ABSTRACT

User interfaces (UI) are essential parts of modern complex computing platforms as it dictates how humans provide inputs to these systems and interpret output from them. Many remote safety and security-critical cyber-physical systems such as industrial PLCs (in manufacturing, power plants, etc.), medical implants are accessible through rich UIs over browsers or dedicated applications that are running on commodity systems or hosts. Similarly, e-banking, e-voting, social networks, and many other remote applications and services are critically dependent on UIs for user authentication and IO. An attacker-controlled host can not only observe user's IO data but also can modify them undetected. Loss of integrity and confidentiality of user inputs can lead to catastrophic failure of critical infrastructures, loss of human lives, leakage of sensitive data. The problem of secure communication between a user and an end-system is known as *trusted path*. Such attacks are not far-fetched as modern software and hardware systems are incredibly complex and span over millions of lines of code. Hence the users are bound to trust a massive trusted computing base or TCB. Exploiting software vulnerabilities of the OS, hypervisors, database systems are very prevalent. Recent technologies such as Trusted execution environments (TEEs) address this problem by reducing the TCB by running isolated environments on the CPU cores, known as enclaves, that are isolated from the OS or hypervisor. However, TEEs do not solve the trusted path problem as TEEs depend on the OS to communicate to the external IO devices. Moreover, the remote attestation mechanism by which a verifier can ensure that she is communicating with the proper enclave is vulnerable to relay attack. In the context of disaggregated computing architecture in modern data centers, the security properties of traditional TEE are insufficient as the trusted path application involves sensitive data not only on the CPU cores but also on the specialized external hardware like accelerators.

In this thesis, we propose mechanisms to build trust in modern computing platforms by addressing the trusted path problem, and we make the following contributions. First, we analyze existing trusted path systems and found several attacks that compromise user IO data integrity and confidentiality. We are the first to analyze the trusted path problem to find a set of essential security properties and implement them in a system named ProtectIOn using a trusted embedded device as an intermediary. This trusted device intercepts all IO data and overlays secure UI on the display signal. Next, we look into Intel SGX and investigate how one can integrate a trusted path solution to TEEs. We notice that the relay attack on the SGX remote attestation can be detrimental to the trusted path security properties. We design ProximiTEE, a system that uses distance bounding to verify physical proximity to an SGX processor. We also show how the distance bounding mechanism can be used in a high frequency to allocate or revoke platforms in data centers without relying on an online PKI. Finally, we look into the disaggregated computing model of the modern data centers where the TEEs are insufficient as the computation is no longer limited to the CPU cores but several external devices such as GPUs, accelerators, etc. We propose our system PIE based on RISC-V architecture that combines the enclaves running on the CPU and firmware external hardware to a single attestable domain that we call platform-wide enclaves. Inside these platform-wide enclaves, individual binaries (enclaves and firmware) can be remotely attested.