Towards a Model of Privacy and Security for Smart Homes

Andreas Jacobsson
Internet of Things and People Research Center
Dept. of Computer Science
Malmö University
Malmö, Sweden
andreas.jacobsson@mah.se

Paul Davidsson
Internet of Things and People Research Center
Dept. of Computer Science
Malmö University
Malmö, Sweden
paul.davidsson@mah.se

***Abstract*— The domain of smart home environments is viewed as a key element of the future Internet, and many homes are becoming "smarter" by using Internet of Things (IoT) technology to improve home security, energy efficiency and comfort. At the same time, enforcing privacy in IoT environments has been identified as one of the main barriers for realizing the vision of the smart home. Based on the results of a risk analysis of a smart home automation system developed in collaboration with leading industrial actors, we outline the first steps towards a general model of privacy and security for smart homes. As such, it is envisioned as support for enforcing system security and enhancing user privacy, and it can thus help to further realize the potential in smart home environments.**

Keywords—smart home; security; privacy; IoT.

I. INTRODUCTION

Homes are currently becoming "smarter" through the use of Internet of Things (IoT) technology to improve home security, energy efficiency, entertainment, and comfort [15]. For instance, it has been estimated that 90 million people around the world will live in smart homes in the near future [7]. Smart home technology is attracting more and more attention from commercial actors, such as, energy companies (e.g., E.On and Direct Energy), home security providers (e.g., Verisure/ Securitas Direct and Frontpoint), software and hardware vendors (e.g., Apple, Samsung/SmartThings, and Google/Nest), and standardization organizations (e.g., ZigBee Alliance). In addition, there are non-commercial stakeholders, such as, various governmental institutions and municipalities, as well as, the end-users.

This situation reinforces the challenges brought on by the complexity and the heterogeneity of massively inter-connected services and devices, and it is argued that there is no well-established practice to design such systems [1]. In particular, methods for dealing with crucial system requirements, such as, security and privacy, are currently missing [10]. As a result, there are multiple vertical solutions where vendors claim to support the whole chain from the sensors and devices to the gateways and servers, with whatever dedicated software that is appropriate in the perspective of the specific company. This creates a complex situation where, among many things, it is hard to avoid customer lock-in, something which may further smother their involvement and commitment. It also creates difficulties for executing system-hygienic tasks, such as, analyzing risks, enhancing privacy, and enforcing information security in these environments.

In IoT systems, particularly in those that involve human actors, understanding the risks related to the use and potential misuse of information about customers, partners, and end-users, is not straightforward and thus requires substantial analysis [4][17]. In fact, enforcing security in IoT systems has been identified as one of the main barriers for realizing the vision of smart, energy-efficient homes and buildings [10]. Based on the main findings from a recently conducted risk analysis study of a smart home system, we take the first steps towards a general model of privacy and security for smart homes.

This paper is organized as follows. First, we go through related work and describe the man observations in terms of the state of the art of privacy and security for smart homes. Then, we give an overview of a case study, where the results from a risk analysis study of a smart home automation system are summarized. The results from the case study and the main observations in the related work point to where more research attention on security and privacy in smart homes should be put. Consequently, we introduce a model of security and privacy for smart homes. The central components of the model are also outlined and discussed in more detail. In the end, the conclusions and suggestions for future work are presented.

II. RELATED WORK

Below, we summarize the most relevant recent work in the area of smart home security and privacy. A more extensive description of related work has been previously published and can be found in [8].

A. Security and Privacy Risk Analysis Contributions

Denning et al. [4] survey the security and privacy landscape in IoT-based smart homes, and provide a strategy for reasoning about security needs. They use a scenario-based method consisting of three components, i.e., the feasibility of

conducting an attack, the attractiveness of the system as a compromised platform, and the damage caused by executing an attack. The first two factors, when combined, provide some indication of the likelihood that an adversary will compromise the device in question, while the third factor helps to weigh the overall risk. A strong merit is the framework for articulating key risks associated with particular devices in the home, which includes identifying human assets, security goals, and device features that may increase the risk posed by individual technologies. However, since the devices and technologies used in the digital home are grouped together, the framework excludes technical nuances, such as, those entailed by problems with, e.g., transport encryption of data, limited CPU-storage on connected units, etc.

The belief that smart home environments add new cyber risks in addition to existing ones is explored in the work of Roman et al. [16], where an account for threats to security and privacy is provided. While their reflection on this is interesting, they do not provide any information on how to identify the risks that are present and how they should be handled. They conclude that, in order to manage the variety of threats facing IoT-connected homes, important problems to analyze that remain are, e.g., data and identity management, user privacy, and methods in support of resilient architectures.

Djemme et al. [5] have proposed a risk assessment framework and software toolkit for cloud service ecosystems, of which the digital home is viewed as an example. They stress that concerns, such as, risk, security, cost, and legal factors underpin the non-functional properties of such ecosystems, and thus highlight the importance of effective risk management methods. The main contribution is a risk assessment model, which comprises four categories, i.e., legal, technical, policy, and general. As such, it excludes the otherwise important user perspective, which of course is central to any risk analysis of the smart home.

Kirkham et al. [9] explore cloud computing in the context of home resource management and propose a risk-based approach to data sharing between the home and its external services using key indicators related to risk, cost, and efficiency. The risk model is based on a use case for home resource management and provides means to calculate the legal risk, the appliance failure risk, and the resource security risk. They point out the need for further study on the integration of risk calculation in IoT-intense domains; especially in smart home environments inhabited by (human) users, where a lot of potentially sensitive data is in traffic. However, a general lack of access to quality data is acknowledged as a hindering factor in further developing knowledge about the risk exposure of smart homes.

B. Security and Privacy Design Contributions

In the work by Babar et al. [3], an embedded security framework for IoT environments is proposed. Based on a review of network-based attacks on IoT systems, they investigate the need to provide built-in security in the connected devices to provide a flexible infrastructure for dynamic prevention, detection, diagnosis, isolation, and countermeasures against successful security breaches. Based on this analysis, they define security needs while taking into account computational time, energy consumption, and memory requirements of the connected devices, i.e., while they set out to do a comprehensive view of security risks, they only focus on hardware and software components. However, they also say that risk analyses that fuel an understanding of both technical, as well as, human aspects, need to be applied to help define the security requirements of IoT-connected homes.

Gan et al. [6] focus on the application of technologies in IoT environments and target security-enhancing solutions to network points of entry. They say that major risks consist of instantiations of malicious software and hacking techniques, and that they are particularly important threats to mitigate by, e.g., authentication procedures in the connected devices and cryptography between the communicating objects.

Van Kranenburg et al. [12] investigate security issues of communicating objects in smart homes. The say that the resource-constrained (e.g., memory and CPU capacity) configuration that characterizes many of the communicating devices in a smart home do not permit to implement standard security solutions, which therefore make smart homes vulnerable to security attacks.

Notra et al. [13] dissect the behavior of household devices in connected homes, and highlight the ease with which security and privacy can be compromised. The most interesting part of their work is the experimental vulnerability analysis of popular smart home devices, in which they have identified a strong need for user-friendly and computer resource-efficient access control mechanisms.

Arabo et al. [2] identify challenges and implications of privacy with respect to connected devices, of which some examples are identity theft, social engineering attacks, points of entry for a cyber attack, and social network-based threats, such as, grooming and cyber-bullying.

Kozlov et al. [11] discuss threats to privacy and security at different architectural levels of the smart home. They especially advertise for privacy control mechanisms, methods to analyze privacy risk levels, and energy aspects of security, privacy, and trust, as they are closely related to energy consumption of the entire smart home infrastructure

C. Main Observations

Based on the related work reviewed above, the following observations can be made:

- There is a general need for empirically based methods, which are based on original quality data, and that support the evaluation of risks in smart home environments. Without such methods, the implemented security solutions risk not meeting the desired security and privacy goals of the smart home.

- There is a general need for the integration of security in design. Risk analysis perspectives are typically put on the connected home from the outside, i.e., risk analysis is not included in the design and development phases of smart homes. Security in design is crucial for mitigating the threats posed at such IoT-connected environments, especially in terms of malware mitigation, access control, and privacy disclosure. Sound security management must also contribute to the overall system requirements, something that is facilitated for during system development and design.
- The risks to user privacy need further specification. As information generated within the smart home often is of a personal nature, and thereby generally must be considered sensitive, exposure to privacy breaches needs attention to illustrate the potential intrusions to the personal sphere of the home.

III. A Risk Analysis Applied on a Smart Home

In a joint research project involving leading industrial actors in the segment of home/building automation, a generic platform that integrates various vendors' systems has been developed[1]. Using this platform, third party software applications can both monitor energy consumption and remotely control electronic devices in the homes and buildings. The open system architecture allows end-users to access various applications through an ecosystem of online services and smartphone applications. In this connected and complex environment, a systematic and empirically founded risk analysis has been undertaken. It was based on the information security risk analysis methodology as described in [14]. This method, below summarized in the form of a case study, is widely used in the information security community and is set to identify and evaluate the most severe potential security threats directed towards an information system.

A. Approach

The platform's risk exposure was systematically reviewed based on its ability to fulfill the three basic goals of system security, i.e., confidentiality, integrity, and availability. The risk analysis was carried out with a group of security engineers, domain experts, and system developers. An open questionnaire was used in order to reason, identify, analyze, and evaluate threats, their linking to system vulnerabilities, as well as, their likeliness of occurrence and potential impact to the smart home. In the end, the likeliness of occurrence and potential impact to the entire smart home was discussed and assessed.

In order to reduce complexity in this task, an information system-based approach to analyzing threats, vulnerabilities, and risk levels of the smart home was applied. The architecture of the smart home automation system was consequently viewed in analogy of an information system and thus divided into subcategories containing software, hardware, information, communication protocols, and the human actors (whether as end-users or as representatives for, e.g., vendors). This means that the system components (sensors, gateways, servers, APIs, applications, mobile devices, etc.) of the smart home were grouped in these categories. Each of the system components was thus analyzed with respect to vulnerabilities and threats related to hardware, software, information, communication, and human aspects. Since the approach was based on original quality data (both system-wise and risk analysis-wise), it can be argued that an adequate overview of the risk exposure of a smart home automation system was generated.

[1] See http://elis.mah.se/ for more information.

B. Results

Out of 32 identified and examined risks, 9 were classified as low and 4 as high, i.e., most of the risks were considered moderate. The risks classified as high were either related to the human factor (e.g., poor password configuration, unauthorized redistribution of confidential information among the system providers, and social engineering or hacking exploitation attacks) or to software components (e.g., inadequate accountability within the in-house gateway as system events were not logged, and inadequate authentication schemes in the API).

Based on this, it was concluded that a main source of risk was connected to the software, and especially in the APIs, and to components within the mobile apps, which permitted users to gain access to system resources without having proper credentials. The hardware-related risks concerned theft, manipulation, and sabotage of the various devices and servers used within the smart home. In particular, a severe risk derived from unauthorized modification/tampering of physical sensors and the in-house gateway in the home. The highest ranked risk with respect to the information processed derived from inadequate access control configuration in the in-house gateway, primarily connected to weak authentication procedures and inadequate separation of privileges between user accounts, i.e., access control. Within network communication, the main risks came from poor authentication and confidentiality settings. In this case, a severe risk related to manipulation, duplication, surveillance, and deletion of information in transit between the sensors, the in-house gateway, and the cloud server. With respect to human-related risks, the most probable risk related to poor password selection, which could lead to that authentication mechanisms were omitted. The most severe consequence was associated with two risks, the first concerned unauthorized redistribution of confidential information among system or cloud providers, the second concerned hacking exploitation attacks or intrusion attempts from malicious actors.

C. Main Observations

Based on the results from the case study, it was found that at least the following issues need attention:

- The most severe risk factor, confirmed in the risk analysis, was a combination of software and the human end-user.
- Security-enhancing mechanisms are particularly important in smart home environments, where a lot of personal information is in flux. In this respect, software security needs particular attention.
- Privacy-enhancing mechanisms are needed to ensure that the home, when connected to the Internet, remains private

rather than becomes public. The user (while remaining private) should be the staring point for this.
- Security and privacy mechanisms (that support both technology and human users) should be included in the design phase of smart homes, and not added as an extra feature when the system has been set to operation.

IV. Towards a Model for Privacy and Security

While a holistic perspective on security in smart homes generally desired, the results from the case study suggest that software security and user privacy should be the main focus. As these requirements not ideally should be put on the system as an added feature afterwards, we propose a model that integrates security and privacy into the design of smart home services and systems. This model is envisioned as general support for both developers and providers of smart homes, as well as, the users, i.e., for the entire smart home ecosystem. It could of course be argued that the users in fact have no interest for such a model, but since not only the digital, but also the physical side of the users and their homes can be affected by, e.g., malware, surveillance and spam attacks, security and privacy cannot be questions that solely concern product developers and service providers. In addition, the model is expected to help raise the level of awareness of privacy and security in general IoT-environments, where sensitive user-generated information is an integral part.

The model is being developed together with an industrial partner that is one of the leading actors in the segment of smart home security services[2]. The main components that have been identified are presented and discussed below.

A. A Generic Description of the Smart Home,

A generic description of the smart home serves as a basis for the model. It will include the different types of components (devices, people, pets, infrastructure, etc.), stakeholders (residents, guests, system providers, etc.), and services (security, energy, comfort, entertainment, etc.) involved in smart homes. This also requires a deep understanding of the data in flux of the smart home. Thus, an information classification scheme is needed. Such as scheme is in fact a categorization of the data generated in smart homes in terms of the contents, structure, as well as, potential implications to the personal privacy. The scheme comprises all the data that is generated, stored, processed, and distributed related to the smart home. This aspect is fundamental in deciding the sensitivity of the information, of which some is personal or private, that is in flux in this type of highly connected human-in-the-loop cyber-physical systems. However, it must of course be considered that the classification of certain data generated in the smart home may only be meaningful in the context of other information. Thus, the study of different structural types of data, such as, metadata, is also included in this context.

B. Risk Analysis Methods

Methods supporting the evaluation of the risk exposure, resulting in a map of the security and privacy risks of smart homes is essential for the deployment of effective security measures. In terms of data collection, such methods could both be qualitative (e.g., a scenario-based study), quantitative (e.g., various software-based products) or semi-quantitative (e.g., as in the case study presented in III). A main point argued here is the need for access to original quality data and that the analysis of the risks includes an evaluation method that helps define the actual need for the security and privacy supporting measures. How personal information is handled in the home environment and the ecosystem of people, machines, information, and other stakeholders involved are key components. It is of course also crucial to include the social behavior of human actors (both as benevolent users and as villains) in this analysis. The results from the case study indicate that the urgency of this analysis is accentuated for software components and human users, but all parts of the smart home must be of course included here. Even so, some of the predicted constraints are, for instance, the physical environment, people coming and going to and from the house, malicious use of benevolent services, etc.

C. Security Design Principles and Technologies

A set of smart home security design principles will be defined, which is based on the requirements concerning confidentiality, integrity, and availability, to enable control of the risk exposure. They will provide empirically founded guidelines on how to mitigate the risks identified in B. This will also comprise the design of a set of appropriate security-enhancing technologies to protect the user information that is collected, modified, and stored within the home, and transferred over the Internet to cloud services and further on to mobile apps. While ensuring data protection, these technologies must also provide resilience against malicious activities (e.g., malware, spyware and hacking attempts, Denial-of-Service attacks, etc.). Since this takes place in an IoT-context, limitations in CPU power on the connected entities, diversity of computing devices, different types of information, home configuration properties, usability aspects, etc. must be taken into account.

D. Privacy-Awareness Support Methods

A set of privacy-aware smart home information management methods will be developed and included in the model. They are envisioned as useful in order to reduce sensitivity, i.e., with respect to unpersonalization, of the smart home information in transit, as well as, in its connection to the digital ecosystem it engages with. Methods for reducing sensitivity in information, such as, adjustable anonymity and linkability, as well as, data minimization and control are thus included in this part of the model. Thereby, the stakeholders' various interests, and the user's in particular, concerning smart home services and information can be met while at the same time preserving privacy.

V. Discussion

When developing the model, it is of course important to take into account the specific circumstances regarding both the technology and the user-interaction that form the smart home environment, i.e., both the user and the technology play central roles. A major challenge is to find effective ways to provide

[2] See http://iotap.mah.se/ismash/ for more information.

users with a comprehensive picture of the entire system, and an indication of the sensitivity of data in transit, while also supporting the management of the home. Digital traces that the users (more or less voluntarily) leave behind when using a smart home can provide meta-information about the family members' habits, i.e., help to build extensive individual and collective profiles of the residents of a home. In addition to the physical consequences that may occur as a result of this, e.g., in terms of burglaries, the idea of the home as a private sphere may no longer prove to be accurate. Instead, the home may become a public area where the companies behind the connected devices will come to know a particular resident better than his/her closest friends or family do.

Since autonomy is already a feature of some IoT solutions developed for the connected home, an interesting challenge is to explore the extent to which security and privacy can be integrated in such a context. Therefore, we will use the model to try to integrate security and privacy in the, at least partially, autonomous decision-making process of the connected entities that form the smart home system. This work will provide valuable insights on the extent to which smart homes could be automated, and pointers for how this could be done in such a way that user privacy can be guarded and information security ensured.

When the security and privacy model is fully developed, the users of smart homes will be able to be in more control of the personally identifiable information generated, and they will also have the means to decide how to use it. For communities, this may imply improved means for energy-efficiency and physical security. With a model of security and privacy in design in place, it may thus contribute to enforcing system security and enhancing user privacy in smart homes.

VI. Concluding Remarks

In this paper, we have accounted for the recent advancements within smart home security and privacy. We have also summarized the results and main observations from a case study involving a risk analysis applied on a smart home automation system. Based on this, we have introduced the main components of a new model for privacy and security in smart homes. The central concepts of the model have been identified in order to address methods supporting the evaluation of risk exposure, security design principles to enable control of the risk exposure, and privacy-aware information management. However, these challenges are difficult to address if there is no understanding of the information in flux of the smart home, which consequently points to the need for information analysis and classification. An interesting idea is also to integrate security and privacy in the, at least partially, autonomous decision-making process of the connected entities that form the smart home system.

The model is envisioned as general support for both developers and service providers of smart homes, as well as, the users of them. Even though it is tailored for smart homes, it is also expected to help raise the level of awareness of privacy and security in general IoT-environments, where sensitive user-generated information is an integral part. When such a model of security and privacy in design is implemented, it will contribute to enforcing system security and enhancing user privacy, and thus helping to further realize the potential in such IoT environments.

VII. Future Work

Future work includes the development of the different parts of the proposed model and to apply the model to real world cases. There is also a need for a general and concise description of the smart home concept that can serve as a reference model for further advancements in the area. Security and privacy aspects related to user interaction and the design of the connected smart home products and services also need further attention. A key challenge towards secure and private smart homes that remains is the analysis and evaluation of risks with respect to the information in flux. With such knowledge in place, the design of security and privacy supporting systems will be efficient and the barrier of growth for energy-efficient and secure Internet-connected homes can be overcome.

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 11 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] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home Automation in the Wild: Challenges and Opportunities", Proc. of the ACM Conference on Human Factors in Computing Systems, 2011.

[2] A. Arabo, I. Brown, and F. El-Moussa, "Privacy in the Age of Mobility and Smart Devices in Smart Homes", Proc. of Int. Conf. on Social Computing, 2012.

[3] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)", Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, 2011.

[4] T. Denning, T. Kohno, and H.M. Levy, "Computer Security and the Modern Home", Comm. of the ACM, Vol. 56, No. 1, 2013 pp. 94-103.

[5] K. Djemme, D.J. Armstrong, M. Krian, and M. Jiang, "A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems", Proc. of the 2nd Int. Conf. on Cloud Computing, GRIDs, and Visualization, 2011.

[6] G. Gan, Z. Lu, and J Jiang, "Internet of Things Security Analysis", IEEE Conf. on Internet Technology and Applications, 2011.

[7] "The Internet of Things: Manage the Complexity, Seize the Opportunity", white paper by Oracle, 2014. Available at http://www.oracle.com/us/solutions/internetofthings/iot-manage-complexity-wp-2193756.pdf Last checked: 2015-06-22.

[8] A. Jacobsson, M. Boldt, and B. Carlsson, “A Risk Analysis on a Smart Home Automation System”, Future Generation Computer Systems, Elsevier, 2015. DOI:10.1016/j.future.2015.09.003.

[9] T. Kirkham, D. Armstrong, K. Djermame, and M. Jiang, “Risk Driven Smart Home Resource Management Using Cloud Services”, Future Generation Computer Systems, Vol. 38, pp. 13-22, 2013.

[10] T. Kowatsch and W. Maass, “Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts”, Knowledge and Technologies in Innovative Information Systems, Lecture Notes in Business Information Processing, Vol. 129, Springer, Dordrecht, 2012, pp. 200-211.

[11] D. Kozlov, J. Veijalainen, and Y. Ali, “Security and Privacy Threats in IoT Architectures”, Proc. of the 7th Int. Conf. on Body Area Networks, 2012.

[12] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, and M. Ratto, “The Internet of Things”, Proc. of the First Berlin Symposium on Internet and Society, 2011.

[13] S. Notra, M. Siddiqi, H.H. Gharakheili, V. Sivaraman, and R. Boreli, “An Experimental Study of Security and Privacy Risks with Emerging Household Appliances”, Proc. of Int. Workshop on Security and Privacy in Machine-to-Machine Communications, 2014.

[14] T.R. Peltier, Information Security Fundamentals, 2nd Ed., Taylor & Francis Group, Boca Raton, 2014.

[15] V. Rickebourg and D. Menga, “The Smart Home Concept: Our Immediate Future”, 1st Int. Conf. on E-Learning in Industrial Electronics, 2006.

[16] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things”, IEEE Computer, Vol. 44, no. 9, 2011, pp. 51-58.

[17] M. Rozenfeld, “The Value of Privacy – Safeguarding Your Information in the Age of the Internet of Everything”, The Institute, IEEE, March 7, 2014.