CSE 564 Project Proposal

Chandrakana Nandi (cnandi), Jeanette Daum (jdaum)

Title: **Specifying and Verifying Security Policies for Smart Homes**

1 Motivation

Smart homes are becoming popular as one of the applications of Internet of Things. Typically, a smart home consists of devices interacting with each other and taking actions autonomously or being controlled remotely by the home inhabitants. In this project, we consider a smart home to be a collection of interacting devices acting autonomously without requiring the user to intervene. A challenge for smart homes is to ensure that there are no security loopholes because they can be exploited by malicious attackers to take control of the house and harm the inhabitants [7, 9]. Before smart homes become as widespread as smart phones are today, it is necessary for the home automation industry to address these concerns.

2 Problem definition

Verifying security and correctness for home automation systems is very important because violation of security can have a negative impact on the lives of the home inhabitants. In this project, our goal is to ensure that a system of interacting smart devices satisfies a set of security properties. We aim to solve the problem of security for smart homes from the point of view of the manufacturers of the smart devices so that they can claim that their devices are verified to be secure and correct and the end users can rely on them. We will focus on the security of the devices and not on the lower level details of a home automation system such as the communication protocols. Some solutions for ensuring security of smart homes have been proposed but they are either too general and do not address the problems specific to smart homes [6] or are based on dynamic techniques [5]. The problem with the latter is that if a security loophole is encountered, then the system has to be stopped which makes it unreliable. Our approach will be static, providing compile time guarantees that the system satisfies a set of security specifications and will also be more expressive than the existing solutions in the sense that it will allow us to specify many different types of security properties.

3 Planned approach

Following is our plan of action for this project:

1. We looked at the existing home automation platforms and found that most of them are closed-source [8, 1, 4, 2, 3].
2. Based on our finding, we have decided to implement our own prototype. To this end, we have designed a high level architecture for modelling smart homes which abstracts away the lower level details such as the communication protocols used by the devices but is expressive enough to model the existing smart systems in the market.
3. We have formalized three types of security and correctness policies for a smart home to satisfy.
4. Based on our architecture, we will implement a platform for developing smart devices.
5. We will design and implement algorithms for verifying the policies.
6. For evaluating our tools, we will develop prototypes of smart systems for which we will specify and verify the three security and correctness policies mentioned above.

4 Evaluation

One of our major contributions will be a high-level architecture for modelling smart homes. We plan to implement a platform based on our architecture and prototypes of smart systems to be executed on that platform. To evaluate the verification tools we plan to develop, we will use these prototypes.

Further, as mentioned in section 3, most of the existing home automation platforms are closed-source. Contacting their manufacturers/developers and requesting them to give us access to the source code, then understanding the code and finally being able to implement verification tools in 8 weeks (which is the amount of time we have remaining) is not feasible because it takes a lot of time to come to any agreement with the companies and it is also risky to rely on their support for getting their platforms to work.

5 Milestones and dates

Items 1, 2 and 3 mentioned in section 3 have already been accomplished. The milestones we aim to meet in the remaining 8 weeks and the corresponding dates are given in table 1.

	milestone	date
1	Implement a platform for developing smart devices based on our smart home architecture and two to three sub-systems to be used for evaluation later	2/8/2016
2	Design algorithms for verifying the three types of security and correctness policies	2/11/2016
3	Implement the algorithm for the first policy	2/18/2016
4	Implement the algorithm for the second policy and prepare the draft of the project report	3/1/2016
5	Implement the algorithm for the third policy and do an evaluation of our tools by verifying all the policies for the benchmarks developed for milestone 1.	3/10/2016
6	Write the final report and prepare the presentation	3/14/2016

Table 1: Milestones and dates

References

[1] *echo*, 2016 (accessed January 15, 2016). `https://echo.newtechnetwork.org/?q=/ntn/login&destination=/ntlp/home`.

[2] *HomeKit*, 2016 (accessed January 15, 2016). `http://www.apple.com/ios/homekit/?cid=wwa-us-kwg-features`.

[3] *Smart Home. Intelligent Living*, 2016 (accessed January 15, 2016). `https://www.smartthings.com/`.

[4] *wink*, 2016 (accessed January 15, 2016). `http://www.wink.com/`.

[5] J. Al-Muhtadi, M. Anand, M. D. Mickunas, and R. Campbell. Secure smart homes using jini and uiuc sesame. In *Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference*, pages 77–85. IEEE, 2000.

[6] M. B. Barcena and C. Wueest. Insecurity in the internet of things. 2015.

[7] T. Denning, T. Kohno, and H. M. Levy. Computer security and the modern home. *Commun. ACM*, 56(1):94–103, Jan. 2013.

[8] C. Dixon, R. Mahajan, S. Agarwal, A. Brush, B. Lee, S. Saroiu, and P. Bahl. The home needs an operating system (and an app store). In *HotNets IX*. ACM, October 2010.

[9] B. Ur, J. Jung, and S. Schechter. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014, July 2013.