NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Haipeng Cai
Washington State University

Sustainable Defenses against Evolving Malware in the Android Ecosystem: A Manifesto

Dec. 12, 2022, 3:10 – 4PM PDT

Team Link: Click here to join the meeting
Meeting ID: 287 304 495 40 | Passcode: wdM7Vw
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 834 528 822#

Abstract:

Learning-based classification dominates malware detectors for Android. However, due to the evolution of the Android ecosystem, existing such techniques are limited by their reliance on new malware samples, which may not be timely available, and constant retraining, which are often costly. A practical detector needs not only to be accurate on particular datasets but, more critically, to be able to sustain its capabilities over time without frequent retraining. In this talk, we will first take a quick look into the dynamics of evolving Android apps in terms of its run-time behaviors throughout a decade history of Android, followed by an overview of the challenges that arose due to the evolution as well as some of the strategies for embracing it. Next, we will dive into one specific study that measures the sustainability of four state-of-the-art learning-based malware detectors across the span of many years, and one recent technique that aims to bring better sustainability to learning-based malware detection. We will end by reflecting on what we have learned in this series of research projects and remaining challenges ahead, as well as envisioning potentially even more sustainable defenses in the future.

Bio:

Haipeng Cai is an Associate Professor in the School of Electrical Engineering and Computer Science (EECS) at Washington State University, Pullman. His research generally lies in software systems and security, with a current focus on program analysis assisted by machine/deep learning methods for security applications to multilingual software, distributed systems, and mobile apps. The main goal of his research is to develop practically scalable and cost-effective techniques and tools that improve the productivity of software developers and the quality of large-scale, complex real-world software systems.