CT Advanced Computing Center (CACC) Security Seminar Series 2022-2023

Speaker: David Starobinski (Boston University)
Date: Wednesday, January 18, 2023
Time: 12:00pm - 1:30pm
Location: ITE 401
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m988feb8b21c8f7f7cb9a33a03b0a53ac
Meeting number (access code): 2624 224 8698
Meeting password: sRdgxbmp883

Network Reconnaissance for the Internet of Things

The Internet of Things (IoT) is a highly complex ecosystem. IoT devices run a multitude of different communication protocols and many devices are non-IP addressable. Discovering and monitoring IoT devices represent major challenges under these circumstances. In this work, we present a universal IoT network reconnaissance tool, called IoT-Scan. IoT-Scan is based on software defined radio (SDR) technology, which allows for a flexible software-based implementation of radio protocols. In the first part of the talk, we present a series of passive, active, multi-channel, and multi-protocol scanning algorithms to speed up the discovery of devices with IoT-Scan. We benchmark the passive scanning algorithms against a theoretical traffic model based on the non-uniform coupon collector problem. We implement the scanning algorithms and compare their performance for four popular IoT protocols: Zigbee, Bluetooth LE, Z-Wave, LoRa. Our experiments show that multi-protocol scanning leads to a 70% reduction in the discovery time of devices versus sequential passive scanning. In the second part of the talk, we consider the complementary problem of a wireless monitor that must implement a multi-channel scanning policy to minimize the Age of Information (AoI) of received information. We model this problem as a Markov Decision Process (MDP). To address the curse of dimensionality, we propose practical scanning policies of low computational complexity. We evaluate these policies using time-series data obtained from real IoT device communication traces, and show that a policy, coined Greedy Expected Area (GEA), performs well in many scenarios.

Bio: David Starobinski is a Professor of Electrical and Computer Engineering, Systems Engineering, and Computer Science at Boston University. He received the B.Sc., M.Sc. and Ph.D degrees, all in Electrical Engineering, from the Technion-Israel Institute of Technology. He also had visiting positions at UC Berkeley, EPFL, and the US DOT Volpe National Transportation Systems Center. Dr. Starobinski received a US National Science Foundation (NSF) CAREER award, a US Department of Energy (DOE) Early Career award, BU ECE Faculty awards for outstanding teaching performance in 2010 and 2020, best paper awards at the WiOpt 2010, IEEE CNS 2016, and IEEE ICBC 2020 conferences, and a 3rd place best paper award at the IEEE WF-IoT 2022 conference. He was on the Editorial Boards of the IEEE Transactions on Information Forensics and Security, IEEE/ACM Transactions on Networking, IEEE Open Journal of the Communications Society. His research interests are in cybersecurity, wireless networking, and network economics.

UCONN

CACC