CAE Tech Talk

21 April 2022

HE and ZKP: Privacy-Enhancing Technologies (1:00 – 1:50 pm EST)

Symbolic Execution for the Win: Pwning CTFs with Angr (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: HE and ZKP: Privacy-Enhancing Technologies

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):

Charles Gouert and Dimitris Mouris, University of Delaware

Description: As cloud computing and data outsourcing become increasingly prevalent, the need for data privacy is critical. Homomorphic encryption allows for algorithms and analytics to be computed on outsourced encrypted data without leaking any information about the underlying plaintexts, while zero-knowledge proofs allow for data verification without revealing secret data to the other party. In this talk, the presenters will briefly introduce these two technologies and discuss state-of-the-art applications utilizing HE and ZKP. Homomorphic encryption techniques can be used to conduct private machine learning inferences on the cloud without revealing any information about user inputs. For instance, a user could encrypt a picture of a

patch of skin, upload it to a cloud server, and receive an inference result indicating whether or not he has skin cancer without ever exposing the picture itself. In terms of ZKP, a user could prove that she casted her vote correctly without revealing who she voted for. This enables building secure and trustworthy electronic voting.

PRESENTATION #2

Topic: Symbolic Execution for the Win: Pwning CTFs with Angr

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): Dr. Bryson Payne, University of North Georgia

Description: Cyber competitions and capture-the-flag (CTF) events are a valuable tool for motivating and engaging students and professionals in cybersecurity and cyber operations beyond traditional education and training. Reverse engineering and binary exploitation challenges are common components of online CTFs, but the tools, techniques and procedures for performing reverse engineering and binary exploitation have a steep learning curve and are not taught in many computer science, IT, and cybersecurity degree programs.

Angr is a Python framework for analyzing binaries across a number of platforms and architectures, originally developed as part of a DARPA Cyber Grand Challenge. It combines both static and dynamic, concrete and symbolic (or "concolic") analysis to enable users to easily analyze how different inputs change the path of a program's execution. For CTF exercises, angr allows competitors to quickly determine the correct input(s) that would satisfy a program's constraints leading to a successful solution, thereby capturing the flag. This introductory presentation will demonstrate how angr can be used to solve CTF challenges (or find real-world vulnerabilities) in a fraction of the time required by debuggers, disassemblers, and decompilers alone.

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