VICEROY NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

Matt Revelle
School of Computing, MSU

Interprocedural Binary Analysis

Apr. 1, 2024, 3:10 – 4PM Pacific

Team Link: Click here to join the meeting
Meeting ID: 268 793 483 658| Passcode: zmEnUH
Call in (audio only) +1 509-498-6399 | Phone Conference ID: 391 220 845#

Abstract:

As software systems continue to become more prolific, the frequency and potential impact of unknown software vulnerabilities also increases. The reverse engineering of program binaries is necessary for identifying and understanding software vulnerabilities when source code is unavailable. Improving the performance of reverse engineers is a crucial component in securing computer systems. Semi-automated analysis workflows which allow reverse engineers to direct automated analyses can improve efficiency and enable the use of analyses that are intractable when applied to a whole program. We will explore how interprocedural binary analysis supports interactive construction of interprocedural control-flow graphs (ICFGs), program exploration, automated simplifications through context- and flow-sensitive analysis, and type inference.

Bio:

Dr. Revelle is an assistant professor of computer science at Montana State University (MSU). He joined MSU in the fall of 2023 and previously served as a Senior Principal Research Scientist at Kudu Dynamics in Boulder, CO. He has over 21 years of computer science experience, including 13 years of computer security experience in vulnerability research, reverse engineering, program analysis, and computer network operations (CNO) software development. He holds a Ph.D. in Computer Science from George Mason University where he focused on machine learning for graph data. He has served as PI on several Defense Advanced Research Projects Agency (DARPA) programs where he led teams developing automated analysis techniques for discovering and reasoning over software vulnerabilities. At Montana State University, he has started the Harnessing Automation in Cybersecurity Reasoning (HACR) Lab where he supports undergraduate and graduate student research and mentors the learn2ctf CTF team. His current research includes the development of novel program analysis and machine learning techniques for cybersecurity tasks such as vulnerability discovery and exploit development.

cyser.wsu.edu

Washington State University · Montana State University · CWU · University of Idaho