**Information Systems Technology and Design (ISTD)**

**PhD Oral Defense**

## Directed Stateful Fuzzing of Wireless Protocols

**Matheus E. Garbelini**

**PhD Candidate**

**Supervisor: Prof. Sudipta Chattopadhyay**

Wednesday, 16th August 2023, 11am – 12pm

Venue: LT 5 (Building 2, Level 5, Room 2.505)

**Abstract:**  Novel attack vectors exploiting vulnerabilities in wireless protocols have spiked in recent years. Not surprisingly, the advantages of leveraging the wireless medium to carry on seemingly invisible attacks from afar, poses new risks and challenges to the state of wireless security. As new technologies are introduced to facilitate our lives through better connectivity, so is the risk of new vulnerabilities being introduced to wireless protocols, being it on the implementation of a given wireless technology or in the standardized design of its protocol. In a perfect world, all software are believed to be extensively tested before upstream deployment. However, this argument has repeatedly been shown to be flawed, resulting in several critical software vulnerabilities in the last decade.

This thesis seeks to explore software testing techniques that can facilitate the discovery of security flaws that, if not fixed, can potentially impair the security and stability of a given wireless ecosystem. Furthermore, due to the mostly closed-source nature of the current wireless ecosystem, we focus on finding vulnerabilities in a systematically and automated fashion such that the security of arbitrary wireless devices can be tested in a practical over-the-air setup. To address such fundamental requirement, this thesis proposes a series of directed and stateful fuzzing techniques that can enable finding protocol vulnerabilities in arbitrary wireless technologies.

To this end, this dissertation guides the reader through generation-based and mutation-based over-the-air fuzzing architectures, while providing insights on how to systematically leverage low-level packet injection, sniffing, vulnerability detection, response validation, and device monitoring to test a variety of widely deployed wireless protocols such as Wi-Fi, Bluetooth Low Energy, Bluetooth Classic and 5G New Radio. Consequently, the proposed fuzzing architectures were able to find impactful implementation vulnerabilities in each of these technologies, yielding more than 50 (fifty) CVEs and over 33,000 USD in bug bounty awards.

In summary, we hope to motivate further research in wireless software security. Particularly, we seek to provide essential tooling and strong foundation that builds the next state-ofthe-art wireless security tools.

**Speaker Bio:**

Matheus E. Garbelini received the bachelor of engineering degree in electronics from the Pontifical Catholic University of Parana, in Brazil. Currently, Matheus is a PhD student, A\*Star SINGA scholar and member of ASSET Research Group. During his time at SUTD, the outcome of his research on automated wireless security testing has revealed several wireless vulnerabilities such as Sweyntooth and Braktooth. His research interests include wireless security, cyber-physical systems, IoTs, and embedded systems.

