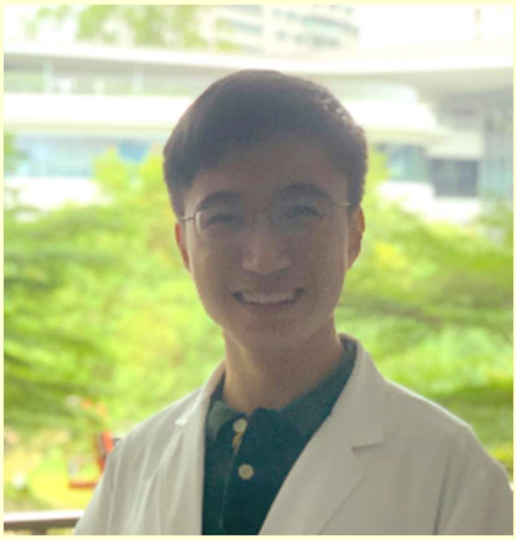
CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar



"Capstone: A Capability-based Foundation for Trustless Secure Memory Access"

Jason Zhijingcheng Yu

Fourth-year PhD student at the School of Computing,
National University of Singapore (NUS)

Monday, August 7th
11:00-12:00 PM
Location: Engineering Hall 2430

Abstract: Capability-based memory isolation is a promising new architectural primitive. Software can access low-level memory only via capability handles rather than raw pointers, which provides a natural interface to enforce security restrictions. Existing architectural capability designs such as CHERI provide spatial safety but fail to extend to other memory models that security-sensitive software designs may desire. In this paper, we propose Capstone, a more expressive architectural capability design that supports multiple existing memory isolation models in a *trustless* setup, i.e., without relying on trusted software components. We show how Capstone is well-suited for environments where privilege boundaries are fluid (dynamically extensible), memory sharing/delegation are desired both temporally and spatially, and where such needs are to be balanced with availability concerns. Capstone can also be implemented efficiently. We present an implementation sketch and through evaluation show that its overhead is below 50% in common use cases. We also prototype a functional emulator for Capstone and use it to demonstrate the *runnable implementations* of six real-world memory models without trusted software components: three types of enclave-based TEEs, a thread scheduler, a memory allocator, and Rust-style memory safety—all within the interface of Capstone.

Biography Jason Zhijingcheng Yu is a 4th-year PhD student working with Prof Prateek Saxena at School of Computing, National University of Singapore (NUS). He works on operating system and architectural security, with a focus on trusted computing and capability-based security in architectures. His first-authored work has been published at venues including ACM CCS 2021, USENIX Security 2022, and USENIX Security 2023. Homepage: https://www.comp.nus.edu.sg/~yuz1996/

Hosted By: Zhou Li