TEMPLE
UNIVERSITY®

\

Spring 2023 Colloquium

Department of Computer and Information Sciences

AI-Enhanced Software Vulnerability and Security Patch Analysis

Xinda Wang

Department of Computer and Information Science
George Mason University

Tuesday, February 14, 2 PM
Room: SERC 306

Abstract: With the increasing popularity of open-source software (OSS), their embedded vulnerabilities have been widely propagating to downstream software. Although timely applying security patches is the best practice to prevent vulnerabilities, OSS users are hard to distinguish and prioritize security patches over tons of non-security patches (i.e., bug fixes, feature updates, etc.) Even worse, software vendors may silently release security patches without providing any explicit advisories. While users are unaware of security patches, attackers can still carefully inspect the patch code changes to exploit unpatched software. Therefore, automatically detecting security patches becomes imperative for software maintenance.

In this talk, I will describe my research efforts to address the above problems. First, I will introduce an empirical study that reveals the insecure behavior of software vendors during maintenance and discloses the existence of silent (hidden) security patches. Second, I will present PatchDB, the first large-scale real-world patch dataset, that enables the training of data-hungry AI models for patch detection and facilitates future vulnerability/patch analysis research. An unsupervised method is developed to efficiently collect security patch samples from a huge number of unlabeled Git commits. Third, I will present GraphSPD, a novel graph learning-based approach for automated security patch detection. By combining rich semantic properties of both pre-patch code and post-patch code in a joint graph structure and adopting a tailored multi-attributed graph convolution network to adapt diverse attributes in a patch graph representation, GraphSPD demonstrates state-of-the-art performance and detects 88 new silent security patches in popular real-world Git projects. Finally, I will conclude by highlighting my research plan towards maximizing AI capabilities in automating the process of software vulnerability and patch management.

Bio: Xinda (Cindy) Wang is a Ph.D. candidate in the Center for Secure Information Systems at George Mason University. She received her B.E. degree in Computer Science from the Harbin Institute of Technology in 2017. Her research interests are AI-enhanced cybersecurity, including software security, container security, and network anomaly detection. As the leading author, she has published papers in flagship security venues such as IEEE S&P, DSN, and CNS. She is the recipient of the IEEE CNS Best Paper Nomination (2020), Tapia Scholarship (2018, 2022), GHC Scholarship(2022), and IMC Suneeth Nayak Scholarship (2020).