In Hardware We Trust? From TPMs to Enclave Computing on RISC-V

The large attack surface of commodity operating systems has motivated academia and industry to develop novel security architectures that provide strong hardware-assisted protection for sensitive applications using the so-called enclaves. However, deployed enclave architectures often lack important security features, and assume threat models which do not cover cross-layer attacks, such as microarchitectural exploits and beyond. Thus, recent academic research has proposed a new line of enclave architectures with distinct features and more comprehensive threat models, many of which were developed on the open RISC-V architecture.

In this talk, we present a brief overview of the Trusted Computing Landscape, its promises and pitfalls. We discuss selected RISC-V based enclave architectures recently proposed, discuss their features, limitations and open challenges which we aim to tackle in our current research using our security architecture CURE. Finally, we shortly report on the insights we gained on cross-layers attacks in the world’s largest hardware security competitions franchise that we have been organizing with Intel and Texas AMU since 2018.