Department of Computer Science

HOLMES: Holistic and Hardware-assisted Control-Flow Security for Microcontroller Systems

Ziming Zhao
SUNY Buffalo

Hosted by Reza Curtmola

Date: Wednesday, December 13, 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=m2b6b86b9f40d828d2ee3f612f7f486e1

http://cs.njit.edu/seminars

Abstract:
Microcontroller (MCU) systems are essential to everyday life and are predicted to reach 1 trillion by 2035. While the benefits of these systems are unparalleled, they are susceptible to cyberattacks, which are occurring at unprecedented levels and often have severe consequences ranging from loss of life to homeland security breaches. Among the attacks targeting MCU systems, control-flow hijacking remains the most dangerous as it can result in arbitrary code execution. It is, however, difficult to secure the control-flow on these systems due to software issues and hardware constraints. On the software front, these systems are usually written in low-level languages, e.g., C, whose lack of safety allows attackers to exploit memory corruption bugs to hijack the control flow. On the hardware front, MCU systems do not have some of the hardware units we take for granted on microprocessor architectures. For example, the Arm Cortex-M MCUs do not have a Memory Management Unit (MMU), without which applications share the same physical address space, making it difficult to enforce isolation or to implement control-flow hijacking mitigation.

In this talk, I will discuss three of our recent works related to control-flow security on MCU systems. The first work, titled "MICROFT: Exploring and Mitigating Cross-state Control-Flow Hijacking Attacks," was partially presented at ACM/IEEE Design Automation Conference (DAC'23). I will discuss a new class of attacks we discovered, namely, return-to-non-secure attacks, on ARM Cortex-M TrustZone, and their mitigation strategies. The second work, titled "SHERLOC: Secure and Holistic Control-Flow Violation Detection on Embedded Systems," was presented at the ACM Conference on Computer and Communications Security (CCS'23). This work introduces a novel mechanism for monitoring control-flow violations in both unprivileged and privileged programs, as well as control-flow transfers between these components. Lastly, in the third work, "ENOLA: Efficient Control-Flow Attestation for Embedded Systems", I discuss our ongoing efforts to enhance existing control-flow attestations by proposing a solution with linear space complexity for measurement and trace data concerning the number of basic blocks, addressing scalability concerns for larger MCU programs.

Bio:
Ziming Zhao is an Assistant Professor at the Department of Computer Science and Engineering (CSE) and the director of the CyberspACe securiTy and forensIcs lab (CactiLab, https://cactilab.github.io/), University at Buffalo. His current research interests include systems and software security, trusted execution environments, formal methods for security, and usable security. He is a recipient of a National Science Foundation (NSF) CAREER award and an NSF CRII award. His research has been supported by the U.S. National Science Foundation, the U.S. Department of Defense, the U.S. Air Force Office of Scientific Research, and the U.S. National Centers of Academic Excellence in Cybersecurity (part of the National Security Agency). His research outcomes have appeared in IEEE Security and Privacy, USENIX Security, ACM CCS, NDSS, ACM MobiSys, ACM/IEEE DAC, ACM IMWUT, ACM TISSEC/TOPS, IEEE TDSC, IEEE TIFS, and more. His contributions have been recognized with best/distinguished paper awards from USENIX Security 2019, ACM AsiaCCS 2022, ACM CODASPY 2014, and ITU Kaleidoscope 2016. He earned his bachelor's and master's degrees from Beijing University of Posts and Telecommunications. He obtained his Ph.D. degree in Computer Science from Arizona State University. CactiLab shares their projects as open source on https://github.com/Cactilab.