write a PHP program to assign any two numbers to two variables and display their sum on screen.
- Write a php program for traffic lights control
- Write a php program to submit data using form $_POST and insert into MySQL database?
- None of the above

Q.10 which one of the following assignments have you submitted in week 1?

- Write a PHP program to assign any number to a variable and display the value using pre-decrement operator (--). Check PHP operators for help.
- Write a PHP program to compute factorial of a number n?
- Write a PHP program to demonstrate post decrement
- Write a PHP program to compare pre-increment with post-increment
- None of the above

Q.11 which one of the following PHP code belongs to your assignment?

- while ($minNum < $maxNum){
- echo "Perform addition: $a + $b = ".$addition."";
- foreach($data s $dataitem)
- $sum = $numberone + $numbertwo;
- None of the above

Q.12 which one of the following PHP code belongs to your assignment?

- $a=++$a;

- $sum(a+b);
- $addition = $a + $b;
- addFunction(10,10);
- None of the above

Q.13 your score for the assignment 1 was:

- Within the 40% -69% Range
- Within the 70%-79% range
- Within the 80%-89% range
- Within the 90%-100% range
- None of the above

Q.14 which one of the following reflection posts were made by you?

- I have learnt to create php classes and objects
- I have learnt to create my first PHP page and coding, assign variables and the different arithmetic operations.
- I have learnt to create database connection to backend using PHP in week 6
- I have learnt email function using php, which is very relevant to my ongoing project
- None of the above

Q.15 which one of the following assignments have you submitted in week 2?

- Write a PHP program to develop gradebook using array
- Write a PHP program to display your favourite fruit from the given choices: Mango, Orange, Apple, Plum, Cherry, pineapple, kewi using PHP Switch statement.
- Write a PHP program to display odd number for array list
- Write a PHP program to sort an array list
- None of the above

Q.16 which one of the following assignments have you submitted in week 2?

- Write a PHP program using an indexed array to store name of cars: Honda, BMW, Toyota, Ford, Audi and Fiat and print them all on screen line by line.
- Develop a bubble sort program using PHP
- Develop push and pop functions of stack using PHP program

- Write a php program to connect to database using PDO and retrieve data using select statement?
- None of the above

Q.17 which one of the following PHP code belongs to your assignment 2?

- print_largest($array);
- While(NOT $thelargetnumber)
- function getLarget($array =array());
- $cars[0]="Honda";
- None of the above

Q.18 which one of the following PHP code belongs to your assignment 2?

- echo $cars[0]." ".$cars[1]." ".$cars[2]." ".$cars[3]." ".$cars[4]." ".$cars[5];
- foreach($numbers in $numbersArray())
- echo $find_favorite_fruite($fruitArray);
- Do While ($num[0] <$num[1])
- None of the above

C –III Introduction email

An introduction email described below, was sent to all participants.

Dear Student,
Please read the following guidelines carefully to start your online PHP & MySQL course.

- Please access the registration page at http:://research.xxx.xxx and complete your registration.
- In order to access the course, select “Learning PHP and MySQL in 5 Weeks”. You are required to submit enrolment key in order to complete your registration & enrolment. The enrolment key is “php”.
- The course is organized in 5 weeks short modules. The contents of the course will be released on day-to-day basis. There are three short beginner level assignments in the first three weeks.
- Students are required to complete week 1 quiz in order to progress to the following week.

- There is no pass or fail but students are required to complete the weekly quizzes in order to promote and able to access content of the following weeks.

As part of our research, we are using a secure authentication system for access to online weekly quizzes. The authentication system will use some challenge questions to confirm your identity. These challenge questions will be based on your interaction with the learning content and your submissions.

Abrar Ullah,
Online Course Tutor

C –IV Collusion Attacks Information:

An email sent to participants regarding collusion attacks:

Dear Student
This course is designed to provide you with the basic skills in developing PHP and MySQL database driven applications.

Besides providing quality training to online students, we are using the online course to help with a research study, which aims to investigate the threats of a student cheating in an online examination with the help of a 3rd party impersonator/helper. There are different types of collusion attacks and the focus of this study is to investigate the following types of collusion attacks:

- Collusion via Phone: In this type of attack, a student shares access credentials (Login ID and Password, and dynamic profile questions and their answers) with a third party attacker remotely via mobile phone to provide him access to online examination. The attacker using the access credentials impersonates as a student and complete online examination. The attacker communicates synchronously with the student during the online examination.
- Collusion via Email: In this type of attack, a student shares access credentials (Login ID and Password, and dynamic profile questions and their answers) with a third party attacker remotely via Email address before the online examination. The attacker uses the access credential impersonates as a student and complete online examination.

To help with the research, can I request you to collect as much information about your dynamic profile questions as possible to perform/simulate the collusion attack via email?

Also, for a collusion attack via phone, please, send me your availability for an hour long skype session.

Best wishes,
Abrar Ullah
Online Course Tutor

C –V Collusion Attack in Non-real-time via Email:

An email was sent to participants for participating in collusion attack via skype:

Dear Student,
As part of our research, we need your help to complete a remote location collusion attack via email. In this attack, we need you to share with us all or a maximum number of dynamic profile questions and their answers for authentication.

Dynamic profile questions are those which are presented to you during your weekly quizzes for authentication and are based on your submissions and learning activities.

Please share as many Challenge questions as possible. If you cannot share your challenge questions, please state a reason in the “Possible Answer/Reason”. See example below for guidance.

Name			
No.	Challenge Question	Possible Answer	Reason for not sharing 1-shared, 2-can share a cue, 3-cannot recall but recognize answer, 4-neither recall nor recognize the answer.
1			
2			

Example:

Name		Student 1	
No.	Challenge Question	Possible Answer	Reason for not sharing OR How do you know the question
1	which one of the following discussion posts were made by you	Something you have posted	Copied the answers in my computer

C –VI Collusion Attack In Real-Time via Skype guidance:

An email was sent to participants for participating in collusion attack via skype:

Dear Student,
As part of our research, we need your help to complete a remote location collusion attack via skype. In this attack, we need you to share with us correct answers to dynamic profile questions related with your learning experience.

Dynamic profile questions are those which are presented to you during your weekly quizzes for authentication and are based on your submissions and learning activities.

The attack will be carried out in a skype session. It is a brief 15 minutes session and the steps are described below.

- You will login to skype using pbaf.authentication using password: Password.
- A simulation attacker account pbaf.attack is already linked with the skype account above.
- The attacker will share with you a dynamic profile question and multiple options from your profile. We need you to identify the correct answer as you would do to any of these questions in your weekly quizzes.
- The attacker will repeat step 3 until all your dynamic profile questions are answered.

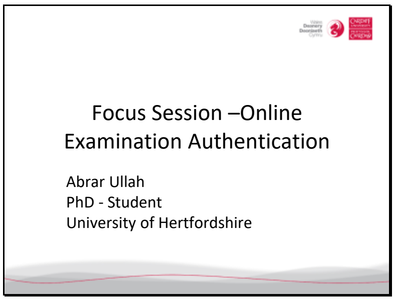
Please send us a convenient day and time for the skype session.

Best wishes,

Appendix D – Supporting Information Focus Group

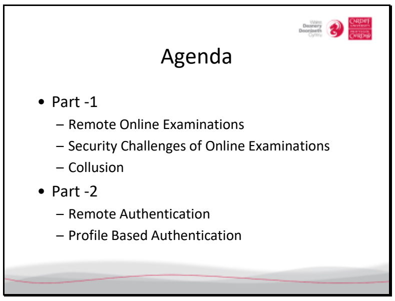
D –I Presentation to Online Programme Tutors

The following slides were presented to online programme tutors in the start of the focus group session.



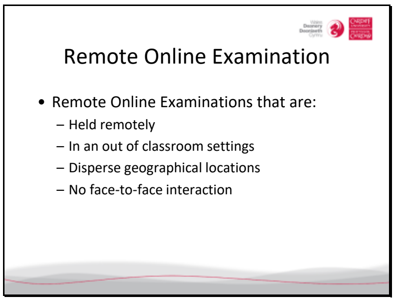
Focus Session –Online Examination Authentication

Abrar Ullah
PhD - Student
University of Hertfordshire



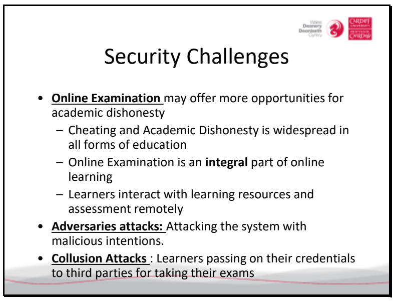
Agenda

- Part -1
  - Remote Online Examinations
  - Security Challenges of Online Examinations
  - Collusion
- Part -2
  - Remote Authentication
  - Profile Based Authentication



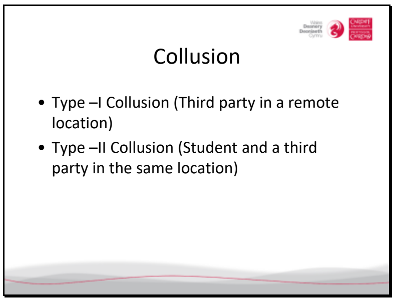
Remote Online Examination

- Remote Online Examinations that are:
  - Held remotely
  - In an out of classroom settings
  - Disperse geographical locations
  - No face-to-face interaction



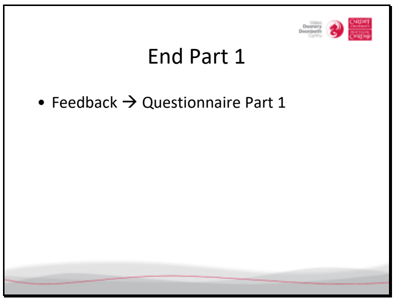
Security Challenges

- **Online Examination** may offer more opportunities for academic dishonesty
  - Cheating and Academic Dishonesty is widespread in all forms of education
  - Online Examination is an **integral** part of online learning
  - Learners interact with learning resources and assessment remotely
- **Adversaries attacks:** Attacking the system with malicious intentions.
- **Collusion Attacks** : Learners passing on their credentials to third parties for taking their exams



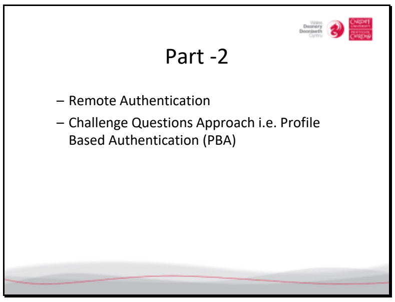
Collusion

- Type –I Collusion (Third party in a remote location)
- Type –II Collusion (Student and a third party in the same location)



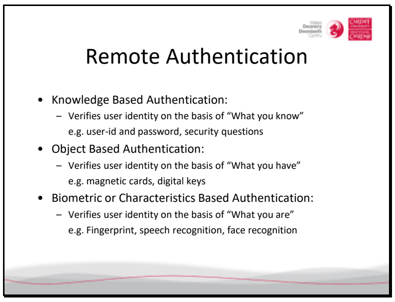
End Part 1

- Feedback → Questionnaire Part 1



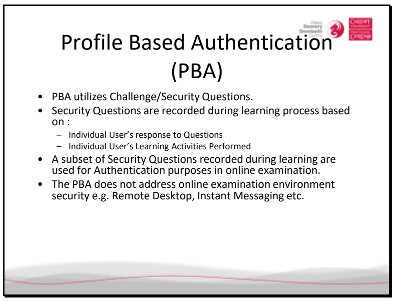
Part -2

- Remote Authentication
- Challenge Questions Approach i.e. Profile Based Authentication (PBA)



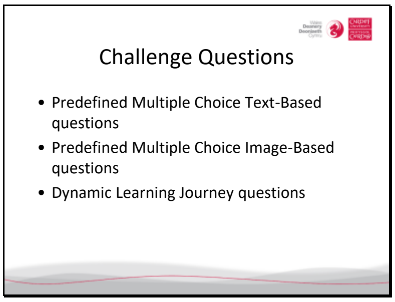
Remote Authentication

- Knowledge Based Authentication:
  - Verifies user identity on the basis of "What you know" e.g. user-id and password, security questions
- Object Based Authentication:
  - Verifies user identity on the basis of "What you have" e.g. magnetic cards, digital keys
- Biometric or Characteristics Based Authentication:
  - Verifies user identity on the basis of "What you are" e.g. Fingerprint, speech recognition, face recognition



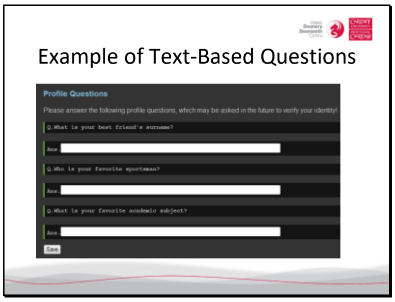
Profile Based Authentication (PBA)

- PBA utilizes Challenge/Security Questions.
- Security Questions are recorded during learning process based on :
  - Individual User's response to Questions
  - Individual User's Learning Activities Performed
- A subset of Security Questions recorded during learning are used for Authentication purposes in online examination.
- The PBA does not address online examination environment security e.g. Remote Desktop, Instant Messaging etc.



Challenge Questions

- Predefined Multiple Choice Text-Based questions
- Predefined Multiple Choice Image-Based questions
- Dynamic Learning Journey questions



Example of Text-Based Questions

Profile Questions

Please answer the following profile questions, which may be asked in the future to verify your identity!

Q.What is your best friend's surname?

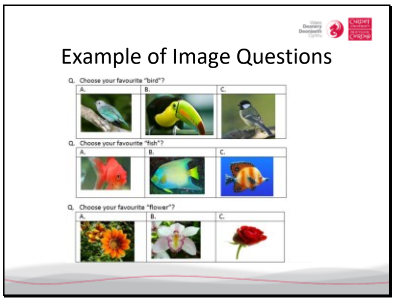
Ans.

Q.Who is your favorite sportsman?

Ans.

Q.What is your favorite academic subject?

Ans.

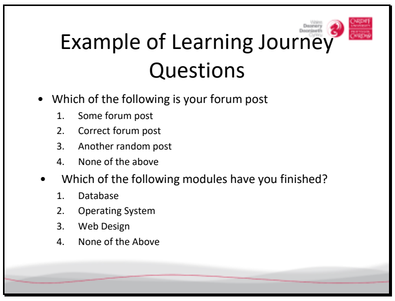


Example of Image Questions

Q. Choose your favourite "bird"?

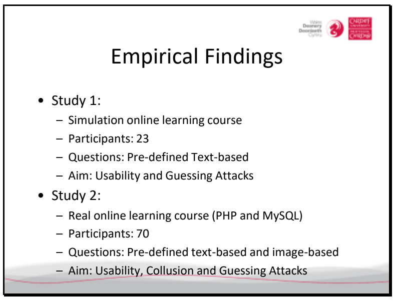
Q. Choose your favourite "fish"?

Q. Choose your favourite "flower"?



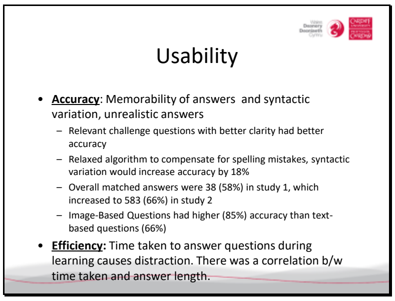
Example of Learning Journey Questions

- Which of the following is your forum post
  1. Some forum post
  2. Correct forum post
  3. Another random post
  4. None of the above
- Which of the following modules have you finished?
  1. Database
  2. Operating System
  3. Web Design
  4. None of the Above



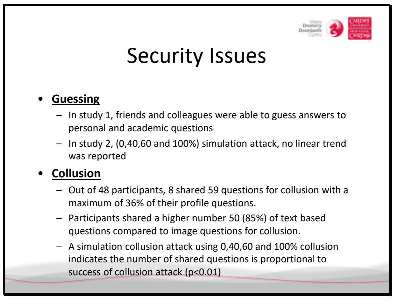
Empirical Findings

- Study 1:
  - Simulation online learning course
  - Participants: 23
  - Questions: Pre-defined Text-based
  - Aim: Usability and Guessing Attacks
- Study 2:
  - Real online learning course (PHP and MySQL)
  - Participants: 70
  - Questions: Pre-defined text-based and image-based
  - Aim: Usability, Collusion and Guessing Attacks



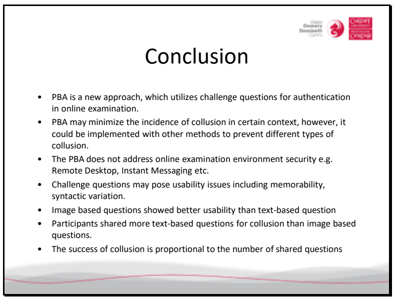
Usability

- **Accuracy**: Memorability of answers and syntactic variation, unrealistic answers
  - Relevant challenge questions with better clarity had better accuracy
  - Relaxed algorithm to compensate for spelling mistakes, syntactic variation would increase accuracy by 18%
  - Overall matched answers were 38 (58%) in study 1, which increased to 583 (66%) in study 2
  - Image-Based Questions had higher (85%) accuracy than text-based questions (66%)
- **Efficiency:** Time taken to answer questions during learning causes distraction. There was a correlation b/w time taken and answer length.



Security Issues

- **Guessing**
  - In study 1, friends and colleagues were able to guess answers to personal and academic questions
  - In study 2, (0,40,60 and 100%) simulation attack, no linear trend was reported
- **Collusion**
  - Out of 48 participants, 8 shared 59 questions for collusion with a maximum of 36% of their profile questions.
  - Participants shared a higher number 50 (85%) of text based questions compared to image questions for collusion.
  - A simulation collusion attack using 0,40,60 and 100% collusion indicates the number of shared questions is proportional to success of collusion attack ($p<0.01$)



Conclusion

- PBA is a new approach, which utilizes challenge questions for authentication in online examination.
- PBA may minimize the incidence of collusion in certain context, however, it could be implemented with other methods to prevent different types of collusion.
- The PBA does not address online examination environment security e.g. Remote Desktop, Instant Messaging etc.
- Challenge questions may pose usability issues including memorability, syntactic variation.
- Image based questions showed better usability than text-based question
- Participants shared more text-based questions for collusion than image based questions.
- The success of collusion is proportional to the number of shared questions

D –II Paper-based Questionnaire:

Participants of the focus group were asked to provide their feedback by responding the following questionnaire.

Part 1

	Questions	Scale
Collusion and Online Examination		
1	How concerned are you about the security of a remote online examination?	1-No concern at all to 5. Strong concern
2	How concerned are you about the authentication methods implemented for the security of a remote online examination	1-No concern at all to 5. Strong concern
3	In your view, how difficult it is for a student to cheat in remote online examination	1-Not difficult at all to 5. Very difficult
4	In your view, how difficult it is for a student to cheat in face-to-face invigilated examination	1-Not difficult at all to 5. Very difficult
5	Consider the threat of a student copying answers from a book or other course material, please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation	1-Not serious at all to 5. Very serious
6	Consider the threat of a student copying answers from the Internet, please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation	1. Not serious at all to 5. Very serious
7	Abetting - Consider the threat of a student getting help from someone else, based in the same location, please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation	1. Not serious at all to 5. Very serious
8	Impersonation - Consider the threat of a student getting help from a third party, based in a remote location, please rate the seriousness of this threat in a remote online examination where there is remote student authentication but no invigilation	1. Not serious at all to 5. Very serious
Part 2		
Please rate the usefulness of the three authentication methods below		
9	Login Identifier and Password Authentication	1. Not useful at all to 5.Very useful
10	Graphical Password Authentication	1. Not useful at all to 5.Very useful
11	Security/Challenge Questions Authentication	1. Not useful at all to 5.Very useful
12	How effective would the Challenge Questions (PBA) approach be to deter impersonation attacks?	1. Not effective at all to 5. Very effective
Please rate the effectiveness of the questions types below while using the PBA method		

13	Pre-defined Text-Based Questions	1. Not useful at all to 5.Very useful
14	Pre-defined Image-Based Questions	1. Not useful at all to 5.Very useful
15	Dynamic Profile Questions	1. Not useful at all to 5.Very useful
16	How usable is the challenge question approach?	1. Not useful at all to 5.Very useful
17	How secure is the challenge question approach in terms of non-collusion based intruder access	1. Not secure to 5. Secure
18	How secure is the challenge question approach in terms of collusion attacks	1. Not secure to 5. Very Secure
19	Given that security and usability may be considered to be a trade-off , on the scale of 1 to 10 please indicate where you think the best option should be	1. Very Secure …. 5. About Equal …. 10.Very usable

D –III Moderator Probes:

A list of probes presented by focus session moderator for discussion.

- **Moderator Presented a Scenario:** *“You setup an online examination for a large group of students located remotely in several continents. They access the examination using the dynamic profile type questions that Presenter 1 was telling us about. We can assume there is quite a time difference and students are allocated a time frame to complete. The student have been proctored using the Proctoring and secure browsing software (ProctorU) method Presenter 2 described”*
- **Probe 1:** In the context of collusion, what do you think is the difference between a banking system, where you are preventing access and an examination system, where you preventing access?
- **Probe 2:** One of the things in the bank is that you want to keep people out. The whole point of bank security is that you don’t want people in. Is that the same or do we need doing the same thing in online examinations to keep people out?
- **Probe 3:** With the challenge question approach (PBA), you do get challenged, so you could be challenged frequently, it ask you questions anytime based on your dynamic profile, of what you have learnt. In dynamic profile,

there could be lots of information and they could ask you randomly anything from your dynamic profile. Does that make it more secure you think?

- **Probe 4:** There is always a possibility that you will get someone to sit next to you at a remote location who is the expert, how do you prevent that, how do you stop people from that. Do you think ProctorU (secure browser + remote proctor) would help?
- **Probe 5:** I would imagine the trick would be to prevent people sitting next to you and doing the thing with and I think that is the biggest problem. I think passing information between two locations like giving a password, the dynamic profile questions (PBA) approach completely destroys that one, because there is so much possibly randomly generated questions that we ask, that you have to keep on passing on that information, so the challenge questions prevents that. The remote proctoring possibility sorts out the person sitting next to you to some extent anyway. Do you think with those two together we could achieve a satisfactory level of confidence?
- **Probe 6:** Can I ask you all everyone with a question to answer yes or no. Supposing we have got a high stake examination say worth about 25% of the course, your own courses now, that the examination you are looking at, you have got the challenge questions (PBA) method and Secure browser + Remote Proctor (ProctorU) together, and you designed the course so it deters collusion as much as you possibly can. Would you be prepared to do that examination now with this system? And you considered the challenge questions from the course work (Dynamic profile questions)

Appendix E – Dynamic Profile Questions Study 6

E –I Study 6 Course Design:

Below is an overview of a three weeks online course:

Week 1

- Let us know about you
- Introduction
- PHP Installation (XAMPP Installation)
- My first PHP page
- PHP Strings and Variables
- Conditional statements
- PHP switch statement
- PHP Arrays
- Project Assignment Week 1 (Write one of the following PHP short programs)
    - Write a PHP program to assign your name to $myname and qualification to $qualification variables and display the output on page with on two separate lines.
    - Write a PHP program to assign any two numbers to two variables and display their sum on screen.
    - Write a PHP program to assign any number to a variable and display the value using pre-increment operator (++). Check PHP operators for help.
    - Write a PHP program to display your favourite fruit from the given choices Mango, Orange, Apple, Plum, and Cherry using a Switch statement.
    - Write a PHP program to Input three numbers n1, n2, and n3 and display the largest on screen?
    - Write a PHP program using an indexed array to store name of cars i.e. Honda, BMW, and Fiat and print them on screen.
    - Write a PHP program using associate array to store student's score i.e. student 1 20%, student 2 40%, student 3 87%, student 4 90% and display them on screen.
- Student Reflection –What have I learned in week 1?
- Week 1 Quiz

Week 2

- PHP Looping -While Loop
- PHP Looping -for Loop
- PHP functions
- PHP & HTML Forms Resource
- $_GET and $_POST methods
- Project Assignment Week 2 (Write one of the following PHP short programs)
    - Write a PHP program using compute and display table of 2 e.g. 2 x 1 =2 to the count of 10 using any of the Looping statements.
    - Using any of the PHP Looping, write a program to display 1-10 even numbers
    - Using a PHP for loop, display values of an array $i = array("BMW", "Honda", "Ford", "Mini");

- Student Reflection –What have I learned about PHP Looping in week 2?
- Week 3 Quiz

Week 3

- MySQL
- PHP MySQL Database connection & insert form data
- Create database connection and get data from Db
- Practice lesson -Select and display data from database
- Where clause, update, delete from database
- Student Reflection –What have I learned about MySQL database functions in week 3
- Week 3 Quiz

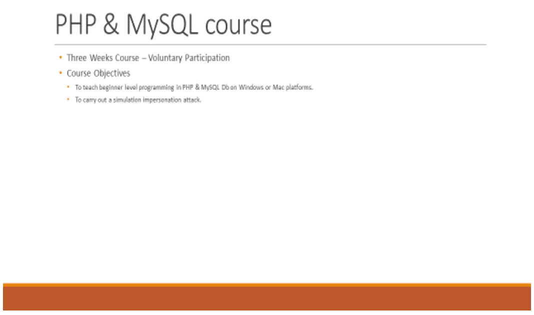
E –II Presentation:

Participants were presented the following slides during the face-to-face registration session.

PHP & MySQL course

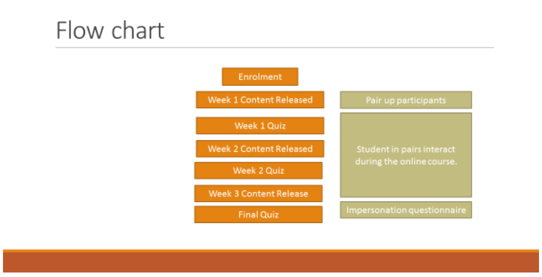
ABRAR ULLAH

PHD SCHOLAR – UNIVERSITY OF HERTFORDSHIRE



PHP & MySQL course

- Three Weeks Course – Voluntary Participation
- Course Objectives
  - To teach beginner level programming in PHP & MySQL Db on Windows or Mac platforms.
  - To carry out a simulation impersonation attack.



Flow chart

Enrolment

Week 1 Content Released

Week 1 Quiz

Week 2 Content Released

Week 2 Quiz

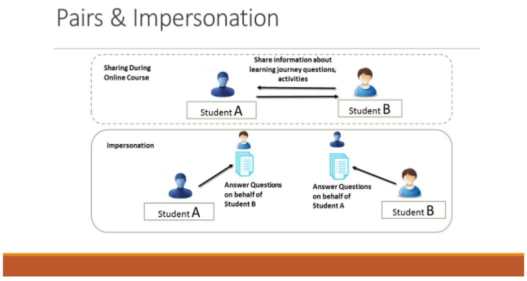
Week 3 Content Release

Final Quiz

Pair up participants

Student in pairs interact during the online course.

Impersonation questionnaire



Pairs & Impersonation

Sharing During Online Course

Share information about learning journey questions, activities

Student A

Student B

Impersonation

Student A

Answer Questions on behalf of Student B

Answer Questions on behalf of Student A

Student B

E –III Dynamic Profile Questions:

The following dynamic profile questions were implemented in study 6. These questions are associated with Introduction, Course Content, Assignments, Forums and Quizzes

Q.1 Which one of the following statements below were written by you?

1. Distraction statement
2. Distraction statement
3. Distraction statement
4. **Correct Answer**
5. None of the above

Q.2 Which one of the following statements below were written by you as a course objective?

6. Distraction statement
7. Distraction statement
8. Distraction statement
9. **Correct Answer**
10. None of the above

Q.3 Which of the following statements were written in your introduction email?

1. Distraction statement
2. **Correct Answer**
3. Distraction statement
4. Distraction statement
5. None of the above

Q.4 Which one of the following course materials were completed by you in week 1?

1. **Correct Answer**
2. Distraction statement
3. Distraction statement
4. Distraction statement
5. None of the above

Q.5 Your score for the week 1 quiz was:

1. Less than 40%
2. Within the 40% -69% Range
3. Within the 80%-89% range
4. Within the 70%-79% range
5. Within the 90%-100% range

Q.6 Which one of the following assignments have you submitted in week 1?

1. Distraction statement
2. Distraction statement
3. Distraction statement
4. **Correct Answer**
5. None of the above

Q.7 Which one of the following assignments have you submitted in week 1?

1. Distraction statement
2. Distraction statement
3. **Correct Answer**
4. Distraction statement
5. None of the above

Q.8 Which one of the following PHP code belongs to your assignment 1?

1. **Correct Answer**
2. Distraction statement
3. Distraction statement
4. Distraction statement
5. None of the above

Q.9 Your score for the assignment 1 was:

1. Less than 40%
2. Within the 40% -69% Range
3. Within the 80%-89% range
4. Within the 70%-79% range
5. Within the 90%-100% range

Q.10 Which one of the following reflection posts were made by you?

1. Distraction statement
2. Distraction statement
3. **Correct Answer**
4. Distraction statement
5. None of the above

Code Review

Q.11 which one of the following is taken from your feedback to code review in week1?

1. Distraction statement
2. Distraction statement
3. **Correct Answer**
4. Distraction statement
5. None of the above

Q.12 which one of the following is taken from your feedback to code review in week2?

1. Distraction statement
2. Distraction statement
3. **Correct Answer**
4. Distraction statement
5. None of the above

Example Exercise

Q.13 which one of the code excerpt was shown in week1 examples?

```
<html>
<body>
          <?php print(“hello world!”); ?>
</body>
</html>
```

```
<html>
<body>
          <?php echo "Hello World"; ?> </body>
</html>
```

```
<html>
<body>
<?php
/* This is my first php page */
echo "This is my first PHP page";
?>
</body>
</html>
```

```
<?php
$str=”Example: My first php page”;
echo “My first php page”;
?>
```

None of the above

Q.14 which one of the following example code excerpt was shown in week1?

```
<?php
$a = 5; // global scope

function myTest()
{
echo $a; // local scope
}

myTest();
?>
```

```
    <?php
$var_str1 = "A variable with global scope"; // global scope

function variableTest()
{
$var_str2="This variable cannot be called outside this function";

echo $var_str2; //Local variable with local scope
echo "<br>";
echo $var_str1; // Local scope
}

variableTest();
?>
```

```
    <?php
    //variable with a global scope
$var1 = 5;

function exampleFunction()
{
  echo ‘variable with a local scope inside a function cannot be accessed outside the function’;
  echo $var2; // local scope
}

exampleFunction();
?>
```

```
    <?php
        $str=”Hello world”;
         $str_cnt=strlen($str);
          echo $str_cnt;
    ?>
```

None of the above

Q.15 which one of the following example code excerpt was shown in week1?

```
    <?php
$cars[0]="Saab";
$cars[1]="Volvo";
$cars[2]="BMW";
$cars[3]="Toyota";
echo $cars[0] . " and " . $cars[1] . " are Swedish cars.";
?>
```

```
    <?php
$num[0]=2;
$num[1]=8;
$num[2]=7;
$num[3]=6;
$num[4]=0;

echo $num[0] . ", " . $num[1] . " and ". $num[3] ." are even numbers.";
?>
```

```
    <?php
$color[0]=”Red”;
$color[1]=”Green”;
$color[2]=”Yellow”;
$color[3]=”Blue”;
$color[4]=”Magenta”;

echo $color[0] . ", " . $color[1] . " and ". $color[3] ." are core RGB colors.";
?>
```

```
    <?php
$score['Alex'] = "30";
$score['Quagmire'] = "80";
$score['Joe'] = "54";

echo "Final score of Alex is " . $score['Alex'] . ".";
?>
```

None of the above

Q.16 which one of the following example code excerpt was shown in week1?

```
    <?php
$num1=30;
$num2=40;

if ($num1 > $num2)
{
echo "$num1 is greater than $num2";
}
else
{
echo "$num2 is greater than $num1";
}
?>
```

```
    <?php
$d=date("D");
if ($d=="Fri")
{
echo "Have a nice weekend!";
}
else
{
echo "Have a nice day!";
}
?>
```

```
    <?php

$string1 = "cake";
$string2 = "foo";

if(!$string1==$string2)
{
echo "cake is a lie";
}
?>
```

```
    <?php
// alphabet comparison
  $a="C";
  $b="X";
  if ($a<$b)
    {
```

```
    echo $a."is smaller than".$b;
    }
// Result : C is smaller than X
?>
```

None of the above

Q.17 which one of the following example code excerpt was shown in week1?

```
    <?php
$x=1;
switch ($x)
{
case 1:
echo "Number 1";
break;
case 2:
echo "Number 2";
break;
case 3:
echo "Number 3";
break;
default:
echo "No number between 1 and 3";
}
?>
```

```
    <?php
$year=$_GET['year'];
      switch ($year) :
       case  0:
          echo  'Monkey';
             break;
       case  1:
          echo 'Rooster';
          break;
       case  2:
          echo 'Dog';
          break;
       case  3:
          echo 'Boar';
          break;
       case  4:
          echo 'Rat';
          break;
       case  5:
          echo 'Ox';
          break;
       case  6:
          echo 'Tiger';
          break;
       case  7:
```

```
      echo 'Rabit';
      break;
    case  8:
      echo 'Dragon';
      break;
    case  9:
      echo 'Snake';
      break;
    case 10:
      echo 'Horse';
      break;
    case 11:
      echo 'Lamb';
      break;
  }
  ?>
```

```
  <?php

$a = "abc";
$b = "def";

switch($c){
  case "a":
    echo "a";
    break;
  case "b":
    echo "b";
    break;
  default:
    echo "default";
    break;
}

?>
```

Will output default

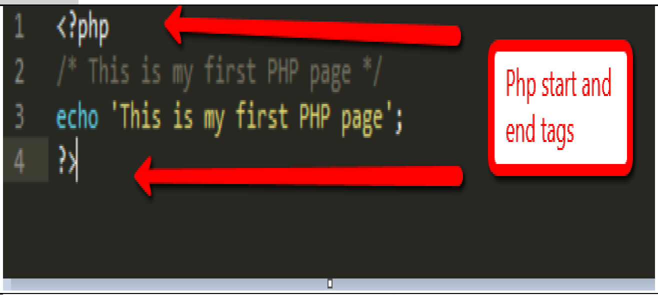
```
  <?php
  $destination = "Tokyo";
  echo "Traveling to $destination<br />";
  switch ($destination){
  case "Las Vegas":
      echo "Bring an extra $500";
      break;
  case "Amsterdam":
      echo "Bring an open mind";
      break;
  case "Egypt":
      echo "Bring 15 bottles of SPF 50 Sunscreen";
      break;
  case "Tokyo":
      echo "Bring lots of money";
```

```
        break;
case "Caribbean Islands":
        echo "Bring a swimsuit";
        break;
}
?>
```

None of the above

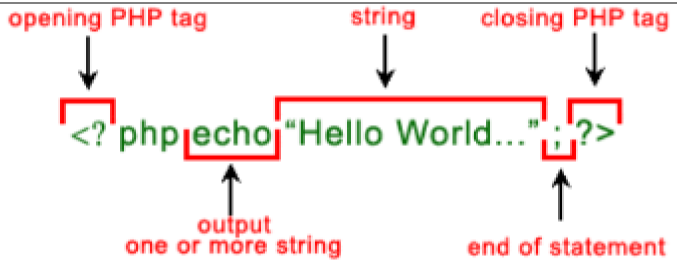
Info Graphics

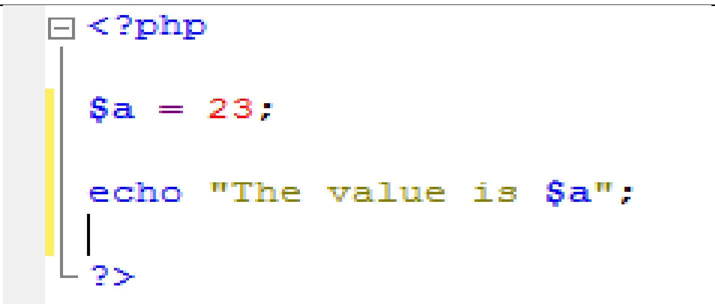
Q. 18 which one of the following images/infographics have you seen in the course content?



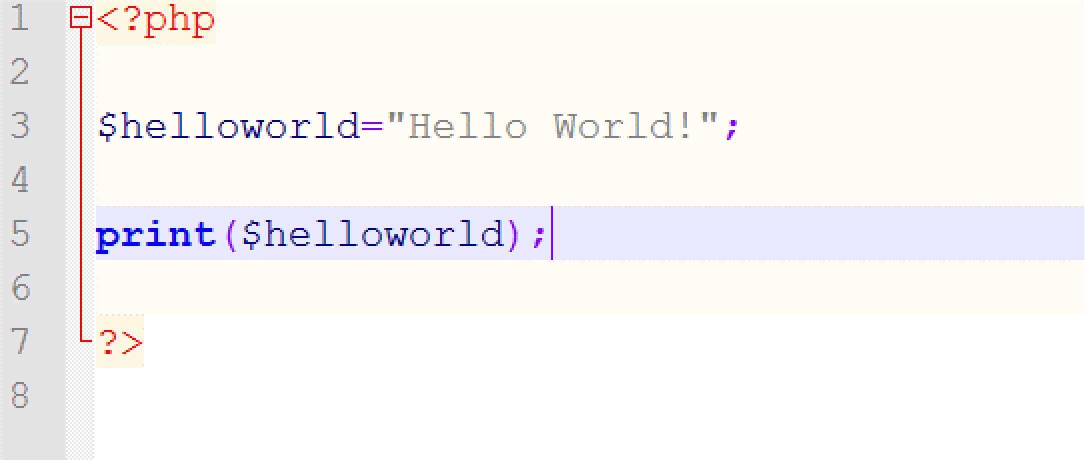
```
<?php
/* This is my first PHP page */
echo 'This is my first PHP page';
?>
```

Php start and end tags





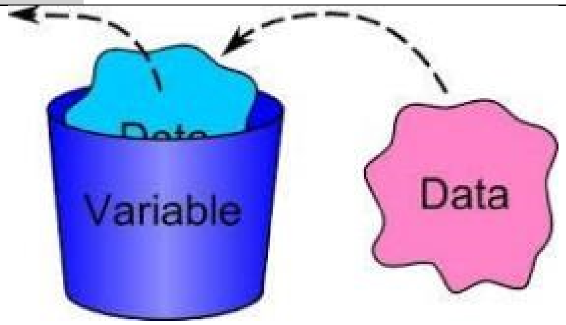
```
<?php

$a = 23;

echo "The value is $a";

?>
```

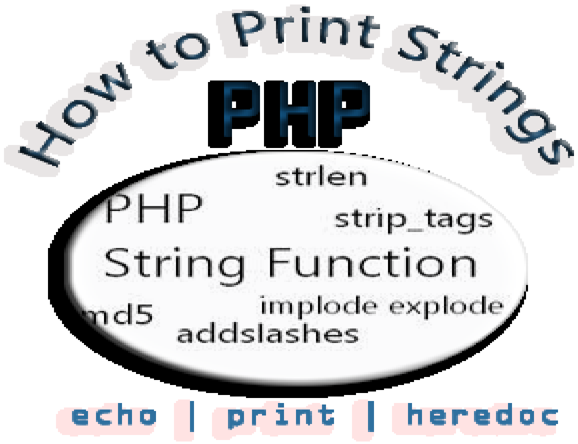


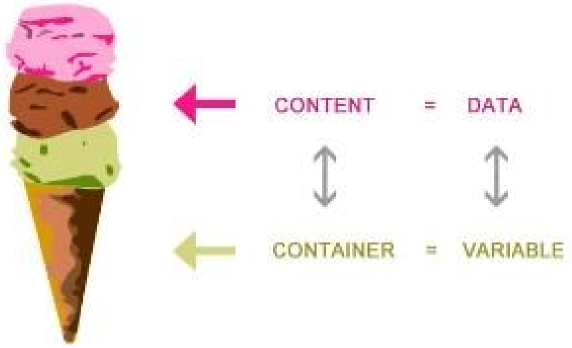
```
<?php

$helloworld="Hello World!";

print($helloworld);

?>

```

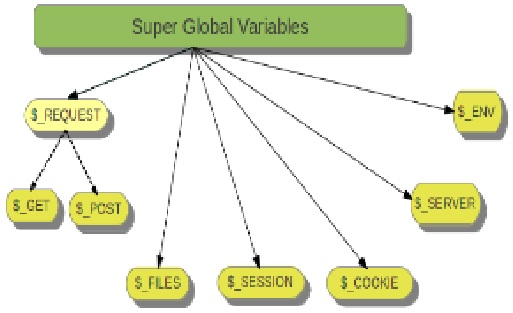
None of the above

Q. 19 which one of the following images/infographics have you seen in the course content?



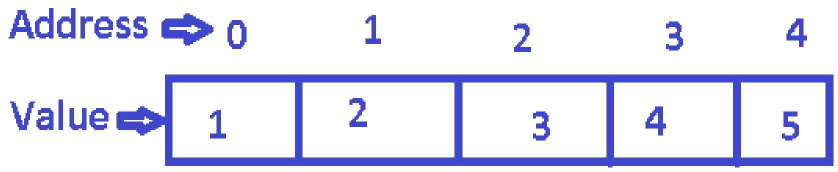


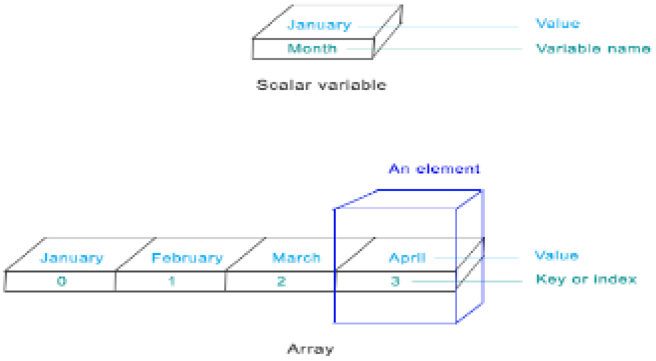


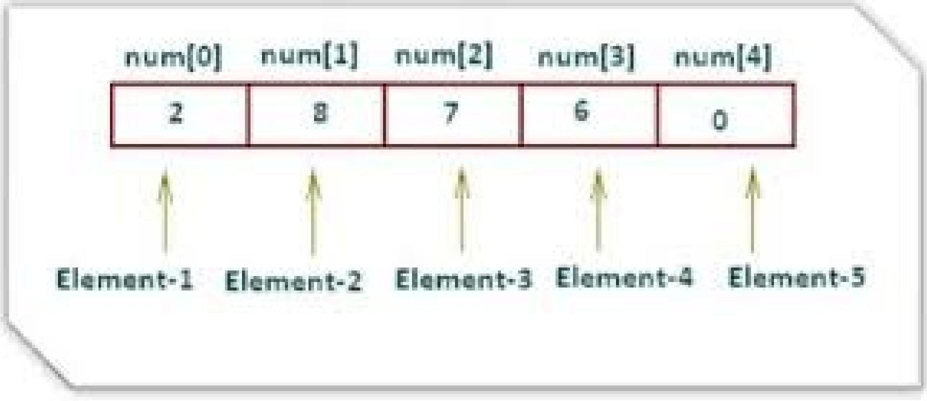


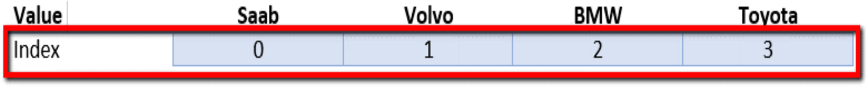
None of the above

Q. 20 which one of the following image have you seen in the course content?





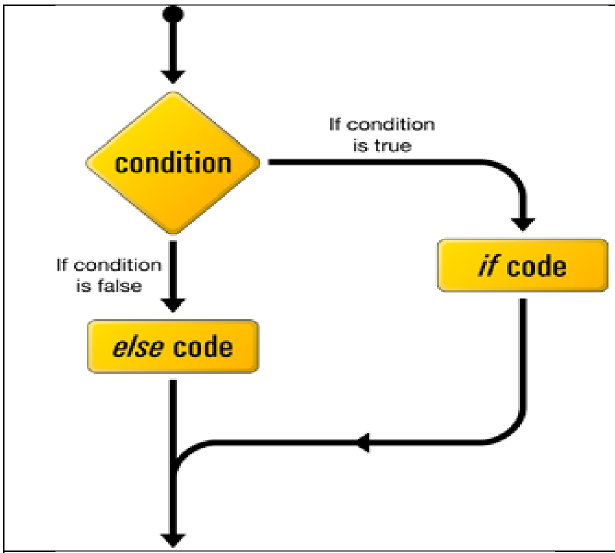


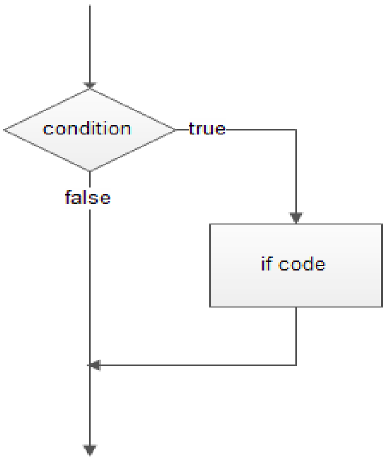


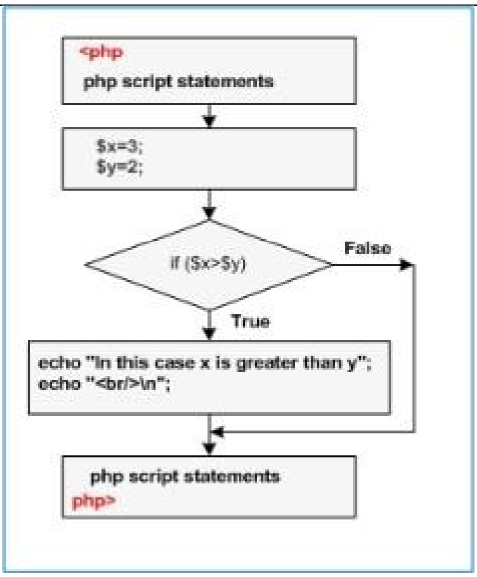
Value	Saab	Volvo	BMW	Toyota
Index	0	1	2	3

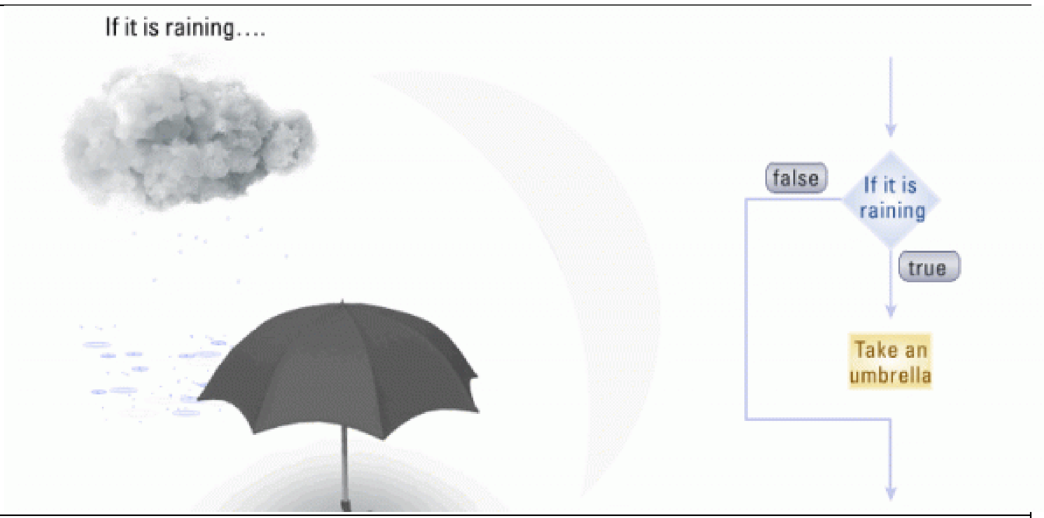
None of the above

Q. 21 Which one of the following image have you seen in the course content?


condition
If condition is true
if code
If condition is false
else code

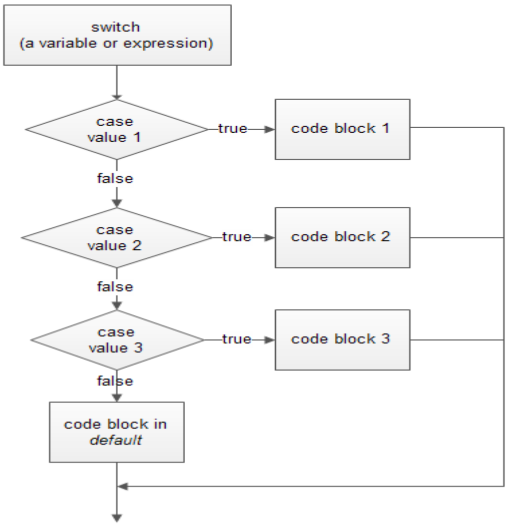

condition
true
false
if code

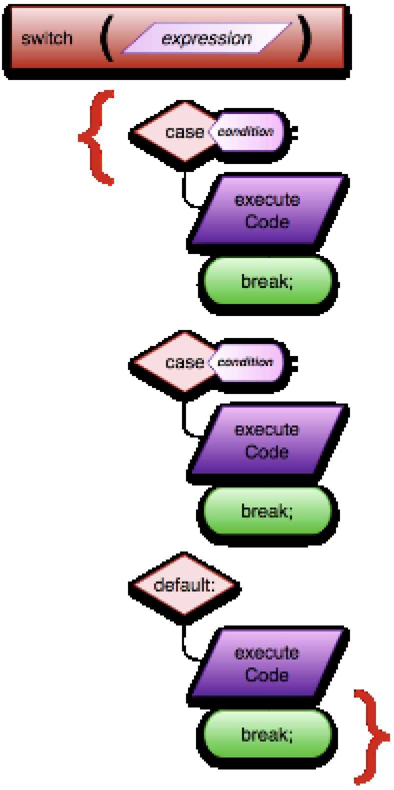

<php
php script statements
$x=3;
$y=2;
if ($x>$y)
False
True
echo "In this case x is greater than y";
echo "<br/>\n";
php script statements
php>



None of the above

Q. 22 which one of the following image have you seen in course content?





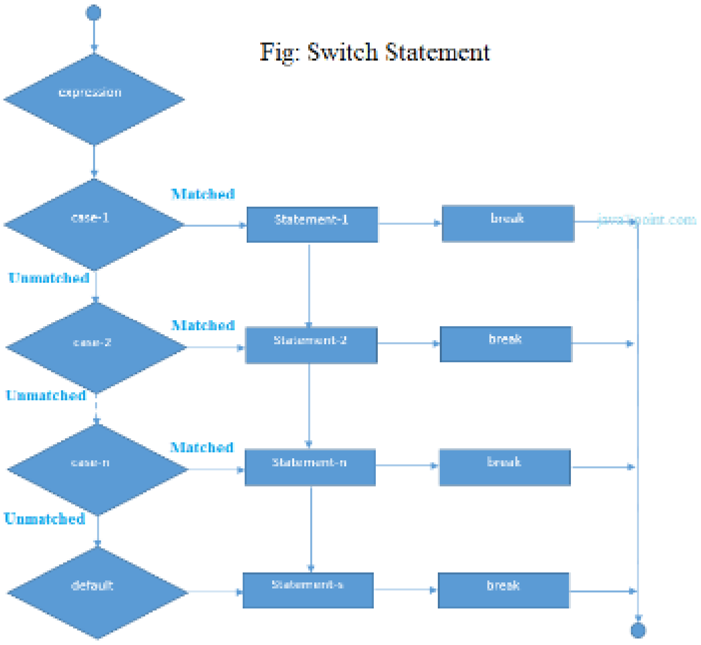
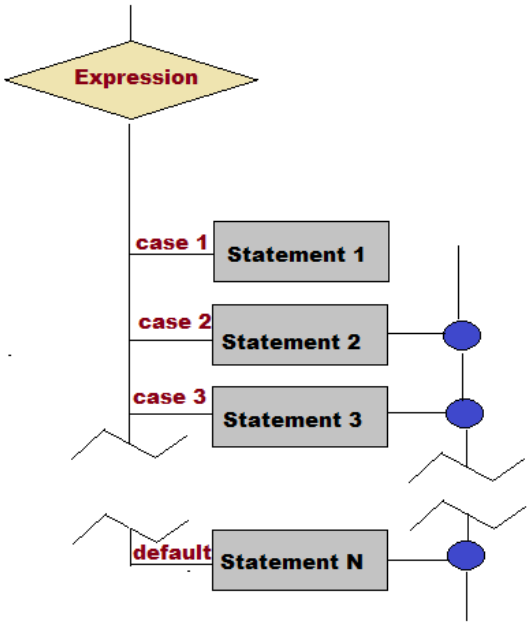
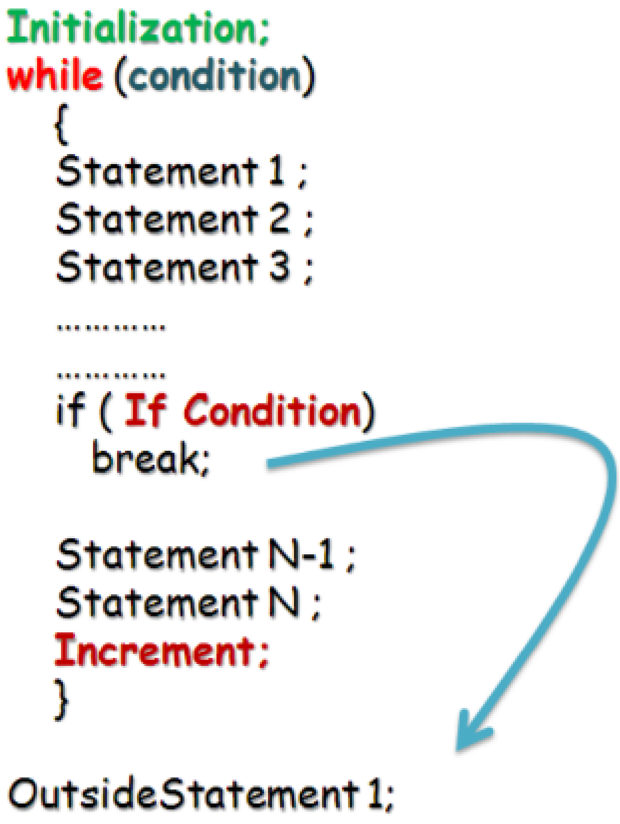


Fig: Switch Statement

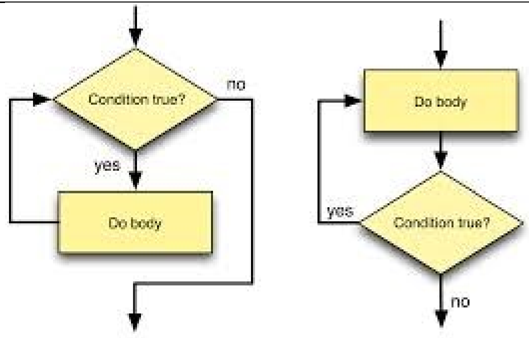


None of the above

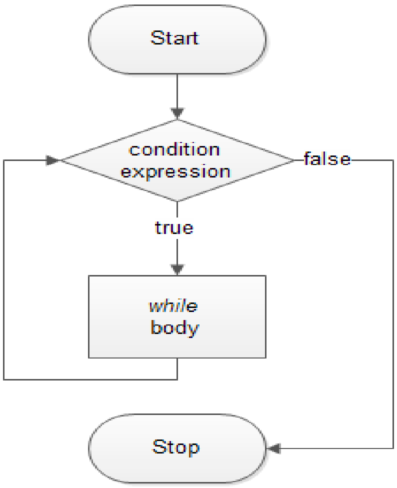
Q. 23 which one of the following image have you seen in course content?

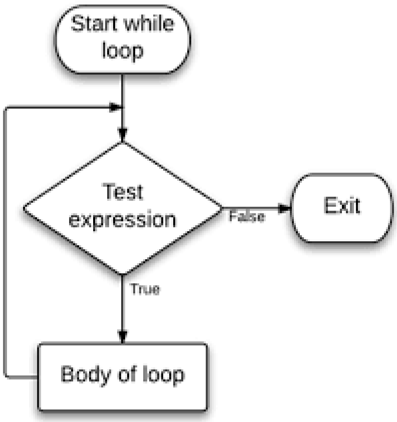


```
Initialization;
while (condition)
   {
   Statement 1 ;
   Statement 2 ;
   Statement 3 ;
   …………
   …………
   if ( If Condition)
     break;

   Statement N-1 ;
   Statement N ;
   Increment;
   }

OutsideStatement 1;
```

<table>
<tr><td>


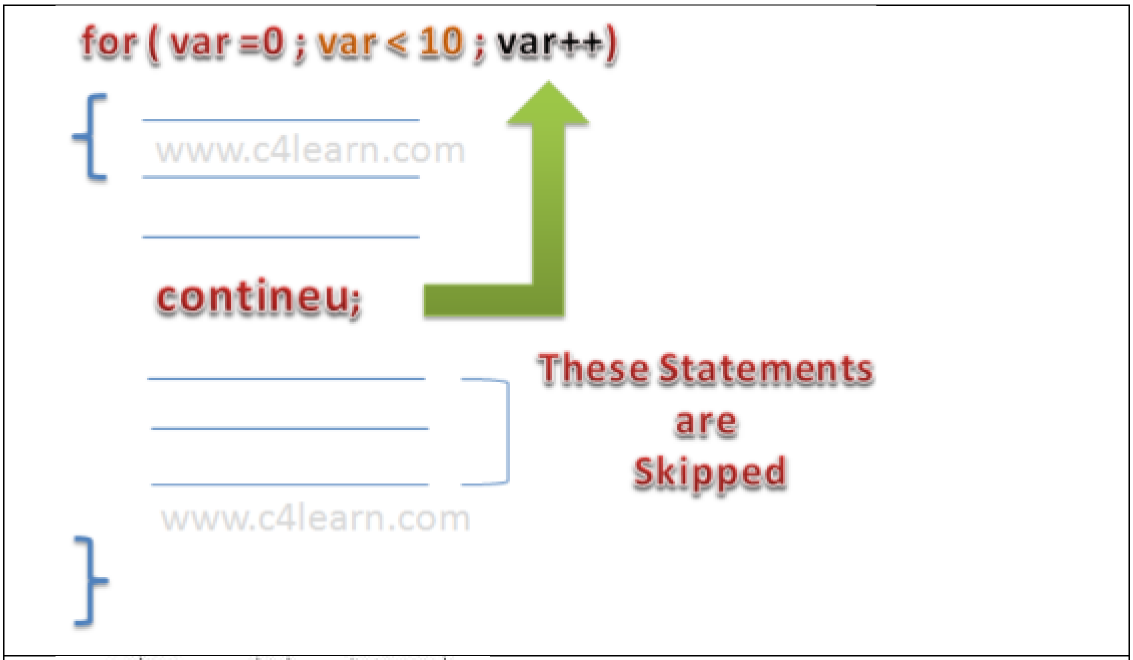
while flowchart

do/while flowchart
</td></tr>
<tr><td>


</td></tr>
<tr><td>


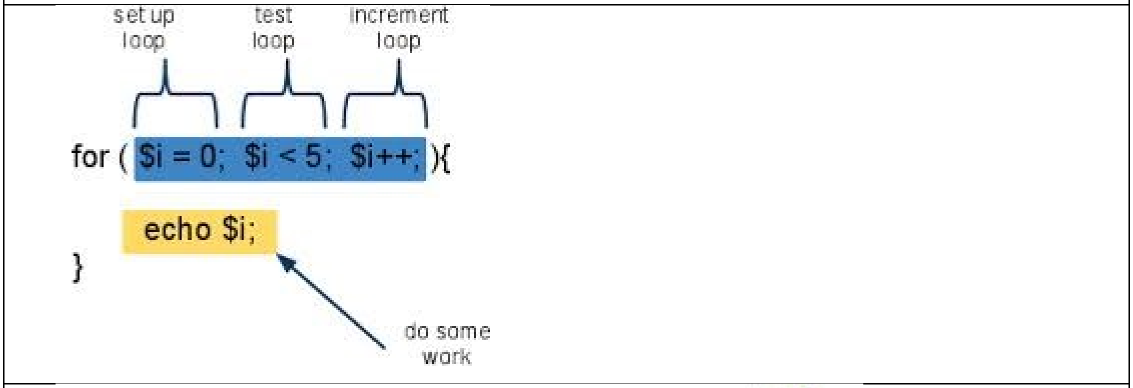
</td></tr>
<tr><td>None of the above</td></tr>
</table>

Q. 24 which one of the following image have you seen in course content?

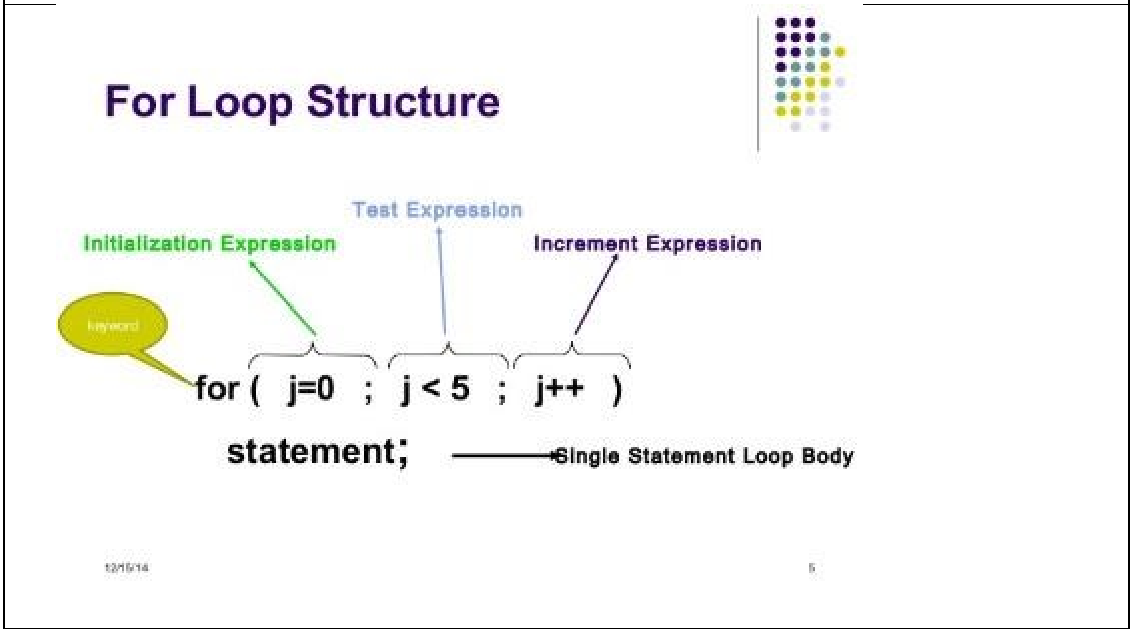


```
for ( var =0 ; var < 10 ; var++)
{
    contineu;
}
```

These Statements are Skipped



```
for ( $i = 0;  $i < 5;  $i++; ){
    echo $i;
}
```

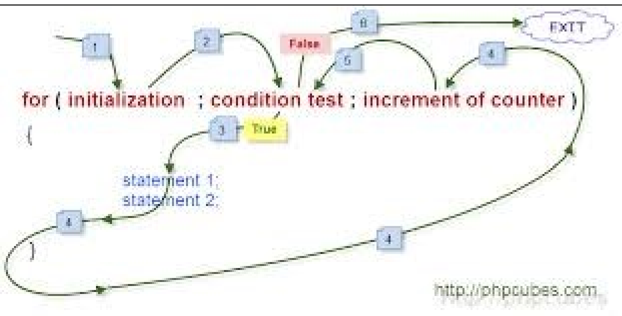


For Loop Structure

```
for (  j=0  ;  j < 5  ;  j++  )
    statement;
```

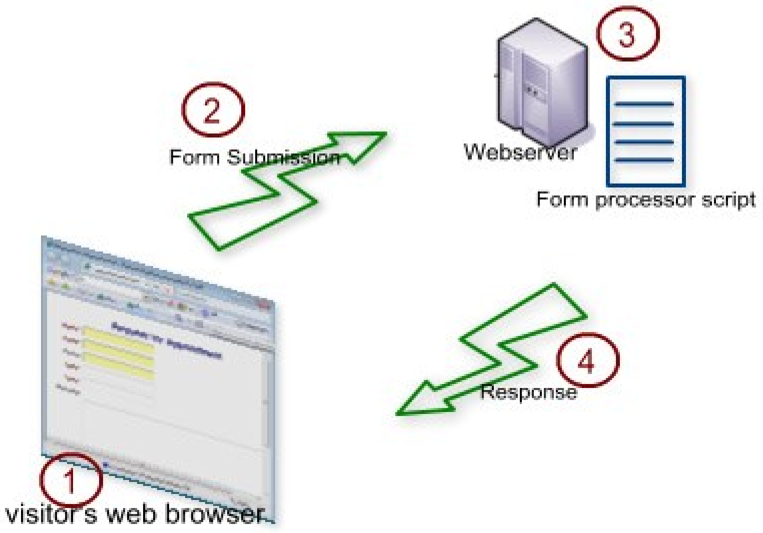
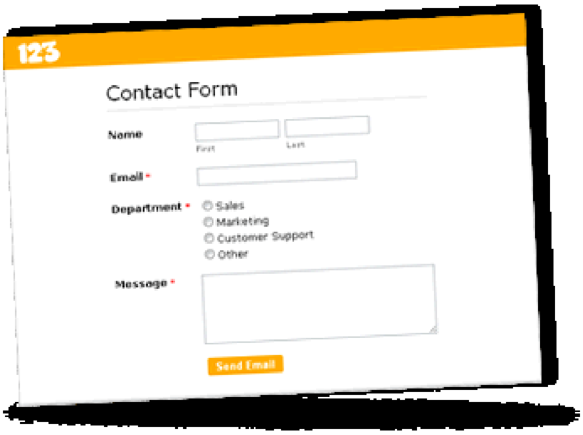
12/15/14

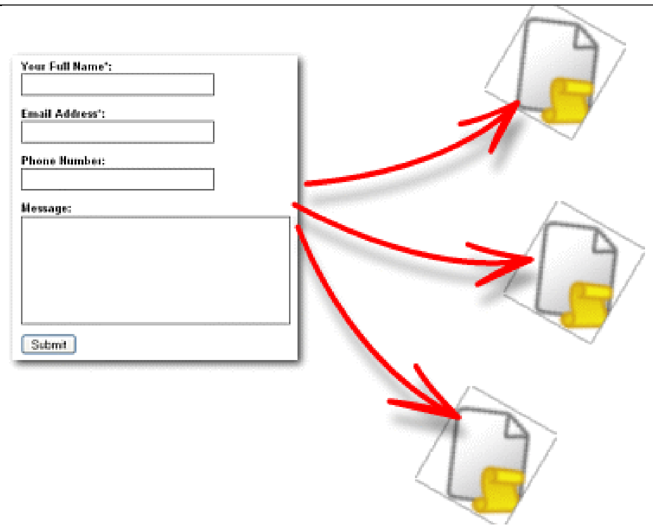
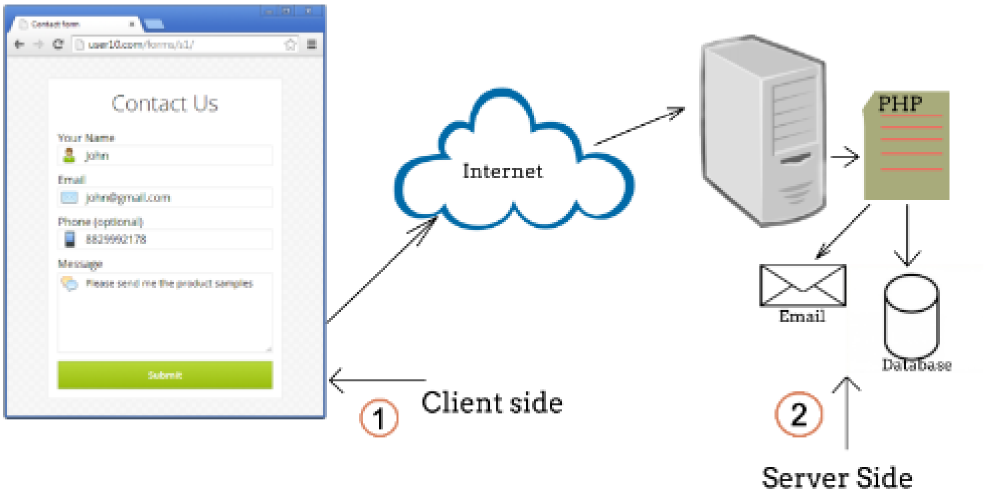
5

 1
2
False
6
EXIT
5
4
for (initialization ; condition test ; increment of counter)
{
3
True
statement 1;
statement 2;
4
}
4
http://phpcubes.com

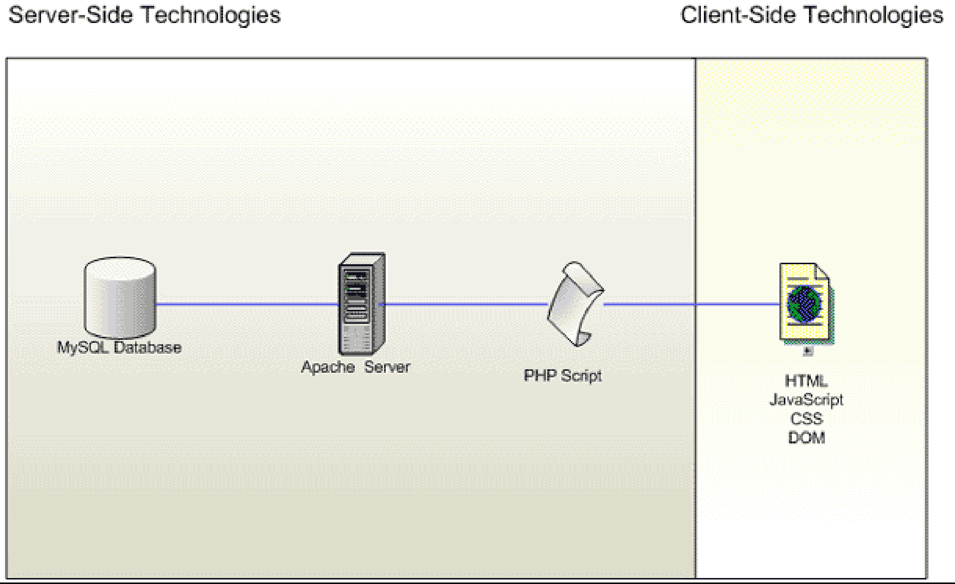
None of the above

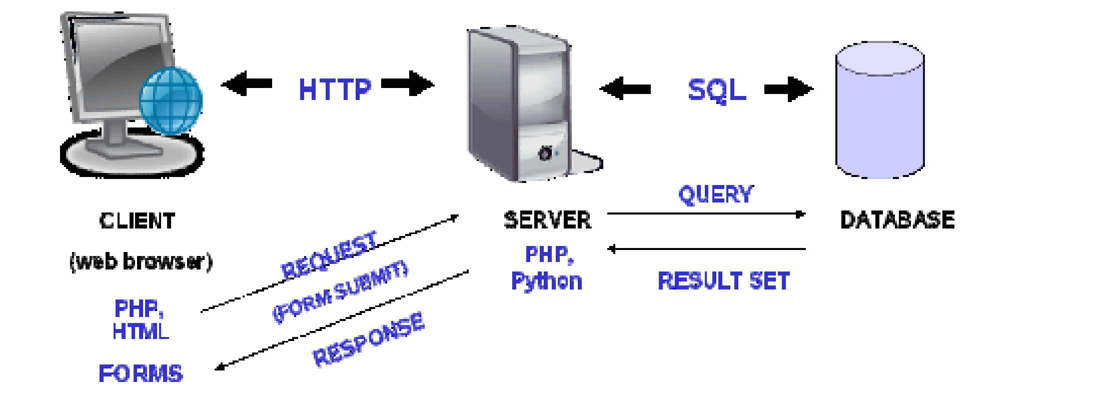
Q. 25 which one of the following image have you seen in course content?

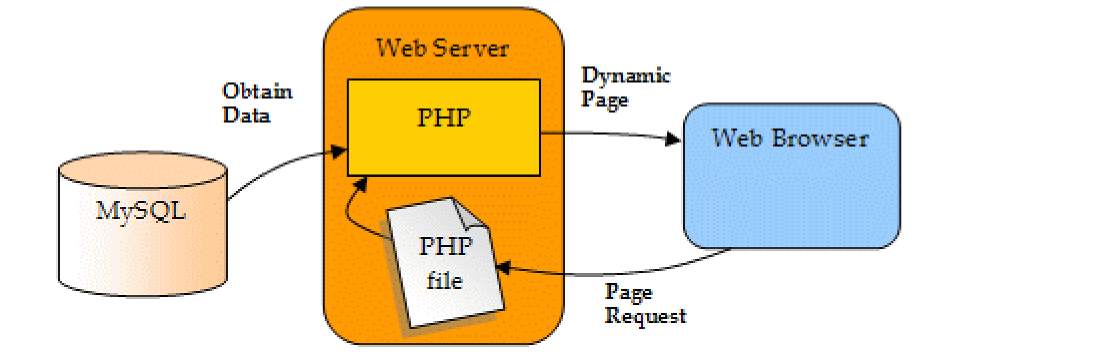
 2 Form Submission Webserver 3 Form processor script 4 Response 1 visitor's web browser
123 Contact Form Name First Last Email * Department * ○ Sales ○ Marketing ○ Customer Support ○ Other Message * Send Email

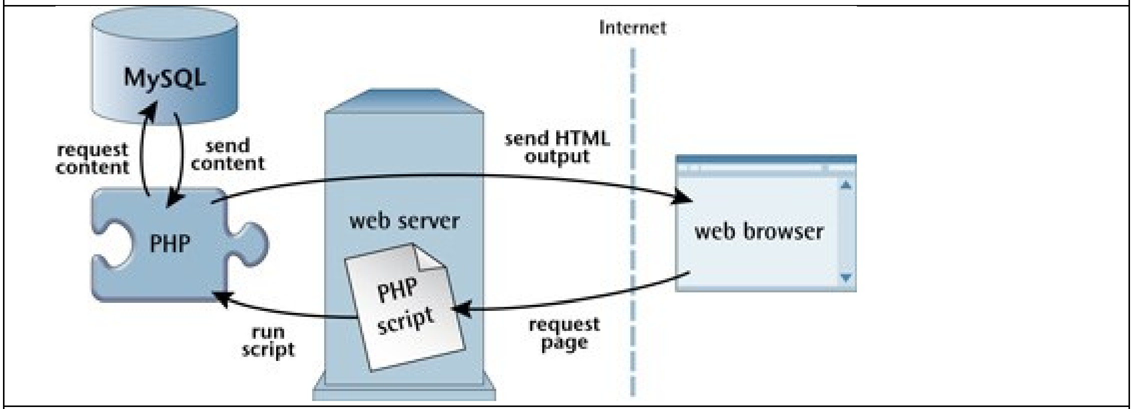
 Your Full Name*: Email Address*: Phone Number: Message: Submit
 Contact Us Your Name: John Email: john@gmail.com Phone (optional): 8829992178 Message: Please send me the product samples user10.com/forms/s1/ Submit Internet PHP Email Database 1 Client side 2 Server Side
None of the above

Q. 26 which one of the following image have you seen in course content?

 Server-Side Technologies Client-Side Technologies MySQL Database Apache Server PHP Script HTML JavaScript CSS DOM







None of the above

Information Collected using choice activity

Q.27 how do you describe your PHP skills before starting this course?

- No prior knowledge of PHP
- Basic knowledge of PHP
- Beginner level programming skills in PHP
- Intermediate level programming skills in PHP
- None of the above

Q. 28 which one of the following PHP environment have you used?

- XAMP
- WAMP
- MAMP
- LAMP
- None of the above

Appendix F – Research publications

The research work reported in this thesis resulted in publication of journal and conference papers. These are listed below:

No	Article /Paper Title
1	**Profile-based Student Authentication in Online Examination (Ullah et al., 2012a), i-society 2012, London UK (IEEE), June-2012**

Abstract: Online examination is an increasingly important component of online courses, and student authentication is widely seen as one of the major concerns for online examinations. In most online examination scenarios, face-to-face supervision is absent, and students may attempt to use third party to increase their scores. This paper aims to investigate authentication challenges to online examinations, review benefits and constraints of existing authentication traits, and discuss alternative techniques. We propose the use of profile-based authentication framework (PBAF) together with a user-id and password for the authentication of students during online examinations. The proposed solution utilizes profile-based challenge questions, which is verified by development of PBAF in a virtual learning environment.

2	**Using Challenge Questions for Student Authentication in Online Examination (Ullah et al., 2012c), International Journal for Infonomics (IJI), Sept-2012**

Abstract: With the growth of Internet and technology in the past decade, online learning has become increasingly popular and evolved. Online examination is an integral and vital component of online learning. Student assessment in online learning is largely submitted remotely without any face-to-face interaction and therefore, student authentication is widely seen as one of the major challenges. This study aims to investigate potential threats to student authentication in the online examinations and analysing the benefits and limitations of the existing authentication approaches. We propose the use of challenge questions for student authentication in the online examinations. For this purpose, we designed a profile-based authentication framework (PBAF) together with a user-id and password for the authentication of students during online examinations, utilizing a cohort of personal and academic questions as challenge questions. We conducted an empirical study on a group of online students from local and overseas Universities. The result shows the impact of questions type on the usability, in particular the amount of time taken by the introduction of the proposed approach. We also conducted a post experiment survey to collect student feedback on the proposed technique.

3	**Usability of Profile-based Student Authentication and Traffic Light System in Online Examination (Ullah et al., 2012b)** **The 7th International Conference for Internet Technology and Secured Transactions, London UK (IEEE) Dec-2012**

Abstract: There has been an increased interest in effective approaches to student authentication, given that online examinations are a crucial component of online learning. The work presented here, is part of an ongoing programme of research on the extent to which challenge questions are an effective approach to student authentication in online examination contexts, where face-to-face invigilation is not in use.

Although the use of challenge questions shows great potential, there are some concerns about its usability in particular relating to memorability. This paper summarizes the findings of an empirical study in which, 23 participants used a framework developed by the authors namely “Profile Based Authentication Framework” (PBAF). Findings from the empirical study suggests that memorability, questions clarity, varied writing syntax and case variation can cause usability issues leading to failed authentication. A traffic light scheme was implemented to improve the usability of challenge questions for online examination authentication

4	**Design, privacy and authentication of challenge questions in online examinations (Ullah et al., 2013)** **IEEE Conference on e-Learning, e-Management and and e-Services (IC3e), Kuching, Malaysia, Dec- 2013**

Abstract: Online examination is an essential part of the online learning and secure authentication is considered vital for the success of online learning. This study is part of an ongoing research on student authentication approaches and the use of challenge questions in online examination authentication. This paper presents the results of an empirical study based on “Profile Based Authentication Framework” (PBAF), which uses challenge questions for student authentication in online examination. The PBAF uses challenge questions related to personal, academic and professional information. These questions inform the usability, security and privacy of PBAF authentication approach. The results presented here summarizes the impact of questions design on the usability based on data collected from challenge questions authentication and a post-experiment survey on the data privacy.

5	**Evaluating security and usability of profile-based challenge questions authentication in online examinations (Ullah et al., 2014a)** **Journal of Internet and Services Appllications (Spriner), Mar- 2014**

Abstract: Student authentication in online learning environments is an increasingly challenging issue due to the inherent absence of physical interaction with online users and the potential security threats to online examinations. This study is part of ongoing research on student authentication in online examinations evaluating the potential benefits of using challenge questions. The authors developed a Profile Based Authentication Framework (PBAF), which utilises challenge questions for students' authentication in online examinations. This paper examines the findings of an empirical study in which 23 participants used the PBAF including an abuse case security analysis of the PBAF approach. The overall usability analysis suggests that PBAF is efficient, effective and usable. However, specific questions need replacement with suitable alternatives due to usability challenges. The results of the current research study suggest that memorability, clarity of questions, syntactic variation and question relevance can cause usability issues leading to authentication failure. A configurable traffic light system was designed and implemented to improve the usability of challenge questions. The security analysis indicates that PBAF is resistant to informed guessing in general, however, specific questions were identified with security issues. The security analysis identifies challenge questions with potential risks of informed guessing by friends and colleagues. The usability, security and traffic light system in a real online course needs further analysis on different settings. The study was performed on a small number of participants in a simulation online course and the results need to be verified in a real world environment on a larger sample size.

6	**Privacy and Usability of Image and Text Based Challenge Questions Authentication in Online Examinations (Ullah et al., 2014c)** **The International Conference on Education Technologies and Computers (IEEE), Sept- 2014**

Abstract: In many online examinations, physical invigilation is often replaced with traditional authentication approaches for student identification. Secure and usable authentication approaches are important for high stake online examinations. A Profile Based Authentication Framework (PBAF) was developed and implemented in a real online learning course embedded with summative online examination. Based on users' experience of using the PBAF in an online course, online questionnaires were used to collect participants' feedback on effectiveness, layout and appearance, user satisfaction, distraction and privacy concerns. Based on overall findings of the quantitative analysis, there was a positive feedback on the use of a hybrid approach utilizing image and text based challenge questions for better usability. However, the number of questions presented during learning and examination processes were reported to be too many and caused distraction. Participants expressed a degree of concern on sharing personal and academic information with little or no privacy concern on using favourite questions ($p < 0.01$).

7 **Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations (Ullah et al., 2014b)**
The 9th International Conference for Internet Technology and Secured Transactions, London UK, Dec -2014

Abstract: In traditional online examination environments, physical interaction is often replaced with authentication mechanisms. The absence of face-to-face interaction increases the number of authentication challenges. The authors developed and implemented a Profile Based Authentication Framework (PBAF) with the aim to integrate learning and examination processes for secure online examinations. The PBAF approach utilizes the widely used knowledge-based authentication mechanisms: login identifier and passwords and challenge questions. These approaches are reported with a number of benefits and limitations in term of usability and security. Previous studies suggests that the use of image-based graphical authentication may provide usable and secure solution. This paper presents the findings of an empirical study, utilizing a hybrid approach combining image and text-based challenge questions in a real online learning environment. A traffic light system was implemented to improve usability of the PBAF. The traffic light system relaxed authentication constraints for a significant number of users' attempts which would otherwise be penalized ($p< 0.01$). An abuse case scenario was designed to assess the security of the PBAF method against impersonation attack. The number of participants in abuse case scenario was small, however, results demonstrate that participants were able to share both text-based and image-based questions for impersonation attack.

8	**Usability of Activity-Based and Image-Based Challenge Questions in Online Student Authentication (Ullah et al., 2015)** **Human Aspects of Information Security, Privacy and Trust, Aug-2015**

Abstract: There has been a renewed interest in secure authentication of students in online examinations. Online examinations are important and high stake assets in the context of remote online learning. The logistical challenges and absence of live invigilation in remote un-supervised online examination makes the identification and authentication process extremely difficult. The authors implemented pre-defined text-based challenge questions for student authentication in online examination using a Profile Based Authentication Framework (PBAF) approach. The pre-defined questions require students to register their answers, which causes distraction and usability challenges. In this study, a non-invasive activity-based learning journey questions approach was implemented combined with the image-based questions, using the PBAF approach. Findings of the study shows significant difference in the efficiency of activity-based and image-based questions during the learning process ($p < 0.01$). There was no significant difference in the accuracy of multiple-choice image-based and activity-based questions ($p > 0.01$). There was a significant difference in the accuracy of activity-based questions and activity-date questions ($p < 0.01$).

9	**A Classification of Threats to Remote Online Examinations** **The 7th IEEE Annual Information Technology, Electronics and Mobile Communication Conference, Oct-2016**

Abstract: Summative online examinations are important assets in online learning environments. There are rising concerns from different stakeholders to the integrity of high stake examinations. Cheating has been one of the main concerns due to remote authentication of students in online environments. The absence of face-to-face interaction, monitoring or invigilation emerged new types of security threats. These threats include intrusion by hackers to collusion and plagiarism by students. This paper is based on a survey of literature to present a threats classification using security abuse case scenarios. Collusion in online examinations has emerged as one of the challenging threats. In a collusion, a student invites a third party helper or contractor to impersonate or aid a student to complete the online test. While mitigation of all types of threats is important, the risk of collusion is increasingly challenging because it is difficult to detect, when a legitimate student involves a third party collaborator to cheat in an online test.