18 February 2021

A Machine Learning Approach for Detecting Cheats of Computer Game (1:00 – 1:50 pm EST)

Securing software supply chains with in-toto (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:

Topic: A Machine Learning Approach for Detecting Cheats of Computer Game

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): Dr. Latifur Khan, University of Texas at Dallas

Description: Cheating in massive multiple online games (MMOGs) adversely affect the game's popularity and reputation among its users. Therefore, game developers invest large amount of efforts to detect and prevent cheats that provide an unfair advantage to cheaters over other naive users during game play. Particularly, MMOG clients share data with the server during game play. Game developers leverage this data to detect cheating. However, detecting cheats is challenging mainly due to the limited client-side information, along with unknown and complex cheating techniques. In this presentation, we aim to leverage machine learning-based models to predict cheats over encrypted game traffic during game play. Concretely, network game traffic during game play from each player can be used to determine whether a cheat is employed. A major challenge in developing such a prediction model is the

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

availability of 12 sufficient training data, which is sparingly available in practice. Game traffic obtained from a few known players can be easily labeled. However, if such players are not a good representation of the population (i.e., other players), then a supervised model trained on labeled game traffic from these set of players may not generalize well for the population. Here, we propose a Graphics Processing Unit (GPU) based scalable transfer learning approach to overcome the constraints of limited labeled data. Our empirical evaluation on a popular MMOG demonstrates significant improvement in cheat prediction compared to other competing methods.

Topic: Securing software supply chains with in-toto

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): Reza Curtmola, New Jersey Institute of Technology

Description: The security of software supply chains is a topic that has been largely overlooked over the past few years, despite numerous recent incidents which show that attacks can happen at any point in this chain, including the most recent one involving SolarWinds. We have developed in-toto, a novel framework that provides insights about processes that occurred in the various steps of the software supply chain. in-toto is the first security mechanism that protects software from the point when the developer commits the code until the end user installs it. in-toto has been deployed into several real-world open source and commercial systems.

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