Title: A systematic review of crime facilitated by consumer Internet of Things

John M Blythe & Shane D Johnson

PUBLISHED IN THE SECURITY JOURNAL

Dawes Centre for Future Crime at UCL, Department of Security and Crime Science, University College London, UK.

Address: Dawes Centre for Future Crime at UCL

UCL Jill Dando Institute of Security and Crime Science

University College London

35 Tavistock Square

London, WC1H 9EZ

shane.johnson@ucl.ac.uk

ABSTRACT

The nature of crime is changing — estimates suggest that at least half of all crime is now committed online. Once everyday objects (e.g. televisions, baby monitors, door locks) that are now internet connected, collectively referred to as the Internet of Things (IoT), have the potential to transform society, but this increase in connectivity may generate new crime opportunities. Here, we conducted a systematic review to inform understanding of these risks. We identify a number of high-level mechanisms through which offenders may exploit the consumer IoT including profiling, physical access control and the control of device audio/visual outputs. The types of crimes identified that could be facilitated by the IoT were wide ranging and included burglary, stalking, and sex crimes through to state level crimes including political subjugation. Our review suggests that the IoT presents substantial new opportunities for offending and intervention is needed now to prevent an IoT crime harvest.

Keywords: Internet of Things, cybercrime, systematic review, crime harvest

INTRODUCTION

The “Internet of Things (IoT)” refers to electronic devices that are internet connected and can communicate and interact with one another (e.g. Maple, 2017). The IoT is considered the next technological revolution, and in the home, products can range from smart locks, to home assistants which afford greater convenience and intelligent living. Currently, it is estimated that the average UK household has ten internet connected products. This is expected to rise to 15 by 2020 (Wrap, 2017). However, consumer adoption of IoT products is lagging behind predictions, largely due to privacy and security concerns (DCMS, 2018). In this article, we systematically review crimes that have or may be facilitated by the consumer IoT. We begin by explaining why we might expect the IoT to facilitate crime and specify what types of devices we are concerned with. We then discuss the approach taken to review the literature and present our findings.

Crime Harvests and the IoT

It is well documented (e.g. Felson, 1994) that many new products and services have led to “crime harvests” (Pease, 1997). These arise when insufficient attention is given to the crime and security implications of new products and services which become prevalent in the legitimate market. Considering the evolution of a product or service, these have a lifecycle which involves four stages: (1) an introduction phase, where use is limited to early adopters; (2) a growth stage in which uptake increases; (3) a maturity stage in which the mass market is reached, and (4) a point where the market is saturated and sales decline.

Crime harvests can take different forms. In the case of the theft of physical products, this tends to occur during the growth and mass market stages of the product lifecycle. During these stages, products are well-known, desirable and sufficiently abundant to make locating/stealing them easy and their sale inconspicuous. Crime harvests have played out many times. Traditional urban examples include vehicle theft in the 1990s (e.g. Laycock, 2004), and mobile phone theft in the noughties (e.g. Mailley, Garcia, Whitehead, & Farrell, 2008). In these, and similar examples, solutions were found — albeit retrospectively — but offenders had exploited vulnerabilities in the design of these products for a considerable amount of time, in some cases decades, before they were addressed.

In the case of physical theft, crime opportunities may reduce with market saturation, since few people will want to buy stolen items at this point. However, for many goods, particularly electronic and (say) automotive ones, manufacturers constantly develop them to increase functionality and sales. Moreover, goods can be exported to countries where market saturation has not occurred. Consequently, opportunities for theft will not always decline with market penetration.

Online, crime opportunities are not limited to the theft of purchased products and so are even less likely to decline. Instead, opportunities will be proportional to the number of people using a service. For example, the introduction of email has allowed fraudsters to adopt “needle in a haystack” approaches – such as phishing scams (Hong, 2012) – to steal (say) victim’s financial data.   With such scams, victims are sent emails from seemingly (but not) genuine sources (e.g. a bank) that include a link to website. If they click on the link, they are directed to a malicious website and asked to provide sensitive information, including their username, password, or bank details. In this case, as the adoption of email services increases, so does the number of crime opportunities.

Recent estimates from the Crime Survey of England and Wales (Office for National Statistics, 2017b) suggest that at least half of all crime is now online. This is likely to be an underestimate because only a handful of incidents of computer misuse are covered in the survey, and victims will often be unaware that they have been victimised. However, what these figures clearly illustrate is that the opportunities afforded by the internet are being exploited.

As noted, the market penetration of IoT devices is increasing. As it grows, crime harvests may emerge and, because different types of devices offer different functions, the potential forms these crime harvests may take may increase. Unlike crime in the “real” world, the IoT may facilitate the commission of crime at low cost, at scale and across geographic boundaries.

Warning signs of a crime harvest for IoT devices already exist. In 2016, attackers exploited hundreds of thousands of internet-connected cameras and Video Recorders, taking advantage of their poor security to build networks of compromised internet connected devices. These *botnets* were then used to launch Distributed Denial of Service (DDoS) attacks, which involve sending massive volumes of requests to online services that, unable to cope with the demand, become inoperable. The 2016 attacks, which used the *Mirai* malware to target servers operated by DYN in the U.S., disrupted online services such as Twitter and Netflix, and were particularly interesting because they represent the first known attack that used compromised IoT devices (as opposed to infected computers). At this time, the volume and types of incidents of crime that have involved IoT devices are limited. However, rather than wait for another crime harvest, the aim of the current article is to draw the issue to the attention of the criminological and related communities, and to take stock of what we already know. To do this, we provide a synthesis of the literature on crime that might be facilitated by the IoT. Before presenting findings, we define what is within scope for the review – including what mean by the IoT in the context of this article – and briefly articulate the methodological approach taken.

The IoT is transformative and spans across multiple domains. Here, we focus specifically on consumer (as opposed to, say, industrial) IoT devices, which may be defined as once everyday objects found around the home that are now internet connected (e.g. smart speakers or smart doorbells). For most devices, a connection to the internet is unnecessary and there will be non-internet connected variants of them. As such, we exclude routers, smart phones and tablets since these (mostly) require an internet connection to function. We also exclude computers (desktops and laptops), because these are very different types of devices. For example, they are high-capacity devices that have been on the market for a long time, have well developed operating systems and user interfaces, and the threats to these devices have been known for some time.

We focus on consumer IoT because the cybercrime challenges associated with it are prevalent and bring unique risks to consumers' security, privacy and safety. Currently, consumer IoT devices lack adequate security provision — poor design choices such as default passwords, inadequate encryption and lack of software updates have allowed consumer IoT devices to be misused for malicious purposes (DCMS, 2018). These have arisen in part due to the companies developing IoT devices either lacking expertise in security, or paying too little attention to it, and the absence of economic incentives (and regulation) to encourage security by design (FTC, 2015). Furthermore, at present, the most prevalent risks associated with insecure IoT devices discussed in the media are DDoS attacks. For these crimes, the direct impact is not generally felt by the consumer or manufacturer, but rather third parties (Schneier, 2018), which reduces the incentive for manufacturers (and consumers) to take the issue seriously.

However, in the future, the crime risks associated with consumer IoT have the potential to be more wide-ranging, impacting on citizens, companies and nations more directly. As discussed, one reason for this is that as well as increasing in ubiquity, the variety of devices that are internet connected – and the actions they are capable of completing – is increasing. For example, Smart TVs and speakers not only allow media to be streamed, but for sound, conversations and people's actions to be monitored and recorded. Many IoT devices now have actuators (e.g. a lock in a security system), which allow actions to be triggered in the physical world (e.g. Banafa, 2016), expanding the ways in which they might be misused.

With these points in mind, the aims of this paper are to provide a systematic review of existing work on cybercrime and the consumer IoT to address the following research questions:

1. *What are the primary mechanisms through which cybercrimes may be committed using IoT devices?*
2. *What cybercrimes have/could be facilitated through consumer IoT devices?*

To be clear, this paper is not about cybercrime in general. This would be beyond the scope of a single article. Instead, our focus is on crimes facilitated by the IoT. In the tradition of situational crime prevention (e.g. Clarke, 1980), it is important to have this clear focus as our aim is to understand the crime opportunities the consumer IoT presents with a view to catalysing and informing attempts to prevent associated crime harvests.

Evidence Synthesis

A brief discussion of our approach to the review is important at this point. We could have conducted a standard ad-hoc literature review, but these are known to be problematic, primarily because they can lead to the synthesis of a biased sample of articles, often limited to those already known to the study authors. Systematic reviews (Higgins & Green, 2011) have emerged as a solution to this. They involve a systematic and transparent search strategy, which includes the a-priori specification of the search terms to be used, databases to be searched, and so on. Consequently, any two authors conducting the search would be expected to find the same articles.

Systematic reviews are most commonly used to synthesise evidence on what works to reduce a problem, such as crime (Weisburd, Farrington and Gill, 2016). However, they can also be used to synthesize the evidence on particular topics (e.g. Cockbain, Bowers and Dimitrova, 2018), which is our aim here.

The specific aim of a systematic review will inform the approach taken to evidence synthesis and the types of studies included. Systematic reviews of what works address questions about something that has already happened, and those conducted in the Campbell tradition (for a discussion of approaches, see Johnson, Bowers and Tilley, 2015) typically focus on experiments that test the impact of interventions. In reviewing that evidence, researchers typically assess the quality of the evidence, as well as the effects observed. More weight is given to high quality studies for which rival explanations for observed effects can be ruled out. Here, the prospective nature of the review presents a methodological challenge. That is, it is difficult to assess the strength of the evidence about something yet to happen. To address our research questions, we draw on the findings of studies that employ a range of methodologies. These include expert speculation — commonly used in *futures* studies — and laboratory experiments intended to identify vulnerabilities in systems, which is an established methodology in the field of information security. While studies employing these approaches cannot demonstrate that an issue will emerge in the "wild", they speak to its plausibility. To make use of such sources of information, we draw on the realist approach (Pawson and Tilley, 2018) to review to identify the potential mechanisms through which IoT devices might be exploited in the future to commit crime. Like systematic reviews conducted in the Campbell tradition, we use a hierarchy of evidence to assess the strength of the evidence on which conclusions are based.

The remainder of the paper is organised as follows. Next, we describe the methodology employed, including a discussion of our search criteria and search strategy. We then provide a synthesis of the findings, considering what types of crime have or could be facilitated by IoT devices, and how such crimes might be committed (i.e. the mechanism through which they are committed). In the discussion, we draw conclusions and articulate why we think the study of crime facilitated by the IoT would benefit from attention from the criminological as well as the information security community (who have almost exclusively researched this issue to date).

METHOD

Systematic review process

We first developed a review protocol (see Higgins & Green, 2011) that was examined by five independent experts. They commented on the research questions, search strategy, inclusion criteria and electronic databases searched. The protocol was updated on the basis of their feedback. After studies were identified for inclusion, they were read, and the findings summarised using a narrative approach.

Inclusion Criteria

We included studies that employed any type of research design. All types of information sources were included with the exception of articles that were not peer-reviewed or that were unavailable in English. We included papers that appeared in the proceedings of information security conferences and magazine articles that had been peer reviewed, PhD theses and student dissertations. We also included literature reviews, as novel information may have been presented by the authors of those reviews that was relevant to the study, but we avoided double counting. Studies were included if they discussed consumer IoT devices or smart home platforms. Studies that discussed other forms of IoT such as smart cities, healthcare, or industrial IoT were excluded. Studies were included if there was a discussion of a crime, attack or a security-related issue. In some cases, studies discussed specific security solutions or countermeasures — these were only included if there was explicit discussion of the type of crime or attack the countermeasure was designed to address (studies that discussed solutions to “cybercrime” were excluded).

Electronic searches

A search of the following databases was conducted in November 2017: Web of Science, ProQuest, ACM Digital Library, IEEE Xplore Digital Library, and Scopus. We limited searches to papers published between 2007 and 2017. The search terms were piloted in order to achieve a balance between sensitivity (retrieving a high proportion of relevant articles) and specificity (retrieving a low proportion of irrelevant articles), and an academic librarian consulted to validate these and the databases used. The final search terms were:

> “IoT” OR “Internet of Things” OR “internet-connected” OR “cyber-physical” OR “M2M” OR “Machine to machine” OR “smart NEAR/3 device*” OR “smart home” OR “connected device*” OR “smart wearable” OR SU.EXACT(“Internet of Things”) OR SU.EXACT(“Internet of Things”) OR SU.EXACT(“Ubiquitous Computing”)
>
> AND
>
> “hack*” OR “risk*” OR “threat*” OR “vulner*” OR “crim*” OR “attack*” OR “exploit” OR “security” OR “privacy” OR “bug” OR SU.EXACT(“Crime”) OR SU.EXACT(“Internet Crime”) OR SU.EXACT(“Computer Crime”)

We also searched for the following subject headings (where allowed by the database): SU.EXACT("Crime") OR SU.EXACT("Internet Crime") OR SU.EXACT("Computer Crime")

AND

"consumer" OR "domestic" OR "wearable" OR "home" OR "house"

Keywords were searched for in the titles, abstracts and indexed subject headings of articles.

Data collection and analysis

Selection of studies

Identified citations and abstracts were imported into www.covidence.org, and duplicates removed. Studies were screened on title and abstract according to our inclusion criteria. One researcher independently screened (i) titles, (ii) abstracts and (iii) full texts against the pre-defined eligibility criteria. Random samples of abstracts were screened by a second researcher at four stages of the review to assess inter-rater reliability and mitigate coder drift (Ratajczyk et al., 2016).

Inter-rater reliability was calculated using the prevalence- and bias-adjusted kappa (PABAK) statistic, which controls for chance agreement (Byrt, Bishop, & Carlin, 1993). The PABAK score of 0.78 indicated high inter-rater agreement (see, Higgins & Green, 2011).

Data extraction and management

A proforma, piloted on a sample of articles to ensure that relevant information was captured (Higgins & Green, 2011), was developed to extract information from each study. It captured:

- Year of study
- Publication type
- Study design
- Quality of evidence (see below)
- Type of evidence (e.g. empirical or simulation)
- Target of crime, method of offending, cybercrimes/harms
- Brief description of study

RESULTS

Summary of search results

The initial database search yielded a total of 3506 published articles (see Figure 1). After removing 798 duplicates, 2708 were screened for eligibility — 198 met the inclusion criteria for full text review. Following full text review, 114 studies were included. Of these, two were from magazine articles, one was a book chapter, 20 were from journal articles and 91 were conference proceedings[1]. Of the 84 excluded, 49 did not discuss a crime-related issue, and 29 were not about consumer IoT. For two, the full text was unavailable, two were not peer reviewed, one was a duplicate and one was unavailable in English.

INSERT FIGURE 1 ABOUT HERE

For urban crimes, specific attack methods are generally associated with some offences but not others. For example, residential burglary may be committed in a variety of ways, but these generally differ to those employed in (say) street robberies. In the context of the IoT,

[1] In computer science, conference papers undergo a rigorous peer-review process.

a single method or combination of them, may be used to commit a range of offences. As such, unlike urban crime, there will be a less direct mapping between particular methods of attack and specific crime types. Consequently, we first outline the types of attacks identified. Strictly speaking, some of these actions (e.g. Denial of Service attacks) may be crimes themselves in many countries, since they violate state laws (e.g. the Computer Misuse Act (1990) in the UK). However, many of these violations may go unnoticed and may not in themselves have harmful consequences for the victim. In the language of realistic evaluation (Pawson & Tilley, 2018), they represent intermediate outcomes that are necessary steps for a crime to be committed, and hence reviewing their possible forms helps to map out what offences might ultimately be possible. With this in mind, after reviewing methods of attack, we outline key mechanisms through which a crime may be committed, and the key cybercrimes/harms that have been discussed. This process of attack method to cybercrime (ultimate outcome) is summarised in Figure 2.

INSERT FIGURE 2 ABOUT HERE

We also examine the strength of the evidence to help assess the extent to which the offences discussed can be considered plausible. For example, a particular type of crime is considered more likely if it had been demonstrated in the real world compared to researchers merely speculating about it. As with systematic reviews of crime reduction interventions, we do this with reference to a hierarchy of evidence. This was developed following an initial reading of the articles and is summarised in Table 1.

INSERT TABLE 1 ABOUT HERE

Methods of attack

A total of eleven attack types were identified which, to ease their presentation and review, are summarised in Table 2. These categories are not mutually exclusive, as attackers may use multiple techniques to exploit a device or network of them. As well as listing the types of attacks identified, in Table 2 we briefly define them and provide example citations.

INSERT TABLE 2 ABOUT HERE

While threats exist at the various stages of the development, deployment and lifecycle of a product (see, Garcia-Morchon, Kumar, Keoh, Hummen and Struik, 2014), most papers focussed on attacks that are launched against purchased IoT devices.

Mechanisms and cybercrimes/harms

Next, we detail the key mechanisms that may be employed to facilitate the cybercrimes/harms discussed in papers. We limit discussion to those for which there was some consensus in the literature (i.e. examples discussed in two or more papers). **Error! Reference source not found.** summarises the intermediate outcomes discussed that can be realised from the types of attacks shown in Table 2. **Error! Reference source not found.** summarises the cybercrimes/harms. In both tables, we provide an indication of the quality of the evidence used to establish the plausibility of the mechanism through which the cybercrimes/harms could be realized.

INSERT TABLE 3 AND TABLE 4 ABOUT HERE

We now elaborate on the content of Tables 3 and 4, discussing papers[2] that employed either an experimental or simulation research design and articulated a clear mechanism between an attack method and the associated cybercrimes/harms. The examples discussed thus represent forms of offending for which the way in which an offense might be carried out was clearly stated and evidence exists to suggest it as plausible, even if there is little or no evidence of this in the "wild" hitherto. We then discuss how these mechanisms may relate to cybercrimes/harms that have been speculatively derived within the literature. For the reader's benefit, methods of attack (see Table 2) are italicised in the text.

Exposing personal user data

Consumer IoT devices can store and process personal data from seemingly innocuous information about a users' activities to personal information (e.g. name and address). Numerous studies demonstrate how device vulnerabilities can lead to data being directly exposed, raising privacy concerns. For example, in a laboratory study Lee, Lee, Shim, Cho, and Choi, (2016) showed how a number of *man-in-the-middle attacks* could be used to obtain personal information (e.g. personal identifiers and health information) from a wearable device. These included exploiting hardware or protocol flaws allowing an unauthorized connection to a wearable device to gather personal data illegally. They also demonstrated that an attacker can *eavesdrop* between a wearable device and services to intercept data exchanged. Such attacks exploit misconfigurations of Bluetooth settings in wearable devices, inadequate authentication (e.g. where a wearable does not differentiate

[2] Due to page constraints, only example citations are included in the text. More details of the full set of papers reviewed can be found in the electronic supplementary material.

between the real user’s smartphone and an attacker’s) and sensitive data exposure, whereby a smartphone application and its firmware do not use encryption to secure data (see also, Lotfy and Hale, 2016).

Other research (Tekeoglu & Tosun, 2015a) has explored the security of Chromecast cloud communications, finding that the control packets used to send user information can be exploited with *replay* and *session hijacking attacks*. The exposed data were sent in clear text (such as the google account being accessed) to the attacker. Other studies have demonstrated that user personal data is sent unencrypted from baby monitors over Wi-Fi packets (Sivaraman, Gharakheili, Vishwanath, Boreli, & Mehani, 2015) and can be exposed through attacks that target device firmware (Badenhop, Ramsey, Mullins, & Mailloux, 2016).

Attackers may also compromise IoT devices to expose sensitive information not stored on them. For example, *side channel attacks* using smart watches can allow attackers to make inferences about sensitive information typed by a user on a smartphone or computer (e.g. Maiti, Jadliwala, He, & Bilogrevic, 2015). This is problematic if the user is entering sensitive information such as emails, search queries and so on (H. Wang et al., 2015). Research has further shown that a malicious app could misuse the gyroscope, accelerometer and magnetometer on a smartwatch to infer a user’s ATM PIN with more than 90% accuracy after only three trials (C. Wang, Guo, Wang, Chen, & Liu, 2016).

The above papers focused on the security of devices tested and on demonstrating the types of attack possible. What they tended not to discuss were the crime types that might be facilitated. For other papers, the reverse was true. It is to these latter papers we next turn. This variability in coverage was common and so this format will be repeated throughout the review. In addition, some of the papers that discussed specific crime types provided little detail about the offenses themselves. Conducting a (branching) systematic review of the research for each of the crime types discussed was beyond the scope of this review. Consequently, following a more realist approach (Pawson and Tilley, 2018), to provide a little more detail about the crimes that might be facilitated by IoT devices[3], we supplement what follows with findings from additional searches.

Directly exposing personal information stored or communicated from IoT devices may lead to a number of crimes. Users' personal information can be used for identity theft (Amin & Giacomoni, 2012; Jacobsson, Boldt, & Carlsson, 2016; Tzezana, 2017), by (for example) inferring a user's social security numbers from the information on their wearable (Aktypi, Nurse, & Goldsmith, 2017). Sexual-related information or other information such as videos and images may be stolen from devices and used to blackmail individuals (Bugeja, Jacobsson, & Davidsson, 2017; Tzezana, 2016). The facilitation of theft and distribution of sexual content via technology has increased in recent years (Powell & Henry, 2018) and has been used to harass, coerce or blackmail victims (Henry & Powell, 2015). For example, in

[3] To be clear, we only used additional references not identified through the systematic search to provide further context about crimes identified through the systematic search.

2014, private photos of Jennifer Lawrence and other high-profile celebrities were leaked online after hackers exploited their iCloud accounts (BBC news, 2017b). As more devices collect, send and receive such data, the opportunities for such offending will increase.

Profiling

Several papers demonstrated that information about consumers' routine activities (e.g. exercise, cooking) and household occupancy can be (in)directly inferred from IoT devices. For example, occupancy in the home correlates with smart meter activity relating to power usage (Chen, Kalra, Irwin, Shenoy, & Albrecht, 2015). Attackers can obtain activity and occupancy information in a number of ways, including *eavesdropping* communications between devices that employ a Bluetooth (Reichherzer, Timm, Earley, Reyes, & Kumar, 2017) or ZigBee connection (Yoshigoe, Dai, Abramson, & Jacobs, 2016)—both commonly used communication protocols in IoT devices.

In a laboratory study, Copos, Levitt, Bishop, and Rowe (2016) analysed the traffic between a Nest thermostat and a smoke detector. They found that with high accuracy, they could identify when the thermostat transitioned between the Home and Auto Away mode (88%) which indicates whether the user is home or not. Other studies have demonstrated how variants of *side channel attacks* can be used to indirectly infer activity patterns (e.g. Anand & Saxena, 2016), although the accuracy of detection depends on the manufacturer, and the specific activity concerned (Reichherzer et al., 2017; Torre et al., 2017). For example, Yoshigoe, Dai, Abramson, and Jacobs, (2016) demonstrated that a smart hub and its cloud server employed a predictable response pattern that can be used to identify when nobody is home (little network traffic is generated homes are unoccupied).

IoT devices also store and communicate large amounts of personal information, which can be used to build user profiles. Jacobsson et al., (2016) liken this to the current mapping of online user behaviour by companies including Facebook and Google but argues that the IoT will allow physical user habits to be plotted, creating detailed personal dossiers of both online and offline behaviour. Companies may also profile to determine behavioural patterns for commercial purposes (e.g. Amin & Giacomoni, 2012) and to tailor unsolicited messages to users (Jacobsson et al., 2016). Companies currently provide predictive insights about peoples' health by tracking wearable and smartphone data to measure stress based on their heart rate, potentially revealing their (mental) health state (Aktypi et al., 2017). Data can be aggregated to make potentially sensitive inferences, such as participation in sporting events, while access to contact lists can allow inferences regarding health conditions and social activity (Aktypi et al., 2017). These may constitute crimes under recently introduced General Data Protection Regulation (GDPR) if adequate consent is not given or the data are processed inappropriately.

Some papers discussed how profiling users could lead to discrimination using information gained from health wearables (Aktypi et al., 2017). Presently, the HR sector analyses job applicants' suitability using information from social network accounts (CIPD, 2013). In the future, information derived from IoT devices may be used to provide insight into applicant's physical and mental health. For example, Aktypi et al., (2017) argue that obesity could be diagnosed using data from wearables and that pregnancy could be detected (resting heart rates increase by 40-50% during pregnancy). The FTC (2015) also has concerns that the collation of information about people may be used discriminately for employment, credit and insurance decisions. The legal implications of using social media data for employee screening are currently unclear (CIPD, 2013) but may be further clarified (in the UK at least) through recent data protection legislation (BBC news, 2017a; CIPD, 2013). However, the law on discrimination applies to both online and offline checks. Thus, information gained regarding applicant's protected characteristics that is misused to discriminate applicants will be illegal. How data is collected from IoT devices is thus of concern.

Several papers suggested that profiling could be used for reconnaissance to facilitate crimes including burglary (discussed further below) and stalking (Aktypi et al., 2017; Jacobsson et al., 2016). Stalking is the repeated and persistent unwanted behaviour of an offender that engenders fear in victims (Paladin, 2018). It is common in cases of domestic abuse (Coleman, 1997), and a review of domestic abuse-related homicides in London indicated that 40% of victims were stalked prior to their death (Metropolitan Police, 2003). Most cases of stalking already involve an online element (Laxton, 2014); however, attacks that exploit the IoT will allow stalking and related offenses to be committed with greater ease and in a more targeted way.

Physical Access Control

As discussed, occupancy detection can help offenders determine if a victim is home or not. Moreover, research has demonstrated that home security devices (e.g. connected door locks) can be exploited to allow unauthorised entry. For example, Ho et al. (2016)

demonstrated that an attacker (with previous authorised access) can evade both the revocation mechanisms (intended to prevent access by particular individuals) on smart locks and the access logging of such devices, giving them unlogged, unauthorized access to a home. This particular problem arises due to vulnerabilities in the network architectures used (e.g. the use of a Device-Gateway-Cloud architecture, where the device lacks a direct connection to the manufacturer’s servers) and access control policies used by a range of smart lock systems. Agadakos et al. (2017) showed that the interconnectedness of various devices (e.g. connected window sensors, smart plugs and smart hub) can also leave homes vulnerable. They demonstrated that the Bluetooth channel for a smart plug was unauthenticated, allowing attackers to use *spoofing attacks* to turn off the smart hub, rendering connected window sensors useless. In this case, homeowners would not be informed if windows were opened or closed.

Other lab-based research (Wurm, Hoang, Arias, Sadeghi, & Jin, 2016) on smart home monitoring systems has identified vulnerabilities in the updating procedure, which can allow attackers to determine if users are home or not. Left unaddressed, as the consumer IoT market grows, this type of vulnerability may be significantly exploited—much like keyless car theft appears to be committed at the moment (BBC news, 2018).

Fernandes, Rahmati, Jung, and Prakash (2017) argue that unnecessary access privileges, referred to as open privileges in smart home platforms, can leave devices vulnerable. For example, a *malware* app that uses privileges in the SmartThings platform can *snoop* on PIN codes as they are created and leak them, giving attackers the codes to unlock connected doors. In a lab-based study, Min and Varadharajan (2015) demonstrate how attackers can exploit integration services (i.e. not just individual devices), including the popular IFTTT (If This Then That), that allows users to create triggers between devices or services (e.g. if light turned on, turn radio on). They show that attackers can take over a user's IFTTT account through the theft of browser cookies and use malware to manipulate IFTTT triggers to perform unauthorised actions (e.g. triggering smart locks to open without alerting the user).

A combination of occupancy detection and the exploitation of devices linked to physical security can facilitate unwanted intrusion in the home and burglaries. Numerous papers discuss how these mechanisms can be triggered (Fernandes et al., 2017; Fernandes, Jung, & Prakash, 2016; Ho et al., 2016; Oluwafemi, Kohno, Gupta, & Patel, 2013a), although they do not always demonstrate the attack, with experts speculating about the possibility instead (e.g. Aktypi et al., 2017).

In the UK, the rate of domestic burglary has been declining with two in every 100 households victim to domestic burglary in 2017 compared to nine in 1995 (Office for National Statistics, 2017c). However, this has started to increase recently (Office for National Statistics, 2017a) and technology may further facilitate this if the vulnerabilities discussed go unaddressed.

Control audio-visual outputs

Research demonstrates that attackers can manipulate and misuse devices, monitoring and controlling the audio/visual outputs of devices or misusing actuators. For example, Bachy et al. (2015) exploited the firmware of Smart TVs using both physical and remote attacks, creating backdoor remote access to the TV from the internet. This allowed them to replace video displayed on the TV and use the device to launch additional attacks. Other lab-based studies have demonstrated that the visual output of surveillance cameras can be reconstructed by *sniffing* camera network traffic (Tekeoglu & Tosun, 2015b). Moreover, due to a lack of encryption, images can be overwritten on many surveillance cameras using a video *replay attack* (Feng, Ye, Swaminathan, & Wei, 2017). As such, critical events may be hidden from the user (e.g. potential intruders) or misinformation communicated (E. Fernandes et al., 2017; Earlence Fernandes et al., 2016).

Research by Obermaier and Hutle (2016) showed that using techniques including traffic analysis and firmware disassembly, attackers could exploit the poor encryption, authentication and access control of cameras. The success and consequences of attacks depended on the camera manufacturer and the attacker's location (physical vs remote), but these vulnerabilities allowed the injection of forged video streams, manipulation of camera functionality, *eavesdropping* on camera streams, and the launch of attacks on the camera server. Xu et al. (2017) also demonstrated that cameras can be exploited in physical proximity attacks through access to cameras feed. However, this type of attack requires physical access to the consumers' smartphone to access the associated software application, or the theft of their sim card to reset the access password. These studies demonstrate that some attacks are more sophisticated, require physical access to products or connected devices, and that success may depend upon the specific vulnerabilities of the consumer device, but that these risks do exist.

Other studies demonstrate that baby monitors are susceptible to hacking. Sivaraman et al. (2015) show that *man-in-the-middle attacks* can facilitate access to camera feeds, allowing attackers to view children. Predators may also misuse IoT devices to groom and exploit children, or broadcast sexual content to them (Tzezana, 2016). Industry reports show that children's toys are also susceptible to hacking, allowing strangers to talk to them (Which?, 2017). The IoT may thus afford further opportunities for predators to gain access to children, in the same way that online social networking services have previously been misused (Mitchell, Finkelhor, Jones, & Wolak, 2010) – for example, Facebook has been used in 33% of cases involving the grooming of children (NSPCC, 2018).

Consumer IoT devices can also be misused to illicit affective responses, causing embarrassment, annoyance or damaging a person's reputation (Denning et al., 2009; E. Fernandes et al., 2017; Tzezana, 2017). For example, audio devices can record private conversations (Denning et al., 2009) and devices with cameras can take embarrassing or sexual photographs (Denning et al., 2009; Tzezana, 2017). Tzenana (2016) argues that various sex crimes could be committed using these devices. For example, offenders may broadcast sexual messages to victims, including children, conduct exhibitionism by displaying sexual images to victims, or engage in voyeurism by observing others for sexual relief. Internet-facilitated sexual offending is increasing and has resulted in a rise in prosecutions and clinical referrals (Seto, 2015), but insecure IoT devices may fuel this type of offending further.

Potential manipulation and misuse of devices

Rahman, Carbunar, and Topkara (2013) demonstrated a number of security weaknesses of the Fitbit wearable. They were able to exploit a Fitbit within a radius of 15 feet and capture files including sensitive personal information (e.g. username, height, weight). They also found Fitbits to be susceptible to *data integrity* attacks allowing attackers to insert fake data without the Fitbit verifying it (e.g. unreasonable step counts). Step counts are linked to (monetary) rewards, which could allow attackers to earn money for steps (e.g. a $20 dollar gift card for steps accumulated) or appear higher on social ranking boards. They were also able to drain the battery of the device 21 times faster by continuously querying it. While these misdemeanours may not be particularly concerning, as devices become more connected and functionality increases, attacks may become more disconcerting.

Other studies show that attackers can gain control of devices to (say) masquerade as a legitimate user to gain control of smart lightbulbs (Sivaraman et al., 2015), exploit RFIDs used on smart locks by emulating or cloning a tag to unlock them (Xu et al., 2017), or *eavesdropping* on device commands to enable remote access to motion switches (Sivaraman et al., 2015). However, it should be noted that not all IoT devices are vulnerable to attack. For example, Visan, Lee, Yang, Smith, and Matson (2017) tested the security of

Samsung SmartThings and found it to be robust to various *man-in-the-middle* and *DoS attacks*.

The manipulation of IoT devices may be used to cause *denial of service* or certain device functions. For example, offenders may use ransomware to lock household devices in exchange for cash (Bugeja et al., 2017) or disrupt their connectivity (e.g. Vemi & Panchev, 2015). More seriously, a number of consumer IoT devices in the home have safety critical monitoring functions (e.g. fire alarms) and offenders may suppress these (e.g. Coppolino, Dalessandro, Dantonio, Levy, & Romano, 2015). Furthermore, offenders may target devices with heating capabilities to cause arson in the home (Chen & Luo, 2012; Greensmith, 2015; Kang, Moon, & Park, 2017) or overload electrical devices such as lightbulbs (Oluwafemi et al., 2013b). Devices with actuators, including household robots, may be used to vandalise homes (Denning et al., 2009; E. Fernandes et al., 2017; Earlence Fernandes et al., 2016). Furthermore, consumer IoT devices may be used for political misuse, with smart assistants hacked to only communicate news from a particular political orientation (Tzezana, 2016).

Of course, the IoT affords many benefits. For example, smart meters and the smart grid have the potential to achieve a more efficient, reliable way of providing gas and electricity to consumers (Smartgrid.gov, 2018). Of course, the security of this infrastructure is critical. Unfortunately, in the UK, the physical tampering of meters already costs consumers and the energy industry about £400 million per year (NPower, 2018). Lo and Ansari (2013) argue that such offending may increase, with *data integrity attacks* used to inject malicious data into smart meters causing false usage results. In a series of studies, Liu and colleagues simulated the impact of these attacks and demonstrated that an attacker can fake the guideline pricing curve (e.g. the cost of electricity during particular periods) and benefit from a 34% reduction in their bill. In another exploit, an attacker fakes the guideline pricing curve during peak load hours (e.g. 8pm) to be low so that significant energy can be consumed at discounted prices. They found that such attacks can significantly unbalance the local power system by increasing the peak to average ratio (in their study by 36%), which can lead to blackouts and a denial of service for energy usage, which has implications beyond energy theft.

Gateway to further attacks

As discussed, we did not examine the security of routers. However, we did consider this in the context of the IoT. Home routers are the gateway between connected devices and the internet, and in a Smart Home can help secure it. Research has shown that this sense of security may be overstated. Sivaraman, Chan, Earl, and Boreli (2016) were able to bypass the security in home routers through malware embedded on an iPhone app which scouts the users' home network for IoT devices and relays this back to an attack server. The malicious app then configures port mappings on the home router (via Universal Plug and Play network protocols) to give the attacker server access to specific devices, which they can then attack.

Others have demonstrated that they can exploit the connection between IoT devices and home routers. This often relies on physical proximity to the device, limiting the potential for this kind of attack. However, research has shown that this can be achieved using unmanned aerial vehicles (UAVs). For example, Vemi and Panchev (2015) were able to automate *man-in-the-middle attacks* by flying UAVs around an area, setting up rogue access points and harvesting important credentials from wireless networks and connected devices. This allowed them to disconnect devices from home routers or launch *DoS attacks* (see also, Xu et al., 2017). Given increases in UAV sales (see Statistica, 2018), this type of attack becomes ever more plausible.

DISCUSSION

In recent decades, criminological research has focused on understanding the factors that facilitate crime and interventions that reduce it. A variety of approaches have been taken, and frameworks developed. The body of evidence continues to grow and there are now many systematic reviews of what works (e.g. see College of Policing, 2018). While this is to be celebrated, for new forms of crime, including those (potentially) facilitated by the IoT, our knowledge of what works to reduce them is limited. Given that at least half of all crime now occurs online, there is a clear need for criminologists to focus on these forms of offending to help better understand and address them. The aim of this review was to systematically take stock of what we know and to map out a research agenda to encourage this.

We found that consumer IoT devices can be exploited using a range of attack methods, which can facilitate a variety of offences. We will not repeat what these are here. However, it is worth noting that some offences may be more likely and affect more people than others. For example, the exploitation of insecure IoT devices is likely to provide a wider variety of opportunities for offenders to commit crimes such as stalking, and provide richer data for them to exploit. For crimes including burglary, one might question if the IoT will increase this form of offending, since offenders already have ways of breaking into homes, and few may possess the necessary IT skills.

However, this segues into a further question about emerging models of crime, particularly *crime as a service* (e.g. Manky, 2013). In the context of cybercrime, an offender may not need the technical skills to commit a crime, as they can pay to use services provided by others. Well-documented examples are DDoS attacks, which can be rented on the dark web for a few dollars (Kaspersky, 2017). If the proliferation of IoT devices *does* increase the volume of crime opportunities, this will provide further incentives for those who provide such services, and for offenders to rent them. In this context, as more people choose to connect their homes to the internet, crimes such as burglary might increasingly be committed through the exploitation of vulnerabilities in the IoT. Critically assessing which crimes are most likely to be facilitated by the IoT would, thus, be a useful avenue for research.

Considering scale, Williams (2017) conducted an assessment of the vulnerabilities of 156,680 consumer IoT devices using the search engine Shodan.io. Thirteen-percent had vulnerabilities. Of these, 53% were printers, 40% were webcams and 7% were smart TVs. These numbers are non-trivial. Moreover, it is worth noting that vulnerabilities in a single device can render a whole smart-home network susceptible to attack.

Apropos the research agenda, at least five themes are worthy of attention. First, criminologists might explore the types of white-collar crime that could be facilitated. They might consider how future legislation may make activities that are currently unregulated criminal. For example, governments are introducing data protection legislation, and reacting to scandals associated with the inappropriate use of social media data. A systematic analysis of how this landscape might/should change would thus be valuable.

Third is measurement. It is widely accepted that much crime goes unreported. For computer misuse, the problem is likely to be considerably worse — data from the Crime Survey of England and Wales suggest that in the UK only 17% of offences are reported to Action Fraud, the UK's national fraud and cyber-crime reporting centre. While surveys can provide estimates of the prevalence of known offences, not all victims will be aware that they have been victimized and hence alternative data collection exercises will be required to estimate the true scale of the problem.

Fourth is understanding the problem. Research on situational crime prevention (SCP: Clarke, 1995) has sought to provide a detailed understanding of the conditions under which crime events occur, what kinds of targets are more vulnerable, and how crimes are carried out. The aim is to identify situational characteristics that might be manipulated to make crime less likely (e.g. Forrester, Chatterton, Pease, & Brown, 1988), and at what stage in a sequence of events interventions might best succeed. Addressing such questions in the context of the IoT may help to understand problems and identify solutions to them. However, it will require detailed data, including the types of devices (and networks of them) that are most vulnerable, network configurations and so on. Again, alternative forms of data collection will likely be required and collaborations with those in the field of information security are likely to be vital. Some of the analytic tools used to understand urban crime problems might be repurposed, but new forms of analysis will also likely be required.

In terms of crime prevention, we are currently exploring the potential of market levers to encourage manufacturers to make IoT devices secure by design (see Blythe and Johnson, 2018, DCMS, 2018). However, it will also be necessary to understand user behaviour as even the best designed system will fail if misused, misconfigured or updates are not installed. Non-compliance in the context of security is concerning but attackers are also known to target the human element (Mitnick & Simon, 2003). Understanding user susceptibility to cybercrimes will thus be important. Whilst much work needs to be done to ensure that the burden for securing IoT devices is reduced (DCMS, 2018), it is recognised that consumers will have to engage in “cyber hygiene” to maintain device security (Blythe, Michie, Watson, & Lefevre, 2017) and derived behavioural insights may be key to this (Coventry, Briggs, Blythe, & Tran, 2014). Firstly, what is needed is a greater focus on usable security to ensure the security of devices matches users’ goals, capabilities and primary tasks – recognising that security is secondary to consumers use of the product (Sasse, 2015). Secondly, crime prevention needs to focus on the facilitators and barriers to cyber hygiene, exploring users' capability, motivation and opportunity to protect themselves and design interventions accordingly (e.g. Blythe & Coventry, 2018). In a recent review, we found that cyberhygiene advice was absent in the user manuals or associated online materials of 90% of IoT devices sampled (Blythe et al, 2019).

As with any research, this review is not without limitations. Chief among these is that while developments in technology are rapid, the publication of academic research is not. As such, we provide a snapshot of research that will need updating. For example, it is possible that some of the vulnerabilities identified will have subsequently been fixed (for some or all devices) while others will be ongoing ‘unpatched’ issues. Moreover, the systematic search did not include industry reports (although our other searches did). Systematically searching these was beyond the scope of the current work but others might do this. Another issue concerns differences in the vocabulary used across disciplines. Research on cybersecurity typically focuses on threats to confidentiality, data integrity and availability as opposed to crime per se. While we do not believe this hampered the review, it is an issue.

At present, and as far as we are aware, we have not witnessed a wide-scale crime harvest associated with the IoT. However, there is no room for complacency — crime harvests have played out time and again. Now is the time to act and part of the aim of this paper was to encourage the criminology community to contribute to this agenda.

REFERENCES

Agadakos, I., Chen, C.-Y., Campanelli, M., Anantharaman, P., Hasan, M., Copos, B., … Lindqvist, U. (2017). Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things. In *CPS-SPC'17* (Vol. 17).

Aktypi, A., Nurse, J. R. C., & Goldsmith, M. (2017). Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In *Proceedings of the 2017 on Multimedia Privacy and Security* (pp. 1–11). Dallas, TX, USA.

Aljosha, J., Johanna, U., Georg, M., Artemios, V. G., & Edgar, W. (2017). Lightweight Address Hopping for Defending the IPv6 IoT. In *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17* (pp. 1–10).

Amin, S. M., & Giacomoni, A. M. (2012). Smart Grid-Safe, Secure, Self-Healing. *IEEE Power & Energy Magazine*, *10*(Jan/Feb 2012), 33–40.

Anand, S. A., & Saxena, N. (2016). Vibreaker: Securing Vibrational Pairing with Deliberate Acoustic Noise. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (pp. 103–108).

Bachy, Y., Basse, F., Nicomette, V., Alata, E., Kaaniche, M., Courrege, J. C., & Lukjanenko, P. (2015). Smart-TV Security Analysis: Practical Experiments. In *Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Smart-TV* (pp. 497–504).

Badenhop, C. W., Ramsey, B. W., Mullins, B. E., & Mailloux, L. O. (2016). Extraction and analysis of non-volatile memory of the ZW0301 module, a Z-Wave transceiver. *Digital Investigation*, *17*, 14–27.

Banafa, A. (2016). Internet of Things (IoT): Security, Privacy and Safety. Retrieved from https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948.

BBC news. (2017a). EU clamps down on social media job snoops. Retrieved from https://www.bbc.co.uk/news/technology-40592516.

BBC news. (2017b). Man jailed for hacking into Jennifer Lawrence’s online account. Retrieved from http://www.bbc.co.uk/newsbeat/article/38741309/man-jailed-for-hacking-into-jennifer-lawrences-online-account.

BBC news. (2018). West Midlands PCC calls car security summit. Retrieved from http://www.bbc.co.uk/news/uk-england-birmingham-43737877.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87–97.

Blythe, J.M., and Johnson, S.D. (2018). *Rapid evidence assessment on labelling schemes and implications for consumer IoT security.* DCMS: London. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf.

Blythe, J. M., Michie, S., Watson, J., & Lefevre, C. E. (2017). Internet of Things in Healthcare: Identifying key malicious threats, end-user protective and problematic behaviours. In *proceedings of the 3rd Digital Health Conference 2017, London, UK.*

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?. Journal of Cybersecurity, 5(1).

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 557–562.

Byrt, T., Bishop, J., & Carlin, J. (1993). Bias, Prevalence and Kappa. *Journal of Clinical Epidemiology*, *46*(5), 423–429.

Chen, D., Kalra, S., Irwin, D., Shenoy, P., & Albrecht, J. (2015). Preventing Occupancy Detection from Smart Meter Data. *IEEE Transactions on Smart Grid*, *6*(5), 2462–2434.

Chen, Y., & Luo, B. (2012). S2A: Secure Smart Household Appliances. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (pp. 217–228).

CIPD. (2013). *Pre-employment checks: an employer's guide*. Retrieved from http://www.cipd.co.uk/binaries/pre-employment-checks_2013.pdf.

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *Brit. J. Criminology*, *20*, 136.

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, *19*, 91–150.

Cockbain, E., Bowers, K., & Dimitrova, G. (2018). Human trafficking for labour exploitation: the results of a two-phase systematic review mapping the European evidence base and synthesising key scientific research evidence. *Journal of Experimental Criminology*, 14(3), 319-360.

Coleman, F. L. (1997). Stalking behavior and the cycle of domestic violence. *Journal of Interpersonal Violence*, *12*(3), 420–432.

College of Policing. (2018). Crime Reduction Toolkit. Retrieved from http://whatworks.college.police.uk/toolkit/Pages/Toolkit.aspx.

Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016). Is Anybody Home? Inferring Activity from Smart Home Network Traffic. In *Security and Privacy Workshops (SPW)* (pp. 245–251). IEEE.

Coppolino, L., Dalessandro, V., Dantonio, S., Levy, L., & Romano, L. (2015). My smart home is under attack. In *IEEE 18th International Conference on Computational Science and Engineering* (pp. 145–151).

Coventry, L., Briggs, P., Blythe, J. M., & Tran, M. (2014). *Using behavioural insights to improve the public' s use of cyber security best practices*. Report for the Department of Business, Innovation and Skills.

DCMS. (2018). *Secure by Design: Improving the cyber security of consumer Internet of Things Report*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

Denning, T., Matuszek, C., Koscher, K., Smith, J. R., & Kohno, T. (2009). A spotlight on security and privacy risks with future household robots. In *Proceedings of the 11th international conference on Ubiquitous computing* (pp. 105–114). ACM.

Felson, M. (1994). *Crime and everyday life.* Thousand Oaks, CA: Pine Forge.

Feng, X., Ye, M., Swaminathan, V., & Wei, S. (2017). Towards the Security of Motion Detection-based Video Surveillance on IoT Devices. In *Proceedings of the on Thematic Workshops of ACM Multimedia 2017* (pp. 228–235). ACM.

Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home

Applications. In *IEEE Symposium on Security and Privacy Security* (pp. 636–654).

Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017). Security Implications of Permission Models in Smart-Home Application Frameworks. *IEEE Security & Privacy*, *15*(2), 24–30.

Forrester, D., Chatterton, M., Pease, K., & Brown, R. (1988). *The Kirkholt burglary prevention project*.

FTC. (2015). *IoT Privacy & Security in a Connected World*. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., & Struik, R. (2014). *Security Considerations in the IP-based Internet of Things. draft-garcia-core-security-06*. Retrieved from https://tools.ietf.org/html/garcia-core-security-03.txt.

Greensmith, J. (2015). Securing the Internet of Things with Responsive Artificial Immune Systems. In *Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation* (pp. 113–120).

Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology*, *48*(1), 104–118.

Higgins, J. ., & Green, S. (2011). *Cochrane Handbook for Systematic Reviews of Interventions*.

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security* (pp. 461–472).

Hoang, N. P., & Pishva, D. (2015). A TOR-based anonymous communication approach to secure smart home appliances. In *International Conference on Advanced Communication Technology, ICACT* (Vol. 3, pp. 517–525).

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81.

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733.

Johnson, S. D., Tilley, N., & Bowers, K. J. (2015). Introducing EMMIE: An evidence rating scale to encourage mixed-method crime prevention synthesis reviews. *Journal of Experimental Criminology*, *11*(3), 459-473.

Kang, W. M., Moon, S. Y., & Park, J. H. (2017). An enhanced security framework for home appliances in smart home. *Human-Centric Computing and Information Sciences*, *7*(1), 6.

Kaspersky. (2017). Kaspersky Lab Research Reveals the Cost and Profitability of Arranging a DDoS Attack. Retrieved from https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-reveals-the-cost-and-profitability-of-arranging-a-ddos-attack.

Kumar, P., Ylianttila, M., Gurtov, A., Lee, S. G., & Lee, H. J. (2014). An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor network-based applications. *Sensors*, *14*(2), 2732–2755.

Laxton, C. (2014). *Virtual World, Real Fear: Women's Aid Report into Online Abuse, Harassment and Stalking*. Bristol: Women's Aid.

Laycock, G. (2004). The UK car theft index: An example of government leverage. In *Understanding and preventing car theft, vol. 17 of crime prevention studies* (pp. 25–44).

Willan: Cullompton.

Lee, M., Lee, K., Shim, J., Cho, S., & Choi, J. (2016). Security threat on wearable services: Empirical study using a commercial smartband. In *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)* (pp. 1–5). IEEE.

Liu, X., Zhou, Z., Diao, W., Li, Z., & Zhang, K. (2015). When Good Becomes Evil: Keystroke Inference with Smartwatch. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, 1273–1285.

Liu, Y., Hu, S., & Ho, T. Y. (2015). Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. In *IEEE/ACM International Conference on Computer-Aided Design,* (pp. 183–190).

Lo, C. H., & Ansari, N. (2013). CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid. *IEEE Transactions on Emerging Topics in Computing*, *1*(1), 33–44.

Lotfy, K., & Hale, M. L. (2016). Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things. In *2016 IEEE International Conference on Mobile Services (MS)* (pp. 25–32). IEEE.

Lyu, M., Sherratt, D., Sivanathan, A., Gharakheili, H. H., Radford, A., & Sivaraman, V. (2017). Quantifying the reflective DDoS attack capability of household IoT devices. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17* (pp. 46–51).

Mailley, J., Garcia, R., Whitehead, S., & Farrell, G. (2008). Phone Theft Index. *Security Journal*, *21*(3), 212–227. Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014).

Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33–59.

Maiti, A., Jadliwala, M., He, J., & Bilogrevic, I. (2015). (Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks using Smartwatches. In *Proceedings of the 2015 ACM International Symposium on Wearable Computers - ISWC '15* (pp. 27–30). New York, New York, USA: ACM Press.

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, (6), 9–13.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155-184.

Metropolitan Police. (2003). Findings from the Multi- agency Domestic Violence Murder Reviews in London. Retrieved from https://paladinservice.co.uk/wp-content/uploads/2013/07/Findings-from-the-Domestic-Homicide-Reviews.pdf

Min, B., & Varadharajan, V. (2015). Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT). In *20th International Conference on Engineering of Complex Computer Systems (ICECCS)* (pp. 80–89). IEEE.

Mitchell, K., Finkelhor, D., Jones, L., & Wolak, J. (2010). Use of social networking sites in online sex crimes against minors: an examination of national incidence and means of utilization. *Journal of Adolescent Health*, *47*(2), 183–190.

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element in Security*. John Wiley & Sons, Ltd.

NPower. (2018). Energy theft. Retrieved from https://www.npower.com/home/help-and-support/meter-readings/meter-tampering/.

NSPCC. (2018). Facebook tops list of sites used for online grooming. Retrieved from https://www.nspcc.org.uk/what-we-do/news-opinion/Facebook-tops-list-online-grooming/.

Obermaier, J., & Hutle, M. (2016). Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security - IoTPTS '16* (pp. 22–28). New York, USA: ACM Press.

Office for National Statistics. (2017a). Crime in England and Wales: year ending December 2017. ONS: London.

Office for National Statistics. (2017b). *Crime survey for England and Wales*.

Office for National Statistics. (2017c). Overview of burglary and other household theft: England and Wales. ONS: London.

Oluwafemi, T., Kohno, T., Gupta, S., & Patel, S. (2013a). Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security. In *Proceedings of the LASER 2013 (LASER 2013)* (pp. 13–24). Retrieved from https://www.usenix.org/laser2013/program/oluwafemi.

Oluwafemi, T., Kohno, T., Gupta, S., & Patel, S. (2013b). Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security. *Proceedings of the LASER 2013 (LASER 2013)*, 13–24.

Paladin. (2018). Paladin's Definition of Stalking. Retrieved from https://paladinservice.co.uk/.

Pawson, R. A. Y., & Tilley, N. (2018). What works in evaluation research?, *34*(3), 291–306.

Pease, K. (1997). Crime reduction. In M. Maguie (Ed.), *The Oxford Handbook of Criminology: Second Edition*. Oxford: Clarendon Press.

Powell, A., & Henry, N. (2018). Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives. *Policing and Society*, *28*(3), 291–307.

Rahman, M., Carbunar, B., & Topkara, U. (2013). *Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device*. https://doi.org/10.1109/TMC.2015.2418774.

Ratajczyk, E., Brady, U., Baggio, J. A., Barnett, A. J., Perez-Ibara, I., Rollins, N., … Janssen, M. A. (2016). Challenges and opportunities in coding the commons: Problems, procedures, and potential solutions in large-N comparative case studies. *International Journal of the Commons*, *10*(2), 440–466.

Reichherzer, T., Timm, M., Earley, N., Reyes, N., & Kumar, V. (2017). Using machine learning techniques to track individuals & their fitness activities. In *Proceedings of the 32nd International Conference on Computers and Their Applications, CATA 2017* (pp. 119–124).

Sasse, A. (2015). Scaring and Bullying People into Security Won't Work. *IEEE Security & Privacy*, *13*(3), 80–83.

Schneier, B. (2018). Click here to kill everybody: Security and survival in a hyper-connected world. WW Norton & Company.

Seto, M. (2015). *Internet-facilitated sexual offending*. Retrieved from https://www.smart.gov/SOMAPI/printerFriendlyPDF/adult-sec4.pdf.

Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016). Smart-Phones Attacking Smart-Homes. *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '16*, 195–200.

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015*, 163–167.

Smartgrid.gov. (2018). What is the Smart Grid? Retrieved from https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

Srinivasan, V., Stankovic, J., & Whitehouse, K. (2008). A fingerprint and timing-based snooping attack on residential sensor systems. *ACM SIGBED Review*, *5*(1), 1–2.

Statistica. (2018). Estimated global commercial drone unit sales in 2016 and 2017 (in 1,000 units). Retrieved from https://www.statista.com/statistics/740428/global-commercial-drone-unit-sales/.

Tekeoglu, A., & Tosun, A. S. (2015a). A closer look into privacy and security of Chromecast multimedia cloud communications. In *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 121–126). IEEE.

Tekeoglu, A., & Tosun, A. Ş. (2015b). Investigating security and privacy of a cloud-based wireless IP camera: NetCam. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2015–Octob*.

Torre, I., Koceva, F., Sanchez, O. R., & Adorni, G. (2017). Fitness Trackers and Wearable Devices: How to Prevent Inference Risks? In *Proceedings of the 11th International*

Conference on Body Area Networks. EAI.

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research*, *4*(1), 18.

Tzezana, R. (2017). High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *Foresight*, *19*(1), 1–14.

Vemi, S. G., & Panchev, C. (2015). Vulnerability testing of wireless access points using Unmanned Aerial Vehicles (UAV). In *Proceedings of the European Conference on e-Learning* (p. 245).

Vigo, R., Yuksel, E., & Dewi Puspa Kencana Ramli, C. (2012). Smart grid security a Smart Meter-centric perspective. In *2012 20th Telecommunications Forum (TELFOR)* (pp. 127–130). IEEE.

Visan, B. A., Lee, J., Yang, B., Smith, A. H., & Matson, E. T. (2017). Vulnerabilities in hub architecture IoT devices. *2017 14th IEEE Annual Consumer Communications and Networking Conference, CCNC 2017*, 83–88.

Wang, C., Guo, X., Wang, Y., Chen, Y., & Liu, B. (2016). Friend or Foe? In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16* (pp. 189–200).

Wang, H., Lai, T. T.-T., & Roy Choudhury, R. (2015). MoLe: Motion Leaks through Smartwatch Sensors. *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking - MobiCom '15*, 155–166.

Wazid, M., Das, A. K., Odelu, V., Kumar, N., & Susilo, W. (2017). Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. *IEEE*

Transactions on Dependable and Secure Computing, *5971*(c).

Which? (2017). Safety alert: see how easy it is for almost anyone to hack your child's connected toys. Retrieved from https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/

Weisburd, D., Farrington, D. P., & Gill, C. (Eds.). (2016). *What works in crime prevention and rehabilitation: Lessons from systematic reviews*. Springer: New York.

Williams, R., McMahon, E., Samtani, S., Patton, M., & Chen, H. (2017). Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. 2017 IEEE International Conference on Intelligence and Security Informatics: Security and Big Data, ISI 2017, 179–181.

Wrap. (2017). *Smart Devices & Secure Data Eradication: the Evidence*. Retrieved from http://www.wrap.org.uk/sites/files/wrap/Data Eradication report Defra.pdf

Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., & Jin, Y. (2016). Security analysis on consumer and industrial IoT devices. *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 519–524.

Xu, H., Sgandurra, D., Mayes, K., Li, P., & Wang, R. (2017). *Analysing the Resilience of the Internet of Things Against Physical and Proximity Attacks* (Vol. 10658).

Yoshigoe, K., Dai, W., Abramson, M., & Jacobs, A. (2016). Overcoming invasion of privacy in smart home environment with synthetic packet injection. *Proceedings of 2015 TRON Symposium, TRONSHOW 2015*, *1*(C).

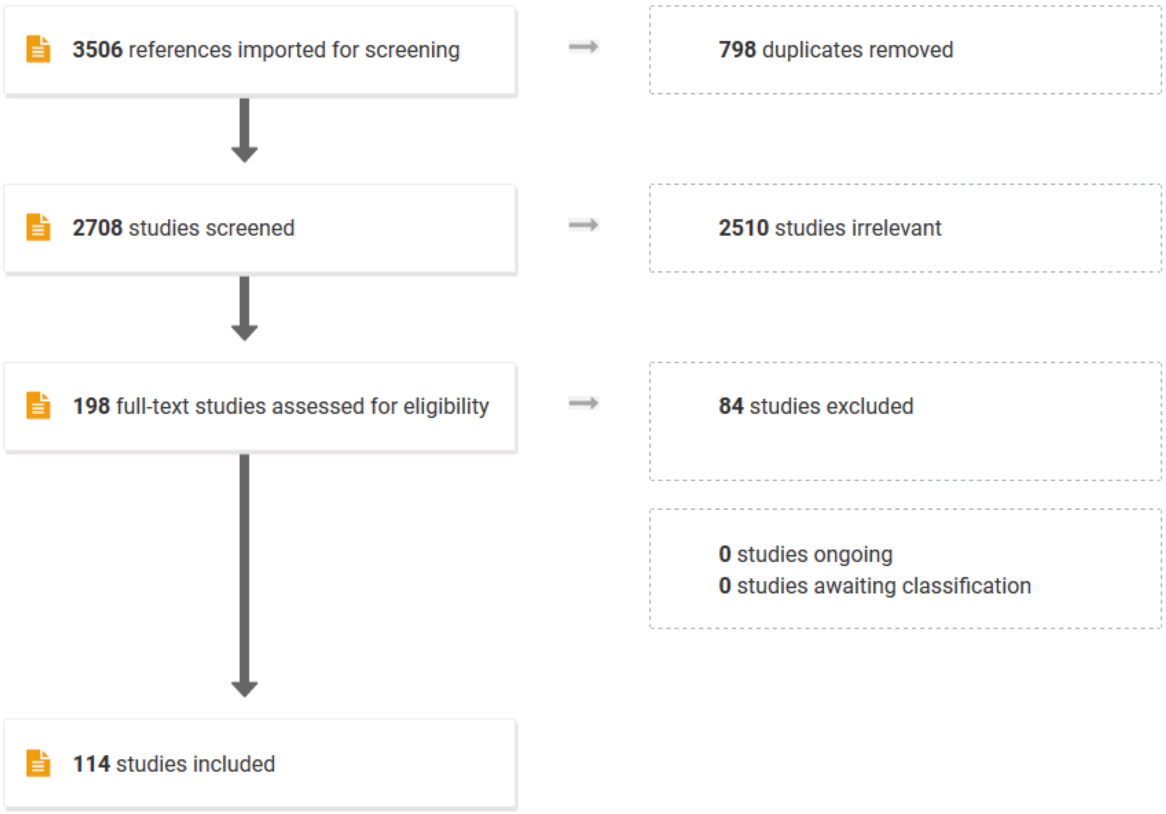

Figure 1. PRISMA chart and attrition in the systematic search process

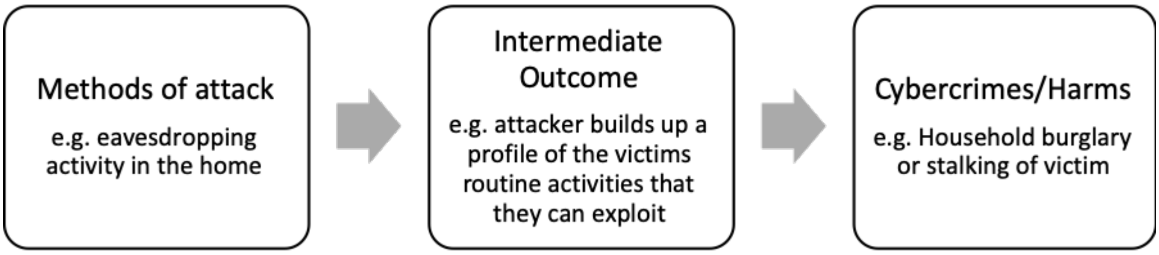
Methods of attack
e.g. eavesdropping activity in the home
Intermediate Outcome
e.g. attacker builds up a profile of the victims routine activities that they can exploit
Cybercrimes/Harms
e.g. Household burglary or stalking of victim

Figure 2. Process of IoT cybercrimes

Table 1. Hierarchy of evidence

Real world	Paper demonstrates an attack/consequence implemented "in the wild" on real IT systems (e.g. an IoT device is remotely infected with malware in the real world)
Experimental (lab-based)	Paper demonstrates an attack/consequence in a lab-based experiment using physical IT systems (e.g. an IoT device is infected with malware in a lab)
Experimental (simulation)	Paper demonstrates an attack/consequence in a computer-generated simulation (e.g. the effects of infecting IoT devices with malware are simulated in-silico)
Expert speculative	Data speculatively derived by a group of experts
Author speculative	Data speculatively derived by the study author
User speculative	Data speculatively derived by a group of users

Table 2. Summary of the key attacks against IoT devices identified

DoS	Denial of Service (DoS) attacks prevent users from accessing individual or associated services (e.g. Aljosha et al., 2017). They include jamming (e.g. Liu, Hu, & Ho, 2015) and flooding attacks (e.g. Thing, 2017), whereby a large volume of requests (e.g. for data or responses of some kind) are sent to a device (from a single source) with the aim of overwhelming it.
DDoS	Distributed Denial of Service (DDoS) attacks (e.g. Lyu et al., 2017) aim to make services (e.g. websites) unavailable by overwhelming them with traffic from multiple sources (e.g. botnets).
Eavesdropping	Unauthorised interception of communications allows attackers to obtain information. It can be achieved directly through (say) sniffing attacks where an attacker captures network packets using an application to intercept data, (Vigo et al., 2012) or indirectly through (say) inference attacks, where the integration and correlation of known data about individuals can lead to the discovery of private data (e.g. Torre, Koceva, Sanchez, & Adorni, 2017).
Malware	Use of malicious software to compromise devices by exploiting soft/hardware vulnerabilities. Exploits include changing the service purpose of the device (Kang et al., 2017). For example, infected devices can be used to send spam email, launch further attacks (e.g. distribute ransomware) (Sivaraman et al., 2016) or steal information.

Man in the Middle attacks	Attacker intercepts communications between devices, allowing them to eavesdrop, intercept, alter or steal information (e.g. Vemi & Panchev, 2015).
Physical attacks	Attacker physically accesses device to tamper with its hardware and settings (Snader, Kravets, & Harris III, 2016).
Data integrity attacks	Attacker attempts to compromise data by inserting, modifying or deleting it (in storage or transmission). Includes replay attacks whereby information is captured and subsequently retransmitted (fraudulently) to trick receiver into completing unauthorized operations (e.g. Kumar et al., 2014), such as unlocking a smart lock.
Spoofing attacks	Attacker masquerades as another to steal information, spread malware, circumvent access controls or send unauthorised commands (e.g. Bugeja, Jacobsson, & Davidsson, 2017).
Side channel attacks	Exploits information gained or inferred from a device despite security existing (e.g. Srinivasan, Stankovic, & Whitehouse, 2008). Examples include monitoring the speed with which a device can encrypt data, or the power consumed to help identify encryption keys.
User impersonation attacks	Attacker attempts to impersonate a user by using their access privileges. These may be obtained through social engineering attacks (e.g. Hoang & Pishva, 2015) or password guessing attacks (e.g. Wazid et al., 2017).

Table 3. Mechanisms and hierarchy of evidence (citations shown in square brackets)

Mechanism category	***Description***	***Real world***	***Empirical (lab based)***	***Empirical (simulation)***	***Speculative (experts)***	***Speculative (author)***	***Speculative (users)***
Exposing personal user data	Information stored or shared on devices can be intercepted by attackers. This data can include sensitive data (e.g. passwords, audio or visual information) or information pertaining to user behaviour and habits (e.g. fitness data).		[1]–[7]		[8]	[9]–[12]	[13]
Profiling	Attacker infers user activities (e.g. running, cooking, transport) and home occupation (in)directly from consumer IoT devices to potentially understand what they are doing at a particular time or to profile their behaviour.		[14]–[27]	[28]		[29]–[35]	
Physical access control	Attacker misuses devices linked to physical access in the home.		[3], [36]–[39]				
Manipulation of device (general)	Attacker remotely controls and manipulates the device. For example, using actuators on household robots to cause damage to household property.		[3], [37], [39]–[42]				
Control audio/visual outputs	Use of audio/visual outputs of IoT devices to control what the user hears/sees		[6], [42]–[45]			[46]	
Supress safety-critical monitoring capabilities	Malicious control or suppression of safety-critical monitoring devices (e.g. fire alarms).		[3]			[33], [47]	

Mechanism category	***Description***	***Real world***	***Empirical (lab based)***	***Empirical (simulation)***	***Speculative (experts)***	***Speculative (author)***	***Speculative (users)***
*Service unavailability and/or restriction**	Connected devices are linked to services in the home including critical (e.g. physical access, heating) and less critical (e.g. internet access) ones. Exploitation can lead to denial of service for consumers or censorship of certain product functions.					[9], [30], [32], [41], [51]–[55]	
*Monitoring/ surveillance**	Exploitation of consumer IoT devices may allow attackers to listen and monitor user activities.		[7], [24], [42], [48]		[8]	[9], [40], [46], [49], [50]	[13]
Gateway to further attacks	Once devices are exploited, attackers may use the device or information gained from it to launch additional attacks. For example, using a device as part of a Botnet to launch DDoS attacks, or using personal information for targeted password guessing.		[56]		[8]	[10], [29], [30], [43], [49], [51]	

[1] Bojinov, Bursztein, and Boneh (2009); [2] Lee, Lee, Shim, Cho, and Choi (2016); [3] Min and Varadharajan (2016); [4] Tang et al. (2017); [5] Tekeoglu and Tosun (2015); [6] Tekeoǧlu and Tosun (2015); [7] Lotfy and Hale (2016); [8] Tzezana (2016); [9] Bugeja (2017); [10] DeMarinis and Fonseca (2017); [11] Ahmad, Sunshine, Kaestner, and Wynne (2015); [12] Hoang and Pishva (2015); [13] Winter (2015); [14] Copos, Levitt, Bishop, and Rowe (2016); [15] Fafoutis, Marchegiani, Papadopoulos, Piechocki, Tryfonas, and Oikonomou (2017); [16] He, Xiao, He, and Pathan (2017); [17] Park, C. Basaran, Park, and Son (2014); [18] Reichherzer, Timm, Earley, Reyes, and Kumar (2017); [19] Sanchez et al. (2014), [20] Snader, Kravets, and Harris (2016); [21] Srinivasan, Stankovic, and Whitehouse (2008a); [22] Srinivasan, Stankovic, and Whitehouse (2008b); [23] Chen, Kalra, Irwin, Shenoy, and Albrecht (2015); [24] Schurgot, Shinberg, and Greenwald (2015); [25] Anand and Saxena (2016); [26] Yoshigoe, Dai, Abramson, and Jacobs (2016); [27] Das, Pathak, Chuah, and Mohapatra (2016); [28] Torre, Koceva, Sanchez, and Adorni (2017); [29] Aktypi, Nurse, and Goldsmith (2017); [30] Amin and Giacomoni (2012); [31] Aouini and Azzouz (2015); [32] Bergmann, Gerdes, Schafer, Junge, and Bormann (2012); [33] Kermani, Zhang, Raghunathan, and Jha (2013); [34] Greensmith (2015); [35] Brauchli and Li (2015); [36] Ho, Leung, Mishra, Hosseini, Song, and Wagner (2016); [37] Agadakos et al. (2017); [38] Fernandes, Rahmati, Jung, and Prakash (2017); [39] Oluwafemi, Kohno, Gupta, and Patel (2013); [40] Denning, Matuszek, Koscher, Smith, and Kohno (2009); [41] Ganguly, Poddar, Dutta, and Nasipuri (2016); [42] Obermaier and Hutle (2016); [43] Bachy et al. (2015); [44] Feng, Ye, Swaminathan, and Wei (2017); [45] Xu, Sgandurra, Mayes, Li, and Wang (2017); [46] Kumar, Gurtov, Iinatti, Ylianttila, and Sain (2016); [47] Coppolino, Dalessandro, Dantonio, Levy, and Romano (2015); [48] Vemi and Panchev (2015); [49] Al Delail and Yeun (2016); [50] Jacobsson, Boldt, and Carlsson (2016); [51] Arabo (2015); [52] Mosenia, Sur-Kolay, Raghunathan, and Jha (2017); [53] Murillo (2016); [54] Vigo, Yuksel, and Dewi Puspa Kencana Ramli (2012); [55] Rehman and Manickam (2016); [56] Lyu, Sherratt, Sivanathan, Gharakheili, Radford, and Sivaraman (2017)

*excludes papers that only discuss attack vectors such as Denial of service and eavesdropping attacks without consideration of the harms that arise from attacks.

Table 4. Cybercrimes/harms and hierarchy of evidence (citations shown in square brackets)

Cybercrimes/harms	***Description***	***Real world***	***Empirical (lab based)***	***Empirical (simulation)***	***Speculative (experts)***	***Speculative (author)***	***Speculative (users)***
Energy theft	Attacker misuses smart meters or other consumer IoT devices to steal electricity, increase utility costs to victims, manipulate energy costs in distribution networks, impact smart grid network or cause blackouts.		[1], [2]	[3]–[10]		[11]–[19]	
Burglary	Information from devices can reveal household occupancy based on user activities (see *profiling*). Further exploitation of connected devices (e.g. smart locks) can allow attackers to gain physical entry.		[20]–[24]		[25]	[13], [19], [31], [20], [23], [24], [26]–[30]	
Sex crimes	Use of consumer IoT devices to facilitate sex-related crimes such as stealing sex-related videos, sexual assault, obscenity, exhibitionism, and voyeurism.				[25], [32]		
Political	Exploiting consumer IoT devices for political gains (e.g. political subjugation and control, and propaganda).				[25], [32]		
Identity theft	Stealing sensitive personal information from devices to commit identity fraud.				[32]	[11], [27], [30]	
Harm to inhabitants	Causing physical or mental harm to individuals including vulnerable groups (e.g. children and older adults) that may be susceptible to nefarious influence. For		[33]			[16], [17], [34], [35] [15], [17], [29]	

Cybercrimes/harms	***Description***	***Real world***	***Empirical (lab based)***	***Empirical (simulation)***	***Speculative (experts)***	***Speculative (author)***	***Speculative (users)***
	example, targeting devices with heating capabilities to cause a fire in the home						
Misinformation	Use of IoT devices to give false or inaccurate information (e.g. false fire alarms).					[23], [24]	
Financial losses (general)	Financial losses arising from exploitation of IoT devices		[36]		[25]	[14], [17], [22], [37], [38]	[36]
Profiling, targeted or unsolicited advertising	Use of information from IoT for targeted advertising and marketing					[27], [30]	
Blackmail	Use of information gained from IoT devices to blackmail individuals				[25], [32]	[14], [39]	
Vandalism	Damage to physical property or household objects arising from exploited devices with actuators					[23], [24], [35]	
Illicit affective response	Use of information gained from IoT devices to cause embarrassment, annoyance or damage reputations					[23], [32], [35]	
Discrimination	Misuse of information from IoT devices (e.g. beliefs, health information) to discriminate against individuals					[18], [27]	
Stalking	Use of information gained from IoT devices (e.g. location) to stalk victims					[27], [30]	

[1] Ganguly, Poddar, Dutta, and Nasipuri (2016); [2] Tweneboah-Koduah, Skouby, and Tadayoni (2017); [3] Lo and Ansari (2013); [4] Liu, Hu, and Ho (2015); [5] Liu *et al.* (2015); [6] Liu and Hu (2015); [7] Liu, Hu, and Zomaya (2016); [8] Liu, Hu, and Ho (2016); [9] Liu and Sun (2016); [10] Liu, Zhou, and Hu (2017); [11] Amin and Giacomoni (2012); [12] Aouini and Azzouz (2015); [13] Bugeja, Jacobsson, and Davidsson (2017a); [14] Bugeja, Jacobsson, and Davidsson (2017b); [15] Chen and Luo (2012); [16] Kermani, Zhang, Raghunathan, and Jha (2013); [17] Kang, Moon, and Park (2017); [18] Winter (2015); [19] Komninos, Philippou, and Pitsillides (2014); Ho, Leung, Mishra, Hosseini, Song, and Wagner (2016); [21] Agadakos *et al.* (2017); [22] Min and Varadharajan (2016); [23] Fernandes, Rahmati, Jung, and Prakash (2017); [24] Fernandes, Jung, and Prakash (2016); [25] Tzezana (2016); [26] Ahmad, Sunshine, Kaestner, and Wynne (2015); [27] Aktypi, Nurse, and Goldsmith (2017); [28] Schurgot, Shinberg, and Greenwald (2015); [29] Greensmith (2015); [30] Jacobsson, Boldt, and Carlsson (2016); [31] Chen, Kalra, Irwin, Shenoy, and Albrecht (2015); [32] Tzezana (2017); [33]Oluwafemi, Kohno, Gupta, and Patel (2013); [34]

Cybercrimes/harms	***Description***	***Real world***	***Empirical (lab based)***	***Empirical (simulation)***	***Speculative (experts)***	***Speculative (author)***	***Speculative (users)***
Bergmann, Gerdes, Schafer, Junge, and Bormann (2012), [35] Denning, Matuszek, Koscher, Smith, and Kohno (2009); [36] Rahman, Carbunar, and Banik (2013); [37] Hoang and Pishva (2015); [38] Mosenia, Sur-Kolay, Raghunathan, and Jha (2017); [39] Obermaier and Hutle (2016)							

REFERENCES

Agadakos, I., Chen, C.-Y., Campanelli, M., Anantharaman, P., Hasan, M., Copos, B., … Lindqvist, U. (2017). Jumping the Air Gap: Modeling Cyber-Physical Attack Paths in the Internet-of-Things. In *CPS-SPC'17* (Vol. 17). https://doi.org/10.1145/3140241.3140252

Ahmad, W., Sunshine, J., Kaestner, C., & Wynne, A. (2015). Enforcing fine-grained security and privacy policies in an ecosystem within an ecosystem. In *Proceedings of the 3rd International Workshop on Mobile Development Lifecycle* (pp. 28–34). https://doi.org/10.1145/2846661.2846664

Aktypi, A., Nurse, J. R. C., & Goldsmith, M. (2017). Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks. In *Proceedings of the 2017 on Multimedia Privacy and Security* (pp. 1–11). Dallas, TX, USA.

Amin, S. M., & Giacomoni, A. M. (2012). Smart Grid-Safe, Secure, Self-Healing. *IEEE Power & Energy Magazine*, *10*(Jan/Feb 2012), 33–40. https://doi.org/10.1109/MPE.2011.943112

Anand, S. A., & Saxena, N. (2016). Vibreaker: Securing Vibrational Pairing with Deliberate Acoustic Noise. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (pp. 103–108). https://doi.org/10.1145/2939918.2939934

Arabo, A. (2015). Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science*, *61*, 227–232. https://doi.org/10.1016/j.procs.2015.09.201

Bachy, Y., Basse, F., Nicomette, V., Alata, E., Kaaniche, M., Courrege, J. C., & Lukjanenko, P. (2015). Smart-TV Security Analysis: Practical Experiments. In *Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Smart-TV* (pp. 497–504). https://doi.org/10.1109/DSN.2015.41

Bergmann, O., Gerdes, S., Schäfer, S., Junge, F., & Bormann, C. (2012). Secure bootstrapping of nodes in a CoAP network. In *2012 IEEE Wireless Communications and Networking Conference Workshops* (pp. 220–225). https://doi.org/10.1109/WCNCW.2012.6215494

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017a). An analysis of malicious threat agents for the smart connected home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, 557–562. https://doi.org/10.1109/PERCOMW.2017.7917623

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017b). On privacy and security challenges in smart connected homes. *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*, 172–175. https://doi.org/10.1109/EISIC.2016.044

Chen, D., Kalra, S., Irwin, D., Shenoy, P., & Albrecht, J. (2015). Preventing Occupancy Detection from Smart Meter Data. *IEEE Transactions on Smart Grid*, *6*(5), 2462–2434.

Chen, Y., & Luo, B. (2012). S2A: Secure Smart Household Appliances. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (pp. 217–228). https://doi.org/10.1145/2133601.2133628

Copos, B., Levitt, K., Bishop, M., & Rowe, J. (2016). Is Anybody Home? Inferring Activity from Smart Home Network Traffic. In *Security and Privacy Workshops (SPW)* (pp. 245–251). IEEE. https://doi.org/10.1109/SPW.2016.48

Coppolino, L., Dalessandro, V., Dantonio, S., Levy, L., & Romano, L. (2015). My smart home is under attack. In *IEEE 18th International Conference on Computational Science and Engineering* (pp. 145–151). https://doi.org/10.1109/CSE.2015.28

Denning, T., Matuszek, C., Koscher, K., Smith, J. R., & Kohno, T. (2009). A spotlight on security and privacy risks with future household robots. In *Proceedings of the 11th international conference on Ubiquitous computing* (pp. 105–114). ACM. https://doi.org/10.1145/1620545.1620564

Fafoutis, X., Marchegiani, L., Papadopoulos, G. Z., Piechocki, R., Tryfonas, T., & Oikonomou, G. (2017). Privacy leakage of physical activity levels in wireless embedded wearable systems. *IEEE Signal Processing Letters*, *24*(2), 136–140. https://doi.org/10.1109/LSP.2016.2642300

Feng, X., Ye, M., Swaminathan, V., & Wei, S. (2017). Towards the Security of Motion Detection-based Video Surveillance on IoT Devices. In *Proceedings of the on Thematic Workshops of ACM Multimedia 2017* (pp. 228–235). ACM. https://doi.org/10.1145/3126686.3126713

Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. In *IEEE Symposium on Security and Privacy Security* (pp. 636–654). https://doi.org/10.1109/SP.2016.44

Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017). Security Implications of Permission Models in Smart-Home Application Frameworks.

IEEE Security & Privacy, *15*(2), 24–30.

Ganguly, P., Poddar, S., Dutta, S., & Nasipuri, M. (2016). Analysis of the Security Anomalies in the Smart Metering Infrastructure and Its Impact on Energy Profiling and Measurement. In *5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*.

Greensmith, J. (2015). Securing the Internet of Things with Responsive Artificial Immune Systems. In *Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation* (pp. 113–120). https://doi.org/10.1145/2739480.2754816

He, J., Xiao, Q., He, P., & Pathan, M. (2017). An Adaptive Privacy Protection Method for Smart Home Environments Using Supervised Learning. *Future Internet*, *9*(1), 7. https://doi.org/10.3390/fi9010007

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security* (pp. 461–472). https://doi.org/10.1145/2897845.2897886

Hoang, N. P., & Pishva, D. (2015). A TOR-based anonymous communication approach to secure smart home appliances. In *International Conference on Advanced Communication Technology, ICACT* (Vol. 3, pp. 517–525). https://doi.org/10.1109/ICACT.2015.7224918

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Kang, W. M., Moon, S. Y., & Park, J. H. (2017). An enhanced security framework for home appliances in smart home. *Human-Centric Computing and Information Sciences*, *7*(1), 6. https://doi.org/10.1186/s13673-017-0087-4

Kermani, M. M., Zhang, M., Raghunathan, A., & Jha, N. K. (2013). Emerging Frontiers in Embedded Security. In *26th International Conference on VLSI Design and the 12th International Conference on Embedded Systems* (pp. 203–208). IEEE. https://doi.org/10.1109/VLSID.2013.222

Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Communications Surveys & Tutorials*, *16*(4), 1933–1954. https://doi.org/10.1109/COMST.2014.2320093

Lee, M., Lee, K., Shim, J., Cho, S., & Choi, J. (2016). Security threat on wearable services: Empirical study using a commercial smartband. In *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCE-Asia.2016.7804766

Liu, Y., Hu, S., & Ho, T. (2016). Leveraging Strategic Detection Techniques for Smart Home Pricing Cyberattacks. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 220–235.

Liu, Y., Hu, S., & Ho, T. Y. (2015). Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. In *IEEE/ACM International Conference on Computer-Aided Design,* (pp. 183–190). https://doi.org/10.1109/ICCAD.2014.7001350

Liu, Y., Hu, S., Wu, J., Shi, Y., Jin, Y., Hu, Y., & Li, X. (2015). Impact assessment of net metering on smart home cyberattack detection. In

Proceedings of the 52nd Annual Design Automation Conference (p. 97). New York, New York, USA: ACM Press. https://doi.org/10.1145/2744769.2747930

Liu, Y., Hu, S., & Zomaya, A. Y. (2016). The Hierarchical Smart Home Cyberattack Detection Considering Power Overloading and Frequency Disturbance. *IEEE Transactions on Industrial Informatics*, *12*(5), 1973–1983. https://doi.org/10.1109/TII.2016.2591911

Liu, Y., Zhou, Y., & Hu, S. (2017). Combating Coordinated Pricing Cyberattack and Energy Theft in Smart Home Cyber-Physical Systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *37*(3), 573–586. https://doi.org/10.1109/TCAD.2017.2717781

Lo, C.-H., & Ansari, N. (2013). CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid. *IEEE Transactions on Emerging Topics in Computing*, *1*(1), 33–44. https://doi.org/10.1109/TETC.2013.2274043

Lotfy, K., & Hale, M. L. (2016). Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things. In *2016 IEEE International Conference on Mobile Services (MS)* (pp. 25–32). IEEE. https://doi.org/10.1109/MobServ.2016.15

Lyu, M., Sherratt, D., Sivanathan, A., Gharakheili, H. H., Radford, A., & Sivaraman, V. (2017). Quantifying the reflective DDoS attack capability of household IoT devices. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks - WiSec '17* (pp. 46–51). https://doi.org/10.1145/3098243.3098264

Min, B., & Varadharajan, V. (2015). Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT). In *20th*

International Conference on Engineering of Complex Computer Systems (ICECCS) (pp. 80–89). IEEE. https://doi.org/10.1109/ICECCS.2015.19

Mosenia, A., Sur-Kolay, S., Raghunathan, A., & Jha, N. K. (2017). DISASTER: Dedicated Intelligent Security Attacks on Sensor-Triggered Emergency Responses. *IEEE Transactions on Multi-Scale Computing Systems*, *3*(4), 255–268. https://doi.org/10.1109/TMSCS.2017.2720660

Murillo, M. (2016). On Vulnerabilities of IoT-Based Consumer-Oriented Closed-Loop Control Automation Systems. In *Cyber-Assurance for the Internet of Things* (pp. 187–208). Hoboken, NJ, USA: John Wiley & Sons, Inc. https://doi.org/10.1002/9781119193784.ch7

Obermaier, J., & Hutle, M. (2016). Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security - IoTPTS ’16* (pp. 22–28). New York, New York, USA: ACM Press. https://doi.org/10.1145/2899007.2899008

Oluwafemi, T., Kohno, T., Gupta, S., & Patel, S. (2013). Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of Home Automation Security. In *Proceedings of the LASER 2013 (LASER 2013)* (pp. 13–24).

Park, H., Basaran, C., Park, T., & Son, S. (2014). Energy-Efficient Privacy Protection for Smart Home Environments Using Behavioral Semantics. *Sensors*, *14*(9), 16235–16257. https://doi.org/10.3390/s140916235

Rahman, M., Carbunar, B., & Banik, M. (2013). Fit and vulnerable: Attacks and defenses for a health monitoring device," in Proceedings of the 6th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs).

Reichherzer, T., Timm, M., Earley, N., Reyes, N., & Kumar, V. (2017). Using machine learning techniques to track individuals & their fitness activities. In *Proceedings of the 32nd International Conference on Computers and Their Applications, CATA 2017* (pp. 119–124).

Sanchez, I., Satta, R., Fovino, I. N., Baldini, G., Steri, G., Shaw, D., & Ciardulli, A. (2014). Privacy leakages in Smart Home wireless technologies. In *2014 International Carnahan Conference on Security Technology (ICCST)* (pp. 1–6). IEEE. https://doi.org/10.1109/CCST.2014.6986977

Schurgot, M. R., Shinberg, D. A., & Greenwald, L. G. (2015). Experiments with security and privacy in IoT networks. *Proceedings of the WoWMoM 2015: A World of Wireless Mobile and Multimedia Networks*. https://doi.org/10.1109/WoWMoM.2015.7158207

Snader, R., Kravets, R., & Harris III, A. F. (2016). CryptoCop: Lightweight, energy-efficient encryption and privacy for wearable devices. *2nd ACM Workshop on Wearable Systems and Applications, WearSys 2016*, 7–12. https://doi.org/10.1145/2935643.2935647

Srinivasan, V., Stankovic, J., & Whitehouse, K. (2008a). A fingerprint and timing-based snooping attack on residential sensor systems. *ACM SIGBED Review*, *5*(1), 1–2. https://doi.org/10.1145/1366283.1366311

Srinivasan, V., Stankovic, J., & Whitehouse, K. (2008b). Protecting your daily in-home activity information from a wireless snooping attack. *Proceedings of the 10th International Conference on Ubiquitous Computing - UbiComp '08*, 202.

https://doi.org/10.1145/1409635.1409663

Tekeoglu, A., & Tosun, A. S. (2015a). A closer look into privacy and security of Chromecast multimedia cloud communications. In *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 121–126). IEEE. https://doi.org/10.1109/INFCOMW.2015.7179371

Tekeoglu, A., & Tosun, A. Ş. (2015b). Investigating security and privacy of a cloud-based wireless IP camera: NetCam. *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, *2015–Octob*. https://doi.org/10.1109/ICCCN.2015.7288421

Torre, I., Koceva, F., Sanchez, O. R., & Adorni, G. (2017). Fitness Trackers and Wearable Devices: How to Prevent Inference Risks? In *Proceedings of the 11th International Conference on Body Area Networks*. EAI. https://doi.org/10.4108/eai.15-12-2016.2267791

Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber Security Threats to IoT Applications and Service Domains. *Wireless Personal Communications*, *95*(1), 169–185. https://doi.org/10.1007/s11277-017-4434-6

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research*, *4*(1), 18. https://doi.org/10.1007/s40309-016-0107-z

Tzezana, R. (2017). High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things. *Foresight*, *19*(1), 1–14. https://doi.org/10.1108/FS-11-2016-0056

Vemi, S. G., & Panchev, C. (2015). Vulnerability testing of wireless access points using Unmanned Aerial Vehicles (UAV). In *Proceedings of the European Conference on e-Learning* (p. 245).

Vigo, R., Yuksel, E., & Dewi Puspa Kencana Ramli, C. (2012). Smart grid security a Smart Meter-centric perspective. In *2012 20th Telecommunications Forum (TELFOR)* (pp. 127–130). IEEE. https://doi.org/10.1109/TELFOR.2012.6419164

Xu, H., Sgandurra, D., Mayes, K., Li, P., & Wang, R. (2017). *Analysing the Resilience of the Internet of Things Against Physical and Proximity Attacks* (Vol. 10658). https://doi.org/10.1007/978-3-319-72395-2

Yoshigoe, K., Dai, W., Abramson, M., & Jacobs, A. (2016). Overcoming invasion of privacy in smart home environment with synthetic packet injection. *Proceedings of 2015 TRON Symposium, TRONSHOW 2015*, *1*(C). https://doi.org/10.1109/TRONSHOW.2014.7396875