CAE Tech Talk

20 April 2023

The Concept of Zero Trust: Tenets, Architecture, and Threats (1:00 – 1:50 pm EST)

Rethinking the Security and Privacy of Bluetooth Low Energy (2:00 – 2:50 pm EST)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. Capitol Technology University (CTU) hosts the presentations using Zoom which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Below is a description of the presentations and logistics of attendance:

PRESENTATION #1

Topic: The Concept of Zero Trust: Tenets, Architecture, and Threats

Time: 1:00pm – 1:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

Presenter(s): Prof. Dipankar Dasgupta, The University of Memphis

Description: Zero trust is a new concept in cybersecurity, it provides a strategy and implementation process to have more secure cyberspace. In this talk, I will introduce the concept of zero with some analogy for illustration. Utilizing the principle of "never trust, always verify, continuous monitoring and isolation", Zero Trust has become important strategy for cybersecurity industry. Different architecture of zero trust, fundamental tenets, and implementation will be discussed. Organizational requirements associated with the zero-trust for information confidentiality, data integrity and availability, authentication, and non-repudiation will also be reviewed including federal guidelines.

PRESENTATION #2

Topic: Rethinking the Security and Privacy of Bluetooth Low Energy

Time: 2:00pm – 2:50 pm EST

Location: https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

Presenter(s): Zhiqiang Lin PhD, The Ohio State University

Description: 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.

In this talk, Dr. Lin will talk about a line of recent research efforts for BLE security and privacy from his 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.

CAE Tech Talks are recorded; view them here:
https://www.caecommunity.org/resources/cae-tech-talk-resources

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov