***Department of Computer Science***

***Doctoral Dissertation Defense***

**Friday, March 8th, 2019 at 2:00 p.m. - 4:00 p.m.**

**Science and Engineering Hall, 4th Floor**

**Conference Room 4605**

**Yinhao Xiao**

B.S. in Information and Computing Science, June 2012, Guangdong University of Technology, Guangzhou, China

M.A. in Mathematics, May 2014, The George Washington University, Washington, D.C., USA

M.S. in Computer Science, Dec 2015, The George Washington University, Washington, D.C., USA

**DISSERTATION:**

***﻿Security and Privacy of Smart Devices***

**FIELD OF STUDY:** System Security

**ADMISSION TO DOCTOR OF SCIENCE PROGRAM:** Fall 2016

**ADVISOR OF THE CANDIDATE’S RESEARCH:**

Professor Xiuzhen Cheng

**EXAMINING COMMITTEE:**

1. Dr. Xiuzhen Cheng, Dept. of Computer Science, GWU

2. Dr. Hyeong-Ah Choi, Dept. of Computer Science, GWU

3. Dr. Arkady Yerukhimovich, Dept. of Computer Science, GWU

4. Dr. Xiang Chen, Electrical and Computer Engineering Depart., GMU

**PRESIDING:**

Professor Xiuzhen Cheng, Dept. of Computer Science

***Department of Computer Science***

***Doctoral Dissertation Defense***

**Friday, March 8th, 2019 at 2:00 p.m. - 4:00 p.m.**

**Science and Engineering Hall, 4th Floor**

**Conference Room 4605**

**Yinhao Xiao**

**School of Engineering and Applied Science**

**The George Washington University**

**“Security and Privacy of Smart Devices”**

**Abstract**

The advent of smart devices, i.e., smartphones and smart home devices, has greatly revolutionized and modernize people's daily lives in every aspect. Yet, the security condition of the devices and their corresponding systems is concerning since traditional security measures fail to cope with them due to limitations of computation power and hardware/firmware heterogeneity. In this dissertation, we present our research on studying the security and privacy issues of smartphones and of smart home devices.

Firstly, we study the OS security of Android devices. In order to facilitate apps to collaborate to finish complex jobs, Android allows isolated apps to communicate through explicit interfaces. However, the communication mechanisms often give additional privilege to apps, which can be exploited by attackers. The Android Task Structure is a widely-used mechanism to facilitate apps' collaboration. Recent research has identified attacks to the mechanism, allowing attackers to spoof UIs in Android. In this work, we present an analysis of the security of the Android task structure. In particular, we analyze the system/app conditions that can cause the task mechanism to leak privilege. Furthermore, we identify new end-to-end attacks that enable attackers to {\em actively} interfere with victim apps to steal sensitive information. Based on our findings, we also develop a task interference checking app for exploits of the Android task structure.

Secondly, we study how the side-channel information publicly available in Android devices can result in severe privacy leakage on social networks. Owing to the various features provided by mobile devices, a user's online social activities are tightly tied to his phone, and are conveniently, sometimes unnecessarily, available to social networks. In this work, we propose a novel attack architecture to show that attackers can infer a user's social network identities behind a mobile device through new dimensions. Specifically, we first developed a correlation between a user's device system states and the social network events, which leverage multiple mechanisms such as learning-based memory regression model, to infer the possible accounts of the user in the social network app. Then we exploited the social network to social network correlation, via which we correlated information across different social networks, to identify the accounts of the target user. We implemented and evaluated these attacks on three popular social networks, and the results corroborate the effectiveness of our design.

Thirdly, we explore the defense mechanisms on strengthening the smart home systems. Smart home systems have become more and more prevailing in recent years. On one hand, they greatly convenience our everyday lives; on the other hand, they suffer from the two notorious security problems, namely the open-port problem and the overprivilege problem, making their security situations extremely worrying and uncheerful. In this work, we proposed a novel credential-less authentication framework, CLAF, to effectively defend against the attacks resulted from these two security problems without the need for sensitive credentials. We further detailed an implementation of CLAF based on the side channels that are publicly available in Android smartphones serving as controllers of smart home systems and presented its workflow in protecting against various attacks caused by the open-port and overprivilege problems. Finally, we tested our CLAF implementation on a real-world smart home system and considered four threat models that cover basically all practical attacks, including Mirai and its variants. We also considered the effectiveness of our CLAF implementation on the SmartApps of the Samsung SmartThings platform, which suffers from the open-port and overprivilege problems. The evaluation results indicate that our CLAF realization can successfully defend against over 90\% attack trials with an average latency less than 1 second.