REMOTE SOFTWARE INTEGRITY VERIFICATION USING TRUSTED COMPUTING GROUP TPM

Guy Fedorkow, Juniper Networks

Jessica Fitzgerald-McKay, USG

July 2019

V2b

Introduction

Remote software integrity verification is a mechanism that can be used to determine the authenticity of software installed on a fielded device such as a router or firewall.

This ppt outlines work submitted as:

- draft-fedorkow-rats-network-device-attestation-00

The work is based on Trusted Computing Group document:

- TCG Remote Integrity Verification: Network Equipment Remote Attestation System
- https://trustedcomputinggroup.org/wp-content/uploads/TCG-NetEq-Attestation-Workflow-Outline_v1r9b_pubrev.pdf

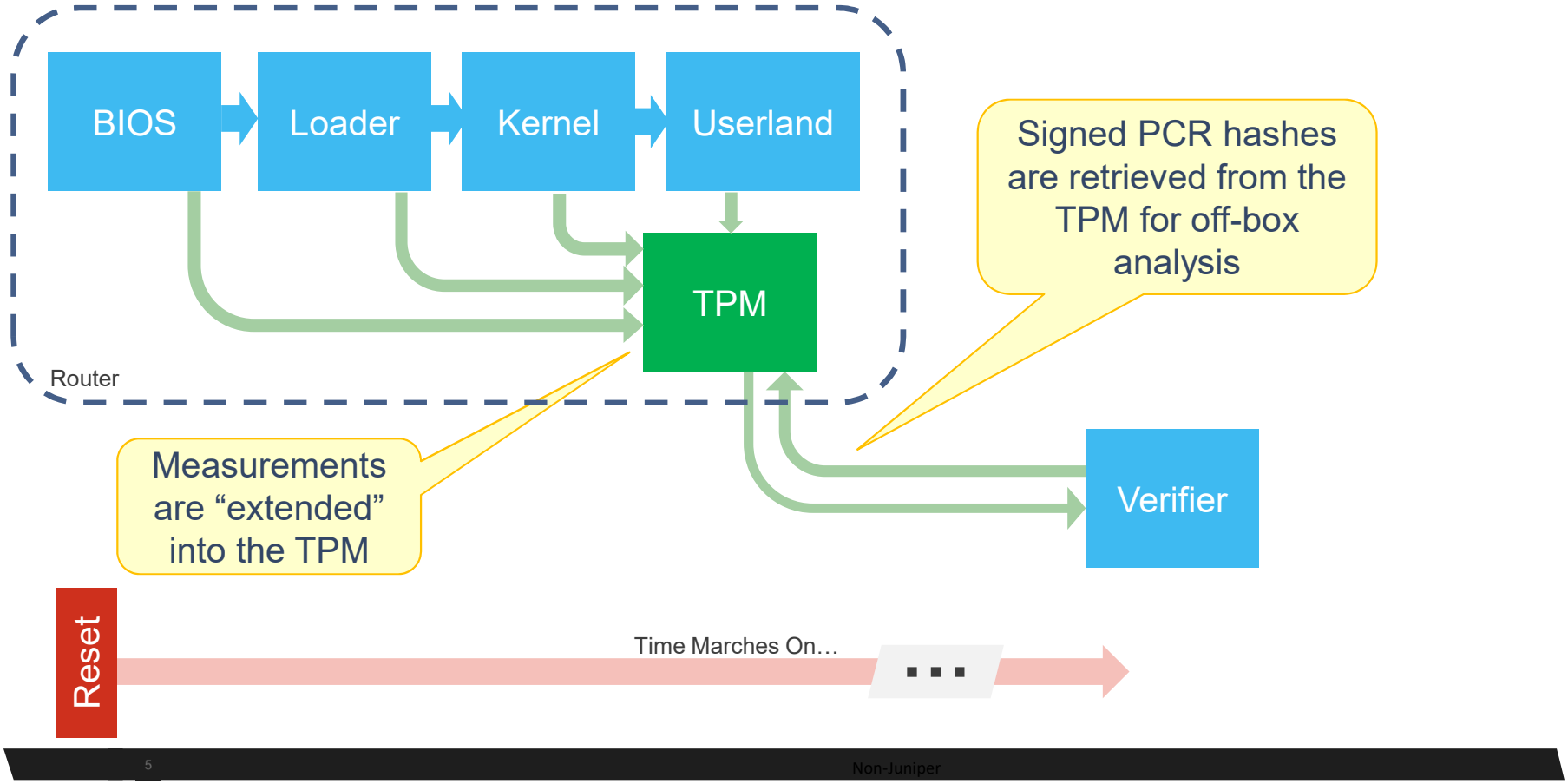
Agenda

- Attestation Technical Overview
- Relevant Documents

Problem Statement

- How do you know what software is actually running on a device?
  - You could ask it, but it might not tell the truth
  - Attestation (‘measured boot’) establishes a chain of trust where each link measures the next before it starts
  - The TPM reports the results, signed by a key known only by the TPM
- A workflow must be established where the entity that wants the validation may query the device in question via standard protocols.
- The workflow should be extensible to cover other use-cases with similar roots of trust.
  - But compatibility with existing TPM practice is critical

TCG Attestation Information Flow



RIV Information Flows

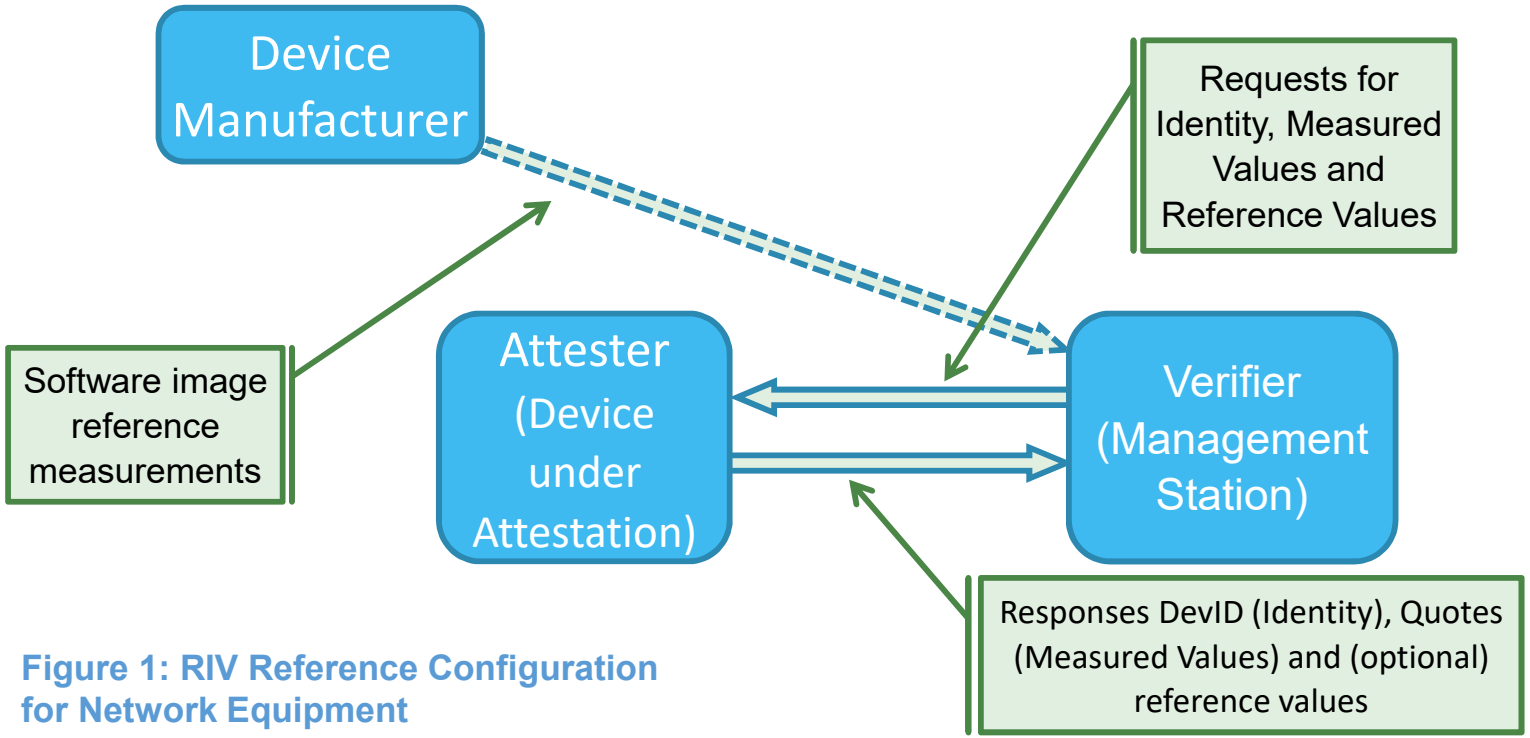


Figure 1: RIV Reference Configuration for Network Equipment

What's So Hard about This?

- Device Health Attestation is dependent on strong device identity
  - No point in attesting the state of a box if you don't know which one it is!
- It's inherently multivendor
  - A single vendor can collect the measurements, but to be useful, someone off-box has to ask for the results and evaluate them
- Software configurations are (almost) infinitely variable.
  - Determining if a chain of hashes is "good" or not is harder than "`if (a==b)`"
  - Common Multi-threaded OSs don't promise deterministic ordering, complicating hash chain analysis

RIV Protocol Summary

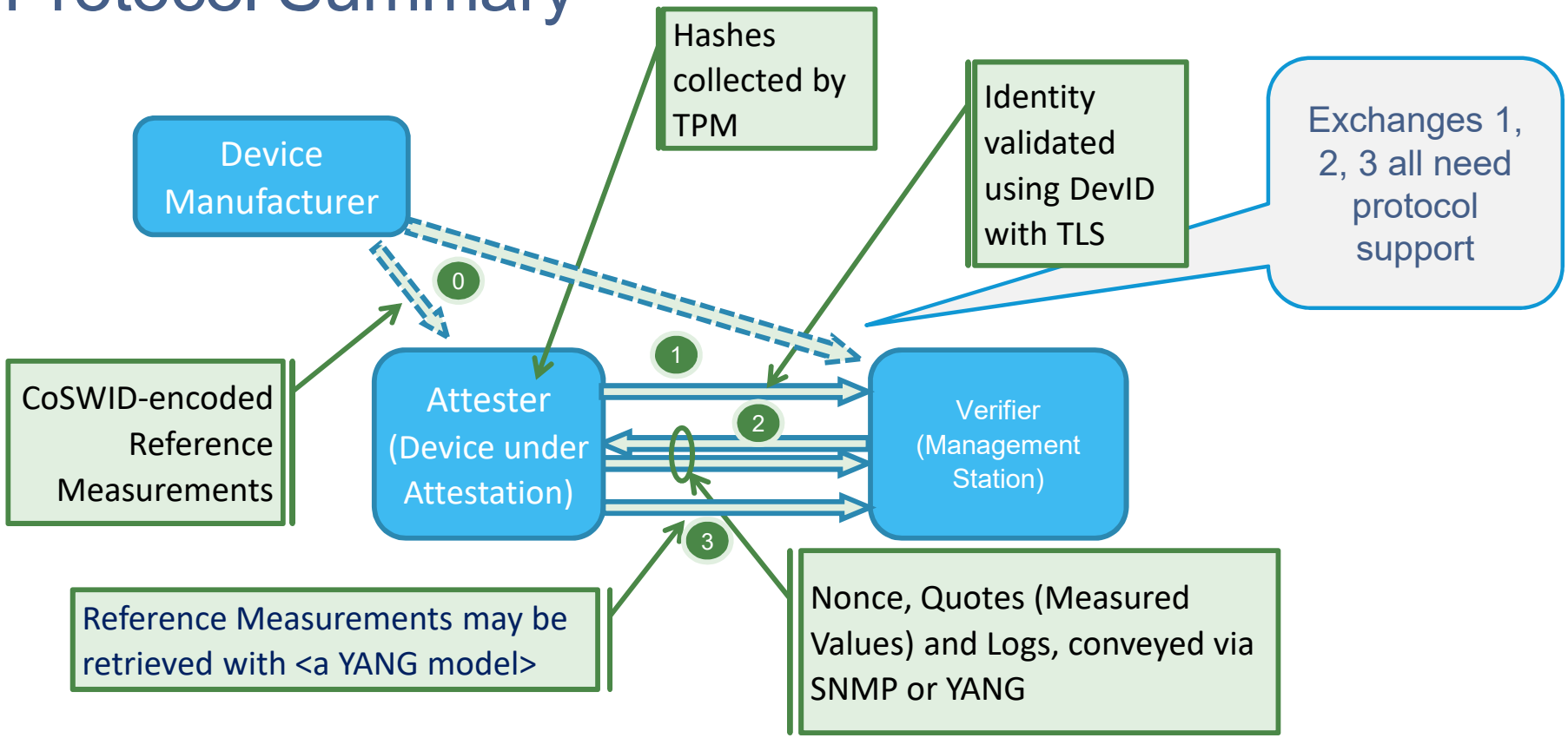


Figure 4: RIV Protocol and Encoding Summary

Remote Integrity Verification (RIV)

- Remote Attestation is a overloaded term with very broad scope
  - RIV provides a narrower scope to enable better focus
- Remote Integrity Verification (RIV) is our proposal for how Remote Attestation should be done with TCG technology
  - Focused on Network Equipment (for now)
    - We know the application well. Other embedded applications may follow
- We want to coordinate this work between TCG and IETF!

Agenda

- Attestation Technical Overview
- Relevant Documents

Participating Organizations

- Several organizations have documents relevant to attestation
  - IETF, TCG, IEEE, ISO, NIST, etc.
- TPM-related attestation docs are in TCG
- Protocol-related docs should be in IETF RATS WG

The RIV Protocol Stack

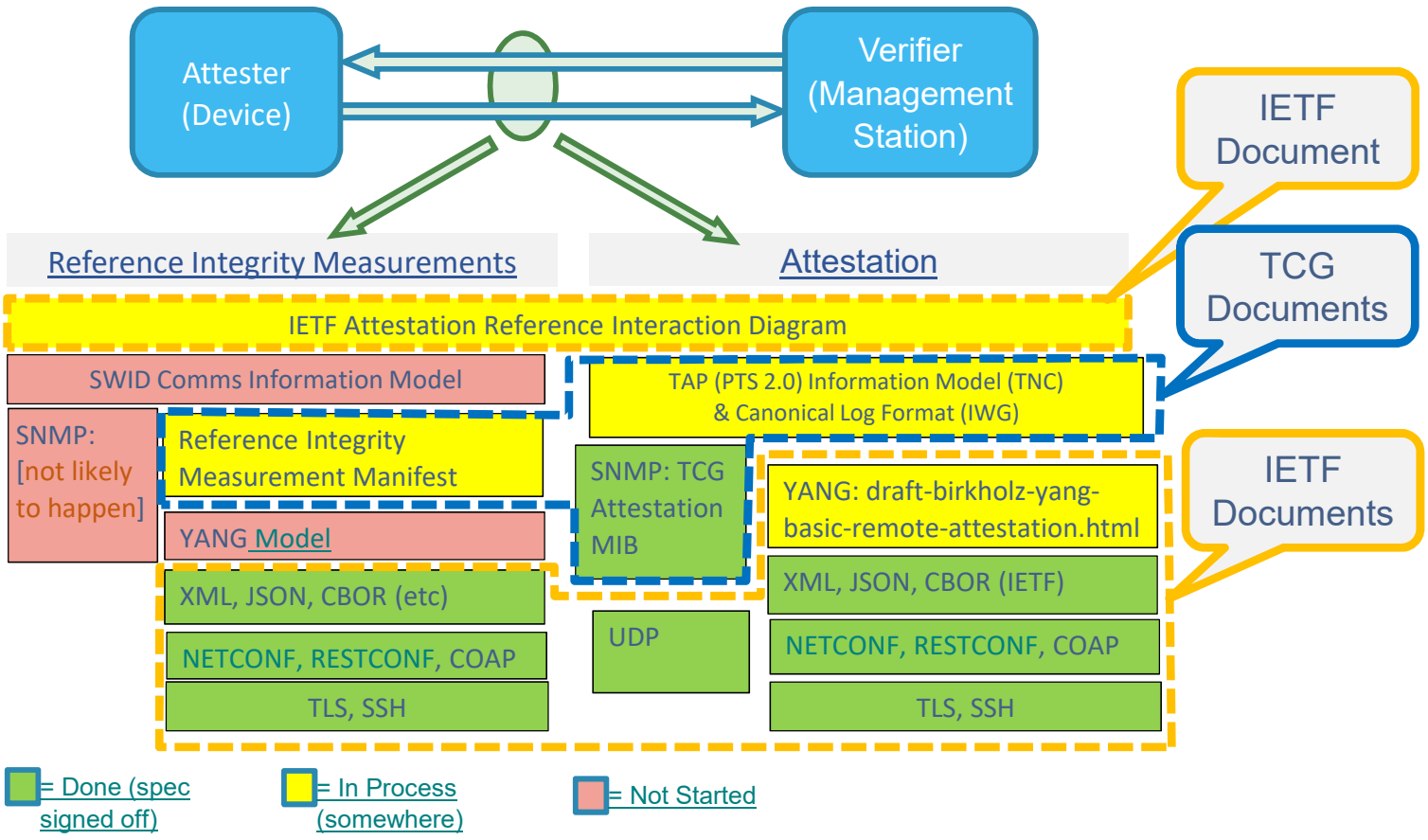


Figure 2: RIV Protocol Stacks

Status of TCG Docs for Attestation

Many TCG documents impinge on attestation:

4+	Done
6	In Process
1+	Not Started

= Done (spec signed off)

= In Process (somewhere)

= Not Started

TCG
TCG Trusted Attestation Protocol (TAP) Information Model for TPM Families 1.2 and 2.0 and DICE Family 1.0, October 30, 2018, DRAFT
SNMP MIB for TPM-Based Attestation, Specification Version 0.8, Revision 0.02, May 22, 2018, DRAFT
Canonical Event Log Format Version: 1.0, Revision: .12, October 16, 2018, DRAFT
TCG PC Client Specific Implementation Specification for Conventional BIOS, February 24th, 2012
TCG EFI Platform Specification For TPM Family 1.1 or 1.2, January 2014
TCG Reference Integrity Measurement Manifest DRAFT
TPM Keys for Platform DevID for TPM2, October 9, 2018, DRAFT
TCG Platform Attribute Credential Profile, Specification Version 1.0, DRAFT
TPM Keys for Platform Identity for TPM 1.2, August 2015, Published
PC Client Specific Platform Firmware Profile Specification Family “2.0”, Level 00 Revision 1.03 Version 51
SWID Comms Information Model

Next Steps

- We'd appreciate help in clarifying the workflow
- We'll add a Security Considerations section to outline mechanisms used to defend against attack
- We want to ensure that the RATS Use Cases cover RIV
  - Interoperability with existing TPM practice is critical

THANKS!

BACKUP

TCG vs IETF Process

	TCG	IETF
Charter	Confidential	Public
Doc Development	Confidential	Public
Initial Review	Confidential	Public
Public Review	Public	All Reviews are Public
Final Result	Public	Public

…So TCG must do a Public Review of the Attestation Workflow document in order to cooperate with IETF.