EDGE Institute

Seminar Series on
Future Edge Networks and
Distributed Intelligence

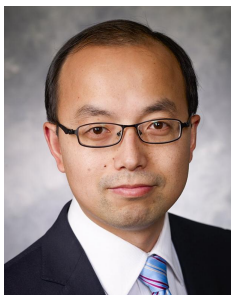
Rethinking the Security and Privacy of Bluetooth Low Energy

Zhiqiang Lin
Department of Computer Science and Engineering
The Ohio State University

December 1, 2022
1:00pm EST
https://osu.zoom.us/j/95283526626?pwd=dGFVZlN1bVV6aUN4R3FiRjU0TVdBdz09

Abstract: Being near range wireless communication technology, Bluetooth Low Energy (BLE) has been widely used in numerous Internet-of-Things (IoT) devices from healthcare, fitness, wearables, to smart homes, because of its extremely lower energy consumption. Unfortunately, the past several years have also witnessed numerous security flaws that have rendered billions of Bluetooth devices vulnerable to attacks. While luckily these flaws have been discovered, there is no reason to believe that current BLE protocols and implementations are free from attacks, since BLE consists of multiple layers with various sub-protocols and components.

In this talk, Dr. Lin will talk about a line of recent efforts for BLE security and privacy from his research group. In particular, he will first discuss the protocol-level downgrade attack, an attack that can force the secure BLE channels into insecure ones to break the data integrity and confidentiality of BLE traffic. Then, he will introduce Bluetooth Address Tracking (BAT) attack, a new protocol-level attack, which can track randomized Bluetooth MAC addresses by using a novel allowlist-based side channel. Next, he will discuss the lessons learned, root causes of the attack, and its countermeasures. Finally, he will conclude his talk by discussing future directions in Bluetooth security and privacy.



Biography: Dr. Zhiqiang Lin is a Distinguished Professor of Engineering at The Ohio State University. His research interests center around systems and software security, with a key focus on (1) developing automated binary analysis techniques for vulnerability discovery and malware analysis, (2) hardening the systems and software from binary code rewriting, virtualization, and trusted execution environment, and (3) the applications of these techniques in Mobile, IoT, Bluetooth, and Connected and Autonomous Vehicles. He has published over 100 papers, many of which appeared in the top venues in cybersecurity. He is a recipient of Harrison Faculty Award for Excellence in Engineering Education, NSF CAREER award, AFOSR Young Investigator award, and Outstanding Faculty Teaching Award. He received his Ph.D. in Computer Science from Purdue University. .