NJIT

Department of Computer Science

Dig Deeper—Mining Object Related Vulnerabilities via Static Analysis

Song Li
Johns Hopkins University

Hosted by Iulian Neamtiu

Date: Monday, February 7, 2022
Coffee: 2:15 PM – 2:30 PM
Seminar: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th Floor Seminar Lecture Hall)
WebEx https://njit.webex.com/njit/j.php?MTID=mc215eaeee0722344c47576e4683c2c84

https://cs.njit.edu/seminars

Abstract:

As a flexible programming language, JavaScript is widely used at both the front end (browser-based programs or mobile applications) and the back end. At the same time, its flexible features, like the prototype chain, introduce multiple vulnerabilities. For example, prototype pollution allows attackers to pollute the built-in methods of objects which will lead to severe consequences like Denial-of-Service (DoS) or session fixation. Such vulnerabilities are hard to detect but can significantly influence the security of the systems.

In this work, I design and develop an open-sourced JavaScript vulnerability detection platform—— ODGen, which can detect multiple vulnerabilities, for instance, OS command injection, Cross-site scripting (XSS), prototype pollution, and path traversal. In this talk, I will talk about 1), how I use static analysis to build Object Dependence Graph (ODG) to detect prototype pollution accurately. 2), how do I extend the generated ODG to detect other types of vulnerabilities. 3), how do I plan to solve the long-standing static analysis efficiency problem in the vulnerability detection domain.

Bio:

Song Li is a Ph.D. candidate at Johns Hopkins University majoring in Computer Science, advised by Dr. Yinzhi Cao. His research interests are primarily focused on security areas such as web security, system security, and program analysis. He uses to work on web tracking and now focuses on static/dynamic analysis -- trying to solve real-world challenging problems like increasing the accuracy and efficiency of vulnerability detection.