Computers & Security 139 (2024) 103687

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Smart homes under siege: Assessing the robustness of physical security against wireless network attacks

Ashley Allen [a], Alexios Mylonas [a,*], Stilianos Vidalis [a], Dimitris Gritzalis [b]

[a] Cybersecurity and Computing Systems Research Group, Department of Computer Science, University of Hertfordshire, United Kingdom
[b] Department of Informatics, Athens University of Economics & Business, Greece

ARTICLE INFO

Keywords:
Cybersecurity
Physical security
Smart home
Smart locks
IoT
Bluetooth
RFID

ABSTRACT

Nowadays domestic smart security devices, such as smart locks, smart doorbells, and security cameras, are becoming increasingly popular with users, due to their ease of use, convenience, and declining prices. Unlike conventional non-smart security devices, such as alarms and locks, performance standards for smart security devices, such as the British TS 621, are not easily understandable by end users due to the technical language employed. Users also have very few sources of unbiased information regarding product performance in real world conditions and protection against attacks from cyber attacker-burglars and, as a result, tend to take manufacturer claims at face value. This means that, as this work proves, users may be exposed to threats, such as theft, impersonation (should an attacker steal their credentials), and even physical injury, if the device fails and is used to prevent access to hazardous environments. As such, this paper deploys several attacks using popular wireless attack vectors (i.e., 433 MHz radio, Bluetooth, and RFID) against domestic smart security devices to assess the protection offered against a cyber attacker-burglar. Our results suggest that users are open to considerable cyber physical attacks, irrespective if they use lesser known (i.e., no name) or branded smart security devices, due to the poor security offered by these devices.

1. Introduction

Smart security devices are now ubiquitous and their popularity is likely to grow considerably over the next decade, where independent research suggests a market of $7.98B by 2027 for smart security devices (Mordor Intelligence, 2022). Advanced home automation and smart security device deployment is an emerging trend. Despite early attempts at home automation during the tail end of the 20th century, it is only within the last decade that these devices have crossed from their traditional home (i.e., in office complexes and multi-tenanted buildings) into the residential sphere. This behaviour brings significant challenges for security professionals looking to ensure that these devices are fit for their stated purpose. It also exposes their end users to new attack vectors against their security and privacy, such as via Bluetooth (Lonzetta et al., 2018; Ho et al., 2016; Ye et al., 2017) and RFID (Chantzis et al., 2021; Mitrokotsa et al., 2010; Touqeer et al., 2021). This is especially true for products like smart locks, smart padlocks, and smart intruder alarms, which will be hereafter referred to as *smart security devices*, as these devices protect users, their data, and their physical spaces. Non-academic research (Spring, 2019) discusses flaws found with the companion applications and the ability to brute-force the Bluetooth encryption used. However, there is limited work on the physical devices themselves and the level of protection they provide.

Considering the performance of "non-smart" or conventional security devices, such as locks and hard-wired intruder alarms, their users can refer to well-established performance standards against an attacker-burglar, such as BS 3621 (Banham Security, 2022), to decide whether a product is suitable for their security needs. Whilst the specifics of these standards are written in technical language, a user only needs to know that the device (e.g., a lock in BS 3621) is compliant to that performance standard to provide a level of protection that an "average" user will find acceptable. The standard lends itself to repeatable testing, which is independent of the skill and technical know-how of the person conducting the test. In contrast, this is not the case for smart door locks, as demonstrated by the most recent performance standard, i.e., *TS 621* (Door and Hardware Federation, 2022). Sections 5 and 6 of *TS 621* discuss attacks against the "smart" features of the lock (i.e., credentials and RF network), stating that *"the initial attack time should be used to find*

a.allen3,a.mylonas
* Corresponding author.
E-mail address: a.mylonas@herts.ac.uk (A. Mylonas).

https://doi.org/10.1016/j.cose.2023.103687
Received 27 October 2023; Received in revised form 9 December 2023; Accepted 23 December 2023
Available online 28 December 2023

a vulnerability and create a process for replicating this". However, if the assessor cannot find a vulnerability, that does not necessarily mean that one does not exist, only that *in this instance* one was not found. In other words, BS 3621 requires that a device passes a set of pre-specified tests, whereas TS 621 only requires that a device outperforms the person testing it. As a result, the protection that is offered by the device is not standardized as in the case of conventional security devices.

Furthermore, users often opt to utilize "lesser known" smart security devices. Contrary to popular, well-known brands that are identified through marketing and previous user knowledge, these devices are more accessible to the market due to their more competitive price. In this work, a lesser known device refers to the practice of selling products either under no name ("white label"), or under a disposable brand name. A disposable brand name contrasts to one such as *Yale* or *Chubb*, where years of marketing and product development have created an impression with the user as to the service and quality that is offered. Instead, a disposable brand can be discarded if it becomes tarnished. As a result, these smart security devices tend to have less after sale software security updates, e.g., see (Jones et al., 2020) for related work in Android devices. As the cost of the components used within smart home security devices decreases, lesser known brands are likely to take a significant slice of the market.

In this context, this paper aims to investigate the protection that is offered by smart security devices (i.e., smart locks, smart padlocks, and smart intruder alarms) against cyber attacker-burglars (Hodges, 2021). To this end, we mount several attacks that aim to circumvent the physical security that is offered by both lesser known and branded smart security devices. To the best of our knowledge, we are the first to assess the protection that is offered by these devices and uncover the threats that their users are exposed to.

The contributions of the paper are as follows:

- It provides a comparison of the physical security that is offered by smart security devices, both lesser known and branded, against an unsophisticated cyber attacker-burglar. To this end, we mount attacks against a representative set of smart security devices, which would allow a cyber attacker-burglar to bypass the smart security device and access the user and their assets.
- It highlights the limited resilience – and in specific cases the lack of protection – which is offered by the smart security devices. Our results suggest that an unsophisticated attacker is able to mount attacks that provide: (i) full control over the device, (ii) cause denial-of-service attack, and (iii) impersonate a legitimate user.
- It uncovers fourteen (14) zero-day vulnerabilities in the assessed devices, which have been communicated to their vendor via responsible disclosure. We shared their details with the security community via submitting them to Common Vulnerability and Exposure knowledge base.[1] We note that, in specific cases, the vulnerabilities cannot be patched, thus, rendering the smart devices insecure.
- We analyse the impact of our findings, our experience with the responsible disclosure process and provide recommendations and workarounds (if any) for the zero-day attacks that we have uncovered.

The rest of the paper is structured as follows. Section 2 discusses background and related work. Section 3 presents our methodology and Section 4 presents our results. Section 5 discusses our findings before the paper is concluded in Section 6.

[1] An interested reader can refer to: CVE-2021-44518, CVE-2021-44905, CVE-2022-46480, CVE-2023-26941, CVE-2023-26942, CVE-2023-26943, CVE-2023-31759, CVE-2023-31761, CVE-2023-31762, CVE-2023-31763, CVE-2023-34553, CVE-2023-39841, CVE-2023-39842, CVE-2023-39843.

2. Background

This section includes a discussion of related work covering 433 MHz radio, Bluetooth, and RFID as attack vectors. Publications were collected via searches on Google Scholar, IEEE Xplore, and ACM Digital Library, with keywords like "smart lock", "smart padlock", and "smart intruder alarm". We have excluded papers presenting generalized wireless attacks against 433 MHz, Wi-Fi, and Bluetooth communication. For more information on these generic attacks the reader may refer to (Montoya et al., 2018; Egli and Netmodule, 2006; Gullberg, 2016), respectively.

2.1. RF frequency vectors

Smart security products often use two radio frequency (RF) based wireless communication vectors, namely radio signals, typically operating at 433 MHz, and Bluetooth operating at 2.4 GHz. Even though the level of embedded security and configuration options differ between them (Ferro and Potorti, 2005; Lackner, 2013), there are commonalities, such as short range and vulnerability to eavesdropping and jamming between the two (Garcia et al., 2016; Khan and Kabir, 2016). Most importantly, each is subject to a Denial of Service (DoS) attack, where a jamming signal is broadcast at the relevant frequency to deny access to the target device, or to redirect users to an "evil twin" device to steal their credentials or monitor their traffic.

The 433 MHz radio band is reserved in many locations in the world for unlicensed use. This means that anyone can, with some restrictions, use this frequency for communication purposes. Devices that utilize this band are cheap, as the technology is mature and easily implemented. It also has a significant range advantage over *higher frequency protocols,* easily reaching 100 m or more. Nonetheless, the narrow-reserved band suffers from significant interference and allows only minimal data transmission due to bandwidth constraints. For this reason, messages are usually limited to "on/off' signals. This is ideally suited to wireless security alarm systems, where communication between the sensor and the base station is usually limited to notifying whether the sensor has been triggered or not.

Few papers relating to the use of 433 MHz radio in smart devices exist. The authors in (Hung and Vinh, 2019), discuss the analysis of an unknown wireless protocol using software-defined radio (SDR). The authors demonstrate that their methodology can be used to analyse a wide range of transmission encodings inside the 433 MHz band. The work in (Ahmad et al., 2018), discusses the impact of foliage on signal transmission in the 433 MHz band. Whilst their paper specifically targets *LoRa* technology, which transmits over a much larger distance, it provides useful background as the physics of physical interference is essentially the same regardless of the underlying protocol. The paper evidences significant signal attenuation, which is something to consider when assessing vulnerabilities in smart wireless alarm systems. 433 MHz communication is, in the main, unidirectional and, as such, behaves in a similar way to User Datagram Protocol (UDP), i.e., a message is sent but not acknowledged. Therefore, if the sensors are blocked from triggering, it may be possible to inhibit communication with the base station and stop message delivery. This type of interference is exhibited in the *RollJam* attack against car security systems (Mould, 2022) and garage door openers (rtl-sdr.com, 2022). Past works, such as (Aras et al., 2017; Csikor et al., 2023), have also focused on additional attacks against radio-frequency systems, such as spoofing and replay.

Bluetooth, and in particular Bluetooth *Low Energy* (*Bluetooth LE; BLE*) is a core communication protocol for smart security devices, as it provides a reasonable transfer rate over a local area and contains a robust set of security protocols (Sevier and Tekeoglu, 2019) that developers can leverage. Current security concerns are discussed broadly in (Kwon et al., 2016; Barua et al., 2022; Qu and Chan, 2016). More specifically, the work in (Jasek, 2016), introduces the *GATTacker* tool, as well as discusses several active and passive methods for *BLE* data acquisition. Abuse of the *Generic Attribute Profile (GATT)* allows for data

compromise, command interception and replay, and denial of service, e.g., as in (Cäsar et al., 2022). *BlueDoor* (Wang et al., 2020) is a method for downgrading the security properties of the protocol used to communicate between devices, potentially allowing compromise and data exfiltration. Moreover, the inherent vulnerabilities and denial of service attack associated with the *Just Works* pairing mode are discussed in (Lounis and Zulkernine, 2019).

The authors of (Garbelini et al., 2020), introduce 13 CVEs covering eleven chipset specific vulnerabilities under the *Sweyntooth* banner. It should again be noted that these are generic hardware vulnerabilities rather than device specific. As such, finding a generic *BLE* vulnerability greatly reduces the attack cost for a plethora of user devices.

2.2. RFID

RFID, along with *Bluetooth*, is one of the most ubiquitous protocols used by smart security systems. Passive *RFID* cards have no power supply, with a small amount of energy being provided via induction loop by the reader. Active tags, on the other hand, have a small onboard battery that can supply power, which enables an active tag to broadcast its availability if needed, as demonstrated for example in (Dogan et al., 2016). In either form, tags can only hold a small amount of data, which is generally read-only. Given that these cards cannot be updated in response to emerging threats, users and system owners must decide whether to remove affected cards from circulation or continue to use them knowing they are insecure. Reader vulnerabilities are easier to address, but potentially insecure cards may be supported for backwards compatibility reasons, as discussed in (Sarma and Engels, 2003).

Even though RFID is old technology with specific security and bandwidth limitations, it is still widely used in smart locks and smart padlocks, as demonstrated in (Aghili et al., 2019; Kumar et al., 2021; Shariq et al., 2021). An *RFID* tag essentially acts as a technically advanced key that must be present for the door to open. However, the *RFID* key is more easily copied than a traditional key (Li et al., 2012). The *RFID* reader embedded in the device also provides an entry point into the system, one that a traditional lock does not have. With the right tools it may be possible to fool the reader without having a valid card (Rysc Corp, 2023).

Finally, a significant amount of research exists into *RFID* itself and potential vulnerabilities. Interested readers should refer to (Xiao et al., 2009; Chantzis et al., 2021; Grover and Berghel, 2011; Rotter, 2008; Williamson Sr et al., 2013; Kim and Kim, 2006).

2.3. IoT vulnerabilities

The work in (Davis et al., 2020) focuses on IoT vulnerability types, such as in the network, software, and encryption, as opposed to our more granular approach that considers wireless attack vectors. A similar study to ours is conducted by Sivaraman et al. (2018), though using different classes of IoT devices, such as cameras, motion sensors, lightbulbs, and power switches. The devices are tested against the protection of confidentiality, integrity, and availability. Their study demonstrates that all the devices tested were exposed to at least one significant threat impairing either the confidentiality, integrity, or availability of their owner. The authors of (Malhotra et al., 2021) focused on IoT vulnerabilities and created a taxonomy of attack types covering physical, network, and software channels. They discussed potential solutions, such as intrusion detection and learning-based security solutions.

Finally, the work in (Vasile et al., 2018) present a comprehensive survey of firmware extraction techniques via JTAG and UART. These are intended as lab-based attacks only, meaning that their use by an actual cyber-burglar in a real-world scenario is unlikely, given the level of access to the device that is required. In addition, past literature has focused on hardware and software protocol attacks. A reader interested for more information could refer to (Valle, 2021; Gupta, 2019; Chantzis et al., 2021).

3. Methodology

This section provides our experimental methodology focusing on the: (a) experimental setup, (b) assumed threat model, and (c) criticality metric used to evaluate the impact of the attacks.

3.1. Experimental setup

Our experiments include three types of smart security devices, namely: (*i*) smart padlocks, (*ii*) smart locks, and (*iii*) smart intruder alarms, which are either branded devices or lesser known ones, as summarized in Table 1. The devices were found via searches on the supplier's web sites, using brand-agnostic terms, such as "smart padlock", "smart lock", and "smart alarm", to avoid bias towards particular brands. The devices were selected based on the following criteria: (a) supplier, (b) availability of English manual, (c) cost, and (d) compatible wireless communication technologies. With regards to the suppliers, we considered two of the biggest global online marketplaces (i.e., Amazon and eBay), as well as two significant "direct to consumer" marketplaces (i.e., Banggood and DealExtreme). As the experiments assess the level of protection that is offered to users, who are not necessarily security or technically savvy, these provide a representative set of suppliers where users are likely to purchase these smart security devices. Similarly, we assumed that prospective new users would search for devices offering an English manual, which would allow the correct device configuration in case of a lesser known brand that is manufactured overseas. We also attempted to ensure a wide spread of wireless

Table 1
Devices used in the experiments.

Device Name	Supplier	Cost	433MHz	Wi-Fi	Bluetooth	RFID
Smart Padlocks						
Bluetooth Bike Lock	eBay.co.uk	£17.99			X	
Bluetooth Padlock	amazon.co.uk	£12.69			X	
eGeeTouch	amazon.co.uk	£19.90			X	X
Smart Locks						
5-in-1 Smart Door Lock	banggood.com	£72.16		X		X
Etekcity 3-in-1	eBay.co.uk	£24.16				X
Fortessa Smart Lock	eBay.co.uk	£35.00			X	
Nuki Smart Lock	amazon.co.uk	£149.00			X	
Tuya Spindle Lock	eBay.co.uk	£55.00			X	
Ultraloq UL3	amazon.co.uk	£334.10			X	
WAFU Keyless Smart Lock	eBay.co.uk	£53.99	X			
WAFU Smart Biometric	dx.com	£40.27			X	
Yale Conexis L1	amazon.co.uk	£149.95	X		X	X
Yale Keyless	amazon.co.uk	£89.95	X			X
Smart Intruder Alarms						
AGSHome Smart Alarm	amazon.co.uk	£55.99	X	X		
Blitzwolf Alarm	banggood.com	£29.99	X	X		
Digoo Smart Alarm	banggood.co.uk	£59.99	X	X		X
Kerui Alarm	amazon.co.uk	£99.99	X	X		
Yale IA-210	ebay.co.uk	£90.00	X			X

communications technologies in the selected devices, with multiple technologies in the same device favoured where possible. The maximum cost of the devices was: £20 for the smart padlocks, £350 for the smart locks, and £100 for the smart alarms. As such, we consider that they are representative of the costs of each product category that a user would be willing to pay to protect their property with such as device.

As described in the threat model in the sequel, we assume that the cyber attacker-burglar possesses only limited resources. As such, we have assumed that affordable hardware is used (max £100 per hardware). Furthermore, it must have documentation that is accessible online (such as tutorial, forum posts, etc.) and software/drivers that are cross-platform (ideally compatible with at least two operating systems). The hardware used is summarized in Table 2.

3.2. Threat model

Our experiments assess the protection of the devices against a threat actor who has limited time to mount attacks against the physical security of an asset, which is in the users' home environment. We assume a typical user, non-security and technology savvy, and a typical home environment. In the following subsections, we further discuss our assumptions for the threat actor.

3.2.1. Access vector

We assume a threat actor who is within near proximity of the device and possesses user or enthusiast grade equipment. For instance, for Bluetooth testing, using an *Kinivo* or *Adafruit* BLE dongle is in scope of our tests, but requiring a professional protocol analyser is not. Furthermore, we assume that the threat actor is capable of mounting attacks using different tactics and techniques that span a spectrum of difficulty, from simple to complicated, given the constraints of time and equipment. With regards to time, attacks should be completed within 30 min.

While there are different remote and local attack vectors at the attacker's disposal during our scenarios, we considered: a) Bluetooth, b) 433 MHz radio, and c) RFID as the attack vectors. The tactics and techniques used for each attack vector are described in Section 3.2.2. Other attacks such as: (i) using the internal debugging protocol interfaces (e.g., refer to (Gao et al., 2019; Liu et al., 2021; Vishwakarma and Lee, 2018)) and (ii) bypassing authentication, e.g., against biometrics, keypad / password-based protocols, are out of scope of this work as they require much longer period of physical access to the device. Furthermore, we do not include any attacks using Z-Wave and Zigbee, which are popular protocols for IoT devices. While there is a number of published exploits for them (e.g., refer to (Vidgren et al., 2013; Vaccari et al., 2017; Razouk et al., 2014) for Zigbee and (Badenhop et al., 2017; Yassein et al., 2018; Kim et al., 2020; Boucif et al., 2020) for Z-Wave), their use in smart security products is limited given the lack of native support in mobile phones. Finally, we did not include any attacks against the companion applications of the device in our experiments, as they fall outside the scope of the work.

Table 2
Hardware used to mount the attacks against the smart security devices.

Device Name	Cost	Access Vector
Baofeng UV-5R radio	£20.08	433MHz
BBC Micro:Bit	£17.95	Bluetooth
HackRF	£73.17	433MHz
Kinivo BTD-400 Bluetooth dongle	£12.25	Bluetooth
NRF51822 dongle	£24.00	Bluetooth
Proxmark3 Easy	£60.00	RFID
Raspberry Pi 3 Model *B+*	£34.99	Bluetooth
Redmi 9C Mobile Phone	£66.99	Bluetooth, RFID
RFID NFC Card Copier	£30.12	RFID
Yardstick One	£90	433MHz

3.2.2. Tactics and techniques, and procedures

Our attacks cover the following attack types: Jamming/Denial of Service (DOS), data manipulation, data interception/sniffing, data recovery at rest/decryption, and cloning/masquerading. Please refer to Table 3 for details.

With regards to the 433 MHz radio access vector we have mounted three attacks, namely: (a) *simple jamming attack,* using either a Yardstick One or HackRF device, (b) *replay attacks,* where the communication on the 433 MHz band is captured and analysed to determine whether it can be replayed to trigger an action by the tested device, and (c) *RollJam attack*, where captured codes are stored and replayed later to get around "rolling code" implementations (Harding, 2022). The work of (Urquhart et al., 2019), discusses defeating an automotive keyfob using the RollJam attack and demonstrates that this provides a strong upper bound for device performance. Thus, if the RollJam attack fails, then the performance of the device can be considered sufficiently robust. Data manipulation attacks are not attempted against this access vector. This is because the data is sent in plaintext format and carries an "on" or "off" command. Data manipulation here would not provide any benefit to an attacker. Data interception is possible and is in fact the key requirement of attacks (b) and (c) above. Note that a person-in-the-middle (PitM) attack is not required when capturing data, as there are no sessions in 433 MHz radio communications. Each command is broadcast and, thus, any listener can receive the data.

We assume that the attacker is able to abuse RFID by: a) *card / fob cloning,* in which a paired RFID tag can be cloned using an over-the-counter RFID cloning handset (BangGood, 2022), and, (b) *encrypted card / fob cloning*, in which any encrypted cards or fobs are cloned.

With regards to Bluetooth we assume that the attacker would utilize: (a) *Sweyntooth attacks* via a family of vulnerabilities known as *Sweyntooth* (Garbelini et al., 2020), (b) session hijacking, using a Bluetooth sniffer such as *Btlejack*, (c) Bluetooth GATT manipulation using the Telefonica *HomePwn* suite (Telefonica, 2022), and (d) a replay attack using the *Gattacker* tool (Kurylowicz, 2022). It is worth noting that the Gattacker attack involves cloning/masquerading. Specifically, the Generic Attribute Profile (GATT) of the target device is cloned and the victim tricked into interacting with the clone rather than the original device. Moreover, one should note that jamming is also possible against Bluetooth. Nonetheless, the equipment required is out of the scope of the threat model.

It is also worth noting that Wi-Fi as an access vector falls outside the scope of this work. Even though, an attacker can capture and decode signals for replay attacks and/or attempt the injection of spoofed commands into the communication channel, this takes considerably more time than the attacks in other aforementioned access vectors. In addition, most locks, padlocks, and alarm systems do not support Wi-Fi (see Table 1), or support Wi-Fi but do not have alphanumeric keypads. The latter rely on *Wi-Fi Protected Setup (WPS)*, which allows a device to connect to a wireless network via a button press or a short PIN entry where a full keyboard is missing. Again, several papers explain how this process can be brute forced successfully and an interested reader could refer to works such as (Viehböck, 2011; Sadeghian, 2013; Chatzisofroniou and Kotzanikolaou, 2021).

3.3. Attack criticality scoring

To assess the impact of a successful attack from a cyber attacker-burglar this work utilises the Common Vulnerability Scoring System (CVSS) v4.0 (FIRST, 2023). CVSS provides widely accepted metrics, namely *Base, Supplemental, Environmental and Threat*, that enable the quantification of the criticality of software vulnerabilities. This work utilizes the Base Score metric and submetrics to capture and assess the criticality of a successful attack. Specifically, from the Base Score, we utilize the submetrics *Attack Vector, Attack Complexity, Attack Requirements, Privileges Required, User Interaction, Confidentiality, Integrity*, and *Availability*. Attack Complexity is evaluated based on the time taken

Table 3
Criticality of attacks in the threat model based on CVSS v4.0.

Attack Name	Attack Vector	Attack Complexity	Attack Requirements	Privileges Required	User Interaction	Confidentiality	Integrity	Availability	CVSS Score
433MHz									
Fob Transmission Jamming	Network	Low	None	None	Passive	None	None	High	7.1
Replay Attack	Network	Low	None	None	Passive	High	High	None	8.6
Rolljam Attack	Network	High	Present	None	Passive	High	High	None	7.6
Sensor to Base Jamming	Network	Low	None	None	None	None	None	High	8.7
Bluetooth									
Sniffing	Network	High	Present	None	Passive	High	High	None	7.6
PITM	Network	High	Present	None	Passive	High	High	None	7.6
Data Manipulation	Network	Low	None	None	None	Low	High	High	8.8
Jamming	Network	Low	None	None	None	None	None	High	8.7
RFID									
Encrypted Tag Cloning	Local	High	Present	None	None	High	High	High	7.5
Tag Cloning	Local	Low	None	None	None	High	High	None	8.5

to set up and deploy an attack, with *Low* reflecting less than 15 min, *High* greater than 15 min. *Attack Requirements* captures the cost of the tools required to perform the attack, with *None* reflecting less than £50 and *Present* £50 or more. The rest of the submetrics are valuated based on the CVSS documentation. Table 3 summarises the criticality of the attacks that are in the scope of this work. CVSS v4.0 vector strings for each vulnerability can be found in Appendix A. Finally, this work aligns with (NVD, 2023) and considers a CVSS score 9.0–10 as Critical, 7.0–8.9 as High, 4.0–6.9 as Medium, and 0.1–3.9 as Low.

4. Experimental results

The following subsections discuss our findings for each attack vector, which are summarised in Tables 4–6. During our experiments, we have uncovered 14 zero-day vulnerabilities, which have been reported to the vendors and published in the Common Vulnerability and Exposure knowledge base, by following an ethical disclosure procedure. It is worth noting that only devices that support the access vectors that are in scope of this work are included in Tables 4–6.

4.1. Protection against 433MHz radio frequency attacks

Our experiments suggest that most of the tested devices can be attacked successfully via the 433 MHz access vector. As shown in Table 4, every lesser known brand device was prone to jamming. This allows an attacker to block messages between remote sensors and the base station, giving unimpeded access to the protected area. Moreover, these devices were also found susceptible to both replay and RollJam attacks. None of the devices used rolling codes (an example of sequential key press is shown in Fig. 1) and none used frequency hopping or

Table 4
Susceptibility on attacks using 433 MHz as the attack vector. N/A represents that the attack cannot be attempted as the device does not support part of this technology (e.g., fobs not available).

Smart Security Device	Fob Transmission Jamming	Sensor to Base Jamming	Replay Attack	RollJam Attack
AGSHome Smart Alarm	Yes	Yes	Yes (CVE-2023–31,763)	Yes
Blitzwolf Alarm	Yes	Yes	Yes (CVE-2023–31,761)	Yes
Digoo Smart Alarm	Yes	Yes	Yes (CVE-2023–31,762)	Yes
Kerui Alarm	Yes	Yes	Yes (CVE-2023–31,759)	Yes
Wafu Keyless Smart Lock	Yes	Yes	Yes (CVE-2023–34,553)	Yes
Yale IA-210	N/A	No	N/A	N/A
Yale Conexis	No	No	No	No
Yale Keyless	No	No	No	No

Table 5
Susceptibility on attacks using Bluetooth as the attack vector.

Smart Security Device	Sniffing	Jamming	Data Manipulation	PITM
Bluetooth Bike Lock	No	No	No	No
Bluetooth Padlock	Yes	No	Yes	Yes
eGeeTouch Smart Padlock	Yes (CVE-2021–44,518)	No	Yes	Yes
Fortessa Smart Lock	No	No	Yes (CVE-2021–44,905)	Yes
Nuki Smart Lock	No	No	No	No
Tuya Spindle Lock	No	No	Yes	Yes
Ultraloq UL3	Yes	No	Yes	Yes (CVE-2022–46,480)
WAFU Smart Biometric Lock	No	No	No	Yes
Yale Conexis	No	No	No	No

Table 6
Susceptibility on attacks using RFID as the attack vector. N/A indicates no encryption present on the tag.

Smart Security Device	Tag Cloning	Encrypted Tag Cloning
5-in-1 Smart Door Lock	Yes (CVE-2023–39,843)	N/A
Digoo Smart Alarm	Yes (CVE-2023–39,842)	N/A
eGeeTouch Smart Padlock	No	No
Etekcity 3-in-1 Lock	Yes (CVE-2023–39,841)	N/A
Yale Conexis	No	Yes (CVE-2023–26,941)
Yale IA-210	No	Yes (CVE-2023–26,942)
Yale Keyless	No	Yes (CVE-2023–26,943)

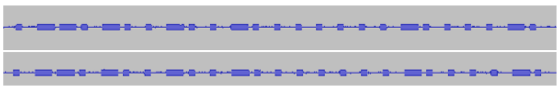

Fig. 1. Sequential key presses on the Kerui alarm arming fob, illustrating the lack of rolling codes.

jamming detection. Rolling codes, such as Keeloq (Indesteege et al., 2008) remove the replay susceptibility, but are still vulnerable to code capture and replay, as with the RollJam attack.

In contrast, the branded smart security products protect their users from the aforementioned attacks. Specifically, all three Yale devices provide frequency hopping, as well as the Yale alarm has built in jamming protection. This is especially important for an alarm as the sensor to base communication uses this channel. As depicted in Table 4, our work uncovers five new CVEs that cannot be patched with a software update.

4.2. Protection against bluetooth attacks

As summarised in Table 5, using Bluetooth as the attack vector provides different opportunities to a cyber attacker-burglar. Specifically, the data manipulation attacks we mounted uncovered that five of nine smart security devices allowed unauthenticated write access. These attacks involved identifying the device via its MAC address then sending a pairing request. In cases where pairing was permitted without any authentication, we then sent several read requests to endpoints specified in the device's Generic Attribute Profile (GATT). If these are successful, write attempts are then made against the same targets. Our experiments suggest that by following this process a threat actor can cause a denial-of-service attack on the *Fortessa* lock and, even worse, unlock the following devices: (i) *Ultraloq UL3*, (ii) *eGeeTouch,* and (iii) *Bluetooth Padlock* devices. The three CVEs represent zero-day attacks against the affected devices. Vendor response is discussed in Section 5. It should be noted that as of the time that this paper was written, none of the affected devices has been patched.

Our experiments uncover that a threat actor would be able to clone the GATT in six of nine devices tested (see Table 5), with five of the nine devices being completely compromised. The only two devices that are not susceptible to any of the Bluetooth attacks that we have mounted were the *Yale Conexis* and the *Bluetooth Bike Lock*. It is worth mentioning that the latter is somewhat surprising as a similar smart security device was previously vulnerable to this attack (Jasek S., 2017). The smart security device worked correctly with its companion app and armed and disarmed successfully, which suggests that the manufacturer has patched the device.

Finally, the results indicate that *Ultraloq UL3* offers poor protection against Bluetooth attacks. In specific, our work uncovered that the device unlocks upon receiving a 16-byte value to a specific service specified via the GATT, which is static. As a result, this value can be easily sniffed and replayed to unlock the device, as shown in Snippet 6 in Appendix B.

4.3. Protection against RFID attacks

The success of the RFID attacks heavily relies on the RFID technology supported by each device, namely using low or high frequency tags. The *eGeeTouch* and the three *Yale* devices use high frequency RFID tags whilst the remaining devices use low frequency tags. All are passive tags, meaning they do not possess an internal power source. As summarised in Table 6, all low frequency tags can be cloned by a threat actor within seconds, thus offering no protection to their users.

As discussed earlier, higher frequency tags support more data transfer. They are also often encrypted, as in *eGeeTouch* padlock, thus, they are less likely to be prone to tag cloning. As summarised in Table 6, this is the case with the Yale smart security devices, which cannot be cloned as there are encrypted. Nonetheless, our experiments uncover that cryptographic standards and guidelines have not been met, thus, exposing their users to tag cloning. This holds true as the three *Yale* devices use Mifare Classic 13.56 MHz cards and use encryption that can be easily bypassed by threat actors. In particular, the cards supplied with the Yale *IA-210* alarm are encrypted using the default encryption key (i.e., **FFFFFFFFFFFF**). As a result, a threat actor can easily decrypt and

Table 7
Susceptibility on attacks using different attack vectors and their criticality. The × symbol is used to indicate attack failure, and ✓ symbol is used to indicate attack success. Empty cells indicate the attack is not relevant to the device. C(ritical), H(igh), M(edium), L(ow), and N(one) indicate Criticality based on CVSS 4.0.

Attack (CVSS Score) \ Security device	Bluetooth Bike Lock	Bluetooth Padlock	eGee Touch	5-in-1 Smart Lock	Etekcity 3-in-1	Fortessa Smart Lock	Nuki Smart Lock	Tuya Spindle Lock	Ultraloq UL3	WAFU Keyless Smart Lock	WAFU Smart Biometric	Yale Conexis L1	Yale Keyless	AGSHome Smart Alarm	Blitzwolf Alarm	Digoo Smart Alarm	Kerui Alarm	Yale IA-210
433 MHz Attack Vector																		
Fob Transmission										✓		×	×	✓	✓	✓	✓	
Jamming (7.1)																		
Replay Attack (8.6)										✓		×	×	✓	✓	✓	✓	
RollJam Attack (7.6)										✓		×	×	✓	✓	✓	✓	
Sensor to Base Jamming (8.7)														✓	✓	✓	✓	×
Bluetooth Attack Vector																		
Sniffing (7.6)	×	✓	✓			×	×	×	✓		×	×						
PITM (7.6)	×	✓	✓			✓	×	✓	✓		✓	×						
Data Manipulation (8.8)	×	✓	✓			✓	×	✓	✓		×	×						
Jamming (8.7)	×	×	×			×	×	×	×		×	×						
RFID Attack Vector																		
Encrypted Tag Cloning (7.5)			×									✓	✓					✓
Tag Cloning (8.5)			×	✓	✓							×	×			✓		×
Criticality based on attack Susceptibility																		
Criticality (CVSS Score)	N	H	H	H	H	H	N	H	H	H	H	H	H	H	H	H	H	H

clone the card. The *Yale Keyless* lock uses a unique set of encryption keys on the first seven blocks, as seen in Snippet 2 in Appendix B. However, our experiments uncover that it uses CRYPTO1, which has been proven to be insecure in 2008 (Courtois et al., 2008). As a result, the card can be decrypted promptly, i.e., within 10–20 s, and cloned as long as the threat actor has brief access to a card or keyfob. It is worth noting that once a card is cloned: *i)* there is no limit on how many times it can be used to open the lock and *ii)* it is impossible for the device user to infer that their card has been cloned and used to open the lock. Finally, the *Yale Conexis* lock also uses non-default keys for the first seven blocks. However, data is also written to other locations on the card during use. The master RFID card is paired with the lock using a physical button on the inside portion of the lock. During every pairing a counter is incremented inside block 2 on the card. During initialization a pair of randomly chosen adjacent blocks are initialized with two random values. These are then incremented in a "tick-tock" manner every time the card is activated – please refer to Snippet 5 in Appendix B. This, coupled with the counter written to block 2, limits the window for use that an attacker has for a cloned card, but does not prevent the occurrence of the attack. While performing the RFID experiments, we uncovered six previously unknown, zero-day vulnerabilities that as part of our responsible disclosure: a) have been reported to the vendors and b) are listed in the Common Vulnerabilities and Exposures (CVE) database (see Table 6). Finally, we note that at the point of submission of this paper, a vendor patch is not available.

5. Discussion

This subsection will discuss the (*i)* criticality of the attacks that a cyber attacker-burglar can successfully mount against the tested devices (*ii)* workarounds or mitigations that can protect the device's owner, as well as (*iii)* inefficiency of relevant performance standards.

Attack Criticality. Table 7 summarizes: (*a)* the criticality of the attacks mounted against the smart security devices that we assessed based on the modified CVSS score, which is discussed in Section 3.3, and (*b)* the susceptibility of the smart security devices to these attacks. As discussed earlier, some devices were vulnerable to more than one attack, thus the overall criticality is computed as the max CVSS score from the applicable attacks.

Our results uncover that almost all the smart security devices (refer to Table 7) that we have tested will fail to protect their users from an unsophisticated cyber attacker-burglar (refer to Section 3.2). This holds true as at least one attack against sixteen out of eighteen devices was successful, as well as having a *High* criticality score. Moreover, our experiments lead to the discovery of 14 zero-day attacks that were possible via the three access vectors used, i.e., 433 MHz, Bluetooth, and RFID. The details of our zero-day attacks have been reported to their vendors, following a responsible disclosure procedure, and have led to 14 published CVEs. In specific, these attacks represent significant flaws in the products that allow an attacker to: (*i)* achieve full control over the device in CVE-2023–31,759, CVE-2023–31,761, CVE-2023–31,762, CVE-2023–31,763, CVE-2023–34,553, CVE-2021–44,518, CVE-2022–46,480, CVE-2023–39,841, CVE-2023–39,842, and CVE-2023–39,843, (*ii)* realise a denial-of-service attack in CVE-2021–44,905, and (*iii)* impersonate a legitimate user in CVE-2023–26,941, CVE-2023–26,942, and CVE-2023–26,943.

From a threat actors' perspective, one would expect 433 MHz and RFID as attack vectors to provide more opportunities to mount a successful attack compared to Bluetooth. This is due to the pervasiveness of Bluetooth in consumer devices, which has led to considerable effort, from academia and industry, to enhance its security. On the contrary, our experiments show that Bluetooth offers considerable opportunities to a cyber attacker-burglar. With regards to their criticality, as the two 433 MHz jamming attacks are trivial to perform their success leads to the manifestation of attacks with considerable criticality, with CVSS scores 7.1 and 8.7 respectively. The criticality of the Bluetooth attacks is limited by the high financial cost of the tools required and the time necessary to prepare for the attack. Finally, amongst the RFID attacks, cloning an encrypted tag has the potential for impact across the three domains of the CIA triad, as seen with the Conexis L1 lock where the use of the cloned tag impairs the availability of the lock's owner.

Inefficiency of performance standards. The BSI Kitemark is currently the "gold standard" for smart lock products sold in the United Kingdom, indicating that they have met or exceeded the performance requirements set out in the testing framework. In the case of mechanical locks (BS3621), this means that they must withstand a specific number of calibrated tests and must perform in a particular manner. For example, they possess at least five levers or pins and have a bolt that extends at least 20 mm from the faceplate when locked. Conversely the current framework for smart locks, i.e., TS621, reads more like the requirements for a penetration test. An attacker is given a certain amount of preparation time and attack time. If they are unable to break into the lock, then it is considered to meet the BSI performance standard. This framework is entirely different conceptually from BS3621. The requirements of BS3621 are replaced with a set of tests that are heavily dependent on the skills of the person performing them. A BS3621-compliant lock will *always* have at least 5 levers and will *always* have a bolt that extends 20 mm or more. However, it is not safe to assume that the same applies with a TS621-compliant smart lock. The smart lock may pass when the tests are conducted by one user but may fail when the tests are performed by a more highly trained or competent user. In addition, the presence of zero-day vulnerabilities, like the ones that have been uncovered in this work, makes the completeness of the tests unclear. This presents significant challenges for users to overcome when purchasing devices and for bodies, such as insurers, when certifying them. For instance, the Yale Conexis L1 has a BSI Kitemark, yet within this work we demonstrate an attack that successfully compromises it.

We also note that other performance standards for smart security devices are used by manufacturers in their promotional material, such as Builders Hardware Manufacturers Association (BHMA) in the US (Schlage, 2023), and BS EN 1303 (Hoppe, 2023) and BS EN 1670 (NBS, 2023) in the UK. However, these standards refer only to the mechanical security of the device. Using such a standard leaves their user in an uncertain position. This holds true as the lock may be physically robust, but the security performance of the cyber component is unknown.

Moreover, there are also instances where ISO quality and software standards are used in marketing material, e.g., ISO 9001 (PS GmbH, 2023) and ISO 27001 (Salto, 2020) respectively. Whilst it is encouraging to see companies attaining to this level of assurance, they are not relevant to the smart security devices themselves and are likely to cause confusion to their users. Adhering to ISO 9001 and ISO 27001 does not imply that the end product is secure. A more pragmatic testing scheme is provided by AV Test, a security company based in Germany (AV Test, 2023). Here, devices are subjected to a number of tests and if they pass, then they are certified for a period of one year. If the manufacturers wish to extend the certification further, an additional retest is required. Whilst there are concerns with regards to the testing process, as the list of tests performed is not available, users have a level of assurance that their device has passed a defined number of requirements. This is more similar to BS 3621, with its defined requirements, than it is to TS 621 with its open-ended approach. Annual certification places the onus on manufacturers to make sure their devices can be updated and for them to produce timely patches if they wish to remain certified by passing the next annual retest.

Mitigation. As mentioned earlier, this work uncovered 14 zero-day vulnerabilities and as a first step we attempted to share them with the device vendors to trigger their mitigation, before sharing them with the security community. In all cases it proved impossible to report a vulnerability via the channels stated on the relevant company website – i.e., no responses were received from any of the vendors. When we widened the disclosure efforts and contacted senior security leaders in the respective companies via LinkedIn, two of the vendors responded.

One in particular was extremely willing to work with us and we had useful and commendable discussions around the affected devices. Similarly, the second vendor took our disclosure report and managed to replicate the attacks internally. Of concern, however, was the fact that while discussing with the vendors we were informed that the devices tested were no longer part of their current range, even though they were still being sold to consumers. This suggests that patches for devices already sold might never be available. This is concerning, as the price point of these devices means that one would not consider this device "disposable". Furthermore, the expectation of security savvy users to upgrade to the latest version to mitigate serious vulnerabilities might be unrealistic given the additional costs. This could adversely affect user confidence in the home IoT space. At the same time, one should also note that only two vendors responded to our disclosure. Despite multiple attempts through a variety of channels, as of the time of submission of this work the rest of the vendors have not acknowledged these vulnerabilities. This could mean that the manufacturers and 3rd party suppliers of these devices are therefore unaware that their smart security devices contain vulnerabilities and so cannot provide any mitigation to their end users.

The resolution or mitigation of these attacks varies depending on the attack vector. For attacks using *433 MHz as the attack vector*, manufacturers could incorporate mechanisms for the detection of jamming signals. For instance, the current British standard (BSI, 2017) grades alarm systems on a scale from 1 (lowest) to 4 (highest). A system with any wireless component can only be rated as grade 2 at most – this is set out in the Europe-wide EN 50,131 standard, as discussed in (Eldes Security, 2023). At this grade, it must register a jamming attempt if a signal is detected for more than 30 s in any 60 s period, which might not be efficient. Based on our experiments, a keyfob press will not exceed one *sec* in duration, so even multiple presses will likely not exceed more than 5 s. We consider that enforcing jamming protection in devices and reducing the jamming identification window to 10 s would effectively nullify simple jamming attacks, which would be sufficient for consumer use. Users with devices lacking this protection could purchase or build a stand-alone jamming detection device. These could be a cost-effective small form factor device (e.g., a Raspberry Pi) that alerts the owner upon jamming attempts by constantly scanning the appropriate frequencies for interference. On the contrary, mitigation of attacks that exploit code reuse is far more challenging. As such, we consider that a security device must not use non-rolling codes for command and control. The use of a shared secret rolling code is easy to implement and any additional hardware needed has low cost. Furthermore, this cost is disproportional to the cost of recalling the devices from consumers. The combination of jamming detection and rolling codes would also address RollJam-style attacks that have been used in our experiments. This holds true, as they rely on a jamming component to steal an active code. If jamming detection with a suitably small window is used, this attack becomes much harder to achieve.

Similarly, RFID attack mitigations rely either on the user, or the device's vendor. Users have control over the most important component, i.e., the RFID tag. Without access to the tag an attack becomes impossible. Keeping these in an RFID blocking wallet or purse thus makes an attacker's task considerably more difficult. At the same time, avoiding low frequency tags is also important if the vendor prioritises the security of the device. Given that these can be instantly cloned, the opportunity for an attacker is considerable. Also, the vendors should avoid shipping smart security devices using RFID technology that is known to be broken. However, apart from one device all the rest that were in our scope were found to either use low frequency tags, or Mifare Classic tags. The encryption used by the latter has been broken since 2008. Instead of using insecure tags vendors must use current secure alternatives, such as the NTAG tag employed by the eGeeTouch padlock. In addition, we consider that vendors should add "over the air" (OTA) updates, via Wi-Fi or Bluetooth, to their devices. OTA updates can configure the device to only support new tag types when those currently used are found to be insecure. Again, we consider that the cost of implementing the aforementioned and supplying their users with more secure tags is disproportionate to the cost of recalling and replacing the smart security device.

For the mitigation of the attacks that use Bluetooth the users are at the mercy of developers. At minimum, we consider that a smart security device must ensure that sensitive data are encrypted, using the relevant standards, and that replay attacks cannot take place. We consider that OTA updates would also help to mitigate new attacks, especially those targeting the Bluetooth chipset itself. Otherwise, vendors could move towards a more costly solution that uses a modular design, where vulnerable components can be removed and replaced in order to provide device robustness. At the same time, users must disable functionality that could be misused by threat actors, which might not be possible as they are not necessarily security and technically savvy. For instance, many Bluetooth attacks in this work could be avoided if proximity-based Bluetooth auto-unlock/auto-disarm features were disabled. Otherwise, the lock can be unlocked even when its legitimate owner Bluetooth device is not near the smart lock's proximity. In this case the owner might wrongly consider that their Bluetooth device cannot be manipulated to unlock the smart lock and thus become less conscious of such attack. However, Bluetooth signals can be transmitted via a proxy and a well-prepared attacker could misuse the auto-unlock feature, thus enabling access to an accomplice who is near the lock. Finally, the users must also be trained to ensure that Bluetooth connections to smart security devices do not remain open once they have opened or closed a door or armed the alarm. This makes it more difficult for an attacker to piggyback on the connection and misuse data in a subsequent attack.

6. Conclusion

This work uncovers that smart security devices such as smart locks, padlocks, and intruder alarms, which are nowadays becoming ubiquitous, expose their users to a number of threats that impair their security. Our experiments suggest that an unsophisticated cyber attacker-burglar can utilise popular wireless technologies, such as RFID and Bluetooth, in order to achieve different attacks that enable them to bypass the device or make it unavailable for its users. We uncover new zero-day attacks that a cyber attacker-burglar can use against the devices in scope and discuss their mitigations or workarounds, as well as our attempts to communicate them to their vendors as part of a responsible disclosure process. Their details have now been shared with the security community via the Common Vulnerability and Exposure knowledge base.

Moreover, our results suggest that further consideration is necessary regarding the assurance that is provided by current performance standards awarded by bodies, such as the British Standards Institute (BSI). As discussed in Section 5, the BSI Kitemark is the "gold standard" for smart lock products sold in the United Kingdom, indicating resilience against an attacker-burglar. Nonetheless, within this work we demonstrate an attack that compromises the Yale Conexis L1, a smart lock that has a BSI Kitemark. Moreover, currently the manufacturers refer in their marketing material to their compliance to performance standards that either do not provide complete and repeatable testing (e.g., TS 621 vs. BS 3621), or are not relevant to the cyber component of the smart security device, as in BHMA, BS EN 1303, and BS EN 1670. This presents significant challenges for users to overcome when purchasing devices and for bodies, such as insurers, when certifying them.

As any other IoT device, their vendors face challenges when bringing their products to the market, which directly impact the likelihood of finding early their vulnerabilities. For instance, often vendors do not create their own chips for common tasks, such as Bluetooth communication, but instead are more likely to use off-the-shelf components and their associated software libraries for this type of interface. This greatly decreases the time to market for a device, but it also exposes users to security risks. This holds true as when a vulnerability is discovered in one of the off-the-shelf components, potentially all devices that share the

same component are vulnerable to the same attack. An example of this is the Sweyntooth collection of exploits (Garbelini et al., 2020). These target specific chipsets rather than software, and the impact in the supply chain was felt far beyond the initial disclosure (Microchip.com, 2023). Amongst the smart security devices that are in scope of this work, less than half have a facility to allow firmware updates. This means that vulnerabilities will remain exploitable for the lifespan of the device. As a result, their users, who might not be security and technically savvy, will continue to be exposed to the attacks that we have demonstrated in this work as long as they use this device, unless the device is recalled or otherwise patched.

Our experiments also highlight that the quality of individual protocol implementation across devices varies. This may stem from poor security design, failure to adopt secure coding standards, or trade-offs imposed by financial and other constraints. For instance, poor implementation practices found include the use of default keys when encrypting fob data, as well as the use the long-broken CRYPTO-1 encryption employed by Mifare Classic cards. More resilient options are available, such as the NTAG format used by the eGeeTouch, or the Mifare DESFire standard, which were expected to be more popular amongst the devices that were in scope of this work. Additionally, the quality of implementation of *different* protocols within the *same device* was found different. As an example, bypassing the Bluetooth implementation of eGeeTouch padlock was trivial, as the device is vulnerable to even simple attacks. Nonetheless, it was the only smart security device where the associated RFID fob could not be decrypted and cloned. This could suggest that the vendors have different priorities in securing the different attack vectors, or again this could stem from poor design issues, code quality, or other additional constraints.

If one considers the considerable limitations with respect to device updates, this work considers that these should be avoided, irrespective of their cost or brand. This holds true, as they might be considered secure at the current point in time due to rigorous testing based on the current known vulnerabilities, but it is unclear whether other undisclosed vulnerabilities exist, which threat actors have discovered and that the manufacturer either does not know about or is not able to patch. Furthermore, the results from this work highlight how important security-by-design and rigorous security testing is for such devices before entering the market, especially if their vendor cannot patch them after a vulnerability has been discovered.

Finally, this work assumes a specific threat model describing the expertise and resources of the attacker and the device's owner. We consider that our threat model represents the most realistic use case of such a smart security device, as these target end users. Nonetheless, other threat models could be developed, e.g., including state-sponsored attacks, but are out of scope of this work and we leave them for future work.

CRediT authorship contribution statement

Ashley Allen: Conceptualization, Methodology, Investigation, Visualization, Writing – original draft. **Alexios Mylonas:** Conceptualization, Methodology, Investigation, Visualization, Writing – original draft, Validation, Supervision. **Stilianos Vidalis:** Methodology, Writing – review & editing, Validation. **Dimitris Gritzalis:** Methodology, Writing – review & editing, Validation, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Appendix A. CVSS v4.0 Vectors

Table 8 includes the CVSS v4.0 vector for each of the attacks that we have attempted based on the threat model (see Section 3).

Table 8
CVSS v4.0 vector strings.

Attack	CVSS Vector	CVSS Score
Fob Transmission Jamming	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	7.1
Replay Attack	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	8.6
Rolljam Attack	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	7.6
Sensor to Base Jamming	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	8.7
Btlejack – Sniffing	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	7.6
Gattacker - PITM	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	7.6
HomePwn – Data Manipulation	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N	8.8
Sweyntooth - Jamming	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	8.7
Encrypted Tag Cloning	CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	7.5
Tag Cloning	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	8.5

Appendix B. – Supplementary material for attacks performed

This section includes supplementary material regarding the attacks that have been discussed in Section 4.

Attacks using RFID as the attack vector. As shown in Snippet 1, upon scanning the RFID tag of the Yale IA-210 alarm, the only information present on the card is the UUID in the first block. As such, a cyber attacker-burglar only needs to duplicate this value to the correct block on a blank card to gain access to the alarm.

```
[=] ----+-------------------------------------------------+
[=] blk | data                                            |
[=] ----+-------------------------------------------------+
[=]   0 | 3D 06 CD 45 B3 88 04 00 C8 42 00 20 00 00 00 16 |
[=]   1 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
[=]   2 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
[=]   3 | FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF |
```

Snippet 1. Data from RFID tag sector 0.

In contrast, as shown in Snippet 2, the tags that are used by the Yale Keyless lock and the Yale Conexis lock use non-default encryption keys:

```
[+] -----+-----+--------------+---+--------------+----
 [+]  Sec | Blk | key A        |res| key B        |res
[+] -----+-----+--------------+---+--------------+----
 [+]  000 | 003 | 681E9E9B3FE9 | N | FFFFFFFFFFFF | D
 [+]  001 | 007 | ADAE73113441 | N | FFFFFFFFFFFF | D
 [+]  002 | 011 | 6C6FAAC8E598 | N | FFFFFFFFFFFF | D
 [+]  003 | 015 | BFBCF91B36CB | N | FFFFFFFFFFFF | D
 [+]  004 | 019 | 58599AF4D3A4 | N | FFFFFFFFFFFF | D
 [+]  005 | 023 | 828340E60956 | N | FFFFFFFFFFFF | D
 [+]  006 | 027 | 5F5E9D3BD48B | N | FFFFFFFFFFFF | D
 [+]  007 | 031 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  008 | 035 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  009 | 039 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  010 | 043 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  011 | 047 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  012 | 051 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  013 | 055 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  014 | 059 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
 [+]  015 | 063 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+] -----+-----+--------------+---+--------------+----
```

Snippet 2. Encryption keys for each sector.

The use of non-default keys is the only defence against cloning used by the RFID implementation on the Yale Keyless Smart Lock. Moreover, Yale Conexis L1 attempts to provide extra protection against tag cloning by adhering to the following protocol. During the initial pairing or following a system reset a counter is incremented in block 2 of the card, as shown in Snippet 3.

```
                "blocks": {
"0": "95E43AA5EE08040002E9981FA7F5D11D",
"1": "095FCA99D806ECCEB9328A6466CA3D10",
"2": "080807000000000000000000000000000",

                "blocks": {
"0": "95E43AA5EE08040002E9981FA7F5D11D",
"1": "095FCA99D806ECCEB9328A6466CA3D10",
"2": "090907000000000000000000000000000",
```

Snippet 3. Pairing increment in block 2 – Yale Conexis L1.

Upon initialization a pair of adjacent blocks is selected and initialized with two random values. As shown in Snippet 4, blocks 4 and 5 have been chosen, namely:

```
"4": "F55129991B00000000000000000000000",
"5": "B858981867000000000000000000000000",
```

Snippet 4. Data initialization during RFID tag pairing, Yale Conexis L1.

These are then incremented in a "tick-tock" manner every time the card is activated as shown in Snippet 5.

```
"4": "F55129991B00000000000000000000000",
"5": "60E0E0E087000000000000000000000000",

"4": "FF931B6B2300000000000000000000000",
"5": "60E0E0E087000000000000000000000000",

"4": "FF931B6B2300000000000000000000000",
"5": "E6EEBEDE6F00000000000000000000000",

"4": "3070F0F047000000000000000000000000",
"5": "E6EEBEDE6F00000000000000000000000",
```

Snippet 5. "Tick-Tock" sector updating during successive tag activation events – Yale Conexis L1.

As a result, the window of time that an attacker can use a cloned card is limited. This holds true since if the original card is used before the cloned card, the value in one of the adjacent blocks will be updated. When the cloned card is presented, it will not match the sequence that is expected by the reader and, thus, will fail to open the lock. Conversely, if the cloned card is used first, then the original card is now out of sync and thus the legitimate owner of the device will no longer be able to open the lock with the RFID card. In this scenario the legitimate user must pair again their card with the lock, once they have gained access to their house via other means (e.g., physical key). This will increment the counter in block 2, and reinitialize two adjacent blocks with new seed values, thereby blocking the cloned card.

Attacks using Bluetooth as the attack vector. Fig. 2 illustrates the data transfer between the *eGeeTouch* lock and the associated companion app. The lock receives a write request to a specific handle:

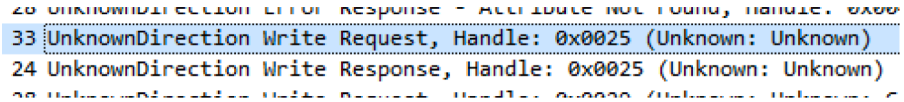

Fig. 2. Write request.

This handle is defined inside the packet with a specific service ID and characteristic:

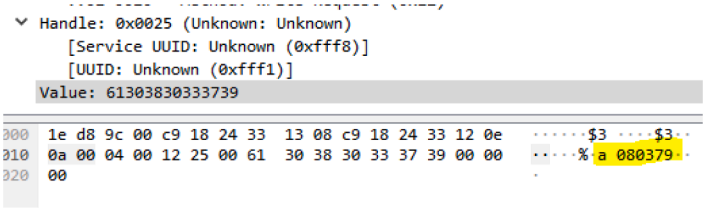

Fig. 3. Write request contents.

The data sent to the device is a padded string that translated into the highlighted payload in Fig. 3. As part of the initial paring process, the *eGeeTouch* lock requests that a password is set. The value shown here is this password (*080379*). As shown in Fig 4, the values sent during the unlock process are sent in plain text, allowing them to be captured and replayed:

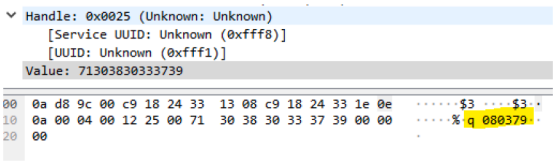

Fig. 4. Unlock event.

Snippet 6 provides additional data regarding the attack of Ultraloq UL3 that has been discussed in Section 4. As shown below, when repeated unlock commands are sent to the Bluetooth handle that controls the unlocking of the device, the same static responses are received. This can be seen in the Snippet below, where every unlock event (having a 16-byte string beginning *08c711*) is followed by the same pattern of responses. These unlock commands can be captured and then replayed thus unlocking the device.

```
2022.11.15 17:59:32.844 | < C | 7200 | 7201 | 08c71149fb1a7105298eaf175bf5166b (   I  q )    [  k)
2022.11.15 17:59:33.047 | > N | 7200 | 7201 | 5970e43108c32af5811fbfb3bfce5400 (Yp 1  *       T )
2022.11.15 17:59:33.766 | > N | 7200 | 7201 | f086584891767d5f32b22674bb2dcb49 (  XH v}_2 &t - I)
2022.11.15 17:59:38.762 | > N | 7200 | 7201 | 2b2dcdae303f8df4fb109e818189fb74 (+-  0?         t)
2022.11.15 17:59:41.244 | < C | 7200 | 7201 | 08c71149fb1a7105298eaf175bf5166b (   I  q )    [  k)
2022.11.15 17:59:41.446 | > N | 7200 | 7201 | 5970e43108c32af5811fbfb3bfce5400 (Yp 1  *       T )
2022.11.15 17:59:42.167 | > N | 7200 | 7201 | f086584891767d5f32b22674bb2dcb49 (  XH v}_2 &t - I)
2022.11.15 17:59:47.147 | > N | 7200 | 7201 | 2b2dcdae303f8df4fb109e818189fb74 (+-  0?         t)
2022.11.15 17:59:49.644 | < C | 7200 | 7201 | 08c71149fb1a7105298eaf175bf5166b (   I  q )    [  k)
2022.11.15 17:59:49.847 | > N | 7200 | 7201 | 5970e43108c32af5811fbfb3bfce5400 (Yp 1  *       T )
2022.11.15 17:59:50.567 | > N | 7200 | 7201 | f086584891767d5f32b22674bb2dcb49 (  XH v}_2 &t - I)
2022.11.15 17:59:55.547 | > N | 7200 | 7201 | 2b2dcdae303f8df4fb109e818189fb74 (+-  0?         t)
2022.11.15 17:59:57.263 | < C | 7200 | 7201 | 08c71149fb1a7105298eaf175bf5166b (   I  q )    [  k)
2022.11.15 17:59:57.467 | > N | 7200 | 7201 | 5970e43108c32af5811fbfb3bfce5400 (Yp 1  *       T )
2022.11.15 17:59:58.187 | > N | 7200 | 7201 | f086584891767d5f32b22674bb2dcb49 (  XH v}_2 &t - I)
2022.11.15 18:00:03.168 | > N | 7200 | 7201 | 2b2dcdae303f8df4fb109e818189fb74 (+-  0?         t)
```

Snippet 6. Communication between the Ultraloq UL3 and its companion app.

References

Aghili, S.F., Mala, H., Kaliyar, P., Conti, M., 2019. SecLAP: secure and lightweight RFID authentication protocol for medical IoT. Future Gener. Comput. Syst. 101, 621–634. https://doi.org/10.1016/j.future.2019.07.004.

Ahmad, K.A., Salleh, M.S., Segaran, J.D., Hashim, F.R., 2018. Impact of foliage on LoRa 433MHz propagation in tropical environment. In: Proceedings of the AIP Conference 1930. AIP, 020009. https://doi.org/10.1063/1.5022903.

Aras, E., Ramachandran, G.S., Lawrence, P., Hughes, D., 2017. Exploring the security vulnerabilities of LoRa. In: Proceedings of the 2017 3rd IEEE International

Conference on Cybernetics (CYBCONF). Exeter. IEEE, pp. 1–6. https://doi.org/10.1109/CYBConf.2017.7985777.
AV Test. (2023). Testing: smart home. Retrieved 12 04, 2023, from https://www.av-test.org/en/internet-of-things/smart-home/.
Badenhop, C.W., Graham, S.R., Ramsey, B.W., Mullins, B.E., Mailloux, L.O., 2017. The Z-Wave routing protocol and its security implications. Comput. Secur. 68, 112–129. https://doi.org/10.1016/j.cose.2017.04.004.
BangGood. (2022, August 14th). RFID NFC card copier reader writer duplicator English 10 frequency programmer for IC ID Cards. Retrieved 12 05, 2023, from https://uk.banggood.com/RFID-NFC-Card-Copier-Reader-Writer-Duplicator-English-10-Frequency-Programmer-for-IC-ID-Cards-p-1752638.html.
Banham Security. (2022, August 14th). BS 3621 and the importance of the British standard. Retrieved 12 05, 2023, from Banham Security: https://www.banham.co.uk/doors-locks/locks/bs3621-locks/.
Barua, A., Al Alamin, M.A., Hossain, M.S., Hossain, E., 2022. Security and privacy threats for Bluetooth low energy in IoT and wearable devices: a comprehensive survey. IEEE Open J. Commun. Soc. 3, 251–281. https://doi.org/10.1109/OJCOMS.2022.3149732.
Boucif N., Golchert F., Siemer A., Felke P., & Gosewehr F. (2020). Crushing the Wave–new Z-Wave vulnerabilities exposed. arXiv preprint arXiv:2001.08497.10.48550/arXiv.2001.08497.
BSI. (2017). Alarm systems. intrusion systems - requirements for interconnections equipment using radio frequency techniques. Retrieved 08 21, 2023, from https://knowledge.bsigroup.com/products/alarm-systems-intrusion-systems-requirements-for-interconnections-equipment-using-radio-frequency-techniques/tracked-changes/details.
Cäsar M., Pawelke T., Steffan J., & Terhorst G. (2022). A survey on Bluetooth low energy security and privacy. Computer Networks, 108712.10.1016/j.comnet.2021.108712.
Chantzis, F., Stais, I., Calderon, P., Deirmentzoglou, E., Woods, B., 2021. Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things. No Starch Press.
Chatzisofroniou, G., Kotzanikolaou, P., Groß, T., Tryfonas, T., 2021. Association attacks in IEEE 802.11: exploiting WiFi usability features (Ed.). Socio-Technical Aspects in Security and Trust. Springer International Publishing, Cham, pp. 107–123.
Courtois N.T., Nohl K., & O'Neil S.. (2008). Algebraic attacks on the crypto-1 stream cipher in MiFare classic and oyster cards. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. https://eprint.iacr.org/2008/166.
Csikor, L., Lim, H.W., Wong, J.W., Ramesh, S., Parameswarath, R.P., Chan, M.C., 2023. RollBack: a new time-agnostic replay attack against the automotive remote keyless entry systems. ACM Trans. Cyber Phys. Syst. https://doi.org/10.1145/3627827.
Davis, B.D., Mason, J.C., Anwar, M., 2020. Vulnerability studies and security postures of IoT devices: a smart home case study. IEEE Internet Things J. 7 (10), 10102–10110. https://doi.org/10.1109/JIOT.2020.2983983.
Dogan, H., Çaglar, M.F., Yavuz, M., Gözel, M.A., 2016. Use of radio frequency identification systems on animal monitoring. Int. J. RF Microwave Comput. Aided Eng. 8, 38–53. https://doi.org/10.1002/mmce.21674.
Door & Hardware Federation. (2022, August 14th). Thief Resistant Electronic Door Locking Devices. Retrieved 12 05, 2023, from DHF TS 621:2018: https://www.dhfonline.org.uk/media/documents/documents35a.pdf.
Egli P., & Netmodule A.G. (2006). Susceptibility of wireless devices to denial of service attacks. Technical white paper, Netmodule AG. Retrieved 12 05, 2023, from https://www.researchgate.net/profile/Peter-Egli/publication/266878242_Susceptibility_of_wireless_devices_to_denial_of_service_attacks/links/59d53583a6fdcc87469561ee/Susceptibility-of-wireless-devices-to-denial-of-service-attacks.pdf.
Eldes Security. (2023). EN 50131: grades in intruder alarm systems. Retrieved 10 09, 2023, from https://eldesalarms.com/articles/en-50131-grades-in-intruder-alarm-systems/.
Ferro, E., Potorti, F., 2005. Bluetooth and Wi-Fi wireless protocols: a survey and a comparison. IEEE Wirel. Commun. 12 (1), 12–26. https://doi.org/10.1109/MWC.2005.1404569.
FIRST. (2023). CVSS v4.0 calculator - PUBLIC PREVIEW. Retrieved 06 19, 2023, from https://www.first.org/cvss/calculator/4.0#.
Gao, C., Luo, L., Zhang, Y., Pearson, B., Fu, X., 2019. Microcontroller based IoT system firmware security: case studies. In: Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), pp. 200–209. https://doi.org/10.1109/ICII.2019.00045.
Garbelini, M.E., Wang, C., Chattopadhyay, S., Sumei, S., Kurniawan, E., 2020. {SweynTooth}: unleashing mayhem over Bluetooth low energy. In: Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC 20), pp. 911–925. Retrieved 12 05, 2023, from. https://www.usenix.org/conference/atc20/presentation/garbelini.
Garcia, F.D., Oswald, D.F., Kasper, T., Pavlidès, P., 2016. Lock it and still lose it-on the (In) security of automotive remote keyless entry systems. In: Proceedings of the USENIX Security Symposium, 53. Austin: Usenix. Retrieved 12 05, 2023, from. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia.
Grover, A., Berghel, H., 2011. A survey of RFID deployment and security issues. J. Inf. Process. Syst. 7 (4), 561–580. https://doi.org/10.3745/JIPS.2011.7.4.561.
Gullberg, P., 2016. Denial of service attack on bluetooth low energy. Denial Serv. Attack Bluetooth Low Energy. https://doi.org/10.13140/RG.2.2.12059.26407. September.
Gupta, A., 2019. The IoT Hacker's Handbook [electronic resource]: A practical Guide to Hacking the Internet of Things. Apress, Walnut, CA.
Harding C. (2022, August 14th). rfcat-rolljam. Retrieved 12 05, 2023, from itHub: https://github.com/exploitagency/rfcat-rolljam.
Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., Wagner, D., 2016. Smart locks: lessons for securing commodity internet of things devices. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. Xi'an. ACM, pp. 461–472. https://doi.org/10.1145/2897845.2897886.
Hodges, D., 2021. Cyber-enabled burglary of smart homes. Comput. Secur. 110, 102418 https://doi.org/10.1016/j.cose.2021.102418.
Hoppe. (2023). BS EN 1303:2015 – cylinders for locks. Retrieved 12 04, 2023, from https://www.hoppe.com/gb-en/products/standards-and-solutions/bs-en-1303/.
Hung, P.D., Vinh, B.T., 2019. Vulnerabilities in IoT devices with software-defined radio. In: Proceedings of the 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS). Singapore. IEEE, pp. 664–668. https://doi.org/10.1109/CCOMS.2019.8821711.
Indesteege, S., Keller, N., Dunkelman, O., Biham, E., Preneel, B., 2008. A practical attack on KeeLoq. Advances in Cryptology–EUROCRYPT 2008: 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings 27. Springer, pp. 1–18. https://doi.org/10.1007/978-3-540-78967-3_1.
Jasek S. (2016). Gattacking Bluetooth smart devices. Black hat USA conference. Las Vegas: Black Hat. Retrieved 12 05, 2023, from https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf.
Jasek S. (2017). Blue picking: hacking Bluetooth smart locks. HITBSecConf. Amsterdam: HITBSecConf. Retrieved 12 05, 2023, from https://archive.conference.hitb.org/hitbsecconf2017ams/sessions/hitb-lab-blue-picking-hacking-bluetooth-smart-locks/.
Jones, K.R., Yen, T.F., Sundaramurthy, S.C., Bardas, A.G., 2020. Deploying android security updates: an extensive study involving manufacturers, carriers, and end users. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA. Association for Computing Machinery, pp. 551–567. https://doi.org/10.1145/3372297.3423346.
Khan, M.A., Kabir, M.A., 2016. Comparison among short range wireless networks: bluetooth, Zig Bee & Wi-Fi. Indones. J. Electr. Eng. Comput. Sci. 30 (1), 276–288. 10.11591/ijeecs.v30.i1.pp276-288.
Kim, J., Kim, H., 2006. Security vulnerability and considerations in mobile RFID environment. In: Proceedings of the 2006 8th International Conference Advanced Communication Technology. 1. Phoenix Park. IEEE, pp. 801–804. https://doi.org/10.1109/ICACT.2006.206085.
Kim, K., Cho, K., Lim, J., Jung, Y.H., Sung, M.S., Kim, S.B., Kim, H.K., 2020. What's your protocol: vulnerabilities and security threats related to Z-Wave protocol. Pervasive Mob. Comput. 66, 101211 https://doi.org/10.1016/j.pmcj.2020.101211.
Kumar, S., Banka, H., Kaushik, B., Sharma, S., 2021. A review and analysis of secure and lightweight ECC-based RFID authentication protocol for internet of vehicles. Trans. Emerg. Telecommun. Technol. 32, e4354. https://doi.org/10.1002/ett.4354.
Kurylowicz P. (2022, August 14th). gattacker. Retrieved 12 05, 2023, from GitHub: https://github.com/securing/gattacker.
Kwon, G., Kim, J., Noh, J., Cho, S., 2016. Bluetooth low energy security vulnerability and improvement method. In: Proceedings of the 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), pp. 1–4. https://doi.org/10.1109/ICCE-Asia.2016.7804832.
Lackner, G., 2013. A comparison of security in wireless network standards with a focus on Bluetooth, WiFi and WiMAX. Int. J. Netw. Secur. 15, 420–436. Retrieved 12 05, 2023, from. http://ijns.jalaxy.com.tw/contents/ijns-v15-n6/ijns-2013-v15-n6-p420-436.pdf.
Li, H., Chen, Y., He, Z., 2012. The survey of RFID attacks and defenses. In: Proceedings of the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4. https://doi.org/10.1109/WiCOM.2012.6478720.
Liu, K., Yang, M., Ling, Z., Yan, H., Zhang, Y., Fu, X., Zhao, W., 2021. On manually reverse engineering communication protocols of linux-based IoT systems. IEEE Internet Things J. 8, 6815–6827. https://doi.org/10.1109/JIOT.2020.3036232.
Lonzetta, A.M., Cope, P., Campbell, J., Mohd, B.J., Hayajneh, T., 2018. Security vulnerabilities in Bluetooth technology as used in IoT. J. Sens. Actuator Netw. 7, 28. https://doi.org/10.3390/jsan7030028.
Lounis, K., Zulkernine, M., 2019. Bluetooth low energy makes "just works" not work. In: Proceedings of the 2019 3rd Cyber Security in Networking Conference (CSNet). Quito. IEEE, pp. 99–106. https://doi.org/10.1109/CSNet47905.2019.9108931.
Malhotra, P., Singh, Y., Anand, P., Bangotra, D.K., Singh, P.K., Hong, W.C., 2021. Internet of things: evolution, concerns and security challenges. Sensors 21, 1809. https://doi.org/10.3390/s21051809.
Microchip.com. (2023). SweynTooth Bluetooth® low energy (BLE) vulnerability. Retrieved 04 07, 2023, from https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/sweyntooth-ble-vulnerability.
Mitrokotsa, A., Rieback, M.R., Tanenbaum, A.S., 2010. Classification of RFID attacks. Inf. Syst. Front. 15693, 14. https://doi.org/10.1007/s10796-009-9210-z.
Montoya, M., Bacles-Min, S., Molnos, A., Fournier, J.J., 2018. SWARD: a secure WAke-up RaDio against denial-of-service on IoT devices. In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks. New York, NY, USA. Association for Computing Machinery, pp. 190–195. https://doi.org/10.1145/3212480.3212488.
Mordor Intelligence. (2022, August 14th). Smart lock market - growth, trends, covid-19 impact, and forecasts (2022 - 2027). Retrieved 12 05, 2023, from https://www.mordorintelligence.com/industry-reports/smart-lock-market.
Mould S. (2022, August 14th). Steve mould hacks into his car with a Hackrf. Retrieved 12 05, 2023, from rtl-sdr.com: https://www.rtl-sdr.com/steve-mould-hacks-into-his-car-with-a-hackrf/.
NBS. (2023). BS EN 1670:2007 building hardware - corrosion resistance - requirements and test methods (Incorporating corrigendum March 2008). Retrieved 12 04, 2023, from https://www.thenbs.com/PublicationIndex/documents/details?Pub=BSI&DocID=285460.

NVD. (2023). Vulnerability metrics. Retrieved 08 05, 2023, from https://nvd.nist.gov/vuln-metrics/cvss.
PS GmbH. (2023). About PS GmbH. Retrieved 12 04, 2023, from https://pslocks.com/en/about-us-ps-locks-with-iso-9001-certification-from-tuev-austria/.
Qu, Y., Chan, P., 2016. Assessing vulnerabilities in bluetooth low energy (BLE) wireless network based IoT systems. In: Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), pp. 42–48. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.63.
Razouk, W., Crosby, G.V., Sekkaki, A., 2014. New security approach for ZigBee weaknesses. Procedia Comput. Sci. 37, 376–381. https://doi.org/10.1016/j.procs.2014.08.056.
Rotter, P., 2008. A framework for assessing RFID system security and privacy risks. IEEE Pervasive Comput. 7 (2), 70–77. https://doi.org/10.1109/MPRV.2008.22.
rtl-sdr.com. (2022, August 14th). Bypassing chamberlain myq garage doors with a jamming sdr attack. Retrieved 12 05, 2023, from https://www.rtl-sdr.com/bypassing-chamberlain-myq-garage-doors-with-a-jamming-sdr-attack/.
Rysc Corp. (2023). ProxmarkPro Kit. Retrieved 06 19, 2023, from https://www.crowdsupply.com/rysc-corp/proxmarkpro#products.
Sadeghian, A., 2013. Analysis of WPS security in wireless access points. In: Proceedings of the 6th International Conference on Security for Information Technology and Communications (SECITC 2013). Bucharest. SECITC. https://doi.org/10.13140/2.1.1869.2164.
Salto. (2020). We just got ISO certified! Retrieved 12 04, 2023, from https://saltosystems.com/en/blog/we-just-got-iso-certified/.
Sarma S., & Engels D.W. (2003). On the future of RFID tags and protocols. Auto ID Center White Paper. Retrieved 12 05, 2023, from https://www.researchgate.net/publication/244437152_On_the_future_of_RFID_tags_and_protocols.
Schlage. (2023). Security Grades. Retrieved 12 04, 2023, from https://www.schlage.com/en/home/support/understand-product-options/functions-grades.html.
Sevier, S., Tekeoglu, A., 2019. Analyzing the security of bluetooth low energy. In: Proceedings of the 2019 International Conference on Electronics, Information, and Communication (ICEIC), pp. 1–5. https://doi.org/10.23919/ELINFOCOM.2019.8706457.
Shariq, M., Singh, K., Bajuri, M.Y., Pantelous, A.A., Ahmadian, A., Salimi, M., 2021. A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario. Sustain. Cities Soc. 75, 103354 https://doi.org/10.1016/j.scs.2021.103354.
Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N., Karliychuk, T., 2018. Smart IoT devices in the home: security and privacy implications. IEEE Technol. Soc. Mag. 37 (2), 71–79. https://doi.org/10.1109/MTS.2018.2826079.
Spring T. (2019). Smart lock turns out to be not so smart, or secure. Retrieved 11 19, 2022, from https://threatpost.com/smart-lock-turns-out-to-be-not-so-smart-or-secure/146091/.
Telefonica. (2022). HomePwn. Retrieved 12 05, 2022, from https://github.com/Telefonica/HomePWN.
Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., Bilal, M., 2021. Smart home security: challenges, issues and solutions at different IoT layers. J. Supercomput. 77, 14053–14089. https://doi.org/10.1007/s11227-021-03825-1.
Urquhart, C., Bellekens, X., Tachtatzis, C., Atkinson, R., Hindy, H., Seeam, A., 2019. Cyber-security internals of a skoda octavia vRS: a hands on approach. IEEE Access 7, 146057–146069. https://doi.org/10.1109/ACCESS.2019.2943837.
Vaccari, I., Cambiaso, E., Aiello, M., 2017. Remotely exploiting at command attacks on zigbee networks. Secur. Commun. Netw 1–9. https://doi.org/10.1155/2017/1723658, 2017.
Valle, J.G., 2021. Practical Hardware Pentesting: A guide to Attacking Embedded Systems and Protecting Them Against the Most Common Hardware Attacks. Packt Publishing, Birmingham.
Vasile, S., Oswald, D., Chothia, T., 2018. Breaking all the things—a systematic survey of firmware extraction techniques for IoT devices. In: Proceedings of the International Conference on Smart Card Research and Advanced Applications, pp. 171–185. https://doi.org/10.1007/978-3-030-15462-2_12.
Vidgren, N., Haataja, K., Patino-Andres, J.L., Ramirez-Sanchis, J.J., Toivanen, P., 2013. Security threats in ZigBee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned. In: Proceedings of the 2013 46th Hawaii International Conference on System Sciences. Wailea. IEEE, pp. 5132–5138. https://doi.org/10.1109/HICSS.2013.475.
Viehböck S. (2011). Brute forcing wi-fi protected setup. Retrieved 12 05, 2023, from https://www.cs.cmu.edu/~rdriley/330/papers/viehboeck_wps.pdf.
Vishwakarma, G., Lee, W., 2018. Exploiting JTAG and its mitigation in IOT: a survey. Future Internet 10. https://doi.org/10.3390/fi10120121.
Wang, J., Hu, F., Zhou, Y., Liu, Y., Zhang, H., Liu, Z., 2020. BlueDoor: breaking the secure information flow via BLE vulnerability. In: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services. Toronto. ACM, pp. 286–298. https://doi.org/10.1145/3386901.3389025.
Williamson Sr, A., Tsay, L.S., Kateeb, I.A., Burton, L., 2013. Solutions for RFID smart tagged card security vulnerabilities. AASRI Procedia 4, 282–287. https://doi.org/10.1016/j.aasri.2013.10.042.
Xiao Q., Gibbons T., Lebrun H., & others. (2009). RFID technology, security vulnerabilities, and countermeasures. Supply Chain the Way to Flat Organization, 357–382. 10.5772/6668.
Yassein, M.B., Mardini, W., Almasri, T., 2018. Evaluation of security regarding Z-Wave wireless protocol. In: Proceedings of the Fourth International Conference on Engineering & MIS 2018. Istanbul. ACM, pp. 1–8. https://doi.org/10.1145/3234698.3234730.
Ye, M., Jiang, N., Yang, H., Yan, Q., 2017. Security analysis of Internet-of-Things: a case study of august smart lock. In: Proceedings of the 2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS). Atlanta. IEEE, pp. 499–504. https://doi.org/10.1109/INFCOMW.2017.8116427.

Mr Ashley Allen is a PhD student in Computer Science at the University of Hertfordshire and a member of the Cybersecurity and Computing Systems research group. He holds an MSc in Computer Science (Cybersecurity) from Staffordshire University, UK. He has more than 20 years' experience working in security roles in both the public and private sector. He is currently an Application Security Engineer for Posit, PBC, a Boston, MA, based data science company. His-research interests include IoT security and federated learning.

Dr Alexios Mylonas is with University of Hertfordshire, where he leads the Cybersecurity and Computing Systems research group. He holds a PhD in Information and Communication Security and a BSc (Hons) in Computer Science from the Athens University of Economics and Business, as well as an MSc in Information Security from Royal Holloway, University of London. His-research interests focus on IoT security, incident response and web security and fraud detection. He has published more than 40 papers in esteemed scientific venues.

Dr Stilianos Vidalis is the Deputy Head of the Dept. of Computer Science at the University of Hertfordshire and a member of the Cybersecurity and Computing Systems research group. He leads the development of an innovative technology that automates threat assessments. He acted as an instructor for the British Armed Forces Intelligence Personnel on penetration testing and digital forensics and as a cyber-expert for the Welsh Government and for the Wales University Officers' Training Corps (WUOTC). His-research interests are in digital forensics and intrusion detection.

Dr Dimitris Gritzalis is a Professor of cybersecurity with the Dept. of Informatics, Athens University of Economics & Business, where he serves as Director for the M.*Sc*. Programme in Information Systems Security. He holds a B.*Sc*. (Mathematics, Univ. of Patras), a M.*Sc*. (Computer Science, City University of New York), and a Ph.D. (Information Systems Security, Univ. of the Aegean). He served as Associate Rector for Research, President for the Greek Computer Society and Associate Data Protection Commissioner of Greece. His-research interests include risk assessment, critical infrastructure protection, and malware. He is the Academic Editor of Computers & Security and the Scientific Editor of the International Journal of Critical Infrastructure Protection