NJIT

Department of Computer Science

Binary Code Hardening and Vulnerability Detection via Value Set Analysis

Sanchuan Chen
Ohio State University

Hosted by Yiannis Koutis

DATE: Wednesday, May 12, 2021
TIME: 1:00 PM - 2:00 PM
LOCATION: https://njit.webex.com/njit/j.php?MTID=m1813556957c6a411abb8af155d0c3fc6

https://cs.njit.edu/seminars

Abstract: Software is complex today and it often contains security vulnerabilities. Being able to harden the software in the presence of vulnerabilities or identify the vulnerabilities before attackers is extremely important. In this talk, I will present a line of my research of how to leverage value set analysis to (1) rewrite the binary code such that the runtime execution is resilient to vulnerability exploitation through taint tracking, and (2) detect the data-race vulnerabilities proactively in the binary code.

In particular, in the first part of my talk, I will present SelectiveTaint, an open source taint analysis framework that only rewrites the binary code of interest by statically identifying the instructions that will never involve taint through value set analysis, thereby significantly improving the performance overhead of taint analysis (1.7x faster when compared to state-of-the-art tools). In the second part of my talk, I will present SGX-Racer, another open source tool particularly for data-race vulnerability discovery in SGX binaries. Through the novel use of value set analysis, I develop a set of enabling techniques including a new lockset-based data race detection algorithm, to systematically explore the possible concurrent executions. Experimental results show that SGX-Racer is able to identify a number of data race vulnerabilities (e.g., CVE-2020-5499) in real world SGX binaries.

Bio: Sanchuan Chen is a Ph.D. candidate at The Ohio State University. His research focuses on using program analysis (particularly binary analysis) to solve emerging and important security problems in both software and hardware. He received his M.E. from Chinese Academy of Sciences, and B.E. from University of Science and Technology of China, all in computer science.