To be published in the International Workshop on Secure Internet of Things 2015 (SIoT 2015) in conjunction with the European Symposium on Research in Computer Security (ESORICS 2015).

Smart Insiders: Exploring the Threat from Insiders using the Internet-of-Things

Jason R.C. Nurse, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, Sadie Creese
Cyber Security Centre, Department of Computer Science,
University of Oxford, UK
{*firstname.lastname*}*@cs.ox.ac.uk*

***Abstract*—The Internet-of-Things (IoT) is set to be one of the most disruptive technology paradigms since the advent of the Internet itself. Market research company Gartner estimates that around 4.9 billion connected things will be in use in 2015, and around 25 billion by 2020. While there are substantial opportunities accompanying IoT, spanning from Healthcare to Energy, there are an equal number of concerns regarding the security and privacy of this plethora of ubiquitous devices. In this position paper we approach security and privacy in IoT from a different perspective to existing research, by considering the impact that IoT may have on the growing problem of *insider threat* within enterprises. Our specific aim is to explore the extent to which IoT may exacerbate the insider-threat challenge for organisations and overview the range of new and adapted attack vectors. Here, we focus especially on (personal) devices which insiders bring and use within their employer's enterprise. As a start to addressing these issues, we outline a broad research agenda to encourage further research in this area.**

***Index Terms*—Internet-of-things security; smart devices; wearables; insider threat; enterprise attack vectors; research agenda**

I. Introduction

Technology features in every part of our lives, from tasks at work and social activities at home to supporting large industries and governments. In effect, technology drives our world. Over recent years, there have been several significant advances in technology ranging from the Internet and the Web, to the diffusion of connected mobile devices on a substantial scale. Today estimates suggest that there are around 14.3 trillion pages online serving billions of users across a similar number of devices spanning the globe [1]. It is this idea of Internet-connected devices that has given rise to the grander idea of the Internet-of-Things. The Internet-of-Things (IoT) is a technology paradigm aiming towards increasing the connectivity of everyday devices [2]. The difference with IoT as compared to previous incarnations (e.g., ubiquitous computing) is that the technologies themselves and the accompanying data science have matured to a point where the vision is fast becoming a reality. There are now intended applications in Energy with the creation of smart grids, Manufacturing towards smarter production and assembly lines, Healthcare to facilitate enhanced monitoring and treatment, and Buildings in the creation of smart homes, offices and cities [3, 4].

As the IoT has increased in popularity, so too has the emphasis on its security and privacy in research and practice. There have been numerous articles outlining the key concerns and challenges across the spectrum of IoT components (e.g., sensors, embedded chips, wireless communication systems, etc.), some with proposals for potential solutions [5–7]. Reflecting on these and other articles, it is evident that there is an overwhelming emphasis on protecting devices and their communications from unauthorised access, hacking and exposure of sensitive information to external malicious parties. In contrast, there is little deliberation on the potential attacks from *insiders* within a system (e.g., an organisation), and the harm that they might intentionally or inadvertently cause.

Insider threats occur when individuals within an organisation misuse their privileged access to cause a negative impact on the confidentiality, integrity or availability of the organisations' systems [8]. The seriousness of the threat from insiders is well known and has been documented in several real-world cases and explored extensively in research [8–10]. We believe that this threat has the potential to become significantly more challenging for organisations to manage in a world of IoT, where everything is a device that may be used to access, store and share sensitive company data; this is a belief shared by many others [11]. In some sense, all devices can be 'insiders' as the traditional perimeters are now so nebulous that it makes little sense not to consider everything as potentially having authorised access. This fact makes understanding how to manage the risk emanating from insiders in IoT environments exceptionally important. Unfortunately, at this point little detailed analysis of this risk has been conducted.

The aim of this paper is therefore to begin a critical, academic discussion on the adapted threat that insiders may pose in the context of IoT. We specifically seek to explore the extent to which IoT may exacerbate the insider-threat challenge and complicate detection approaches, by investigating the range of attacks that may be possible with IoT devices used by insiders. This research aims to focus on the current state of play but also seeks to be forward-looking in considering emerging threats, and thus, identifying areas for additional research.

This paper is structured as follows: Section II reflects on the nature of IoT, with a focus on the general security and privacy issues with this new technology. Next, Section III examines the threat from insiders, including the state-of-the-art in current research. Section IV builds on the work in the previous sections and aims to explore how IoT, and particularly personal IoT devices used by insiders, may exacerbate the insider-threat challenge. In Section V we consider the range of

To be published in the International Workshop on Secure Internet of Things 2015 (SIoT 2015) in conjunction with the European Symposium on Research in Computer Security (ESORICS 2015).

attack vectors enabled and those made much easier for insiders through the use of IoT devices. We present a brief research agenda in Section VI to identify areas for future work, before concluding in Section VII.

II. The Internet-of-Things and security and privacy

A. The IoT paradigm

The Internet-of-Things (IoT) can be defined as a networked infrastructure composed of billions of identifiable 'things' interacting and communicating with each other to achieve common goals. Today this is a growing reality through the integration of several enabling technologies [2, 12], which can be classified in three layers: hardware, middleware and application. The hardware layer is composed of all the physical devices present on the network. Some examples are wearable technology, smartphones, sensors and devices with Radio Frequency Identification (RFID) tags, and wireless (e.g., Bluetooth, ZigBee, WiFi) connections. These devices can all be characterised in three working processes: identification, sensors and communication. While the application layer is the software used to visualise, interpret or process the necessary data, the middleware is an intermediate software layer that bridges hardware and applications. Middleware has the crucial role of facilitating the implementation of new software and services without much concern as to the hardware that is used at the lower layers.

Although there has been significant work in these enabling layers, there is still a large amount of research and development in progress to enable more effective use and broader adoption of IoT. One of the key challenges at this point is achieving high interoperability between devices; a difficulty due to the high level of device heterogeneity. Moreover, because of the constrained resources of these devices, there are a number of new security and privacy challenges as will be discussed below.

B. Security and privacy issues

The unique nature of IoT with numerous devices of limited capabilities (processing, power and memory constraints) constantly interacting, makes IoT especially vulnerable to attacks. Devices are susceptible to physical attacks if protection is not provided, regardless of whether this is due to economic reasons, device limitations or carelessness [13]. Remote sensors without protection, unlocked devices (e.g., smartphones), unsecure communications or removable media (e.g., camera card) are just a few examples.

Along with the intensive network communications necessary with IoT come conventional Internet security and privacy problems. These are accentuated by the fact that IoT devices tend to implement less secure primitives due to their capability constraints. An example is the use of insecure remote login methods [2]. Another concern is that secure and reliable devices do not naturally result in a secure system. The process of combining and configuring the interactions between devices and resulting systems also has a bearing on security. This is particularly important in IoT where devices can often switch between host networks. In what follows, we reflect on a few of the major security and privacy issues in IoT.

1) Security: Security in IoT relies on many different factors, but in particular, considers maintaining the confidentiality, integrity and availability of systems and data [6].

Confidentiality in IoT, much like general information security, refers to the creation of a private channel of communication between devices. The major difference with the IoT paradigm is the limited resources on devices affecting their ability to implement standard cryptographic protocols. To address this problem, a number of Key Management Systems protocols and security frameworks have been proposed [14]. Unfortunately, their acceptance has been very limited and as such, there are continued calls for further, more applied research in this area [5].

Maintaining the integrity of data, IoT services and devices requires mechanisms which prevent the modification of data, whether it be on the device or during communications. Solutions proposed for device and data integrity include secure boot and the creation of access control policies referring to trusted identities and credentials [7]. For data in transit, traditional mechanisms to prevent attacks (such as man-in-the-middle) could be used, but the challenge here is when devices broadcast information without partnering devices (e.g., sensors network), and the attacks that could accompany such communications [6].

Finally, IoT services must be available when called upon by authorised parties. This includes ensuring that communication channels are protected, and IoT devices and services are resistant to denial-of-service (DoS) attacks. A common solution to prevent abuse is the use of authentication mechanisms associated with usage quotas. However, the ad-hoc nature of IoT makes it essential to provide authentication mechanisms able to create trust when devices have no previous knowledge of each other and the services that may be on offer [15]. Compromised IoT devices can also be a serious problem as they can be used to launch DoS attacks against wider systems (e.g., attacks via smart home devices [16]).

2) Privacy: Privacy in IoT can be assured by giving people and devices control over the data they generate. This scenario is feasible in a decentralised topology, where devices are likely to have control over their own data and share this with other devices they trust. In centralised scenarios where a single device manages the data, trust will typically only need to be placed in that entity to maintain data privacy. Another significant challenge which IoT creates is that of unwanted tracking and monitoring [5]. Surveillance, even from individuals or organisations, becomes a real issue and potentially one that could threaten not only privacy but an individual's well-being (e.g., connected health devices). There is also the issue of user and usage profiling threats and their impact on an individual's privacy. A subset of these issues has been considered in existing research, with some articles (e.g., [17,18]) proposing new privacy models to support broader IoT concepts such as smart cities.

III. The state-of-the-art in insider threat

A. Scoping the insider-threat problem

Insider threat is an ever-growing problem for organisations. The in-depth knowledge that insiders possess of the security practices and monitoring policies, places organisations in dire situations if these attacks are executed. As such, detecting insiders is a significant challenge, and one which has attracted the interest of researchers for over a decade. Insightful discourses have been ranging from recognising elements in attacks [10] and identifying behavioural factors [19], to the detection of anomalies indicative of suspicious and malicious insider activity [19, 20].

A pioneering effort to assess insider attacks was the CMU-CERT Insider Threat project [10]. They classified insider threats into four categories, namely sabotage, Intellectual Property (IP) theft, data and financial fraud, and espionage. Using System Dynamics as a framework, they identified and described 'critical paths' which most insiders follow in a series of MERIT (Management and Education of the Risk of Insider Threat) models, isolating suspicious behaviour. In addition, they distinguished between insiders who act maliciously and those who facilitate an attack unintentionally or expose their organisation to unnecessary risk, either by violating policies (to facilitate their daily activities) to or by being careless (victims of phishing attacks) [21].

Similar frameworks elaborate on factors which may be considered as precursors of an attack, by focusing on capability, motivation and opportunity as key attributes of an insider threat [9], or by examining attributes related to the organisation and environment [22]. We have also contributed to this discussion by developing a framework to capture the full insider-threat spectrum. Our framework defines why insiders attack (catalysts, motivations, personality aspects), behaviours indicative of a current or impending attack (both physical and cyber), and core assets and vulnerabilities which are usually exploited in these attacks [8].

B. Reflecting on current detection research

A different strand of research has focused on developing systems to detect insider attacks. For instance, researchers have explored data from organisations' databases regarding activities on employees' laptops [23]. They applied seventeen different algorithms for anomaly detection, which were adjusted on recognising well-established malicious behaviour, to identify if these techniques were efficient in capturing inside activity. In addition, they provided a visual language for illustrating features, baselines and peer groups relevant to insider threat. In a similar vain, Eldardiry *et al.* describe how to extract features from employees' activities and suggest a detection system which processes these features to identify deviations [24].

Parveen *et al.* detail an unsupervised learning algorithm which develops a set of sequences from dynamic data streams denoting insider-threat behaviour [25]. The unsupervised learning techniques endeavour to define common behaviour and provide the means to distinguish data streams containing uncommon, thus potentially malicious behaviours. Chen *et al.* [26] use similar unsupervised learning techniques to identify insider threats. Their system processes information from recorded access logs and performs statistical analysis to calculate deviations of users' activities.

Other frameworks have tried to incorporate psychological and behavioural factors into anomaly detection algorithms. Magklaras and Furnell [27] build profiles of users' behaviour and evaluate how these may determine the level of threat that could arise from a particular insider. Legg *et al.* [28] describe a three-tier alert system to indicate suspicious behaviours. The first level of alerts detects violations on corporates' policies, the second level is based on calculating anomalies (i.e., values exceeding a certain threshold) in specific employees' behaviours (e.g., login anomalies) by assessing more than one hundred features, and the third level of alerts detects deviations from the user's normal profile.

The vast majority of the systems proposed today are driven by the data available to perform anomaly detection. Thus, the effectiveness of these systems is limited to specific types of insider attacks and to particular aspects of network activity. The mainstream datasets used analyse information on insider email communication, file access logs and Web activity, and focus primarily on workstations instead of data from portable devices which could be connected to the network. Furthermore, information from abstract models regarding the motivation of the attackers and the behavioural aspects exhibited during these attacks is not considered by detection systems, due to challenges in linking cyber behaviour with personality traits. To our knowledge, there is not a detection approach or system which accommodates data generated from devices considered part of IoT or incorporating data regarding insiders' behaviour. This is an interesting challenge given the uniqueness of attacks possible with IoT (as enumerated below), and the large volume of data generated via IoT devices which can have an impact on the efficiency and applicability of current detection methods.

IV. The challenge with IoT and insider threats

Thus far in this article, we have engaged in a state-of-the-art review of two key aspects that impact organisations today. From this analysis, it is clear that in both of these areas there are still significant challenges to be addressed. In IoT, research is in progress on everything from the standardisation of protocols to the deployment of effective security measures. Research on insider threats is much more advanced than in IoT but as shown in Section III, how to adequately detect and respond to attacks are still unsolved problems.

As we move into a world where IoT is a natural part of people's lives, businesses face a remarkable challenge in understanding and addressing the associated risks and protecting themselves from the range of new insider attacks (malicious and unintentional). The novelty of these attacks is not what they target, but rather, the ease with which they can be launched and through the use of devices likely unknown,

possibly undetectable, and certainly unmanaged by the enterprise. Here, and for the remainder of this section, we scope our work especially to personal IoT devices such as wearables (e.g., smart-watches, smart-glasses, activity trackers) and smart devices including phones, displays and pens. These are largely unexplored areas in terms of insider attacks and as such, deserve more academic and industrial emphasis.

In examining the challenge of IoT use in organisations, it would be prudent to consider other similar paradigms and the impact that they have had on enterprises. One such paradigm is Bring Your Own Device (BYOD). BYOD represented a fundamental shift in corporate computing where employees were allowed, and even encouraged, to bring their personal devices (e.g., laptops, tablets, smartphones) to the workplace and use them for work activities including accessing company systems, files and data [29]. The main driving forces of BYOD from an enterprise perspective are cost and efficiency. Specifically, employers could provide less office technology, while also benefiting from the newer, likely more feature-rich personal devices that are with employees at work and at home.

Since its inception however, BYOD has been plagued with several challenges, particularly as it pertains to the security of enterprise systems and data, and the privacy of individual's personal information [30]. Data leakage (via stolen, lost or compromised devices), malware (i.e., compromised personal devices infecting corporate networks) and distributed denial-of-service (DDOS) attacks are three of the main insider-threat concerns for organisations. In response to this risk, companies have introduced a range of BYOD policies, and where possible, backed them with Mobile Device Management (MDM) solutions capable of remote device management (including functions such as compartmentalisation of sensitive data and remote data wipe). Nonetheless, even with these strategies in place, reports highlight that current employee behaviour (whether accidental or intentional) still significantly contributes to the struggle enterprise IT has in dealing with BYOD [31, 32].

In terms of the use of IoT within organisations, unfortunately there are numerous of the same security and privacy challenges faced by BYOD, but fewer of the advantages. One of the main reasons for this was mentioned in Section II and relates to the fact that a vast majority of these devices have limited processing and storage capabilities, thus making them not ideal for typical work-related tasks. They can however, be compromised in the same way as BYOD, especially considering their constrained security setups [33, 34]. Furthermore, as some of them can connect to the network (e.g., Google Glass, Samsung Gear S smart-watch, Livescribe WiFi smart-pen), they could be capable of infecting corporate servers, or being used as an insider-based platform for further attacks.

The challenge with IoT is exacerbated by the number and variety of devices that will enter the enterprise, many of which employees will attempt to connect (directly or indirectly) to the corporate network to maintain Internet connectivity. From a malicious insider perspective, these devices provide yet another pathway to attack, and one which is arguably much harder for organisations to detect. This is a concerning factor given that detection on existing systems is not a solved problem [8, 10], and to our knowledge there are no detection systems which accommodate for data generated from IoT devices. The added difficulty with IoT could also be attributed to the wide variety of these devices — any 'thing' might be connected next — and the fact that due to advances in technology, these devices can often be easily and discretely concealed (e.g., smart-pens, life-logging cameras).

To consider the unintentional insider threat and situations such as lost, stolen or compromised devices, MDM-type solutions for IoT might seem ideal. However, given (a) the limitations in processing power of these devices and (b) the privacy concerns surrounding monitoring data on these highly personal devices (i.e., wearables and smart systems), such solutions are likely to be generally infeasible. Moreover, if Gartner is to be believed, a notable number of organisational BYOD policies will fail over the next few years due to MDM solutions that are too restrictive and not accommodating to employees' privacy requirements and general needs [35].

Thus far we have outlined the challenge facing the use of IoT within organisations and how such use could facilitate insider threats. Next, we introduce the attack vectors and the context surrounding attacks, followed by a detailed presentation of some of these vectors (including initial thoughts about mapping such vectors to existing attack taxonomies [36]) and case examples of their exploitation.

V. Understanding and defining the attack vectors

A. Introducing attack vectors and the context of attacks

An attack vector defines the means through which a threat may compromise the security of a system or its data. As a first step to protecting a system, it is advantageous to understand the vectors of attack and their context (e.g., what is the asset being threatened, what might be the impact of the attack). To define these aspects and structure our analysis, we apply the A^4 modelling approach used by VERIS to describe cyber incidents [37]. This approach considers four key *A*s in defining attacks, namely assets, actors, attributes, and actions.

Assets are items of value to an enterprise, and can include data (e.g., company files, client or supplier records, business plans, source code), IP, systems and hardware, personnel and even the reputation of the organisation. Any of these could be affected either directly or indirectly by an attack. *Actors* define the individuals that launch the attack against the asset. As discussed in Section III, there are two broad types of actor: the malicious insider and the unintentional insider. Both of these entities can have a significant impact on the enterprise.

Attributes capture the impact of the attack on the asset. There are at least 5 areas of interest here: data access, data exfiltration, data leakage, system sabotage and reputation or employee harm. These areas can be associated with the high-level goals of an insider, i.e., sabotage, IP theft, fraud, and espionage. For instance, an insider may steal sensitive company data and share with an outsider for a financial sum, thus committing IP theft. *Actions* specify the steps involved

in attacking an asset. A combination of these steps constitutes the insider-attack vector. It is important to note that not all of the actions involved might be malevolent, and often it is the last step which truly identifies the attack.

The first three of these areas (or *A*s) provide useful context for an attack (which is defined in the fourth area). In particular, they help an organisation to understand and model key details about the perpetrators of the attack (and their motives), identify the assets affected and assess the impact of the attack.

B. Defining attack vectors

There has been a notable amount of isolated research on attack vectors in IoT ([7]) and within insider threat ([10]). There is little academic analysis or thought however, on cases where personal IoT devices can be used to craft novel and hard to detect insider attacks. Our aim here is to define and present several forms of attack, with the overarching goal of drawing attention to the real challenges that enterprises (will) face as consumer technology permeates the workplace.

The number of personal IoT devices used within enterprises via employees with wearables or smart devices is constantly growing. A preliminary list of such devices includes: smartphones, tablets, smart-glasses, smart-watches, smart-pens, activity trackers, life-logging devices and apps, and smart-displays; smart-contact lenses may also be on the way [38]. Although different devices, they all overlap in functionality. For instance, smart-glasses and smartphones have cameras that can take pictures and record video. Our attack vectors, of which we only present a few of the most salient ones here, are therefore structured around the features these devices have rather than the devices themselves. Below, we present the vectors according to the broad types of attacker; it should be noted however, that depending on the specific scenario these may vary. We then briefly consider these vectors in the context of existing attack taxonomies.

Attack vectors (AV) of malicious insiders (MI)

MI-AV1: Using a smart-device camera, the insider discretely takes a video of another employee entering their login credentials into a system and then subsequently analyses the video to determine those details. This is a variation on the traditional shoulder-surfing attack. A semi-automated version of this attack using IoT devices can be seen in [39]. [*Applies to any device with a camera.*]

MI-AV2: Using a smart-device camera, the insider discretely takes a photo or video of sensitive organisational data or IP and then intentionally shares it with a third-party (e.g., competitor or nation state). This sharing could also be in the context of the insider taking this data with them to a new job in another organisation. The real issue with such an attack is that it offers an effective alternative to techniques such as email-based data exfiltration (likely to be detected by firewalls) or data copying via external drives (detectable by most anomaly detection systems). [*Applies to any device with a camera.*]

MI-AV3: Using the audio recorder on a smart device, the insider discretely records a private conversation or meeting with a colleague, collaborator, supervisor or business partner, and uses it later to blackmail them into assisting in a more comprehensive attack (e.g., sabotaging a system via planting a logic bomb, where the coerced employee helps cover tracks). Alternately, the insider may choose to leak the recording immediately to a third-party (e.g., a competitor or the media). [*Applies to any device with an audio recorder.*]

MI-AV4: Using the storage system on a smart device, the insider is able to copy sensitive data (e.g., IP or files) from the organisation's computers to the device and remove it from the enterprise. Bluetooth or NFC may be preferred for this attack as organisations now tend to monitor USB connections. [*Applies to any device with a storage capability.*]

MI-AV5: Using a smart device, the insider discretely scans sensitive items (e.g., contactless ID or bank cards) belonging to the organisation's customers or suppliers during a transaction. Through this scanning, the insider is able to skim sensitive data about the individual (e.g., card numbers or names) which could then be taken out of the enterprise, potentially being sold to a third party. Performing this task is not trivial, but research has shown that it is possible [40, 41]. [*Applies to any device with a device scanner (e.g., NFC) and storage capability.*]

MI-AV6: Using a smart device infected with malware (e.g., virus, backdoor, or trojan), the insider connects (e.g., using USB, Bluetooth, NFC or WiFi) to the organisation's network or computer infrastructure. The aim could be to infect the enterprise and set the foundation for a later attack either intentionally or unintentionally in the case where the insider is more focused on another task (e.g., charging their device) or assumes the infection will not spread to the network. Both cases result could in system sabotage (e.g., deleting computer files) or unauthorised access (e.g., a backdoor to access sensitive corporate files or intellectual property). [*Applies to any device with a storage capability.*]

MI-AV7: The insider creates/configures a smart device able to be used as a hardware-based backdoor into the organisation. They then disguise the device and secretly bring it into the organisation where it is installed and setup on the corporate network. This backdoor could be the platform for more directed attacks including passively collecting data or planting malicious scripts. A real example of how a smart device could be used as physical backdoor to office networks can be seen in [42]; this could help to adapt similar current attacks (e.g., insider KVM attacks [43]) and add a level of sophistication which makes them more difficult to detect. [*Applies to any device capable of acting as an access point.*]

MI-AV8: Using a smart device with a network analysis application installed, the insider connects to the WiFi network and then engages in full-scale, unauthorised network reconnaissance. This includes identifying the devices on the network (with MAC addresses and manufacturers), monitoring individual device connections to the network, scanning the devices for open ports, and pinging devices. The insider could use this data in an attempt to compromise specific devices or disrupt their services, or leak the data online for anyone to view. One existing and freely available network analysis

application is Fing - Network Tools [44]. [*Applies to any device with capable of polling a network.*]

Attack vectors caused by unintentional insiders (UI)

UI-AV1: Using a smart-device camera, the insider takes a photo or video of sensitive enterprise data or IP to use to work remotely, and then shares it with a third-party host (e.g., Google or Dropbox). This third-party account is then breached by a malicious entity resulting in the sensitive data being exposed. [*Applies to any device with a camera.*]

UI-AV2: Using a smart-device camera, the insider takes a photo or video of the office space, which unknown to them contains sensitive information (e.g., login details on a white-board – such as the case in [45]), and they then share it publicly (e.g., on social media). [*Applies to any device with a camera.*]

UI-AV3: An improperly configured or inadequately protected smart device is compromised by a malicious third-party, who then use the device's camera to view potentially sensitive information (including documents or meetings) and to spy on company employees. There are examples of how such attacks might be launched on devices such as Smart TVs with web cameras and Google Glass [46,47]. [*Applies to any device with a camera.*]

UI-AV4: Through accident or inability to properly use a smart device, the insider activates an audio feature (such as Siri or Google Now) which records part of a sensitive conversation and thus, exposes enterprise data to a third-party (Apple or Google in this case). If this third-party was to pass on this data (e.g., to an advertising agency) or the user's account was compromised (such data is typically saved in search logs), this sensitive data would be shared even more widely. [*Applies to any device with a camera.*]

UI-AV5: An improperly configured or inadequately protected smart device is compromised by a malicious third-party, who then accesses company data (e.g., emails, work calendars) cached on the device. Two variations on this attack include: (1) the third-party infecting the smart device and then using that device once inside the organisation to infect other devices; and (2) through hacking of smart devices which facilitate payments (e.g., via CurrentC or Apple Pay), an external attacker is able to steal company credit card details or make illegitimate charges. Regarding the latter point, some of these services have already been hacked, while there are concerns about the security of the others [48, 49]. [*Applies to any device with a storage (or data entry or payment) capability.*]

UI-AV6: Assume that an attacker was able to compromise an insider's improperly configured or inadequately protected location-tracking smart device (e.g, Garmin smart-watch) account and access the GPS or route logs. They could use this information to make inferences about potential company clients and suppliers, or prospective business partnerships (based on places visited by the individual). This knowledge may then be exposed with the aim of sabotaging such relationships or selling it to a competing company. [*Applies to any device with a location tracker.*]

UI-AV7: As a result of improperly configured or inadequately protected insider smart devices (e.g., a smart-watch and a paired smartphone), the communications channel between them is compromised by a malicious third-party. This party then gathers enterprise data via the notifications, schedules, messages synchronised across devices. Further detail on such attacks on wearables can be found in [50]. We note that this attack could be conducted by another insider as well. [*Applies to any device with a notification and storage capability.*]

UI-AV8: The theft, loss or exploitation of a smart ID device (potentially one issued by the company or a personal one granted with special permissions) used to access organisational data, office rooms, building facilities or property. In the case of theft or exploitation, this could be an attack launched by an external party aiming to gain unauthorised access to the enterprise, or by a malicious insider. An example of a related real-world attack which exploits the authentication mechanisms in smart devices and property can be viewed in [51]. [*Applies to any device with an access capability.*]

In addition to identifying various forms of attack, we conducted a preliminary investigation into the ability of existing attack taxonomies to model these threats. One of the main reasons for this was to determine whether pursuing a new taxonomy might be necessary, i.e., helpful in defining the insider threat IoT problem. Amongst the taxonomies considered, Howard and Longstaff's [36] was one of the most promising and this was ideal given its reputation. Their taxonomy identifies several key aspects that form a part of an attack (incident) including: Tools used, Vulnerabilities exploited, Actions taken, Assets targeted, and Unauthorised results. The real benefit of their model is in its encompassing nature at both the aspect and aspect-category level. This was such that for the most of the aspects, a number of their existing categories could apply, or be adapted to model insider IoT attacks. For instance, autonomous agents or malware can be launched (via an IoT device) to exploit some system configuration weakness in an enterprise system which leads to data being stolen.

There were some modifications necessary however, to be able to directly apply Howard and Longstaff's taxonomy to define insider IoT attacks. For the Tool aspect for instance, the existing categories (namely, physical attack, information exchange, user command, script, autonomous agent, toolkit, distributed tool or data tap) were unable to capture the range of attack means capable with IoT devices. We therefore added a new category called 'physical device functionality', with the sub-categories: camera, audio recorder, storage system, device scanner, network scanner, access point, and location tracker. Moreover, for the Actions aspect which possessed typical attack categories including scan, flood, read, steal and delete, we added a 'record' category. This category had picture taking, video recording and audio recording, as its main sub-categories; therefore, directly allowing many of the attack vectors enumerated above. For the Assets targeted aspect, the existing taxonomy was largely adequate, and as such we made only two additions to the categories, namely,

'personnel' and 'events' (e.g., meetings). These would allow for the consideration and modelling of intangibles (e.g., the secret recording of a private meeting using an IoT device) not considered in some attack assessments.

Through the modifications presented above, we were able to engage in an initial adaptation of an existing model for the purposes of creating a draft taxonomy, which is broad enough to capture insider IoT attacks. While this is a promising start, we must stress that this is preliminary work and will need to be assessed and evaluated in greater detail in future research. As more is understood about these attack vectors, this will lead to a more complete taxonomy, which in turn should lead to better detection approaches targeting these attacks.

C. Case studies of the attacks applied and the enterprise risk

This section builds on the research thus far, and presents two examples of the contexts in which such attacks might occur. These cover a malicious and an unintentional insider-threat scenario. Here, we deliberately consider attacks using current IoT devices to make this section more relatable, but future IoT could lead to much more sophisticated attacks.

1) Case study 1: Employee blackmail: A junior IT staff member for a small manufacturer was reprimanded by the company CEO because of claims that he was verbally abusing other employees. In reality, the CEO had an affair with an employee that the insider had been flirting with. After later discovering that he was likely to be dismissed, he prepared a plan to get revenge. He had read a report a few weeks earlier by the Bitdefender Research Team [52], which discussed the fact that it was possible to sniff and intercept the communication between a smart-watch and a smartphone. This was perfect as the CEO recently purchased a new smart-watch. The insider then used the report's knowledge and underground hacking forums to research how to collect communications data, and find weaknesses in poor Bluetooth encryption implementations that would allow access to the information. Amongst the equipment purchased, the insider even bought the same watch to trial the attacks. Once the attack was prepared, the insider launched it against the CEO, and was able to collect data on incoming phone calls, SMS and emails, and general calendar information; these were of a work and personal nature. Finally, the insider blackmailed the CEO with the information collected (some of which highlighted his affair), and threatened to share it with his wife and children unless he was given a large severance package and promised exemplary references.

Reflecting on the 4*A*s for this case, there are: *Assets*: Sensitive company and personal information; *Actors*: Malicious insider; *Attributes*: Unauthorised data access then used for blackmail and fraud; and *Actions*: Attack Vector – UI-AV7 (where an insider is the perpetrator). This case highlights a key weakness in IoT devices, i.e., the limited security features with these devices (as discussed in Section II) and a clever attack building on personal knowledge helped by current reports and malicious Web forums.

2) Case study 2: Malware infection: Sensitive company IP and personal data about several senior managers of an aeronautical firm was posted online. This led to damage in the company's reputation, a drop in its stock prices, and embarrassment to the managers and their family members. Upon investigation, the IT department of the enterprise discovered that some of the work-provided smartphones of those employees were infected by WireLurker and Mekie malware [53]. These malware monitor and collect data from any iOS device connected (via USB) to an infected OS X computer; WireLurker in particular, also can install downloaded third-party apps as well as automatically generated malicious applications onto the device. Given that the malware was found on several phones, IT checked all of the computers in the company and discovered that the computer in one of the meeting rooms was the source of the infection. That computer was extensively used by all managers to charge their phones and was used as media control during client presentations as well. A few managers even had allowed visitors to use the computer. IT concluded that one of the visitors may have placed the malware onto the machine and could be responsible for the attack (deliberate or not) and subsequent data leakage.

The 4*A*s for this case are: *Assets:* Sensitive company IP and personal information; *Actors:* Unintentional insider threat; *Attributes:* Damage to the reputation and standings of the enterprise and its senior employees; and *Actions:* Attack Vector – UI-AV5. The challenge with this case is the difficulty in protecting mobile devices from inadvertent compromise and being used as a platform for other attacks (e.g., data extraction). A core reality is that these devices often hold very important and, even in the cases of a work device, very personal data.

D. Insider IoT attacks of the future

Thus far, we have presented attacks largely possible with IoT devices available today. In this section, we take a step into the future to briefly consider attacks that may be possible in a world where IoT devices are commonplace, and a significant number of devices are connected. To begin, we start by outlining some details of an IoT smart office, and introduce the context of the attack case. Next, we present an insider attack that could be possible in this fully connected world.

The Case: A multinational technology company has opened its new headquarters, equipped with the latest technologies and IoT devices. The security of the building is a top priority, given that it is where they develop and house their most sensitive IP. With this in mind, in addition to all the sensors that ensure offices are eco-friendly (e.g., smart lights, displays) and highly convenient for employees, there are several wireless cameras and other smart devices to monitor employees. Access to the building is granted by a two-factor authentication using the corporate phone (NFC) and biometrics (fingerprint). No personal property is allowed to enter to the building and people are checked again at the exit. The company is especially concerned about any electronic device that might be used to steal IP. Smartphones are controlled by corporate IT, so

pictures cannot be taken of IP without their knowledge. The organisation has a largely in-house maintenance service that provides cleaning services, food and smart food equipment. Smart mugs connect via a local wireless network to coffee machines and kettles, and are all designed to have coffee ready for employee breaks. Smart mug warmers also keep coffee warm and recharge the batteries of the mug.

The Attack: A product engineer, frustrated with her slow career progress in the company, decides to steal designs for a new technology device (IP). As part of her plan she colludes with the smart mugs supplier to replace the mugs of the company with very similar ones. The new mugs are identical in appearance but they have been modified to incorporate a new WiFi promiscuous receiver that captures WiFi packets and stores them to the mug's internal memory. Every few months, the cleaners would take some of the dirty mugs off the company premises to replace their rechargeable batteries and bring in new ones (that have been specially cleaned); security officers would conduct spot checks of the mug shipments coming in, but never in great detail. The engineer had also modified the new mugs' battery management software to stop some of them from charging after a few weeks, thus speeding up the need to replace the mugs. As mugs were replaced, the insider would collect the old mugs from the cleaners and pay them for their help. Through this attack, the disgruntled engineer would be able to capture WiFi communications for many months, that then could be decrypted to discover sensitive information and possibly IP.

VI. Reflections and outline of a research agenda

The attacks outlined in Section V present a glimpse into the adapted threat from insiders possible with IoT. As was hinted in earlier sections, the real challenge with these attacks is that current insider-threat detection approaches are generally ill-prepared to address them. At the technical level for instance, different devices use numerous protocols and organisations' monitoring systems do not cater for such diversity. Moreover, collecting data on IoT devices and incorporating it into detection systems is a significant challenge, which also has several privacy implications. To make matters worse, many of the attack vectors presented in Section V involve recording data, but can be conducted without leaving any digital trace on enterprise systems (e.g., taking a photo of sensitive IP). At the social level, we have already witnessed companies struggle with creating a security-aware culture with BYOD [32]; this is likely to be significantly harder in the IoT world.

A key aspect that we re-emphasis here is that while a number of the attack vectors identified in this article are, in part, similar in type to BYOD attacks, there are crucial differences which make IoT a more significant problem. The most substantial difference is the IoT vision itself, which involves a vast variety of devices where any 'thing' (a light bulb, a tea cup, or a pair of shoes) could be connected and fully instrumented. This fundamentally blurs enterprise boundaries and perimeters, and is very different to any BYOD attack setup. With IoT, it is extremely difficult for organisations to collect, manage or assess data from devices because the perimeters (i.e., what is internal versus external) are constantly shifting. Our paper is grounded in current IoT devices to help elucidate the challenges with IoT and insider threats that exist today. In the future however, practically any device may be used as an attack platform, as we highlighted in Section V-D; this is the fast-approaching reality.

In what follows, we outline a broad research agenda focused on key problems in the IoT and insider-threat space, to encourage more directed research in this area. Going forward, it is imperative that organisations possess solutions, both technical and social/cultural, to address the emerging attack vectors from employees' use of IoT devices. The research community will play a critical role in this process and advances in this field.

One of the first important areas for research, is in comprehensively documenting and modelling IoT attack vectors, of which we outline an initial set in this paper, to aid in the understanding of this new threat. A central part of this process could be the complete definition (and evaluation) of an adapted taxonomy for insider attacks using IoT devices; this would build on our initial work in this paper regarding Howard and Longstaff's [36] model. Such a taxonomy would create a standardised foundation for modelling and threat analysis. With this knowledge, research could then focus on extending detection systems (e.g., [10, 24, 28]) to account for data from IoT logs where possible, and types of attacks to monitor for. This would also involve redesigning reasoning modules to correlate attacks with digital activity from these devices (likely fused with other corporate data points). The trialling and evaluation of these defensive systems will be essential, as given the unique nature of IoT devices, false positives could be a significant initial hurdle.

A next potential avenue for future research is in investigating the extent to which advances in MDM-type solutions for insider-attack prevention and detection, can be adapted to IoT. As we mentioned in Section IV, this is not a trivial problem if only due to resource constraints on IoT devices. Nonetheless, MDM has proved useful in managing BYOD paradigms, especially via facilities for secure containerised storage, data access and remote management. As such, there is potential value in an in-depth analysis of the adaptability of such solutions. The ideal case is that through this analysis, unique systems could be designed and created that could work with the limited resources on smart devices to address the insider IoT challenge.

Another strand of research could focus on attacks which do not leave a digital trace, and propose ways through which these may be deterred and detected. A possible preventive solution could explore how to design appropriate IoT policies. For example, no unauthorised IoT devices in work meetings, or the detection for the physically impossible (e.g., a single user authenticating to internal databases from two different locations at the same time). An initial attempt at recognising the leakage of sensitive data with the use of IoT is presented by Choi *et al.* [54]. They demonstrate how watermarking technologies may potentially be used to deter, and subsequently identify

the leakage of sensitive information even when insiders use micro devices. While this is an admirable start, a substantial amount of additional research is needed in this space if we are to tackle this growing problem.

There are also challenges of a different nature emerging from legal and ethical issues. We mentioned in Section III that the effectiveness of the detection systems relies on the datasets available. Laws are legislated to prohibit the collection and processing of data that may impeach employees' rights to privacy, as we previously discussed in Nurse *et al.* [8]. In many countries for example, processing datasets such as email activity would be considered a violation of data protection legislation. These challenges are even greater in the IoT discipline, since most of the devices are personal, and thus ethical and legal issues apply; we covered some of the privacy and surveillance issues in Section II. Finding a balance between collecting and processing sensitive data to detect insider attacks using IoT, while preserving employees' privacy is a key challenge which will also need to be further assessed in research and practice.

Finally, in this paper we elaborated on attacks derived from the more personal IoT devices. There is scope however, for insider attacks in cases where organisation-deployed IoT devices support consumers and also, the critical infrastructure. From a consumer perspective, IoT devices installed in enterprises or homes (e.g., smart thermostats, cameras, monitoring systems and door locks) typically share data with device manufacturers (via a private cloud) as part of the service or for after-purchase support. The reality is, therefore, that this data cloud (which may store sensitive information including where people are, their various habits or preferences) could be inappropriately accessed by a rouge employee at the manufacturer, and used either to invade a person's privacy directly or as part of a larger data breach [55]. We have already seen such privacy attacks by employees in the past, even within enterprises such as Google [56]. This is a significant challenge particularly when we consider how connected offices and homes will become in future years and the vast amount of data that will be available to manufacturers (and third-parties) and their employees.

From a critical infrastructure perspective, there are various other concerns as well. Smart grids for energy distributions, smart sewers and smart dams for control flows provide unique opportunities for attacks where the impact would have significant effects, not only on an organisational level but on a national and societal level as well. Fortunately, this area has attracted a significant research emphasis over the last few years [57, 58]. As some of those articles suggest however, there is more to be done both in terms of research and adoption of proposed security mechanisms, not to mention the development of usable systems capable of reducing the likelihood of accidental incidents [59].

VII. Conclusion

This paper considered the implications that the use of IoT devices may have on the insider-threat landscape for organisations. Research on IoT devices is still very much 'in progress' and the security concerns are mainly only being considered for external attacks. This factor, coupled with the difficulties which detection systems currently face in identifying insider threats, provide a unique means for insiders to successfully execute attacks using IoT devices. This article highlighted a few salient examples of how IoT devices, especially personal ones (e.g., smart-watches, smart-pens, smart-glasses), can be used by insiders to conduct such attacks. We also examined and discussed these attacks in the context of a few key case scenarios. We believe that there is scope for the current insider-threat detection approaches to be extended to accommodate IoT devices, but there are several challenges to be addressed first. Organisations need to recognise the threat at hand, and begin to construct systems and networks capable of being resilient to future IoT environments, where any 'thing' may be an insider. Overall, we believe that this provides a fertile area for future research to ensure that organisations are protected from this new avenue of threat.

References

[1] Business Insider, "24 Mind-blowing facts about the size of the Internet," 2013, http://www.businessinsider.com/24-mind-blowing-facts-about-business-2013-6.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] Government Office for Science, "Internet of things: making the most of the second digital revolution," UK Government, Tech. Rep., 2014.

[4] A. Solanas, C. Patsakis, M. Conti, I. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. Pérez-Martínez, R. Pietro, D. Perrea, and A. Martínez-Ballesté, "Smart health: a context-aware health paradigm within smart cities," *Communications Magazine, IEEE*, vol. 52, no. 8, pp. 74–81, 2014.

[5] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *International Conference on Privacy and Security in Mobile Systems (PRISMS)*. IEEE, 2014, pp. 1–8.

[6] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[7] A. W. Atamli and A. Martin, "Threat-Based Security Analysis for the Internet of Things," in *Workshop on Secure Internet of Things (SIoT)*. IEEE, 2014, pp. 35–43.

[8] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," in *IEEE Security and Privacy Workshops (SPW)*. IEEE, 2014.

[9] K. R. Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Information Security Technical report*, vol. 15, no. 3, pp. 112–133, 2010.

[10] D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes*, 1st ed. Addison-Wesley Professional, 2012.

[11] Accellion, Inc., "UK Enterprises Unprepared For New Age of 'Wear Your Own Device'," 2014, http://www.accellion.com/about-us/press/press-releases/uk-enterprises-unprepared-new-age-wear-your-own-device.

[12] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[13] Sopohs, "Security threat trends 2015," Tech. Rep., 2014.

[14] N. Hong, "A security framework for the internet of things based on public key infrastructure," in *Advanced Materials Research*, vol. 671, 2013, pp. 3223–3226.

[15] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, 2013.

[16] BBC, "Fridge sends spam emails as attack hits smart gadgets," 2014, http://www.bbc.co.uk/news/technology-25780908.

[17] A. Martínez-Ballesté, P. Pérez-Martínez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *Communications Magazine, IEEE*, vol. 51, no. 6, pp. 136–141, 2013.

[18] C. Patsakis, P. Laird, M. Clear, M. Bouroche, and A. Solanas, "Interoperable privacy-aware e-participation within smart cities," *Computer*, vol. 48, no. 1, pp. 52–58, 2015.

[19] E. D. Shaw and H. V. Stock, "Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall," Symantec, Tech. Rep., 2011.

[20] P. A. Legg, N. Moffat, J. R. C. Nurse, J. Happa, I. Agrafiotis, M. Goldsmith, and S. Creese, "Towards a conceptual model and reasoning structure for insider threat detection," *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, vol. 4, no. 4, pp. 20–37, 2013.

[21] O. Buckley, J. R. C. Nurse, P. A. Legg, M. Goldsmith, and S. Creese, "Reflecting on the ability of enterprise security policy to address accidental insider threat," in *Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, 2014.

[22] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, "Insiders behaving badly: Addressing bad actors and their actions," *Trans. Info. For. Sec.*, vol. 5, no. 1, pp. 169–179, 2010.

[23] E. Ted, H. G. Goldberg, A. Memory, W. T. Young, B. Rees, R. Pierce, D. Huang, M. Reardon, D. A. Bader, E. Chow *et al.*, "Detecting insider threats in a real corporate database of computer usage activity," in *19th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2013, pp. 1393–1401.

[24] H. Eldardiry, E. Bart, J. Liu, J. Hanley, B. Price, and O. Brdiczka, "Multi-domain information fusion for insider threat detection," in *IEEE Security and Privacy Workshops (SPW)*, 2013, pp. 45–51.

[25] P. Parveen, N. McDaniel, V. S. Hariharan, B. Thuraisingham, and L. Khan, "Unsupervised ensemble based learning for insider threat detection," in *International Conference on Privacy, Security, Risk and Trust (PASSAT)*. IEEE, 2012, pp. 718–727.

[26] Y. Chen and B. Malin, "Detection of anomalous insiders in collaborative environments via relational analysis of access logs," in *Proceedings of the first ACM conference on Data and application security and privacy*. ACM, 2011, pp. 63–74.

[27] G. B. Magklaras and S. M. Furnell, "Insider threat prediction tool: Evaluating the probability of IT misuse," *Computers and Security*, vol. 21, no. 1, pp. 62–73, 2002.

[28] P. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Automated insider threat detection system using user and role-based profile assessment," *IEEE Systems Journal*, 2015.

[29] G. Thomson, "BYOD: enabling the chaos," *Network Security*, vol. 2012, no. 2, pp. 5–8, 2012.

[30] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, "A review of bring your own device on security issues," *SAGE Open*, vol. 5, no. 2, 2015.

[31] IDG Connect, "UK: "Wipe Data" & Employees' BYOD Privacy Concerns," 2014, http://www.idgconnect.com/blog-abstract/9028/uk-wipe-data-employees-byod-privacy-concerns.

[32] ZDNet, "BYOD employees 'indifferent' to enterprise security," 2015, http://www.zdnet.com/article/byod-employees-indifferent-to-enterprise-security/.

[33] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 2, pp. 961–987, 2014.

[34] M. Rahman, B. Carbunar, and M. Banik, "Fit and vulnerable: Attacks and defenses for a health monitoring device," in *13th PETS Symposium*, 2013.

[35] Gartner, "Gartner Reveals 2014 Mobility Predictions," 2014, http://www.gartner.com/newsroom/id/2648515.

[36] J. D. Howard and T. A. Longstaff, "A common language for computer security incidents," *Sandia National Laboratories*, 1998.

[37] VERIS, "VERIS: The Vocabulary for Event Recording and Incident Sharing," 2015, http://veriscommunity.net.

[38] Business Insider, "Google Wants To Create Smart Contact Lenses With Cameras Inside," 2014, http://www.businessinsider.com/googles-smart-contact-lens-concept-2014-4.

[39] PCMagazine, "Stealing Passwords With Google Glass, Smartwatches, Web Cams, Whatever!" 2014, http://uk.pcmag.com/opinion/34730/stealing-passwords-with-google-glass-smartwatches.

[40] T. P. Diakos, J. A. Briffa, T. W. Brown, and S. Wesemeyer, "Eavesdropping near-field contactless payments: a quantitative analysis," *Journal of Engineering*, vol. 1, no. 1, 2013.

[41] Y. Oren, D. Schirman, and A. Wool, "Range extension attacks on contactless smart cards," in *ESORICS*. Springer, 2013, pp. 646–663.

[42] TunnelsUp, "Raspberry Pi: Phoning Home Using a Reverse Remote SSH Tunnel," 2013, http://www.tunnelsup.com/raspberry-pi-phoning-home-using-a-reverse-remote-ssh-tunnel/.

[43] SC Magazine UK, "Barclays KVM attack down to rogue employee," 2014, http://www.scmagazineuk.com/barclays-kvm-attack-down-to-rogue-employee/article/334694/.

[44] Overlook, "Fing - Network Tools," 2014, http://www.overlooksoft.com/.

[45] PCMag Digital Group, "World Cup 2014 Wi-Fi password accidentally shared with the world," 2014, http://www.geek.com/news/world-cup-2014-wi-fi-password-accidentally-shared-with-the-world-1597797/.

[46] Kaspersky Lab ZAO, "The world at your fingertips... and theirs too," 2014, https://securelist.com/blog/research/66435/the-world-at-your-fingertips-and-theirs-too/.

[47] B. Michéle and A. Karpow, "Watch and be watched: Compromising all smart tv generations," in *IEEE 11th Consumer Communications and Networking Conference (CCNC)*. IEEE, 2014, pp. 351–356.

[48] Business Insider, "Wal-Mart's Answer To Apple Pay Has Already Been Hacked," 2014, http://uk.businessinsider.com/currentc-hacked-2014-10.

[49] Gizmodo, "How Safe Can Apple Pay Really Be?" 2014, http://gizmodo.com/how-safe-can-apple-pay-really-be-1633065822.

[50] Symantec, "How safe is your quantified self?" Tech. Rep., 2014.

[51] The New York Times, "Keeping Your Car Safe From Electronic Thieves," 2015, http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[52] Bitdefender, "Bitdefender Research Exposes Security Risks of Android Wearable Devices ," 2014, http://www.darkreading.com/partner-perspectives/bitdefender/bitdefender-research-exposes-security-risks-of-android-wearable-devices-/a/d-id/1318005.

[53] Palo Alto Networks, "Wire Lurker: A New Era in iOS and OS X Malware," 2014, https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf.

[54] J. J. U. Choi, S. Ae Chun, and J.-W. Cho, "Smart securegov: mobile government security framework," in *Proceedings of the 15th Annual International Conference on Digital Government Research*. ACM, 2014, pp. 91–99.

[55] J. R. C. Nurse, "Exploring the risks to identity security and privacy in cyberspace," *XRDS Magazine*, vol. 21, no. 3, pp. 42–47, 2015.

[56] Gawker, "GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)," 2010, http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats.

[57] F. Aloula, A. Al-Alia, R. Al-Dalkya, M. Al-Mardinia, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 1–6, 2012.

[58] D. Formby, S. S. Jung, S. Walters, and R. Beyah, "A physical overlay framework for insider threat mitigation of power system devices," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2014, pp. 970–975.

[59] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in *Third International Workshop on Cyberspace Safety and Security (CSS)*. IEEE, 2011, pp. 21–26.