Sudharsun Lakshmi Narasimhan (Aalto, Ericsson), Jukka Ylitalo (Ericsson), Lachlan J. Gunn (Aalto)

Remote Attestation of User Space Applications at Runtime

- Modern attacks target user-space processes at run-time, bypassing launch-time checks.
- Existing attestation techniques focus on boot or access time, not ongoing behavior.
- **Goal:** Enable remote parties to continuously verify interaction with anomaly-assessed process.

Trust Model

- The Kernel is trusted and enforces process isolation.
- The user space Temporal CNN inference process is trusted, kernel-launched, binary-verified, and strictly isolated (no IPC / network connection).
- All other user-space processes are untrusted.

System Overview

- eBPF enables efficient system call tracing in the kernel; events are relayed to the Temporal Convolutional Neural Network (TCNN) via the Loadable Kernel Module (LKM).
- TCNN detects syscall anomalies and is trained on the ADFA-LD dataset (Accuracy 96%).
- LKM attests each session to the ML verdict by signing data with a kernel-protected post-quantum key and transmitting it to the verifier.
- Trusted Platform Module anchors kernel public key, boot state, and ML binary for remote attestation; verifier checks signed data and notifies the relaying party of process secure state.

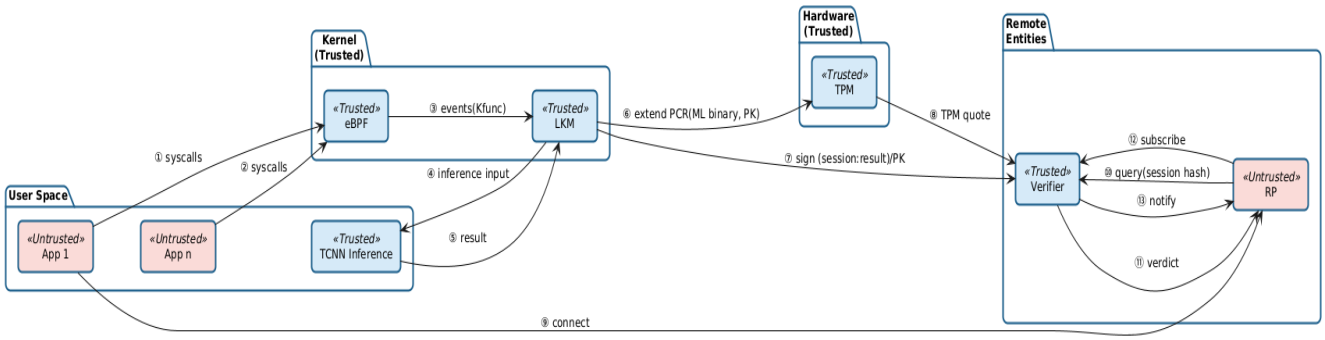

Figure 1: Runtime Attestation

Ongoing Work:

- Kernel-enforced process-to-session attestation context for remote verification.
- Investigating Intel SGX integration to protect against stronger adversaries that compromise user-space memory isolation.

Future Work:

- Enhance detection with syscall arguments and fine-grained runtime context.
- Per-process context tracking in neural inference; evaluation on diverse datasets and attack types.

Aalto University

ERICSSON