CAE Forum

Wednesday, November 2, 2022

The use of Steganography and Steganalysis Trends in Computer Forensics (1:00 - 1:50 pm EST)

Vulnerabilities of Machine Learning Algorithms to Adversarial Attacks for Cyber-Physical Power Systems (2:00 – 2:50 pm EST)

Mark your calendar and come join us for CAE Forum! CAE Forum is a live, real-time, online, academic forum where members of the CAE community give non-technical presentations on topics of value to the CAE community. CAE Forum is about sharing your ideas, knowledge, and expertise to empower and strengthen our community. It's that simple. CAE Forum presentations are normally held on the first Wednesday of each month during the Fall and Spring semesters.

PRESENTATION #1

Title/Topic: The use of Steganography and Steganalysis Trends in Computer Forensics

Time: 1:00 - 1:50 pm EST

Location: https://caecommunity.zoom.us/j/83488759886

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

Audience: Students, Professors, Govt.

Presenter(s): Dinesh Reddy, Our Lady of the Lake University

Description: Steganography is the art and science of writing hidden messages. The goal is to hide information in files so that even if the files with hidden information are intercepted, it is not clear that information is hidden in those files. Steganalysis is the process of analyzing a file or files for hidden content. Steganalysis can show the likelihood that a given file has additional information hidden in it, by using tools such as S-Tools and Invisible Secrets. A forensic examiner must be very familiar with techniques and trends in steganography and steganalysis. This means a forensic examiner should be able to do steganography and steganalysis by knowing multiple techniques and best practices for hiding/scrambling and recovering information.

PRESENTATION #2

Title/Topic: Vulnerabilities of Machine Learning Algorithms to Adversarial Attacks for Cyber-Physical Power Systems

Time: 2:00 - 2:50 pm EST

Location: https://caecommunity.zoom.us/j/83488759886

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

Audience: Students, Professors, Govt.

Presenter(s): Tapadhir Das, University of Nevada, Reno

Description: Artificial intelligence (AI) techniques have been widely employed to monitor, control, and manage Cyber-Physical Power Systems (CPPS). AI algorithms provide several advantages over analytical algorithms including modeling flexibility and applicability to real-time control and operation. However, AI algorithms, especially those dependent on machine learning (ML), could be exposed to multiple attack vectors through unsecured and unencrypted communications. Recent attacks have shown several vulnerabilities of ML algorithms to adversarial attacks. Attacks can include fabricated samples, poisoned data, and changes in model architecture to make deliberate errors. Therefore, it has become crucial to ensure the security, reliability, and robustness of deployed ML algorithms against adversarial attacks. This chapter discusses the vulnerabilities of ML algorithms to adversarial attacks, possible attack vectors, real-work examples of adversarial attacks on ML algorithms, numerical examples, and discussions to enhance ML algorithms against adversarial attacks in CPPS.

A recording of the live presentation will be available following the pre of the presentation at: https://www.caecommunity.org/resources/cae-forum-resources

Contact us at: caeforum@caecommunity.org