An Analysis of Malicious Threat Agents for the Smart Connected Home

Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson
Internet of Things and People Research Center and Department of Computer Science
Malmö University, Malmö Sweden,
{joseph.bugeja, andreas.jacobsson, paul.davidsson}@mah.se

***Abstract* — Smart connected home systems aim to enhance the comfort, convenience, security, entertainment, and health of the householders and their guests. Despite their advantages, their interconnected characteristics make smart home devices and services prone to various cybersecurity and privacy threats. In this paper, we analyze six classes of malicious threat agents for smart connected homes. We also identify four different motives and three distinct capability levels that can be used to group the different intruders. Based on this, we propose a new threat model that can be used for threat profiling. Both hypothetical and real-life examples of attacks are used throughout the paper. In reflecting on this work, we also observe motivations and agents that are not covered in standard agent taxonomies.**

Keywords—connected home; IoT; smart home; threat agent; threat agent motivations; threat agent capabilities.

I. Introduction

The Internet of Things (IoT) computing paradigm is growing rapidly with, e.g., Gartner predicts a growth from 5 billion connected devices in 2015 to 25 billion by 2020 [1]. The availability of affordable Internet-connected household devices, such as light bulbs, cameras, TVs, thermostats, and locks, is stimulating the growth of what we refer to as smart connected homes. Surveys in the US and Canada indicate that 90% of those surveyed are willing to purchase a smart home system to enhance personal and family security, and 70% to promote energy efficiency [2].

A smart connected home is a residence that uses IoT technology to create a comfortable environment and an effective lifestyle. In comparison to a traditional home that features mainly local control, typically in the form of switches and buttons, appliances that are disconnected from the broadband or cellular network, and access that is limited to a restricted set of people, commonly in the form of physical access and at set times, this is not the case with the contemporary smart home. This technologically-augmented version of a home may employ sophisticated controls (e.g. voice-based interfaces), connection to Internet-based cloud services (e.g. for analytical processing purposes), and internal/external accessibility from several actors (e.g. service providers for security monitoring purposes). Furthermore, the access of certain entities could be available on a continuous basis, may include privileged access, and in certain cases could involve individuals with hostile intentions that are unknown to the householders. The increasing number of groups of people interested in the connected home, the widespread availability and proliferation of IoT devices in the living spaces, and escalating reports about security and privacy breaches has prompted us to conduct this study.

While there has been considerable research works from both academia and industry that study the cybersecurity and privacy threats connected to the smart home environment, we observe that the focus of most studies continue to be on asset or vulnerability analysis, while assessments based on the types of threat agents are rarer. Threat agents are commonly categorized into human (e.g. hacker), technological (e.g. power supplies), and environmental (e.g. fire) actors [4]. We believe that the motivations and resources for carrying out an attack make humans potentially dangerous threat sources. Studying the human threat agent, in particular the intent and abilities of the attackers, contributes to creating effective mitigation techniques and planning approaches. We also include software threats, in particular viruses, worms, and Trojans, as attacking parameters. Thus, in this paper, we seek to address this research gap by systematically analyzing the malicious smart connected home external threat agents, their socio-psychological characteristics, and propose a new threat model that can be used for threat profiling. Specifically, in this work we aim to provide answers as to: (i) who are the malicious human threat agents, (ii) what are their motivations, and (iii) what are their capabilities. Identifying the threat agents and their typology is an important step to deal with risks effectively, and to develop effective risk mitigation strategies. Moreover, such insights help assess the amount of time, effort, and money required to defend against the threats posed to smart connected homes.

In conducting this study, we looked at different documentary sources. Our main focus was on scientific literature, but to have a more holistic and current perspective we also included industry reports, news articles, penetration testing reports, and hacking conferences. The major scientific articles were mainly retrieved through Google Scholar and the rest through a manual Internet search process. Search keywords included vendor names that have an IoT presence and connected devices that are common in home environments. Retrieved search results

978-1-5090-4338-5/17/$31.00 ©2017 IEEE

were then analyzed for incidents or vulnerabilities. Once such instances were found, the CVE database maintained by MITRE, CERT/CC vulnerability notes, security research blogs, and forums were used to gain additional insight.

The remainder of this paper is organized as follows. In Section II, we provide background, examples of security and privacy threats, and threat agent taxonomies. Next, we identify the main hostile threat agents, their motivations, and capabilities. The results and insights regarding the current research gaps are discussed in Section IV. Finally, Section V, conclusions are drawn and directions of future work are specified.

II. BACKGROUND

In this section, we discuss the smart connected home and then we describe potential information security and privacy threats. Finally, we highlight some security and privacy requirements in the context of a smart connected home.

A. The Smart Connected Home

A smart connected home is made up of a set of hardware nodes, e.g. sensors, actuators, and smart devices, communication channels, e.g. wired/wireless protocols, and software services that implement functions to meet the residents' goals. Typically, these functions tend to be related to enhancing security, improving healthcare/lifestyle support, efficient energy management, and providing tailored entertainment. This also allows for remote, and possibly automated, control, management, and operation of connected devices (e.g. smart lightning), typically over an IP-based network, such as the Internet.

In order to clarify the concept of the smart connected home, let us take as an example of a home that implements services related to energy management. Specifically, if we look at a use-case related to online reading of consumption and technical data from a residence, then we can identify the smart meter as the core IoT device and the residents, energy supplier, and the Distribution System Operator (DSO) as the main actors in this system. This setup is shown in Figure 1.

The householders are interested in being invoiced the correct energy consumption and production bill, protection of their personal data, and insight into their own energy consumption and production. The energy supplier is interested in providing the households with electrical power, perform billing, and reduction of fraud. The DSO is interested in outage management, remote power switching, and in collecting smart meter measurement data. In addition to the hardware elements, the smart house contains information assets such as monitored data, configuration data, and switch data.

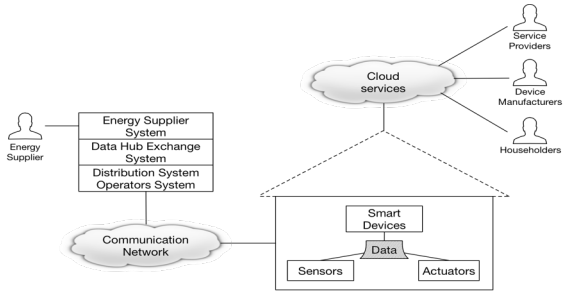

Fig 1. Smart connected home implementing the home energy management use-case. The house is connected to the smart grid via a proprietary communication network. Householders can potentially access the home appliances through an Internet-enabled cloud infrastructure, possibly owned and managed by device manufacturers and service providers.

B. Smart Connected Home Security and Privacy Threats

A threat can be defined as a possible danger that might exploit vulnerabilities in a system to cause potential harm [5]. If we consider the home energy management use-case, a threat scenario could be where a hacker penetrates a smart home and extracts resident-related data from the system. In the data, the threat agent may note that the residents will be disconnected as they may have failed to pay the bills. This threat impacts the individual's privacy as there is information theft about the customer to be switched off and may impact the DSO by a lawsuit for not implementing strict access control procedures.

At a rudimentary level, computer security requirements can be broken down into three main requirements: confidentiality, integrity, and availability [6]. Confidentiality entails applying rules to limit unauthorized access to information. For instance, unauthorized access to connected health devices may reveal personal health information. Integrity is also necessary for providing a reliable service. An integrity compromise may have life-threating outcomes, e.g., if used against medical devices such as insulin pumps. IoT availability is essential, for example, if a smart lock is not online when expected. Then, the residents may be prevented to enter their own house, or a malicious threat agent may be granted (unlawful) entry.

The concept of privacy involves the users' right to controlling, editing, managing, and deleting information about themselves and also deciding when, how, and the extent to which information is communicated to others [7]. As an example, being able to eavesdrop on conversations in a living room is a privacy threat.

C. Threat Agent Classifications

There are different threat assessment methodologies that assess threats by focusing on the analysis of their attackers. For example, Sandia National Laboratories at the Department of Homeland Security developed the Operational Threat Assessment (OTA) methodology which identifies and measures cybersecurity threats faced by a system [8]. The OTA uses a General Threat Matrix (GTM) to help analysts characterize threats based on their overall capabilities and to categorize them into a common vocabulary. The methodology however, does not identify the threat agents, and instead concentrates on building a GTM.

A similar methodology, Intel's Threat Agent Risk Assessment (TARA), provides predictive output that can be understood by non-expert audiences [9] [10]. It relies on three components: Threat Agent Library (TAL), Common Exposure Library (CEL), and Methods and Objectives Library (MOL). The TAL captures twenty-two different agent types (archetypes) and eight characteristics of threat agents: intent, access, outcome, limits, resource, skill level, objective, and visibility. The CEL enumerates information security vulnerabilities and exposures at Intel, although other CELs are publically available. The third component, the MOL, lists known threat agent objectives, i.e., what the agents want to accomplish and their most likelihood methods. In contrast to OTA, that focuses on

the role of a technical personnel as a possible threat source, TARA takes a more extensive approach identifying several attacker profiles together with their methods and objectives.

Another classification scheme is the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [11]. ICS-CERT identifies five external threat agents: national governments, terrorists, spies and organized crime groups, hacktivists, and hackers. ICS-CERT also has an insider threat database that identifies malicious events involving insiders dating back to the 1950s. Additionally, it collaborates with international and private sector Computer Emergency Response Teams in sharing control systems-related security incidents and mitigation measures. Even though in terms of agent types ICS-CERT is not as extensive as TAL, we observe that an adaptation of this scheme is popular amongst agent typologies such as those as presented by the European Union Agency for Network and Information Security [12].

Given ICS-CERT's strong ties with real-world security incidents, its considerable cybersecurity database, and the generic nature of the identified roles, we use this scheme as a basis for identifying treat agents of a smart connected home.

III. Threat Agents, Motivations, And Capabilities

In the following sections, we present a taxonomy of possible intruders. Then, we highlight the main threat agent motivations, and capabilities associated with different threat agents.

A. Threat Agents

There are various threat agents that can target a smart connected home. In this section, we adapt and expand on the ICS-CERT taxonomy to describe the different agent classes and supplement them with hypothetical and real-life examples. The list of hostile threat agents ordered from the most capable to the least capable includes:

Nation states: Enemy state attackers are groups of highly sophisticated individuals that are funded by governments and associated with a military unit. Nation states can have offensive cyber capabilities and use them against an adversary. For instance, researchers have found a way to take down the power grid, possibly causing a widespread blackout, by remotely manipulating shut-off devices installed on air conditioners[1]. Given the presence of such a device in a smart connected home, this threat can be exploited by state-sponsored attacks as part of cyber warfare. A recent attack involved a ZigBee worm targeting Philips Hue smart lights system that can be exploited, for instance through war-driving and war-flying, to disable possibly the city lights within a few minutes [13]. Similarly, Internet routers, such as those located in smart homes, can be used by intelligence agencies, to conduct offensive cyber operations for instance targeting systems and communications of top adversaries[2]. Moreover, smart home devices capable of transmitting audiovisual data can be used by state actors in national surveillance efforts [14]. Typically, nation states make use of advanced threat tactics such as customized malware, spear phishing attacks, and zero-day attacks.

Terrorists: Persons who rely on violence to support personal socio-political agenda. While traditional terrorists are focused on physical attacks to promote terror, cyber-terrorists typically focus on targeting information systems, e.g. IoT systems. In the smart connected home, targeted attacks are likely to focus on individuals or families that are well known so that the attacks will obtain maximum news coverage. Although, this is unlikely [14], for instance, life-sustaining health devices such as pacemakers are increasingly configurable remotely and have been demonstrated to be vulnerable to attacks. Terrorists commonly use social engineering and data mining methods to support their efforts as well as tools to conduct cybercrime in order to fund operations [16].

Competitors and organized crime: Private criminal organizations have been known to be quite resourceful and sophisticated. However, in this category, we also include commercial competitors (industrial spies) that compete for revenues or resources (e.g. acquisitions). For instance, an attacker may attempt to obtain a copy of a device firmware in order to harm its competitors' reputation. Similarly, using the same attack vector, attackers can reverse engineer the device's software and use parts of it for their own product. An approach to achieve this is through hardware Trojans. These are malicious code modifications to an integrated circuit that can be used to enable a perpetrator access to data or software running on a device [17]. Attackers can also compromise a smart appliance, such as a refrigerator, to send out malicious email messages to other potential victims to grow their botnets. Botnets composed of smart home appliances and other devices in IoT networks can be infected and turned into slaves by attackers [18]. Moreover, compromising a smart device, such as Nest Thermostat, may also turn the learning thermostat into a spy that listens to the routines of the inhabitants and provides a backdoor to their local network, which has been previously pointed out by Hernandez et al. [19]. Once inside a smart home network, cybercriminals can potentially launch ransomware attacks, locking devices in exchange for cash or for instance steal personal data and use it for blackmail or sell in bulk in underground marketplaces (cf. Micro [14]).

Hacktivists: In this category, individuals or groups of individual pursue a political or social agenda often related to human rights and freedom of information. The group known as Anonymous is one such example. Hacktivist activity is often centered on disrupting businesses and targeting individuals, such as CEOs, to gain media coverage and public attention [20]. Included in this group would be stunt hackers who seek fame or promotional advantages by hacking devices, especially IoT devices, to prove that it can be done. A particular case of stunt-hacks are the attacks against baby monitors. Several video baby monitors from different manufacturers have been reported for vulnerabilities [21]. Homes of specific individuals can also be targeted. For instance, Anonymous denial-of-service (DoS) attacks on payment processors believed to be hindering WikiLeaks' operations[3]. Hacktivists are often asso-

[1] https://goo.gl/5828tL

[2] https://www.wired.com/2013/09/nsa-router-hacking/

[3] https://goo.gl/IRNjY8

ciated with engaging in activities such as DoS, fraud, and identity theft [22].

Thieves: This threat agent includes individuals that are associated with stealing mostly for personal financial gain. As an example, researchers [15] have demonstrated how vulnerabilities in devices, such as Chamberlain MyQ system (a universal smartphone garage door controller) and Ubi (a voice-activated hub), could allow a thief to be notified when a garage door is opened/closed or when the residents are at home and thus indicating a window of opportunity to rob the house. However, thieves could also be after stealing electricity, disrupting a video-over-IP system, exploiting sensitive documentation, hardware resources or media. Thieves tend to be linked to DoS, spoofing, and system intrusion.

Hackers: This group includes malicious individuals, script kiddies, and employees of an organization who may be disgruntled, nosy, or whistle-blowers. Employees involved in support functions often have access to customer accounts in order to troubleshoot requests and inquiries from clients. Consumer support agents in the case of an Internet-connected door lock company may be able to lock or unlock doors remotely [20]. Additionally, it may include stalkers [14], pranksters, cyberbullies, and predators that may use online chat forums and instant messaging to find and communicate with minors, and also to track down a person's location to inflict harm or embarrassment. In this case, IoT devices such as security systems can be leveraged by perpetrators to commit acts of bullying. Hackers tend to use ready-made tools and applications that others develop. Classical examples of attacks could involve viruses, worms, and phishing.

B. Threat Motivations

There are many motivations and often they are aligned with the nature of the threat agents themselves. Based on the analysis of FBI cyber-attack data [23], for a smart connected home environment, we can group the intruders' defining motivations into four distinct classes:

***Curiosity*:** A threat agent moved by curiosity to experiment and try things out is expected to go in an extreme way in order to fulfill this need. A typical threat for a smart home could be a prankster with intent of causing concern or confusion [24]. This is typically, associated with the hackers' threat source and tends to be driven by intellectual challenge. Under this motive, there can also be academia, research, and curious consumers as threat sources but these are excluded as threat agents given their unlikeness to breach security for malicious purposes.

Personal gain: It can be monetary gain, acquisition of knowledge, peer recognition, and related. Threat agents tend to be more motivated when there is a financial gain behind their actions. A typical threat scenario for this can be an individual trying to hack a smart connected home to gain access for bragging rights or for instance a spammer [24]. Stunt hackers are typically inspired by peer recognition. Industrial spies are typically motivated to gain competitive advantages by capturing individual intellectual property. In the case of the energy-focused smart connected home, the motives might be related to disruption of service, stealing of electricity, and as well unethical to defame an organization or an individual [25].

Terrorism: Traditional terrorist and cyber-terrorist actions have the unique goal of inflicting violence or fear related behavior. Common motivation factors here can include blackmail, destruction, exploitation, and revenge. One attack demonstrated by researchers is to set smart lightning into a strobe pattern that can possibly trigger epileptic seizures to people [13]. Terrorists could also target smart home resourceful devices, such as gateways, to anonymize their traces and encrypt their activities. However, there is little evidence for terrorism motivated attacks on smart connected homes [12].

***National interests*:** Political interests drive a number of threat agents. A legitimate threat agent can crack into a terrorist's computer to learn of an impeding attack, and an illegitimate agent can attack a device to learn the inhabitants' details. For example, a state-sponsored attacker that infects millions of IoT-based systems, e.g., remote monitoring systems, and smart devices, e.g., smart TV-sets, and then exploit the infected systems and devices to spy on a person of interest or to conduct an attack on a large scale.

C. Threat Agent Capabilities

Although threat agents can be clearly differentiated, their capability to execute successful attacks is what differentiates them as a threat to the smart connected home. Capability measures the adversary's skills, availability of attack tools or resources to acquire such tools, and knowledge about the target system or component [26]. Figure 2 is a threat model that identifies different threat agent profiles.

We observe that threat sources for the smart connected home can be classified into three broad capability levels:

Low: The threat agent has relatively meek capabilities and resources commonly involving very few people. Typically, this includes political pressure groups, amateur hackers, and commercial rivals. Generally, this involves a small amount of equipment, e.g. laptop and wireless antennas, script programming, and common off-the-shelf tools. For instance, an attacker at this level, could be a script kiddie that may randomly scan the Internet using IoT search engines like Shodan and Censys to find vulnerable components. Hacktivists are also not known to be wealthy organization and thus even though they may have sources of revenue derived from crime, they are associated with this level [27].

Moderate: At this level, the typical threat agent has modest capabilities and resources, and the attacks commonly involve a small number of persons. Commonly, this includes competent

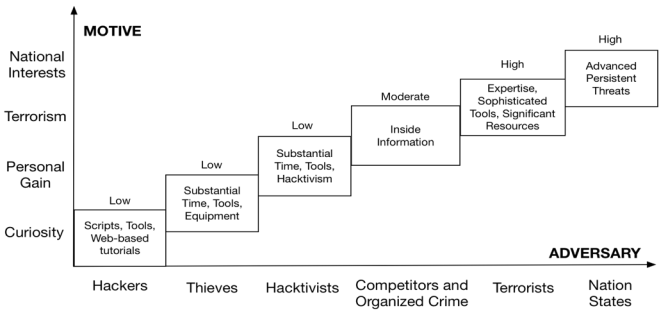

Fig 2. The main smart connected home hostile threat agents alongside their possible primary motivations and associated capability levels.

individuals, e.g. insiders, and small organized terrorist criminal groups. Generally, this level involves some amount of equipment and publically available attack data and attack tools. Criminals may have significant budgets, high-performance computing, experience, and thus although their skills can be primarily categorized as moderate, especially when linked to terrorism or organized crime, the capability level including the cost of defense can grow to high [28].

High: At this level, the typical threat agent is highly capable and has significant resources. Ordinarily, this involves committed entities such as intelligence agencies and well-organized terrorists or criminal groups. In general, attacks in this class may involve several people and may involve the coordination of several threat agents. Advanced persistent threats, exploit kits, bespoke attacks, and large equipment may be used to conduct committed attacks. Furthermore, this level may include social engineering methods such as direct persuasion, bribery, and coercion.

IV. Discussion

The increasing growth of IoT devices within smart home environments has led to greater security and privacy risks to the householders and eventually also to the critical infrastructure upon which a country relies.

To explain the risks in more detail, we consider a scenario consisting of house tenants purchasing a smart lightning system to enhance convenience and safety. This system can be controlled using a mobile application or directly from the product vendor's website. However, the system has design vulnerabilities, notably related to insufficient authentication and authorization. A hacker notices that the vendor's website implements a weak password policy, allowing the creation of easily guessable passwords such as "123456". By developing a simple script, e.g. using Python, a hacker can guess login credentials and potentially blackout entire homes. The impact of this attack can be a nuisance but it can create chaos and may allow a different threat agent, e.g. a thief, the right opportunity to rob a house possibly without being noticed.

In Table I, we classify the main types of attacks presented in this paper into security and privacy threats. From Table I, we note that every threat agent has the potential to compromise the smart connected home assets in different ways. Hacktivists and nation states are mostly interested in disrupting a service as part of cyber warfare or to satisfy a political or social agenda. Competitors and organized crime are interested in acquiring competitive advantage and in other cases to use the home as part of a supply-chain to attack critical infrastructure. Terrorists mostly seek violence and promoting terror but are not after exploiting privacy threats. It appears that terrorists are the most uncommon or unlikely threat source in smart connected homes [12][14]. Thieves are mostly after financial gain and sometimes for personal satisfaction. Hackers tend to be associated with the curiosity motive and commonly includes individuals that do not have the resources to create sophisticated attack tools. As a general observation, we note that reported security vulnerabilities tend to involve factors that are typically associated with low capability levels, such as those employed by the hackers' class.

TABLE I. High-profile attacks initiated by malicious human threat agents targeting a smart connected home setup

Threat Agent	Typical Compromise Methods	
	Security	***Privacy***
Nation states	Attack a communication device, e.g. home router, to disrupt or corrupt smart home services (availability)	Attack on sensors, e.g. cameras, to eavesdrop communication of adversaries
Terrorists	Attack an actuator, e.g. insulin pump, to inject medication, possibly overdosing a patient (integrity)	N/A[4]
Competitors and Organized Crime	Attack a smart appliance, e.g. refrigerator, to help grow a criminally-funded botnet (integrity) Attack a device firmware to get a competitor's software (confidentiality)	Attack on sensors, e.g. microphones, to snoop on private conversations
Hacktivists	Attack a smart home network to disrupt its services (availability)	Attack the smart home network resources to intercept sensitive communication
Thieves	Attack a smart home alarm system to rob a house (availability)	Attack a smart home hub to detect when the residents are away
Hackers	Attack a smart home network to gather information, e.g. credentials, about the user (confidentiality)	Attack a smart home device, e.g. a baby monitor, to cause chaos

We note that other threat agents with different motives and capabilities may be involved in future. One particular threat agent category is composed of groups selling distributed denial-of-service or malware-as-a-service. Their motive might be partly driven by personal gain but may also be linked to terrorism. In our case, we are also not distinguishing between the defining motivation, co-motivation(s), subordinate motivation, binding, and personal motivation [29]. In doing so, first hand data and possibly interviews with different threat agents would be required. Alas, we have noted the lack of public databases that are specifically focused on IoT vulnerabilities or incidents.

The number and type of incidents also escalate the importance of security education and awareness of the householders. Hackers are often able to break smart home systems, because these are not protected by their users, e.g. default or weak passwords are used. These aspects would be more difficult to handle without also changing the behavior of the users. This is something that cannot be done solely through technology. Here, the role of consumer associations and cybersecurity agencies is key to help raise security awareness, e.g. by providing support and guidance on topics such as how to choose, operate, and control smart home devices and services.

Furthermore, as a general reflection we observe that the previous works and models used are focused on more traditional web-based systems, and not on IoT systems such as smart connected homes. We believe that such models need to be extended to cope with additional types of threat agents, e.g.

[4] Typically, terrorists are not after privacy threat but after physical attacks, damage/loss of assets, and outages

thieves, and capabilities, e.g. Bluetooth and WiFi sniffing, that may be important for smart connected homes, but not for traditional web-based systems.

V. Conclusions And Future Work

A home is the place where privacy is expected to be respected. In comparison to the traditional home, the smart connected home can be accessed by different entities, some of which carry malicious intentions, and thus causing a security or privacy threat to the residents.

In this work, we set out to explore the typical categories of malicious human threat agents, their motivations, and capabilities. We have done this by exploring both hypothetical and real-life examples of attacks. As a result, we have identified six main classes of hostile human threat agents (nation states, terrorists, competitors and organized crime, hacktivists, thieves, and hackers), four broad motivation factors (curiosity, personal gain, terrorism, and national interests), and three different capability levels (low, moderate, and high). These three components form a threat model that can be used for profiling threats caused by humans in smart connected homes.

Moreover, we have discussed the limitations of existing models, the importance of security education and awareness, and the need to have first hand data in order to make more rigorous analysis and to help us better generalize on the findings. Especially, we see it is a priority to have IoT security vulnerability and incident databases that are open to information security researchers. This will help us also to better evaluate the model proposed in this paper.

In conclusion, we believe that identifying the smart home malicious threat agent profiles will give home users, security researchers, and device and system manufacturers, a better understanding of what kinds of attacks they can expect, and thus provide a more efficient protection strategy.

Looking towards the future, there are several avenues being explored to advance the research presented in this paper. The first is on designing a framework in which the motivation of the attacker is included to perform a quantitative security analysis of a smart connected home for different types of attackers. One possible way of doing so is by extending attack trees with attacker profiles. Related to this, is future work that elaborates on the skills needed to attack smart homes, i.e. the expertise required and corresponding aspects, e.g. networks, operating systems, and embedded systems. Overall, this might give a complementary indication on the vulnerability level of smart homes. A different line of future research, is connected to formally modeling attack descriptions, e.g. using Isabelle framework (an interactive proof assistant that supports formal specification and verification, e.g. through high-order logic). This allows for conducting advanced analysis possibly enumerating all potential attacks with respect to the model.

Acknowledgement

This work has been carried out within the research profile "Internet of Things and People", funded by the Knowledge Foundation and Malmö University in collaboration with 10 business partners. The authors would also like to thank all the members of the research profile project "Intelligent Support for Privacy Management in Smart Homes".

References

[1] Gartner, "Gartner says 6.4 Billion connected," 2015 [Online]. Available: http://www.gartner.com/newsroom/id/3165317.

[2] iControl, "State of the Smart Home," 2015 [Online]. Available: https://goo.gl/u2HBtw.

[3] J. Bugeja *et al.*, "On Privacy and Security Challenges in Smart Connected Homes," *European Conference in Intelligence Security Informatics*, 2016.

[4] A. Amini *et al.*, "Threat Modeling Approaches for Securing Cloud Computing," *Journal of Applied Science*, vol. 15, no. 7, pp. 953-967, 2015.

[5] H. G. Brauch, "Concepts of security threats, challenges, vulnerabilities and risks," *Coping with Global Environmental Change*, 2011.

[6] A. M. Nia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, 2016.

[7] M. Deng *et al.*, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3-32, 2011.

[8] M. Mateski *et al.*, "Cyber threat metrics," *Sandia National Laboratories*, 2012.

[9] T. Casey *et al.*, "Threat agents: a necessary component of threat analysis," *Proceedings of the sixth annual workshop on cyber security and information intelligence*, 2010.

[10] M. Rosenquist, "Prioritizing information security risks with threat agent risk assessment," *Intel Corporation White Paper*, 2009.

[11] D. Gray *et al.*, "Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution," 2015.

[12] D. Barnard-Wills *et al.*, "ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media," *ENISA (The European Network and Information Security Agency)*, 2014.

[13] E. Ronen *et al.*, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," 2016.

[14] T. Micro., "The Usual Suspects: IoT Attackers and Motivations," 2016 [Online]. Available: https://goo.gl/5Mqt6d.

[15] Veracode., "Veracode White Paper – The Internet of Things: Security Research Study.," 2015 [Online]. Available: https://goo.gl/uFU8gL.

[16] J. Sheldon, "State of the art: Attackers and targets in cyberspace," *Journal of Military and Strategic Studies*, vol. 14, no. 2, 2012.

[17] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design and Test of Computers*, vol. 27, no. 1, pp. 10-25, 2010.

[18] N. P. Hoang and D. Pishva, "A TOR-based anonymous communication approach to secure smart home appliances," *17th International Conference on Advanced Communication Technology*, pp. 517-525, 2015.

[19] G. Hernandez *et al.*, "Smart nest thermostat: A smart spy in your home," *Black Hat USA*, 2014.

[20] N. Dhanjani, "Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts," O'Reilly Media, Inc., 2015.

[21] M. Stanislav and T. Beardsley, "HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities," 2015.

[22] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security*, vol. 4, pp. 65-88, 2015.

[23] A. Shostack, "Threat modeling: Designing for security," John Wiley & Sons, 2014.

[24] C. S. Alliance., "Future-proofing the Connected World:13 Steps to Developing Secure IoT Products," 2016 [Online]. Available: https://goo.gl/Qtev4f.

[25] K. Adak *et al.*, "Advanced Metering Infrastructure Security," 2009.

[26] S. Vidalis and A. Jones, "Analyzing Threat Agents and Their Attributes.," *ECIW*, pp. 369-380, 2005.

[27] T. Macaulay, "RIoT Control: Understanding and Managing Risks and the Internet of Things," Elsevier, 2016.

[28] O. Whitehouse, "Security of Things: An Implementers' Guide to Cybersecurity for Internet of Things Devices and Beyond," *NCC Group,* 2014.

[29] T. Casey, "Understanding cyberthreat motivations to improve defense," 2015 [Online]. Available: https://goo.gl/t6pfzz.