From CPUs to Peripherals: The Next Frontier of Confidential Computing

Shweta Shinde
ETH Zurich

Abstract:

Trusted execution environments in several existing and upcoming CPUs demonstrate the success of confidential computing. However, these advances come with the caveat that they leave out peripherals both on mobile (e.g., camera, display) and server (e.g., GPUs, FPGAs) platforms. On the accelerator side, stand-alone support for device-side TEEs (e.g., Nvidia confidential computation) is necessary but not sufficient. This, while desirable, extending the notion of confidential computing from CPUs to peripherals is not straightforward.

In this talk, I will highlight the basic building blocks such as hardware changes, performance impact, and compatibility, necessary to address this broad goal. Then I will dive into one concrete instance of this challenge. As a case in point, I will consider the Arm Confidential Computing Architecture (CCA) design--an upcoming TEE feature in Armv9. I will use this to highlight the need to address the gap between CPUs and accelerators on server platforms. On the upside, we observe that CCA offers the right abstraction. The challenge is in using these mechanisms securely to allow confidential VMs to use accelerators as a first-class abstraction. Further, it is crucial to rely on hardware-based memory protection to preserve performance with strong security guarantees. We use a principled approach of extending CCA security invariants to device-side access while addressing several critical security gaps. Our solution, Acai [1], achieves these goals without changes to hardware or software on the CPU and the accelerator as well as achieves strong security guarantees with small performance overheads.

Bio:

Shweta Shinde is an assistant professor at ETH Zurich, where she leads the Secure and Trustworthy Systems Group. Her research is broadly at the intersection of trusted computing, system security, program analysis, and formal verification.

[1] ACAI: Protecting Accelerator Execution with Arm Confidential Computing Architecture
Supraja Sridhara, Andrin Bertschi, Benedict Schlüter, Mark Kuhne, Fabio Aliberti, Shweta Shinde
To appear at USENIX Security Symposium (USENIX Security 2024)