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

Just log in as "Guest" and enter your 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

dataset called PatchDB (https://sunlab-gmu.github.io/PatchDB/) that consists of 12K security patches and 23K non-security patches in C/C++. Among the 12K security patches, 4K are from the NVD-based dataset and 8K are from the wild-based dataset. Second, we propose a graph neural network based security patch detection system that represents patches as graphs with richer semantics and utilizes a patch-tailored graph model for detection. Experimental results show our system can significantly outperform the state-of-the-art approaches on security patch detection.

PRESENTATION #2

Topic: A Metrics-Driven Approach to Prioritizing Vulnerability Mitigation

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): Massimiliano Albanese, George Mason University

Description: One of the first lines of defense against cyberattacks is to understand, evaluate, and mitigate the weaknesses and vulnerabilities that a system exposes to malicious users. To address this need, several metrics and scoring systems have been developed, providing security analysts and practitioners with a means of quantifying the severity of common weaknesses and vulnerabilities found in software. However, these scoring systems rely on predefined notions of risk, use fixed equations to compute numerical scores, and do not provide users with the flexibility to fine-tune such equations or consider new variables. In many cases, numerical scores are too coarse-grained to provide meaningful rankings of thousands of known vulnerabilities. Furthermore, these scores and rankings are updated infrequently, making them less valuable in a rapidly evolving cybersecurity landscape. In this talk, I will present a generic approach to designing customizable and tunable vulnerability metrics, which gives system administrators significant control over the scoring and ranking process. I will also present a web-based system, the Mason Vulnerability Scoring Framework (MVSF), which we designed to make these capabilities available to the broader research community.

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