



20 October 2022

Security Patch Identification on Open-Source Software (1:00 – 1:50 pm EST)

A Metrics-Driven Approach to Prioritizing Vulnerability Mitigation (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: Security Patch Identification on Open-Source Software

Time: 1:00pm – 1:50 pm EST

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

Join as Guest and enter a name. No password required.

Presenter(s): Dr. Kun Sun, George Mason University

Description: With the increasing popularity of open-source software, embedded vulnerabilities have been widely propagating to downstream software. For the sake of reputation or underestimation, software vendors are prone to silently release security patches without publishing any advisories (e.g., CVE). This trend leaves users unaware of security patches and provides attackers good chances to exploit unpatched vulnerabilities. Therefore, detecting those secret security patches becomes imperative for secure software maintenance. Here we report two of our works on addressing this problem. First, security patches, embedding both vulnerable code and the corresponding fixes, are of great significance to vulnerability detection and software maintenance; however, the existing open-sourced patch datasets suffer from insufficient samples and low varieties. We construct and open source a large-scale patch

