CAE Tech Talk

18 November 2021

Securing Cyber-Physical Systems by Platform Reboot (1:00 – 1:50 pm EST)

Practical adversarial attack against speech recognition Platforms (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: Securing Cyber-Physical Systems by Platform Reboot

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): Monowar Hasan, Wichita State University

Description: In this talk, the presenter will discuss techniques to secure cyber-physical systems (CPS) against cyberattacks, especially those are focused on causing physical damage to the plants. Physical plants that form the core of CPS have stringent safety requirements. The presenter will present their ideas on ensuring the "safety" of the physical plant even when the platform is compromised. In particular, the presenter will present two different approaches to achieve this goal: (a) restart-based mechanism, which utilizes complete system restarts and software reloads, and (b) hypervisor-based design that utilizes Trusted Execution Environment (TEE) such as ARM TrustZone.

PRESENTATION #2

Topic: Practical adversarial attack against speech recognition Platforms

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): Shengzhi Zhang, Boston University

Description: The popularity of ASR (automatic speech recognition) systems, like Google Voice, Cortana, Amazon Echo, brings in security concerns, as demonstrated by recent attacks. The impacts of such threats, however, are less clear, since they are either less stealthy (producing noise-like voice commands), requiring the physical presence of an attack device (using ultrasound), or not practical (unable to attack the physical speech recognition devices). In this talk, the presenter will show that not only are more practical and surreptitious attacks feasible but they can even be automatically constructed. Specifically, the voice commands can be stealthily embedded into songs, which, when played, can effectively control the target system through ASR without being noticed. The presenter will present the novel techniques that address a key technical challenge: integrating the commands into a song in a way that can be effectively recognized by ASR through the air, in the presence of background noise, while not being detected by a human listener. Our research shows that this can be done automatically against real world ASR systems, and even devices like Google Home, Amazon Echo, Apple Siri, etc.

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