NJIT

Department of Computer Science

Attack surface reduction through system call filtering

Seyedhamed Ghavamnia
Stony Brook University

Hosted by Jing Li

Date: Monday, January 23, 2023
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=m9742141661ca5109fbedccabadefdda8

http://cs.njit.edu/seminars

Abstract:
Attack surface reduction through removing unnecessary application features and code, referred to as debloating, is a promising technique for improving security without incurring any additional overhead. Applying this technique to the operating system kernel can reduce the risk of privilege escalation attacks. Since userspace programs mainly leverage system calls to interact with the kernel, restricting access to any system call can potentially prevent an attacker from exploiting a vulnerability in the kernel. The main challenge in this area of work is to perform a sound analysis that does not mistakenly identify parts of the code that the program requires as supplementary. In this talk, I will show how we can use static analysis to identify the system call requirements of a userspace program and neutralize previously disclosed Linux kernel vulnerabilities by filtering those deemed unnecessary. Furthermore, I will discuss the potential of deprivileging programs by analyzing their system call requirements.

Bio:
Seyedhamed Ghavamnia is a sixth-year Ph.D. candidate in Computer Science at Stony Brook University, advised by Michalis Polychronakis. His research interests lie at the intersection of software security and programming languages. During his Ph.D., Seyedhamed has primarily focused on performing attack surface reduction through software debloating. The main challenge in this area of work is to perform a sound analysis that can maximize code and feature removal without breaking the program. He has published research papers in top security conferences, including IEEE Security and Privacy (S&P), Usenix Security Symposium, ACM CCS, and other prestigious conferences, such as RAID.
.