Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations

Nasser S. Abouzakhar
School of Computer Science, College Lane, University of Hertfordshire, Hatfield, UK
N.Abouzakhar@herts.ac.uk

Abstract: Most of current industries and their critical infrastructure rely heavily on the Internet for everything. The increase in the online services and operations for various industries has led to an increase in different security threats and malicious activities. In US, the department of homeland security reported recently that there have been 200 attacks on core critical infrastructures in the transportation, energy, and communication industries (Erwin et al., 2012). This paper is concerned with the growing dependence of modern society on the Internet, which has become an ideal channel and vital source of malicious activities and various security threats. These threats could have an impact on different distributed systems within and across all the critical infrastructures, such as industrial networks, financial online systems and services, nuclear power generation and control systems, airlines and railway traffic controllers, satellite communication networks, national healthcare information systems … etc. The major problem is that the existing Internet mechanisms and protocols are not appropriately designed to deal with such recently developed problems. Therefore, a rigorous research is required to develop security approaches and technologies that are capable of responding to this new evolving context. This paper presents various security threats and incidents over the past recent years on different critical infrastructure domains. It introduces some security measures including vulnerability assessment and penetration testing approaches for critical infrastructure.

Keywords: Critical infrastructure protection, cyber security, security threats and violations

1. Introduction

Critical infrastructure cyber security is concerned with the protection and response to malicious activities that involve the critical infrastructure of a particular country. It is about the protection of electronic systems from malicious electronic attack and the means of dealing with such attacks. Critical infrastructure cyber security comprises technical, operational and managerial activities, and relates to the application processes, electronic systems and to the information stored and processed by such systems. During recent years the context of cyber security threats to critical infrastructure has changed dramatically as the Web and Internet technologies have driven the global expansion. In Europe, the European Programme for Critical Infrastructure Protection (EPCIP) is concerned with the protection of critical infrastructure in the EU. The EPCIP developed a procedure for identifying and designating European Critical Infrastructure (ECI), which is implemented by the European Commission's directive EU COM (2006) 786. This directive indicates that European critical infrastructure represents a situation that in case of a security incident or violation, which may affect a hosted country and at least one other European Member State.

Critical infrastructure systems are increasingly being targeted by attackers. This is due to the fact that most of such systems rely on weak security mechanisms. Cyber security threats include such issues as energy and power generation failures, online banking systems malfunction, transportation accidents, and hazardous material accidents. Figure 1 shows different infrastructure that were commonly referred to as "critical". In December 2011, the FBI's cyber division released the news that the infrastructure systems of three US cities have been attacked. FBI reported that hackers hit key services and had accessed crucial water and power services (BBC News, 2011)

"We just had a circumstance where we had three cities, one of them a major city within the US, where you had several hackers that had made their way into SCADA systems within the city." and "Essentially it was an ego trip for the hacker because he had control of that city's system and he could dump raw sewage into the lake, he could shut down the power plant at the mall - a wide array of things"

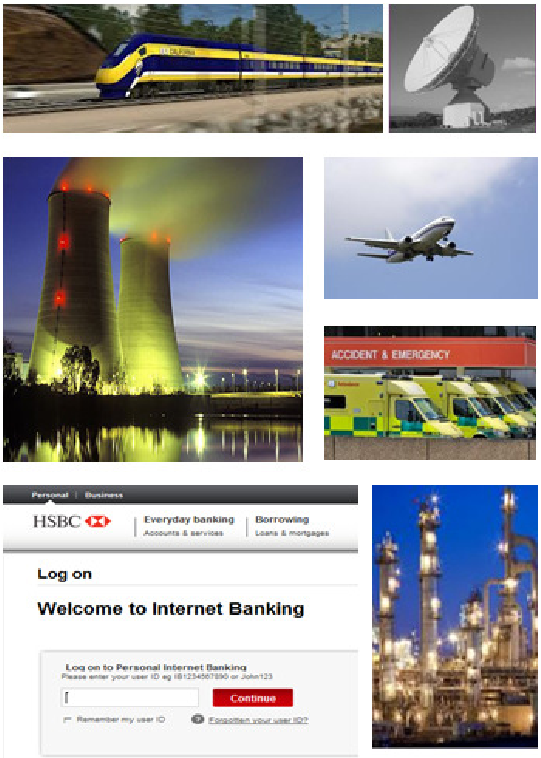


Figure 1: Examples of Critical Infrastructure

In 2010, another major security violation incident took place that was the spread of Stuxnet malware. Stuxnet is a complex piece of malware believed to be the first to target a real critical infrastructure such as nuclear power station. It is considered as one of the most sophisticated worms ever detected that uses six different methods that allowed it to spread (Fildes, 2010). Unlike most malware, Stuxnet aims to target specific industrial control systems that are traditionally not connected to the internet for security reasons using USB keys. It is designed to spy on and reprogram industrial control systems and to seek out a specific configuration of Siemens made SCADA (Supervisory Control and Data Acquisition) systems. Once SCADA system is hijacked by Stuxnet, the worm can reprogram PLC (Programmable Logic Controller) to give new instructions to linked machine. This is to cause damage to motors used in uranium-enrichment centrifuges. The PLC is an electronic device that generates control signals, for example, it monitors temperature and turn on coolers if a gauge exceeds a certain temperature as part of an industrial process. Stuxnet is able to inject code into the ladder logic of PLCs, monitor Profibus protocol and then manipulates the operations of the PLC to interrupt processes and modify output (Knapp, 2011). Stuxnet is a kind of malware that cannot be detected until it has been deployed and it infects parts of the control system that is uneasy to monitor. Therefore, security professionals need to change their perception and attitude toward critical infrastructure security to be able to deal with such malicious incidents (Symantec, 2010).

In 2010, Symantec carried out a critical infrastructure protection study. This study included 1,580 private businesses that are involved in industries that are considered providers of critical infrastructure services. The respondents are companies from 15 countries worldwide, with median company had between 1,000 and 2,499 employees. Figure 2 shows the results of one of the companies' responses to a question about the company's experience with four different types of attacks (Symantec, 2010). The results show that average of only 29% were completely sure these attacks never happened in their companies. The rest i.e. about 71% were either not completely sure, suspect or pretty sure that those attacks have happened to their companies. Such statistics indicate that there is a lot of work needs to be done by all parties involved including management, security professionals, governments … etc. to improve the situation.

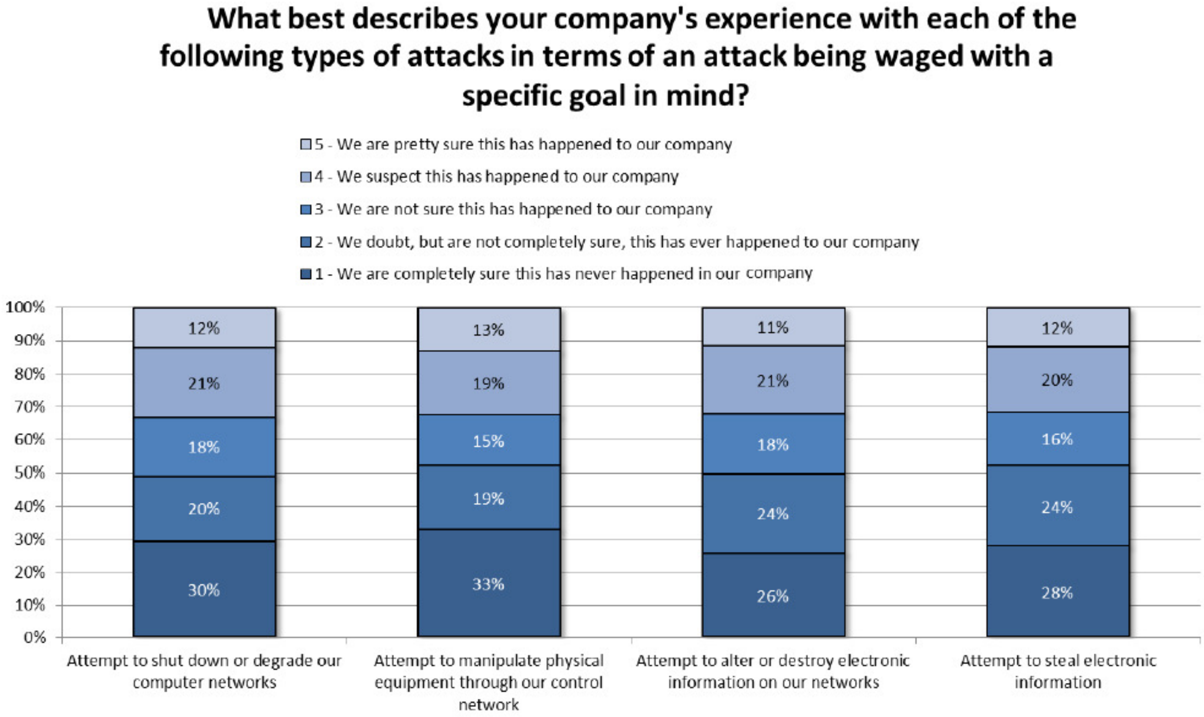


Figure 2: Symantec Survey of Critical Infrastructure based Companies in 2010

Security experts predict that there will be an increase in such attacks and malicious activities due to lack of knowledge about cyber security threats and lack of proper security measures. Therefore, proper cyber security training and intelligent security measures need to be considered in order to be able to address recent sophisticated kind of threats. This includes monitoring application sessions and defining up to the level security policies to control all internal processes and communications (Knapp, 2011). In Europe, Member States are pursuing Critical Infrastructure Protection (CIP) initiatives aimed at working with different organisations and industries to address cyber security threats.

2. Critical Infrastructure Security Threats

Critical infrastructure represents a system or a number of systems that perform critical functions and operations. Such systems are considered critical if they could impact any other critical processes and/or devices, or provide a pathway/channel to other critical system(s), or are used to protect critical systems (Knapp, 2011) (US (NRC), 2010). Figure 3 shows a general logical diagram provided by the US. NRC (Nuclear Regulatory Commission) for identifying critical systems (US (NRC), 2010).

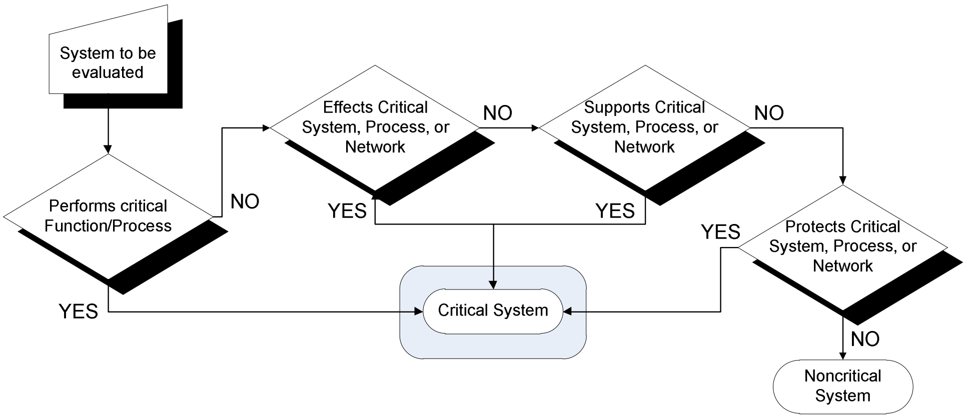

System to be evaluated
Performs critical Function/Process
NO
Effects Critical System, Process, or Network
NO
Supports Critical System, Process, or Network
NO
YES
YES
YES
Protects Critical System, Process, or Network
YES
Critical System
NO
Noncritical System

Figure 3: NRC Flow Diagram for Identifying Critical Systems

Manipulating a particular process in a critical system could cause certain threshold levels to build beyond safe operating parameters which then could result in loss of life and/or loss of critical services. Such a manipulation event could be performed using a Man-in-the-Middle attack to change control process parameters and its feedback loop using a targeted malware. For example, a successful cyber-attack can block, delay or manipulate the intended operation, thereby preventing a service provider from generating necessary energy output or from obtaining production metrics. This section presents various security threats and violations over the past recent years on different critical infrastructure domains including industrial networks, healthcare services, telecommunication networks, and banking systems.

2.1 Industrial Networks

An industrial network performs an operational process of a control or manufacturing system to carry out a particular operation. It consists of a supervisory network, business network of enterprise operations and control process networks (Knapp, 2011). The increasing persistence and sophistication of attacks on industrial networks in general and energy systems in particular requires effective solutions that are capable of mitigating such attacks. In 2009, the International Chief Security Officer (CSO) of the American Society for Industrial Security (ASIS) reported that (Ghansah, 2009)

“The electric grid is highly dependent on computer-based control systems. These systems are increasingly connected to open networks such as the internet, exposing them to cyber risks.”

Various entities such as hacking individuals, organizations and even states are involved in probing U.S. power grid systems on a daily basis. In 2009, the Department of Homeland Security (DHS) has reported that (Ghansah, 2009)

“Cyber spies, likely from China and Russia, have managed to inject malicious software into the electric grid, water, sewage, and other infrastructure control software. This software could enable malicious users to take control of key facilities or networks via the Internet, causing power outages and tremendous damage to all sectors of the economy.”

Satellite imagery of nuclear power stations and power grids can easily be located online using Google map. Online vulnerable systems and components such as unsecured servers, SCADA systems and network resources are remotely accessible to anyone with an Internet connection and with a basic knowledge of using attacking tools. The SQL Slammer Worm is one of those tools that are able to disrupt electric system control systems. Cyber-attacks incidents could result in shutting down portions of power plants, breaking into electrical utilities, disturbing cities lights and electricity, grid failures or catastrophic problems (Vaas, 2012) (Andres and Loudermilk, 2012) (Ghansah, 2009). IOActive discovered security vulnerability in many Smart Meters, where a malware managed to spread quickly throughout a neighbourhood, affecting the electric system controls, causing power disruptions and calibration modifications rendering the power meters inoperable (Davis, 2009).

Industrial networks have moved towards more effective mechanisms of managing industrial systems such as power generation and distribution. Such systems have become to rely on networked SCADA systems that use network protocols and about 85% of all analogue relay systems such as meters, demand response systems, control systems … etc. are now digital (Andres and Loudermilk, 2012). Most of the industrial network protocols are sensitive to DoS attacks that using a significant amount of overwhelming traffic could lead to protocol failure. Improper digital network configurations often lead to information leaks between SCADA systems, business networks and the Internet and pose a significant threat to network reliability. Network information leaks can allow worms and/or hackers to disabling safeguards and have a direct access to vulnerable SCADA systems (Ghansah, 2009). The end result could be taking a service offline, production failures, financial losses, life-threatening incident due to misinformation.

The SCADA systems are built using public or proprietary communication protocols such as Profibus. Those protocols are used for communicating between an MTU (Master Terminal Unit) and one or more RTUs (Remote Terminal Units). The SCADA protocols provide transmission specifications to interconnect master station and substation computers, RTUs, IEDs (Intelligent Electronic Devices) (Ghansah, 2009). Profibus is one of the common industrial protocols which were developed to achieve interoperability among systems in the energy utility. An attacker with the appropriate network reconnaissance techniques can access captures and analyses Profibus messages. This attack provides the attacker with information about network topology, device functionality, memory addresses and other data. A hacker can launch a replay attack with knowledge of normal Profibus traffic patterns simulates responses to the master while sending fabricated messages to outstation devices (Ghansah, 2009). Figure 4 shows some common industrial network vulnerabilities and security threats such as poor firewall configurations, insecure wireless links, weak control access mechanisms, remote access vulnerabilities … etc.

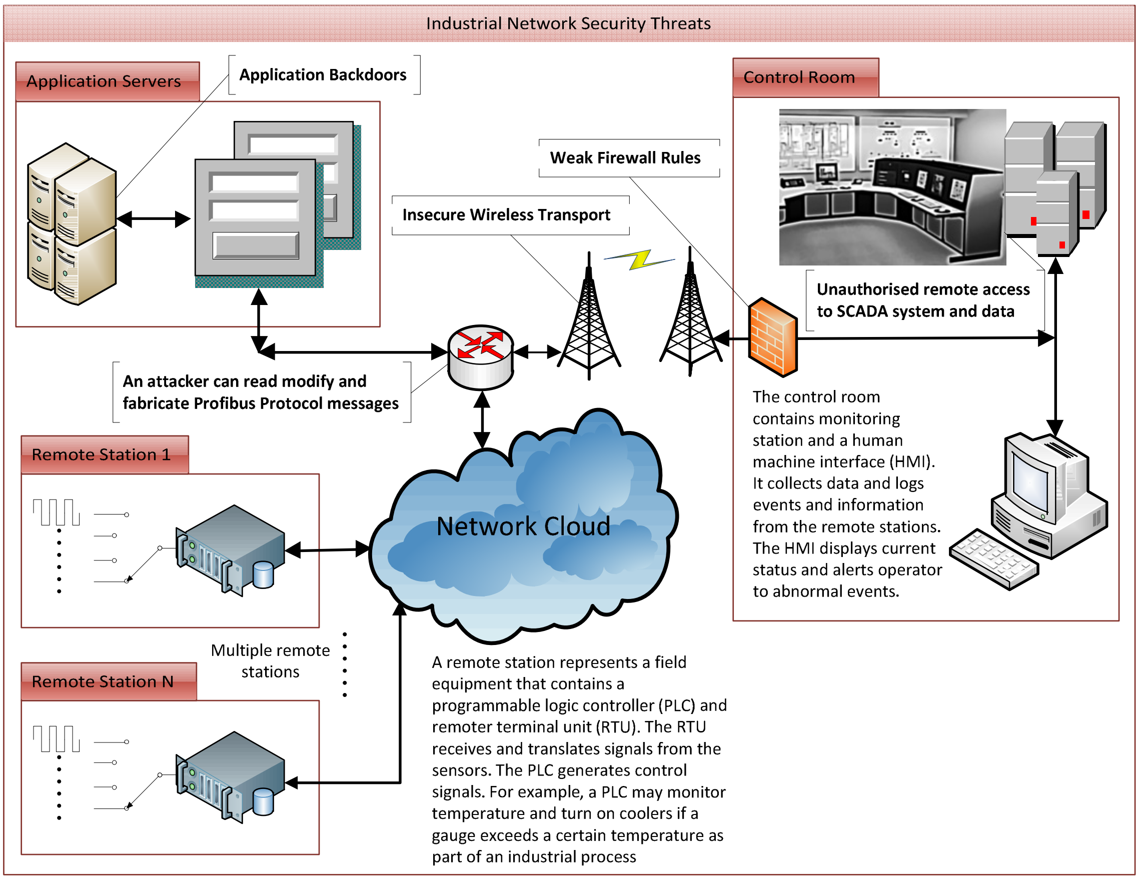

Industrial Network Security Threats
Application Servers
Application Backdoors
Control Room
Weak Firewall Rules
Insecure Wireless Transport
Unauthorised remote access to SCADA system and data
An attacker can read modify and fabricate Profibus Protocol messages
The control room contains monitoring station and a human machine interface (HMI). It collects data and logs events and information from the remote stations. The HMI displays current status and alerts operator to abnormal events.
Remote Station 1
Network Cloud
Multiple remote stations
Remote Station N
A remote station represents a field equipment that contains a programmable logic controller (PLC) and remoter terminal unit (RTU). The RTU receives and translates signals from the sensors. The PLC generates control signals. For example, a PLC may monitor temperature and turn on coolers if a gauge exceeds a certain temperature as part of an industrial process

Figure 4: Industrial Network Security Threats

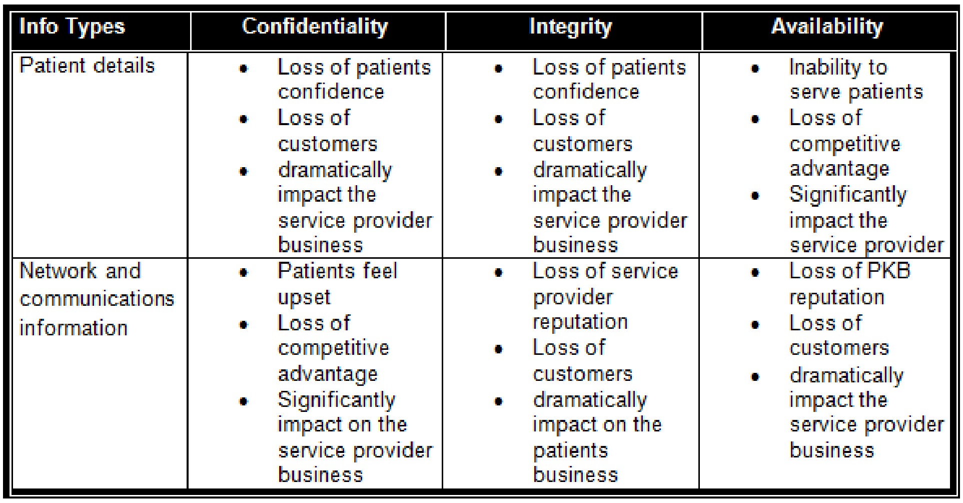
As an intelligent malware Stuxnet manages to inject code into the ladder logic of PLCs, monitors Profibus protocol and then manipulates the operations of the PLC to interrupt control processes and modify operation results. Profibus is an industrial protocol developed by the Central Association for the Electrical Industry in Germany. It is a Master/Slave protocol that uses a token for communications between a master and one or more slaves. A master Profibus node represents a PLC or RTU and a slave is sensor or other control system device. One of the major limitations of Profibus is lack of authentication to many of its functions allowing for unauthorised control over all slaves. This could result in disrupting the protocol functions or injecting code into a slave node. Stuxnet is able to exploit Profibus and compromise a PLC as a master node allowing Stuxnet to issue commands to the relevant slave nodes to sabotage the process (Knapp, 2011) (Jonathan, 2010).

2.2 Healthcare

The emergence of Web-based Healthcare applications has generated various risks to patients information security. Malicious software and operations pose a major threat to the security of EPHI (Electronic Patient Healthcare Information), especially those supporting medical identity theft and healthcare fraud. Moreover, the proliferation of handheld devices, such as smart phones, has created an environment in which patients' wireless communications and healthcare staff emails can be intercepted. Lack of effective policies and security controls by healthcare service providers poses a security risk in terms of accessibility to patients' files, such as valid diagnosis and treatment information. Recent developed malware is able to exploit various healthcare system vulnerabilities and continue to grow. Such problems could have a negative impact on patients and affect the proper use of their medication and drugs. This makes healthcare service providers in general, and hospitals and patients in particular, at risk.

The critical information attributes which have an impact on a healthcare service provider operations are patients' details/information and network communication information. Table 1 includes definition for the assigned impact levels and their possible effects on a healthcare service provider. Definition of impact levels in table 1 are meant to help healthcare service provider's management team to understand that the loss of security attributes to those pieces of information (patients' details and network and communications information) can impact the service provider in different ways and degrees.

Table 1: Definition of Impact Levels



Info Types	Confidentiality	Integrity	Availability
Patient details	• Loss of patients confidence • Loss of customers • dramatically impact the service provider business	• Loss of patients confidence • Loss of customers • dramatically impact the service provider business	• Inability to serve patients • Loss of competitive advantage • Significantly impact the service provider
Network and communications information	• Patients feel upset • Loss of competitive advantage • Significantly impact on the service provider business	• Loss of service provider reputation • Loss of customers • dramatically impact on the patients business	• Loss of PKB reputation • Loss of customers • dramatically impact the service provider business

Healthcare service providers are leveraging the networked nature of the Internet and want to take the full advantage of the Internet and distributed computing to serve their customers/patients. Nowadays healthcare services providers are connected to the Internet, have various systems to worry about and are facing an increased number of vulnerabilities and security threats. Such threats represent conditions with a potential to cause damage to an organisation's business and/or system resources including databases and communication links. Threats may come from a system's vulnerabilities, unauthorised access, an insider performing illegitimate activities, natural disasters such as earthquakes, flooding, storms, lightning ... etc. Threats are divided into two types, external security threats and internal security threats. Examples of external security threats include denial of service (DoS) attacks, remote brute-force, man-in-the middle attack. Password sniffing, Trojan horses, Data tampering are examples of internal security threats. Such attacks are a direct threat to the confidentiality, integrity, and availability of a healthcare service provider's information assets. The HIPAA (Health Insurance Probability and Accountability Act) security rules and procedures have introduced various solutions to minimize such threats and risks.

2.3 Telecommunication Networks

Computer networks, satellite communication systems and links allow unauthorized users to gain access to private information and critical resources. The satellite networks represent one of the major communication systems that face significant security challenges. Attacks such as DoS (Denial of Service) on satellites could cause business and military communications to become unavailable at critical moments and prevent legitimate clients from accessing necessary service(s). Space assets satellite systems are increasingly vulnerable to various attacks, such as RF jamming and network traffic spoofing. Jamming involves intentionally masking a target signal with another RF signal using a little jamming power, which can result in a signal degradation or total signal loss. Spoofing involves transmitting false information to the satellite in order to overpower the intended signal. This is to send the receiver a malicious signal and fooling it into using a false signal for further processing (Northcutt, 2007). Such attacks could lead to disruption of communications and prevention of service access.

To attack a satellite does not require a state space capability. The Tamil Tigers Liberation Front (LTTE), a Sri Lankan separatist group classified as terrorist group, has recently been blamed for illegally using INTELSAT satellites. The LTTE used INTELSAT to broadcast radio and TV transmissions via the use of an empty transponder (Ma et al. 2010). Satellite transponders represent the access points that are configured to retransmit any signal being sent to them and are susceptible to various vulnerabilities. If a transponder has unused bandwidth, a hijacker could easily identify a vacant place on the transponder, using a spectrum analyzer, to broadcast their own transmissions. An attacker can create a DoS condition by turning on an uplink carrier with a great enough signal-to-noise ratio (SNR) into the victim's satellite on the same frequency as the intended signal (Daly, 2007). The victim transponder processes the incoming carrier frequency along with the intended signal and re-transmits both of them down to the receiver. The attacker's signal may impair the intended signal at the receiver making it unable to distinguish the intended signal from the attacker's signal. Moreover, the attacker's signal raises the background noise of the transponder and causes a reduction in the SNR of all the intended signals, which makes them uneasy to recover. With today's DSP (Digital Signal Processing) systems it is becoming trivial to launch such attacks. The uplink signal from the hijacker is transmitted to the satellite in a highly directed beam, which makes finding the attacker extremely difficult (Daly, 2007). This ability to hack into commercial satellites could lead to a disastrous situation in global communications. The development of effective security models and solutions is a viable response to the rapidly increasing number of malicious activities on satellite systems and Internet services.

3. Security Measures

It is important for organisations managing critical systems to deploy all necessary security solutions and carry out a regular security assessment and auditing. Security assessment must be carried out by experienced professionals to gather information and to perform necessary tests. The security assessment is a process that includes interview with key personnel managing the critical system, review of available systems and documentation and carry out comparisons with relevant standards. A security audit is a systematic technical evaluation of an organisation system(s) and service(s) by measuring how well they confirm to standards and guidelines provided by different organisations such as British Standards (BSs), OSI, NIST … etc. Through these efforts, the assessment team should be able to plan a strategy to identify security vulnerabilities and propose solutions to meet the critical infrastructure's security needs. The assessment process includes reviewing the security requirements for critical network architecture and addressing the issues of end-to-end communication infrastructure uniquely pertaining to critical system communications and access control mechanisms. The assessment process should consider technical standards in studying and specifying the requirement details and evaluation of system architecture and services in terms of meeting the necessary security needs. Effective security assessment includes vulnerability assessment and penetration testing services which must be performed regularly to suit critical infrastructure systems as follows:

- Vulnerability assessment is concerned with the evaluation of network configurations, firewalls, vulnerable critical services and/or systems ... etc. using vulnerability scanners. Vulnerability scanners are useful in terms of ensuring the security of services and systems. For example, vulnerability scanners could be used to determine if there are any unauthorised activities are occurring or information leakage is taking place in a power grid network or in a SCADA system. Figure 5 shows a proposed flow chart for a vulnerability assessment to critical infrastructure.

- Penetration test is carried out to perform an external penetration test on all the network systems including servers, databases, communication links ... etc. In general, the testing team should not be given any prior information about the network architecture.

Such assessment should involve using necessary tools to evaluate, test and analyse the security operations and infrastructure. It also should define the countermeasures to security threats and violations. Stallings (2011) had identified the necessary countermeasure to major Outsiders and insiders' threats/attacks. Some of the attacks are common for both outsiders and insiders' threats. In Europe, Member States are required to conduct a security assessment of the threats and violations relating to the designating ECI. Member States have to report to the EC every two years on the security threats, risks and vulnerabilities the various European Critical Infrastructure (ECI) services are facing (The EC directive, 2008). The final outcomes and results of the assessment and auditing are intended to provide the organisation with recommendations to improve security.

As many organisations are migrating to cloud services, much of their infrastructure will now be controlled by a third-party Cloud Service Provider (CSP). The extensive use of virtual machines (VMs) in developing cloud infrastructure presents various security concerns for organisations as customers of a public cloud service (Winkler, 2012). Migration to cloud environment brings unique security challenges to critical systems such as virtual threats. Virtualisation uses more complex processes than traditional systems and DoS attacks to VMs have become equally more complex. Therefore, relying on protection techniques traditionally implemented against DoS is insufficient. The operating system (OS) vulnerabilities on the host system can flow upward into the VM OS. Therefore, a compromise of the host OS would allow an attacker to access all VM processes and services. Table 2 lists the major security Cloud-siders threats and necessary countermeasures (Winkler, 2012) (Krutz and Vines 2010) (Winkler, 2011).

Effective critical systems security is based on various factors such as proper policies, procedures, management support, and appropriate implementation. Therefore, critical infrastructure requires a comprehensive security policy that details not only physical security requirements but also includes information protection and systems security considerations. This includes preparation of an acceptable-use policy addressing the appropriate use of corporate technology resources and the actions management will take resulting from the violation of this policy. Password policies are important to specify when passwords must be used, how strong they must be, and how they must be stored and processed. The lack of a password policy and appropriate password controls could lead to unauthorized access to systems and information. Polices are required to conform to specific professional organization such as the OSI's regulations applicable to the communication or use of data. Security policy is the foundation of critical systems security plan and implementation. The lack of security policy could have a negative impact on a critical service provider's performance and ability to meet the industry standards and regulations. In Europe, the EPCIP developed a procedure for identifying critical assets of the European Critical Infrastructure (ECI), which is implemented by the European Commission's directive 2008/114/EC. This directive insists that Member States must ensure that an operator security plan (OSP) is in place for each designated ECI to identify the critical assets of the ECI and the available security policies and measures for protecting them (The EC directive, 2008).

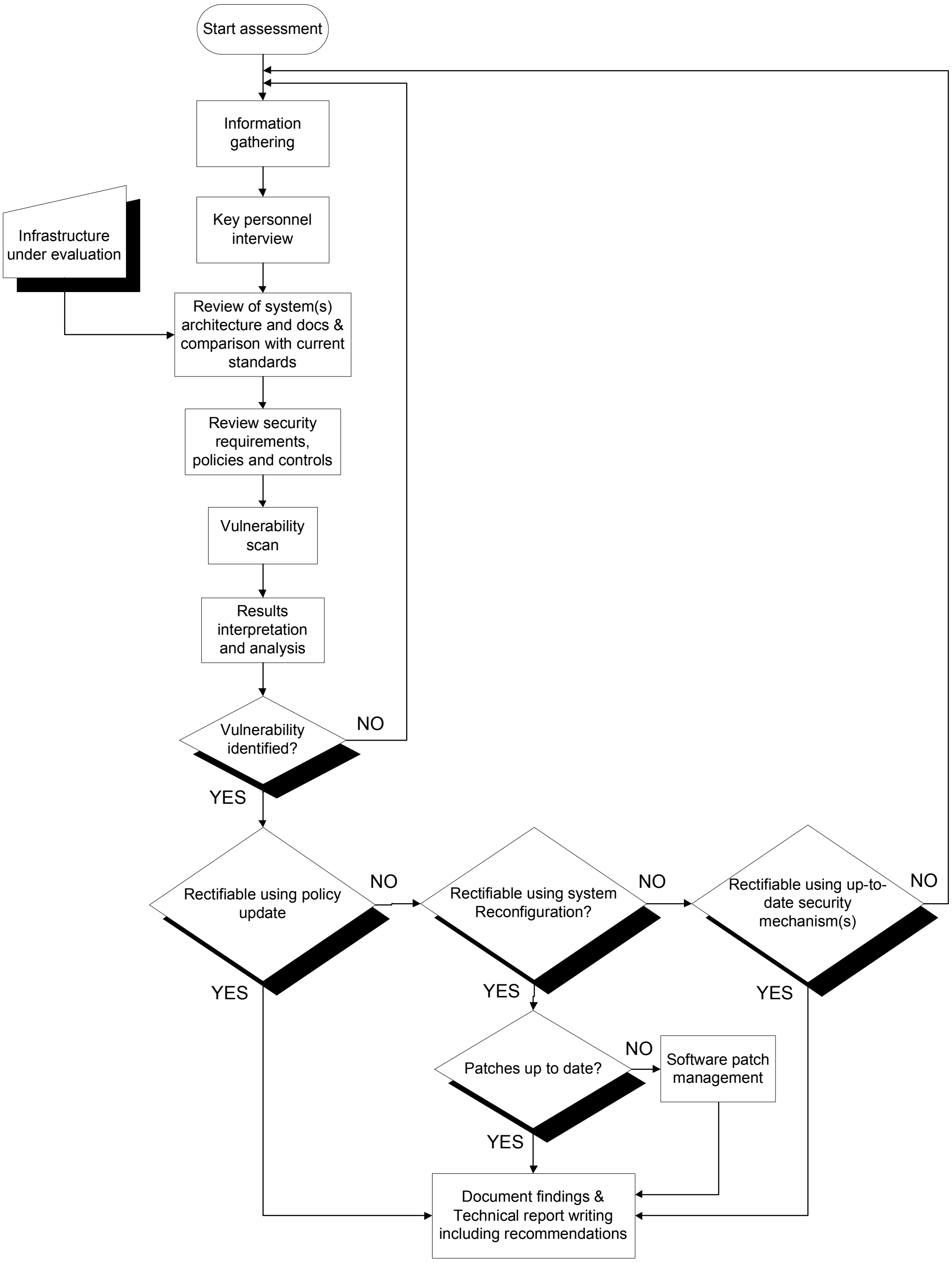
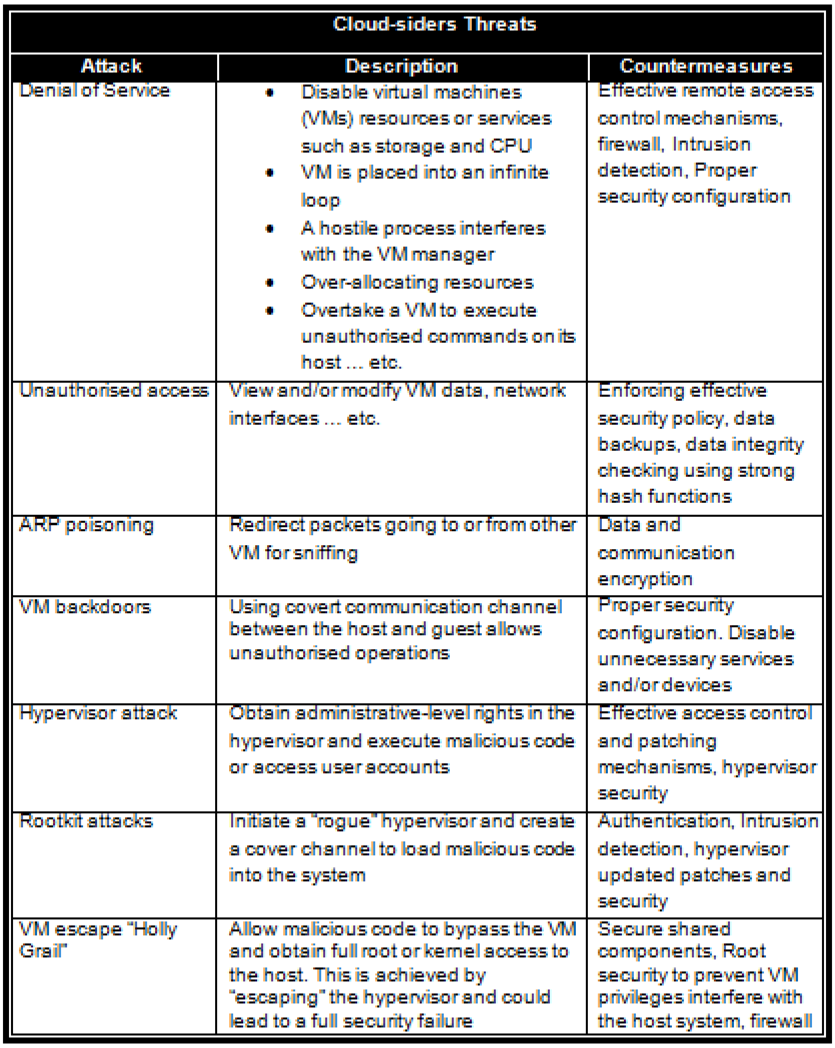

Start assessment
Information gathering
Key personnel interview
Infrastructure under evaluation
Review of system(s) architecture and docs & comparison with current standards
Review security requirements, policies and controls
Vulnerability scan
Results interpretation and analysis
Vulnerability identified?
NO
YES
Rectifiable using policy update
NO
Rectifiable using system Reconfiguration?
NO
Rectifiable using up-to-date security mechanism(s)
NO
YES
YES
YES
Patches up to date?
NO
Software patch management
YES
Document findings & Technical report writing including recommendations

Figure 5: Vulnerability Assessment to Critical Infrastructure

4. Conclusion

Due to the fact that different critical infrastructure systems reply on weak security mechanisms, such systems are increasingly targeted by attackers. Various complex malwares have been developed to target improperly protected critical infrastructure. Critical infrastructure service providers must seek implementing cost-effective and comprehensive secured solutions for their system operations. Various critical industries have demonstrated a desire to ensure the security of their systems architecture and infrastructure. This paper provided a brief survey to recent security threats and vulnerabilities to different critical infrastructure systems including industrial networks, healthcare systems, telecommunication services and online banking. For example, Stuxnet is able to inject code into the ladder logic of PLCs, manipulates the operations of the PLC to interrupt processes and modify output. In this paper, various security measures have been presented including assessment process to infrastructure architecture and systems in terms of vulnerability assessment, security policies, procedures and solutions. In Europe, the European Commission's directive insists that Member States must carry out a security assessment of the threats and violations relating to the designating ECI.

Table 2: Cloud-siders Threats and Countermeasures



Cloud-siders Threats		
Attack	Description	Countermeasures
Denial of Service	• Disable virtual machines (VMs) resources or services such as storage and CPU • VM is placed into an infinite loop • A hostile process interferes with the VM manager • Over-allocating resources • Overtake a VM to execute unauthorised commands on its host … etc.	Effective remote access control mechanisms, firewall, Intrusion detection, Proper security configuration
Unauthorised access	View and/or modify VM data, network interfaces … etc.	Enforcing effective security policy, data backups, data integrity checking using strong hash functions
ARP poisoning	Redirect packets going to or from other VM for sniffing	Data and communication encryption
VM backdoors	Using covert communication channel between the host and guest allows unauthorised operations	Proper security configuration. Disable unnecessary services and/or devices
Hypervisor attack	Obtain administrative-level rights in the hypervisor and execute malicious code or access user accounts	Effective access control and patching mechanisms, hypervisor security
Rootkit attacks	Initiate a "rogue" hypervisor and create a cover channel to load malicious code into the system	Authentication, Intrusion detection, hypervisor updated patches and security
VM escape "Holly Grail"	Allow malicious code to bypass the VM and obtain full root or kernel access to the host. This is achieved by "escaping" the hypervisor and could lead to a full security failure	Secure shared components, Root security to prevent VM privileges interfere with the host system, firewall

Migration to cloud computing based services and environment brings unique security challenges to critical systems such as VM threats. A summary of cloud-siders threats and countermeasures are listed in section 3. The lack of proper security policy could have a negative impact on the performance of critical systems and ability of critical service providers to meet the industry standards and regulations. European Member States must ensure that an OSP is in place for each designated ECI. This is to identify the critical systems and assets as well as the available security measures for protecting them. Critical infrastructure service providers can improve their security posture by taking into consideration the proposed security measures and assessment strategy. The final outcomes and results of security assessment and auditing are intended to provide organisations with recommendations to improve security.

Bibliography

Andres, Richard B. and Loudermilk, Micah J. (2012), National Security & Distributed Power Generation. livebetter Magazine Issue Number 24, Sep 2012

BBC News, (2011), FBI says hackers hit key services in three US cities, http://www.bbc.co.uk/news/technology-16157883 [accessed on 22nd December, 2012]

Daly, John C. K. (2007), LTTE: Technologically innovative rebels, http://www.isn.ethz.ch/isn [accessed on 3rd Oct 2012]

Davis, Mike (2009), IOActive Unveils Smart Grid Security Research, http://www.ioactive.com/services_grid_research.html [accessed on 26th January, 2013]

Erwin, I. Sandra, Stew Magnuson, Dan Parsons and Yasmin Tadjdeh, November, (2012), Top Five Threats to National Security in the Coming Decade, http://www.nationaldefensemagazine.org/archive/2012/November/Pages/TopFiveThreatstoNationalSecurityintheComingDecade.aspx [accessed on 1st Oct 2012]

Fildes, Jonathan (2010), Stuxnet worm 'targeted high-value Iranian assets, BBC News, http://www.bbc.co.uk/news/technology-11388018 [accessed on 22nd December, 2012]

Ghansah, Isaac, (2009), Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks, California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2012-047

Knapp, Eric D. (2011), Industrial Network Security, Syngress.

Krutz, Ronald and Vines, Russell (2010), Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley.

Ma, Ting Hui, Yee L. and Ma, Maode (2010), Protecting Satellite Networks from Disassociation DoS Attacks, Communication Systems (ICCS), IEEE International Conference
Northcutt, Stephen (2007), Are Satellites Vulnerable to Hackers? http://www.sans.edu/research/security-laboratory/article/satellite-dos [accessed on 1st Oct 2012]

Northcutt, Stephen (2007), Denial of Service. http://www.sans.edu/research/security-laboratory/article/denial-of-service [accessed on 1st Oct 2012]

Stallings, William (2011), Cryptography and Network Security: Principles and Practices, Fifth Edition, Pearson.

Symantec (2010), Symantec Critical Infrastructure Protection Study – Global Results

The EC directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm [accessed on 22nd January, 2013]

US Nuclear Regulatory Commission (NRC), Regulatory Guide 5.71 (2010), Cyber Security Programs for Nuclear Facilities, Washington, DC

Vaas, Lisa (2012), Nuclear power plant cybersecurity warnings silenced by legal threats, http://nakedsecurity.sophos.com/2012/10/31/nuclear-security-silence/ [accessed on 3rd Oct 2012]

Winkler, Vic (2011), Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. ISBN 978-1-59749-592-9

Winkler, Vic (2012), Cloud Computing: Virtual Cloud Security Concerns, Technet Magazine, Microsoft