



CAE Tech Talk



National Centers of Academic Excellence

17 December 2020

Insecure, unsafe, and lying software (1:00 – 1:50pm EST) and What You See is NOT What You Get: Discovering and Tracking Ad-Driven Social Engineering Attack Campaigns (2 – 2:50pm 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.

Topic: Insecure, unsafe, and lying software

Time: 1:00pm – 1:50pm EST

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

Presenter(s): Eduardo B. Fernandez (Eduardo Fernandez-Buglioni), Florida Atlantic University

Description: Software systems are now an integral part of our life, databases stored by a variety of institutions define who we are, what we own, what is our expertise, our jobs, as well as holding our flight reservations, tickets for concerts, appointments, etc. In other words, they hold a panorama of our past, present, and future life. Most parts of this panorama persist through our whole life, and even beyond. We need therefore to expect that this data is accurate, protected properly, and designed appropriately. The institutions that hold all this data have an enormous influence in our lives and must be trustworthy. However, due to greed or negligence sometimes software systems turn against us. We show three recent examples of software that was intentionally mishandled by three important corporations: an insecure software, the Equifax credit database, which leaked 150 millions of individual records; a lying software used by Volkswagen to deceive emission controls which pollutes our air; and unsafe software to control the Boeing 737MAX, responsible for killing 346 people. We describe details of these cases to see the errors and intentional decisions that produced these outcomes, and discuss how we can avoid these problems to happen.

Topic: What You See is NOT What You Get: Discovering and Tracking Ad-Driven Social Engineering Attack Campaigns

Time: 2:00pm – 2:50pm EST

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

Presenter(s): Phani Vadrevu, University of New Orleans

Description: Malicious ads often use social engineering (SE) tactics to coax users into downloading unwanted software, purchasing fake products or services, or giving up valuable personal information. These ads are often served by low-tier ad networks that may not have the technical means (or simply the will) to patrol the ad content they serve to curtail abuse. In this work, we proposed a system for large-scale automatic discovery and tracking of SE Attack Campaigns delivered via Malicious Advertisements (SEACMA). Our system can provide valuable information that could be used to improve defense systems against social engineering attacks and malicious ads in general.

CAE Tech Talks are recorded; view them here:

<https://www.caecommunity.org/content/cae-tech-talk-resources>

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