Protecting IoT Ecosystems and AI Leveraging TCG Standards

Today’s Presenter

Thorsten Stremlau
Systems Principle Architect
NVIDIA

Thorsten Stremlau is a Systems Principal Architect at NVIDIA . He is known for identifying digital transformation strategies and integrating AI and technologies into the product development processes to improve security capabilities . Thorsten has been part of TCG for over 20 years and is currently the co-chair of the Marketing Work Group.

Trusted Computing Group (TCG)

Open Standards for Trusted Computing

- TCG is the only group focused on Trusted Computing standards
- You know TCG for our technical specs & guidance such as:
  - Trusted Platform Module (TPM = ISO 11889)
  - Self-encrypting drives (SED)
  - Trusted Network Communications (TNC)
- TPM specification implemented in more than a billion devices
  - Chips integrated into PCs, servers, printers, kiosks, industrial systems, and many embedded systems

TRUSTED® COMPUTING GROUP

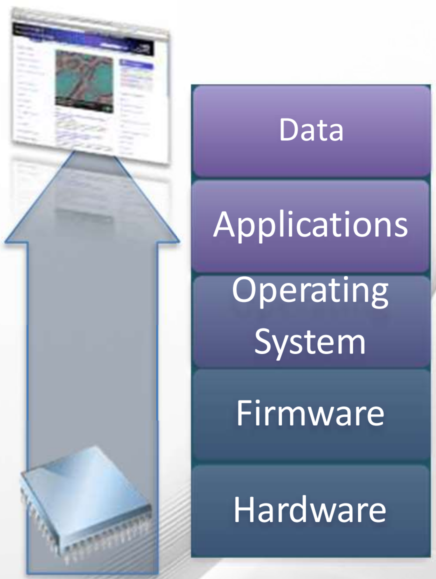
Agenda

- Providing a Foundation for Security
- Different Regulatory Action on AI
- The Problem Statement
- The Four AI Elements
- What TCG standards can be used to mitigate
    - TPM/MARS
    - DICE
    - FIM
    - RIM
    - CyRes

Providing a Foundation for Security

- **Ensure platforms are resilient to attacks**
  - Firmware and data are security-critical components
  - Must remain available and trustworthy in face of attacks
    - ***Protect*** firmware and critical data from unauthorized changes
    - ***Detect*** and ***Recover*** from problems

- **Provide secure and scalable means to recover systems, applications, and AI/enterprise data**
  - These mechanisms must themselves be resilient to tampering/corruption by destructive malware
  - Built upon trust in the platform recovery support



TRUSTED® COMPUTING GROUP

Spinal Tap: Conversion Error

Company fined £44,000 after 27,000 chickens die after overheating after farm ventilator failure

CENTRAL | ANIMALS | MELTON MOWBRAY | LEICESTERSHIRE | Thursday 28 April 2022 at 9:11pm

Credit: PA Images

https://www.itv.com/news/central/2022-04-28/company-fined-44k-after-27000-chickens-die-due-to-ventilation-failure

TRUSTED® COMPUTING GROUP

EU AI ACT

EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Establish and implement **risk management** processes

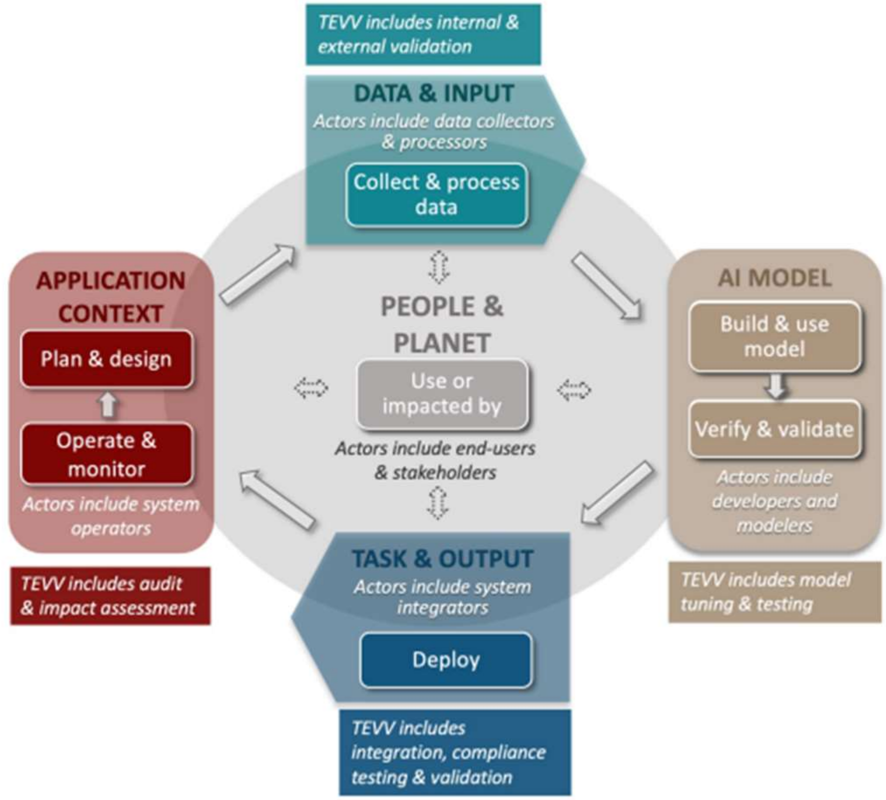
&

In light of the **intended purpose** of the AI system

- Use high-quality **training, validation and testing data** (relevant, representative etc.)
- Establish **documentation** and design logging features (traceability & auditability)
- Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)
- Ensure **human oversight** (measures built into the system and/or to be implemented by users)
- Ensure **robustness**, **accuracy** and **cybersecurity**

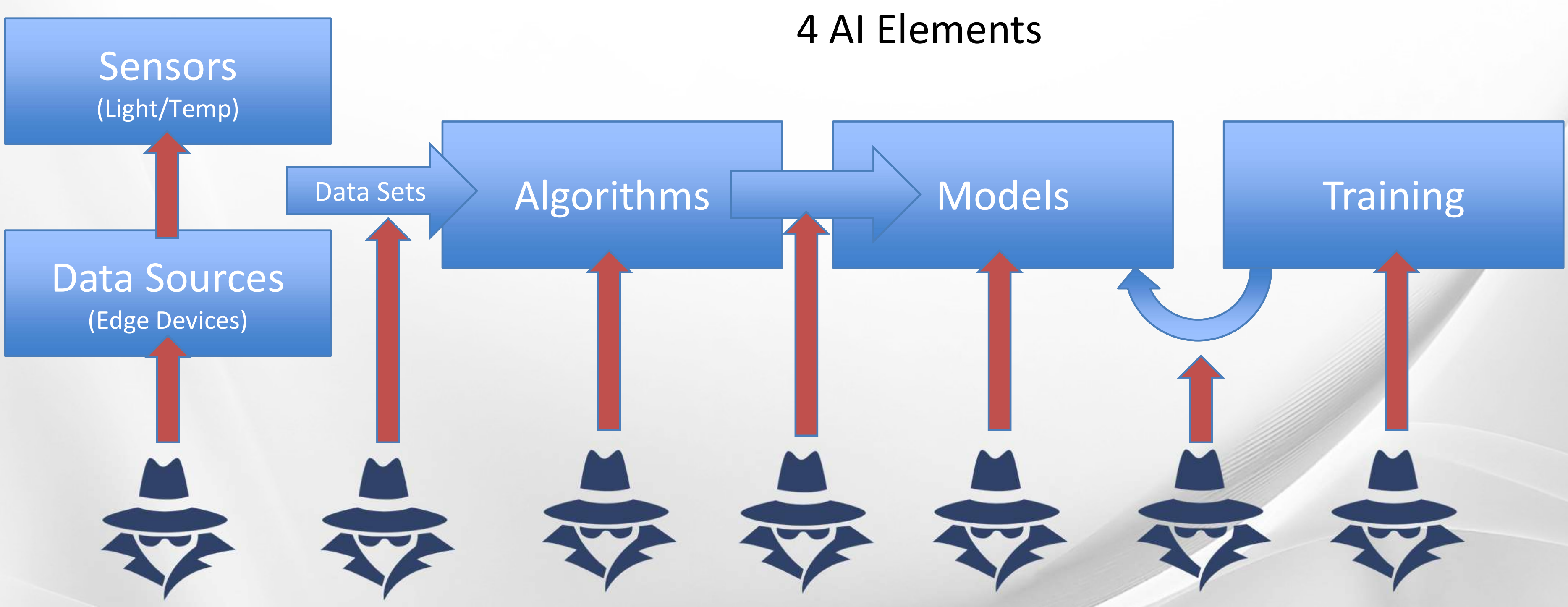
TRUSTED® COMPUTING GROUP

Figure 1: Lifecycle and Key Dimensions of an AI System. Modified from OECD (2022) OECD Framework for the Classification of AI systems | OECD Digital Economy Papers. Risk management should be continuous, timely, and performed throughout the AI system lifecycle, starting with the plan & design function in the application context.



Test, Evaluation, Verification, and Validation (TEVV)

Multiple Attack Surfaces



Problem Statement

How to protect AI against illicit modifications and injection of erroneous data

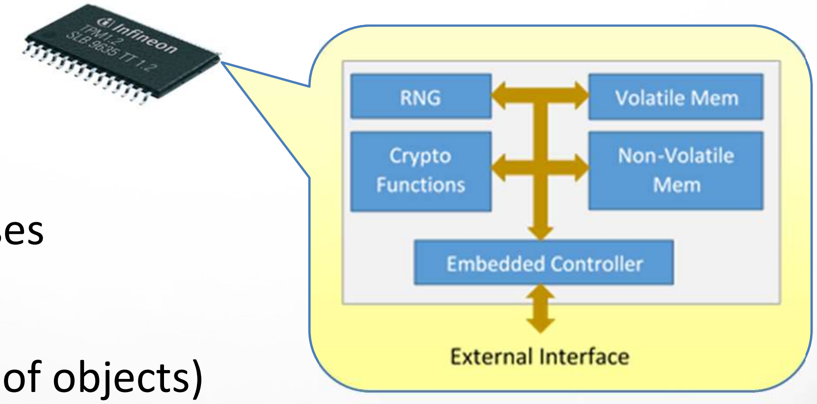
What we would like to do:

1. Ensure the integrity of the data flow and attest to data sources
2. Ensure algorithms are not modified by untrusted sources
3. Establish Integrity and attestation of models
4. Properly identify and attest training sources and input

Trusted Platform Module (TPM)

The *__Standard__* *Hardware Root of Trust*

- Trusted Platform Module (TPM)
  - Self-contained security processor
  - Inexpensive & small (~0.1 watt, ~$1)
  - Connects to inexpensive processor buses
- TPM provides:
  - Secure storage of boot state (= hashes of objects)
  - Secure storage of runtime state (= hashes of software applications)
  - Secure storage of cryptographic secrets (e.g. private keys)
  - Cryptographic-quality Random Number Generator
  - Resistance to physical attack (i.e. reverse-engineering) to keep private keys private
- Specified by Trusted Computing Group, a standards group



Platform Configuration Register (PCR)

- PCR Values can only be 'extended', no direct write
  - PCR_{new} = Hash(Digest + PCR_{old})
  - Digest is computed by host machine
- PCRs are usually only resettable by a reset of the TPM
- TPM can bind secrets and policies to the value of a PCR
- TCG defines number of PCRs and which measurements should be stored in them.

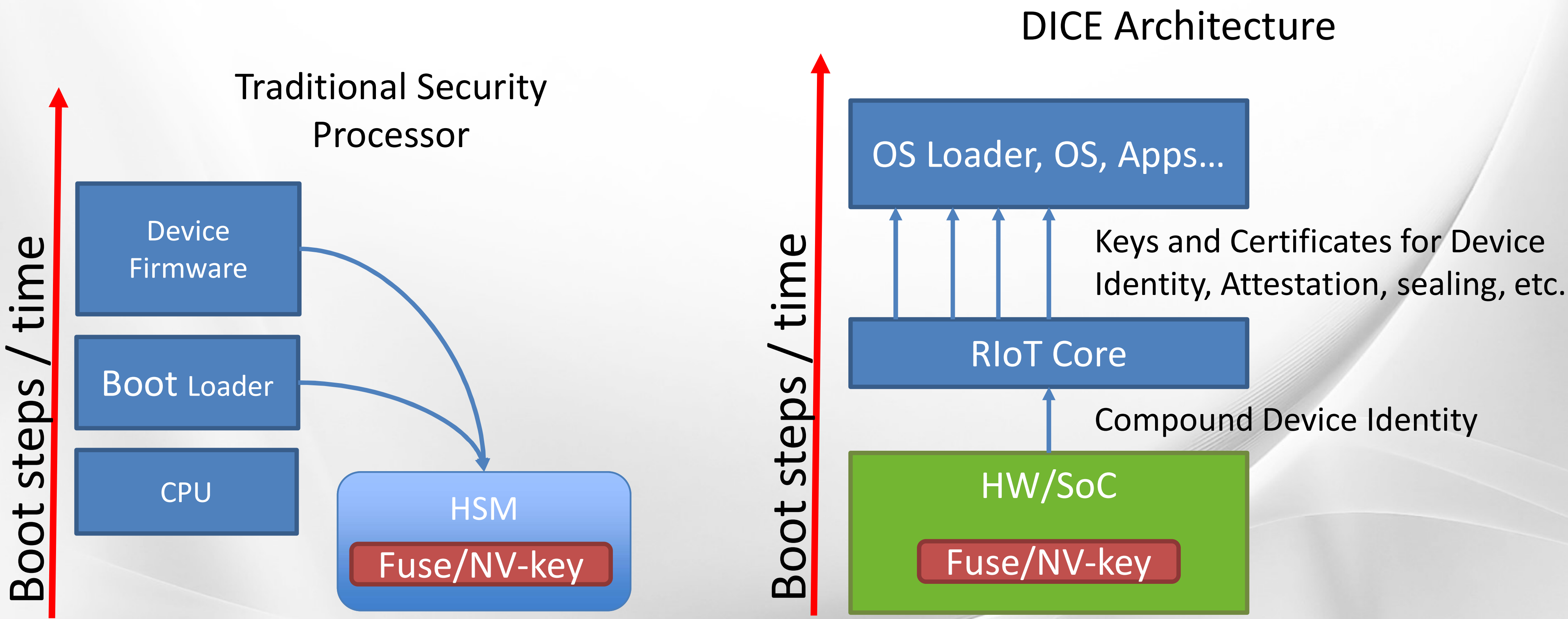
DICE

- Device Identifier Composition Engine (DICE, TCG)
- A specification from the Root of Trust for Measurement subgroup in the Trusted Computing Group (TCG)
- Foundational security for HW at near zero cost
- Simple hardware requirements mean DICE is adaptable to most any system or component
- Provides HW-based identity and attestation, and a foundation for sealing, data integrity, device recovery and update

THE DICE MODEL

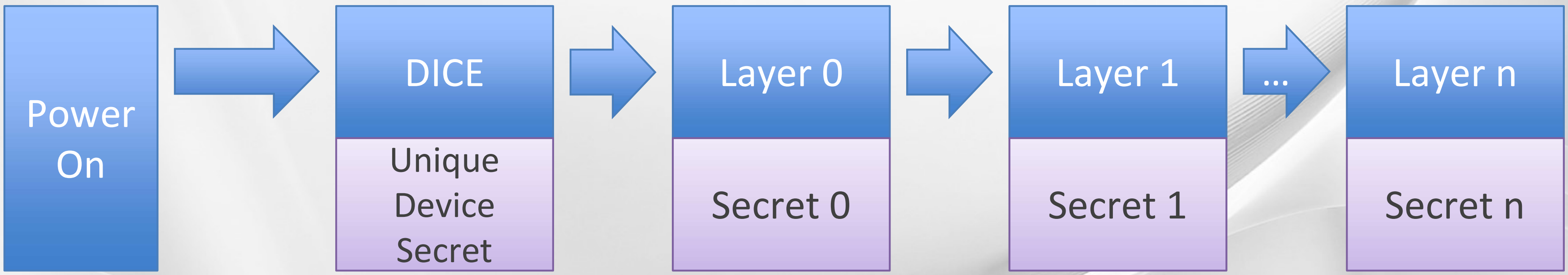
- In a DICE Architecture device startup (boot) is layered
- Beginning with a Unique Device Secret (UDS), secrets/keys are created that are unique to the device and each layer and configuration
- This derivation method means that if different code or configuration is booted, secrets are different
- If a vulnerability exists and a secret is disclosed, patching the code automatically re-keys the device

THE DICE MODEL



THE DICE MODEL

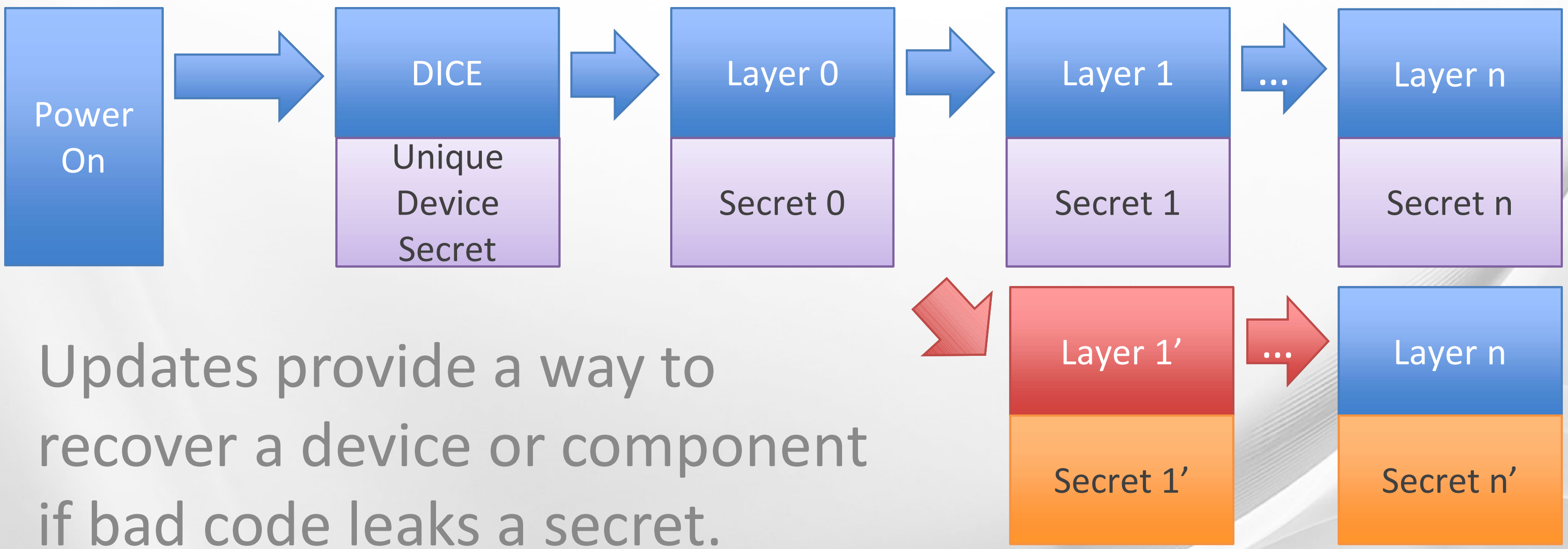
- Power-on (reset) unconditionally starts the DICE
- DICE has exclusive access to the UDS
- Each layer computes the secret for next layer (via OWF)
- In this derivation chain, each layer must protect the secret it receives



TRUSTED COMPUTING GROUP

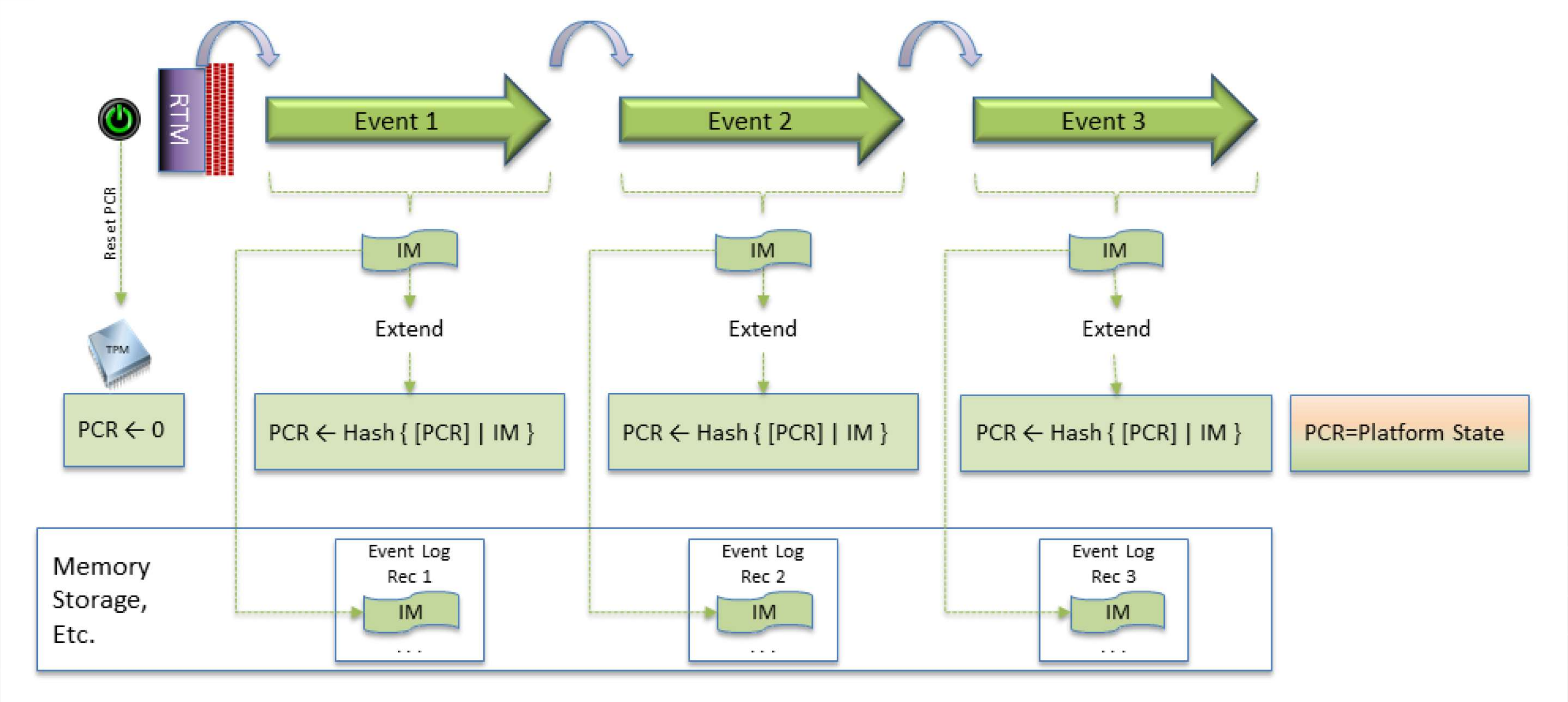
WHEN SOMETHING CHANGES

- The branch illustrates the result of a code/config change

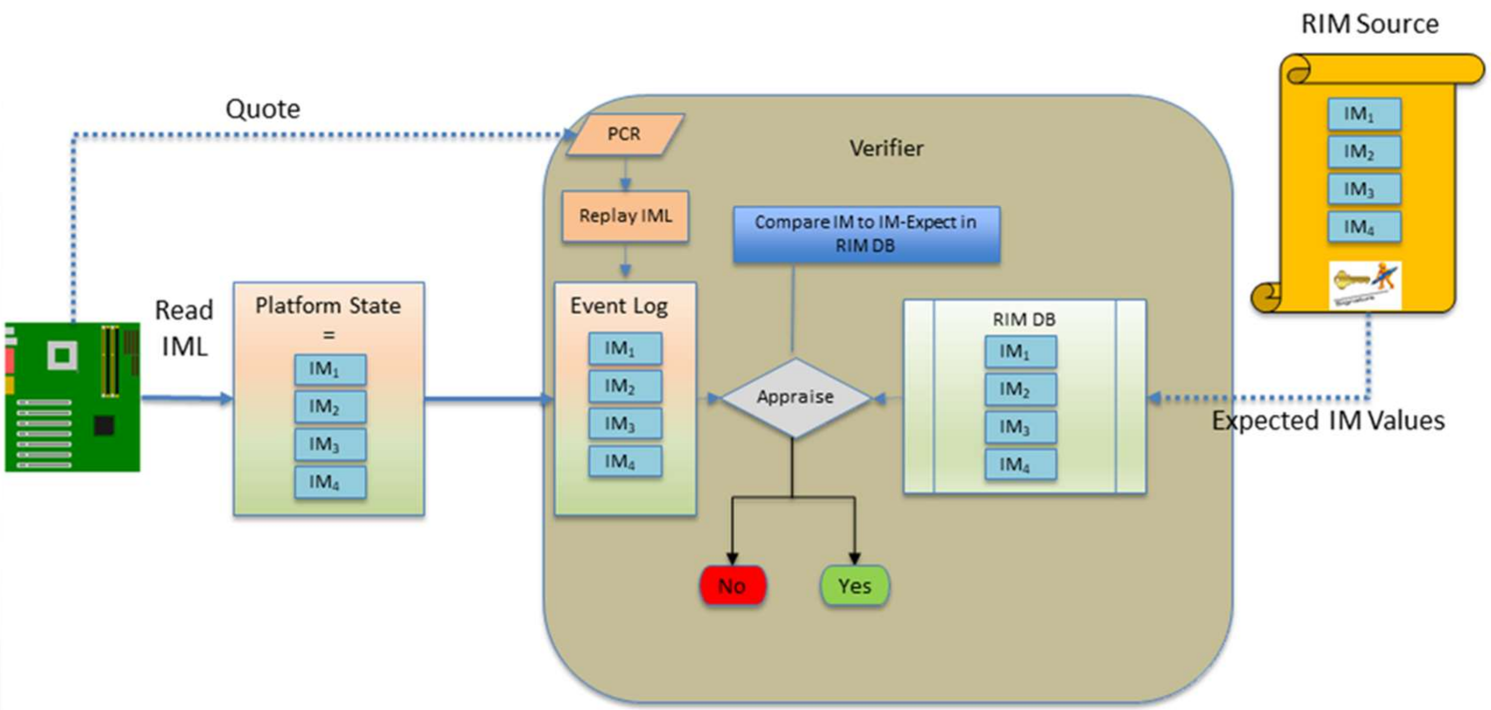


- Updates provide a way to recover a device or component if bad code leaks a secret.

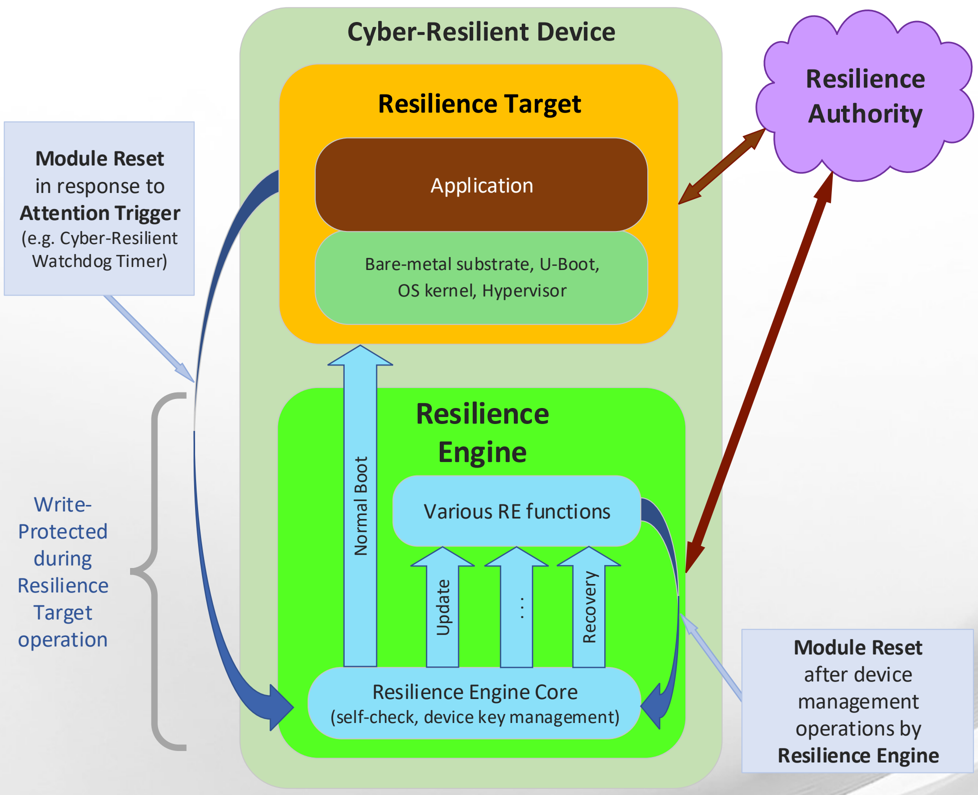
Integrity Measurement



TRUSTED® COMPUTING GROUP



CyRes Workgroup



Call to Action

TRUSTED®
COMPUTING
GROUP

Questions?
Post Your Questions Now

Thank You!

Contacting Trusted Computing Group

Website:
www.trustedcomputinggroup.org
Email:
admin@trustedcomputinggroup.org
LinkedIn:
https://www.linkedin.com/groups/4555624
Twitter:
@TrustedComputin