A taxonomy of cyber-physical threats and impact in the smart home

A taxonomy of cyber-physical threats and impact in the smart home

Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R. J. Fontaine, Avgoustinos Filippoupolitis, Etienne Roesch

Computing and Information Systems
University of Greenwich, UK
E: r.j.heartfield@gre.ac.uk

Abstract

In the past, home automation was a small market for technology enthusiasts. Interconnectivity between devices was down to the owner's technical skills and creativity, while security was non-existent or primitive, because cyber threats were also largely non-existent or primitive. This is not the case any more. The adoption of Internet of Things technologies, cloud computing, artificial intelligence and an increasingly wide range of sensing and actuation capabilities has led to smart homes that are more practical, but also genuinely attractive targets for cyber attacks. Here, we classify applicable cyber threats according to a novel taxonomy, focusing not only on the attack vectors that can be used, but also the potential impact on the systems and ultimately on the occupants and their domestic life. Utilising the taxonomy, we classify twenty five different smart home attacks, providing further examples of legitimate, yet vulnerable smart home configurations which can lead to second-order attack vectors. We then review existing smart home defence mechanisms and discuss open research problems.

1. Introduction

As homes adopt Internet of Things (IoT) technologies and become increasingly smart by utilising networked sensing and actuation, cloud computing and artificial intelligence, they naturally become more vulnerable to threats in cyber space. Some of these threats are entirely new. The majority are not, but applying them in a domestic context generates second-order threats to the physical and emotional safety of the occupants to an extent not previously experienced. Here, we present a taxonomy of cyber threats to smart homes already observed in the wild or in controlled experiments, as well as potential future vulnerabilities exposed by specific smart home configurations and technology adoption.

Smart home cyber security is usually addressed as an extension of the smart grid, looking almost exclusively at energy-related attacks [1]. This has begun to change. Indicatively, Lin and Bergmann [2] have taken a holistic perspective on smart home privacy and security, identifying the combination and convergence of heterogeneous technologies, with lack of specialised security knowledge, as two key challenges exacerbating the cyber threat to smart home environments. Here, we look more deeply at the technical building blocks of cyber threats to smart homes, identifying key classification criteria that help to shape the attack landscape. We do not claim that this taxonomy can be exhaustive. However, in identifying and characterising existing and potential future cyber threats to the smart home, we are able to highlight motivations, resources, vulnerabilities and crucially their impact, so as to help establish the problem space for defence measures that would address them.

2. Related Work

The smart home is not a fundamentally new technological paradigm. So, although there has not been a taxonomy of cyber threats for smart homes before, it is meaningful to contrast against related work that is more general for IoT or previously established areas, such as wireless sensor networks and networked embedded systems. In 2010, Babar et al. [3] were the first to propose a taxonomy of IoT cyber threats, but only provided a high-level overview of security requirements and types of threats in terms of communication, identity management, storage management, embedded security, physical threats and dynamic binding. More recent work by Jing et al. [4] has looked at IoT security from the perspective of security needs at the application layer, the transportation layer and what they refer to as the perception layer, which is where the data collection occurs. The resulting architecture is effectively a taxonomy of the types of threats at each layer, which, interestingly, includes smart home security as one of the requirements at the application layer, but does not elaborate further. Another area of interest is privacy in IoT, where Ziegeldorf et al. [5] have classified the impact of an IoT privacy breach as relating to identification, tracking, profiling, privacy-violating interaction, lifecycle transitions, inventory attacks and linkage. This is a well thought-out taxonomy, but is naturally limited to privacy and does

not consider the technical properties of a smart home or the second-order impact on its occupants. In Nawir et al. [6], the authors have presented a taxonomy of IoT security attacks, classified according to device property, location, access level and protocol type. Their analysis includes security issues related to the healthcare, transportation and smart home domains, but this classification is not present in their taxonomy. Finally, a taxonomy of IoT based smart environments is presented in the work of Ahmed et al. [7], which classifies the IoT environment based on communication enablers, network types, technologies, local area wireless standards, objectives, and characteristics. The security aspects are only briefly touched upon as part of the technologies category.

In Table 1, we summarise existing taxonomies to highlight the current perceived extensions of the security problem space in the smart home domain. We emphasise in particular on the key security properties, the vulnerabilities and particular factors making smart home IoT security challenging, as well as any recommendations for security and novel challenges for research as identified by each existing taxonomy.

Here, we consider the large variety of technical configurations of current smart homes, provide a detailed description of the attack surface and take into account each attack's impact on domestic life, as supported and shaped by a smart home, extending to the potential impact on the occupants' physical and emotional wellbeing too.

3. A taxonomy of cyber threats to smart home

A primary motivation for developing this taxonomy is to establish a systematic means for classifying attack vectors and the their impact as a holistic view of cyber threats within the context of the smart home. Hence, we are not only concerned with identifying extant or emerging attack vectors (e.g., as a result of technology convergence in the household), but also establishing the physical, domestic and emotional impact for human occupants. With these objectives in mind, to direct the construction of taxonomy criteria we start with the following questions:

- By what means can an attacker target the smart home?
  This involves identifying the different ways and conditions by which an attack might be distributed and automated in the smart home, which are vital to distinguish between explicit vulnerabilities in systems and second-order threats which are manifested by a household's specific configuration.

- How is the cyber security of a smart home compromised by an attack?
  A consequence of technology convergence in the smart home is the cascading effect of compromise of one system to others. For example, a breach of confidentiality, integrity and availability resulting from a vulnerability in a single device may result in shared exploitation across interdependent systems. A secure system may be rendered vulnerable by the insecurities of a lesser protected platform on which it relies. Stealing the WiFi keys from the firmware of a smart light-bulb inadvertently affects the confidentiality of other devices connected to the same WiFi access point.

- In what ways will cyber-physical systems in the smart home respond to attacks?
  Establishing the different ways in which physical systems respond to cyber threats is important in understanding the risks to occupants and even for detecting threats by monitoring both cyber and physical system behaviour.

- What are the direct consequences of an attack for smart home occupants?
  Conventional security breaches in cyberspace typically result in financial loss, breaches of data privacy or loss of control of computer devices. In the smart home, by compromising or disrupting household appliances and systems, the consequences can extend not only to cyberspace but also to physical space, whereby the physical privacy, safety and well-being of occupants are threatened.

- How do occupants experience the impact of different attacks against the smart home?
  Smart homes are typically set up for convenience, security and energy efficiency, but these can all be severely disrupted by a cyber security breach, leading to adverse experience on the affected users' daily lives, ranging from mild inconvenience to loss of time and intense frustration due to goal blockage.

- How will occupants respond emotionally as a result of an attack against the smart home?
  While different people respond differently, stress, anxiety and privacy-seeking behaviour [8] are some of the expected short-term and long-term effects that need to be taken into account.

We use this set of questions as the basis for our root taxonomy criteria: *Attack Vector*, *Impact on Systems* and *Impact on Domestic Life*. In the following sections, each set of answers is translated into specific categories with relevant examples observed in the wild or carried out as research experiments.

In Figure 1, each of the root classification criteria is shown with basic high-level interactions. These interactions represent causal relationships which can be used to generate a classification of a smart home cyber threat. In section 7, we practically demonstrate how these interactions are represented as linearly separable steps, irrespective of the number of attack vectors and variable impact they may have. Moreover, we highlight how this approach

Table 1: Summary of existing taxonomies with applicability in smart home cyber security

Reference	Key security properties	Vulnerabilities/challenges	Security recommended	Open problems identified
Komninos et al. [1]	Confidentiality Resilience Reliability, availability	Connected to Internet Physical tampering		Auto-immunity to threats
Lin et al. [2]	Confidentiality Authentication Access control	Phys./netw. accessibility Constrained resources Heterogeneity	Gateway architecture	Auto-configuration Updates
Nawir et al. [6]	Smart meter integrity Privacy Non-repudiation Authorisation	Remote connectivity Physical tampering Malicious actuation	Techn. countermeasures Regulatory initiatives	Standardisation Impact evaluation, metrics Intrusion detection Logging for audit/forensics
Ziegeldorf et al.[5]	Privacy	Identification Tracking Profiling Linkage		Detection of sensitive content

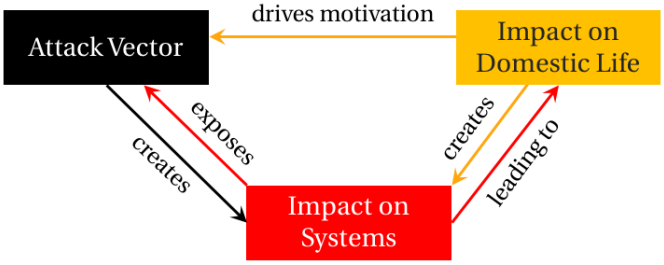

Figure 1: Causal relationship between root criteria in smart home cyber-threat taxonomy

can be used to benefit different types of research related to the cyber security of smart homes.

4. Attack vector

IoT proliferation, integration of sensors, actuators and low-powered wireless communications in domestic households, alongside traditional home-broadband WiFi and Internet services, have positioned the smart home as a nexus of information technology connectivity. In the past, these technologies were typically designed and reserved for specialist environments, such as industrial control, embedded sensing or medical data collection. In the smart home, they have now converged within a general consumer landscape. In a positive sense, the smart home becomes a catalyst for the transformation of domestic life through ubiquitous access to rich and interactive technology. However, almost paradoxically, it also inherits the emerging risks and vulnerabilities that come with the dependency on these technologies.

Within the context of the smart home, it is the occupants who make the ultimate decision to install a new wireless security lock, presence sensor or voice-controlled assistant, as privacy and security concerns are carried out according to occupants' risk attitude [9], personal and social circumstances. By comparison, for smart offices and smart cities, introducing IoT systems requires rigorous ethical, policy and even legislative evaluation before deployment. This positions the smart home in many ways as a pilot environment for future deployment of emerging IoT technologies to wider public contexts ([10, 11]).

For the immediate future, the smart home technology landscape is likely to be volatile, consisting of both legacy and emerging IoT platforms, each with their own security risks. The threat landscape relates to the communication medium and control software used, as well as threats in the supply chain, side channel attacks and the sensory channel. Below, we detail each of these categories with examples.

4.1. CM (Communication medium)

This is the means by which sensors, actuators, devices and applications communicate in a smart home. It is symptomatic of rapid innovation within the field of IoT that several communication protocols deployed within the smart home will become obsolete over time. Consequently, the technologies evaluated in this taxonomy constitute by no means an exhaustive list, but at the time of writing, all are implemented within a range of smart home technologies and platforms and have been shown to contain technical vulnerabilities that have been exploited.

4.1.1. CM-HI: Home Internet

Internet-connected households are by no means a new phenomenon. However, the advent of the smart home has positioned home internet connectivity as one of the primary gateways for attackers to gain access to devices, sensors and actuators in the household traditionally isolated from the outside world.

Although home Internet is served externally to the household via physical (e.g., copper or fibre broadband cabling) or wireless means (e.g., cellular), as a communication medium, it can be targeted both directly or indirectly. For example, direct targeting attempts to identify the public IP address assigned to the home internet gateway in order to fingerprint services exposed to the Internet. Indirect targeting relates to solicited connectivity via the home Internet connection originating from internal smart home devices or occupants toward Internet resources, which are under the control of an attacker (e.g., a compromised cloud service or a household occupant opening a phishing email).

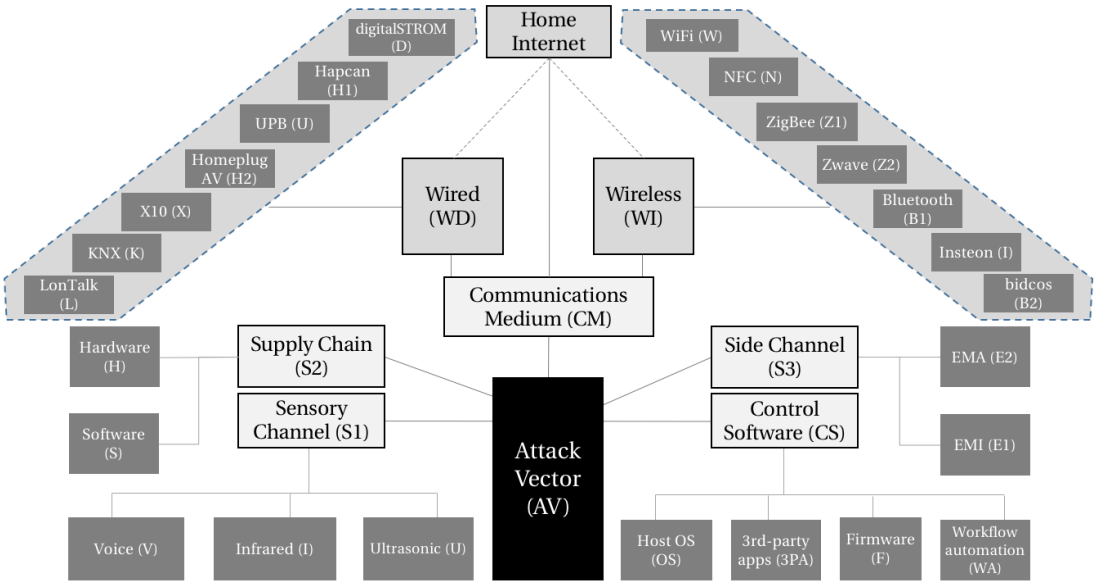

Figure 2: Smart home attack Vector classification criteria

As the vast majority of smart home platforms rely on the home Internet gateway to reach respective cloud services in order to function, if an attacker can compromise a smart home Internet gateway they may be able to disrupt or gain control of almost every Internet-connected device in the household. Stamm et al. [12] have illustrated that by simply accessing a malicious web page an attacker can execute a Java applet with code on the client device that fingerprints home Internet routers' internal IP addressing. On accessing the attacker web page, a basic script is executed that establishes a reverse socket connection back from the household client to the attack web server, where the returned client IP address provides an indication of the internal addressing schema. This is subsequently used to enumerate whether web services (i.e., router administration websites) are hosted on any internal addresses, followed by identification of different router models by querying web page content found (e.g., logos, text). Once a router model is recognised, an attacker then issues a login query with the model's default vendor credentials (which are often not changed by household users) in order to access the home Internet gateway and change key configuration settings. With this type of threat, no specific vulnerability of the home Internet medium is exploited. The authors have argued that reliance on the default control of blocking all unsolicited inbound connectivity creates a false sense of security, as this type of access can be achieved by home users mistakenly running malicious code on internal devices which subsequently provide access to the internal network, where all outbound connectivity and home internet router administration is enabled by default.

As of May 2018, an initial report by *Cisco Talos* dramatically reinforced the growing vulnerability of home internet gateways by identifying a large scale advanced persistent threat against SOHO routers titled *VPNFilter*. Analysis of *VPNFilter* revealed a modular, multi-stage malware capable of conducting intelligence gathering activities, as well as possessing "kill switch" denial of service capabilities against LinkSys, MikroTik, Netgear, Qnap and TP-Link SOHO router platforms typically deployed as home network internet gateways. Consisting of a three stage infection and command and control process, stage one installs a persistent boot loader into BusyBox or Linux based firmware, attempting to create an initial connection to an attacker server by downloading from seed URLs originating from *Photobucket.com* which then extract server IP addresses hidden in image EXIF meta-data; in the event of failure, a backup domain *toknownall.com* is used with the same process. Stage two proceeds to download a non-persistent module from the attacker server, running in a local working directory which contacts a C2 server to execute commands. Stage three expands the malware functionality by installing a non-persistent packet sniffing module which intercepts traffic and attempts to extract HTTP authentication strings, as well as a communication plugin for remote communication over Tor.

The researchers claimed that since 2016 *VPNFilter* may have compromised over 500,000 SOHO routers in over 54 countries (many of which were common household internet router devices). They also noted that whilst no known exploits were uncovered regarding the initial infection vector, many of the infected home routers discovered were old or unpatched with widely known vulnerabilities, open source exploits and typically shipped with default login credentials.

4.1.2. CM-WD: Wired

Wired communication is increasingly rare in smart home environments, although still practical for applications that

require very high throughput rates, such as video streaming from multiple security cameras, or would benefit from the natural physical protection to sniffing and interference that wires can offer over wireless. Of course, this does not protect against attacks that have penetrated the network and may originate from the Internet or from inside the network, such as malware infections and social engineering.

Generally, within the home environment fully-fledged structured cabling is undesirable and impractical due to installation requirements. However, where a building's construction may introduce undue attenuation to wireless transmission signals (e.g., through steelworks or thick brick walls), often this has led to utilisation of existing power-line wiring for transmitting data between devices.

4.1.3. CM-WD-X: X10

One of the oldest home automation protocols, X10 was designed for power line communications. Improvements on the X10 protocol resulted in the A10 protocol, but without any added security. In 2011, researchers demonstrated a device that can be plugged into a power outlet outside a building to jam the X10 signals that control lights, doors, air conditioning and physical security systems [13].

4.1.4. CM-WD-K: KNX

Like X10, KNX is a relatively old home and building automation system that was designed to provide connectivity between heating, ventilation, air and cooling systems which in the past had no means of communicating to report their status or to provide remote configuration. Over time, IP extensions have been built into KNX gateways to facilitate greater functionality and integration between system components in home and building automation deployments. However, by leveraging IP-to-KNX connectivity [14], Antonini et al. have demonstrated a practical attack against a real-world KNX home automation platform, by successfully sending arbitrary commands to actuators. The attack is achieved by distributing a malware from a compromised IP host to KNX enabled actuators over the IP-to-KNX network gateway, no-password protected actuators execute arbitrary commands within the malware command-set causing an operating system reset which amounts to a DoS impact. In the case of password protection, the malware simulates a device malfunction over the KNX network (as device actions are not authenticated or verified), which results in controller reprogramming of the actuator with its password; as KNX does not use packet encryption, the resultant plaintext passphrase sent over the network is then sniffed over the network by the malware and used to reprogram KNX actuators.

4.1.5. CM-WD-H: HAPCAN

The Home Automation Project based on Controller Area Network (HAPCAN) is an open source hardware framework which has been developed using the CAN 2.0B standard [15]. Analysis of the HAPCAN specification show a potential design flaw in the communication protocol which may allow an attacker to exploit the arbitration mechanism within the CAN bus. A rogue node can exploit the arbitration mechanism within CAN by constantly transmitting message IDs with a dominant bit set on the bus. The arbitration mechanism processes message IDs with the dominant bit (0) with a higher priority over the recessive bit (1), i.e. a packet with message ID of 0000 will have higher priority over a packet with message ID 1111, thus by constantly submitting a message ID of 0 to the bus an attacker will take over the control of the arbitration. This attack leads other modules on the bus being starved of communication between each other, which effectively makes them unavailable.

In HAPCAN, denial of service can also be achieved by exploiting the fact that all nodes are interconnected in series, and therefore a failure of one module affects overall availability. Furthermore, as HAPCAN utilises the CAN protocol, the protocol itself is at risk to several additional CAN vulnerabilities, such as request overload and false request to send [16], or rogue node packet amplification exhausting [17]. Here, it is important to note that an attacker requires physical access to the communication bus, e.g., by implanting a rogue node through the supply chain.

4.1.6. CM-WD-U: Universal Power Bus

Universal Powerline Bus (UPB) is intended to be an X10 replacement with superior reliability (lower susceptibility to powerline noise and increased range). However, UPB has no encryption and therefore any attack that is able to sniff data from the powerline (such as using a rogue UPB node) is able to read and inject data in the network.

4.1.7. CM-WD-H: HomePlug AV

In 2010, Puppe and Vanderauwera conducted a research project into the security of the HomePlug AV protocol [18]. They were able to execute dictionary attacks against the Devolo dLAN HomePlug's use of 56-bit DES network encryption within 20 minutes. Furthermore, it was shown that a simple DoS attack could be executed by doctoring the rate at which an attacker HomePlug device sends management packets (which are broadcast to all HomePlugs' in the network), whereby packet loss on a member HomePlug was shown to be as high as 30% on receiving a high rate of management packets sent with the wrong network encryption key.

In 2014, Tasker [19] demonstrated how to infiltrate a HomePlugAV network, using the ON Network's PL500 HomePlugAV device . Tasker identified that the MAC address of a HomePlug powerline station (STA) is used to derive a Device Access Key (DAK), which in turn can be used to tell target STAs to join a rogue HomePlugAV network. HomePlugAV traffic can be passively sniffed to identify MAC addresses to calculate the DAKs of available STAs and enrol them on the attacker network. Whilst this causes a temporary outage of the STAs if connected to an existing network, it is momentary and if the attacker

leaves the network, normal communication with the legitimate HomePlug network will resume (thus the intrusion can go unnoticed by a occupant). Here, a successful attack allows for complete access to target data and it was identified that at that time at least eleven brands of HomePlug AV device were vulnerable to the attack due to the DAK derivation method used to join the network - which if left unchanged makes the attack practically indefensible. A similar, but more complicated attack against DAKs was undertaken in [20], whereby a DAK passphrase generation technique was implemented to gain access to a neighboring HomePlug AV network.

For attacks against HomePlug devices to be practical, access to the same power line is required, for example within an apartment complex with a shared power feed, as practically demonstrated by Dudek [20] between two apartments in the same tower block in France.

4.1.8. CM-WD-L: LonTalk

LonTalk is a building and home automation protocol optimised to control actuation and sensing devices as part of a LonWorks platform, originally developed in proprietary format by Echelon Corporation, but now adopted as a ISO/IEC standard. Like other wired powerline building automation protocols ported to the smart home environment (e.g., X10, UPB, KNX). Despite recent resurgence of LonTalk as a viable means of smart home automation, the protocol has been assessed to be insecure by default by a cryptanalysis report in 2015 [21]. Specifically, the EN 14908 algorithm used by LonTalk as part of its the Open Smart Grid protocol implementation uses a 48-bit key encryption key which can be trivially bruteforced [22]. An online article by BusinessWire reported that LonTalk was estimated to be implemented in over 90 million devices world-wide as of 2010.

4.1.9. CM-WD-DS: digitalSTROM

Recently, Brauchli and Li [23] identified viable attacks on digitalSTROM (DS), a smart home system with growing popularity throughout Europe based on home powerline networking. DS uses a proprietary unencrypted protocol (DS485) [24], typically consisting of an optional DS server and at least one DS meter and filter per circuit, with a number of terminal blocks connected to a DS chip for each device (e.g., fridge, fire alarm, heater, coffee maker etc.). Brauchli and Li have discussed theoretical attacks, such as uploading power readings to a remote server for occupancy detection to manipulating lights and household appliances, by exploiting the DS Android app's public interface through an Android intent cross-app message on a compromised smart phone. Whilst a compromised smartphone is required as an entry vector into the powerline, once this is established, the DS protocol provides unrestricted access to launch arbitrary commands against any connected appliances.

4.1.10. CM-Wireless

The majority of modern smart homes utilise wireless communications and as a result are vulnerable to the security threats that are inherent in a wireless medium. For example, the signals containing sensor data or actuation commands can be captured by an adversary in the vicinity, which makes strong encryption and countermeasures against replay attacks particularly important. At the same time, wireless control can be rather trivially disrupted via communication jamming.

4.1.11. CM-WI-W: WiFi

As most homes already have a Wi-Fi router, Wi-Fi is a common technology for connecting to smart home devices, such as a smart lights and smart plugs. However, security wise this also makes the Wi-Fi router the central point of failure of the smart home setup. This is significant because there are multiple free applications available on the Internet for acquiring the password for Wi-Fi connections. Interestingly, by having access to the home Wi-Fi password, it may also be a smart home device that exposes it. This is the case where devices, such as smart light bulbs, need to communicate network configuration data between them. Masquerading as a new light bulb joining the network, researchers have demonstrated how to access security credentials, such as the home Wi-Fi password if no security measures are taken specifically for the light bulb to light bulb communication [25]. A practical example of such an attack was demonstrated by Chapman in 2014 against the LIFX lightbulbs [26], where in the presence of more than one bulb, a master is elected and network configuration and information is passed between master and slave bulbs using an insecure IPv6 over low-power wireless personal area networks implementation.

WiFi de-authentication attacks present a well-known vulnerability in the 802.11 protocol and can be utilised to lead to denial of service with de-authentication packets, or as a mechanism to perform Wi-Fi Protected Access (WPA) password cracking via sniffing a household WiFi-enabled device's WPA 4-way handshake after they have been de-authenticated from the WiFi access point. In the same context, de-authentication can also be used to mount phishing attacks. For example, *WiFiphisher* can be used to execute a de-authentication attack for firstly disconnecting user devices (e.g., mobiles, tablets etc.) from the household WiFi access point, followed by a "Evil Twin" man-in-the-middle attack (e.g., SSID spoofing) to collect WiFi passwords from the unsuspecting occupants [27]. Here, the fact that WiFi is such a common protocol benefits the attacker, as there are several tools (indicatively, Aircrack-ng, MDK3, Void11, Scapy, Zulu and open-source project wifijammer software) and off-the-shelf hardware devices (indicatively, nodeMCU with ESP8266 DeAuther [28] and the WiFi Pineapple device [29]) that are readily available. WiFi de-authentication is by no means new, but in the context of the smart home, the loss of WiFi means loss of Internet connectivity in the household, on which IoT

platforms are increasingly dependent in order to function. Whilst the vulnerability in question was addressed in 2009 by introduction of the 802.11w RFC, which strengthened the authenticity and integrity of WiFi management packets, consumer-based router manufacturers do not often implement this extension into their WiFi protocol stack. So, even though 802.11w is available in most recent Linux kernels and Windows OS (since Windows 8), often this feature must be disabled in order for it to be compatible with household WiFi routers.

A newer type of WiFi attack that can affect a smart home is the key re-installation attack (KRACK) [30], which targets the four-way handshake of the WiFi WPA2 encryption protocol. To connect to an access point with WPA2 security, a Linux or Android-based device negotiates a unique session-specific encryption key using a four-way handshake, where the key is installed after receiving message three out of four. However, to cope with lost or dropped packets, an access point will retransmit message three if an acknowledgement is not received from the connecting device, and each time this message is received, the target device reinstalls the same encryption key; thereby resetting the nonce value (in each packet) and receive replay counter. In this case, an attacker can force nonce resets by collecting and replaying message three. This can be used to decrypt, replay packets and even inject new packets depending on the target protocol. Linux and Android operating systems (OSs) are particularly vulnerable.

In January 2018, the *WiFi Alliance* released new WiFi security enhancements entitled "WPA3". WPA3 includes new protections and enhancements on the existing WPA2 standard, such as default unauthenticated encryption to public networks, individual device data encryption (aiming to prevent complete compromise of the network if the WiFi key is compromised), protection against key re-installation attacks (e.g., KRACK), as well as prevention of brute-force attacks (through rate-limiting of device connectivity). WPA3 also mandates Protected Management Frames as part of the certification (which has also been extended to WPA2), preventing forced de-authentication attacks from occurring [31]. However, as with WPA2, there remains no specific mechanisms to address the threat of Evil Twin access points where an attacker may strategically force unsuspecting smart devices to fall-back to a more insecure version of the WPA2 security standard (or no WPA protection at all). Furthermore, the expected lengthy transition period from WPA2 to WPA3 for all WiFi enabled households and SOHO devices worldwide means that existing WiFi vulnerabilities are likely to pertain for an unknown length of time. More generally, growing reliance on WiFi connectivity as an enabler of the smart home continues positioning this communication medium as a key target for attacks that aim to disrupt and gain access to the household, whether by disrupting WiFi services or compromising vulnerable devices which rely on WiFi for connectivity.

4.1.12. CM-WI-ZG: ZigBee

ZigBee is one of the most popular protocols used in smart homes. An example attack that has been demonstrated in the smart home cyber security literature is a sinkhole attack [32], where a rogue node infiltrates a network of ZigBee wireless sensors and increases its transmission power, so as to be able to reach the ZigBee coordinator with fewer hops and as such be preferred by the Ad hoc On-Demand Distance Vector (AODV) routing protocol used for routing packets by the other sensors. In this position, the rogue node can choose not to forward the packets (and consequently the sensor data or the actuation commands) to their legitimate destination or to modify them before doing so. Notably, performing attacks in ZigBee networks is facilitated by readily available exploitation frameworks, such as KillerBee [33].

ZigBee and emerging IPv6 over Low power Wireless Personal Area Network technologies, such as Google's open source protocol *Thread*, rely on the IEEE 802.15.4 radio standard for physical layer and media access control. Jenkins et al. [34] have demonstrated how different implementations between 802.15.4 radio receivers can be used to achieve device fingerprinting and facilitate targeted attacks, distinguishing between a device that uses ZigBee or Thread (or another future protocol), then identifying the product vendor allows attackers to analyse the smart home and target known vulnerabilities in its devices.

4.1.13. CM-WI-Z: ZWave

Devices using the Z-Wave communication protocol can implement the Z-Wave security layer, which uses symmetric cryptography to provide encryption and authentication services, so as to limit sniffing, replaying and injecting wireless commands. However, different Z-Wave devices share the same secret key. So, physical access to an external sensor, such as a passive infrared sensor outside the property can help access the key, which could work also for the front door, as demonstrated in [35]. A comprehensive hacking toolkit named *EZ-Wave* has been developed by Hall and Ramsey for exploiting Z-Wave networks using software-defined radios. The *EZ-Wave* toolkit is built on top of the Python Scapy-radio library and consists of a network discovery and active network enumeration functions, device interrogation to elicit device name, firm versions, configuration settings and execution of supported command classes, as well as determination of Z-Wave's module generation using physical network layer (packet preamble length) manipulation [36]. The authors also demonstrated that Z-Wave toolkit can facilitate attacks which result in cyber-physical impact on smart devices, with an example of causing vulnerable Z-Wave enabled industrial and compact fluorescent light bulbs to fail (the latter of which are commonly used in modern homes). With two HackRFs, *EZ-Wave* was utilised to request supported capability classes exposed by the Z-Wave devices' application program interface (API), executing these unauthenticated due to lack of encryption on the device. This allowed the

researchers to repeatedly turn on and off the Z-Wave enabled industrial and compact fluorescent bulbs in 1 s "on" and 3 s "off" cycles, causing them to break [37].

4.1.14. CM-WI-B: Bluetooth

Bluetooth is becoming increasingly common in smart home environments. That is because it is at the same time an efficient communication protocol and a good mechanism for evaluating proximity through signal strength (especially Bluetooth Low Energy). In [38], Ho et al. have described how two attackers can unlock a smart lock using a Bluetooth relay device. If attacker A is in close proximity to the legitimate user and attacker B near the lock, then when B touches the smart lock to begin the touch-to-unlock procedure, the message containing the authentication challenge is captured by the Bluetooth relay device and is forwarded to attacker A (via Wi-Fi or some other communication channel). Upon receiving the relayed challenge, attacker A broadcasts it masquerading as the lock, and this is received by the legitimate owner's device, which returns a legitimate response. Attacker A captures this and relays it to attacker B, and in turn to the smart lock, which accepts it and unlocks. Similar attacks have often been demonstrated for unlocking cars that feature keyless entry [39].

4.1.15. CM-WI-N: NFC

Over the last decade, Near Field Communications (NFC) has considerably evolved from its original inception in Radio Frequency Identification (RFID) technology. In standard RFID platforms, systems utilise short range wireless communication medium at low frequency ranges (30-300 KHz); commonly consisting of an identification tag (e.g., transponder), which responds passively by reflecting a signal or actively by broadcasting a signal. NFC (and by extension RFID), are commonly used in physical security systems, such as door entry or physical authentication systems across a variety of industries which require physical security controls (e.g., corporate building access, hotel room keys [40]). Within the context of the smart home, NFC technologies have been employed to provide the same benefits for physical security, as users are able to utilise their mobile devices as front-door keys.

However, due to a lack of definable NFC wireless communication standards and a proliferation of NFC-enabled systems, a number of vulnerabilities have been found across a range of NFC implementations. For example, NFC is vulnerable to remote eavesdropping attacks assuming that an attacker has a powerful enough receiver to capture a NFC signal [41] (by design, NFC requires extremely close proximity between the transponder and receiver, e.g., up to 10 cm). However, based on the device's role (i.e. active or passive communication) which is limited by the type of device (e.g., mobile, payment card etc.), the viable distance for an attacker can vary from 1 m to about 10 m. NFC implementation is often application-specific and even vendor-specific, in many cases omitting security measures. Haselsteiner et. al. [42] have demonstrated data corruption, data modification, data insertion and man-in-the-middle attacks against NFC systems. Other attack vectors have been suggested by Francis et al. in [43], who have demonstrated that it is possible for an RFID tag to be replayed or emulated on a NFC-enabled device. In one example [44], a cloning procedure was successfully implemented through the emulation of the behaviour of a legitimate NFC token .

4.1.16. CM-BC: BidCos

The Bidirectional Communication Standard (BidCos) is a wireless communication protocol operating at the 868 Mhz frequency and developed for the HomeMatic smart home system, used primarily in Germany. Whilst the BidCos protocol claims to support AES-128 encryption, it has been shown by Laufer et al. [45] that the encryption is used for authentication purposes only and that any data exchange taking place is actually unencrypted and does not provide data confidentially. In [46], Kodra has demonstrated that this allows an attacker to easily sniff data on the BidCos network. Moreover, the protocol data unit [47] also allows an attacker to replay packets on the wireless network, which Kodra has demonstrated experimentally against a Homematic testbed in [46]. In [45], Laufer et al. also demonstrated that it was possible to register a malicious node on the smart home network or reconfigure the system in such a way that nodes would change their control unit, if the user had not changed their default password (which was highly likely, because at the time an implementation bug was causing authentication problems if the password had been changed).

4.1.17. CM-WI-I: Insteon

Insteon is a home area network protocol that utilises both wireless and wired connectivity to create a dual-mesh topology for communication between devices. The protocol aims to enforce network security via link control so that users cannot create links which would allow control over a neighbour's smart home, but researchers have shown that the RF process is vulnerable to man-in-the-middle attacks, as Insteon device IDs can be easily sniffed. At DEFCON 23, Peter Shipley demonstrated that by reverse engineering the Insteon RF transmission protocol and its Cyclic Redundancy Check (CRC) algorithm, in reality, it did not use or enforce any encryption in the link-layer at all [48]; allowing attackers to sniff traffic, conduct replay attacks and issue arbitrary actuation commands.

4.2. CS: Control Software

Control software refers to the methods by which devices in the smart home are monitored, configured and operated (e.g., to trigger actuation, request sensor data or install updates). Control software is a prime target for attackers, where diverse software features can expose attack

vectors through use of third party apps and vulnerabilities in the operating system or firmware.

4.2.1. CS-3PA: Third party apps

One of the key drivers of innovation and adoption of smart home technologies is the emergence of programming frameworks that facilitate the development of third party apps, for the same manufacturer or for integration of devices across multiple manufacturers. Popular examples are the Samsung SmartThings *SmartApps*, Apple HomeKit apps and Vera apps. In 2016, Fernandes et al. [49] carried out static analysis, runtime testing and manual analysis of 499 *SmartApps* and found that more than half of them were over-privileged due to too coarse-grained capabilities. Notably, one of the key threats demonstrated was remote lock-picking via a backdoor pin code injection attack. The exploitation functioned by allowing the researchers to generate a HTTPS link that led to the authentic SmartThings login page, which then exploited a flaw in the app allowing redirection of the user credentials (once submitted) from the SmartThings webpage to an attacker-controlled domain. Crucially, it was noted by the researchers that coarse permission binding between smart apps and smart devices was often forced upon the developers by the integration framework used. For example, analysis of the API exposure between *Samsung SmartThings* platform integration and a Zwave lock highlighted that the device is exposes all of its capabilities to the *SmartThings* platform such as "capability.actuator, capability.lock, capability.battery ... etc.". The researchers remarked that a smart app requesting one of these API functions will be prompted by *SmartThings* for user authentication, which then provides the requested access to the Zwave lock device. However, following successful authorisation, the user's smart app not only gains access to the requested resource, but also to all of the other aforementioned capabilities exposed by the Zwave lock device at the same time. As a result, the smart app is granted the the ability to perform functions that it may not have been intended for and therefore if compromised provides a key attack vector to compromise third-party integration between smart apps and smart devices in the household.. Poor authentication and authorisation frameworks and implementation is also demonstrated in research carried out by Jacoby [50], who demonstrated successful compromise of his network-attached storage by exploiting the insecure authentication measures of its web server application (where the main configuration file containing account password hashes was made available to anyone on the internal network). Jacoby also carried out a man-in-the-middle attack against his smart TV by exploiting the cloud application services used to populate multimedia information, which was made possible due to a lack of authentication or encryption used by the TV when downloading content from the network and Internet.

4.2.2. CS-OS: Host OS

To effectively manage and scale heterogeneous devices within the smart home and ensure practical usability for the home user, control software tends to be designed to operate through a single host operating system, such as a smartphone or home hub. In the case of the former, Android has become a popular OS platform in which to develop smart home applications, but is also known for having security flaws regarding application over-privilege or cross-talk. For example, an attack against the DigitalSTROM home automation system [23] was practically facilitated by exploiting the *intent cross-app message* functionality provided by the Android OS for inter-communication between applications. In an attack against the Wink relay controller in [51], the privacy of the system was breached through the Android Debug Bridge (ADB) service. In 2017, Neiderman reported that *Tizen OS*, Samsung's IoT operating system, which used extensively on washing machines, refrigerators and other appliances, was vulnerable to at least forty zero-day attack vectors [52, 53]. Of note was the observation that the particularly insecure strcpy() function (superseded by strcpy_s()) in the C language had been used, even though it is widely known to easily lead to buffer overflow conditions due a lack of bounds checking on input size for the destinations fixed-length buffer. In this case, the buffer overflow vulnerability enables an attacker to execute arbitrary code on the OS, by injecting malicious input which will trigger the applications memory stack to overflow and execute the remaining bytes (which correspond to the attacker's code) with the permission rights of the host program; which if running with root permissions may grant control of the platform to the attacker.

4.3. CS-F: Firmware

Firmware configuration and type is often dependent on the device circuitry, chipset and hardware board. Therefore, many security vulnerabilities in smart homes are often device-specific, caused by flaws or lack of security protocols employed in their design or implementation. Here, we have chosen a few indicative examples in a variety of systems, starting with the lack of state validation in the key exchange protocol handler programmed in the ZWave door lock firmware of a smart lock analysed in [54]. Another example is the common vulnerability exposure code issued to a dishwasher's firmware web server [55], which allows an attacker to traverse and map out the underlying web directory and gain access to sensitive data, such as configuration files and database credentials.

Firmware vulnerabilities identified in the WeMo control software were found to be related to the use of a proprietary protocol that is router-dependent and piggybacks across a household's WiFi network. In 2013, researchers discovered five vulnerabilities in WeMO related to hard-coding of cryptographic keys, downloading firmware codes without integrity checks based on the absence of a local certificate to verify the integrity of SSL connections, clear-text transmission of sensitive information, unintended proxy

or intermediary protocol configuration and improper restriction of XML external entity referencing (which related to the peerAddresses API which could be attacked through XML injection potentially revealing contents of local device system files). These vulnerabilities were later issued in a CERT advisory [56]. Indicatively, in the case of the unintended proxy, the flaw existed within WeMo's use of the universal plug and play over the session traversal for network address translation (NAT) (*STUN*) protocol, which bypasses network address translation firewalls and consequently enables attackers to connect directly to the WeMo devices over the Internet. Of course, these vulnerabilities were later patched in a firmware upgrade, but until then would give attackers the ability to utilise WeMo devices within a Botnet or conduct cyber-physical attacks, such as flipping a switch at a very fast rate to cause electrical damage. Until patched in newer versions, a vulnerability on the firmware of Amazon Echo would allow raw audio captured by the system microphone to be forwarded to an attacker server. The attack required physical access to the debug pads on the bottom of the device (after removing the rubber base), and attaching a secure digital (SD) card to the diagnostic interfaces. From there, a persistent implant was installed into the firmware to provide root access, gaining remote shells and exfiltrating audio recording [57].

In [58], the white hat hacker group *Exploiteers* disclosed firmware vulnerabilities in over 43 Internet of Things devices from home automation devices such as the Wink hub to an LG smart refrigerator. In most cases, insecure access to the operating system via universal asynchronous receiver/transmitter (UART) interfaces allowed direct root access to system firmware for reverse engineering and injection of malicious code. Here, UART interfaces were found to be vulnerable due to the lack of secure UART bootloader which utilise encryption and authentication. This is considered a standard method for offensive exploitation of IoT systems, but one can argue that this, and generally the vast majority of firmware attack approaches, require physical access and are therefore often impractical. Of course, there is also the possibility of a supply chain attack, where the firmware has been compromised before it reaches the buyer (see Section 4.5 for more details).

4.3.1. CS-WA: Workflow automation

Beyond third party apps, the development of which requires programming skills, users can create their own automated workflows and event-driven links with their smart home systems, using If This Then that (IFTTT) *applets*, Zapier *worfklows*, Stringify *flows* and other workflow automation services. An example IFTTT applet may set "location of the user's smartphone is at home" or "user's smartphone connected to home Wi-Fi" as the trigger and "unlock the front door" as the action. In this case, an adversary that might have found it impossible to target the smart lock itself, may instead target one of the triggers in the user-defined *applet*.

As workflow automation platforms can gain significant access in defining, controlling and triggering system behaviour and interaction in the smart home, this makes them a prime target for semantic social engineering attacks [59]. Whilst an attacker may not necessarily target a specific vulnerability in workflow automation platforms themselves, a successfully crafted phishing email that deceives a user into divulging their account's username and password potentially provides an attacker with the ability to edit, delete and create new workflow automation rules in the target household. By example, soon after Heartbleed OpenSSL vulnerability was made public in 2014, attacks began to craft phishing attacks targeting the IFTTT service aiming to gain access to victims accounts by spoofing emails requesting users to reset their passwords in light of the vulnerability affecting account security [60]. Depending on the degree of integration and different systems within the smart home, an attacker may have the ability to exfiltrate data, delete rules as a form of denial of service, as well as introduce new rules that would result in physical impact (detailed in section 5).

4.4. S1: Sensory channel

While research in relation to the security of sensing tends to focus on the data sharing, storage and processing, attackers may also maliciously manipulate the process at the level of data collection by exploiting physical weaknesses of the sensors themselves. Below, we have included an indicative list of such sensory channel exploitations.

4.4.1. S1-U: Ultrasonic

Ultrasonic sensing is commonly used for physical security applications in smart homes, for example for presence detection [61], but is also applicable to indoor positioning [62]. Ultrasonic sensing can be deceived by jamming the signal and replaying it slightly later, so as to generate the impression of longer physical distance [63] or by producing a new but similar ultrasonic pulse [64]. In some cases, ultrasonic sensors can be bypassed by moving very slowly in front of them or by wearing a costume made of anechoic material that absorbs sound waves [65].

In 2017, ultrasonic attacks against a range of popular voice-controlled smart home assistants were demonstrated experimentally by generating human inaudible voice commands in the 20 KHz frequency range that were detected and processed. Zhang et al. have shown how to perform what they call a "Dolphin" attack [66] by modulating low-frequency voice as baseband signals on an ultrasonic carrier, which are then effectively demodulated by voice capture speech recognition systems on the receiving hardware. Their results have shown that 15 out of 16 voice control systems (consisting of both mobile devices and home assistants, such as Amazon Echo Alexa) recognised the ultrasonic voice commands and (where applicable) 13 out of 13 platforms activated in response to the ultrasonic commands. However, it was also shown that the

modulation parameters and maximum effective distance for recognition and activation varies significantly between different platforms. Nevertheless, the researchers demonstrated how the attack can be performed in a mobile nature using a relatively simple attack implementation, consisting of a Samsung Galaxy S6 Edge smartphone, ultrasonic transducer and a low-cost amplifier (where the transducer and amplifier cost no more than 3 dollars). Given this inexpensive and portable attack platform, the practicality of executing remote-controlled rogue ultrasonic voice injection attacks becomes an attractive prospect for attackers targeting voice-controlled systems.

Using the same premise, theoretically, an infrasonic attack (which by current convention would be named a "whale" attack) would pose the same threat to voice-controlled system microphones that are able to detect acoustic noise below 20Hz. To date, there have been no publicised infrasonic attacks against smart home or IoT systems. However, infrasound has been studied extensively as to its adverse effects on human subjects and therefore any future attack that aims to generate or inject infrasound in the smart home could potentially lead to harmful effects on occupants' physical and mental well-being.

4.4.2. S1-V: Voice

Google assistant, Amazon's Alexa and Apple's Siri are examples of personal assistant services that allow voice-activated control of a rapidly expanding range of smart home systems. From the perspective of security, voice becomes a sensory channel for the transmission of smart home actuation commands and exfiltration of information. Yet, this is a channel that is not normally monitored by technical cyber security measures. [1].

In addition, personal assistant services tend to offer third party apps (CS-3PA), such as Google Assistant's *Actions* and Amazon Alexa's *Skills*, which expand massively the range of systems and functionality that can be controlled. Equally important is that modern voice-activated systems do not need to learn their users' voice, as exemplified in 2017 by a Burger King television advert which activated voice-controlled Amazon Echo devices by intentionally embedding a voice command [68] and by the rogue dollhouse orders issued when "Alexa, can you play dollhouse with me and get me a dollhouse?" was heard on a television programme [69]. Consider a situation where a compromised smart toy [70, 71, 72] plays a pre-recorded voice command, such as "Alexa, unlock front door", as demonstrated in Figure 5. In April 2018, security researchers from Checkmarx developed a proof-of-concept malware that takes advantage of the platform's third-party app integration (see section 4.2.1, called *Alexa Skills*, which puts the device in an continual audio recording state to eavesdrop on audio in the household and then export recorded transcripts to a third-party system [73]. By disguising the malware as a simple calculator app, activated via "Alexa, open calculator", the Echo API (*Amazon Lambda*) associated with the skill launches a second request to covertly record audio input. However, the activity can be visually detected by occupants if they recognise that the blue light on the device (which indicates it is listening for voice input).

In 2016, research carried out in [74] demonstrated how hidden voice commands can be carried out on personal assistants and a range of smart device with voice-controlled applications. The researchers were able to generate voice commands, unintelligible to human listeners, but interpretable by voice-controlled speech recognition systems in smart devices. Using a black box model, they were able to obfuscate commands with an audio mangler and using Mel-Frequency Cepstrum transformation, without any understanding of the target system's configuration (in this case, the Google Nows speech recognition system). For phrases "Ok Google" and "Turn airplane mode on", the Google system was able to interpret with 95% and 45% accuracy respectively, compared to human transcribers' 22% and 24%. In the case of a white box approach, where an attacker has full knowledge of the internals of the speech recognition system, utilising a hidden Markov model (HMM), the researchers generated a target audio phrase derived as a sequence of HMM states compressed by minimising the number of speech frames. Their testing showed that a speech recognition system targeted (CMU Sphinx) accurately interpreted 82% of obfuscated commands, compared to 0% for human transcribers.

4.4.3. S1-IR: Infrared

The broad range of infrared applications varies from communication between home appliances (IR remote), distance measuring or medical equipment such as medical fusion pumps [75], where researchers have used an external infrared transmitter to alter medication dosage. Recent work carried out by researchers at Ben-Gurion University has demonstrated how CCTV security cameras with infrared functionality can be used as a data exfiltration medium to export data from a compromised device in an air-gapped network [76]. Here, the researchers blink infrared LEDs in a morse-code-like pattern to transmit binary data to a receiver over a distance of tens of meters. The attack functions by utilising the infrared light as a sensory that can be encoded and decoded to exchange data. By employing basic "on-off keying", binary frequency-shift keying and amplitude-shift keying modulation techniques, the researchers have demonstrated that the absence / presence of a signal, the frequency of change and the illumi-

[1] Although not in the context of smart homes, the principle of exploiting the fact that a speaker-microphone pair is a security-wise unmonitored communication link has been used by Diao et al. [67] to bypass the permission settings of a smartphone. Their experimental application needed only access to the speaker to whisper a command such as "call x number", which is picked up by the phone's microphone, and recognised by Google Voice Services, which in turn initiates the call (also using text-to-speech to exfiltrate sensitive information)

nation of the light can be used to generate a bit datastream for infiltration (e.g., command and control) or exfiltration of data, respectively.The attack positions smart IR-enabled CCTV smart platforms as viable attack vectors for steal sensitive data from a compromised smart home network. The researchers have also highlighted that the same vulnerabilities are likely to exist with doorbell cameras equipped with IR LEDs, which are typically installed (unlike CCTV cameras) at locations and heights which provide easier line of sight for an attacker to exchange data via IR signals.

4.5. S2: Supply Chain

The extreme diversity between devices, actuators and sensors, as well as control software and third-party applications means that the smart home is particularly vulnerable to a supply chain attack. Here, were refer to the supply chain as exploitation of the method of distribution and delivery of hardware and/or software components for devices in the smart home, whereby the supply chain positions an attacker to embed malware, gain control of, or sabotage these devices and interdependent systems in the household. As an example, the second-hand sale of smart home technology in popular online marketplaces such as *Amazon* and *Ebay* allows provides an ideal supply chain for threat actors to distribute malware-infected products.

4.5.1. S2-S: Software

In 2014, a cyber espionage grouped named *DragonFly* targeting supply chains in industrial control software suppliers were found to be replacing legitimate files in suppliers' software distribution websites with their own malware-infected versions of the software [77]. Specifically, the attackers "trojanised" existing, legitimate industrial control system (ICS) software by first compromising the website of the software suppliers and replacing the existing ICS software with malware-infected versions allowing remote access.. In smart home platforms, this attack targets a legitimate and trusted software supply chain for household devices (e.g., providing firmware, operating system or third-party software). A compromise of the software supply chain may result in subsequent attacks on smart home devices control software as a result of installing compromised software (see section 4.2).

Software supply chain threats can also be observed through the side-loading of malicious applications on smartphones and tablets, where such devices are often application control hubs for smart home automation and control. Side-loading involves the installation of an application on a smart device outside of the security of a monitored application marketplace (e.g., Google Play, Apple App Store), where the integrity of the software supplier cannot be verified. This may involve downloading an application via a URL or advertisement hosted on a website or presented through another app that is being used. In 2016, a remote access Trojan called *DroidJack* posing as the popular android application *Pokemon Go* was identified by security company Proofpoint. At the time of discovery, *Pokemon Go* was not available in specific countries, whereby the Trojan APK seemingly offered the application unofficially via a side-loading installation [78]. On installation, in addition to standard *Pokemon Go* permissions, *DroidJack* would additionally request access to read web history, change network connectivity, directly call phone numbers, edit text messages, record audio, modify contacts, as well as retrieve apps running at startup. This would effectively grant the malware complete control over the Android device, and as a result of any smart home devices controlled by it. Inspection by analysts showed that three classes had been added in the Trojanised app, with one of them creating a channel to a hardcoded command and control domain and port.

For smart homes, the software supply chain is particularly vulnerable to audio/video streaming in social media platforms, such as YouTube, where the provenance of data is often unknown and can be uploaded by any user. Here, voice-controlled systems are specifically targeted with the aim to make speaker-equipped household devices play malicious audio supplied through these services, as exemplified by recent YouTube adverts and Television shows triggering home automation systems [68, 79]. The media hosting entity in the software supply chain host can be trusted, such as YouTube, or untrusted, such as illegal streaming websites.

4.5.2. S2-H: Hardware

Supply chain attacks on hardware include physical damage or tampering of system components used in the construction of IoT devices (such as memory, wireless antennas, interface buses, firmware etc.) or devices that have been intercepted by attackers and compromised. The latter can involve sabotaging the integrity of an internal component or inserting malicious implants, so as to provide the attacker some form of control of the system when activated [80].

4.6. S3: Side-Channel

Side-channel attacks are a well-studied area of research in computer security, especially in the field of cryptography for attempting to gain knowledge about a system based on electromagnetic emanations from its hardware. Such knowledge, such as frequency spectrum, power fluctuations and electromagnetic interference provide insight into the state of a system or the function it is performing. Side-channel attacks can also use modules present on modern processors to create covert communication channels. In [81], the authors have used a hardware random number generation module that operates across CPU cores and virtual machines, to construct a covert channel with a capacity of up to 200 kbit/s. Although the capacity depends on the system's load, the approach results in a reliable and low-error channel. An approach that can

exfiltrate data from air-gapped computers without audio hardware and speakers has been presented in [82]. The proposed approach uses noises emitted by the CPU and chassis fans, and controls the acoustic signals they produce using a specialised software. The binary data produced are then transmitted to a nearby mobile phone. The method achieved a transmission rate of 900 bits/hour and the authors demonstrated that it can also be used for IoT devices that contain fans of various sizes. In the following sections, we further elaborate on the side-channel attacks related to electromagnetic emanations and interference, as these are more closely related to the context of a smart home.

4.6.1. S3-EMA (Electromagnetic Emanations)

Here, an example would be the electromagnetic emanations leaking from unfiltered powerlines. In [83], Eney et al. have demonstrated the viability of measuring a home's powerline activity with such accuracy that they could identify what the occupants were watching on television. Their method was reproducible and accurate enough across a wide range of modern television sets.

4.6.2. S3-EMI (Electromagnetic Interference)

Instead of passive eavesdropping emanations to elicit information from a system, electromagnetic interference is either an intentional or unintentional threat which disturbs the correct operation of a system. In the smart home, it has the potential to damage consumer electronics attached to the powerline or used within a directional electromagnetic antenna and has been used as an attack vector in multiple real-world cases associated to robbery and causing criminal damage [84, 85]. Kune et al. have demonstrated experimentally in [86] that at certain distances electronic devices containing microphones are vulnerable to injection of rogue radio signals.

5. Impact on systems:

A primary consideration in proposing this taxonomy is the nature of impact that different cyber and cyber-physical attacks can have on the occupants of a smart home. Here, we follow the terminology introduced in [65], where a cyber-physical attack is defined as a "security breach in cyber space, which adversely affects physical space, leading to breach of physical privacy, unauthorised actuation, incorrect actuation, delayed actuation or prevented actuation, as summarised in Table 2.

In terms of cyber impact, we adopt the standard CIA triad of confidentiality, integrity, availability and include a further property of non-repudiation. This is not exhaustive, as authenticity and other extensions of the CIA triad can be considered, but we argue that the four chosen are of relatively higher priority in a smart home context.

5.1. Physical impact

5.1.1. P-BPP: Breach of physical privacy

While in the traditional grid, energy consumption information is collected once a month, the use of smart meters allows frequent energy consumption reporting, typically in 15 or 30-minute intervals. The transmission of highly granular energy data leads to the risk of eavesdropping attacks targeting valuable physical privacy information about the presence of a household's occupants at a particular point in time or their lifestyles in the longer term [88].

An attack demonstrated by Veracode demonstrated the ability to breach physical privacy in a household by hijacking the Wink Relay touch-enabled controller to turn on its microphone and record audio in a household. Here, privacy is breached through audio means, by taking advantage of the Android Debug Bridge (ADB) [51]. ADB was later disabled by the vendor in a subsequent software update.

Increasingly, smart home devices come equipped with Internet access which are left poorly secured and as a result expose vulnerabilities over physical privacy. For example, Internet devicescanning search engines (such as Shodan), allow attackers to identify open ports of nodes, indexing the header or banner information of responsive nodes; which can include information such device type, model, vendor, firmware version other open protocols. As Lin and Bergmann have identified in [2], simple queries such as "has_screenshot:true port:554" on Shodan returns a list of cameras, their IP addresses, geographic location and captured screen-shots. More often than not, results include both internal and external home surveillance systems; granting malicious actors remote visibility over everything (including other devices which could be used for further, lateral intrusion) in the smart home.

Real-world threats to smart home privacy have been materially observed in recent vulnerabilities in home video baby-monitor devices. Over the past three years, a number of reports have identified vulnerable baby monitor cameras, which allowed perpetrators to visually spy on children [89, 90, 91].

5.1.2. P-UA: Unauthorised actuation

Any attack leading to the hijacking of a smart home's actuation commands could lead to unauthorised actuation. Here, an example would be the unlocking of a smart lock [70, 54], as well as the unauthorised switching on or off of lights, heating, ventilation, air conditioning, etc. A network traversal vulnerability discovered in WeMo smart home devices provided attackers with the ability to remote connect and execute commands that would allow them to be utilise in a botnet or to cause physical damage such as electrical faults.

5.1.3. P-IA: Incorrect actuation

At small scale, a simple related attack would be one that would continuously increase the temperature read-

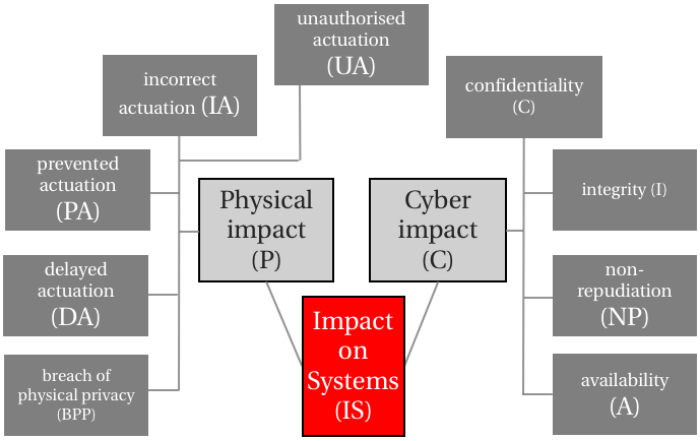

Figure 3: Impact on system's taxonomy criteria

Table 2: Definitions of physical impact on systems

Physical Impact	Definition
Breach of physical privacy	Be watched, listened to, or recorded against one's wishes [87]
Unauthorised actuation	Actuation initiated without the approval of an authorised user [65]
Incorrect actuation	Actuation not as required by authorised user [65]
Delayed actuation	Actuation initiated or completed later than desired by authorised user [65]
Prevented actuation	Authorised user unable to initiate desired actuation [65]

ings of a thermostat, forcing it to keep lowering the temperature in the rooms. At much larger scale, cyber attacks against smart homes at community level could cause large-area power system blackouts through cascading effects. Liu et al. [92] have studied analytically and via simulation adversarial cases, where an attacker manipulates the electricity price to overload transmission lines by forming peak energy loads, or increases the energy load's fluctuation to disturb the power system dynamics. Both lead to cascading outages in the power grid.

Incorrect actuation can also occur as a result of "unintentional actuation", that is, actuation executed as a result of automatic functionality configured through a users smart home appliance. For example, in [38] the researchers explain how the *August* and *Danalock* smart lock appliances automatically unlock the doors they are connected to when the occupier (with the smartphone app and a Bluetooth BLE connectivity) is within a 50 metre radius. However, these locks assume that occupants always enters and leaves via the same door and therefore automatically unlocks the same door when the occupant is within the BLE connectivity radius. In shared accommodation or areas with high crime rates such behaviour is highly undesirable.

5.1.4. P-DA: Delayed actuation

Attacks affecting the availability of a smart home's communication network can lead to delayed transmission of commands and consequently delayed actuation. The smart home ZigBee sinkhole attack in [32] demonstrated how a rogue node can advertise itself as a favourable route to a ZigBee controller, whereby ZigBee sensors (containing actuation commands) which utilise the rogue node for data transport may result in a delayed actuation if the rogue node drop or manipulates the data.

P-PA: Prevented actuation

One popular feature provided by smart home technology providers is vacation mode, typically involving turning on and off of lights and other devices, so as to create the impression that the occupants are in while they are away. Fernandes, Jung and Prakash [49] have proposed a "disabling vacation mode" attack, where their own SmartApp interferes with the occupancy simulation by raising a false mode change event. This prevents the actuation expected by the occupants while they are away.

5.2. Cyber impact

C-C: Confidentiality

Here, an example is the door lock pin code snooping attack demonstrated in [49]. In their proof of concept implementation, the authors have developed a battery monitor *SmartApp*, which exploits an over-privilege issue in Samsung's SmartThings environment, to view plain text pin codes and leak them via a short message service (SMS) message. Unauthorised access to this information would likely lead to unauthorised physical actuation as a second-order physical effect (P-UA).

5.2.1. C-I: Integrity

Breaching the integrity of data or a service is a common route for a cyber-physical attack targeting actuation. In

that sense, most cyber security breaches in a smart home will involve some form of unauthorised manipulation of data. An interesting early example would be the malware infections caused by digital photo frames reported in 2009 [93]. The infection would occur when some of these devices were connected to a computer via USB to load new photos. In 2014, a large scale phishing attack discovered was discovered by Proofpoint [94], where it was found that source-addresses of phishing messages included smart home appliances such as internet-connected fridges, where it was surmised that these devices were likely used as message relays/proxies for forwarding the malicious emails which is a common practice in obfuscating the source of a phishing campaign.

5.2.2. C-A: Availability

Common examples of availability attacks are denial of service and jamming. In a Wi-Fi based smart home, denial of service would involve first gain access to the home network and then flooding with meaningless network traffic its smart devices, such as security cameras, rendering them unable to receive commands or transmit data. Communication jamming has also been studied extensively for some of the main communication protocols used in smart homes. For example, Jokar, Nicanfar and Leung [95] have demonstrated wide-band denial, pulse denial and jamming designed specifically for IEEE 802.15.4, which is the basis for ZigBee.

An major threat to the cloud-supported availability of the smart home was exemplified by a major Amazon Web Services outage on February 27th 2017, for which many IoT smart home vendors rely on for cloud services. The outage of the AWS S3 storage platform resulted in multiple vendors system going down and a many reports from smart home occupants claiming that they were unable to turn off appliances such as WiFi connected ovens, alarms and loss of functionality for physical security appliances and multimedia systems [96].

5.2.3. C-NP: Non-repudiation

Within the smart home, non-repudiation is associated to an occupant's ability to provide evidence that distinguishes legitimate computer activity generated by themselves or fellow occupants and activity which has been executed by a malicious actor. Here, examples include a compromised smart meter which increases the energy consumption [97] and rogue payments through home assistants using audio-based attack vectors [79]. Future risks may well include compromised devices (such as smart fridges [98]), which are under the command and control of a botnet [99] or used as message relays for attack communications.

6. Impact on domestic life:

We have proposed a number of potential attack vectors and associated physical and cyber impacts, which almost certainly have wider applicability beyond the scope and context of the smart home (e.g., smart city, hospital, school, warehouse etc.). However, another primary motivation for this taxonomy is to identify specifically how such threats, within the unique smart home setting, directly affect domestic life.

Smart home environments aiming to enhance home security [100], well-being, especially for the elderly and disabled [101, 102, 103], energy efficiency and financial savings [104], and enable greater workspace and vocational flexibility, are expected to provide a significant positive impact to domestic life. Paradoxically, by merging cyber and physical worlds, they introduce new threats to each of these aspects. As a result, confidence in smart home technologies and consequently their adoption is undermined where cyber security is not proportionate to realistic threats to home security, well-being, energy efficiency, household finances and vocational flexibility.

6.1. DC: Direct Consequences

Cyber attacks aim to interfere with the usage of devices or services that are provided to the user, where the effects can have direct and possibly long term consequences on the users life. One of the most common consequences, and indeed purposes, is related to financial aspects of a successful attack. For example, ransomware [105] limits a user's ability to use devices or services that are targeted in the attack until they pay a required amount. Targets for this type of attacks are most often companies, but attacks on homes may increase significantly. Possibilities of threats and actual attacks make the home an unsafe environment that can effect a users well-being. cyber attacks can be aimed toward users health, physical health through interference with implantable and wearable medical devices [106], and toward psychological well-being. Intrusion to a user's home in the form of different cyber attacks can affect their psychological well-being through decreased privacy [107, 8], loss of control [108, 109] and inconvenience.

6.1.1. DC-F: Financial

Financial loss due to the cyber attack of IoT devices at home can be consequence of a burglary, increase of the household bills, malware infection of the user's software, possible blackmails after spying household members or children, access to a bank account, malfunction of devices or usage of a user's confidential information for making unauthorised purchases.

PenTest Partners developed the first Ransomware for smart thermostats that effectively gives an attacker to control the temperature of a household [97]. By exploiting the Adobe Air package contained in the system files of the thermostats linux image, the researchers were able to gain root access to activate the heating and cooling in a household at the same time; wasting lots of power and increasing the energy bills of the homeowner. At the same time they

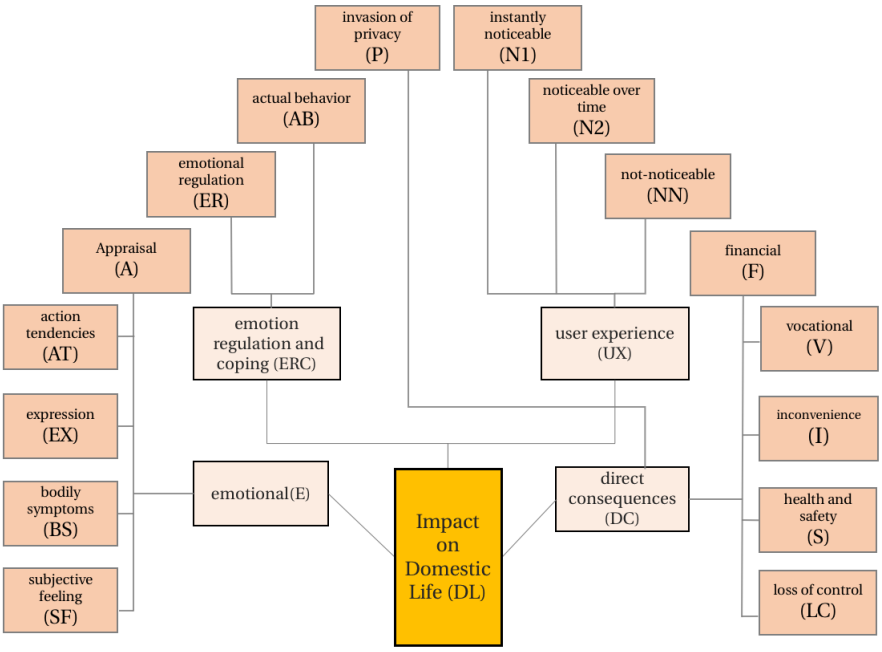

Figure 4: Impact on domestic life taxonomy criteria

were then able to lock users out of the thermostat by applying a pin to the device.

6.1.2. DC-V: Vocational

Over the past few decades, the increase in technology availability in the home has enabled it to become an increasingly productive environment for remote working. For example, the office for national statistics in the UK reported that from 1998 to 2014, the proportion of people working from home in the UK rose from 2.9 million to 4.9 million [110]. However, increase in home working and the advancement of ubiquitous connectivity in the household is symptomatically increasing organisations' exposure to cyber threats which users are not equipped to mitigate; especially if organisations rely solely on a locked-down laptop and VPN software or router for defence. For instance, it is common practice for employees to discuss business matters and share company information and data by voice or video (e.g., conference calls), which may be confidential. In the past, threats to this communication medium were low as only very targeted attacks (such as physical bugging) posed a risk. In the smart home, this information may now be picked up more easily by exploiting poorly protected IoT devices with built-in microphone systems, such as personal assistant services (e.g., Google Home, Amazon Echo), children toys and other voice-controlled house-hold appliances.

Using a different perspective outside of cyber risk, an article by Digitist magazine [111] considered the smart home as an environment that may begin to have an adverse impact on employee productivity due to constant interruptions by smart devices and their activity within the household; which in turn could force organisations away from popular home working models.

6.2. DC-S: Health and Safety

Here, we refer to impact on physical health rather than emotional health. In one of the first security analyses published for smart lights [112], researchers from the University of Washington investigated whether it is possible to cause physical harm in an exploited smart home. Their hypothesis was that one avenue for this would be to cause compact fluorescent lamps to explode. Although three of the 10 in their experiments did explode, the effect was not significant. It was perhaps more significant that by taking control of the lamps, they were also able to produce fluctuations at an appropriate frequency to induce seizures, which would be harmful to occupants suffering from epilepsy. This is not an attack that can be discarded as unrealistic. There has been at least one case of a real-world security breach that had such aim (albeit not in the context of a smart home). In 2008, the website of not-for-profit Epilepsy Foundations website was defaced, introducing flashing animations chosen to cause migraines or seizures to visitors that suffer from epilepsy. At least some of the visitors were affected [113]. Also, more recently, a journalist known to suffer from epilepsy received a twitter message reading "You deserve a seizure for your posts" along with an animated image showing a blinding strobe light, which did in fact cause him a seizure. The person behind the message was arrested a few months later [114].

More recently, household gas cookers have been released with WiFi connectivity that allows for remotely control of the oven with the physical presence of occupants;

through the use of an Android application that even includes a chat function [115]. Although there have been no examples of exploitation to date, the security of the oven is underpinned by both the protection of the mobile application and WiFi environment in which it has been employed. Were such a device to be successfully exploited, the physical consequences could be severe.

6.2.1. DC-P: Invasion of privacy

As complementary to cyber impact through loss of confidentiality (IS-C-C) and physical impact through a breach of physical privacy (IS-P-BPP), here we focus on impact to privacy from the psychological perspective; that is, the regulated activity carried out by an occupant experiencing a violation of privacy with respect to psychological dimensions of privacy (solitude, reserve, isolation, anonymity, intimacy) [116]. Apart from the obvious threat of breaching physical privacy by physical means, an invasion of privacy would occur when an unauthorised party received unacceptable or inappropriate access to someones personal information [117]. In 2012, empirical research carried out by Oulasvirta et al. [8] demonstrated that breaching the psychological dimensions of privacy causes annoyance, concern, anxiety and even rage for household occupants. Focusing on continuous video surveillance within homes, the researchers found that the potential of invasion of these dimensions of privacy through video surveillance causes noticeable changes in the behaviour of the participants. Participants were consistently aware of the surveillance and exhibited privacy-seeking behaviour through ceasing specific behaviour completely, hiding, acting privately and manipulating sensors, as well as changing their practices to actively avoid surveillance (e.g., meeting outside the home for private conversations). This kind of behaviour is expected for occupants of a smart home who perceive that their physical privacy may be breached through a compromised IoT device that captures audio or video. Early examples of real world compromise have been reported for Internet-connected baby monitors [89]. However, as IoT devices through sensing and actuation continue to augment domestic life, such as tracking occupant activity (e.g., from taking a shower to cooking and evening meal or sleeping), an invasion of privacy extends to recording daily life, habitual schedules and activity recognition. Whilst experimental results for video surveillance in the home provide early indications of occupant behaviour when there is a noticeable invasion of privacy, understanding how occupants will respond to a realisation that they are being observed in data through a compromised smart home meter, light bulb, scale or TV is an important challenge.

6.2.2. DC-LC: Loss of control

Control over devices is one of the purposes of the usage of the IoT devices, and it could be taken away through different forms of cyber attacks. Loss of control is manifested through taking control away from a user where third party gains partial or complete control and access over user's IoT devices and household. Loss of the control over the situation can be perceived as threatening while increases in perception of control are associated with better physical health, greater social support, self-acceptance, a sense of purpose in life, autonomy, mastery, growth and positive relationships and a general sense of satisfaction with the quality of ones life and general wellbeing [109]. An example of the cyber attack with control loss can be random triggering alarms in the users or activation of different IoT devices with a goal of creating fearful and threatening situation.

6.2.3. DC-I: Inconvenience

One of the most obvious direct consequences of cyber attacks is inconvenience caused by interruption of functionality of IoT devices in the situations when users expect to rely on them. It can be manifested through time consuming as opposed to time saving that should be one of the benefits of usage of the IoT devices. Programmed morning routines with the purpose of saving time (alarm clock, preparing coffee, heating the home, closing the garage or entrance doors) can easily become an additional task for users if they have to deal with delay, malfunctioning or failure of the programmed IoT devices ([96]). Instead of enjoying initially desired automation of everyday functions users can face the opposite outcome if their devices are attacked.

6.3. UX: User experience

The degree by which a cyber attack in the smart home is visible to household occupants depends on its immediate or long term effects on the user experience of systems which have been affected. For example, attacks that are noticeable in the moment of the execution (by activation of different devices [60], jamming of traffic [118], or resulting in the loss of control over devices [97]) can immediately activate occupants' awareness that their household may be under attack. On the other hand, some cyber attacks are more discreet in execution, such as providing a backdoor to control devices [56] or to conduct recognaissance [48], which may not be immediately obvious to occupants until a such time that they observe anomalous system behaviour, or never at all if the attack does not impact or alter system functionality and performance.

Users of IoT devices are often unaware of cyber attacks or when their devices are used for malicious purposes ([119]), which leads to a lack of action and decreases actions of prevention as well (especially where technical defences are unable address such threats).

6.3.1. UX-N1: Instantly noticeable

As occupants of the smart home begin to rely on smart devices and systems for every day tasks, disruption to the services can indicate either a malfunction or also a potential cyber threat. In both cases, household users may immediately notice degradation of performance, such as decreased responsiveness of IoT devices, delayed, prevented

actuation, incorrect or unauthorised activation of alarms, garage doors etc. In general, an attack in the household that would be instantly noticeable is an attack where the user notices that they have either lost control of their household devices or that someone else is controlling them as well [56, 51, 97].

6.3.2. UX-N2: Noticeable over time

Certain attacks against the smart home do not generate cyber and/or physical impact which is immediately obvious or noticeable by a user. For example, where an attacker has gained remote access to a system such as security camera or baby monitor unless the occupant is actively trying to access the system at the same time they may be unaware some else is logged in and viewing the video feed [90]. However, over a period of time, behaviours exhibited by targeted systems or second-order symptoms observed in interdependent platforms may generate a visible footprint in which household users become aware that an exploitation has occurred or is indeed still on-going.

6.3.3. UX-NN: Not noticeable

In the case where an attack is not noticeable by household occupants, attack vectors tend to focus on gaining persistent remote access (rather than denying a system) in order to conduct further reconnaissance, such as penetrating the network further through lateral movement into other devices [25] or to gain passive control over household systems as a means to launch external attacks on other platforms; building a botnet of smart devices [56].

In general, more often than not, users are not aware that their IoT devices are being attacked, irrespective of whether an attack exhibits anomalous behaviours that are visibly obvious. Nevertheless, attacks that are able to infiltrate the smart home without exhibiting noticeable signs to household occupants pose a significant threat to occupants safety and well-being; especially if technical defences are also unable to detect them.

6.4. E: Emotional

The home is meant to be a safe haven to experience privacy, control and personal autonomy. A cyberspace violation affecting a smart home may thus lead to considerable and long-lasting emotional impact. Attacks may even be designed specifically to cause the occupant to experience high levels of stress and discomfort, for example by triggering fake alarms, as demonstrated in [49], where the authors have shown how to raise fake physical device events, such as the report of increased levels of carbon monoxide. In a recent occurrence, the hijacking of an Internet-connected teddy bear resulted in two million voice recordings between parents and children being made publicly available on the internet [120]. Further, Pentest Partners demonstrated how it is possible to gain complete root access to an Internet-enabled adult sex toy, capturing streaming video from the device and changing its configuration [121]. In both cases, access to such sensitive and private information leads to significant emotional impact and second order threats, from blackmailing, publicly shaming on the Internet, damaging a persons reputation, or gaining access to other systems the occupants may use in the household (e.g., by stealing Wi-Fi passwords). In fact, eliciting a particular emotional response from a household occupant, with or without their knowledge, can be used as part of a social engineering attack [59].

More generally, emotional distress as a consequence of a cyber attack is related to personal sense of the loss of control and privacy, a decreased ability to function on a daily basis, to work, and even long-lasting deleterious financial and legal consequences. The realisation that one is a victim of such an attack, specifically targeting the intimacy of one's home, can trigger an emotional experience akin to physical abuse, in the process also leading to lower trust levels in IoT technology. Further, such emotional consequences are likely to be felt and re-lived over significant periods of times, over months or years. Once an occupant realises they have been a victim of an attack and progressively acquires the full understanding of the consequences, it is likely they will experience relapses of related emotional events, affecting their personal well-being and recovering process, and will have to engage in renewed coping strategies, to mitigate such emotional consequences. Whereas there is no theoretical framework that fully describes the emotional engagement of IoT users, a significant understanding, we posit, can be gained by drawing inspiration from emotional psychology. An emotional experience can be measured and compared, and serve in the elaboration of user models and the prediction of behaviour. Communities, comprising cyber-security specialists, industrial interests and policy makers, can benefit from this information to delineate features and courses of conduct that will place the user's well-being at the centre of the design of IoT and smart home technology, as well as to help formulate training to condition emotional responses as result of suspected or realised attacks.

An emotional experience is best described over time at the specific granularity that pertains to the aspects that one seeks to exemplify [122]: In other words, emotional reactions will vary in duration and amplitude, function to contextual and personal aspects. Following a smart home cyber security incident, the immediate aftermath is the realisation that an attack has occurred, and gradually becoming aware of its consequences, as victims evaluate dimensions of the event against their personal belief system and core personality. In the longer term, the user reacts and copes with the consequences, involving a series of emotional states in relation to the recovering process. Whereas the long term scale corresponds to broader emotional experiences, the immediate aftermath relates to the evaluative processes that support the personal understanding of the event by the user. Importantly, evaluative processes both drive the amplitude of the experience over time and determine the emotions perceived, such as anger and irritation

[123], that is the valenced reactions that ensue. In addition to evaluative processes, emotional reactions typically comprise reactions in four other systems, action tendencies, bodily reactions, expression and subjective feeling, which can also be measured. Activation in all five systems determine the shape, content and intensity of emotional experience [122].

6.4.1. E-A: Appraisal

Evaluative processes following a smart home cyber security breach are most likely to engage strongly dimensions about familiarity, privacy, coping resources and power [124]. The same attack can be appraised differently by different persons, depending on personality [125], expectations and level of knowledge about risks and the consequences of the breached security [126]. The ensuing emotion process depends on the precise appraisal that is made by the person. In the case of a man-in-the-middle media injection attack on a smart TV [50], a user becomes instantly aware that a smart TV is controlled by a third-party. While the attacker is controlling the changing of videos, content images, links or audio files, the user will realise that their device is hijacked and begin to think about how to stop exposure to unwanted content. This is especially the case if the content is not appropriate for children, or if it is harmful for the user (e.g., videos that cause epileptic seizures). Appraisal actions here can lead to thoughts about invaded privacy, loss of control, about who is behind the attack and whether the attack is aimed specifically at the victim or if it is random. Instead of immediate action, here different appraisals may inadvertently increase an occupant's exposure to the attacker by leading them to an evaluative state that does not result in a direct mitigating action (e.g., by removing device network connectivity to disrupt attacker control).

6.4.2. E-AT: Action tendencies

Action tendencies are tendencies to behave in certain ways that are elicited by the emotion process [127]. Experience of the attack can range from having a desire to escape from the situation and to stop using devices, to investing all effort into solving the problem that occurred [124]. Beris et al. [126] have shown that depending on risk perception and emotional stance toward breached security, a range of different tendencies to act can occur. Categorisation of different attitudes and behaviours could be used to predict which members of the household are the "weakest links" and, with their attitude towards IoT devices increase the home's cyber risk, and as a result need education or training. Intrusion in the private life and space can make people ready to defend their privacy with any available means. Acting from emotional affect is known to bring intensive reactions of fighting for the justice, especially when anger and fear are experienced [128, 129]. Dramatic cybercrime consequences, in the form of suicide, are found at both ends, attackers side [130] as well as the victim's side [131]. Ambiguous and geographically diverse legislation for cyber crime [132] has its share in expectancy, predictability and differences in behavioural outcomes related to cyber attacks.

6.4.3. E-B: Bodily symptoms

Possible bodily symptoms [127] during a cyber attack can include hyperventilation, blood pressure and heart beat increases [124]. An interesting recent example of related research is the experiment carried out by Canetti et al. [133], which used salivary cortisol as a measure of the stress caused, to show that cyber attacks make people more likely to express threat perceptions. The intensity of bodily reactions as a result of cyber attack events depends on initial psychological and physical condition of the users, as well as the level of integration and dependency occupants place on smart home systems. Symptoms can also depend on the nature of the cyber attack, and if it was especially aimed to harm a users health. Direct intention to harm a specific person was shown in the case of an epileptic journalist who suffered a seizure after viewing an image that was sent purposely to him, with the intention of causing seizure, as a punishment for his online posts [114].

6.4.4. E-EX: Expression

Possible emotional reactions [127] could range from a hopeless expressionless reaction to shaking, frowning and saying loud angry words [124]. Individuals differ whether they are emotionally expressive or unexpressive [134]. Gross and Levenson (1993) showed that emotional expression can be reduced by suppression, but that suppression would not have an effect on a subjective experience of emotion. In the case of an attack on the Home assistant audio loop denial of service, a user could repeatedly try to activate the system by using voice commands, and experience inconvenience and annoyance with malfunction of the devices by using loud angry words which can further increase stress. Another person would not express their emotions, but that should not be taken as a sign that the person is not experiencing intensive unpleasant emotions.

6.4.5. E-SF: Subjective feeling

Subjective feeling refers to the subjective experience that characterises the emotion [127]. The situation of being a victim of a cyber attack presents a stressful event for victims who are likely to experience negative feelings such as anger, fear, sadness, insecurity and shame often accompanied with the feeling of surprise [124]. In a study on adolescents [135], it was found that those with greater Internet attachment were more likely to experience cyber victimisation and greater symptoms of anxiety and depression. With reliance on IoT devices in the home, it is important to take such results into account to develop strategies for decreasing negative impacts of attachment to IoT technology and possible emotional difficulties. In the case of hacking of baby monitors, parents experience an intensive fear for the privacy of their child, as well as fear

of potential abuse of the observed and recorded material. It will also lead to anger, which in turn can escalate into undesired actions.

6.5. Emotion regulation and coping

6.5.1. ERC-:Emotional Regulation

The most prevalent approach to emotion regulation emphasises reappraisal and suppression [136] as its two different styles. It includes re-evaluation of the situation with the goal of better coping with it, and it can modify an emotional impact. In the case of cyber attack in the household, a person can realise that impact of the attack is not significant, and choose to continue as it did not happen. The adaptive aspect of this style is that a person continues as there was no attack, while the maladaptive aspect can include repetition of the attack as a consequence of the lack of any activity to protect the household. Suppression includes inhibition of expression of the emotional process [136]. which can have beneficial impact by decreasing emotional expression and negative emotions, but can also stimulate ignorance of the real threats that would need attention to be prevented. Rumination is another emotion regulation style which includes repetitive and recurrent focus on the reasons for the situation that occurred [137].

After a cyber attack in one's smart home, emotions can maintain for a while as well as action tendencies that accompany them, so feeling of violation, shame, anxiety and anger can persist as well as desire for justice or revenge can occur [124]. Persistence of emotions related to the cyber attack could bring to behaviour that include changing IoT devices as a result of dissatisfaction with the protection [124].

6.5.2. ERC-:Actual behaviour

Actual behaviour depends on the context, emotional processes and emotional regulation. In order to know how a person actually behaves during and after a cyber attack in the smart home, one needs to know more about behaviour that is emotionally driven and more about accompanied emotional processes (appraisal of the event, action tendencies, bodily reactions, expression, and subjective feeling). The component process model offers [123, 138] an integrative theoretical frame to understand all phases of the emotional process and reactions, which are crucial to understand an emotional impact of cyber attack on users well-being.

7. Taxonomic classification examples

In this section, we provide an example of four hypothetical attack scenarios that are practically facilitated by a combination of insecure smart home devices, configurations and automation rules defined by household occupants. We then classify 24 different smart home cyber threats against the taxonomy criteria to identify shared characteristics between threats that help to identify key areas for developing defences.

For each attack, in Table 3 we provide an overview of taxonomy classification and in Figures 5, 6 and 7 taxonomic attack graphs. Here, an attack graph represents a time-based model of taxonomic classification for a smart home attack to establish interdependent attack characteristics and elicit key interactions between attack vectors and associated impact to help formulate approaches of potential defence. In Table 3, although we acknowledge that a becoming aware that one has been the victim of any of such attacks will elicit an emotional reaction, we provide a prediction as to which emotional components would be most strongly involved, for attacks that a victim are more likely to perceive as threatening. This distinction allows us to distinguish, for instance, attacks that would simply be annoying, e.g. powerline jamming, versus attacks that are more personal and would thus be more saliant, e.g. baby monitor back-door internet reconnaissance. Whereas the former would elicit cognitive evaluations and some kind of an emotional expression, the latter attack is likely to include much more visceral reactions.

In each attack graph, we also visually encapsulate specific classification criteria within three distinct areas of study (threat prevent, detection and cyber-physical crime victim support) to highlight attack characteristics which would provide meaningful information to researchers and developers of technical defences, as well as researchers and practitioners of behavioural, environmental and emotional psychology science. For example, in the case of the latter, analysing a specific attacks cyber-physical impact and associated affects on domestic life in the smart home can help to develop understanding and processes for supporting victims of these kind of attacks. Below we describe each area of study and provide indicative selection criteria within an attack graph:

1. **Threat prevention**. This is an approach to defence that relies on preemptive measures to mitigate threats. Examples include identifying and patching vulnerabilities in devices or software, enforcing multi-factor authentication, blocking system actions or responses that are potentially dangerous (this may include potentially danger user actions or automation rules that an occupant is attempting to configure). Typically, threat prevention relies on a robust understanding of the technical security of protocols, software and hardware devices deployed with a smart home and establishing rules and protections for secure inter-communication.
2. **Threat detection.** This is a pro-active control in defending against attacks, whereby a crucial component in identifying anomalous or known malicious activity pro-actively (for triggering threat prevention mechanisms) is the ability to collect and audit interactions between systems in the household (whether machine-to-machine, or machine-to-human). Here,

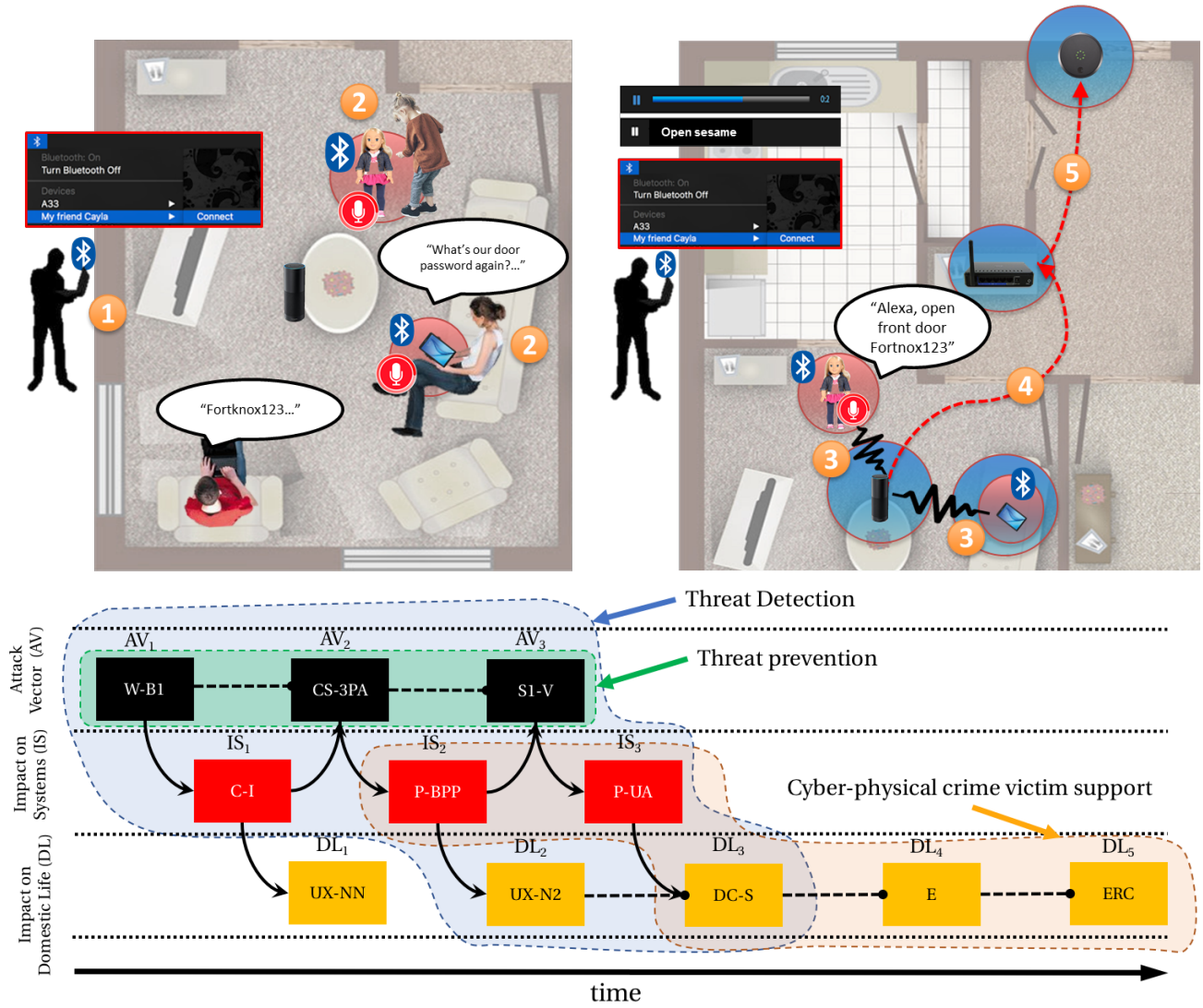

Figure 5: Example of household audio sniffing and injection attack and taxonomic attack graph of rogue voice-injection actuation (arrowhead lines indicate attack impact steps, dashed lines indicate second-order impact facilitated by a previous step in the same category, but not directly caused by it)

this relies on being able to measure and analyse the footprint generated by cyber-physical systems in a household for intrusion detection; whereby the aggregation of cyber and physical indicators can help establish measurable relationship between attack vectors and their associated impact [17].

3. **Cyber-physical crime victim support.** A successful cyber attack in the smart home can have a profound effect on domestic life, with direct consequences leading to financial loss, breaches of health and safety, as well as cascading emotional impact seriously impacting occupants physical and psychological well-being. Understanding how different kinds of cyber and physical impact in a smart home cyber attack affect domestic life, can help to inform the development of processes and systems for support of such victims.

7.1. Second-order threats to Smart homes: vulnerabilities in configuration and automation

Following on from the *Attack Vector* and *Impact on Systems* categories described in the previous section, here we demonstrate how the combination of different interacting technologies in the smart home can expose further second-order vulnerabilities which manifest as a consequence of automation and system configuration in the smart home.

Rogue voice-injection actuation

Here we demonstrate the viability of audio sniffing and injection as cyber threat through the *Cayla Doll* [72]. In Figure 5, an attacker with local proximity (e.g., 30 m depending on equipment) connects to the *Cayla Doll*'s open Bluetooth interface (1), activates the microphone function to record occupant conversations (2) (here a comparative

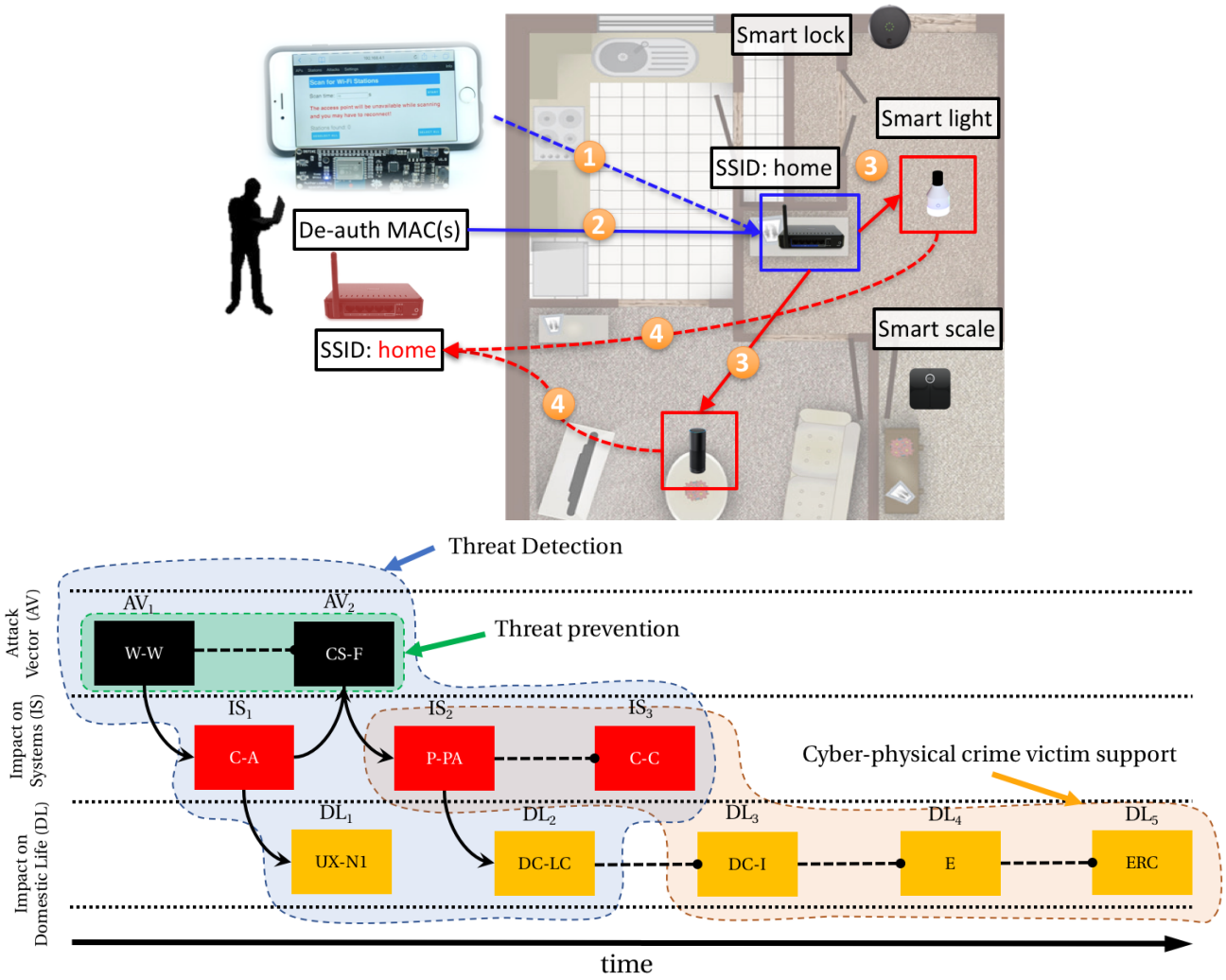

Figure 6: Example of household WiFi de-authentication attack on targeted WiFi endpoints and taxonomic attack graph of household WiFi de-authentication attack (arrowhead lines indicate attack impact steps, dashed lines indicate second-order impact facilitated by a previous step in the same category, but not directly caused by it)

approach would be to exploit a compromised Bluetooth enabled device such a smart phone or tablet the same attack vector exists (2)). The attacker plays a voice audio file through the *Cayla* doll (or Bluetooth smart device) speaker (3) which relays the command via a home automation hub (e.g., Amazon Echo), or directly to a voice-controlled actuation/sensing device (4) to execute actuation on a sensor - in this case unlocking a smart lock on the front door when the occupants are not in [107]. Today, most smart locks require a pin in order to perform locking and unlocking from audio or an app, however the remote audio access provided by the *Cayla Doll* this pin can recorded when it is used and replayed later to unlock the front door. Obviously, audio sniffing and rogue injection can be used to conduct a host activities (such as ordering equipment from Amazon via the Echo), however here it is the automation configuration within the household the facilities the attack end-to-end; requiring only a single vulnerable device (i.e., *Cayla Doll*) to compromise the otherwise secure systems (Echo, smart lock etc.). Figure 5 also shows the respective the attack graph taxonomy classification for rogue voice-injection attack.

WiFi de-authentication (with Evil-Twin)

Here, we describe the execution of a WiFi Evil Twin attack through de-authenticating a households WiFi devices. In Figure 5, an attacker with local proximity (e.g., 30 to 100 m depending on equipment) scans (1) for WiFi access points using a portable WiFi de-authentication device [29]. On selecting a target WiFi access point, (2) the attacker identifies connected WiFi nodes and targets specific MAC address to de-authenticate from the WiFi access point. On receiving de-authentication requests from the attacker for targeted endpoints MACs (3), the WiFi access point de-authenticates the endpoints from the WiFi network. At this stage, the attacker has launched a duplicate access point with a spoofed SSID and MAC address of the household WiFi at a greater signal-strength than

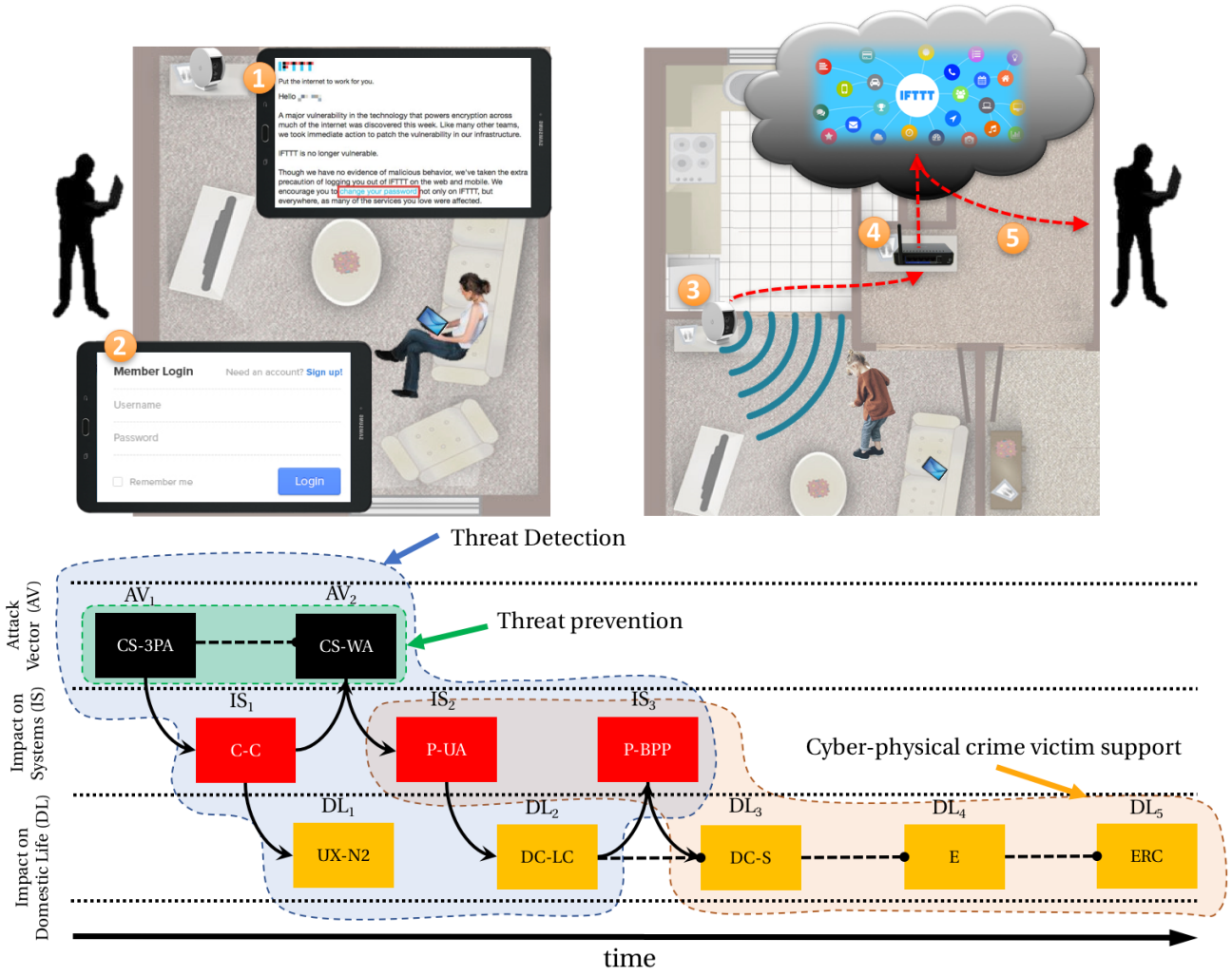

Figure 7: Example of workflow account phishing and injection of automation rules in compromised account and taxonomic attack graph of workflow account phishing and rule injection attack (arrowhead lines indicate attack impact steps, dashed lines indicate second-order impact facilitated by a previous step in the same category, but not directly caused by it)

the legitiamte household access point (4), where the de-authenticated endpoints configurations automatically re-connect, but this time to the attacker access point. On connection to the Evil Twin WiFi, the endpoints attempt to conduct a WPA 4-way handshake and inadvertently reveal the household WiFi password allowing the attacker to both sniff all the traffic of the connected endpoints, conduct denial of service against them, as well as access the household WiFi for further exploitation. An alternative, at stage 4, would be to prompt for a password to the Evil Twin WiFi access point where occupants would manually supply the household WiFi password [27]. Figure 6 also shows the respective attack graph taxonomy classification for the Evil Twin WiFi de-authentication attack.

Workflow automation phishing

In this attack, we show how a semantic social engineering attack [59] can be used to gain cyber-physical control of a smart home by utilising targeted phishing e-mails to capture household occupants credentials to worfklow automation platforms (note *IFTTT* is shown here as a hypothetical example, but crucially has been subject to related semantic attacks in 2014 [60]). Initially an attacker will craft a targeted e-mail to an occupant requesting them to reset their IFTTT credentials through a malicious URL (1), which subsequently leads the occupant to a spoofed login webpage for IFTTT (2), assuming the occupant is deceived and enters their credentials they are redirected to the legitimate website whilst at the same time supplying their IFTTT credentials to the attacker. The attacker now has access to the occupants account in which existing integration with household devices and system is available to the attacker to manipulate, in Figure 7 we assume that the household have integrated their internal video camera CCTV system (which also has motion detection capabilities). Using this particular scenario, the attacker is now free to add an existing trigger event to the camera system (3), which sends a picture from the camera to them on ac-

Table 3: Taxonomic classification of smart home cyber threats

Ref	Threat Description	Attack Vector (AV)	Impact on Systems (IS)		Impact on Domestic Life (DC)		
			Cyber	Physical	Direct Consequences	UX	Emotional
[13]	Power-line device jamming	CM-WD-X	C-A	P-PA	DC-LC, DC-I	UX-N1	E-A, E-AT, E-Exp
[97]	Thermostat embedded ransomware and root access	CS-3PA, CS-OS	C-A, C-NP	P-UA, P-PA	DC-F, DC-S, DC-LC, DC-I	UX-N1	E-A, E-AT, E-B, E-Ex, E-SF
[55]	Dishwasher web server directory traversal	CS-F	C-C, C-A	P-UA, P-IA	DC-F, DC-S, DC-LC, DC-I	UX-NN	-
[25]	Lightbulb to Lightbulb WiFi credentials sniffing	CS-WI-W	C-C	P-BPP	DC-F, DC-V DC-LC	UX-NN	-
[64]	Ultrasonic presence sensor spoofing	S1-U	C-I	P-IA	DC-S, DC-LC	UX-N1	E-A, E-AT, E-B, E-Ex, E-S
[90]	Baby monitor back-door Internet reconnaissance	CM-WI-W, CS-3PA	C-C	P-BPP	DC-S, DC-LC, DC-I, DC-P	UX-N2	E-A, E-AT, E-B, E-Ex, E-SF
[38]	BLE automated smart lock door opening	CM-WI-B, CS-3PA	C-I	P-IA	DC-F, DC-S, DC-LC	UX-N2	E-A, E-AT, E-B, E-Ex, E-SF
[70]	Spoofed voice activating smart lock	CM-WI-B, S1-V	C-I	P-UA	DC-F, DC-S, DC-LC	UX-N2	E-A, E-AT, E-B, E-Ex, E-SF
[72]	Doctored eDoll app apk	CS-3PA	C-I	P-IA	DC-F, DC-S, DC-LC	UX-N2	E-A, E-AT, E-B, E-Ex, E-SF
[83]	Side-channel power-line data sniffing	S1-EMI	C-I	P-BPP	DC-V,DC-S	UX-NN	-
[51]	Audio eavesdropping through smart hub controller	CS-3PA	C-I	C-BPP	DC-F, DC-V	UX-NN	-
[48]	Insteon node ID sniffing	CM-WD-I	C-C	P-BPP	DC-LC	UX-NN	-
[93]	Digital photo frame malware	CS-OS	C-I	P-UA	DC-F, DC-LC	UX-N2	E-A, E-AT, E-Exp
[92]	Smart home power generator tripping	CS-F	C-A	P-PA	DC-F,DC-V,DC-S, DC-I	UX-N1	E-A, E-AT, E-B, E-Ex, E-SF
[23]	Device data/sensor readings exfiltration	CM-WD-D, CS-3PA	C-C	P-BPP	DC-F, DC-S, DC-LC	UX-NN	-
[139]	Home assistant audio loop denial of service	S1-V	C-I	P-IA, P-UA	DC-LC, DC-I	UX-N1	E-A, E-AT, E-B, E-Ex, E-SF
[49]	Smart lock backdoor pin code injection	CS-3PA	C-I	P-IA	DC-F,DC-V,DC-S, DC-I	UX-NN	-
[96]	AWS S3 cloud-service outage denial of service	CS-3PA, CS-OS	C-A	P-IA, P-PA	DC-S, DC-LC, DC-I	UX-N1	E-A, E-AT, E-B, E-Ex, E-SF
[32]	ZigBee sinkhole attack	CM-WI-Z1	C-I	P-PA, P-DA, IA	DC-LC, DC-I	UX-N2	E-A, E-AT, E-Ex
[56]	Remote access for WeMo command and control	CM-WI-W	C-I, C-C	P-UA, P-PA	DC-F,DC-S, DC-LC	UX-N2	E-A, E-AT, E-Ex
[50]	Man-in-the-middle smart TV injection	CS-3PA	C-C, C-I,	P-BPP	DC-F, DC-I, DC-LC	UX-N1	E-A, E-AT, E-B, E-Ex, E-SF
[79]	Rogue payment via audio-triggered home assistant	S1-V	C-I	P-UA	DC-F, DC-LC	UX-N2	E-A, E-AT, E-B, E-Ex, E-SF
[19]	Rogue HomePlug AV network infiltration	CM-WD-H	C-C, C-I	P-BPP	DC-F,DC-LC,DC-S	UX-N2	E-A, E-AT, E-B, E-Ex, E-SF
[29]	WiFi device de-authentication	CM-WI-W, CS-F	C-A, C-I	P-PA	DC-LC, DC-I	UX-N1	E-A, E-AT, E-Ex
[60]	Workflow automation phishing	CS-3PA, CS-WA	C-A, C-C	P-PA	DC-LC, DC-I	UX-N1	E-A, E-AT, E-B, E-Ex, E-SF

tivation of the camera's motion sensor detection. Considering this breach of physical privacy in the household and the relative simplicity of executing this semantic attack to gain such access, the impact can be particular sinister. For example, in this household scenario, were the attacker aiming to capture indecent pictures of children, by accessing the camera system and adjusting the worfklow automation platform rules they are able to forward pictures which may capture activity of the child living in this household everytime the child activates the motion sensor. Figure 7 also shows the respective the attack graph taxonomy classification for a workflow automation phishing attack.

8. Defending against cyber-physical threats in the smart home

Security in the smart home is quickly becoming a complex and unique information security challenge in its own right. The emergence of pervasive and heterogeneous machine-to-machine and human-to-machine connectivity in the household forms a formidable threat landscape that combines actuators, sensors, computational, electronic and mechanical devices and humans. So, it is not only the adoption of vulnerable Internet-connected devices that places the smart home at risk, but also the cyber-physical fusion of previously isolated systems, where the effects of an attack in cyberspace (e.g., exploiting a smart home device's cloud service software) may now result to impact in physical space (e.g., turning on the cooker's gas stove) [65]. Although the concept of the smart home is still maturing, sophisticated attack vectors have already moved from the research lab environment to real-world deployment [99, 94], which means that it is now imperative that defenses are developed to protect against attack vectors that would undermine the uptake and practical benefits of smart home technology.

There are many facets of traditional cyber security that apply to the smart home, as well as elements of security which have much wider application. For example, at an IoT device level, chipset manufactures have proposed architectures [140, 141] and developed dedicated hardware security modules for secure boot and firmware integrity, authentication and update security [142], all of which are highly applicable to the security of devices in smart cities and industrial environments. However, in the context of the smart home, defence that relies on hardware modules dedicated to firmware device security can be impractical, as it is primarily a pre-emptive security control by nature, and typically required to be integrated in devices at the design and development stage, thus leaving many existing devices in the household without these components vulnerable to attack. Here, our focus is specifically on defences that have been designed for or evaluated specifically on smart homes.

As early as 2000, the concept of securing embedded smart home systems was first explored by Al-Muhtadi et al. [143], who introduced a prototype extension of the SESAME (Secure European System for Applications in a Multi-vendor Environment) security protocol [144]. Their adapted *Tiny SESAME* system utilised an embedded Java virtual machine module to perform the SESAME protocol's functions for authentication, authorisation, confidentiality, integrity and access services within resource constrained smart home devices. The researchers presented an experimental deployment within a smart home testbed consisting of *Tiny SESAME* equipped toaster, door, videocassette recorder, alarm system and fridge. However, no actual attacks on the security platform were evaluated to demonstrate its empirical utility.

Naturally, early research on the security of smart homes relates to authentication and authorisation. A simple approach implemented by Qutayri et al. [145] in 2008 re-

quires the user to enter a username and a password, which is sent via SMS to a home server that establishes the authenticity of the user against a database. Then, the home server initiates a session including the phone number that sent the SMS and a randomly generated number which expires after the session ends. The users are assigned access levels based on their role (e.g., a supervisor can setup accounts for other users), and there is also provision for encryption of the communication between the mobile station and the home server. The same year, Jeong et al. [146] explored the idea of using low-cost smartcards for authentication, focusing particularly on the challenges posed by smart home devices' resource restrictions. What they proposed was a lightweight scheme based on a one-time password protocol and simple operations using one-way hash functions, so as to incur very low computation load. The protocol assumes that a symmetric key is shared between a home gateway server and an integrated authentication server, which sits outside the home network, is trusted by the users and performs authentication, authorisation and accounting. Users are authenticated through single-sign-on and can access other home services without additional authentication procedures. The protocol was analysed only theoretically and rather briefly for replay, man-in-the-middle, denial of service and stolen-verifier attacks, and there was no practical implementation or experimental evaluation of its practicality.

Chifor et al. [147] have introduced a lightweight identity stack providing a digital identity to the users and the individual devices. Its purpose is to be integrated in existing operating systems or smart home IoT frameworks. The application scenario is on a smart home device which is connected to an untrusted Cloud platform and relays input commands to a users smartphone for authorisation. Their work extends the authentication messages of the passwordless "Fast IDentity Online" (FIDO) mode, which was originally designed for smartphones. Some degree of theft resistance is achieved by adding a keep-alive mechanism. The authors ensured that their approach is practical from a network delay perspective by implementing and evaluating it on the open-source Kaa IoT Cloud platform. The delay added for 30 nodes was around 150-200 ms, which should be acceptable for most smart home applications. However, this value did not take into account the time taken by the cryptographic operations running on the devices, as this part of their evaluation was simulated on a desktop device.

Much less lightweight but certainly attractive is the direction of utilising Blockchain technologies to decentralise security measures. While generally very challenging in terms of computational overhead, energy consumption and network delays, it has been shown by [148] et al. that a lightweight instantiation eliminating the concepts of coins and of Proof of Work can be practical in a smart home. In their proposed system, each smart home is equipped with a "miner" device, which is both powerful and always online, and is responsible for handling all communication within and external to the home. The miner also preserves a private blockchain, which controls and audits communications. Evaluated in simulation, their system appears to introduce only minimal overhead in terms of traffic, processing time and energy consumption. Along similar lines, the European project GHOST [149] proposes a defence infrastructure where it is the integrity of the code running on smart home gateways that is certified by the use of Blockchain technology. However, this work has not yet been evaluated experimentally.

Rahmati et al. [150] have observed that emerging smart home platforms use permission models, which, inspired by smartphone operating systems, group functionally similar device operations into separate units and require users to grant apps access to devices at that granularity. This leads to overprivileged access for apps that do not require access to all of the granted device operations, and higher risk to users than needed because physical device operations are risk-asymmetric. For instance, from their example, "door.unlock" provides access to burglars, while "door.lock" may lead to getting locked out. So, the authors have argued that the combination of overprivileged apps and mixed-risk operations increases the damage potential. Their solution is to move away from grouping based on functional similarity to grouping based on risk similarity. Their proposed scheme, Tyche, uses app rewriting techniques to enforce risk-based permissions. Through a survey of 400 users, they measured risk perceptions for different types of smart home cyber threats that could be caused by overprivilege. Based on their findings, they grouped a physical devices operations into three groups of risk (low, medium, high), for 146 operations across 61 types of devices. Evaluating this new model on three existing SmartApps, they found that these apps can be written in a way that reduces access to high-risk operations by 60% without decreasing functionality or increasing user decision overhead.

Beyond preventative measures, such as authentication and authorisation, researchers have also worked on security monitoring, verification, detection, countermeasure decision support and other more active security measures. For example, assuming a software defined network (SDN) underlying the infrastructure for a smart home, Wang et al. [151] have proposed a model whereby Android programs perform dynamic taint propagation to analyse the spread of risks posed by suspicious apps connected to a smart home's gateway. For each taint path, probabilistic risk analysis assists the defender in recognising network threats caused by malware infection and to estimate the losses of associated taint sources. They incorporated a finite state machine to represent the taint propagation analysis situations at various configuration settings and deployments of safeguards. Their experimental evaluation was performed on a smart home setup involving a smart home gateway, a SDN controller, and OpenFlow switch and a wireless access point. Using behavioural analysis associated with 60 families of real malware, they showed

that the approach is promising, especially as the number of taint paths associated with the propagation rules discovered through taint analysis is increased.

In the wider sphere of information security, there is currently a distinct lack of digital forensics methodologies for IoT and cyber-physical systems. Some initial work has been carried out by Do et al. [152] on smart home information gathering for the purposes of digital forensics. A first model is evaluated on the forensic examination of LIFX smart lights and a Belkin WEMO switch, starting from a passive forensic adversary constrained by the strict principles of forensic soundness and comparing against stronger adversaries with reduced constraints. While generalisation beyond these devices is risky, an interesting observation is that even the passive forensic adversary can obtain significant evidential data, such as determining the identities and locations of devices.

In the commercial space, traditional anti-virus vendors have entered the emerging smart home security market by adapting the concept of traditional unified threat management gatewaysm commonly deployed within enterprise networks, for smart home networks. Platforms developed by Norton [119], F-Secure [153], McAfee [154], BitDefender [153], Dojo [155] and Cujo [156] seemlessly integrate into household networks by either replacing an existing home WiFi router or by assuming the role of its network gateway to the Internet. Each vendor security platform are very similar in design to each other and employ conceptually the same security architecture and protection mechanisms. For example, in order to provide access to high-end threat detection capabilities (historically reserved to enterprise security systems) via a resource-constrained home router, network and device data is collected by each platform locally and then sent to vendor cloud infrastructure where the smart home data is processed by proprietary threat detection analytics using machine learning and heuristics algorithms to establish attack signatures. This architecture allows for efficient crowd-sourcing of threat detection which is shared between all smart home subscribers of the security platform (as per the approach taken by modern anti-virus software). It is here where a wide array of security services such as anti-malware/virus protection, parental access control, secure DNS services, deep packet inspection, intrusion detection and prevention functionality, authentication and authorisation policy, as well as user security incident reporting and system configuration dashboards are provided; the latter in the form of an online or mobile user application.

Whilst the concept of offloading resource intensive threat detection to the cloud certainly provides an economical and practical means to provider high-end security services in the household, it remains unclear how such systems can respond dynamically and autonomously to cyber-physical threats in real-time; especially as access to the advanced threat detection capabilities of the vendor cloud system is subject to end-to-end network delay and Internet availability. Current commercial smart home security platforms focus almost entirely on IP network and device traffic analysis, which constitutes only a small portion of the potential connectivity landscape in the smart home. As shown in section 1, smart home attacks vectors can manifest over a vast set of different communication mediums, control systems and sensory channels, that so far have received little attention from a security monitoring perspective. Therefore, in practice, sole reliance on traditional IP network analysis for capturing the full remit of existing and future potential cyber threats in the household is no longer sufficient.

9. Open research challenges

9.1. Smart home living labs for cyber security research

Experimentation in IoT is progressing well across the research community, but usually at the level of individual devices, especially when users are involved. However, there is much less progress in developing smart home living labs, so as to be able to evaluate different threats, their impact and the effectiveness and appropriateness of corresponding countermeasures in the real conditions of living in a household. This would allow to study the second order effects of different attacks and exploitation of interdependencies and unwanted interactions between systems, such as the "rogue voice-injection actuation" example presented in Section 7.1. It would also allow to study the human-system interaction considerations of smart home cyber security, and the additional challenge introduced by the potentially different preferences and cyber security attitudes of the different members of a household.

9.2. Cyber-physical intrusion detection for smart homes

Similarly to cyber-physical systems [17, 157], intrusion detection not only can benefit from but may even necessitate the use of data sources from physical space, in addition to network and processing data. For example, attacks that exploit the audio link between devices (such as the speaker of a babycam issuing a voice activation command) cannot be detected by monitoring only network traffic, as in conventional network environments. Similarly, information from physical sensors (such as occupancy sensors) on the absence of occupants a home at a specific point in time can be valuable information for the detection of command injection attacks.

9.3. Privacy metrics for smart homes

The vast majority of IoT technologies employ a cloud approach, even if not strictly necessary for technical reasons. For example, a simple on/off actuation command for a smart lightbulb could be delivered directly from the user's smartphone to the smart lights hub and to the light bulb. Instead, most manufacturers involve transmission of this information to their cloud, which raises privacy concerns. At the same time, the presence or not of people in a smart home can be inferred through the level of wireless

network activity (e.g., of ZigBee traffic). IoT privacy is currently a vibrant area of research, looking at IoT systems usually in isolation. In the context of a smart home, an interesting research question is whether it is possible to define smart home privacy metrics (i.e., how much privacy is offered by a smart home of a given configuration?).

9.4. Support for smart home security breach victims

While for physical crime, societies have created a range of support systems for the victims, there is no equivalent provision for cyber crime. For victims of cyber attacks in smart homes, where there may be physical damage caused and the emotional impact can be profound, there is perhaps greater need for establishing frameworks for recovering from the cyber and physical damage caused, and also for designing counselling to be provided to the occupants affected. As we have shown in section 7, here the taxonomy attack graphs can help to guide investigations for different smart home attacks (to highlight key attack behaviours) in order to aid understanding of their impact on victims.

9.5. Smart home cyber hygiene and Human-as-a-Security-Sensor

A common approach towards prevention of cyber threats is to improve the security posture of individuals and organisations by developing guidance and advice for implementing basic security measures (e.g., keeping software updated, using multi-factor authentication online, choosing complex passwords etc.). However, existing "cyber hygiene" recommendations are likely to cover only a small portion of the smart home threat landscape, especially as many attack vectors manifest as a result of cyber-physical connectivity. We anticipate that new smart home cyber hygiene efforts leading to the definition of simple, best-practice techniques for IoT systems in the household will lead to improved prevention and detection efficacy against cyber-physical threats by equipping users with the efficacy to detect potential threats to the household through a core set of recommendations (e.g., that it probably is not good security practice to connect one's cooker to the cloud via their WiFi network if it cannot be turned off when the service is unavailable [96]). Linked to this is the Human-as-a-Security-Sensor (HaaSS) paradigm of actively involving users as human sensors. The concept has already been proven for conventional desktop systems [158], but in the space-constrained interface of smartphones and embedded systems within smart homes environments, the user is afforded a lot less information or time to spot suspicious activity and the potential impact of threats can introduce physical and emotional consequences which influence user decision making processes. Development of mechanisms for HaaSS reporting, as well as measuring the reliability of these reports can facilitate integration within a technical smart home security platform. User telemetry helps influence the decision making and response of defence systems, but also augments threat detection performance through human sensing of context, which a technical system would not have access to. Furthermore, by integrating the user as part of the defence, second-order benefits may be realised, such as conditioning the emotional state of users when exposed to the impact of an attack or the nurturing of proactive coping strategies to tune user response in a way that supports defense.

9.6. The cyber security economics of smart homes

The introduction of cyber security in smart homes naturally comes with increased financial costs for the manufacturers and buyers, but also carries an economic value in terms of the assets and wellbeing of occupants that it contributes in protecting. Related concepts, such as security pricing, security investment [159] and cyber insurance [160] at the level of organisations and enterprise network environments, are being investigated, but there is no equivalent work for smart homes. Of particular interest is the concept of smart home cyber insurance, which can complement traditional home insurance.

10. Conclusions

A first hurdle in carrying out research on the security of smart homes is to identify the mechanisms for launching attacks against them and their potential impact. We have conducted a survey of cyber threats in a smart home environment and produced a taxonomy to categorise these threats systematically, considering the attack vectors, as well as the impact on systems and consequently on the occupants of a smart home. Taking into consideration the different characteristics of these attacks, we have also identified where existing technical defences practical to household users are applicable to address such threats. In doing so, we have aimed to help establish the problem space, allowing researchers from a variety of disciplines to identify areas where they can contribute, and specifically for cyber-physical and IoT security researchers to pick attacks and systems for evaluating their technologies.

Acknowledgment

This work has been funded by the European Coordinated Research on Long-term Challenges in Information and Communication Sciences and Technologies ERA-NET (CHIST-ERA), under project COCOON, EPSRC grant number EP/P016448/1.

References

[1] N. Komninos, E. Philippou, and A. Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4): 1933–1954, 2014.

[2] H. Lin and N. W. Bergmann. Iot privacy and security challenges for smart home environments. *Information*, 7(3):44, 2016.

[3] Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the internet of things (iot). *Recent Trends in Network Security and Applications*, pages 420–429, 2010.

[4] Qi Jing, Athanasios V Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. Security of the internet of things: Perspectives and challenges. *Wireless Networks*, 20(8):2481–2501, 2014.

[5] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7(12):2728–2742, 2014.

[6] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, and Ong Bi Lynn. Internet of things (iot): Taxonomy of security attacks. In *Electronic Design (ICED), 2016 3rd International Conference on*, pages 321–326. IEEE, 2016.

[7] Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, 23(5):10–16, 2016.

[8] A Oulasvirta, A. Pihlajamaa, J. Perki, D. Ray, T. Vhkangas, T. Hasu, N. Vainio, and P. Myllymki. Long-term effects of ubiquitous surveillance in the home. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 40–50. ACM, 2012.

[9] Amir Rahmati, Earlence Fernandes, Kevin Eykholt, and Atul Prakash. Tyche: Risk-based permissions for smart home platforms. *arXiv preprint arXiv:1801.04609*, 2018.

[10] P.N. Dawadi, D.J. Cook, M. Schmitter-Edgecombe, and C. Parsey. Automated assessment of cognitive health using smart home technologies. *Technology and health care*, 21(4): 323–343, 2013.

[11] T.Y. Chung, I. Mashal, O. Alsaryrah, T.H. Hsu, C.H. Chang, and W.H. Kuo. Design and implementation of light-weight smart home gateway for social web of thing. In *Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on*, pages 425–430. IEEE, 2014.

[12] Sid Stamm, Zulfikar Ramzan, and Markus Jakobsson. Drive-by pharming. In *International Conference on Information and Communications Security*, pages 495–506. Springer, Berlin, Heidelberg, 2006.

[13] D Kennedy and R Simon. Pentesting over power lines. 2011.

[14] A. Antonini, F. Maggi, and S. Zanero. A practical attack against a knx-based building automation system. In *Proceedings of the 2nd International Symposium on ICS and SCADA Cyber Security Research 2014*, pages 53–60. BCS, 2014.

[15] HAPCAN. HAPCAN: about project - basic information, 2017. URL `http://hapcan.com/project/basis/`.

[16] Subhojeet Mukherjee, Hossein Shirazi, Indrakshi Ray, Jeremy Daily, and Rose Gamble. Practical dos attacks on embedded networks in commercial vehicles. In *Information Systems Security*, pages 23–42. Springer, 2016.

[17] Anatolij Bezemskij, George Loukas, Richard J Anthony, Diane Gan, et al. Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle. 2016.

[18] J. Vanderauwera A. Puppe. Research project: Homeplug security, 2010. URL `http://www.delaat.net/rp/2009-2010/p19/report.pdf0`.

[19] B. Tasker. Vulnerability: Infiltrating a network via powerline (HomePlugAV) adapters, 2014. URL `https://www.bentasker.co.uk/documentation/security/282-infiltrating-a-network-via-powerline-homeplugav-adapters`.

[20] S. Dudek. HomePlugAV PLC: practical attacks and backdooring, 2015. URL `http://www.synacktiv.com/ressources/NSC2014-HomePlugAV_attacks-Sebastien_Dudek.pdf`.

[21] Echelon Corporation. 90 million energy-aware lonworks devices worldwide, 2010. URL `http://www.businesswire.com/news/home/20100412005544/en/90-Million-Energy-Aware-LonWorks-Devices-Worldwide(2010)`.

[22] Philipp Jovanovic and Samuel Neves. Practical cryptanalysis of the open smart grid protocol. In *International Workshop on Fast Software Encryption*, pages 297–316. Springer, Berlin, Heidelberg, 2015.

[23] A. Brauchli and D. Li. A solution based analysis of attack vectors on smart home systems. In *Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on*, pages 1–6. IEEE, 2015.

[24] digitalStrom. digitalstrom basic concepts. Technical report, 08 2015. URL `http://developer.digitalstrom.org/Architecture/ds-basics.pdf`.

[25] Wakefield, Jane. Smart LED light bulbs leak wi-fi passwords, 2014. URL `http://www.bbc.co.uk/news/technology-28208905`.

[26] A. Chapman. Hacking into internet connected light bulbs, 2014. URL `https://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs/`.

[27] G. Chatzisofroniou. Getting the most out of evil twin, 2016. URL `https://census-labs.com/media/bsidesath2016-wifiphisher.pdf`.

[28] spacehuhn. Esp8266 deauther - github project, 2017. URL `ESP8266Deauther`.

[29] D. Kitchen and S. Kinne. The wifi pineapple wireless auditing platform, 2017. URL `https://www.wifipineapple.com/`.

[30] Mathy Vanhoef and Frank Piessens. Key reinstallation attacks: Forcing nonce reuse in wpa2. In *Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS)*. ACM, 2017.

[31] WiFi Alliance. Discover wi-fi - security, 2019. URL `https://www.wi-fi.org/discover-wi-fi/security`.

[32] L. Coppolino, V. DAlessandro, S. DAntonio, L. Levy, and L. Omano. My smart home is under attack. In *Computational Science and Engineering (CSE), 2015 IEEE 18th International Conference on*, pages 141–151. IEEE, 2015.

[33] Joshua Wright. Killerbee: practical zigbee exploitation framework. In *11th ToorCon conference, San Diego*, 2009.

[34] I. R. Jenkins, R. Shapiro, S. Bratus, T. Goodspeed, R. Speers, and D. Dowd. Short paper: speaking the local dialect: exploiting differences between ieee 802.15. 4 receivers with commodity radios for fingerprinting, targeted attacks, and wids evasion. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless and mobile networks*, pages 63–68. ACM, 2014.

[35] Badenhop, C. and Ramsey, B. Carols of the z-wave security layer; or, robbing keys from peter to unlock paul, 2016. URL `http://openwall.info/wiki/_media/people/solar/pocorgtfo12.pdf`.

[36] J. Hall and B. Ramsey. Tools for evaluating and exploiting z-wave networks using software-defined radios, 2018. URL `https://github.com/cureHsu/EZ-Wave`.

[37] Ms. Smith. Ez-wave: A z-wave hacking tool capable of breaking bulbs, abusing z-wave devices, 2018. URL `https://www.csoonline.com/article/3024217/security/ez-wave-z-wave-hacking-tool-capable-of-breaking-bulbs-and-abusing-z-wave-devices.html`.

[38] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, pages 461–472. ACM, 2016.

[39] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *In proceedings of the 18th Annual Network and Distributed System Security Symposium*. The Internet Society, 2011.

[40] Hongwei Du. Nfc technology: Today and tomorrow. *International Journal of Future Computer and Communication*, 2(4): 351, 2013.

[41] Todd Kennedy and Ray Hunt. A review of wpan security: attacks and prevention. In *Proceedings of the international conference on mobile technology, applications, and systems*, page 56. ACM, 2008.

[42] Ernst Haselsteiner and Klemens Breitfuß. Security in near field

communication (nfc). In *Workshop on RFID security*, pages 12–14, 2006.

[43] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Potential misuse of nfc enabled mobile phones with embedded security elements as contactless attack platforms. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pages 1–8. IEEE, 2009.

[44] Keith E Mayes, Konstantinos Markantonakis, Lishoy Francis, and GP Hancke. Nfc security threats. *Smart Card Technology International Magazine*, pages 42–47, 2010.

[45] Sathya Laufer and Christian Mallas. *Attacking HomeMatic*. Dec 2013. URL `https://media.ccc.de/v/30C3_-_5444_-_en_-_saal_g_-_201312301600_-_attacking_homematic_-_sathya_-_malli#video&t=84`.

[46] Suela Kodra. Smart home hacking. Master's thesis, NTNU, 2016.

[47] Alexander Frimmel, Aimen Tawfik, Hermann Wagner, and Michael Zach. *Projektarbeit "Secure Smart Home"*. Jan 2016. URL `https://leanstartupsecurity.com/wp-content/uploads/2017/01/Projektarbeit_Secure_SmartHome_Dokumentation_v1.2_20150628.pdf`.

[48] Peter Shipley. Insteon: False security and deceptive, 2015. URL `https://www.youtube.com/watch?v=dy1LTQLmPtM`.

[49] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. Security analysis of emerging smart home applications. In *IEEE Symposium on Security and Privacy (SP)*, pages 636–654. IEEE, 2016.

[50] D. Jacoby. How i hacked my home, 2014. URL `https://blog.kaspersky.com/how-i-hacked-my-home/5756/`.

[51] Sachchidanand Singh and Nirmala Singh. Internet of things (iot): Security challenges, business opportunities & reference architecture for e-commerce. In *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pages 1577–1581. IEEE, 2015.

[52] A. Drozhzhin. Tizen os: 40 new vulnerabilities, 2017. URL `https://blog.kaspersky.com/tizen-40-bugs/14525/`.

[53] P. Bright. Samsungs tizen is riddled with security flaws, amateurishly written, 2017. URL `https://arstechnica.co.uk/gadgets/2017/04/samsungs-tizen-is-riddled-with-security-flaws-amateurishly-written/`.

[54] Behrang Fouladi and Sahand Ghanoun. Security evaluation of the z-wave wireless protocol. In *Black Hat USA*. Black Hat, 2013.

[55] MITRE. Cve-2017-7240. Technical report, 2017. URL `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7240`.

[56] CERT. Vulnerability note vu 656302, 2014. URL `http://www.kb.cert.org/vuls/id/656302`.

[57] Dan Goodwin. How a hacked amazon echo could secretly capture your most intimate moments, 2017. URL `https://arstechnica.co.uk/information-technology/2017/08/how-hackers-could-turn-an-amazon-echo-into-a-secret-bugging-device/`.

[58] Resno. Welcome to the exploitee.rs wiki, 2017. URL `https://www.exploitee.rs/`.

[59] R. Heartfield and G. Loukas. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3):37, 2016.

[60] G. Cluley. In the wake of heartbleed, watch out for phishing attacks, disguised as password reset emails, 2014. URL `https://hotforsecurity.bitdefender.com/blog/in-the-wake-of-heartbleed-watch-out-for-phishing-attacks-disguised-as-password-reset-emails-8372.html`.

[61] Elliptic Labs. Elliptic labs introduces ultrasonic presence detection technology, inner peace, for intelligent personal assistants and other home devices, Feb 2017. URL `http://www.ellipticlabs.com/2017/02/28/elliptic-labs-introduces-ultrasonic-presence-detection-technology-inner-peace-for-intelligent-personal-assistants-and-other-home-devices/`.

[62] Jian Li, Guangjie Han, Chunsheng Zhu, and Guiqing Sun. An indoor ultrasonic positioning system based on toa for internet of things. *Mobile Information Systems*, 2016, 2016.

[63] Sahar Sedighpour, Srdjan Čapkun, Saurabh Ganeriwal, and Mani Srivastava. Distance enlargement and reduction attacks on ultrasound ranging. In *Proceedings of the 3rd international conference on Embedded networked sensor systems*, pages 312–312. ACM, 2005.

[64] Kahraman D Akdemir, Deniz Karakoyunlu, Taskin Padir, and Berk Sunar. An emerging threat: eve meets a robot. In *International Conference on Trusted Systems*, pages 271–289. Springer, 2010.

[65] George Loukas. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann, 2015.

[66] Guoming Zhang, Chen Yan, Xiaoyu Ji, Taimin Zhang, Tianchen Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. *arXiv preprint arXiv:1708.09537*, 2017.

[67] Wenrui Diao, Xiangyu Liu, Zhe Zhou, and Kehuan Zhang. Your voice assistant is mine: How to abuse speakers to steal information and control your phone. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, pages 63–74. ACM, 2014.

[68] Engadget. Burger king wreaks havoc on google assistant with whopper ad (update), 2017. URL `https://www.engadget.com/2017/04/12/burger-king-wreaks-havoc-on-google-assistant-with-whopper-ad/`. [Online; accessed 30-June-2017].

[69] K. Morsley. Amazon echo rogue payment warning after tv show causes 'alexa' to order dolls houses, 2017. URL `http://www.telegraph.co.uk/news/2017/01/08/amazon-echo-rogue-payment-warning-tv-show-causes-alexa-order/`.

[70] BBC Technology. How hackers could use doll to open your front door, 2016. URL `http://www.bbc.co.uk/news/technology-38966285`.

[71] Tim Medim. Doll hacking: The good, the bad(words) and the ugly (features), 2015. URL `http://blog.threat.actor/2015/11/doll-hacking-good-badwords-and-ugly.html`.

[72] Pentest Partners. New, easier ways to make my friend cayla swear, 2016. URL `https://www.pentestpartners.com/blog/new-easier-ways-to-make-my-friend-cayla-swear/`.

[73] Checkmarx. Amazon echo: Alexa leveraged as a silent eavesdropper. Technical report, 10 2018. URL `https://info.checkmarx.com/wp-alexa`.

[74] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, and W. Zhou. Hidden voice commands. In *USENIX Security Symposium*, pages 513–530. USENIX, 2016.

[75] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. This aint your dose: Sensor spoofing attack on medical infusion pump. In *10th USENIX Workshop on Offensive Technologies*. USENIX, 2016.

[76] Dima Bykhovsky Guri, Mordechai and Yuval Elovici. air-jumper: Covert air-gap exfiltration/infiltration via security cameras and infrared (ir). *arXiv preprint arXiv:1709.05742*, pages 1–15, 2017.

[77] CERT-UK. Cyber-security risks in the supply chain, 2015. URL `https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf`.

[78] Proofpoint. Droidjack uses side-loadit's super effective! backdoored pokemon go android app found, 2016. URL `https://www.proofpoint.com/us/threat-insight/post/droidjack-uses-side-load-backdoored-pokemon-go-android-app`.

[79] Katie Morley. Amazon echo rogue payment warning after tv show causes alexa to order dolls houses, 2017. URL `http://www.telegraph.co.uk/news/2017/01/08/amazon-echo-rogue-payment-warning-tv-show-causes-alexa-order/`.

[80] Miller, F. John. Supply Chain Attack Framework and Attack Patterns, 2013. URL `https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Cyber-security-risks-in-the-supply-chain.pdf`.

[81] Dmitry Evtyushkin and Dmitry Ponomarev. Covert channels

through random number generator: Mechanisms, capacity estimation and mitigations. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 843–857. ACM, 2016.

[82] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. *arXiv preprint arXiv:1606.05915*, 2016.

[83] M. Enev, S. Gupta, T. Kohno, and S. N. Patel. Televisions, video privacy, and powerline electromagnetic interference. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 537–550. ACM, 2011.

[84] F. Sabath. What can be learned from documented intentional electromagnetic interference (iemi) attacks? In *General Assembly and Scientific Symposium, 2011 XXXth URSI*, pages 1–4. IEEE, 2011.

[85] F. Sabath. Threat of electromagnetic terrorism. In *EUROEM 2012 Book of Abstracts*, 2012.

[86] Denis Foo Kune, John Backes, Shane Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating emi signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*, pages 145–159. IEEE, 2013.

[87] NA Moreham. Beyond information: physical privacy in english law. *The Cambridge Law Journal*, 73(2):350–377, 2014.

[88] Isaac Ghansah. Smart grid cyber security potential threats, vulnerabilities and risks. *California Energy Commission, PIER Energy-Related Environmental Research Program, CEC-500-2012-047*, 2009.

[89] The Mirror. Wake up baby: Man hacks into 10-month-old's baby monitor to watch sleeping infant, 2014. URL `http://www.mirror.co.uk/news/world-news/man-hacks-10-month-olds-baby-monitor-3468827`.

[90] K. Albrecht and L. Mcintyre. Privacy nightmare: When baby monitors go bad. *Privacy Nightmare: When Baby Monitors Go Bad [Opinion]. IEEE Technology and Society Magazine*, 34(3):14–19, 2015.

[91] The Independent. Baby monitors 'hacked': Parents warned to be vigilant after voices heard coming from speakers, 2016. URL `http://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked-parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html`.

[92] Y. Liu, S. Hu, and A. Y Zomaya. The hierarchical smart home cyberattack detection considering power overloading and frequency disturbance. *IEEE Transactions on Industrial Informatics*, 12(5):1973–1983, 2016.

[93] Tarala, Kelli K. Dangers of digital photo frames, 2009. URL `http://www.enclavesecurity.com/dangers-of-digital-photo-frames/`.

[94] Proofpoint. Your fridge is full of spam, part ii: Details, 2014. URL `https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM-Part-2`.

[95] Paria Jokar, Hasen Nicanfar, and Victor CM Leung. Specification-based intrusion detection for home area networks in smart grids. In *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 208–213. IEEE, 2011.

[96] Rand Hindi. Thanks for breaking our connected homes, amazon, 2017. URL `https://medium.com/snips-ai/thanks-for-breaking-our-connected-homes-amazon-c820a8849021`.

[97] Pentest Partners. Thermostat ransomware: a lesson in iot security, 2016. URL `https://www.pentestpartners.com/blog/thermostat-ransomware-a-lesson-in-iot-security/`.

[98] Exploiteers. Lg smart refrigerator (lfx31995st), 2017. URL `https://www.exploitee.rs/index.php/LG_Smart_Refrigerator_(LFX31995ST)\%E2\%80\%8B`.

[99] Proofpoint. Proofpoint uncovers internet of things (iot) cyberattack, 2014. URL `http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799`.

[100] Rosslin John Robles, Tai-hoon Kim, D Cook, and S Das. A review on security in smart home development. *International Journal of Advanced Science and Technology*, 15, 2010.

[101] P. Leijdekkers, V. Gay, and E Lawrence. Smart homecare system for health tele-monitoring. In *Digital Society, 2007. ICDS'07. First International Conference on*, pages 3–3. IEEE, 2007.

[102] George Demiris and Brian K. Hensel. Technologies for an aging society: a systematic review of "smart home" applications. *Yearbook of medical informatics International Medical Informatics Association*, 3:33–40, 2008.

[103] M. C. Domingo. An overview of the internet of things for people with disabilities. *Journal of Network and Computer Applications*, 35(2):584–596, 2012. URL `https://www.cutter.com/article/social-engineering-internet-everything-492251`.

[104] Marco Jahn, Marc Jentsch, Christian R Prause, Ferry Pramudianto, Amro Al-Akkad, and Rene Reiners. The energy aware smart home. In *2010 5th International Conference on Future Information Technology (FutureTech)*, pages 1–8. IEEE, 2010.

[105] Digital Guardian. A history of ransomware attacks: The biggest and worst ransomware attacks of all time, 2017. URL `https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time`.

[106] International Risk Governing Center. Governing cybersecurity risks and benefits of the internet of things: Connected medical and health devices and connected vehicles. In *IRGC Expert Workshop Swiss Re CGD 15 - 16 November*, 2016.

[107] D. B. Lombardi and M. R. Ciceri. More than defense in daily experience of privacy: The functions of privacy in digital and physical environments. *Europe's journal of psychology*, 12(1): 115, 2016.

[108] Ram N. Infurna, F. J. and D. Gerstorf. Level and change in perceived control predict 19-year mortality: Findings from the americans changing lives study. *Developmental Psychology*, 49 (10):1833, 2013.

[109] F. E. Owusu-Ansah. Control perceptions and control appraisal: Relation to measures of subjective well-being. *Ghana medical journal*, 42(2), 2008.

[110] Office for national statistics. Record proportion of people in employment are home workers, 2014. URL `http://webarchive.nationalarchives.gov.uk/20160105210705/http://www.ons.gov.uk/ons/rel/lmac/characteristics-of-home-workers/2014/sty-home-workers.html`.

[111] J. Boitnott. Are smart homes distracting your employees?, 2016. URL `http://www.digitalistmag.com/digital-economy/2017/05/11/big-data-problem-with-machine-learning-05084700`.

[112] Temitope Oluwafemi, Tadayoshi Kohno, Sidhant Gupta, and Shwetak Patel. Experimental security analyses of non-networked compact fluorescent lamps: A case study of home automation security. In *LASER*, pages 13–24, 2013.

[113] K. Poulsen. Hackers assault epilepsy patients via computer, 2008.

[114] Kang, Cecilia. A Tweet to Kurt Eichenwald, a Strobe and a Seizure. Now, an Arrest, 2017. URL `https://www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html?\_r=0`.

[115] Samsung. Slide-in gas flex duo range with dual door, 2017. URL `http://www.samsung.com/us/home-appliances/ranges/slide-in/nx58k9850ss-slide-in-gas-flex-duo-range-with-dual-door-stainless-steel-nx58k9850ss-aa/`.

[116] Darhl M Pedersen. Model for types of privacy by privacy functions. *Journal of environmental psychology*, 19(4):397–405, 1999.

[117] N. J. Marshall. Privacy and environment. *Human ecology*, 1 (2):93–110, 1972.

[118] P. Jokar and V. Leung. Intrusion detection and prevention for zigbee-based home area networks in smart grids. *IEEE Transactions on Smart Grid*, 99(1), 2016.

[119] Symantec. Introducing norton core, 2017. URL https://us.norton.com/core.

[120] L. Franceeschi-Bicchierai. Internet of things teddy bear leaked 2 million parent and kids message recordings, 2017. URL https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings.

[121] Pentest Partners. Vulnerable wi-fi dildo camera endoscope. yes really, 2017. URL https://www.pentestpartners.com/security-blog/vulnerable-wi-fi-dildo-camera-endoscope-yes-really/.

[122] Klaus R Scherer. Emotions. In *Introduction to Social Psychology: A European Perspective*. Oxford: Blackwell, 3rd edition, 2000.

[123] K. R. Scherer. Level and change in perceived control predict 19-year mortality: Findings from the americans changing lives study. *Appraisal considered as a process of multilevel sequential checking. Appraisal processes in emotion: Theory, methods, research*, 92(120):57, 2001.

[124] S. Budimir and J. Fontaine. Emotion psychology meets cybersecurity, qualitative research, preliminary data, July 2017.

[125] S. G. van de Weijer and E. R. Leukfeldt. Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7):407–412, 2017.

[126] O. Beris, A. Beautement, and M. A. Sasse. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop*, pages 73–84. ACM, 2015.

[127] J. J. Fontaine, K. R. Scherer, and C. (Eds.) Soriano. Components of emotional meaning: A sourcebook. 2013.

[128] J. Dippong and C. Fitch. Emotions in criminological theory: Insights from social psychology. *Sociology Compass*, 11(4), 2017.

[129] S. J. Sherman and J. L. Hoffmann. The psychology and law of voluntary manslaughter: what can psychology research teach us about the "heat of passion" defense? *Journal of Behavioral Decision Making*, 20(5):499–519, 2007.

[130] C. Bankoff. Reddit co-founder and jstor hacker aaron swartz commits suicide, 2013. URL http://nymag.com/daily/intelligencer/2013/01/jstor-hacker-aaron-swartz-commits-suicide.html.

[131] S. Malm. Two suicides are linked to Ashley Madison leak: Texas police chief takes his own life just days after his email is leaked in cheating website hack, 2015. URL http://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html.

[132] S. Oh and K. Lee. The need for specific penalties for hacking in criminal law. *The Scientific World Journal*, 2014.

[133] D. Canetti, M. Gross, I. Waismel-Manor, A. Levanon, and H. Cohen. How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychology, Behavior, and Social Networking*, 20(2):72–77, 2017.

[134] J. J. Gross, O. P. John, and J. M. Richards. The dissociation of emotion expression from emotion experience: A personality perspective. *Personality and Social Psychology Bulletin*, 26 (6):712–726, 2000.

[135] B. Holfeld and P. Sukhawathanakul. Associations between internet attachment, cyber victimization, and internalizing symptoms among adolescents. *Cyberpsychology, Behavior, and Social Networking*, 20(2):91–96, 2017.

[136] J. J. Gross. Antecedent-and response-focused emotion regulation: divergent consequences for experience, expression, and physiology. *Journal of personality and social psychology*, 74 (1):224, 1998.

[137] E. Watkins and S. Baracaia. Why do people ruminate in dysphoric moods? *Personality and individual differences*, 30(5): 723–734, 2001.

[138] K. R. Scherer. What are emotions? and how can they be measured? *Social science information*, 44(4):695–729, 2005.

[139] DailyMail. The 'smart' speakers that won't stop talking to each other: Watch amazon's echo dot get stuck in an 'infinite loop' chatting to google's home, 2016. URL http://www.dailymail.co.uk/sciencetech/article-3987694/The-smart-speakers-won-t-stop-talking-Watch-Amazon-s-Echo-Dot-stuck-infinite-loop-chatting-Google-s-Home.html.

[140] ARM. Arm platform security architecture overview. Technical report, 10 2017. URL http://pages.arm.com/rs/312-SAX-488/images/PSA-Introductory-Architecture-Overview.pdf.

[141] B. Moran, M. Meric, and H. Tschofenig. A firmware update architecture for internet of things devices draft-moran-suit-architecture-00, 2018. URL https://tools.ietf.org/html/draft-moran-suit-architecture-00.

[142] Digi-Key. Add firmware security to an iot design with a single chip, 2018. URL https://www.digikey.co.uk/en/articles/techzone/2018/jan/add-firmware-security-to-an-iot-design-with-a-single-chip.

[143] Jalal Al-Muhtadi, Manish Anand, M Dennis Mickunas, and Roy Campbell. Secure smart homes using jini and uiuc sesame. In *16th Annual Conference on Computer Security Applications (ACSAC)*., pages 77–85. IEEE, 2000.

[144] P. V. McMahon. Sesame v2 public key and authorisation extensions to kerberos. In *In Network and Distributed System Security*, pages 114–131. IEEE, 1995.

[145] M. Al-Qutayri, H. Barada, S. Al-Mehairi, and J. Nuaimi. A framework for an end-to-end secure wireless smart home system. In *2008 2nd Annual IEEE Systems Conference*, pages 1–7. IEEE, 2008.

[146] J. Jeong, M. Y. Chung, and H. Choo. Integrated otp-based user authentication scheme using smart cards in home networks. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, pages 294–294. IEEE, 2008.

[147] Bogdan-Cosmin Chifor, Ion Bica, Victor-Valeriu Patriciu, and Florin Pop. A security authorization scheme for smart home internet of things devices. *Future Generation Computer Systems*, 2017. ISSN 0167-739X. doi: https://doi.org/10.1016/j.future.2017.05.048. URL http://www.sciencedirect.com/science/article/pii/S0167739X17311020.

[148] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017. doi: 10.1109/PERCOMW.2017.7917634.

[149] A Collen, NA Nijdam, J Augusto-Gonzalez, SK Katsikas, KM Giannoutakis, G Spathoulas, E Gelenbe, N Ghavami, M Volkamer, P Haller, et al. Ghost-safe-guarding home iot environments with personalised real-time risk control. In *IS-CIS*, 2018.

[150] A. Rahmati, E. Fernandes, K. Eykholt, and A. Prakash. Tyche: Risk-based permissions for smart home platforms. *arXiv preprint arXiv:1801.04609*, pages 1 – 15, 2018. URL https://arxiv.org/pdf/1801.04609.pdf.

[151] P. Wang, K. M. Chao, C. C. Lo, W. H. Lin, H. C. Lin, and W. Chao. Using malware for software-defined networkingbased smart home security management through a taint checking approach. *International Journal of Distributed Sensor Networks*, 12(8), 2016.

[152] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, 138:1 – 12, 2018. ISSN 1389-1286. doi: https://doi.org/10.1016/j.comnet.2018.03.024. URL http://www.sciencedirect.com/science/article/pii/S1389128618301440.

[153] Bitdefender. Bitdefender box, 2018. URL https://www.bitdefender.com/box/.

[154] McAfee. Mcafee secure home platform, 2018. URL http://securehomeplatform.mcafee.com/docs/SHP-Whitepaper-Protecting-the-Home-Front_hires.pdf.

[155] Natasha Lomas. Dojo is designed to protect your smart home

from itself, 2015. URL https://techcrunch.com/2015/11/19/dojo-labs/.

[156] Cujo. Why would anyone want to hack your thermostat?, 2017. URL https://www.getcujo.com.

[157] Tuan Phan Vuong, George Loukas, and Diane Gan. Performance evaluation of cyber-physical intrusion detection on a robotic vehicle. In *2015 IEEE International Conference on Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, pages 2106–2113. IEEE, 2015.

[158] R. Heartfield and G. Loukas. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers and Security*, 76:101–127, 2018.

[159] M. Chronopoulos, E. Panaousis, and J. Grossklags. An options approach to cybersecurity investment. *IEEE Access*.

[160] Ranjan Pal, Leana Golubchik, Konstantinos Psounis, and Pan Hui. Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets. *IEEE Transactions on Dependable and Secure Computing*, 2017.