POLITECNICO DI TORINO
PhD Program in Computer and Control Engineering

Zero-Trust Security of Network Nodes

Supervisor: Prof. Antonio Lioy

Candidate: Silvia Sisinni

Abstract

The research work presented in this thesis took place around the exploration of the founding principles of Zero-Trust Security, focusing on secure device identification, root of trust establishment, and continuous integrity verification mechanisms. Motivated by the need to reliably identify and continuously monitor computational entities in modern ICT infrastructures, this research advances the state-of-the-art in remote attestation and trusted communication protocols across various technological domains.

A key contribution of this thesis is the introduction of novel methodologies for attesting lightweight virtual entities, particularly OCI containers and Kubernetes pods. Starting from these remote attestation methodologies, a new cloud service model, Remote Attestation of Lightweight Virtual Entities as a Service (RALVEaS), is proposed, in order to provide cloud tenants with enhanced security assurances in dynamic cloud environments. In parallel, the research work addressed the problem of securing Precision Time Protocol (PTP)-based Time Distribution Networks, introducing attestation methods capable of detecting configuration compromises in nodes critical to precise timing distribution.

Furthermore, the thesis addresses critical security challenges in IoT and embedded devices by designing and evaluating advanced hardware-based security features specifically tailored for resource-constrained IoT environments. Key contributions include implementing secure boot procedures, establishing secure device identities via the DICE specification, and embedding the DICE Layering Architecture into Keystone Security Monitor firmware for privacy-preserving enclave attestation. Additionally, the research introduces runtime integrity monitoring mechanisms for both Trusted Execution Environments (TEE) and Rich Execution Environments (REE), incorporating Data Execution Prevention and a firmware TPM. Empirical validation within the SPIRS project confirmed the practical effectiveness and robustness of these security enhancements.

Lastly, this work defines Trusted Communication Channels wherein endpoint identity and integrity are implicitly attested through the use of cryptographic identities bound to the device identity and software integrity measurements. These trusted communication channels have been integrated and validated within Industry 4.0 and 5G network scenarios, effectively enabling Zero-Trust Architectures for these critical infrastructures. Collectively, the outcomes of this thesis represent an advancement towards effective Zero-Trust infrastructures across cloud, IoT, industrial, and telecommunications domains.