1 Work-in-Progress: Enabling Secure Boot for Real-Time Restart-Based Cyber-Physical Systems

A secure boot mechanism is presented which restores real-time embedded systems into a secure computing environment after every restart.

1.1 Introduction

The Simplex architecture is used in lots of Real-Time Embedded Systems to control Cyber-Physical Systems. This architecture consists of a complex partition and a safety one. The complex partition integrates systems timers and monitors to detect faults and trigger resets. The safety partition is controlled by a fully verified controller which is state dependent and makes sure no unsafe states are reached. This by itself does not protect against malicious code or OS to be loaded on the device so secure boot is used to make sure the devices start at a secure state.

1.2 System and Adversary Models

The system is restarted to be reset into a safe environment if the monitoring unit detects an attack, if the timer for the periodic restart expired or if a watchdog timer detects failure of a critical component. The system is considered to be composed of n periodic tasks and one sporadic restart task.

The safety unit and root of trust are assumed to be out of reach of any attacker. The attacker is assumed to have no physical access to the device, all attacks need to be launched remotely using software.

1.3 Proposed Design

Secure boot using TPM. Secure boot restarts add overhead and thus need to be taken into account when checking whether scheduling will still guarantee all tasks to be executed before deadline.

1.4 Discussion

1.5 Related Work

1.6 Conclusion and Future Work