15 November 2018

FR-WARD: Fast Retransmit as a Wary but Ample Response to Distributed Denial-of-Service Attacks from the Internet of Things (1:10-1:50 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. We are a warm group that shares technical knowledge. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. You can attend from just about anywhere (office, home, etc.) Capitol Technology University (CTU) hosts the presentations using their online delivery platform (Adobe Connect) 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 presentation(s) and logistics of attendance:

Date: Thursday, November 15 2018

Time: 1:10-1:50 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

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

Title/Topic: FR-WARD: Fast Retransmit as a Wary but Ample Response to Distributed Denial-of-Service Attacks from the Internet of Things

Audience Skill Level: All levels

Presenter(s): Samuel Mergendahl – University of Oregon

Description:

While the Internet of Things (IoT) becomes increasingly popular and ubiquitous, IoT devices often remain unprotected and can be exploited to launch large-scale distributed denial-of-service (DDoS) attacks. One could attempt to employ traditional DDoS defense solutions, but these solutions are hardly suitable in IoT environments since they seldom consider the resource constraints of IoT devices.

We present FR-WARD, a system that defends against DDoS attacks launched from an IoT network. FR-

WARD operates close to potential attack sources at the gateway of an IoT network and drops packets to throttle any DDoS traffic that attempts to leave the IoT network. However, in order to properly react to traffic too difficult to categorically label as good or bad, FR-WARD employs a novel response based on the fast retransmit and flow control mechanisms of the Transmission Control Protocol (TCP) which minimizes the energy consumption and network latency of benign IoT devices within the policed network.

AND

Title/Topic: Car Hacking for Ethical Hackers

Time: 2:00 – 2:40 pm ET

Audience Skill Level: All levels

Presenter(s): Dr. Bryson Payne, University of North Georgia

Description:

Internet-connected and self-driving cars are becoming commonplace on our highways, and car hacking has become a timely area of research. This presentation details how to add a module on car hacking into a semester-long ethical hacking cybersecurity course or as a standalone lab, including full installation and setup of all the open-source tools necessary to implement the hands-on labs. Also provided are an introduction to the CAN (controller area network) bus in modern automobiles and a brief history of car hacking.

CAE Tech Talks are also recorded

Recordings are posted to the website: https://capitol.instructure.com/courses/510/external_tools/66

Pdf versions of the presentations are posted to: https://capitol.instructure.com/courses/510/files

Contact

CAE Tech Talk events are advertised thru email and posted to the news and calendar section of the CAE community website: www.caecommunity.org

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