SET YOUR TITLE USING \title

I. Conclusion

1.1 Overview

This chapter summarizes the research and results found during experimental evaluation. Section 1.2 reiterates notable conclusions derived from experimentation and statistical analysis. Section 1.3 synthesizes findings to underline security and privacy risks internet of things (IoT) devices present to the home and provides practical recommendations for future IoT security. Lastly, Section 1.4 provides possibilities for future work with the Classification, Identification, an Tracking of IoT (CITIoT) tool.

1.2 Research Conclusions

The research was successful in analyzing data leakage from smart home devices using the CITIoT tool. As hypothesized, an eavesdropper was able to collect traffic from outside a smart home network to successfully identify devices, track user's presence, and deduce events such as when a door is opened or when a camera senses motion inside the home. Device classification was 94% successful with all 8 Wi-Fi devices and 9 out of 10 Bluetooth Low Energy (BLE) devices categorized each day. On average, the tool was 94% successful in identifying events. The tool failed to identify 6% of events and identified 3 events per day that did not actually occur. The tool was 100% successful in determining if the user was in the home or not. When the Mitigation of IoT Leakage (MIoTL) tool was operating, however, CITIoT failed to identify any Wi-Fi devices and events correctly. **To do** (1) These conclusions support

the original hypothesis.

A total of 6.5 GB and 43.4 million packets were captured throughout experimentation. On average, preprocessing took seconds, network mapping took seconds, classification took seconds, and tracking took seconds. The captures and results took GB of hard drive space resulting in an average GB per ten-hour day of testing.

1.3 Research Significance

In recent years, smart home devices have become one of the most popular categories in the IoT accounting for $3.5 billion of a $292 billion industry; over 29 million smart home devices are expected to ship in 2017, a 63 percent increase over 2016 [1]. As the modern home gets smarter it also becomes more vulnerable to attacks that were reserved to computers and networks. IoT devices constantly communicate data that enable an eavesdropper to infer information about people and devices within a smart home. Users must be aware of what their devices are advertising and how this information can be used against them.

For example, using the results from the CITIoT tool found during experimentation a few observations can be made about the user and smart home that have security implications: (i) the user was away from the home from 0800-1100 four days out of the week, (ii) the user used a BLE lock to secure their home, and (iii) the user has a Wi-Fi based security camera and motion sensor in their home. The event identification results point to times in the packet capture when the BLE lock was used, and from further examination it was observed that the communication between the user device and BLE lock was not encrypted and passwords were sent in the clear. Using this information and simple replay attacks, we were able to change the user and administrator password or unlock the lock at will. With the knowledge of when the user is away from the home an adversary can predict a good time to attempt to

gain access to the smart home. The adversary also knows to be aware of a Wi-Fi camera and motion sensor.

Many of the vulnerabilities used in this work take advantage of information that is not encrypted at the lower levels of the Wi-Fi and BLE protocols, therefore, to create more secure smart home devices, developers must consider security from the physical layer on up. For Wi-Fi, this includes periodically changing Media Access Control (MAC) addresses, randomizing frame size (FSize), and encrypting lower-layer data packets. In BLE, devices need to make their advertisements private. Also, common operational security methods can help prevent against smart home device attacks. For example, users should be aware that routine schedules leave them vulnerable to pattern-of-life modeling– a threat which is increased by smart devices. Maintaining unpredictable schedules will help prevent attacks. Similarly, turning on or off lights while away from home can trick an observer into thinking someone is home. It is also important to have situational awareness of potential eavesdroppers or suspicious devices around when accessing smart locks or other devices.

While these recommendations can improve the security of smart home environments, none of these ideas are new. Why, then, have these fixes not been implemented to secure against privacy leakage? In response to rapid growth of the IoT market, efforts to limit power, develop devices quickly, and other design constraints drive developers toward poor security implementation, leaving devices vulnerable. Also, while the areas of network and computer security have seen more adversarial pressure, the smart home is relatively new. Until recently, outlets, locks, and light-bulbs were not connected to networks. This is the same evolution of vehicles as they become connected to the Internet and, therefore, open to attack. The privacy implications demonstrated in this work, however, require that developers of IoT technologies consider security in design and engage with the computer security community to create

more secure smart homes.

1.4 Future Work

There are a number of avenues to take in extending the CITIoT system as the field of IoT devices and security is constantly growing. The following suggests four future work options based off this research:

- First, the number, type, and manufacturer of devices used within the **SHAA!** (**SHAA!**) can be expanded to test if the fingerprinting methods extend to other IoT devices. Only a limited selection of Wi-Fi devices were used in training the classifier.

- Second, the MAC tracker unit only observes when a user is home or away and could be expanded to track device locations within the home for better reconnaissance and tracking. A more significant tracking capability would greatly increase the CITIoT tool's ability to stress the security implications of smart home devices.

- Third, the classifier currently uses a hands-on method for training. Machine learning may be able to assist in training the classifier more efficiently and accurately.

- Fourth, program execution can be improved. Processing time and hard drive usage are limiting factors for a small battery powered device such as a Raspberry Pi and could limit the capabilities of remotely operating the CITIoT tool.

1.5 Chapter Summary

This chapter concludes the background, design, test methodology, and results of this research. It considers the synthesis of research conclusions with the real-world

implications of smart home device leakage while providing areas for future work in improving the CITIoT tool.

To do...

- ☐ 1 (p. 1): Make sure this is true.

Bibliography

1. Consumer Technology Association. "Record Year Ahead: Consumer Enthusiasm for Connectivity to Propel Tech Industry to Record-Setting Revenues," 2017. [Last accessed August 27, 2017], *https://www.cta.tech/News/Press-Releases/2016/January/Record-Year-Ahead-Consumer-Enthusiasm-for-Connect.aspx*.