Problems of privacy and security in cyber physical systems of intellectual houses

Bohdan Havano[1]

1. Computer engineering, Lviv Polytechnic National University, Ukraine, Lviv, Bandery str., E-mail: havano.bohdan@gmail.com

In this paper, is presented an overview of the privacy and security challenges directed towards the smart house domain. Also, were identified constraints, evaluated solutions, and a number of challenges and research issues where further investigation is required. I have identified four significant challenges that need to be solved: identity management, risk assessment methods, information flow control approaches, and security management methods.

Keywords – smart house, cyber physical system, IoT, privacy, security.

Introduction

A smart connected house 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. However, the increasing deployment of Internet-connected devices in the house expose the residents to privacy and security risks as personal information becomes remotely accessible in different ways.

Research directions

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. It 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 [1], and is further complicated by the disparate sometimes non-interoperable technologies, and the lack of global ID schemes. 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 houses have been identified as an important security and privacy requirement [2].

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 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 [3].

Similarly, it was observed [2] 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 houses. Moreover, there is a shortage of privacy by design measures in the smart house space [3].

Conclusion

A house is the place where privacy must be respected. In comparison to traditional digital systems, most smart house devices have processing power, memory, and energy limitations. This makes the development of effective security and privacy measures harder to implement in the smart house environment. Moreover, privacy concerns are intricate and not always readily evident. Even so, enforcing privacy and security in houses must be considered a prioritized task. I have surveyed the most pertinent security and privacy challenges of smart connected houses. 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, i 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 houses but are also common to other IoT application areas.

References

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

[2] 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

[3] 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