Implementing Hardware Roots of Trust:
The Trusted Platform Module Comes of Age
Sponsored by the Trusted Computing Group (TCG)

Speakers: Gal Shpantzer, John Pescatore (SANS Institute)
Chris Hallum (Microsoft) and Stacy Cannady (Cisco Systems)

SANS INSTITUTE

Scope and Audience

- This webcast is primarily oriented toward CISOs and server / desktop / mobile security decision-makers.
- They need to respond to the higher end of the threat curve (both ongoing audit and intrusion), while addressing ongoing seismic shifts in IT.
- Trusted Platform Module (TPM) use cases include higher trust in confidentiality / integrity of handheld devices, desktop / server virtualization, cloud and consumerization of user devices.

Why is Hardware Root of Trust Needed? (1)

- A hardware root of trust can help with a variety of security issues, broadly divided into pre-boot and post-boot.
- In pre-boot, the TPM helps to secure the boot process against low-level malware and attest / measure integrity
- In post-boot, TPM can help with multiple use cases, such as root of trust for authentication and sensitive mobile apps like micropayments, as well as network layer security (Trusted Network Connect)

Why is Hardware Root of Trust Needed? (2)

- Malware can embed itself “below” the operating system (OS), where the software anti-malware packages run.
- This can be in the OS loader or in third-party boot drivers.
- One known example (in SANS’ view, the leading edge of such malware) is Mebromi, thought to be the first BIOS rootkit found in the wild, in 2011 (http://mason.gmu.edu/~msherif/isa564/fall11/projects/bios.pdf).

Do I Know You? Can I Trust You?

- **Two basic requirements for transacting business:**
  - **Do I know you?** A computer receives a network connection
    - What is the identity of the requesting computer?
    - What proof is there that the claim of identity is genuine?
  - **Can I trust you?**

How can these two computers establish whether either of them is operating as designed or that a compromise has occurred?

Identity alone is not enough for trust – what if one computer has been compromised with spyware?

What is the basis for a genuine claim of software integrity (or lack thereof)?

If you know the answers, you know whether to transact business or not

This is "Alice"

No HW-based identity to confirm it's Alice, so it isn't Alice.

NO DEAL

This is Alice, but my PC has spyware

HW-based identity check confirms it. The HW also states that Alice's computer is compromised.

NO DEAL

"The future is already here — it's just not evenly distributed." — William Gibson

- **$250 Chromebook from Samsung, with TPM for boot integrity of Chrome OS**
- **Hardware root of trust for cloud? CloudHSM is an HSM by SafeNet, deployed in Amazon Web Services (AWS), to:**

"**...***securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you.*"

AWS CloudHSM FAQ

SANS INSTITUTE

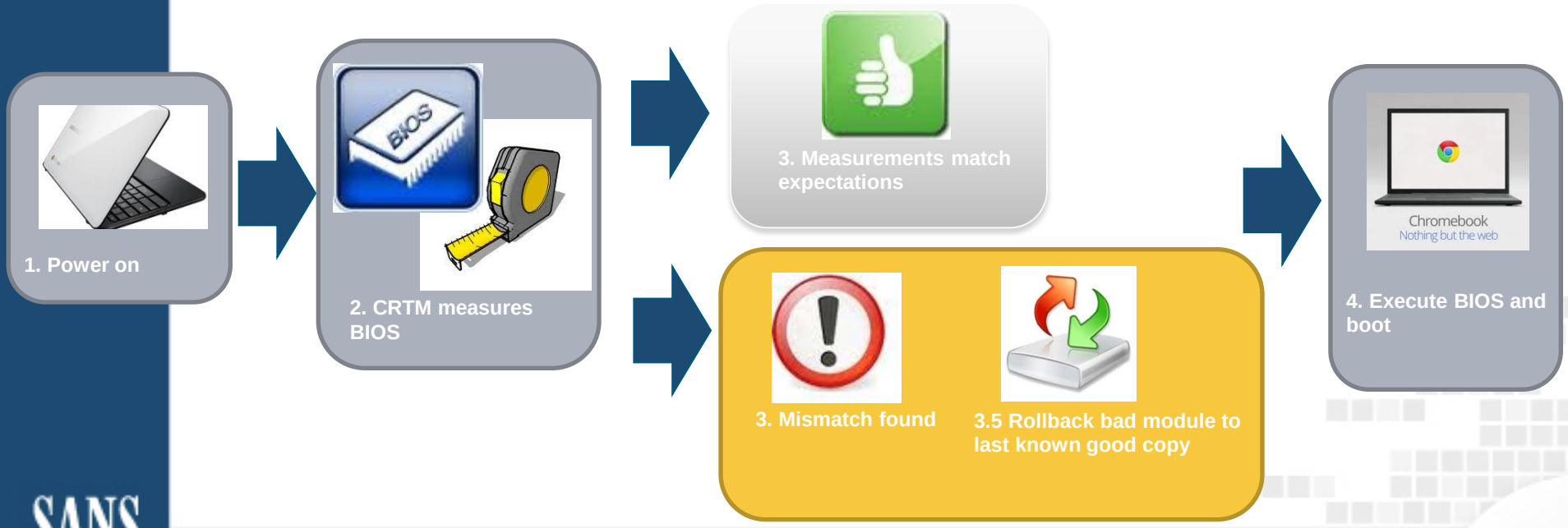
Chromebook Use of TPM

- "Google's Chromebook—A Self-Healing Computer"
- Power on, measure BIOS with HW security
- Decide go/no-go, based on measurement match/mismatch
- If match, proceed to execute BIOS and boot
- If mismatch, perform "rollback" to last known good copy
- This is in a $250 consumer device—available now.

Chromebook's Solution to "Can I Trust You?"

Chromebook uses TPM to find and correct corruption in firmware

1. TPM and Core Root of Trust for Measurement (CRTM) measure BIOS at boot
2. Measurements are internally verified
3. If a mismatch is found, the offending module is rolled back to the Last Known Good
4. Then boot continues



PWC's Solution to "Do I Know You?"

- **Requirement: Security hardware to protect a X.509 certificate for VPN log on**
  - Solution must be inexpensive and hassle-free
- **What PWC did:**
  - TPM-aware CSP installed under MS-CAPI in PWC PCs
  - PWC identity certs imported into MS-CAPI, under the TPM-aware CSP (TPM protects the cert)
  - User-entered PIN authorizes TPM to release cert for login to PWC networks

PWC and TPM for VPN authentication

- Chose the TPM route because it's an open standard with multiple vendor support
- TPM was already in 95% of PwC laptops
- Considered USB tokens and smartcards, passed on those due to cost of ownership (lost/stolen), not standards-based, didn't want additional device, etc.
- Already had software PKI in place but wanted hardware-based storage, due to threat of stolen keys
- Deployed 35,000 endpoints in 2010 (first public mention)

PwC and TPM for VPN authentication

- Gautam Muralidharan from PwC, about the TPM deployment, at a 2011 NSA conference
- "…the best kept secret in information security.
- It is a well defined Open Standard and has low costs to deploy
- The only universal security device in different brands of PCs that worked for us."

- https://www.ncsi.com/nsatc11/presentations/tuesday/real_world/muralidharan.pdf

CloudHSM in AWS (SafeNet)

- EAL4+ HSM in a VPC on AWS
- Hardware root of trust for cryptographic operations
- Tamper-resistant, secure key management, reduces latency compared to off-cloud HSM
- Increases security compared with software-based key management
- $5,000 per device, plus usage fees

Taking Advantage of Ubiquity

- Hardware self-encrypting drives (SEDs) for notebooks/servers
- Hardware Trusted Platform Module (TPM) in tablets/notebooks/servers
- Virtual TPMs in phones/tablets
- HSMs in cloud
- You probably already own a lot of hardware with a TPM in it.
- If not, look at specifying TPMs in upgrade cycles and planning for use cases that include TPM.

Standards-Based, Vendor- and Community-Supported

TCG is an open standards organization, supported by hardware and software vendors including:

- AMD, ARM, Intel & NVIDIA (CPU & GPU)
- Gemalto, Infineon Technologies & Phoenix (BIOS & security hardware)
- NetApp, Oracle, Seagate & Western Digital (Storage)
- Dell, HP, IBM, Lenovo & Sony (Notebooks/Servers)
- Nokia, Panasonic & Samsung (Mobile)
- Juniper & Cisco (Network)
- Microsoft & Red Hat (OS, major closed/open source)
- Absolute, McAfee, Wave Systems, WinMagic, Credant, Cryptomill, Softex (Management)

Standards-Based, Vendor and Community Supported

- TPM specification version 1.2 is published as ISO/IEC 11889 Parts 1-4.
- The concept of the hardware root of trust is supported by the National Security Agency (NSA) High Assurance Platform (HAP).
- NSA's HAP is based on Embedded Security Module (ESM). *"At boot time and at runtime, a HAP device measures software in a trusted manner before that software is allowed to execute."*

- *Source: http://www.nsa.gov/ia/_files/HAP_Brochure.pdf*

Standards-based, Vendor and Community Supported

The National Institute of Standards and Technology (NIST) has issued several special publications on trust, including firmware/BIOS security and hardware root of trust (SP-800-147, 155 and 164).

From SP-164:

"Hardware RoTs are preferred over software RoTs due to their immutability, smaller attack surfaces and more reliable behavior. They can provide a higher degree of assurance that they can be relied upon to perform their trusted function or functions."

NIST on Hardware Roots of Trust for Mobile Security

NIST enumerates hardware roots of trust (or "trusted software," perhaps virtual TPM) for:

Storage of cryptographic keys and 'critical security parameters'

-"...*to verify digital signatures associated with software/firmware and create assertions based on the result*"

-Integrity "*through the use and maintenance of tamper evident locations for the purpose of securely storing measurements and assertions...* such as the TPM method for extending Platform Configuration Registers, PCRs)"

NIST on Hardware Roots of Trust for Mobile Security (Continued)

NIST enumerates hardware (or "trusted software") roots of trust for:

-Reporting "to manage identities and sign assertions for the purposes of generating device integrity reports. It has the capability to reliably cryptographically bind an entity to the information it provides…" ←Relies on Measurement and Integrity.

-Measurement "has the capability to make inherently reliable integrity measurements and is the root of the chain of transitive trust for subsequent measurement agents." <-- Integrity and Reporting roots of trust use the Measurement facility

NIST on Hardware Roots of Trust for Mobile Security (Continued)

"The key point is that mobile devices need to implement the security capabilities and services defined above in trustworthy hardware, firmware and software components."

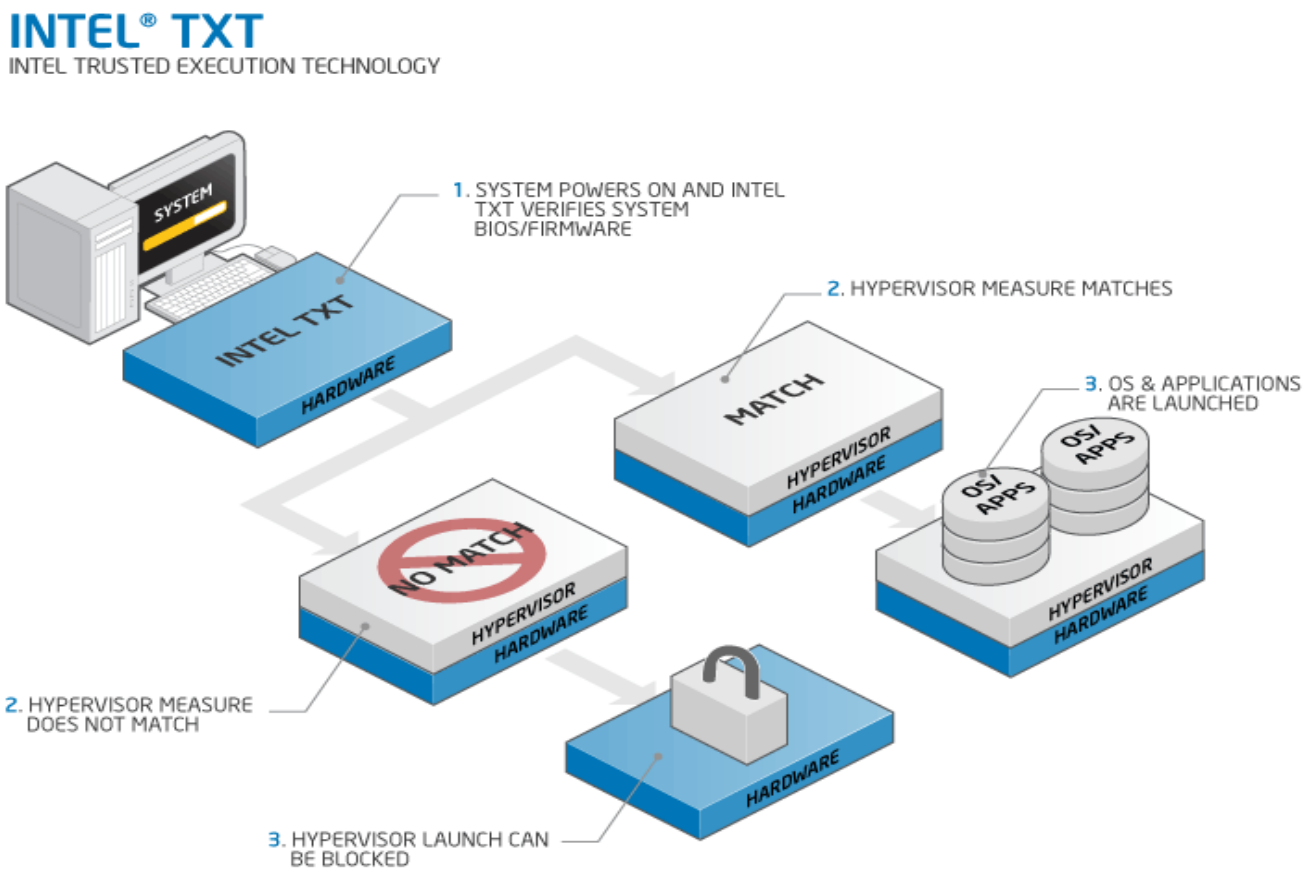
Note that the TPM concept can be implemented in any of those ways. Today we have dedicated "hard" TPM chips, but also virtual TPMs inside processors.

NIST SP-800-164

Virtualization (Server)

- Intel Trusted Execution Technology (TXT) uses hardware binding for VMs spinning up. Requires a TPM.
- Example use case: Geofencing for regulatory compliance.
- VMs can't spin up unless run on specific hardware, which is easier to locate than a VM.

Intel TXT



Virtualization (SecureView Desktop)

- SecureView is an Air Force Research Lab (AFRL) project with industry, to create secure multi-level workstations (Unclassified up to TS on same machine).
- TPM is included as part of the unlock mechanism for multiple encrypted virtual machines (VMs), each at its own level.

Virtualization (SecureView Desktop) Measured Launch for XenClient

"• Verify Xen Client installation integrity, prevent offline tampering of installation or configuration state

• Measured Launch

– Intel TXT used to establish DRTM, measure Xen Client primary components on every boot

– Extend measurements to include secondary components

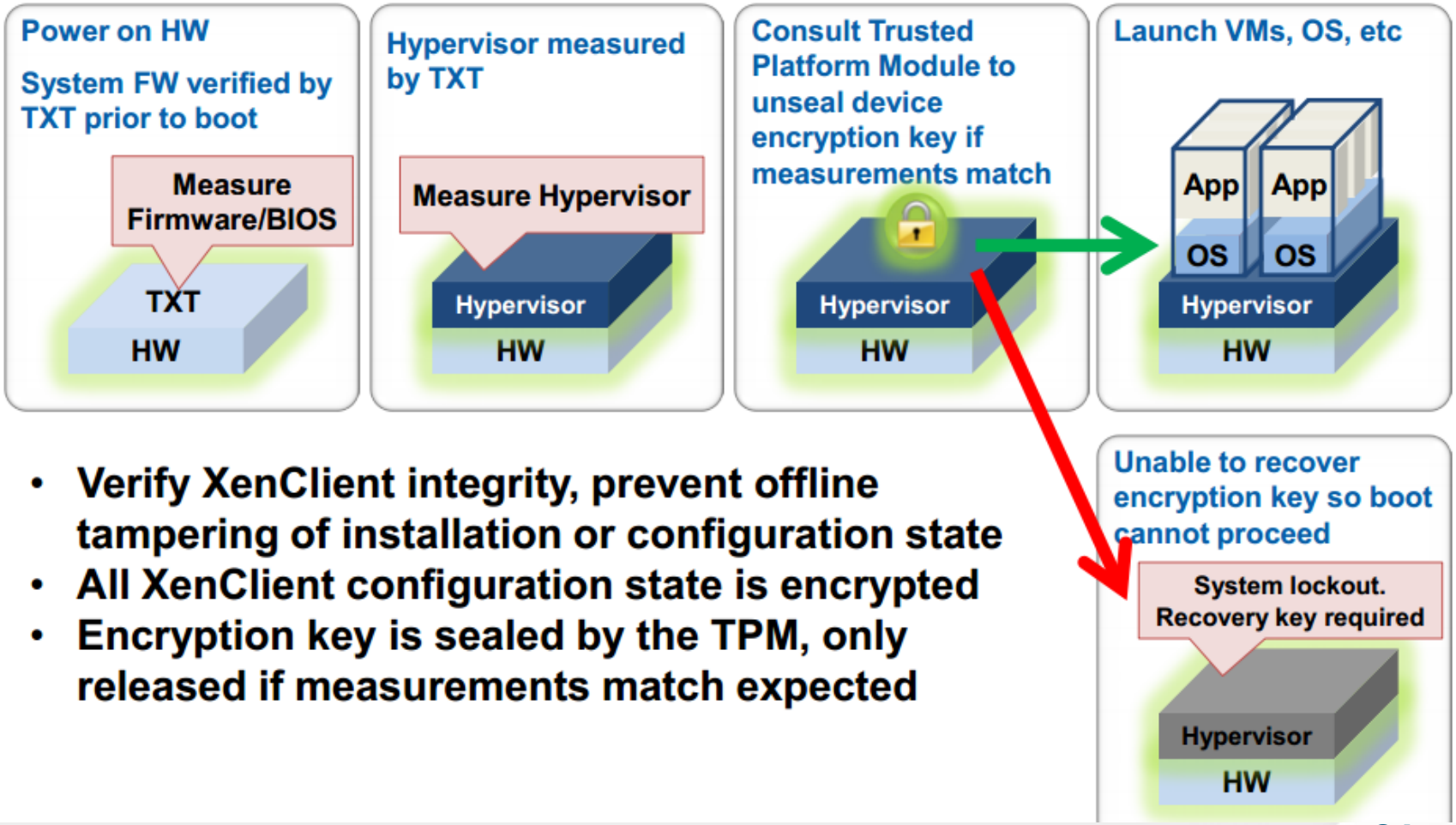
– Trusted Platform Module PCRs reflect the state and configuration of system

• All XenClient device configuration state is encrypted

– Encryption key is sealed by the TPM, only released if PCR values match those expected "

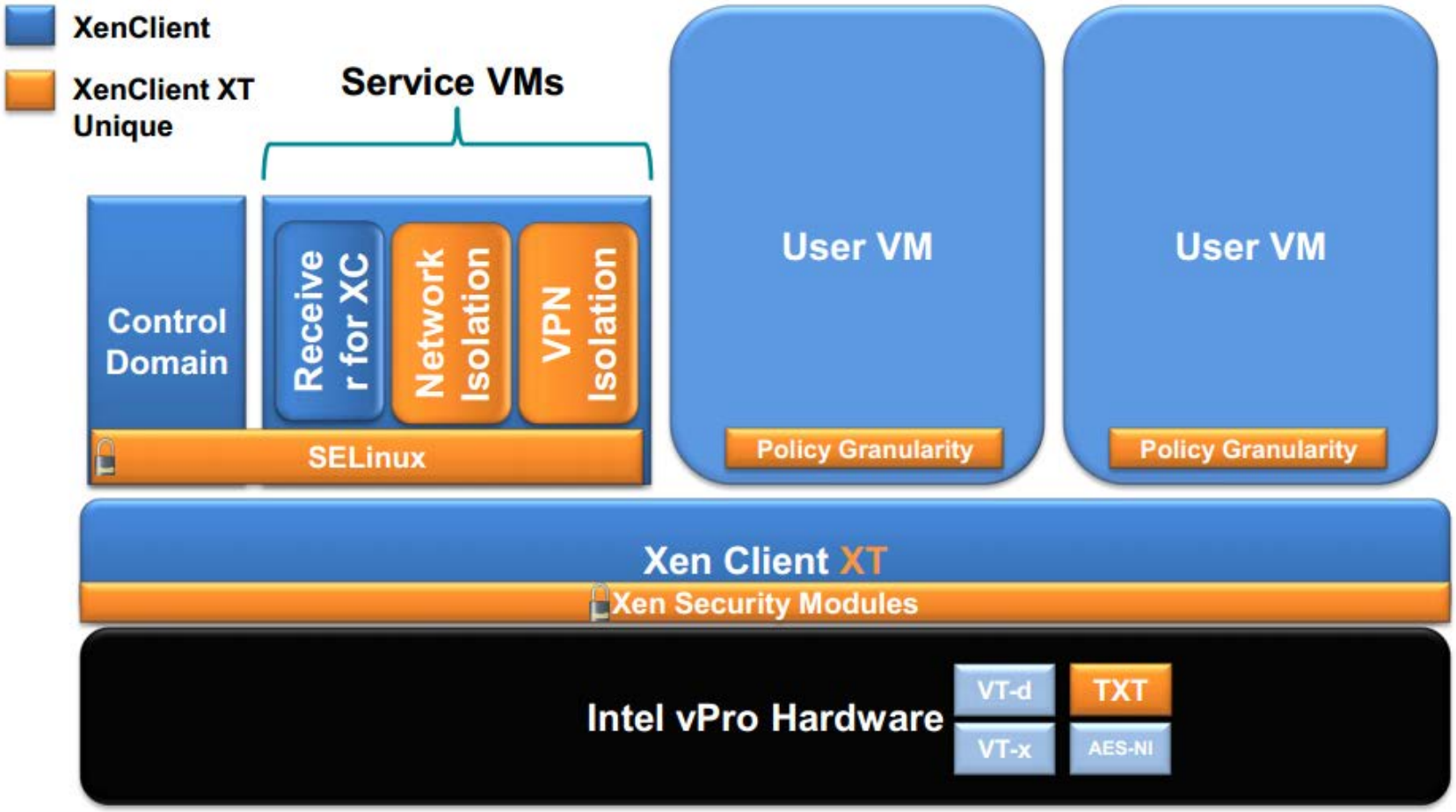
https://www.ncsi.com/nsatc11/presentations/thursday/real_world/durante.pdf
Slide 25

Virtualization (SecureView Desktop)
XenClient XT: Trusted Execution Technology



- Verify XenClient integrity, prevent offline tampering of installation or configuration state
- All XenClient configuration state is encrypted
- Encryption key is sealed by the TPM, only released if measurements match expected

Virtualization (SecureView Desktop)
XenClient XT Architecture



Microsoft's View of TCG and TPM

- TCG mission is critical for industry
- Group member and board participant
- Windows is taking deep dependencies on TCG technologies
- Using UEFI for root of trust
- Using TPM for securing data, integrity validation, increased entropy
- Supporting enhanced SED's for drive data protection
- We will continue to find new and interesting ways to use UEFI and TPM in future products

History of UEFI and TPM IN Windows

Windows Vista / 7	Windows 8	Windows 8.1
BitLocker	Trusted Boot ASLR Bitlocker Measured Boot Virtual Smart Cards Certificate Storage Visual Studio	Trusted Boot ASLR Bitlocker Measured Boot Virtual Smart Cards Certificate Storage Visual Studio TPM Key Attestation Provable PC Health

TPM Use in Windows – Key Features

- **Trusted Boot**
  - Leverages UEFI as the Windows root of trust
  - UEFI Secure Boot ensures malware is unable to start before the OS
- **BitLocker**
  - Protects data at rest with full volume encryption
  - Uses TPM to protect keys that are used to unlock protected drives
- **Virtual Smartcards**
  - Provides 2FA with a virtualized Smart Card solution
  - Uses TPM to protect users digital identity (certificate)

TPM Use in Windows – Key Features

- **TPM Based KSP**
  - Data within the Windows Key Storage Provider is protected with HW
  - Uses TPM to encrypted/decrypt keys; prevents export and replay
- **TPM Key Attestation (new in Windows 8.1)**
  - Enables resources to implement access control policy that can request confirmation that certificate and keys being used by a client have been securely provisioned, stored, and maintained
  - Uses TPM related metadata for access control policy
- **Measured Boot**
  - Measurements of firmware and critical Windows boot files are taken
  - Uses TPM to securely measure and persist Measured Boot data
- **Provable PC Health (new in Windows 8.1)**
  - A free cloud based service that assembles system integrity and security related configuration and sends it to the cloud for remote analysis
  - Uses TPM derived Measured Boot data for health analysis

What Will Be Available in the Near Future?

- Virtual TPM (for example the TrustZone available on ARM devices and Atom on Intel Atom devices)
- Haswell (new architecture from Intel)
- Mobile devices with TPMs allow Google to incorporate TPM use in its Five-year Identity Plan (May 2013)

Conclusion

- TPM has more than a decade of R&D invested
- Participation by some of the IT industry's biggest players, from handheld to server
- Use cases include increased trust in the integrity of firmware/software stack and confidentiality of data
- Bare metal and virtual, client and server-side, including HSMs in the cloud and multilevel classified machines
- Hardware roots of trust are becoming ubiquitously available and cheap
- TPM is embedding hardware-enabled security from cheap consumer devices all the way to enterprise-grade datacenter infrastructure.

References

- TCG members: http://www.trustedcomputinggroup.org/members/
- Mebromi paper from GMU.edu http://mason.gmu.edu/~msherif/isa564/fall11/projects/bios.pdf
- Google Five Year Identity Plan http://goo.gl/DFLnS
- NSA's High Assurance Platform (HAP) http://www.nsa.gov/ia/programs/h_a_p/resource_library/index.shtml
- NIST Special Publications SP 147, 155, 164
- Windows TPM Provider - http://msdn.microsoft.com/en-us/library/windows/desktop/aa376484(v=vs.85).aspx
- Windows TPM 2.0 Hardware Interface Table - http://download.microsoft.com/download/9/3/1/9310398B-2F4F-4E27-B57B-DFAA9723B6D5/tpm-2.0-hardware-interface-table.docx
- Windows Virtual SmartCards - http://download.microsoft.com/download/5/A/B/5ABDDED2-F56E-427D-88C1-411EA0DBFF42/Understanding%20and%20Evaluating%20Virtual%20Smart%20Cards.docx
- Intel TXT graphic http://www.intel.com/content/www/us/en/architecture-and-technology/intel-trusted-execution-technology-graphic.html
- ARM TrustZone virtual TPM http://www.arm.com/products/processors/technologies/trustzone.php

References

- SecureView Multi-Level Desktop with TPM: https://www.ncsi.com/nsatc11/presentations/thursday/real_world/durante.pdf (See slides 22, 25-26)
- Google Chromebook and TPM: http://www.chromium.org/developers/design-documents/tpm-usage
- AWS/SafeNet CloudHSM: http://aws.typepad.com/aws/2013/03/aws-cloud-hsm-secure-key-storage-and-cryptographic-operations.html
- PwC TPM Authentication Case Study: https://www.ncsi.com/nsatc11/presentations/tuesday/real_world/muralidharan.pdf
- NIST SP-800-164: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
- NSA High Assurance Platform (HAP): *http://www.nsa.gov/ia/_files/HAP_Brochure.pdf*