

Title

Tock: A Safe and Secure Operating System for Root-of-Trust Hardware

Abstract

Root-of-trust hardware still needs software, and that software must be robust. Tock is an operating system for microcontrollers in domains where security and robustness are critical. The Tock kernel is written in Rust and enforces strict isolation between applications which execute as userspace processes. The architecture of the OS is designed to minimize the amount of trusted code and enable compile-time checks to prevent runtime failures. This talk will introduce Tock, the key design decisions behind the OS, and how Tock can be used in root-of-trust applications. I will also share highlights on the ongoing research within Tock, what's next for the project, and how you can use Tock for your application.

Bio

Brad Campbell is an Associate Professor in the Computer Science and Electrical and Computer Engineering departments at the University of Virginia. He is a member of the Link Lab at UVA, a cross-disciplinary research lab focused on cyber-physical systems. He received his Ph.D. in Computer Science from the University of Michigan in 2017, and his B.S. in Computer Engineering also from the University of Michigan. His research concentrates on designing low-power, self-powered, and resilient wireless smart devices and networks that are fault tolerant, privacy-preserving, and scalable, with applications in smart buildings and smart cities. His work has led to numerous open-source hardware and software platforms, and his work on self-powered energy meters is currently being commercialized. Brad received an NSF CAREER award in 2022, and a best paper award at DFHS'19. Brad has served on the organizing and technical program committees of numerous conferences, including MobiCom, SenSys, IPSN, BuildSys, and MobiSys.