presented by

Firmware Integrity Measurements and Attestation

UEFI 2020 Virtual Plugfest

October 21, 2020

Presented by Dick Wilkins, Ph.D., Phoenix Technologies

Meet the Presenter

Dick Wilkins, Ph.D.
Principal Technology Liaison
Member Company: Phoenix Technologies

Legal Stuff

Agenda

- NIST SP 800-155
- Why it Wasn’t Implemented
- What NIST has Done
- What the TCG and Others are Doing
- What’s Next/Call to Action
- Questions?

NIST SP 800-155

- NIST, part of the US Gov. Commerce Dept., Published Draft Special Publication "BIOS Integrity Measurement Guidelines," in December 2011
- The guidelines describe a secure firmware measurement and reporting chain to detect unauthorized modifications that may affect the security of platforms
  - Detects changes to code
  - Detects changes to configuration parameters
  - An external "verifier" can react to these changes

Not Widely Accepted

- The approach has been considered valuable
- Prototypes were developed
- But the guidelines have not been widely implemented
- Why? Many reasons… Maybe???
  - Too focused on firmware, what about other platform changes (hardware, after firmware)?
  - Too specific and tied to TPM hardware?
  - Not enough specific details provided?
  - Unexpected levels of complexity?
  - Limited standards for use by cooperating participants?

NIST comes to TCG

- In 2018 NIST proposed a collaboration with the Trusted Computing Group (TCG) on SP 800-155
- The TCG working groups would create detailed specifications needed to meet the guidelines proposed in 800-155

NIST comes to TCG (cont.)

- NIST contributed the text of SP 800-155 to the TCG as a starting point for specifications
- After the TCG specifications are published, NIST is likely to provide new guidelines
- This updated/new NIST document will likely point to the TCG specs as an implementation example

TCG Working Groups Involved

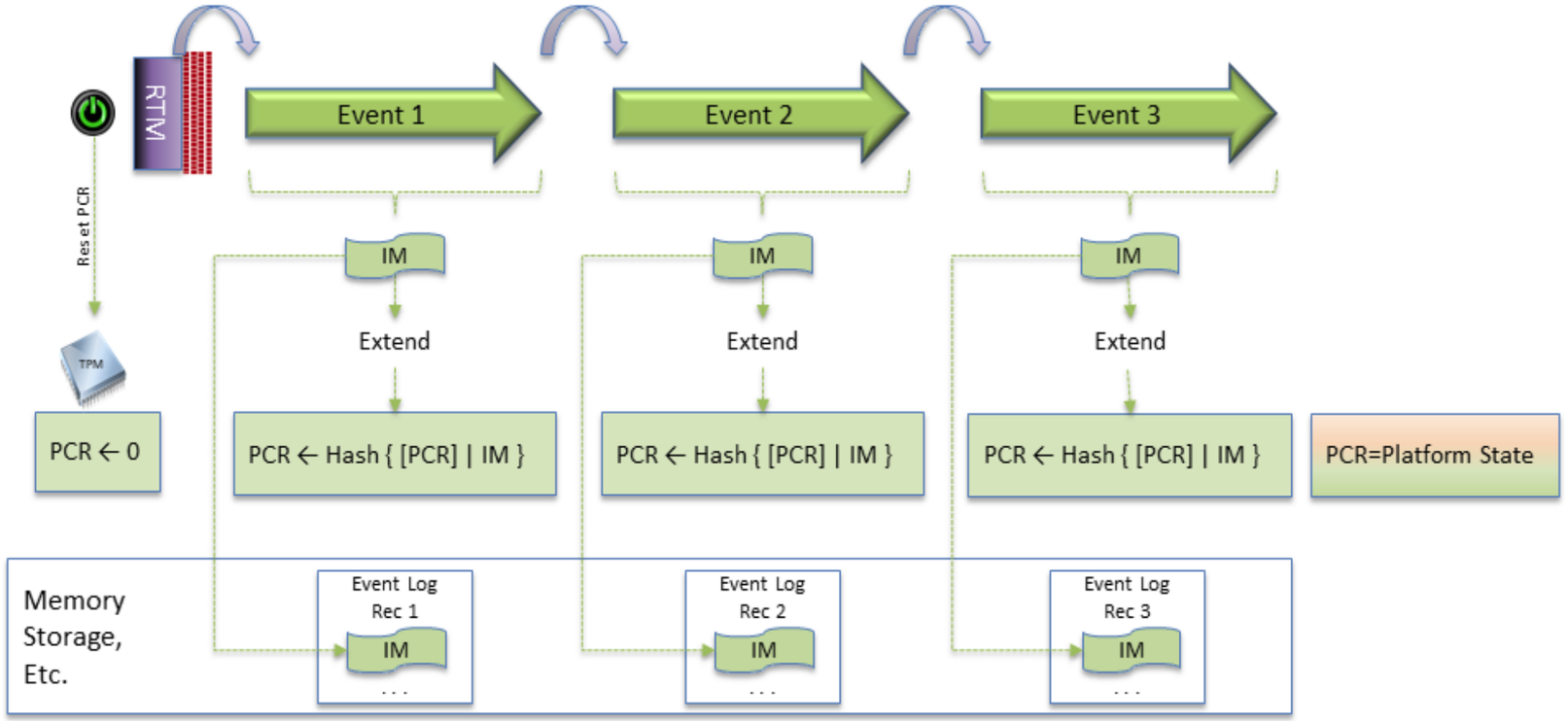
- PC Client Working Group
- Server Working group
- Attestation Working Group
- Infrastructure Working Group
- Trusted Network Communications Working Group
- DICE Working Group

Other Non-TCG Groups Weigh In

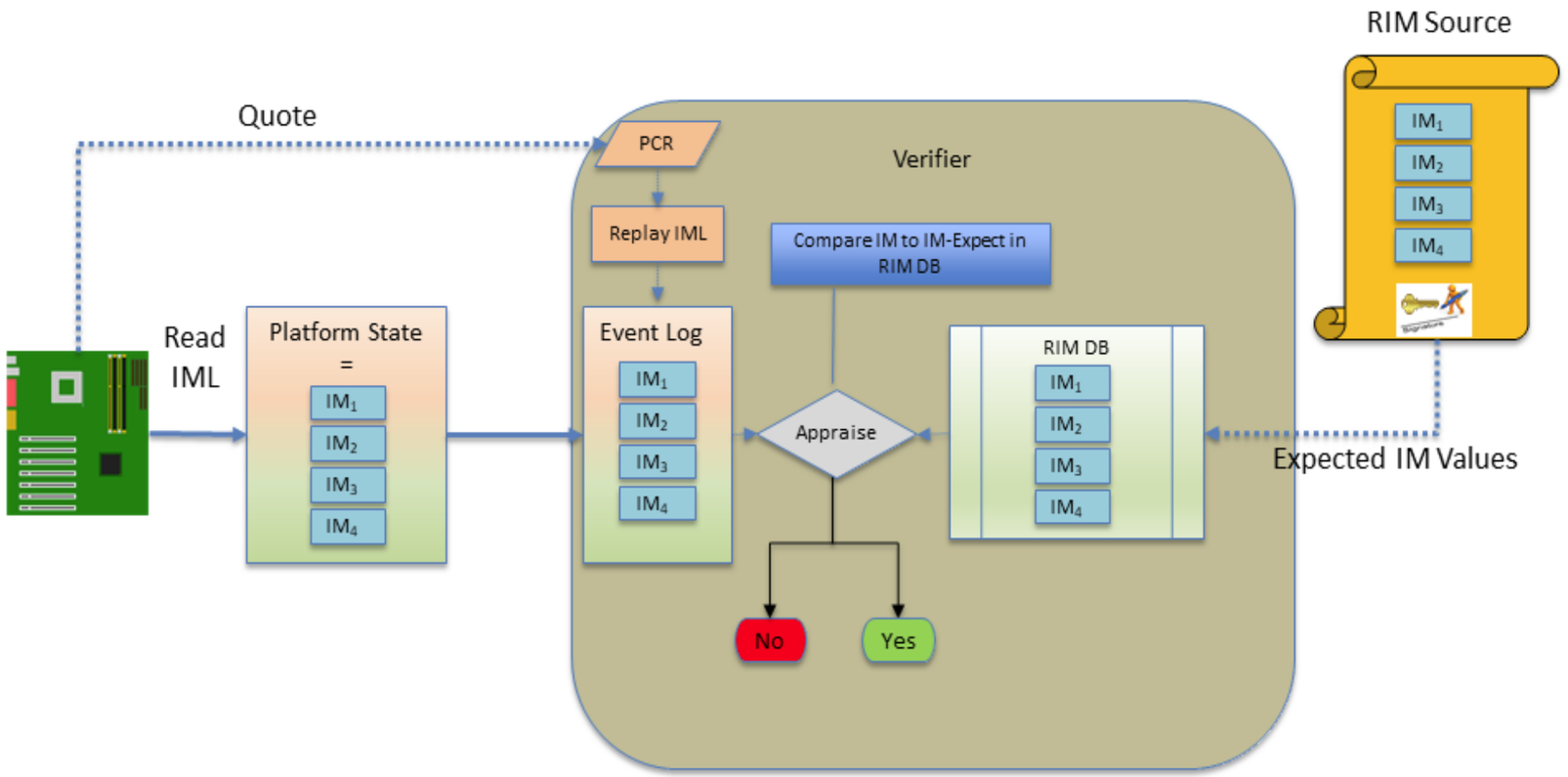
In addition to TCG, several other groups have taken up the challenge

- Internet Engineering Task Force (IETF)
- Distributed Management Task Force (DMTF)
- Open Compute Project (OCP)
- Fast Identity On-line (FIDO) Alliance
- World Wide Web Consortium (W3C)
- Global Platform

TCG Measured Boot Process



How Measurements Could be Verified



Many Levels of Complexity Appear

- Enterprises don’t just care about PCs and Servers
- What about BMCs, appliances, mobile devices, IoT (including resource constrained devices)?
- Many suppliers may need to provide integrity measurements (IMs)
- There may be many suppliers of input data in various formats
- There may be many verifiers who all need to get the same answer from the input data
- How will golden IMs be safely transmitted and validated?
- And others….

What is TCG Doing?

- The various TCG working groups have been busy developing specifications
- They have also been updating published specs to enable this model
- Their scope tends to be…
  - How do we measure a platform and attest to its code and configuration
  - How to encapsulate measurements and securely send them to a Verifier (Measurement Assessment Authority, a ‘MAA’ in 800-155 speak)
  - **NOT** what to do if a platform fails verification

Current TCG Specs and Status

TCG PC Client Platform Firmware Profile Specification Family 2.0 Level 00 Revision 1.05 (Draft for Public Review)

PC Client Work Group Specification

- This is the latest version of the PFP for PC Clients
- It provides:
    1. Usage of PCR registers in the Pre-Operating System state through the transition to OS-Present state
    2. How Platform Firmware, or a component thereof, contributes to the Root of Trust for Measurement (RTM) of the platform, specifically through extending digests (measurement) of code to a TPM based Platform Configuration Register (PCR) and documentation of that measurement in a log (event log)
    3. Behavior entering, during, and exiting power and initialization states
    4. Guidelines for Option ROMS

TCG Specs, Continued (Server PFP)

- Server Management Domain Firmware Profile Specification Rev 1.0 (Draft for Public Review)
- Server Working Group Specification
  - Similar purpose to the PC Client spec but targeting Server BMCs

TCG Specs, Continued (FIM)

TCG PC Client Platform Firmware Integrity Measurement Version 1.0 Revision 24 (Draft for Public Review)

PC Client Work Group Specification

- This is a new spec draft (driven from 800-155)
- It provides a framework for determining the configuration of PC Client platforms and what firmware has been run to initialize the system to a booted state

TCG Specs, Continued (RIM)

TCG Reference Integrity Manifest (RIM) Information Model Version 1.00 Revision 0.15 (Draft for Public Review)

Infrastructure Work Group Specification

- This is a new spec draft
- It provides:
  1. Definitions of structures that a Verifier uses to validate expected values (Assertions) against actual values (Evidence)
  2. An abstract structure for assembling reference measurements (Assertions) that manufacturers and other supply chain entities assert as expected values

TCG Specs, Continued (RIM)

TCG PC Client Reference Integrity Manifest Specification Version 0.15 (Draft for Public Review)

PC Client Work Group Specification

- This is a new spec draft
- It takes the generic RIM from the infrastructure group and makes it specific for PC Client platforms

TCG Specs, Continued

TCG Attestation Framework Version 1.0 (Pending draft release)

Attestation Working Group

- Defines an Attestation Architecture and the roles of the various actors involved and the data flows between them
- Tries to be a central reference for related terms
- An attestation architecture describes the creation, conveyance, and appraisal of attestation evidence

TCG Specs, Continued (TAP)

TCG Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0 (Published)

Trusted Network Communications (TNC) Work Group

- This is an existing Published Spec
- It provides:
  1. Definition of attestation evidence conveyed between an Attester and a Verifier
  2. It is communications protocol neutral

IETF Activities

RATS – Remote Attestation Procedures Working Group

Adopted:

- RATS Architecture - https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
- Entity Attestation Token (EAT) - https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
- A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs (CHARRA)
- https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/

Under consideration:

- Reference Interaction Models for Remote Attestation Procedures - https://datatracker.ietf.org/doc/draft-birkholz-rats-referenceinteraction-model/
- Trusted Path Routing using Remote Attestation - https://datatracker.ietf.org/doc/draft-voit-rats-trusted-path-routing/
- RESTful Attested Resources (REAR) - https://datatracker.ietf.org/doc/draft-shaw-rats-rear/
- Attestation Event Stream Subscription - https://datatracker.ietf.org/doc/draft-birkholz-rats-network-device-subscription/
- Time-based Uni-directional Attestation - https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/
- A CBOR Tag for Unprotected CWT Claims Sets - https://datatracker.ietf.org/doc/draft-birkholz-rats-uccs/
- A CWT Claims Set Definition for RATS Endorsement Tokens - https://datatracker.ietf.org/doc/draft-birkholz-rats-endorsement-eat/
- Reference Integrity Measurement Extension for Concise Software Identities - https://datatracker.ietf.org/doc/draft-birkholz-ratscoswid-rim/
- More…

Thanks to Ned Smith @ Intel and the TCG Attestation group

What's Next?

- Enterprise and government customers want this!
- The TCG continues to develop and update specs. Including specs for other platform types (servers, IoT, etc.)
- Many other groups are actively involved, this is a multi-faceted effort
- All parts of the UEFI Firmware supply chain need to pay attention (don't be blindsided)
- Many issues remain, i.e.
  - Some measurements are "brittle"
  - The creation, delivery and storage of "Golden Measurements" are not necessarily clear/complete, yet
  - What are the roles and responsibilities of "Verifiers"?
  - Many efforts underway are developing overlapping and uncoordinated standards. How will these be reconciled?
  - Etc., etc.

Call to Action

- Make sure you have engineering resources assigned to study the effects of this on your products
- Review the draft and published specs for their implications
- Consider participating with the TCG, and other groups, on the development of this technology

Questions?

Thanks for attending the UEFI 2020 Virtual Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by