TRUSTED® COMPUTING GROUP

Overview of TCG Technologies for Device Identification and Attestation

Guy Fedorkow

Juniper Networks

Feb 29, 2024

Problem Statement

- How do you know what software is actually running on a box?
- You could ask it, but it might not tell the truth
- Attestation (aka ‘measured boot’) establishes a chain of trust where each link measures the next link before it starts, and reports the results
- But the chain must start at a known-secure point – called a Root of Trust.

This ppt describes the three Root of Trust mechanisms specified by TCG as part of an ecosystem for Attestation

TRUSTED COMPUTING GROUP

What's a Root of Trust

- Definition

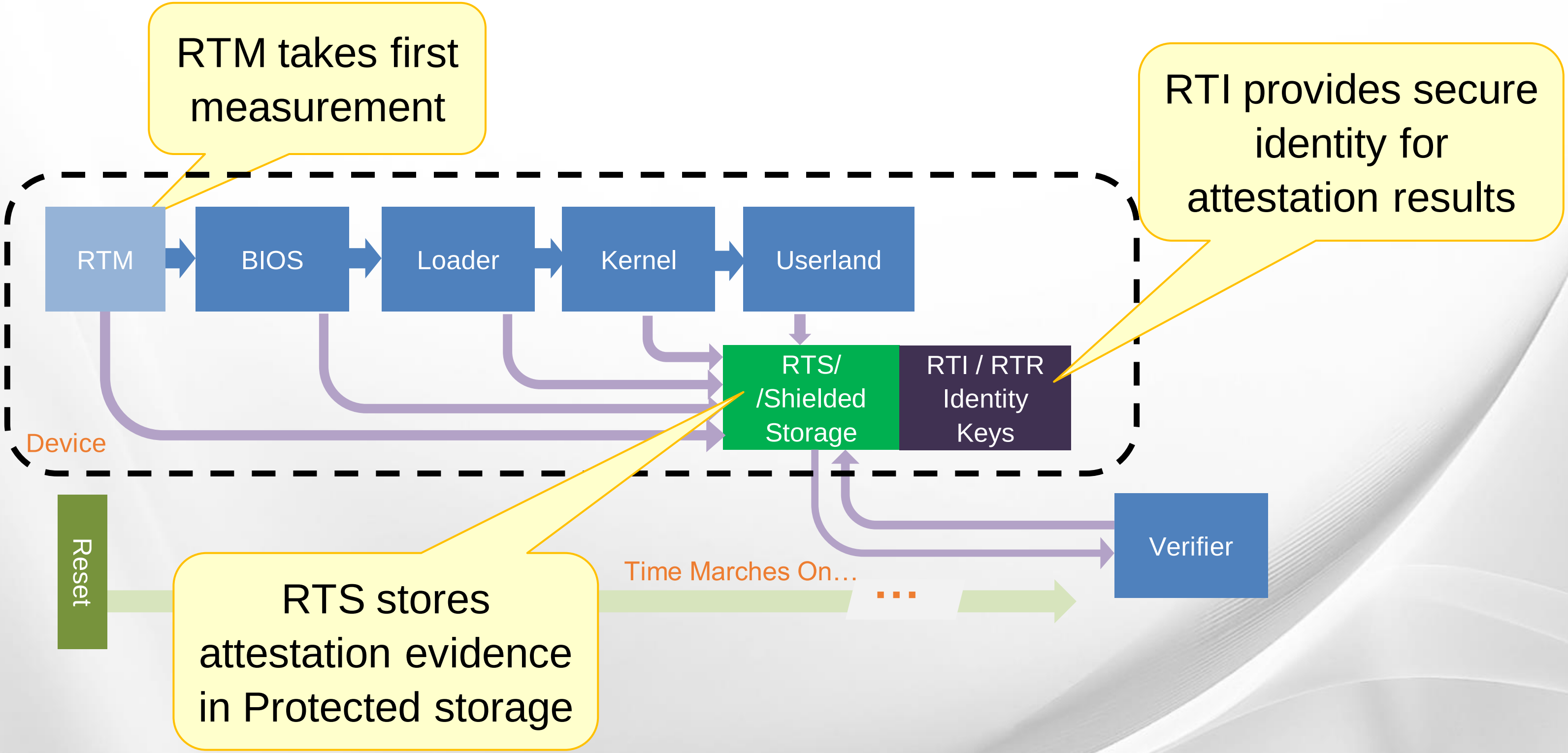
  "A component that performs one or more security-specific functions, such as measurement, storage, reporting, verification, and/or update. It is trusted always to behave in the expected manner, because its misbehavior cannot be detected (such as by measurement) under normal operation."

- Roots of Trust must be carefully isolated from system and application software to ensure they can't be inadvertently modified.
- Dedicated hardware or specialized processor features are usually required for a reliable Root of Trust

Root of Trust Functions

- RTM – Root of Trust for Measurement
  - Measures First Mutable Code to start the attestation chain
- RTS – Root of Trust for Storage
  - Provides Shielded storage for keys and measurements
- RTI/RTR – Root of Trust for Identity, Reporting
  - Protects a difficult-to-hack digital identity for each device (e.g., a signed copy of the serial number and vendor name)

Roots of Trust in Attestation


RTM takes first measurement
RTI provides secure identity for attestation results
RTM
BIOS
Loader
Kernel
Userland
RTS/ /Shielded Storage
RTI / RTR Identity Keys
Device
Verifier
Reset
Time Marches On…
…
RTS stores attestation evidence in Protected storage

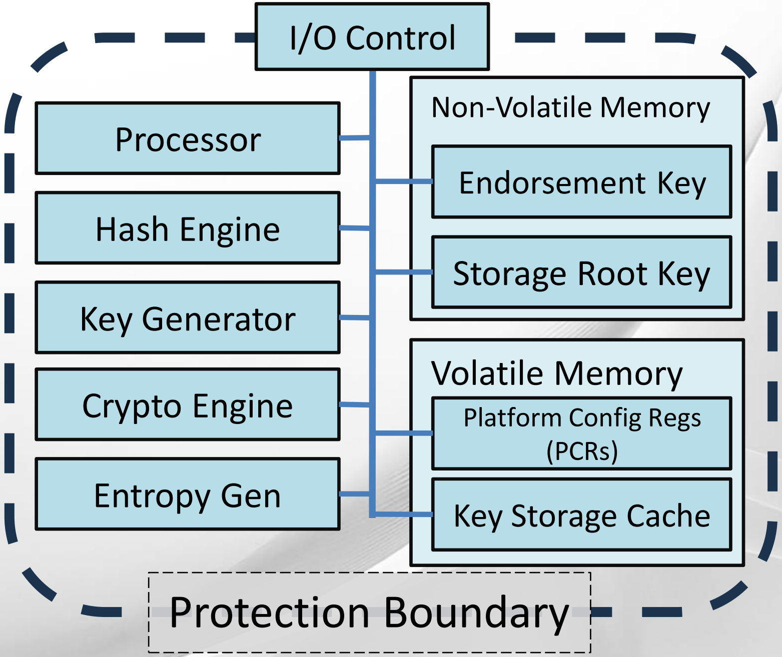
TCG RoT Technologies

TCG currently specifies three Root of Trust technologies:

- TPM
  - Small, isolated crypto-processor
  - Either a hardware chip or firmware in a processor’s trusted enclave
- MARS
  - Minimal set of TPM-like features, designed to be embedded as an IP block in small processors or microcontrollers.
- DICE
  - Very light hardware requirements, dependent on distributed software implementation to manage the chain of trust.

TPM

- Self Contained, low-power Crypto Processor
- Secure storage for keys, attestation results and other data
- Rich TCG support environment, libraries, guidance documents, etc


I/O Control

Processor

Hash Engine

Key Generator

Crypto Engine

Entropy Gen

Non-Volatile Memory

Endorsement Key

Storage Root Key

Volatile Memory

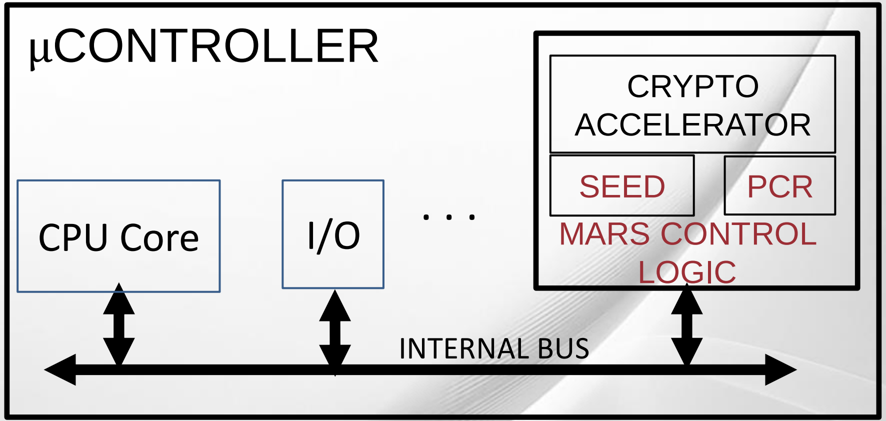
Platform Config Regs (PCRs)

Key Storage Cache

Protection Boundary

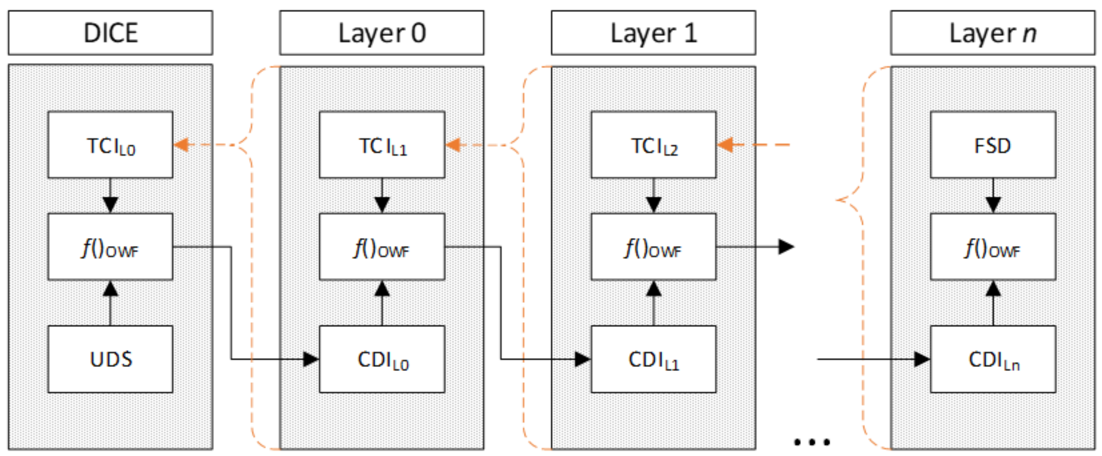
MARS

- Like a minimal TPM with functions essential for Identity and Attestation
- Designed as an Intellectual Property block for inclusion on small processors and controllers
- Not API-compatible with TPM, but offers very similar modes of interaction.



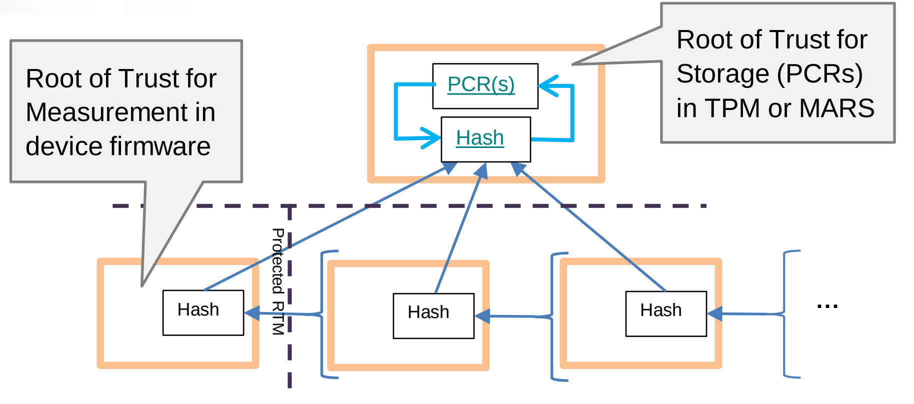
DICE

- Very simple hardware requirements
- The rest of DICE can be done in software
  - Optional DPE hardware can simplify some software handoff steps
- Uses a “Distributed Model”, rather than focusing on a single element like the TPM or MARS.
- Different approach for Attestation



TRUSTED® COMPUTING GROUP

Comparing Attestation Models

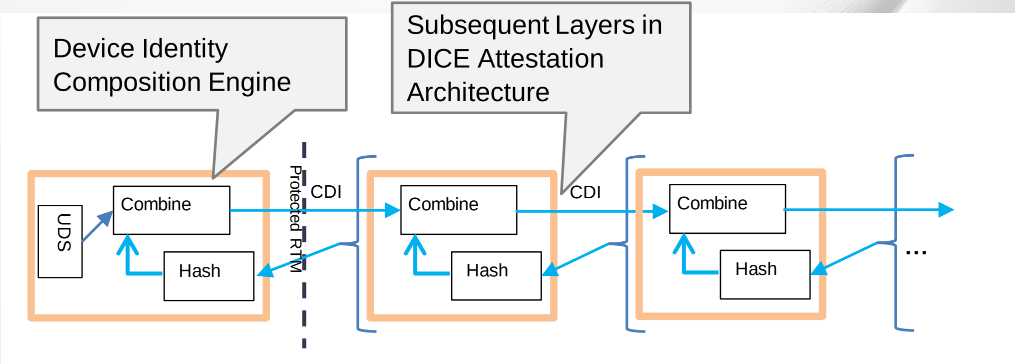


Root of Trust for Measurement in device firmware

Root of Trust for Storage (PCRs) in TPM or MARS

TPM / MARS Attestation

DICE Attestation



Device Identity Composition Engine

Subsequent Layers in DICE Attestation Architecture

TRUSTED®
COMPUTING
GROUP

Comparison Summary

	TPM	MARS	DICE
RTM **(Root of Trust for Measurement)**	An RTM is Required by all three, but out of scope		
RTS **(Root of Trust for Storage)**	PCRs to store measurements. Many other Protected Storage capabilities.	One or more PCRs to store measurements.	Hardware secures initial UDS secret. Then each layer secures its own secrets.
RTR **(Root of Trust for Reporting)**	TPM signs attestation reports	MARS hardware signs attestation reports	Final layer reports aggregate attestation chain
Hardware Overhead	A chip, or firmware in an enclave	Intellectual Property block in silicon	UDS hardware latch

For More Information

- Overview of TCG Technologies for Device Identification and Attestation Version 1.0 Revision 1.37

https://trustedcomputinggroup.org/wp-content/uploads/Overview-of-TCG-Technologies-for-Device-Identification-and-Attestation-Version-1.0-Revision-1.37_5Feb24-2.pdf

Thank You!

For More Information

- TCG Glossary Version 1.1 - https://trustedcomputinggroup.org/resource/tcg-glossary/
- TCG Root of Trust Specification - https://trustedcomputinggroup.org/wp-content/uploads/TCG_Roots_of_Trust_Specification_v0p20_PUBLIC_REVIEW.pdf
- TPM 2.0 *Trusted Platform Module Library Family "2.0" Specification - Parts 1-4 and Code, Revision 1.59* https://trustedcomputinggroup.org/resource/tpm-library-specification/
- *TPM 2.0 Mobile Reference Architecture*, Revision 142, 16 December 2014, https://trustedcomputinggroup.org/resource/tpm-2-0-mobile-reference-architecture-specification/
- IETF Remote Attestation ProcedureS (RATS) Architecture, https://datatracker.ietf.org/doc/rfc9334/
- DICE *Hardware Requirements for a Device Identifier Composition Engine* https://trustedcomputinggroup.org/resource/hardware-requirements-for-a-device-identifier-composition-engine/
- DICE Layering Architecture - https://trustedcomputinggroup.org/wp-content/uploads/DICE-Layering-Architecture-r19_pub.pdf
- DICE Attestation Architecture - https://trustedcomputinggroup.org/resource/dice-attestation-architecture/
- DICE Protection Environment - [public review] https://trustedcomputinggroup.org/wp-content/uploads/TCG-DICE-Protection-Environment-Specification_14february2023-1.pdf
- *Measurement and Attestation RootS (MARS) Library Specification*, https://trustedcomputinggroup.org/resource/mars-library-specification/
- TCG Network Equipment - https://trustedcomputinggroup.org/resource/tcg-guidance-securing-network-equipment/
- *Trusted Computing Platforms: TPM2.0 in Context*, Graeme Proudler, Liqun Chen, Chris Dalton, Springer 2014
- IETF RIV *TPM-based Network Device Remote Integrity Verification* - https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/