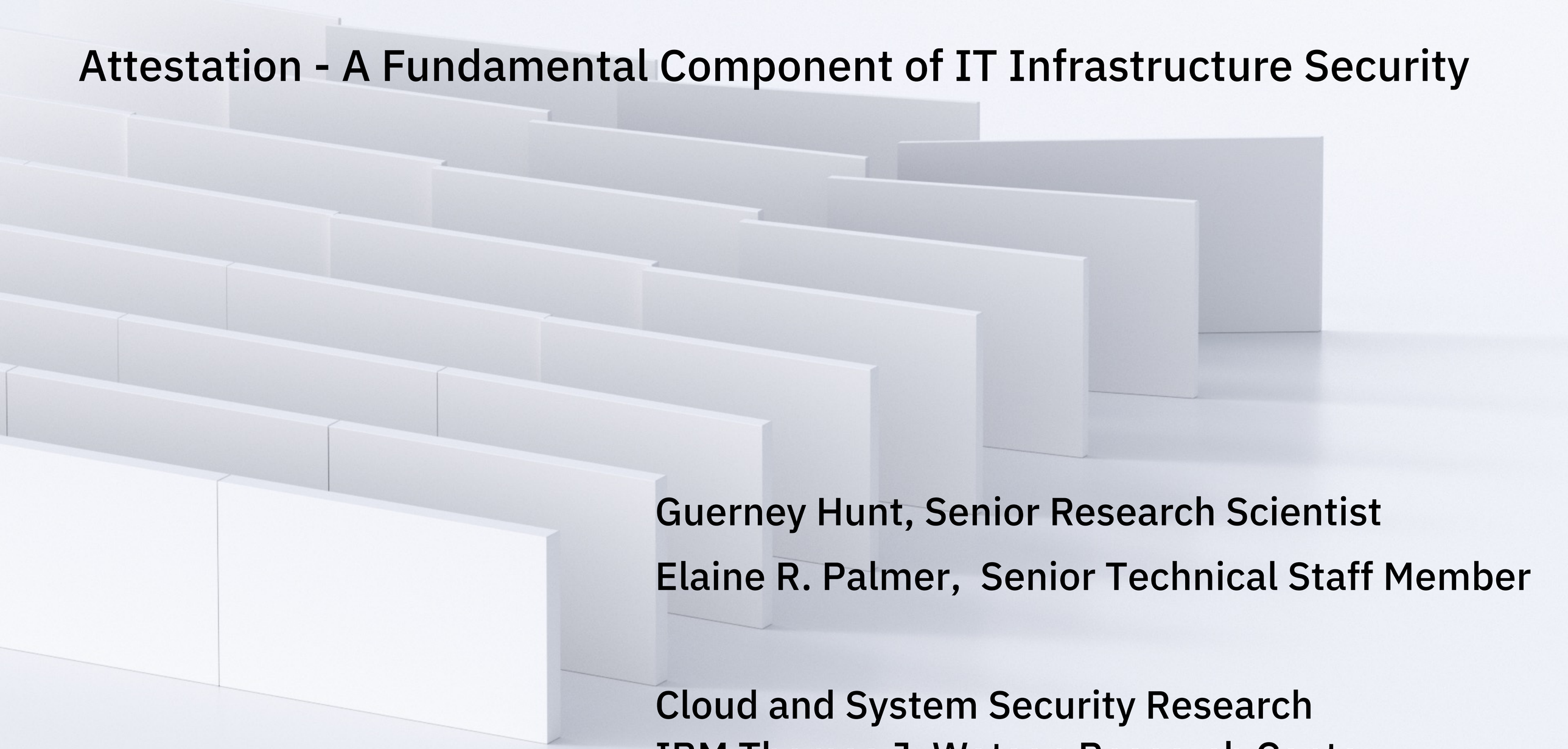
Attestation - A Fundamental Component of IT Infrastructure Security



Guerney Hunt, Senior Research Scientist

Elaine R. Palmer, Senior Technical Staff Member

Cloud and System Security Research
IBM Thomas J. Watson Research Center

IBM **Research**

IBM

Talk Outline

Terminology level set

Standards

Examples of attestation currently in use in IT infrastructure

Attestation

Generic
An **official** verification of something as true or authentic.

The process of attestation arises from the tradition of seeking independent verification of recorded events.

Computing
Attestation **allows a program to authenticate itself** and remote attestation is a means for one system to make reliable statements about the software it is running to another system. The remote party can then make authorization decisions based on that information.

Secure boot

Verified boot

Unique ID

Validated boot

Boot integrity

Measured boot

Trusted boot

Secure boot

Before you execute any file, verify the digital signature on it. . .

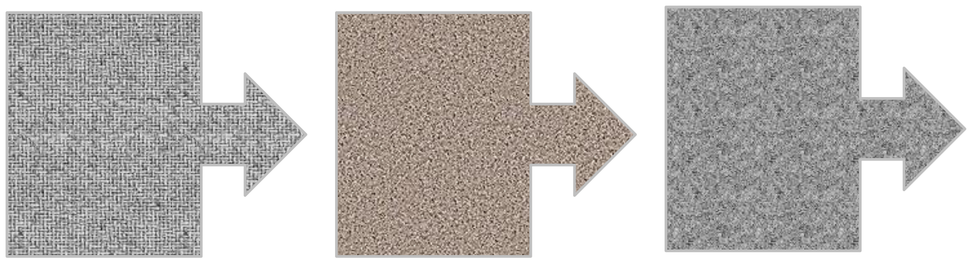
using the public key of the company you expected to sign it. . .

to make sure that nothing was modified after it was signed.

Measured boot

Before you execute anything, keep a record of it. . .

in a place that can’t be tampered with.



Unique ID

Each device has to have a unique secret that can be used to verify who/whose it is. This is often done by public key cryptography and certificates.

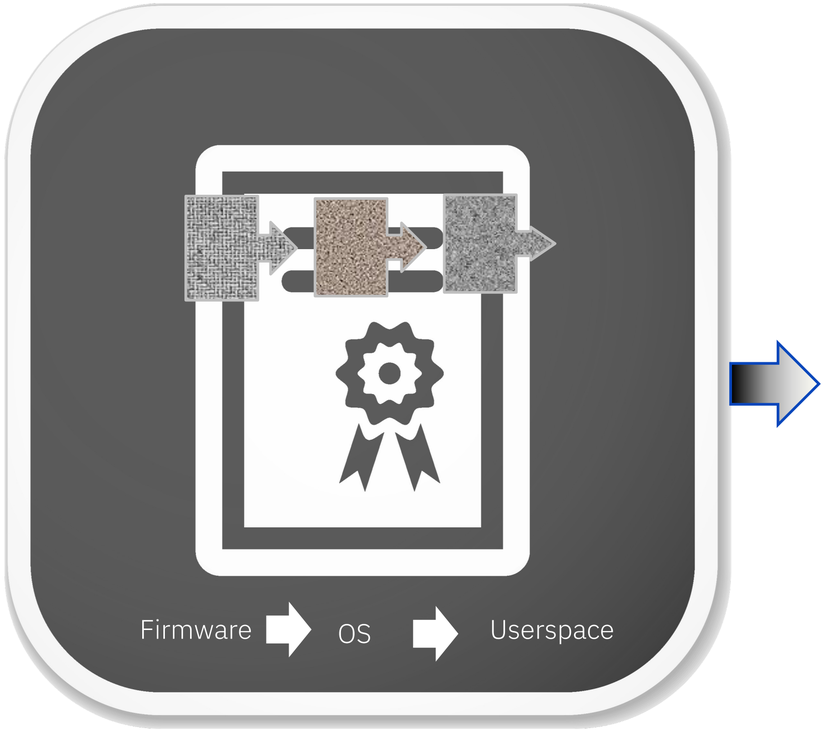
Without the ability to authenticate the signer, attestation is of no value.

Example: TPM has a certificate signed by the manufacturer I indicating it is a valid TPM. OEM places a certificate indicating this TPM is in their product.

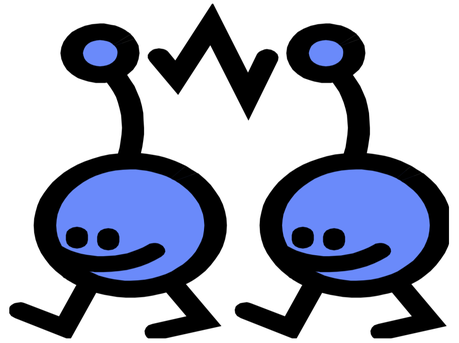
Signers of these certificates can be traced to a trusted source.

Attestation

Send out verifiable evidence of what was recorded.



How they work together



Secure Boot

“Without me, you can’t trust your measurements.”

Measured Boot + Attestation

“Without me, you might never know that you’re running an old copy of the OS.”

Authentication

“Without me, you do not know who you are talking to.”

Standards

Open Compute Project

Trusted Computing Group

DMTF Security Protocol and Data Model (SPDM)

Open Compute Project - the environment

In Cloud data centers, servers are filled with a plethora of devices (e.g., subsystems, peripherals, accelerators,. . .)

containing software, hardware, and firmware from multiple global suppliers.

To add to the complexity, those servers are typically configured on demand.

Until OCP’s Attestation specification,

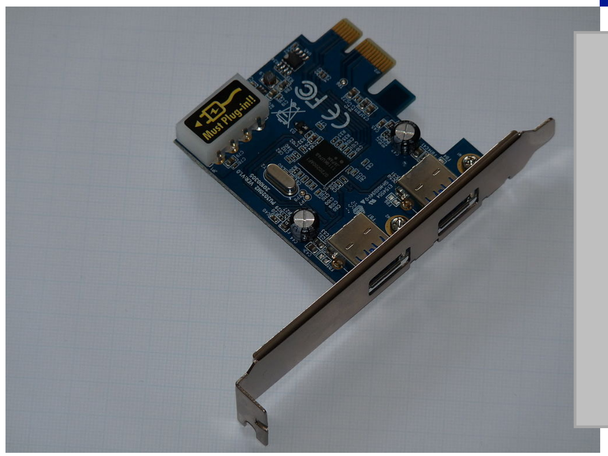
servers had no standardized, open,
and automated mechanism to

dynamically establish and verify trust in those devices.

Contract terms and conditions with trusted suppliers are necessary, but not sufficient.

Attestation Evidence

Device reports its “measurements” to server



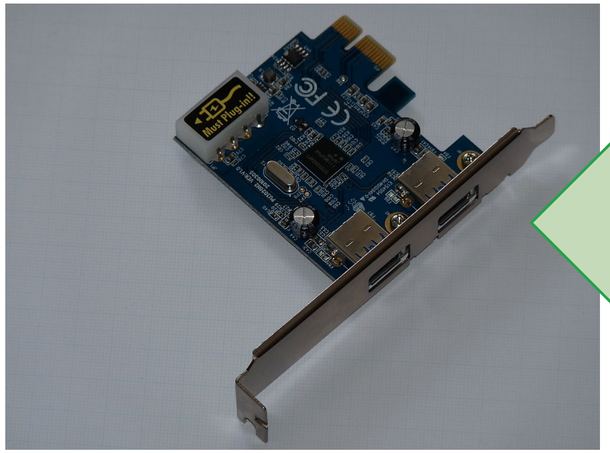
PCIe card with two USB_3.0 ports, 2013,
photo courtesy of Dmitry G under public domain

This is what I am.
This is who made me.
This is the firmware I’m running.
Can I come in?

Photo licensed under CC1.0

Attestation Verification

Server verifies device’s configuration



PCIe card with two USB_3.0 ports, 2013,
photo courtesy of Dmitry G under public domain

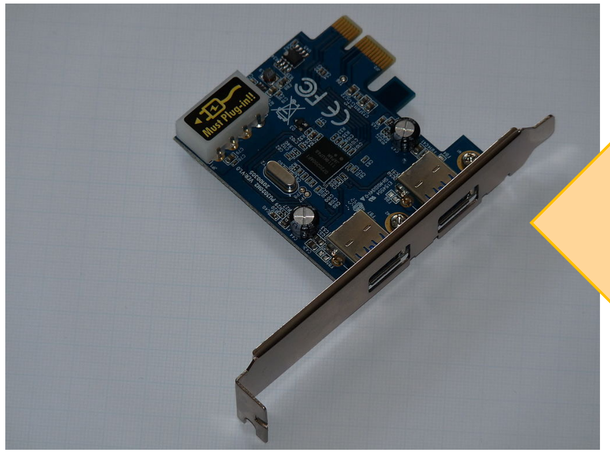
I expected you.
I trust your manufacturer.
You’re running the right firmware.
I’ll let you in.

Photo licensed under CC1.0

Or. . .

Attestation Verification

Server verifies device's configuration



PCIe card with two USB_3.0 ports, 2013,
photo courtesy of Dmitry G under public domain

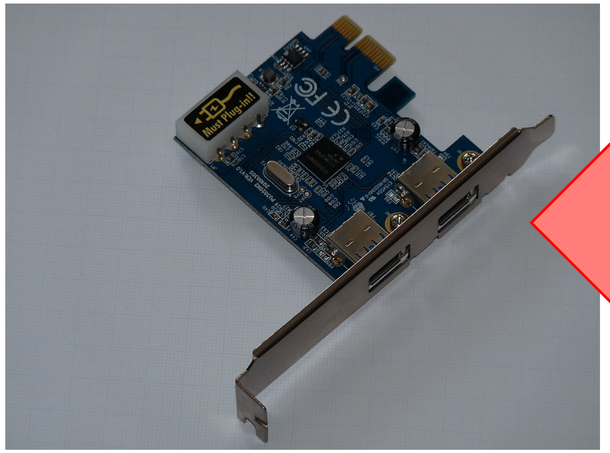
I expected you.
I trust your manufacturer.
You're running old, buggy firmware.
Try again when you're fixed.

Photo licensed under CC1.0

Or. . .

Attestation Verification

Server verifies device’s configuration

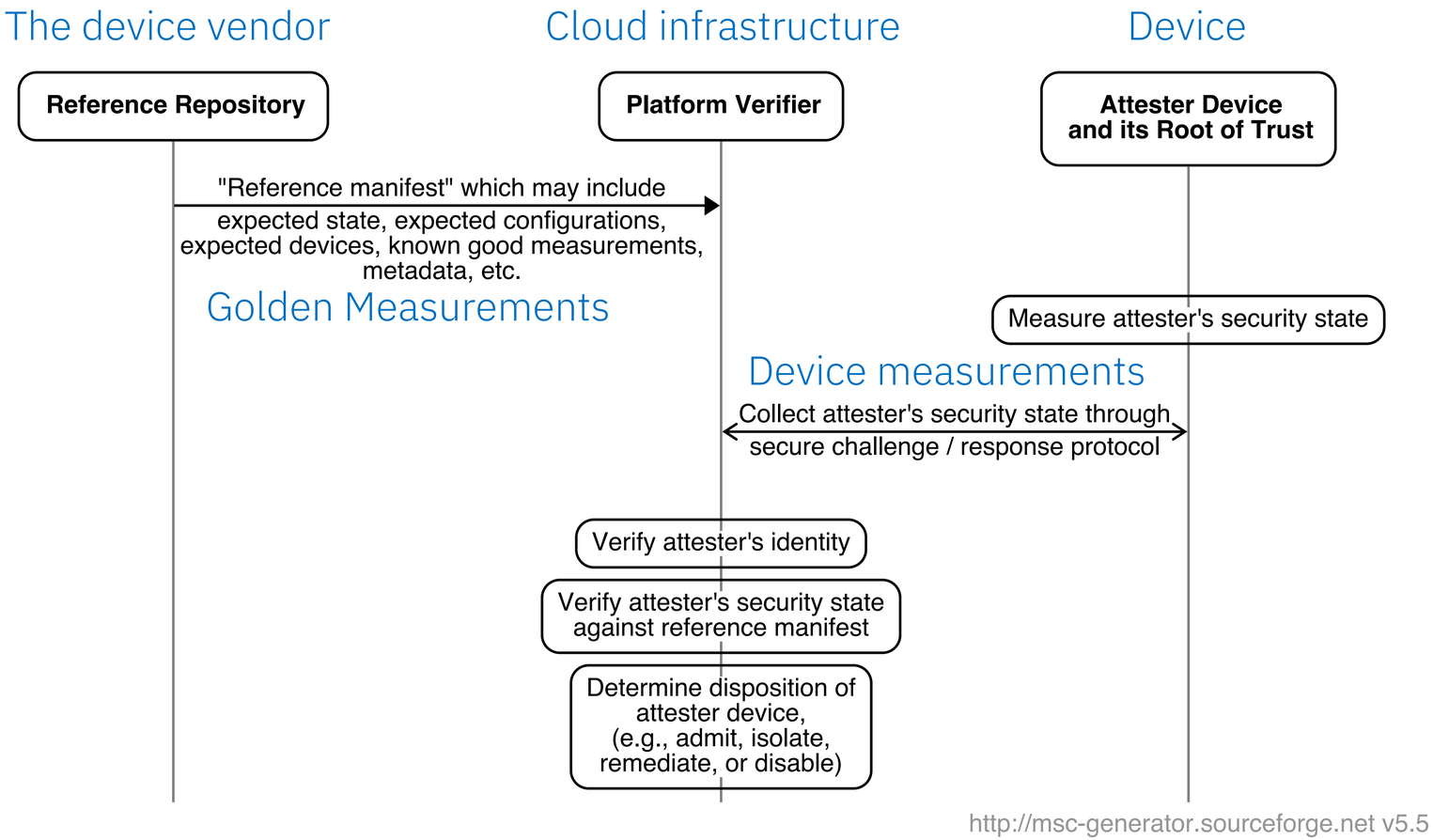


PCIe card with two USB_3.0 ports, 2013,
photo courtesy of Dmitry G under public domain

I don’t know anything about you.
You can’t come in.

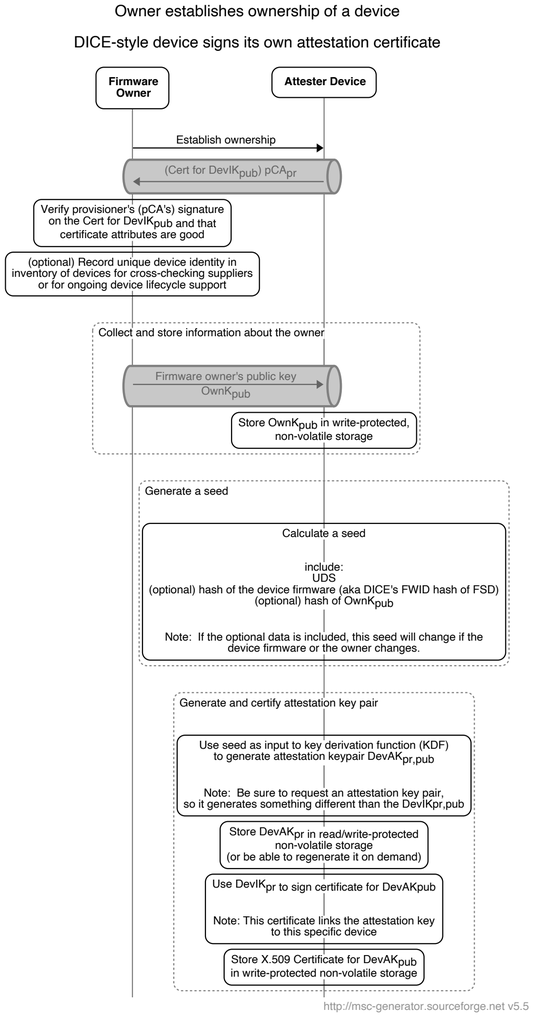
Photo licensed under CC1.0

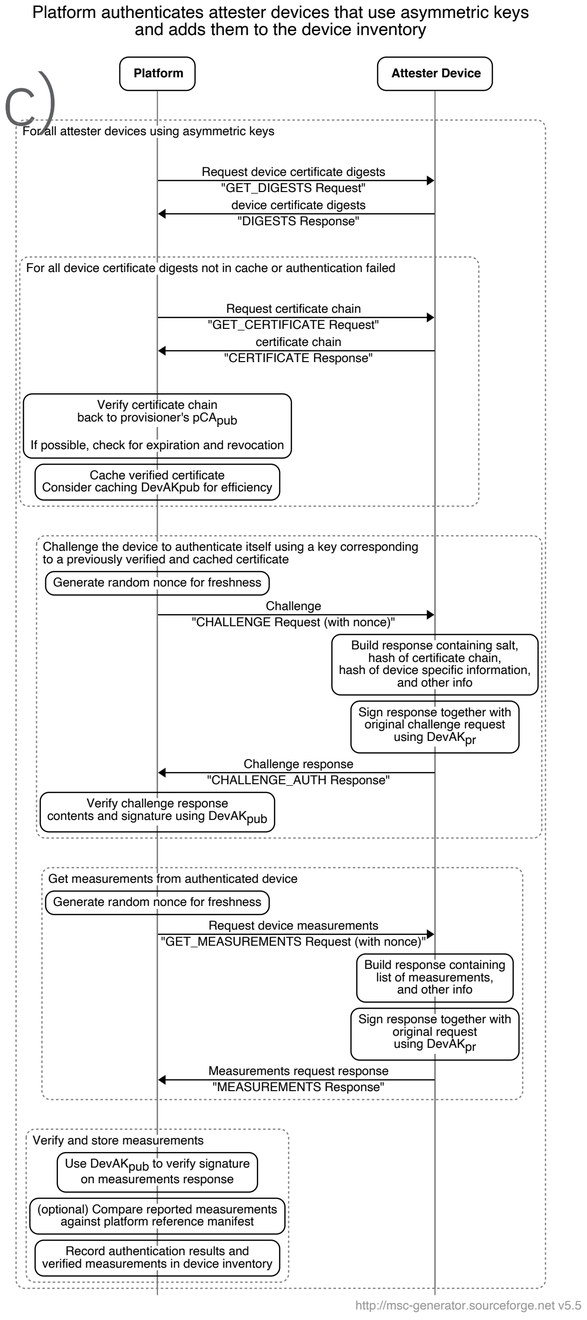
The ”big picture” protocol



Some steps (like a challenge) have been omitted for simplicity

Protocol eye tests (find them in the spec)





TCG

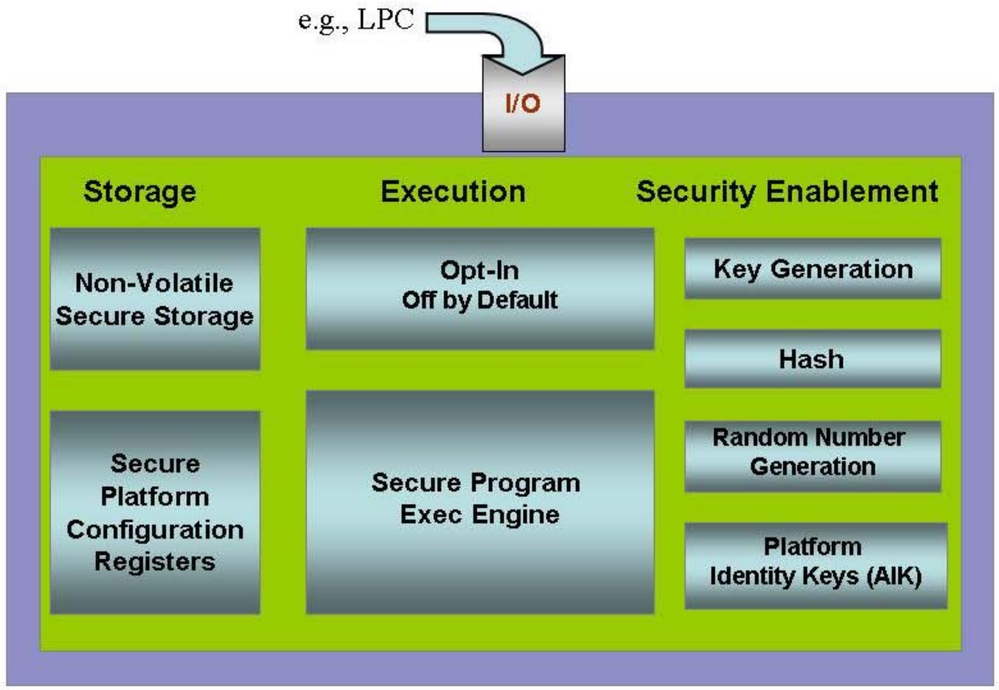
Laptops, Servers, Cloud data centers, HPC data centers contain a plethora of devices (e.g., subsystems, peripherals, accelerators,. . .) which contain software, hardware, and firmware from multiple global suppliers.

Defining protocols and hardware utilized as a basis for securing/identifying computing environments.

TPM

TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate a platform. These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.

A vTPM is a software-based representation of a physical Trusted Platform Module 2.0 chip.



Source: Trusted Computing Group: https://trustedcomputinggroup.org

DMTF: Securing links between host/devices and devices

Computer systems whether stand alone or cloud-based data centers, are filled with a plethora of devices (e.g., subsystems, peripherals, accelerators,. . .). These devices contain software, hardware, and firmware from multiple global suppliers.

All programmable components need to be authenticated and attested to assure the status of the system.

SPDM's Overall Goals

- All SPDM features fall into at least one of following main goals:
- Device Attestation and Authentication
  - The ability to attest various aspects of a device such as firmware integrity and device identity
- Secure Communication over any Transport
  - Provide the ability to secure communication of any data or management traffic over any transport
  - Work with industry partners to ensure data in-flight is secure for all parts of the infrastructure (e.g. storage, network fabrics, etc.)

All DMTF specifications are available at: https://www.dmtf.org/standards/published_documents

Source: www.dmtf.org

All SPDM features fall into at least one of the following **main goals**:

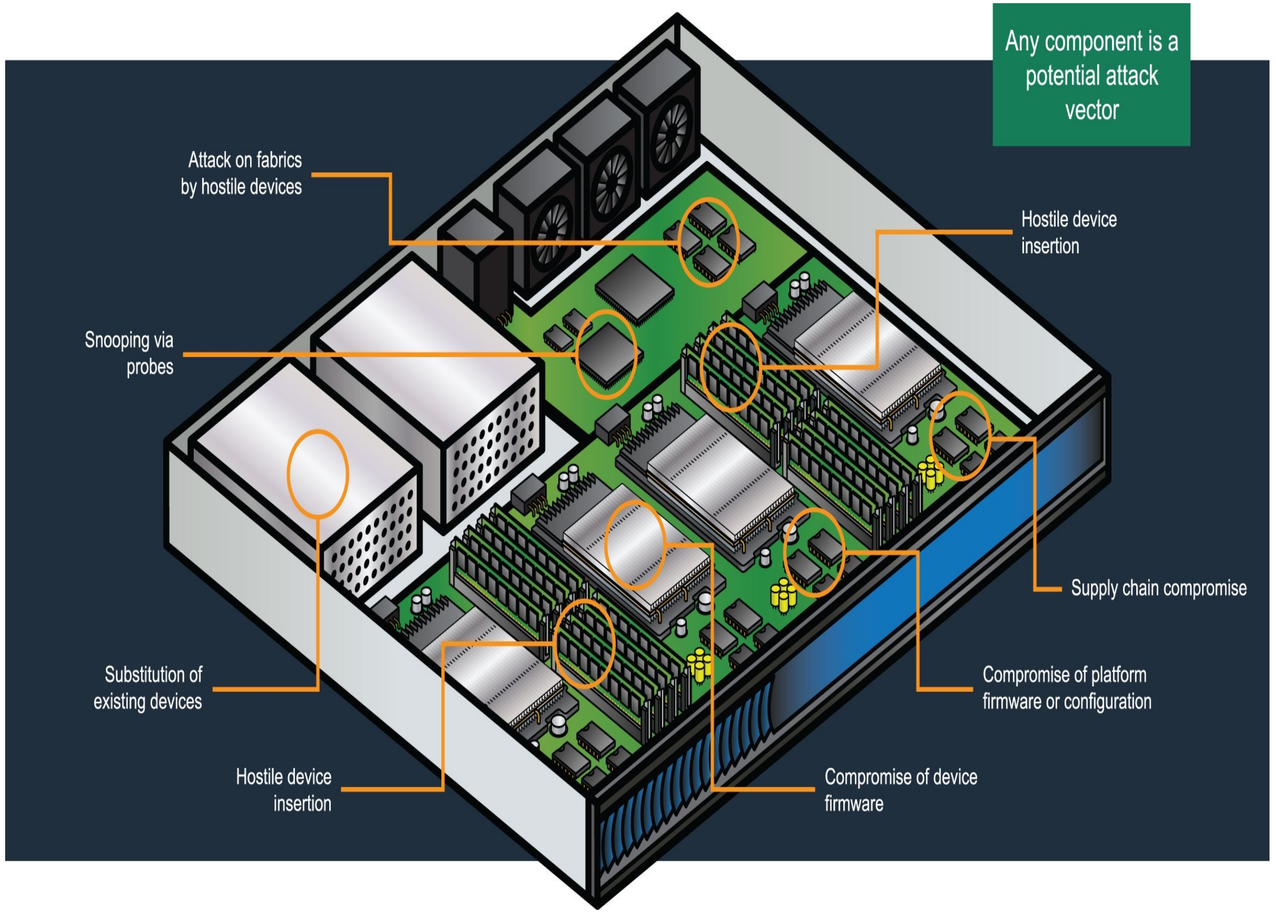
Device Attestation and Authentication

- The ability to attest various aspects of a device such as firmware integrity and device identity

Secure Communication over any Transport

- Provide the ability to secure communication of any data or management traffic over any transport

- Work with industry partners to ensure data in-flight is secure for all parts of the infrastructure (e.g., storage, network fabrics, etc.)



Source: www.dmtf.org

SPDM Feature Summary (2023)

Version 1.0: (22 December 2019)

- Measurement Support
- Device Attestation and Authentication

Version 1.1: (17 August 2020)

- Secure Session
  - Public Key Exchange
  - Symmetric Key Exchange
- Mutual Authentication

Version 1.2: (21 December 2021)

- Supports installation of certificates
- Allows for alias certificates derived from device certificates
- Send and receive large SPDM messages (chunks)
- Added SM2, SM3, SM4 algorithms to supported list
- New OIDs added
- Deprecated basic mutual authentication in CHALLENGE and CHALLENGE_AUTH

Source: www.dmtf.org

SPDM Feature Summary (2023)

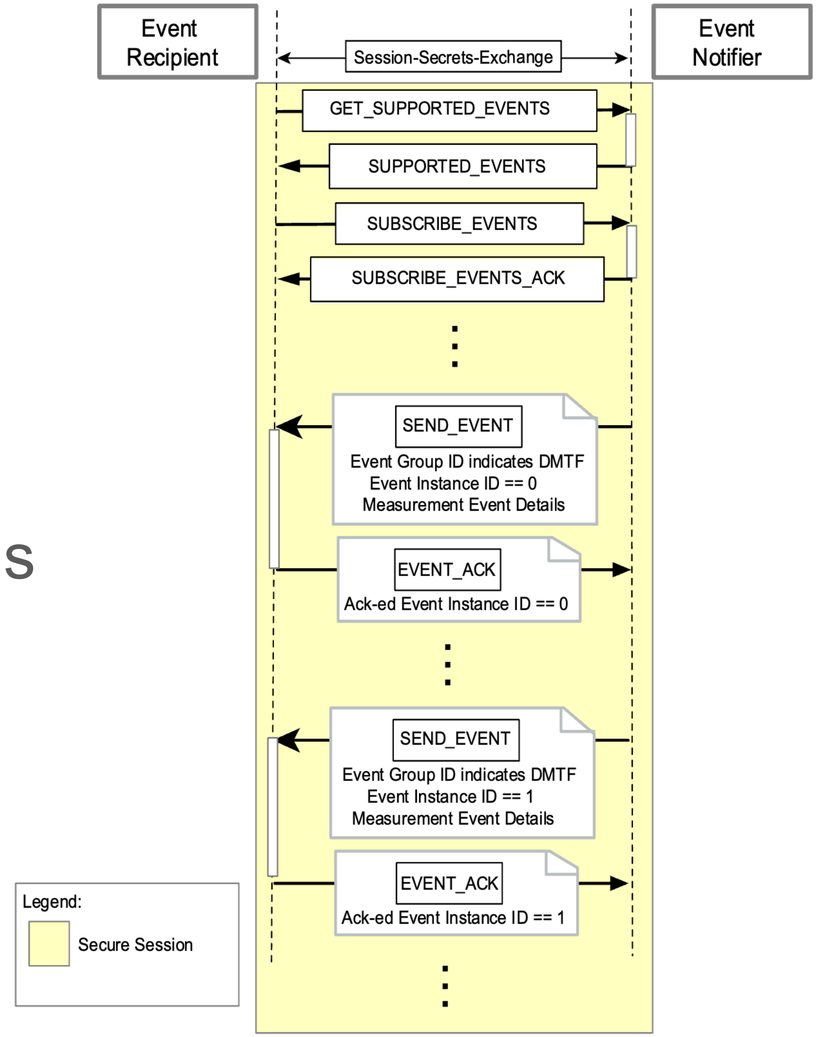
Version 1.3 (17 May 2023)

- Event Notification Mechanism
- Multi Key Support
- New Measurements
- Measurement Extension Log
- Structured Manifest format
- End Point Info

Source: www.dmtf.org

Event Mechanism

- Subscribed events
  - Interested Event Types
- All event notifications in a Secure Session
- Event Types could be extended by other standards bodies
- Can discovery supported event types and subscribe
- Notifications are ACK’d



Source: www.dmtf.org

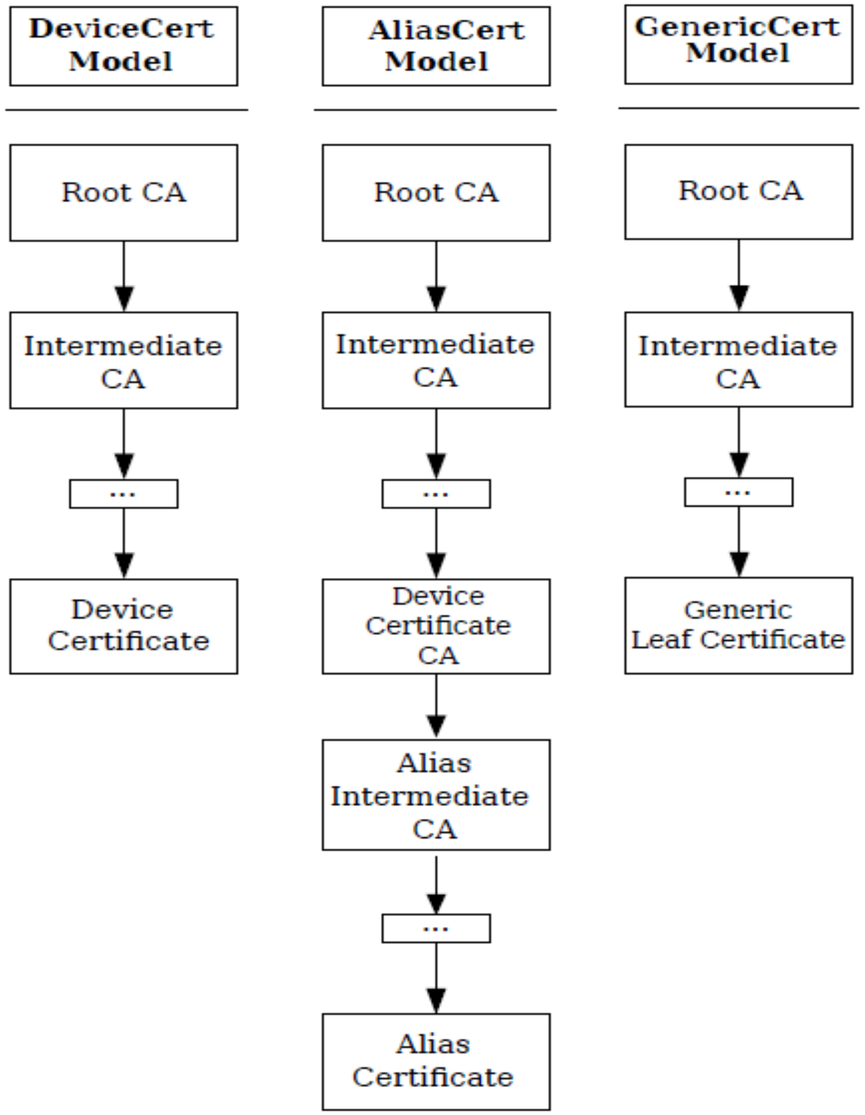
Multi Key Support

- Previous versions of SPDM only allowed one key pair per negotiated asymmetric algorithm
- Ability to use more than one key pair for a negotiated asymmetric algorithm
  - Up to 8 key pairs supported per asymmetric algorithm
- Every key pair could be dedicated for use case, like different key pairs for CHALLENGE and GET_MEASUREMENTS signature generations
- Requester is allowed to associate each key pair with an individual device certificate to enable one or more use cases
  - Multi Key Support enables additional use cases such as certificate provisioning in production or customer environments
  - Improved security posture
- Key pairs are identified by a unique KeyPairID

Source: www.dmtf.org

Generic Certificates Support

- What is a Generic Certificate or Certificate chain?
  - A Certificate or Certificate Chain that could not be qualified as a Device Certificate nor Alias Certificate
- New Feature
  - Generic Certificate model is introduced to support Multiple Asymmetric Keys use cases
  - Generic Certificate Model is the most flexible (or least restrictive) of the certificate models
  - Generic Certificate Model applies to certificates in slots greater than 0.
    - A Device or Alias Certificate is required in slot 0.



Source: www.dmtf.org

New Measurements

- `NewMeasurementRequested` field is introduced in the request attributes of the GET_MEASUREMENTS request.
  - If Responder has any changes affecting measurements that are requested by Requester but not yet applied (for example, pending changes due to a firmware update), then these new measurement values should be returned instead of current measurements (if requested using the value in the field above)
  - If there are no pending changes, then current measurements are returned regardless of the value in `NewMeasurementRequested` field
- This enables the Requester to prepare as well as to apply policy as per the system

Source: www.dmtf.org

Measurement Extension Log (MEL) and Hash-Extended Measurements (HEM)

- Responder may support reporting of measurements thru an “extend” scheme
  - Initialize HEM = HashSize bytes of 0s
  - For each extend operation, perform HEM = hash(Concatenate(HEM, DataToExtend)) for all data elements to extend
- The MEL is the collection of DataToExtend
  - Could include configuration measurements, firmware measurements, version number, etc.
  - The MEL may be preserved across resets
- An example of such a scheme is the Platform Configuration Register "extend" function in Trusted Platform Modules.
- There is a new MeasurementValueType 0x08 introduced for HEM

Source: www.dmtf.org

SPDM Summary

- SPDM protocol is a prominent industry standard for Component and Device Attestation
- Has traction among other industry standard organizations and among component and system vendors
  - DMTF plans to submit the SPDM specification to ISO for ratification
- DMTF seeks participation, collaboration and input from the industry and academia
- Use cases and specification work are expanding
- Ongoing work
  - SPDM over TCP/IP (SAS, SATA, and NVMe over fabrics) Binding
  - SPDM over Storage Binding
  - Authorization

Source: www.dmtf.org

Examples of attestation currently in use in IT infrastructure

IBM Cloud®

IBM Z®

IBM Power Systems®

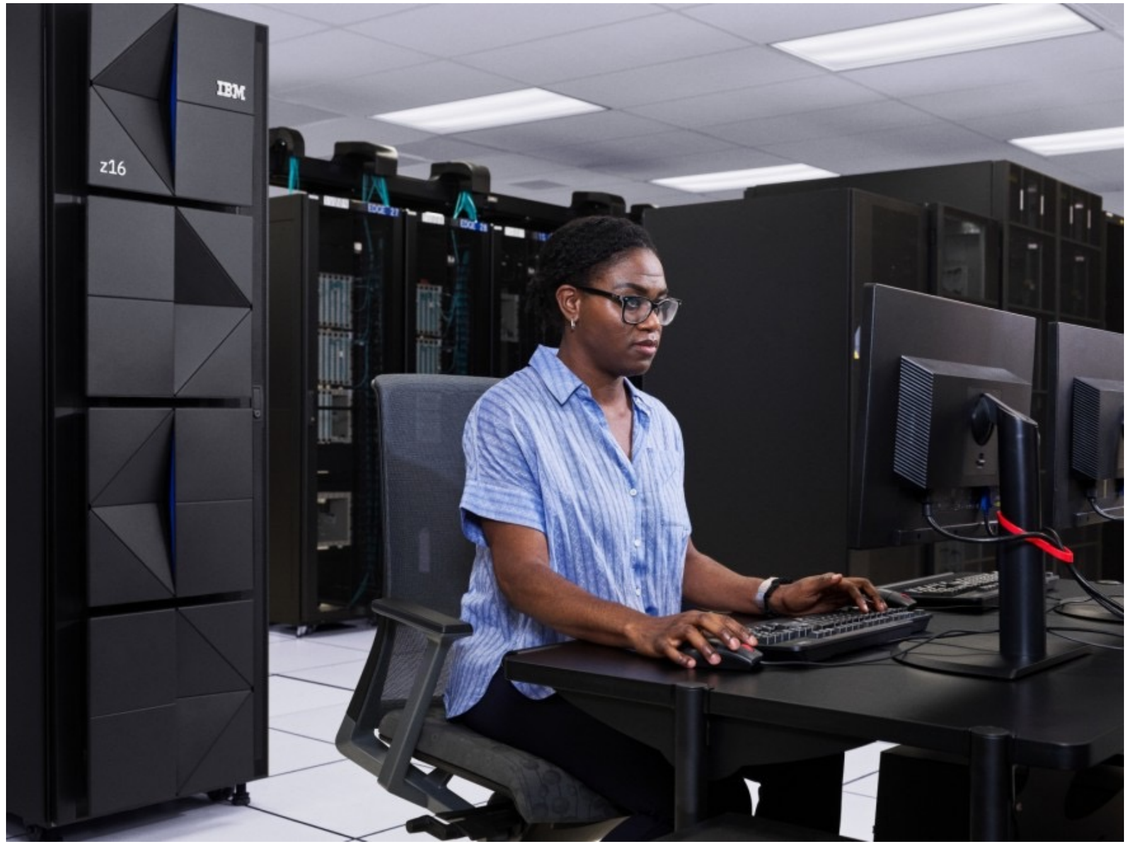
Microsoft Azure®

Google Cloud™

IBM, IBM Z, IBM Power Systems, and IBM Cloud are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.
Microsoft and Microsoft Azure are trademarks of Microsoft Corporation in the United States, other countries, or both.
Google Cloud is a trademark of Google LLC.

Since 2018

IBM Z®
Firmware Integrity Monitoring



Secure Boot

Builds on a hardware root of trust

Records measurements in Trusted Platform Modules (TPMs)

Verifies digital signatures prior to execution

Captures security logs for internal analysis

Call Home Service

Periodically requests measurements using a challenge and response protocol that prevents replay and other attacks

Captures console data, security logs, and local analysis data

Reports lack of responses or data

Trusted Third Party Validation

Verifies authenticity of responses and data using public keys registered during manufacturing

Compares measurements across multiple releases and expected configurations

Identifies configuration mismatches and suspected tampering

Continuous Monitoring

Extends integrity monitoring beyond boot time to run time

Continuously monitors firmware, operating system, and application executables and immutable files

Alerts Product Engineering and service support teams as needed

Microsoft Azure Attestation

Validates that a platform is trusted

Platforms can be

- Trusted Execution Environments (TEEs)
- Trusted Platform Modules (TPMs)
- Virtual Machines (VMs)
- Confidential VMs

Verifies that platforms satisfy default or customized policies before issuing tokens or releasing keys

Processes attestation evidence in multiple formats (e.g., TPM quotes and logs, ECDSA Attestation, and others)

Source: Microsoft Azure Attestation, https://azure.microsoft.com/en-us/products/azure-attestation/, retrieved 2023-11-07.

IBM Cloud

Firmware and Operating System Monitoring

- Keylime provides a highly scalable measured boot attestation and runtime integrity measurement solution.
  - TPM chip used for hardware root of trust
  - IMA Integrity Measurement Architecture
- All hardware must pass attestation prior to customer use.
- Attestation operated on a continual basis.
- Fulfills regulatory (FedRAMP, HITRUST) and customer requirements for a strong security posture.

Reference: Cloud Native Computing Foundation Blog

Google Cloud Boot Integrity (of the stack)

Relies on Titan, a hardware root of trust custom-designed by Google

Measurements from three layers (firmware, Operating System, and Userspace) are recorded by Titan.

Credentials allowing machines to participate in production operations are only released to machines with measurements proving that they booted the intended stack.

Additional version controls and revocation schemes are used

Source: How Google enforces boot integrity on production machines, https://cloud.google.com/docs/security/boot-integrity/, retrieved 2023-11-07.

Google Cloud Remote Attestation (of hardware components)

Relies on roots of trust for measurement (RTMs) in component devices within a machine (e.g., smart NIC, storage, memory controller)

Each device responds to challenges and requests to send its measurements for collection and forwarding.

Redfish is the preferred protocol.

A remote verifier uses a policy to verify signatures on the responses and compares the collection of responses to valid machine configurations.

Machines that fail aggregated attestation verification are identified for repair.

Those that pass are put into production service.

Source: Remote attestation of disaggregated machines, https://cloud.google.com/docs/security/remote-attestation, retrieved 2023-11-07.

IBM Power Systems

Firmware and Operating System Measurements

Secure and Trusted Boot

Builds on a hardware root of trust

Records measurements in Trusted Platform Modules (TPMs) and virtual TPMs (vTPMs)

Verifies digital signatures prior to execution

Maintains security logs

Measurements

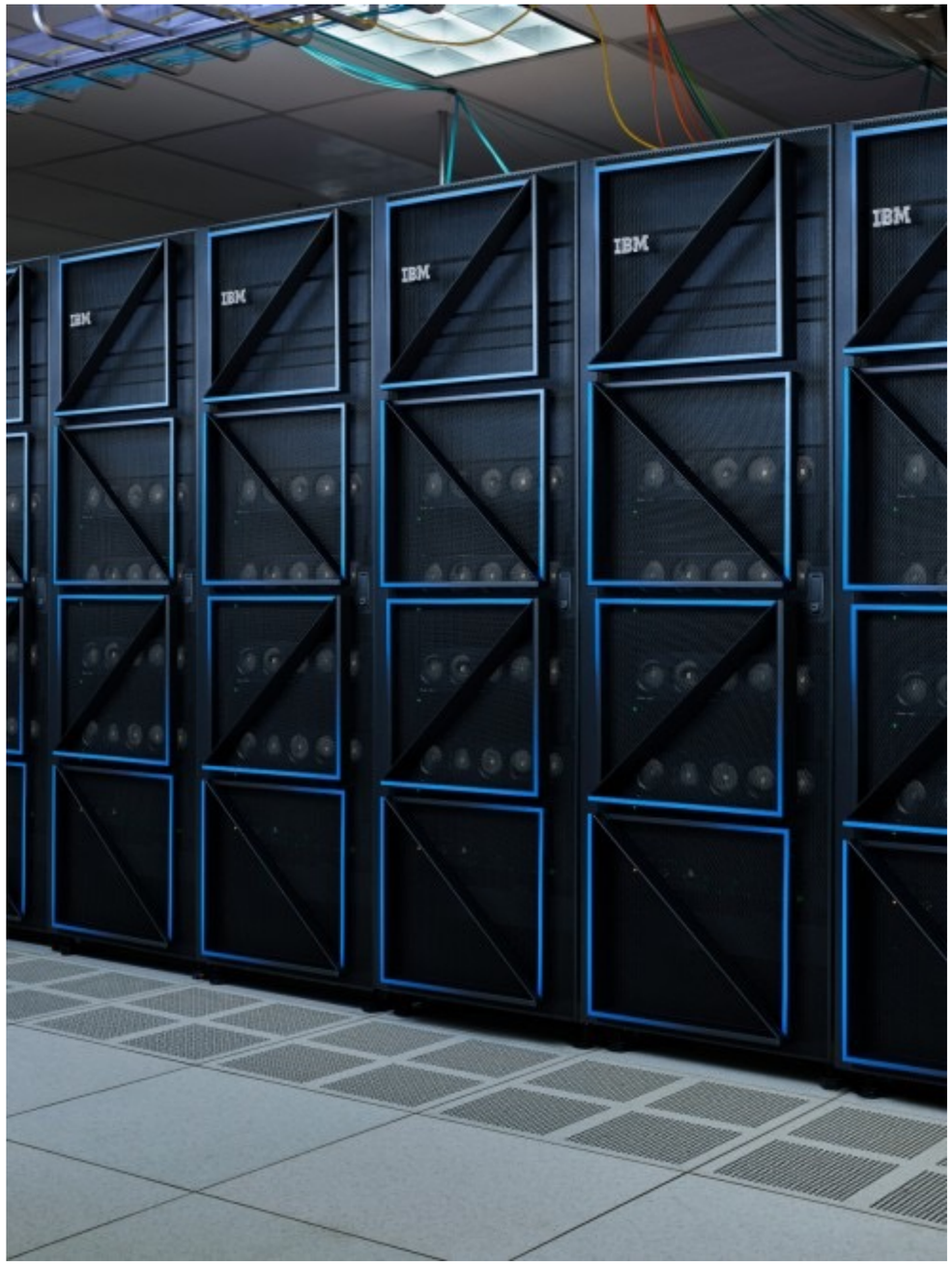
Begins at hardware root of trust measuring first mutable firmware

Each layer in the stack measures the next:

- System firmware
- Hypervisor
- Partition firmware

Continues with virtualization and measurements to vTPM:

- Partition firmware
- Operating Systems



Thank you

© 2023 International Business Machines Corporation

IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

THIS DOCUMENT IS DISTRIBUTED “AS IS” WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT, SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY.

Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

Not all offerings are available in every country in which IBM operates.

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.