The Trusted Platform Module (TPM)

Olav Ligaarden

Nasjonal sikkerhetsmyndighet

AFSecurity Seminar, University of Oslo, 2014-01-29

Outline

- TPM and trusted computing
- The TPM in more detail
- Examples: The TPM and Microsoft Windows
- Conclusion
- Further reading

Outline

- **TPM and trusted computing**
  - Trusted platform module
  - Trusted computing
  - The grand vision of trusted computing
- The TPM in more detail
- Examples: The TPM and Microsoft Windows
- Conclusion
- Further reading

Trusted platform module

- A tamper-resistant security chip that is soldered to the computer’s motherboard
  - Perform cryptographic operations and protects small amounts of sensitive data
  - A passive device
  - Manufacturers include Infineon, Atmel, Broadcom, etc.
  - Inexpensive (< $1)

- Specification
  - Made by the Trusted Computing Group (TCG)
  - The current version is 1.2
  - A draft of the TPM 2.0 specification is in review

Trusted computing

- Generally refers to systems that use hardware to support security in software
  - TPM, CPUs with secure modes, etc.

- Also covers infrastructure relying on the above
  - Applications, network access control (NAC), secure storage devices, etc.

- The main goal is to build trust in entire system for some purpose
  - The TPM plays an important role here

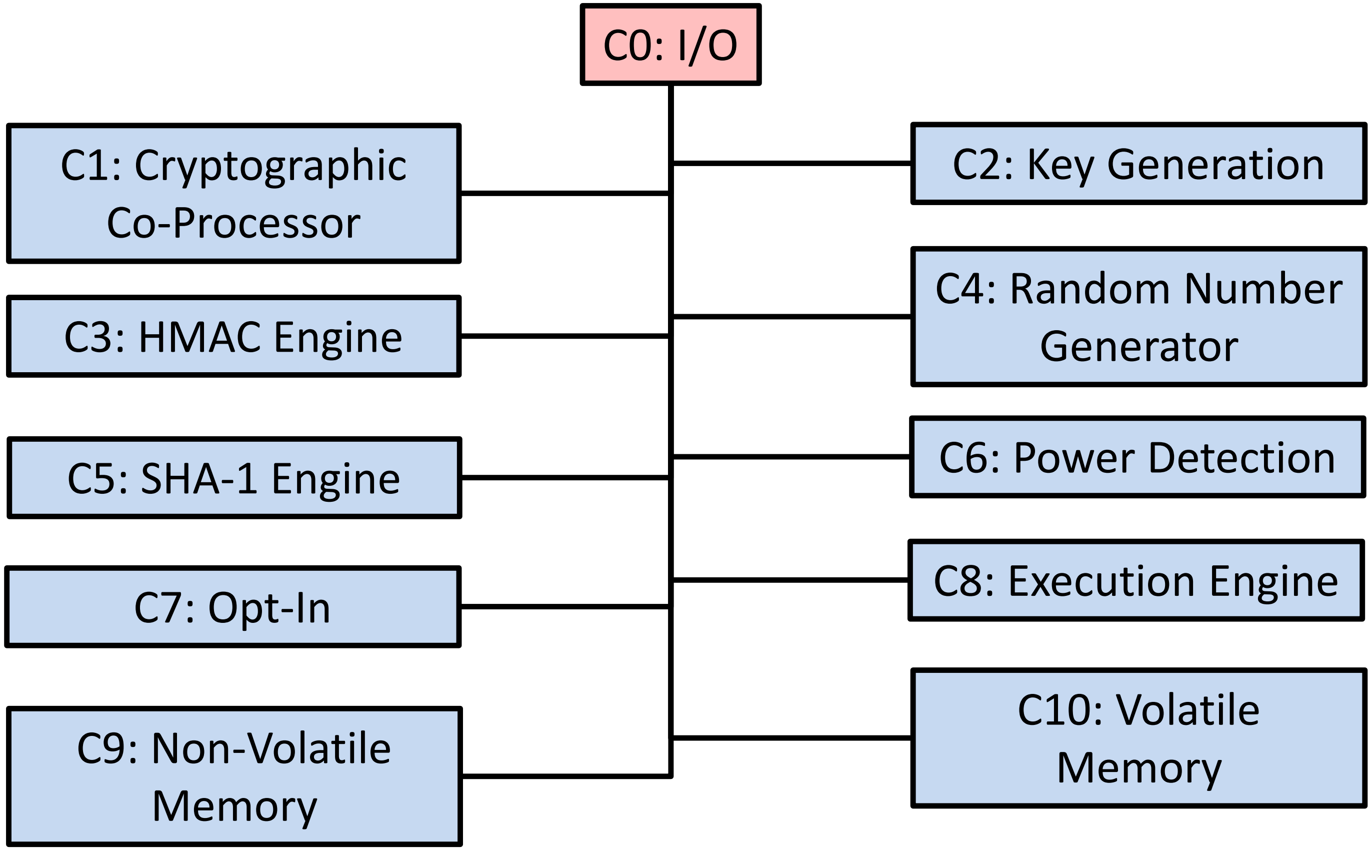
The grand vision of trusted computing

- Before logging in, I know that the computer is good
- Computers that are not up-to-date are routed to a DMZ to perform updates before they are allowed to connect to the network
- Confirm exactly which machines we are talking to and whether they run good software before providing them with sensitive data
- Use hardware to protect all of my data, including secret keys, from being stolen and transmitted over the network

Outline

- TPM and trusted computing
- **The TPM in more detail**
  - What is in a TPM?
  - What TPMs provide
  - Debunking of myths
  - What is it good for?
- Examples: The TPM and Microsoft Windows
- Conclusion
- Further Reading

What is in a TPM?



C0: I/O

C1: Cryptographic Co-Processor

C2: Key Generation

C3: HMAC Engine

C4: Random Number Generator

C5: SHA-1 Engine

C6: Power Detection

C7: Opt-In

C8: Execution Engine

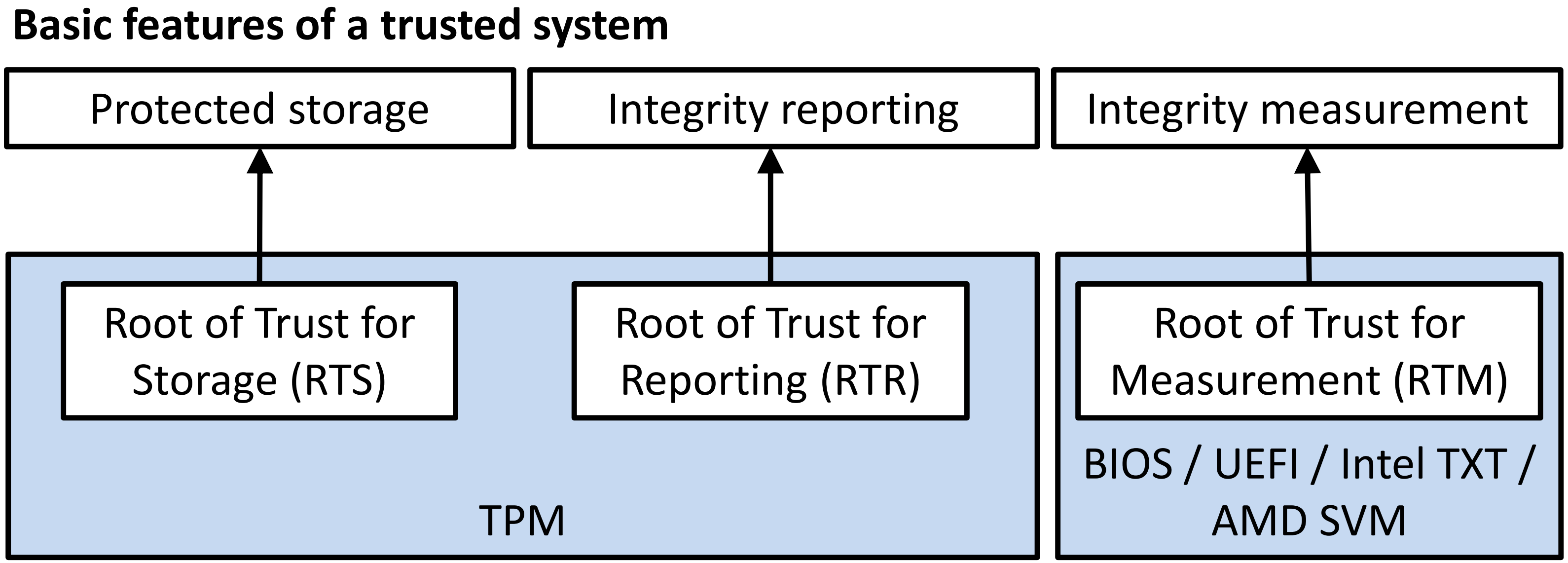
C9: Non-Volatile Memory

C10: Volatile Memory

What TPMs provide

- Roots of trust
- Platform configuration registers (PCRs)
- RSA keys
  - Root keys
  - Non-root keys
- ... and more!

Roots of trust


Basic features of a trusted system
Protected storage
Integrity reporting
Integrity measurement
Root of Trust for Storage (RTS)
Root of Trust for Reporting (RTR)
Root of Trust for Measurement (RTM)
TPM
BIOS / UEFI / Intel TXT / AMD SVM

- The thing that you base all other trust on
- Trusted inherently
  - Must be trusted because misbehavior may not be detected
  - Technical evaluation based on the specification by competent experts

Roots of trust cont.

- Root of trust for measurement (RTM)
  - Capable of making inherently reliable integrity measurements
  - Root of the chain of transitive trust

- Root of trust for storage (RTS)
  - Capable of storing integrity measurements in a safe and reliable way
  - Capable of protecting secrets
    - Not all of them are protected directly

- Root of trust for reporting (RTR)
  - Capable of reliably reporting information held by the RTS

Platform configuration registers

- Series of 20-byte registers (size of a SHA-1 hash)
- Most modern TPMs have 24 registers
- Used to store system measurements
  - Measurements may also be stored in Stored Measurement Log (SML)
- Highly constrained behavior
  - Reset to known value at boot
  - Data can only be stored with Extend operation

Platform Configuration Registers cont.

- Use **Extend** operation to store data in a PCR
  - Current PCR value: **Y** (SHA-1 hash)
  - New measurement: **X** (Data ≤ 20 byte / SHA-1 hash of this data)
  - New PCR value: **hash(Y || X) = Z**
  - hash(Y || X) ≠ hash(X || Y)

- Perform the same hash chain to verify PCR values

- Computationally infeasible to forge (must break SHA-1)
  - Current PCR value is N, while desired value is M
  - hash(N || X) = M; violates the one-way assumption

TPM root keys

- **Endorsement Key (EK)**: The key that the TPM uses in its role as Root of Trust for Reporting
  - Unique platform identity
    - Trust in all other keys comes down to trust in the EK
  - Should be generated in TPM during manufacture time in a secure environment

- **Storage Root Key (SRK)**: The key that the TPM uses in its role as Root of Trust for Storage
  - Used to protect other keys and data via encryption

- These keys **never** leave the TPM

TPM non-root keys

- All TPM keys are RSA keys, but have specialized roles
  - Encryption/Decryption: Storage, Sealing, Binding
  - Signing/Reporting: Identity, Signing
    - Identity keys are better known as Attestation Identity Keys (AIKs)

- Stored in “blobs” outside the TPM
  - Private half is encrypted by Storage Root Key (or other key)
  - Integrity protection on other data

- Loaded into the TPM when needed

What is the TPM good for?

- Machine authentication
- Machine attestation
- Data protection

Machine Authentication

- Use TPM to identify a machine
  - TPM is soldered to the motherboard
  - Keys are cryptographically bound to a particular TPM

- Signing-based authentication
  - This data passed through machine X

- Encryption-based authentication
  - Only machine X can read this data

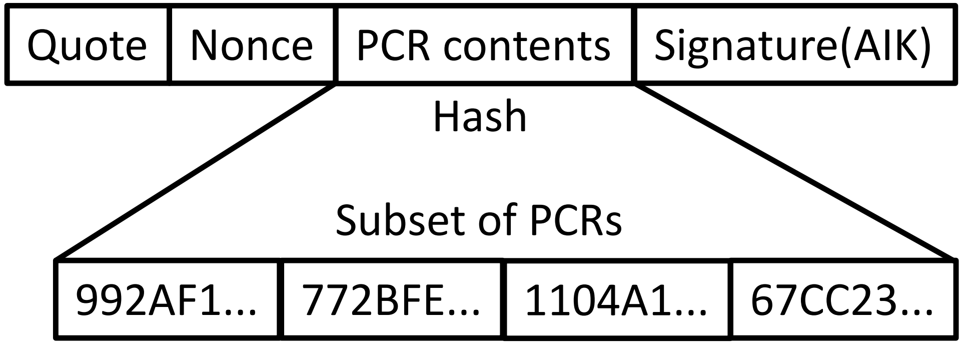
- One of the simplest TPM applications

Machine Attestation

Attestation: *the presentation of verifiable evidence about machine state to a remote party*

- Primary tool is quote
  - Contains the verifiable evidence in the form of a signed report of a subset of PCRs
- Remote verifier check the state of the machine based on signed reports from the TPM
- Have the potential of checking whether a piece of software is trustworthy

Quotes



Quote | Nonce | PCR contents | Signature(AIK)

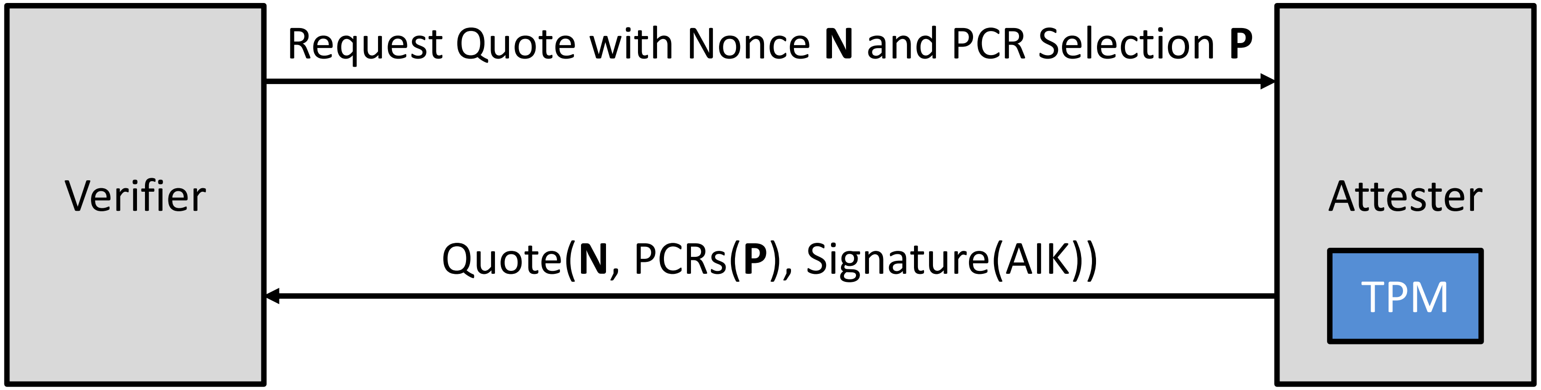
Hash

Subset of PCRs

992AF1... | 772BFE... | 1104A1... | 67CC23...

- Nonce for freshness, provided by verifier
  - A freshly generated random value
- Hash of a subset of PCR values
- Should be signed using an Attestation Identity Key (AIK)

Using quotes


Verifier
Request Quote with Nonce **N** and PCR Selection **P**
Quote(**N**, PCRs(**P**), Signature(AIK))
Attester
TPM

- Attester decides
  - Willing to give this state info to verifier?
- Verifier decides
  - Is quote valid and from a legitimate TPM?
  - Is nonce the same as I provided? If fresh, proves quote is current
  - Are PCRs in a state I approve of?

Attestation is not easy

- PCR values are very fragile
  - Any change in measurement value will change the hash unpredictably!
    - Did it update the date or add a rootkit?
  - Things start in different order and there are timing conditions
- Extremely difficult to predict PCR values
  - Holy grail of measurement: golden values reflecting good/bad state
- Still useful
  - Is my machine the same as yesterday?

Debunking of Myths

- The TPM controls boot
  - Passive device
  - Cannot stop the machine from booting, but can protect data

- The TPM is tamper-proof
  - Tamper-resistant ... for consumer products
  - Tremendously good for their cost!
    - Cost < $1
    - Cost researchers > $100,000 to break
  - Not designed with government tamper-resistance standards in mind

Debunking of Myths cont.

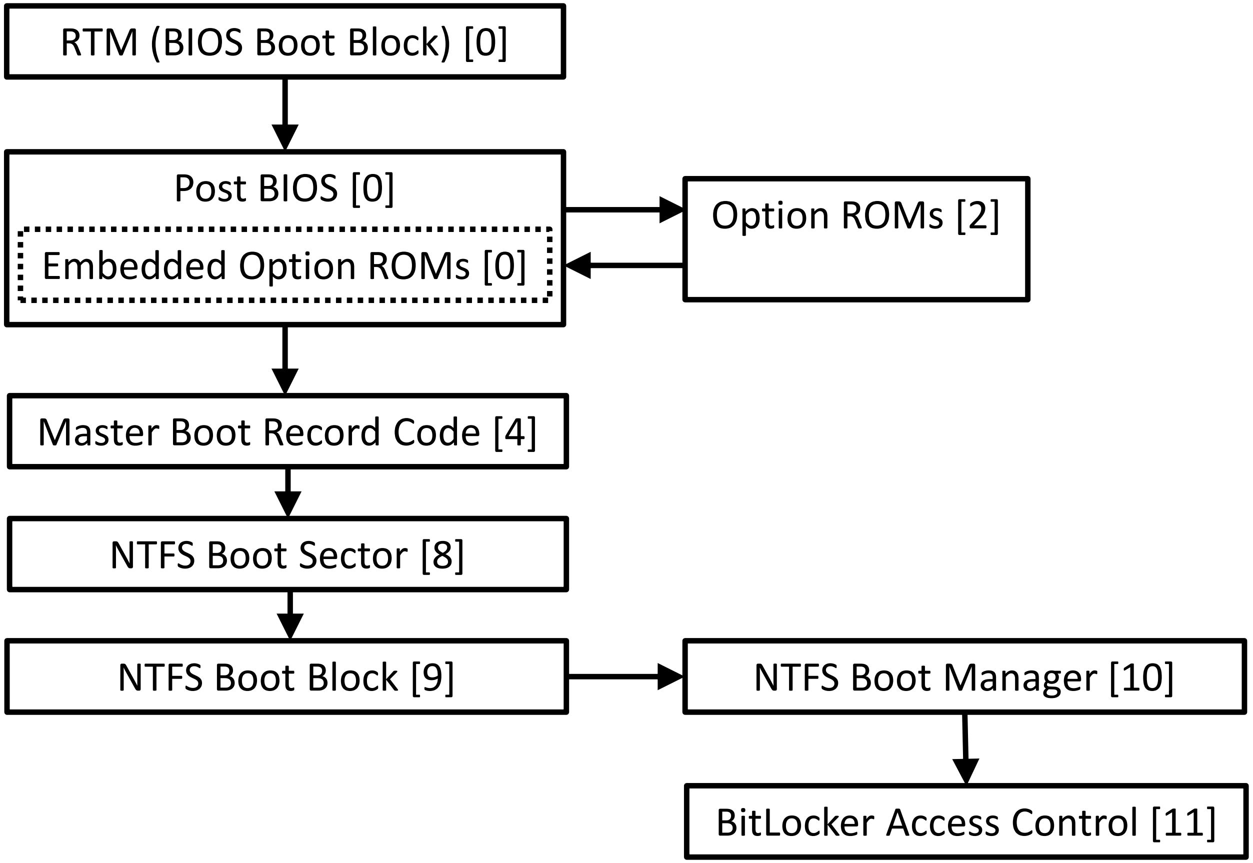
- The TPM works for Disney/Microsoft/etc
  - Originally pitched for DRM use
  - The TPM belongs to the owner of the machine, which has full control
  - One reason why TPMs have so many privacy features

- You can delegate all crypto to the TPM
  - Highly constrained cryptographic functionality
    - Prevents many attacks
  - Too slow!
    - Cost is priority, not performance

Outline

- TPM and trusted computing
- The TPM in more detail
- **Examples: The TPM and Microsoft Windows**
  - TPM, BitLocker, Windows 7, and conventional BIOS
    - Measurement of components
    - Decryption of BitLocker encrypted data
  - Multifactor authentication
  - The Evil Maid
  - TPM, BitLocker, Windows 8.X, and UEFI
    - Secured Boot
  - Other uses of the TPM on Windows 8.X
- Conclusion
- Further Reading

Measurement of components



RTM (BIOS Boot Block) [0]

Post BIOS [0]

Embedded Option ROMs [0]

Option ROMs [2]

Master Boot Record Code [4]

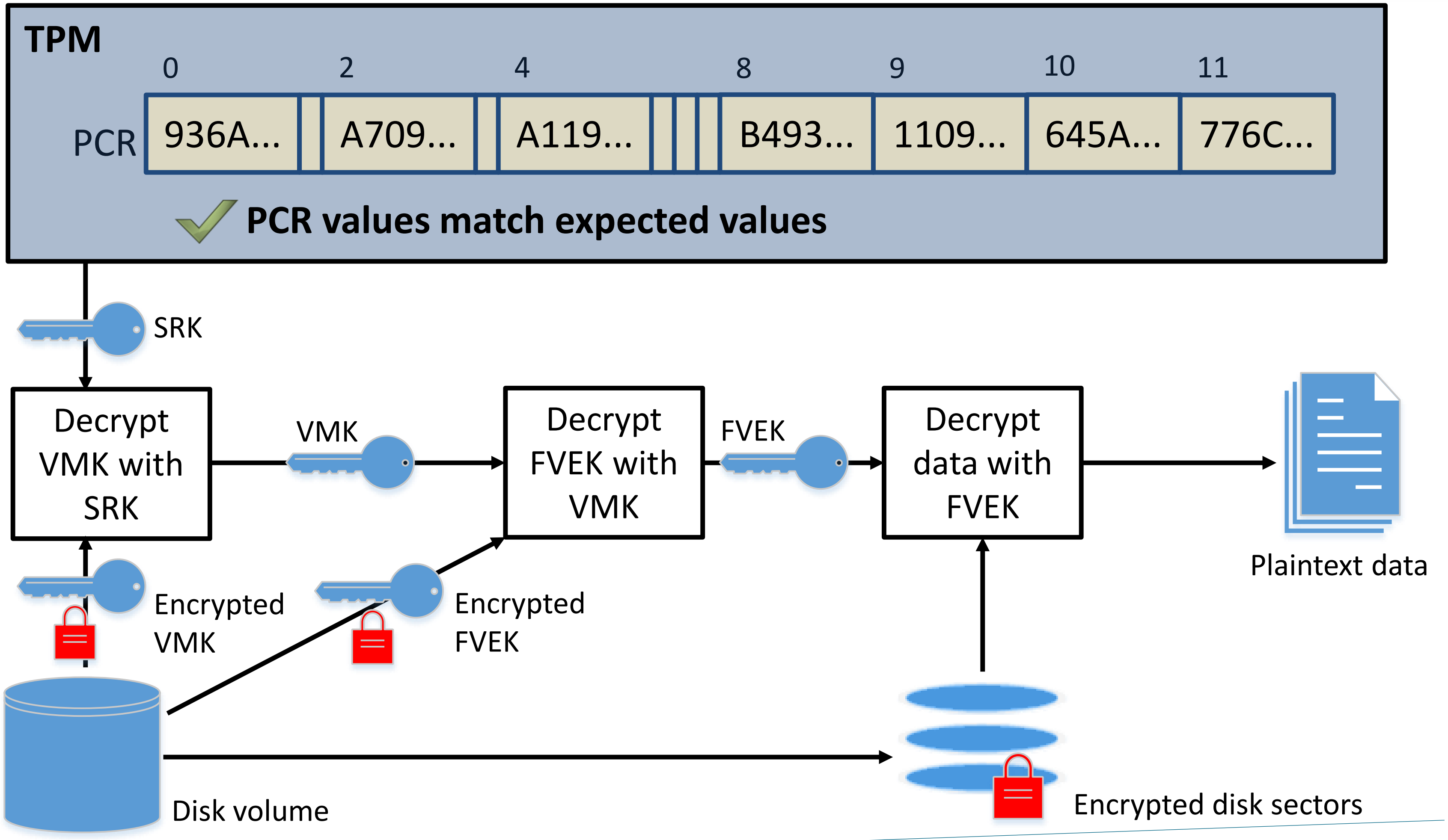
NTFS Boot Sector [8]

NTFS Boot Block [9]

NTFS Boot Manager [10]

BitLocker Access Control [11]

Decryption of BitLocker encrypted data



TPM

	0		2		4				8	9	10	11
PCR	936A...		A709...		A119...				B493...	1109...	645A...	776C...

✓ **PCR values match expected values**

Multifactor authentication

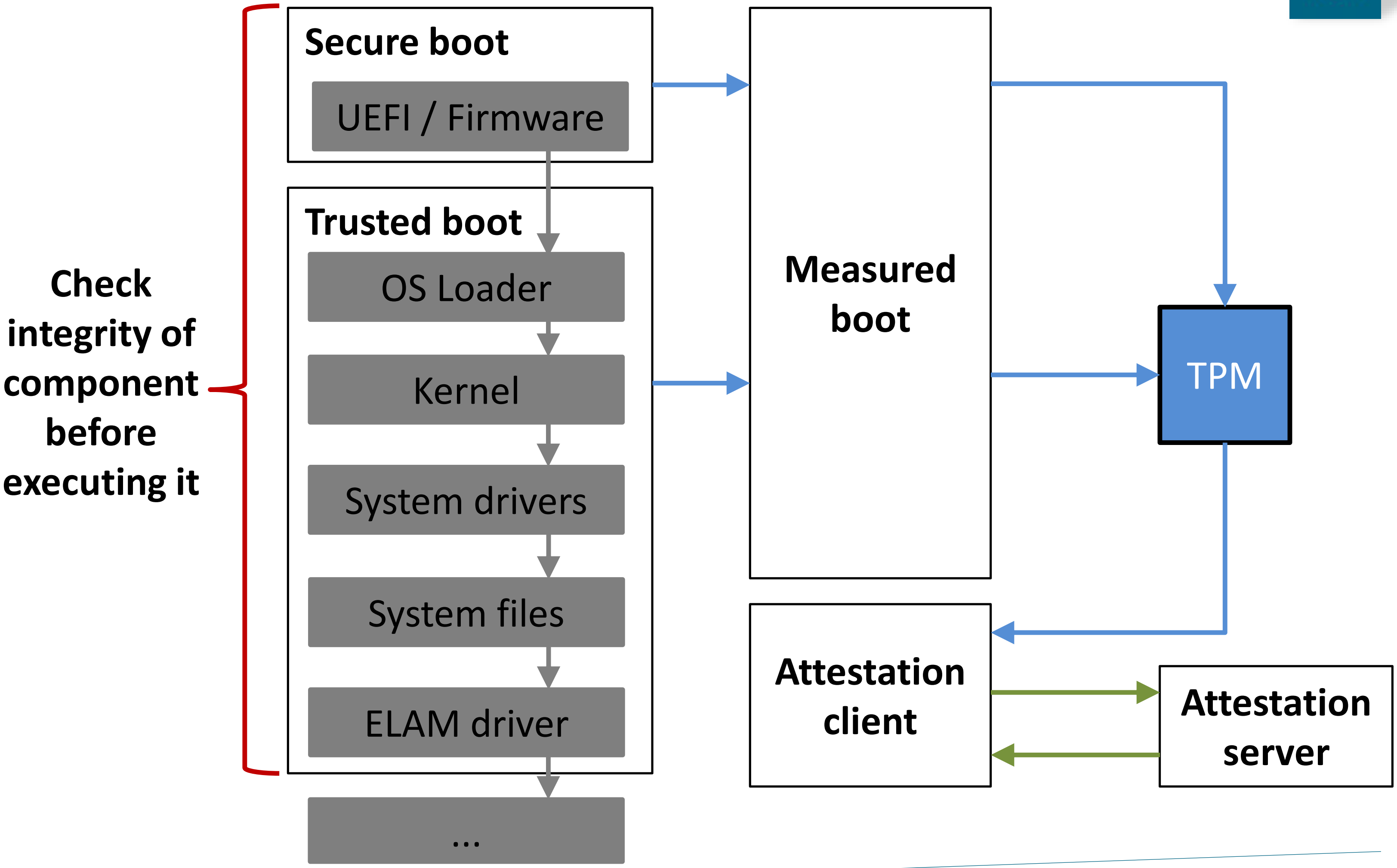
- TPM only
  - Retrieve Full Volume Encryption Key from memory after boot
- TPM + PIN or Enhanced PIN
  - Volume Master Key is sealed by both TPM and PIN
  - Anti-hammering technology to prevent dictionary attacks
- TPM + USB
  - Storage Root Key decrypts an intermediate key
  - This key is combined with the key on the USB to create another intermediate key
  - The intermediate key is used to decrypt the Volume Master Key
- TPM + PIN or Enhanced PIN + USB

The Evil Maid

- You leave the laptop in the hotel room
- Evil maid sneaks into room
  - Boots the laptop from an evil USB stick and replace the MBR with an evil MBR which contains a fake PIN prompt
- You power on the laptop, enter the correct PIN, the evil MBR say that the PIN is incorrect, and the machine reboots
  - The evil MBR has sniffed the PIN and written it to disk
  - The evil MBR has replaced itself with the correct MBR
  - Everything is OK on the next boot
- The evil maid sneaks back into the room and retrieves the PIN and possibly the machine

Source: The Invisible Things Lab's blog

Secured Boot



Check integrity of component before executing it

Secure boot

UEFI / Firmware

Trusted boot

OS Loader

Kernel

System drivers

System files

ELAM driver

...

Measured boot

TPM

Attestation client

Attestation server

Other uses of the TPM on Windows 8.X

- Network unlock
  - No pin required if on a trusted network
  - Pin required when roaming
- TPM based certificate storage
  - The certificate template can be configured to specify the TPM to protect/store the private key
  - Software can never discover the private key
- TPM based virtual smart card
  - The TPM act as a permanently inserted smart card
  - Simulate a smart card reader

Conclusion

- TPM is a tamper-resistant security chip that can be used for
  - Machine authentication
  - Machine attestation (to some extent)
  - Data protection
- There exists a number of applications that make use of the TPM
  - Especially on the Windows platform
- But there are a number of problems that needs to be solved before we can fulfill the grand vision of Trusted Computing
- Considering the cost of a TPM, you get a lot of security for your money!

Further reading

- David Challener et al. A Practical Guide to Trusted Computing, IBM Press, 2008.
- Ariel Segall. Introduction to Trusted Computing, 2012. http://opensecuritytraining.info/IntroToTrustedComputing.html
- TCG. TPM Main Specification, Level 2 Version 1.2, Revision 116, 2011. http://www.trustedcomputinggroup.org/resources/tpm_main_specification
- ISO/IEC. ISO/IEC 11889:2009 – Trusted Platform Module, 2009.
  - Recommend “Part 1: Overview” and “Part 2: Design principles”