TCG Cyber Resilient Technologies

Embedded Technologies Expo & Conference
June 26, 2019

Rob Spiger

TCG Cyber Resilient Technologies Workgroup Co-chair and
TCG Vice President

Microsoft Principal Security Strategist

Agenda

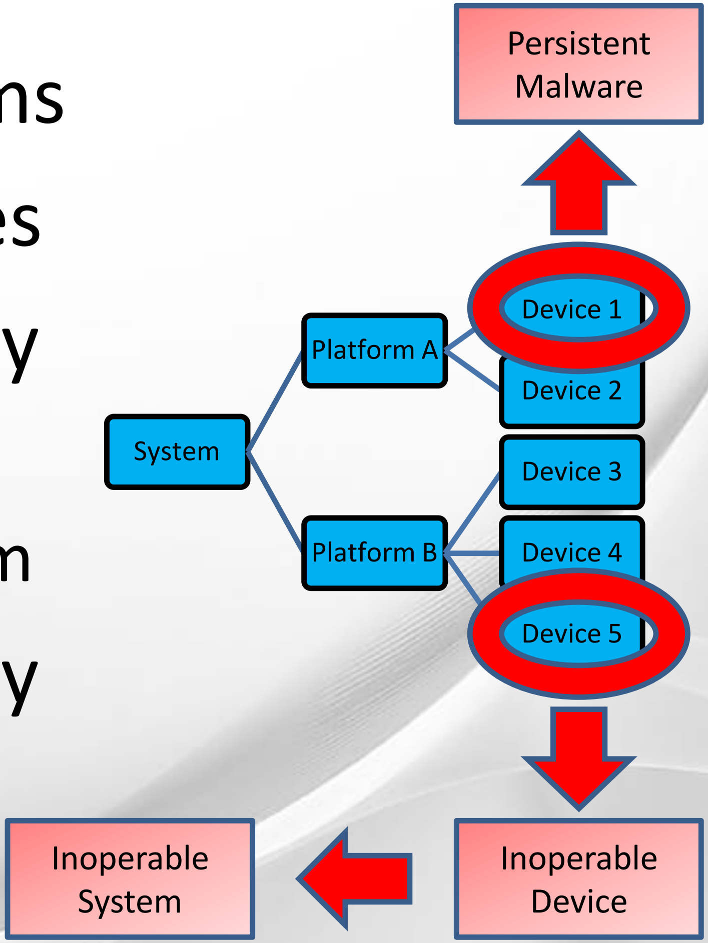
- Motivation: NIST SP 800-193 (Platform Firmware Resiliency Guidelines)
- TCG Cyber Resilient Technologies Workgroup:
  - Goals
  - Scope and Structure
  - Deliverables
- Work in progress
  - Representative scenarios
  - Draft definitions
  - Relationship with roots of trust
  - Cyber Resilient Building Blocks
- What comes next

NIST Special Publication 800-193 : Platform Firmware Resiliency Guidelines

- Published by NIST in May 2018
- North star for many of the TCG participants
- Potential for widespread remote attacks to cripple systems
- Protection of firmware and critical data
- Looks at how to better protect systems and reliably recover

NIST SP 800-193:
Devices are Important

- Systems are made of platforms
- Platforms are made of devices
- Devices are crucial to integrity and availability of systems
  - Device attacks corrupt a system
- Without devices, systems may fail to operate
  - Device attacks may cause permanent damage



NIST SP 800-193:
System Architecture Diagram

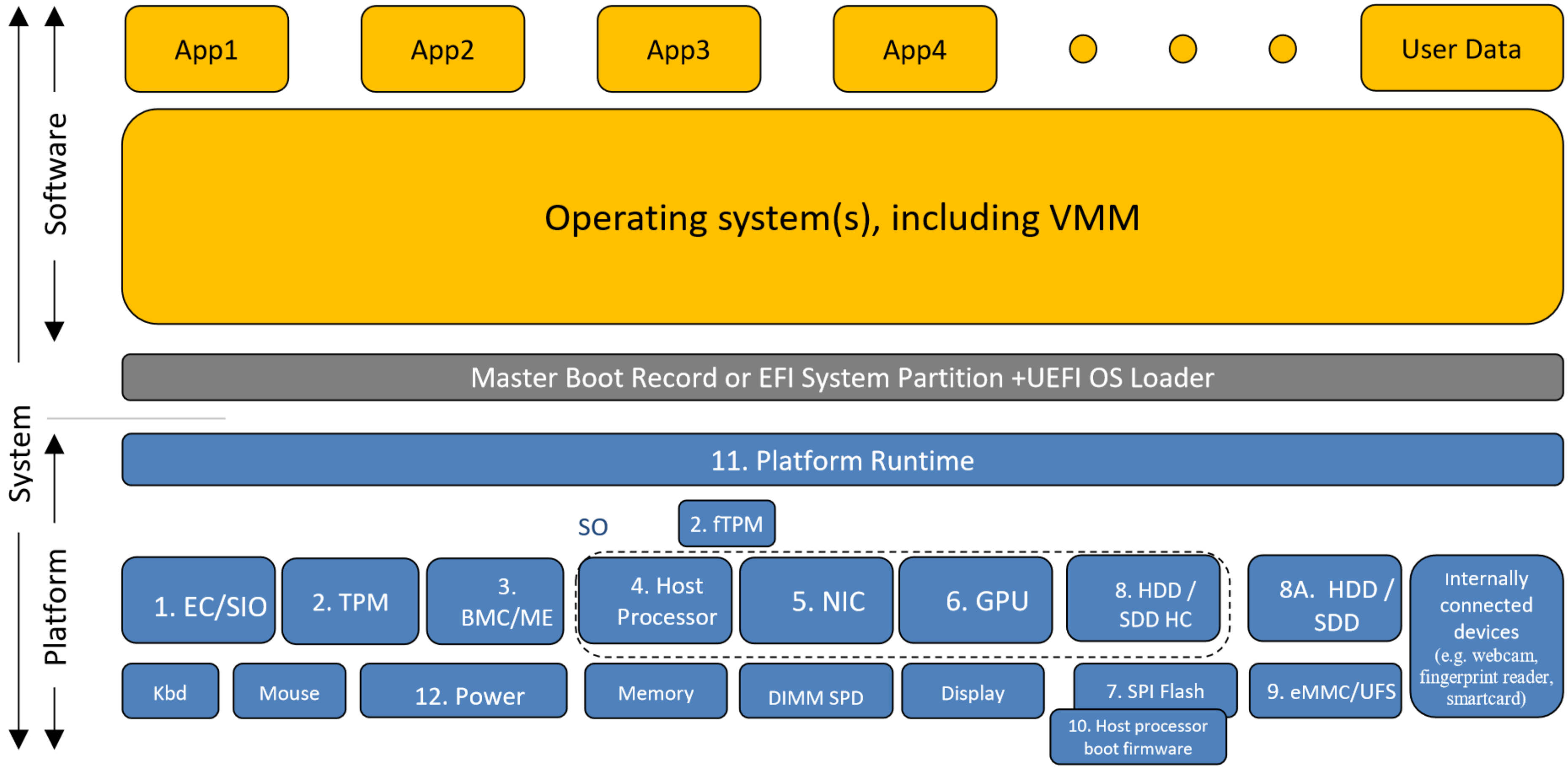


Figure 1: High-Level System Architecture

NIST SP 800-193: Definition of Resiliency

- Resiliency applied to information systems as:

  "ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources"

- Need to expect attacks and respond…
  - Understand platform and devices deeply
  - Increase **Protection** against attacks for platforms and devices
  - **Detect** when attacks have occurred
  - **Recover** from attacks to a state of integrity

NIST SP 800-193: Roots and Chains of Trust

- Root of trust/chain of trust concept
  - A component performing security-specific functions
  - Trusted to always behave in an expected manner
  - Its misbehavior cannot be detected
  - Can be start of a chain of trust to deliver more complex functionality (like recovery)
- Roots of trust in 800-193
  - Update: Authenticates updates prior to persisting
  - Detection: Authenticates code prior to execution and looks for malware/corruption
  - Recovery: Restores code/config regardless of malware

TCG Workgroup:
Cyber Resilient Technologies

Created in June 2018

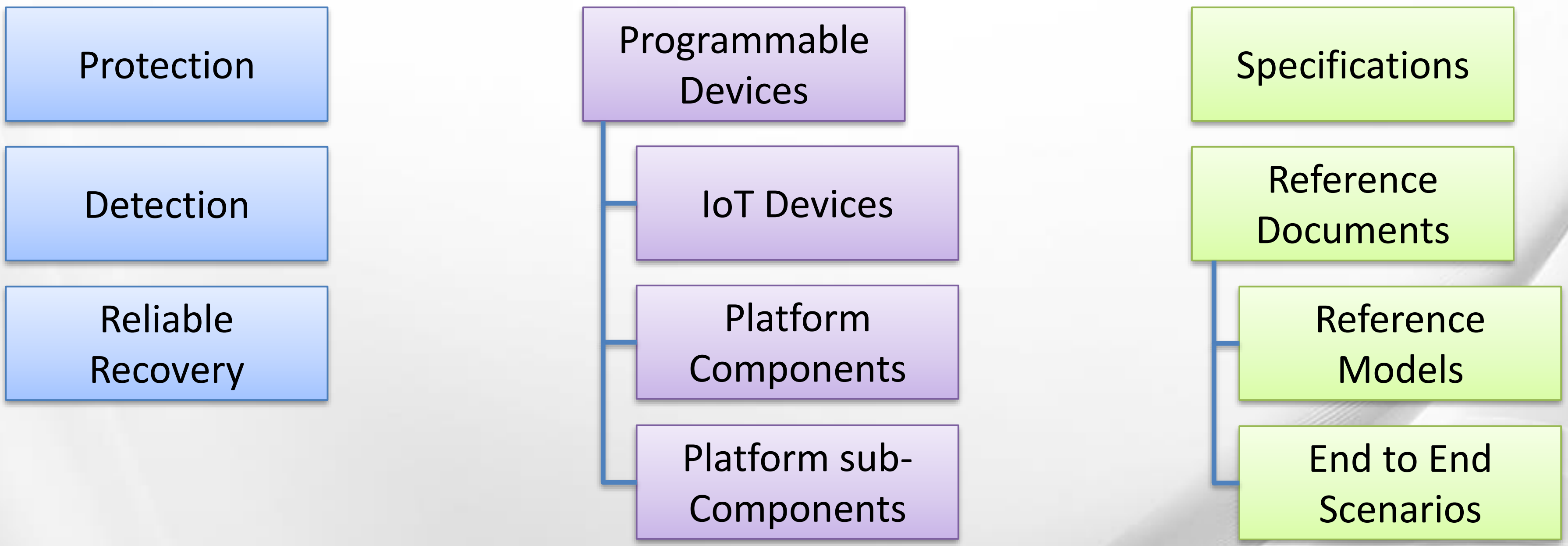
Goals in Progress:

- Explain how to implement 800-193 using TCG technologies
- Explore how TCG technologies help satisfy protection, detection and recovery requirements
- Manage autonomous components without a person

Future Goals:

- Improve software detection using attestation
- Address recovery authorization challenges

Cyber Resilient Technologies Workgroup Scope



Security Focus

- Protection
- Detection
- Reliable Recovery

Context (Abstract)

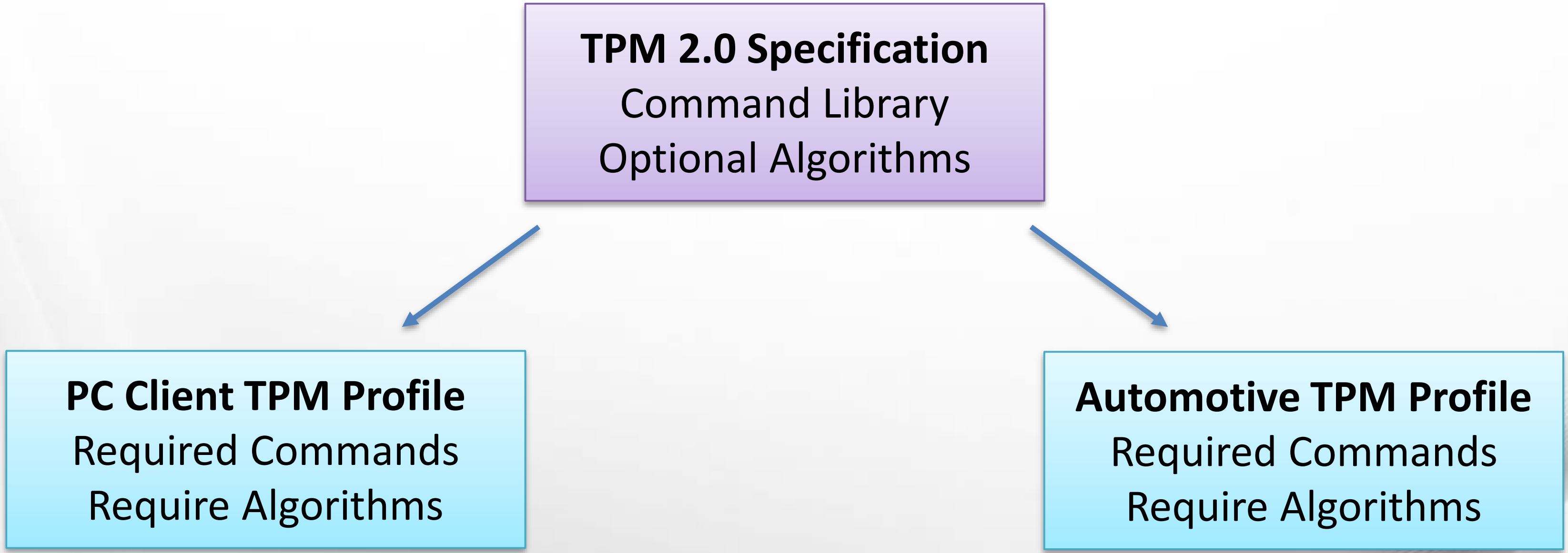
- Programmable Devices
  - IoT Devices
  - Platform Components
  - Platform sub-Components

Output

- Specifications
- Reference Documents
  - Reference Models
  - End to End Scenarios

- Defining abstract building blocks to help with resilience
- Drawing from existing standards whenever possible

TCG Building Block Example: Relationship to Platform Requirements



TPM 2.0 Specification
Command Library
Optional Algorithms

PC Client TPM Profile
Required Commands
Require Algorithms

Automotive TPM Profile
Required Commands
Require Algorithms

- TCG defines platform independent building blocks
- TCG platform workgroup define requirements in the context of a specific type of platform
- Similar model for cyber resilient building blocks

Resilient
Building Block Deliverables

In Progress:

- Protecting persistent storage except through authorized recovery or update mechanisms
- Failsafe mechanisms for pushing updates to out of date and/or compromised devices

Future:

- Provisioning mechanisms to deploy resiliency policies and obtain updates
- Discovery mechanisms for device resiliency characteristics and manufacturer maintenance updates
- Hardware and software mechanisms to reliably trigger recovery, and protocols, if required
- Mechanisms to recover from vendor, operator, customer or technology failures

Scenarios Considered

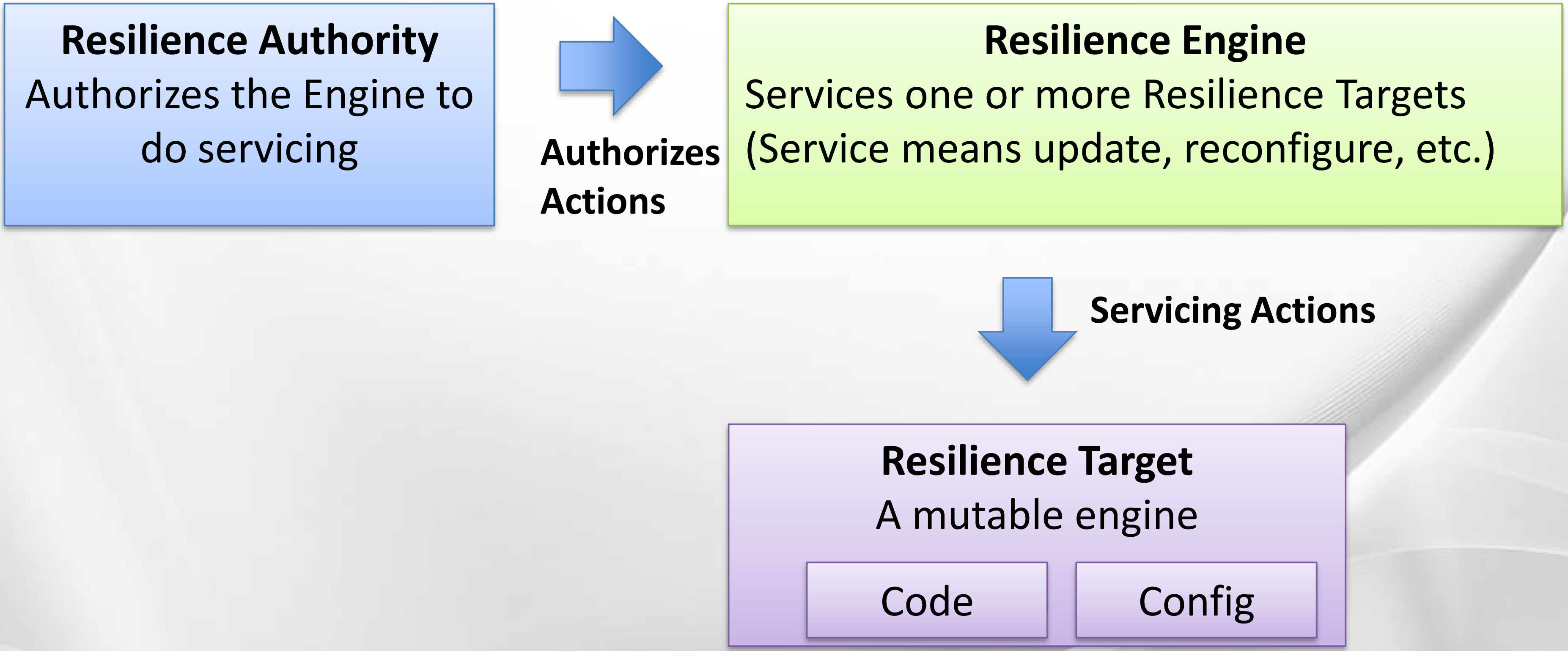
- Microcontroller-based Smart Device
- Network connected Security Camera
- Management of a High-Availability Industrial Controller
- Firmware Management of a sub-component of a computing platform (for example: a Storage Controller in a PC/Server)
- Management of Nodes in Sensor Networks
- Management of Embedded Controller Units (ECU) in Automotive Domain

Focus for each scenario is how they could be better using resilient technologies

Draft Definitions

- **Resilience Target** - A mutable engine that is serviceable by one or more Resilience Engines.
- **Resilience Engine** - An engine that services one or more local Resilience Targets. A Resilience Engine recognizes one or more Resilience Authorities for servicing instructions.
- **Resilience Authority** - An entity that authorizes a Resilience Engine to perform servicing actions on a Resilience Target.

Definitions Visually



Resilience Authority
Authorizes the Engine to do servicing

Authorizes Actions

Resilience Engine
Services one or more Resilience Targets
(Service means update, reconfigure, etc.)

Servicing Actions

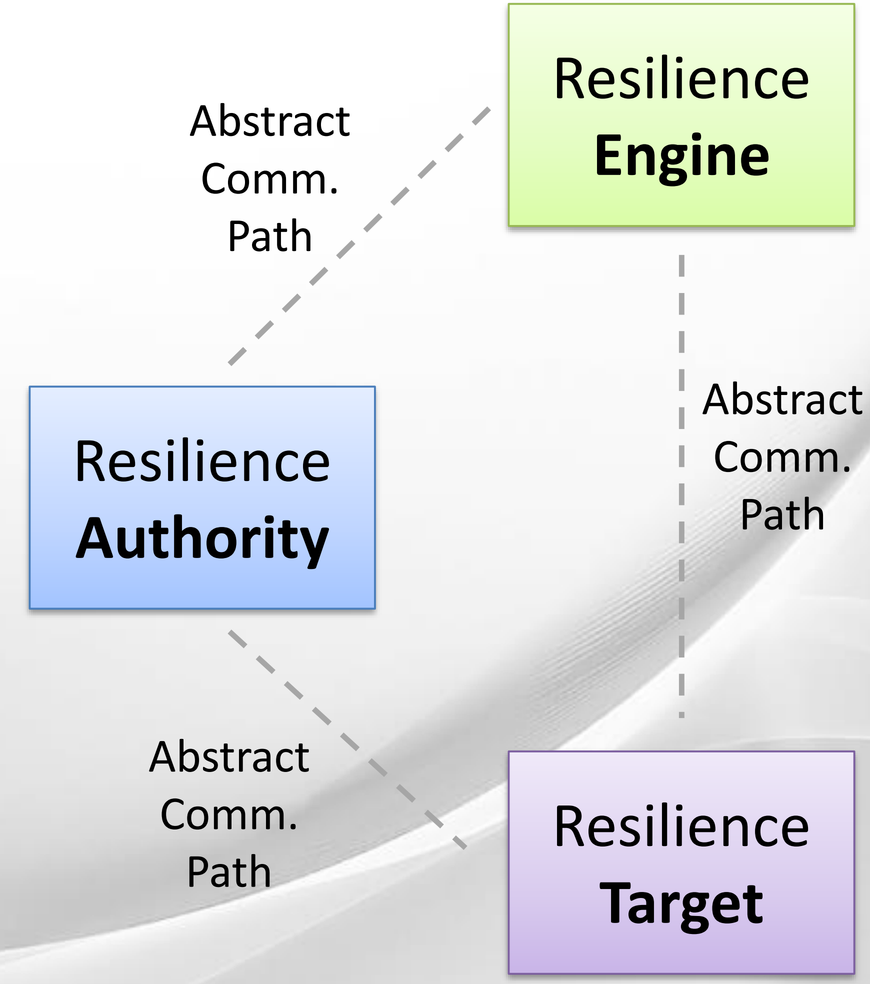
Resilience Target
A mutable engine

Code

Config

Relationships Between Terms

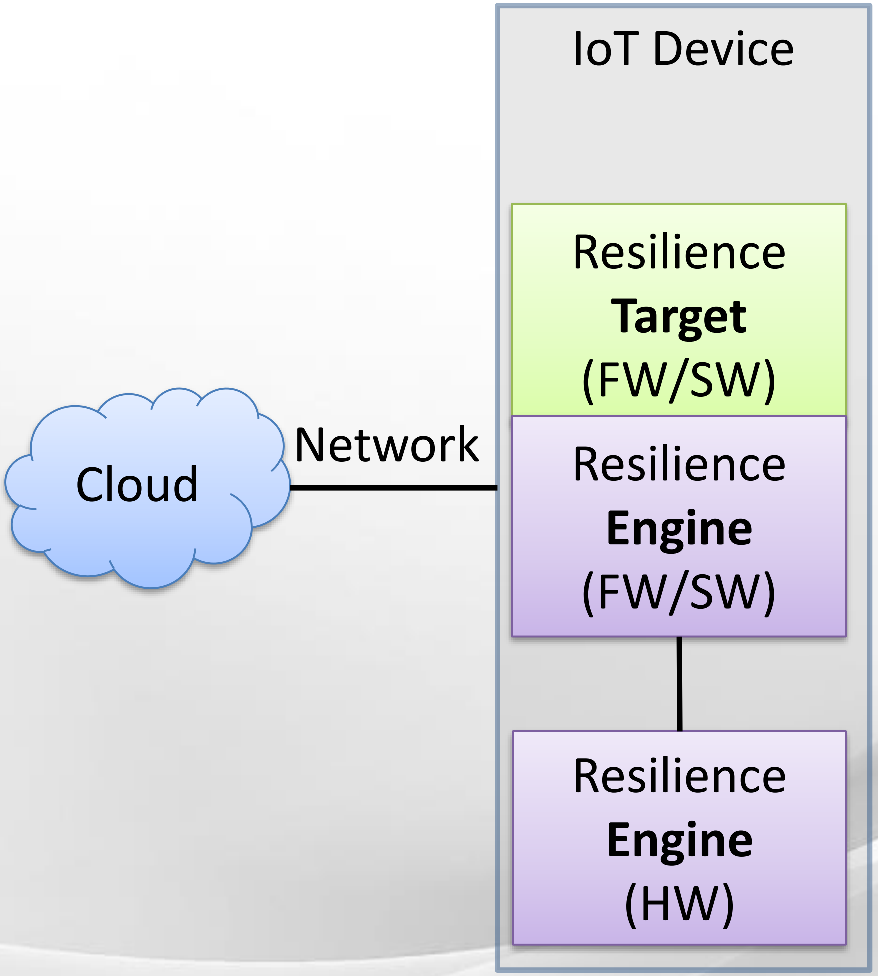
- Note: The Engine is local to the Target
- Solutions are likely to have communication between all three entities
- Example: The Target attesting its health to the Authority



Roots of Trust

- NIST SP 800-193 defined new roots of trust: Update, Detection and Recovery
- With TPM, TCG defined roots of trust for Storage, Measurement and Reporting
- Note: The Resilience Engine definition is separate from the roots of trust for Storage, Reporting and Measurement
- Roots of Trust for Storage, Reporting and Measurement could be optional in some resilient architectures
  - Example: Target is regularly overwritten entirely

IoT Example with a Remote Resilience Authority


IoT Device
Resilience **Target** (FW/SW)
Cloud
Network
Resilience **Engine** (FW/SW)
Resilience **Engine** (HW)

Basic Building Blocks

- Secure Execution Environment – “Safe place to stand” for the Resilience Engine
    - Ensures a potentially compromised Resilience Target cannot affect recovery during runtime
- Protection Latches (Write-Lock, Read-Lock)
    - Ensures a potentially compromised Resilience Target cannot affect the persistent storage of the Resilience Engine
- Watchdog Timers
    - Ensures a potentially compromised Resilience Target cannot affect the Resilience Engine from performing the recovery

Watchdog Timer Types

- Conventional Watchdog
  - “I hope malware doesn’t cancel me”
- Latchable Watchdog Timer
  - “Once you set me, I will power cycle”
- Authenticated Watchdog Timer
  - “Get someone to vouch that you’re healthy and I’ll let you keep running for another day”
- Wakeup Watchdog Timer
  - “I promise to wake you up even when malware tells you to sleep forever”

What is Next in the TCG Cyber Resilient Technology Workgroup

- Complete abstract library of cyber resilient building blocks specification
- Work with other TCG workgroups for developing platform specific guidance

Thank you and please consider joining us! ☺

Additional Information

- NIST Special Publication 800-193:

  https://csrc.nist.gov/publications/detail/sp/800-193/final
- TCG Home Page:

  https://trustedcomputinggroup.org/
- TCG Cyber Resilient Technology workgroup:

  https://trustedcomputinggroup.org/work-groups/cyber-resilient-technologies/
- Microsoft Cyber-Resilient Platform Program:

  http://aka.ms/cyres