2016 European Intelligence and Security Informatics Conference

On Privacy and Security Challenges in Smart Connected Homes

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 homes have become increasingly popular for IoT products and services with a lot of promises for improving the quality of life of individuals. Nevertheless, the heterogeneous, dynamic, and Internet-connected nature of this environment adds new concerns as private data becomes accessible, often without the householders' awareness. This accessibility alongside with the rising risks of data security and privacy breaches, makes smart home security a critical topic that deserves scrutiny. In this paper, we present an overview of the privacy and security challenges directed towards the smart home domain. We also identify constraints, evaluate solutions, and discuss a number of challenges and research issues where further investigation is required.**

Keywords—smart home; security; privacy; IoT.

I. Introduction

Smart homes have been around for some time. Among the first smart home devices was a 100 pounds "Kitchen Computer" offered by Neiman Marcus in 1969 that was selling for $10,000 and required the residents to take a programming course to enter and read recipes. Since then, many versions of smart homes have been developed, such as MavHome [1], which are typically also Internet-connected to allow for remote monitoring and control. These smart connected homes make use of many different sensing technologies. Recent smart home devices feature microphones for voice interaction and use of cloud for storage or processing purposes. Additionally, they may feature programming frameworks allowing for the development of smart home services, such as Apple's HomeKit, Google's Weave/Brillo, and Samsung's SmartThings. Nowadays, any home can be easily retrofitted with personalized, affordable, and potentially 'smart' devices.

A smart connected home can be defined as a residence incorporating a range of sensors, systems, and devices that can be remotely accessed, controlled, and monitored via a communication network [2]. According to a recent study [3], the global smart home market in 2015 was valued at $9.8 billion and is estimated to reach $43 billion in 2020. According to another study [4] the smart home market is anticipated to double in the US with family safety being the greatest motivator.

However, the increasing deployment of Internet-connected devices in the home expose the residents to privacy and security risks as personal information becomes remotely accessible in new ways. An attacker can, for instance, eavesdrop on the wireless transmission of sensors and detect activities such as showering, toileting, and sleeping [5]. Also, a malicious actor may remotely take over control of the home devices using them to hack the household or as a platform to launch attacks to other domains, e.g. to overload the energy grid. Successful attacks to various commercial off-the-shelf products have been performed [6–8]. These attacks are not only hypothetical, e.g. in 2014 over 73,000 video cameras were found to be streaming their surveillance footage on the web.

In this paper, we study the security and privacy challenges in smart connected homes. Section II provides an introduction to core technologies. Section III discusses smart connected home characteristics that make the implementation of generic security and privacy constraints challenging. Section IV presents an overview of mitigation strategies that can be applied across the different layers of a smart connected home. Some of the most urgent research topics are discussed in Section V. Finally, Section VI concludes the paper and identifies future work.

II. Smart Home Technology

Typically, a smart connected home comprises a multitude of connected devices belonging to a variety of application areas. Commonly, the application areas are broadly categorized into four groups: entertainment, energy, security, and healthcare [9]. Entertainment aims to maximize the occupants' comfort and convenience by providing personalized amusement content and social communication services. Energy apps are targeted to provide efficient energy consumption and management. The security domain offers services designed to monitor, detect, and control security and safety threats. Healthcare apps are focused on providing mobile health services and fitness support. Arguably, the healthcare domain carries the widest spectrum of risks ranging from eavesdropping to fatal hacking. As an example, Fig. 1, shows a typical smart home architecture.

Fundamentally, we regard a smart connected home as composed of devices, communication, and services.

A. Devices

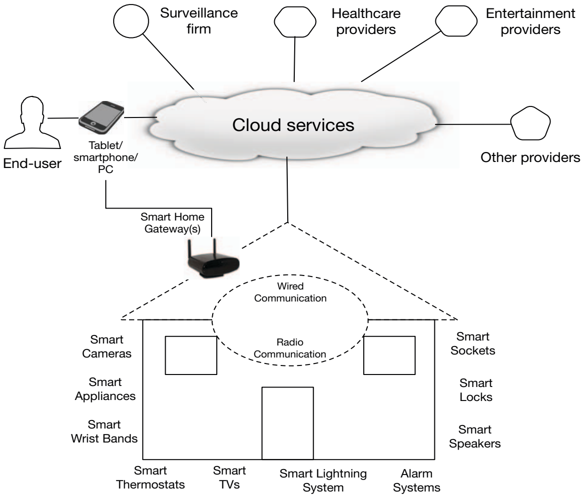
Smart home devices are hardware units typically comprising sensors, actuators, gateways, and smart objects. The separate device types are:

1) Sensors measure a physical property of the environment or physical entity. Sensors can range from wearables (e.g. bracelets) to non-wearable (e.g. IP cameras) sensors. Video cameras are considered the most privacy-violating sensors [10] together with microphones.

2) Actuators perform actions such as switching on/off or dimming lights, closing windows, triggering alarms, etc.

978-1-5090-2857-3/16 $31.00 © 2016 IEEE
DOI 10.1109/EISIC.2016.21

Fig. 1. Smart connected home architecture. It consists of connected devices belonging to different applications and gateways. Gateways provide connectivity to service providers and other external entities.



3) Gateway serves as an access point to the home commonly allowing the owner or another entity the facilities to monitor, control, and manage the home appliances or sensors remotely. Also, it serves as an aggregation point in order to send measured data to an external network such as utility companies.

4) Smart objects are devices composed of sensors and/or actuators, that are connected to the Home Area Network. Examples of this include smart appliances such as smart locks that answer doorbells and provide for time-based access controls.

B. Communication

A typical smart connected home uses a variety of communication protocols. These range from wired to radio communication protocols. Generally, sensors communicate using home automation protocols such as KNX, Zigbee, Z-Wave, and DASH7 or through network communication protocols such as Wi-Fi, Bluetooth, 6LoWPAN, IEEE 802.15.4 or cellular technology. RFID and NFC technologies are also used to monitor and track occupants especially in the healthcare domain, and are commonly employed in smart door locks.

C. Services

Services are software applications hosted in the cloud or inside the home environment that have responsibilities to implement automation, device management, decision making, etc. A special category of services are controllers that allow for management of connected devices. Typically, the households run such software over their smartphones or tablets to locally or remotely interact with a device.

III. Security And Privacy Challenges

The connected home may contain sensitive data (e.g. personal photos, videos, and digital diaries), and devices such as IP cameras that may be remotely activated and accessible from anywhere. Additionally, it may feature microphones that may listen to private conversations. For instance, smart speaker systems such as Amazon Echo and Google Home feature microphones that are programmed to listen to ‘wake up’ commands and voice input to complete tasks such as dimming lights and playing music. This makes the need for stringent security requirements, due to the importance of the private information. However, adapting standard security controls to smart connected homes is challenging as identified by Lee et al. [11]. Below, we expand the mentioned challenges and map them to different architecture layers.

A. Device Issues

Resource constraints**:** Smart home devices are often battery-driven and use low-power CPUs with low clock rates and small throughput. This makes computationally expensive cryptographic algorithms, such as RSA, difficult to port to such low powered devices [12]. This is also hampered by RAM and flash memory limitations.

Headless nature: Typical IoT devices do not feature a keyboard, mouse, and screen. This may force end-users to rely on smartphones or websites to input parameters. Additionally, this makes mechanisms such as the “notice and consent” more challenging to implement in smart connected homes.

Tamper resistant packages**:** Smart home devices are most of the time physically accessible making them prone to physical tampering attacks. Sometimes, the homeowners can conduct this attack for instance by tampering with smart meters to reduce billing costs. However, technical tampering may also be conducted by other entities for instance to facilitate a break-in.

B. Communication Issues

Heterogeneous protocols: The different communication protocols possibly used to interconnect the devices in a smart connected home require the use of bridges, hubs or gateways. Additionally, a device may use a proprietary protocol (e.g. non IP-based) locally and a standard one to connect to the cloud. These factors coupled with hardware limitations could lead network engineers to opt for weaker encryption schemes [13].

Dynamic characteristics: Devices such as wearables can join or leave the home network anytime and possibly from anywhere. This raises the need to develop resilient security algorithms, and makes tracking and asset management a challenge. The multiprotocol communication characteristics together with the varying device capabilities also make traditional security schemes unsuitable for home devices [14].

C. Service Issues

Longevity expectations: Mitigating security vulnerabilities requires remote reprogramming. However, this might not be possible for all devices as the operating system, protocol stack or firmware might not support dynamic patches. Moreover, some devices for instance smart meters are designed and expected to stay online for many years without requiring that components be replaced or directly maintained.

IV. Security And Privacy Mitigation Approaches

Technological approaches to mitigate security and privacy threats can be split into device and communication (network) level solutions [8]. In our work, following the architecture described in Section II, we also add service level mitigations. The identified techniques are an adaptation of the work of Anwar et al. [15] on the integrated healthcare paradigm to the smart connected home domain. Examples are identified from recent academic and industry sources.

A. Device Level Approaches

Device level security focuses on safeguards that are backed-in devices. This involves techniques such as hardware encryption, fail-secure device design, and device-based access control mechanisms. Approaches that propose embedding security architectures, including enhancing the Datagram Transport Layer Security [16] and implementing within hardware ciphers IEEE 802.15.4-compliant link layer security procedures [17] have been suggested. Also, optimized versions of cryptographic algorithms, such as the ECDSA, have been developed for constrained environments.

Different platforms have been also built that consider security and privacy earlier on in the design phase. One such platform is RERUM [18]. This covers security at all layers of the network protocol stack, with emphasis on device controls. It implements device protection by using secure bootstrapping, cognitive radio technology, and access control mechanisms.

From the industry side, safeguards may involve the use of hardware and firmware certified to Common Criteria and EMVCo IC Security Evaluation. Moreover, it may include the use of cryptographic algorithms that are approved for instance by the National Institute of Standards and Technology.

The current challenge still remains that most of the devices have severe resource constraints and the emerging standards are mostly experimental limiting their broader applicability and industrial acceptability. Additionally, it may not be feasible on a large scale with potentially high additional costs compared to the cost of traditional IoT devices.

B. Communication Level Approaches

Communication level solutions are effective when data is being transmitted between devices, services, and end-users. Popular schemes involve the use of Virtual Private Networks (VPN), firewalls, and Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). This approach is usually implemented in a central gateway/proxy and in the cloud.

The applicability of firewalls, IDS and IPS, within the smart connected home context has been discussed by Mantas et al. [19]. Instead of using firewalls and IDS/IPS approach, Nguyen et al. [20] use a TOR-based anonymous system to help protect user privacy and make the smart home appliances more secure.

Recently, specialized smart home devices that connect to the home router acting as network gatekeepers started appearing in the market. For instance, Cujo, Dojo and Keezel are examples of this. Cujo and Dojo act as firewall devices monitoring, analyzing, and blocking threats in real-time. Keezel creates a VPN tunnel to encrypt devices and connections.

Security organizations such as the European Network Information Security Agency and Cloud Security Alliance have in recent years come up with extensive documentation that especially elaborates on network level safeguards.

However, in practice the challenge remains that some devices may roam around the network and communicate over encrypted channels. This makes traffic analysis difficult unless deep-packet inspection technology is supported. Furthermore, devices may still be prone to local attacks, for instance, malicious code installed through a compromised memory stick.

C. Service Level Approaches

Service level approaches are focused on high-level software resources. Typical approaches involve secure development processes such as security testing, secure design principles, and data masking. The latter may include the use of privacy preserving techniques such as k-anonymity and cryptographic schemes, such as Attribute-Based Encryption.

From the industry perspective, organizations such as the Open Web Application Security Project are involved in providing secure development guidance such as assessment frameworks and testing guides for developing IoT devices. Other organizations such as Builditsecure.ly and I Am the Cavalry provide guidance to build up security engineering processes. There are also sites such as BugCrowd that allow developers to have security analysts perform code reviews.

In practice, however, there is no official governing body or organization that provides the assurance to end-users about the reputation a particular service provider carries. Furthermore, certain techniques while they increase privacy or security may carry side-effects. For instance, they may lead to information loss, and may affect personalization features required for certain home devices.

V. Smart Connected Home Research Directions

Following the observations from the previous sections, several critical security and privacy issues might go unnoticed or poorly addressed by researchers as the commercial side of this paradigm is evolving at high pace. This section discusses some prominent areas where further investigation is required.

Identity management: Devices, especially when connected to the Internet, and allow for the operation and control by third-parties require strong authentication and authorization controls. Designing an effective identity management solution requires the design of secure key management protocols. However, this is hard to implement for wireless sensor network setups [11], and is further complicated by the disparate sometimes non-interoperable technologies, and the lack of global ID schemes [21]. Another challenging aspect is that authentication procedures can be complicated for particular individuals and may raise additional privacy concerns.

Risk assessment methods: It is hard for the house owner to estimate the financial value of his/her private data. This is because they might not be aware of which personal data that is collected and whether that data has been divulged to parties that they are not aware of. Also, they may not necessarily understand how easy it is to extract such data and use it for nefarious purposes.

The need for empirical risk evaluation methods for use within smart connected homes have been identified as an important security and privacy requirement [22].

Information flow control approaches: The aggregation of sensed data can provide intimate data on the behaviors and activities of residents. Easier-to-understand user interfaces that can help display privacy risks more intuitively, and at the same time offer configurable functions to control subsequent uses and dissemination of such data [23] are needed. This is also a challenging requirement to meet as IoT devices may be designed to act autonomously without any manual guidance from users. Similarly, there is a need to develop effective measures that allow for securely deleting stored data especially to meet regulatory requirements.

Security management methods: Information security management methods including better approaches to patching, updates, and provisioning of information to households are missing [24]. Similarly, it was observed [22] that a need for the integration of security in design and of sound secure management processes is typically not included in the development of smart connected homes. Moreover, there is a shortage of privacy by design measures in the smart home space [24].

VI. Conclusions And Future Work

A home is the place where privacy is expected to be respected. In comparison to traditional digital systems, most smart home devices have processing power, memory, and energy limitations. This makes the development of effective security and privacy measures harder to implement in the smart home environment. Moreover, privacy concerns are intricate and not always readily evident. Even so, enforcing privacy and security in homes must be considered a prioritized task.

We have surveyed the most pertinent security and privacy challenges of smart connected homes. Additionally, we have identified mitigation approaches at different architecture levels, and proposed areas where further research is required.

As a common observation, several initiatives are currently forming to implement security and strengthen user privacy Despite this, we have identified four significant challenges that need to be addressed: identity management, risk assessment methods, information flow control approaches, and security management methods. Such challenges are amplified in the domain of smart homes but are also common to other IoT application areas.

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] D. J. Cook *et al.*, "MavHome: An agent-based smart home," *IEEE International Conference on Pervasive Computing and Communications, San Diego, CA, USA*, pp. 521-524, 2003

[2] N. King, "Smart home - A Definition," *Milton Keynes: Intertek Research and Testing Centre*, 2003

[3] Statista, 2015 [Online]. Available: https://goo.gl/89rRIa

[4] August and Xfinity, "The Safe and Smart Home: Security in the Smart Home Era," 2016 [Online]. Available: http://goo.gl/UGWb5Z

[5] V. Srinivasan *et al.*, "Protecting your daily in-home activity information from a wireless snooping attack," 10th international conference on Ubiquitous computing, pp. 202-211, 2008

[6] B. Ur *et al.*, "The current state of access control for smart devices in homes," Workshop on Home Usable Privacy and Security, 2013

[7] S. Notra *et al.*, "An experimental study of security and privacy risks with emerging household appliances," IEEE Conference on Communications and Network Security, pp. 79-84, 2014

[8] V. Sivaraman *et al.*, "Network-level security and privacy control for smart-home IoT devices," Wireless and Mobile Computing, Networking and Communications, pp. 163-167, 2015

[9] T. D. P. Mendes *et al.*, "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources," *Energies*, vol. 8, no. 7, pp. 7279-7311, 2015

[10] C. Debes *et al.*, "Monitoring Activities of Daily Living in Smart Homes: Understanding human behavior," *IEEE Signal Processing Magazine*, vol. 33, no. 2, pp. 81-94, 2016

[11] C. Lee *et al.*, "Securing smart home: Technologies, security challenges, and security requirements," IEEE Conference on Communications and Network Security, pp. 67-72, 2014

[12] K. Islam *et al.*, "Security and privacy considerations for wireless sensor networks in smart home environments," *Computer Supported Cooperative Work in Design, IEEE 16th International Conference on*, pp. 626-633, 2012

[13] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, pp. 103-105, 2003

[14] M. M. Hossain *et al.*, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," Services, pp. 21-28, 2015

[15] M. Anwar *et al.*, "Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges," *Health Policy and Technology*, vol. 4, pp. 299-311, 2015

[16] S. L. Keoh *et al.*, "Securing the internet of things: A standardization perspective," *Internet of Things Journal, IEEE*, vol. 1, no. 3, pp. 265-275, 2014

[17] D. Altolini *et al.*, "Low power link layer security for IoT: Implementation and performance analysis," Wireless Communications and Mobile Computing Conference, pp. 919-925, 2013

[18] H. C. Pohls *et al.*, "RERUM: Building a reliable IoT upon privacy-and security-enabled smart objects," Wireless Communications and Networking Conference Workshops, pp. 122-127, 2014

[19] G. Mantas *et al.*, "Security in smart home environment," *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*, pp. 170-191, 2010

[20] N. P. Hoang and D. Pishva, "A TOR-based anonymous communication approach to secure smart home appliances," Advanced Communication Technology, pp. 517-525, 2015

[21] A. Riahi *et al.*, "A systemic approach for IoT security," Distributed Computing in Sensor Systems, pp. 351-355, 2013

[22] A. Jacobsson and P. Davidsson, "Towards a Model of Privacy and Security for Smart Homes," *IEEE 2nd World Forum on Internet of Things*, vol. 2, pp. 727-732, 2015

[23] M. Henze *et al.*, "A comprehensive approach to privacy in the cloud-based Internet of Things," *Future Generation Computer Systems*, vol. 56, pp. 701-718, 2016

[24] 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