

PV204 Security technologies



Trusted Boot, TPM, SGX

Petr Švenda  svenda@fi.muni.cz  [@rngsec](https://twitter.com/rngsec)

Centre for Research on Cryptography and Security, Masaryk University

CRCS

Centre for Research on
Cryptography and Security

Please comment on slides with anything unclear, incorrect or suggestions for improvement
<https://drive.google.com/file/d/1i8K1d8JplesLnMbf8S4QUNs3UEXhLbUr/view?usp=sharing>

www.fi.muni.cz/crocs

Overview

- Booting chain of programs
- BIOS as root of trust
- Verified and Measured boot
- Trusted boot in the wild
 - Trusted Platform Module
 - Chromium, Windows 8/10/11, UEFI...
- Dynamic root of trust
 - Intel's TXT, SGX

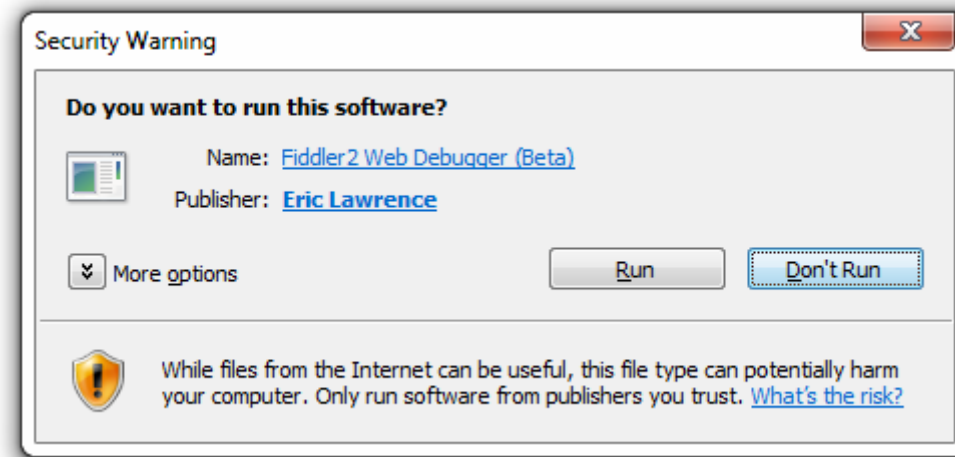
Motivation – untrusted host platform

- Traditional role of operating system
 - Isolate processes
 - Manage privileges, authorize operations
- But how to deal with
 - Debugger, disassembler
 - Intercepted multimedia output
 - Malware run along with banking app
 - Keyloggers, Evil maid
 - System administrators, Service providers
 - ...



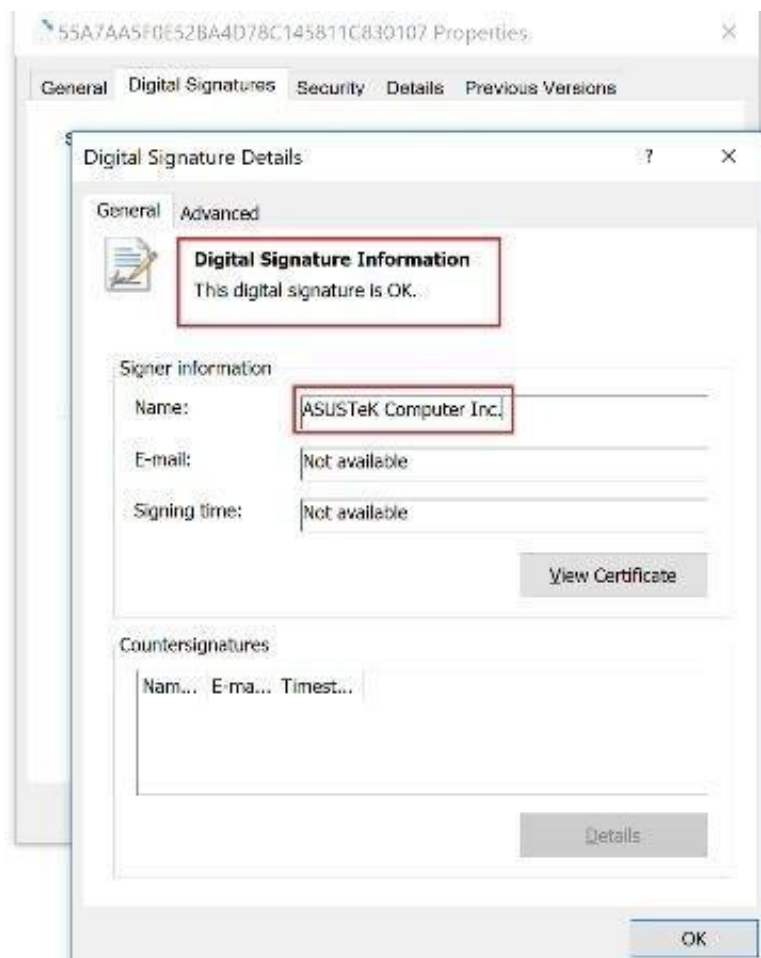
Solution?

- Code signing (e.g., Microsoft Authenticode)
 - Application binary is signed, PKI used to verify certificate
 - If not signed, user is notified
 - Mandatory signing for selected applications (drivers...)



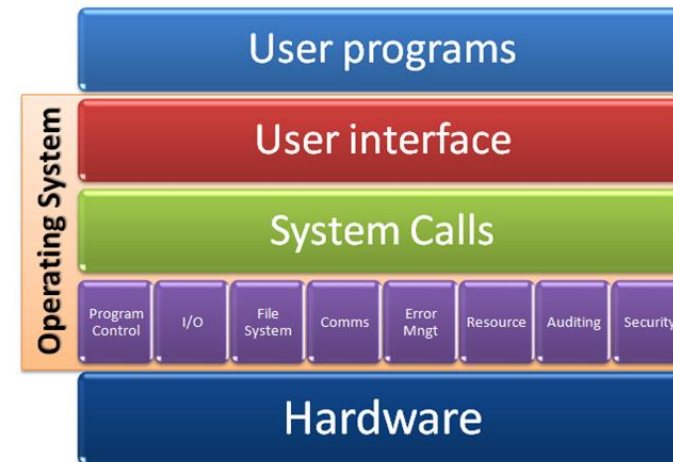
? Signed == Secure?

Signed == Secure?



Trust in program's functionality

- Trust in a program code?
 - Signed code may still contain bugs and vulnerabilities
- Trust **only** in a program code?
 - Underlying OS layers
 - Underlying firmware
 - Underlying hardware
 - Memory used by the program
 - Other code with access to the program's memory/code
 - ...
- The program is almost never executed “alone”

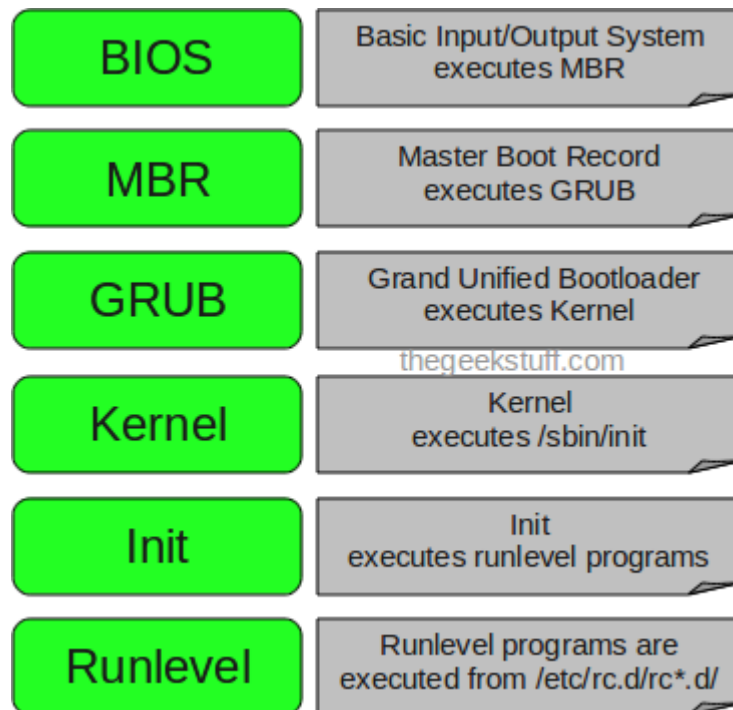


Problem statement

- How to make sure that valid programs run only within valid environment?
 1. Is it possible to start valid “clean” environment on previously compromised machine?
 2. Is it possible to prevent tampering of apps against an attacker with physical access?
 3. How to prove what apps are running on local machine to a remote party?

Classical boot chain

Linux



Windows



How to detect that BIOS or OS Loader was modified?
(evil maid, bootkit...)

<http://www.thegeekstuff.com/2011/02/linux-boot-process/>

<http://social.technet.microsoft.com/wiki/contents/articles/11341.the-windows-7-boot-process-sbsl.aspx>

How to arrive at the expected chain of apps?

1. Just trust the whole boot process
2. Make all applications in protected read-only memory
 - If read-only => cannot be (maliciously) modified. But is it really what is running?
3. Signature-based approach: [Verified boot](#)
 - Before next app is executed, its signature is verified
 - Requires valid (unforged) public key (integrity)
 - Requires trust to owner of private key (signs only valid applications)
 - (but which particular apps were executed is not known, only that they were signed)
4. Create un-spoofable log what executed: [Measured boot](#)
 - Before next app is executed, its hash (“measurement”) is added to un-spoofable log (TPM’s PCR)
 - Will NOT prevent run of unwanted app, but environment cannot lie about what was executed
 - Requires (protected) log storage (Trusted Platform Module)
 - May require authentication of log (Remote attestation)

Trusted boot



“Verified” boot
(signatures)



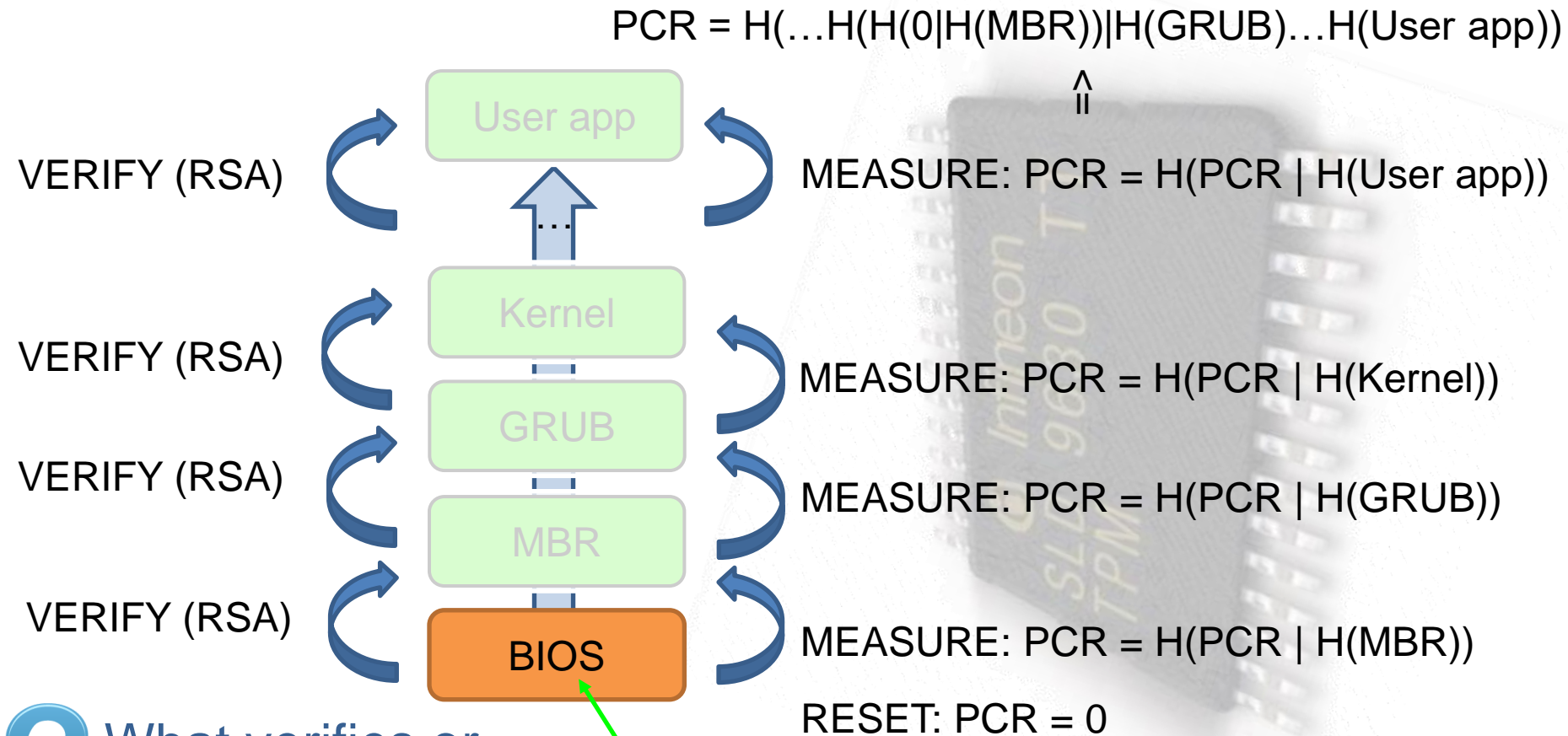
“Measured” boot
(cumulative hash)



Verified and measured approaches can be combined

“Verified” boot

“Measured” boot



? What verifies or measures BIOS?

Nothing => BIOS is Root of Trust

TPMLog.txt

User app

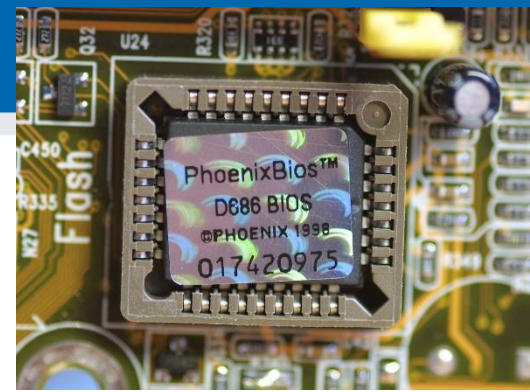
Kernel

GRUB

MBR
BIOS

Root of trust (for verified/measured boot)

- Verified and Measured boot need some **root of trust**
 - Initial piece of code that nobody verifies/measures
- Static root of trust
 - Start building trusted chain after reset of whole device
- Dynamic root of trust
 - Start building trusted chain without reset of device (faster)
- What can be root of trust?
 - static root of trust: BIOS, UEFI firmware, Intel Boot Guard, AMD Platform Security Processor
 - dynamic root of trust: Intel TXT, Intel SGX, Pluton
- Root of trust requires special protection
 - As nobody verifies than nobody will detect eventual modification of it



BIOS as root of trust

- First code executed on CPU of target machine
- Privileged access to hardware
 - E.g., can write into memory of OS code via DMA
- Provides code for System Management Mode (SMM)
 - Routines executed during the whole platform runtime
 - x86 feature since 386, all normal execution is suspended
 - Used for power management, memory errors, hardware-assisted debugger...
 - Very powerful mode (=> also target of “ring -2” rootkits)

BIOS – security considerations

- How BIOS verifies integrity of next module to run?
- Where public key(s) for verification are stored?
- How to handle updates of signing keys?
- How BIOS checks signatures on its own updates?
- How BIOS can be compromised?



How BIOS can be compromised?

1. Maliciously written by BIOS vendor (backdoor)
 2. Replacement of genuine BIOS by malicious one
 - By physical flash (SPI programmer) of BIOS code
 - By lack of flashing protection mechanism by original BIOS
 - By code logic flaws in BIOS locking mechanisms
 3. Modification of other code/data used by BIOS
 - Bug in parsing unsigned data...
- Currently used protections:
 - Chipset-enforced protection of flash memory with BIOS
 - BIOS signature verification before new version is written
 - Hardware-aided check of executed code (TPM, TXT, SGX)
 - Check of BIOS signature before execution by CPU (IBG)

BIOS write locking – “locks”

- Prevent unauthorized BIOS flash (from host OS)
- Allow for authorized BIOS changes
 - BIOS upgrade, signing keys update
 - Change of persistent configurations (boot device...)
- Locking mechanism (locks) for BIOS memory write
 1. Locks are unlocked after reboot
 2. Signature on new BIOS version is verified by old BIOS, and new is flashed eventually (before locking locks)
 3. BIOS configuration (boot device priority) is written before locking locks
 4. Locks locked before handling execution to other code

Attacks against BIOS locks

1. Attacks typically via BIOS code vulnerability
 - BIOS usually does not takes (much) user input, but may parse BIOS update blob with some parts unsigned (logo)
 - Buffer overflow in logo parsing => Locks are not locked yet => write own BIOS
 - <http://invisiblethingslab.com/resources/bh09usa/Attacking%20Intel%20BIOS.pdf>
2. Write into flash memory by SPI programmer



Which one is more serious? Different attacker models

1. Is remote, but patchable
2. Is local attacker, but requires design changes to prevent



Impact: Attack against Tails live-CD distro

- Tails is live-CD Linux distribution
- Designed to provide security even on previously compromised computer
 - Boot complete fresh OS from live-CD + security tools
- Attack 1: Physical BIOS modification
 - Modified BIOS inserts malicious code into Tails during boot time
 - Known thread, physical access to computer assumed
- Attack 2: SMM rootkit (LightEater)
 - Bug in BIOS exploited by remote party to modify SMM routines
- Main issue: Tails tries to start with clean erased computer, but some elements still persist erase (BIOS modifications)

INTEL BOOT GUARD (IBG)

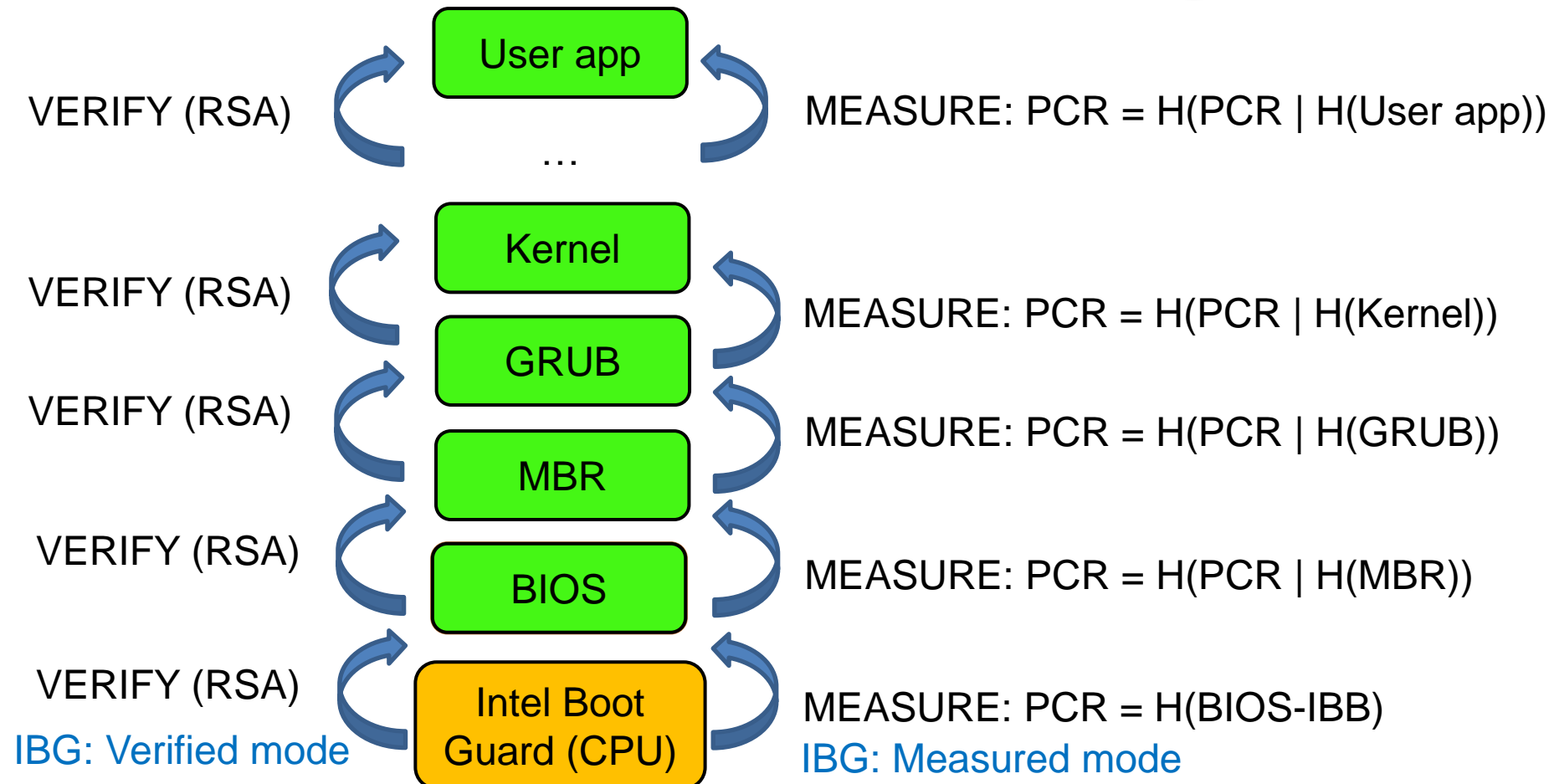
Intel Boot Guard (IBG)

- Feature to protect BIOS
 - Piece of trusted processor-provided, ROM-based code
 - Runs first after reset, verifies *Initial Boot Block (IBB)*
- 1. “Measured” boot mode (TPM-based)
 - Passively extends TPM’s PCRs by hash of IBB
- 2. “Verified” boot mode (digital signature)
 - OEM vendor hardcodes public key via fuses into CPU
 - Intel Boot Guard checks signature of IBB by OEM’s key
 - Only vendor-approved IBB=>BIOS=>OS is executed
- 3. Combination of measured and verified mode

Intel Boot Guard – new root of trust



AMD Platform Security Processor (PSP) provides same functionality as IBG



Intel Boot Guard – security improvements

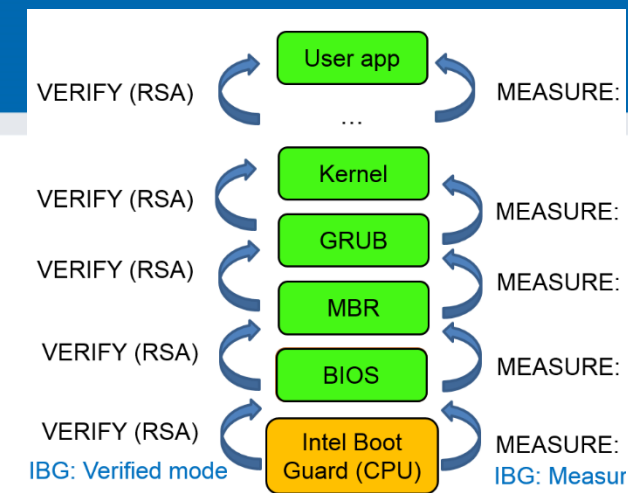
- What attacks are mitigated by Intel Boot Guard?
- Direct BIOS flash by SPI programmer
 - Mitigated, signature/measurement mismatch
- Remote change of BIOS / BIOS data
 - Mitigated, signature/measurement mismatch
- Other bug(s) in BIOS code
 - Not mitigated, signed code still contains bug
- Any new attacks opened by IBG?

How hard is to incorporate backdoor?

- OEM vendor can sign backdoored BIOS
 - But multiple OEM vendors exist, open-source bootloaders (coreboot)
- Intel Boot Guard is written by Intel only
 - But OEM fuses own verification public key, right?
 - But it is the IBG code that actually verifies a signature!
- Trivial (potential) backdoor (inside IBG code inside CPU)
 - if (IBB[SOME_OFFSET] == BACKDOOR_MAGIC) then always load provided BIOS (no signature check)
 - Or possibly verify by some other public key (secure even when BACKDOOR_MAGIC is leaked)

Short summary

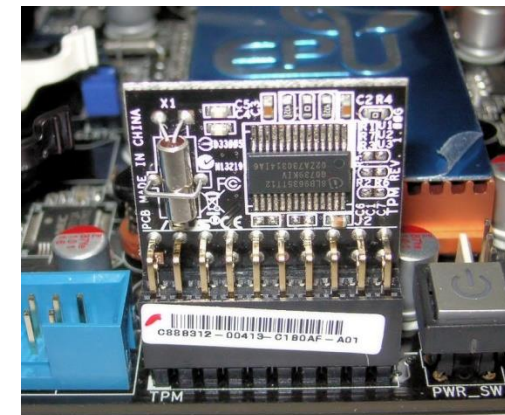
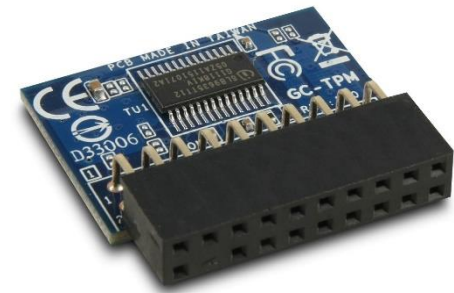
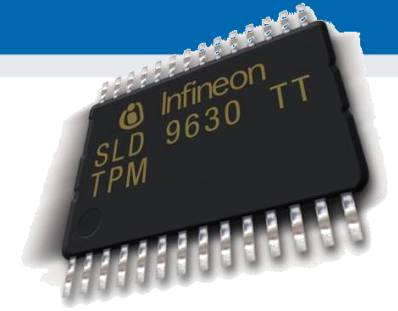
- Signature-based “verified” boot approach
 - Whitelisting approach – run only what is signed
 - Robust signature process needed (trust in private key owner)
 - Integrity of verification public key is critical
 - Key management is necessary (multiple keys, key updates)
- “Measured” boot approach
 - Un-spoofable log of hashes of executed code
 - Can be remotely verified (remote attestation, explained later)
- Root of trust needs to be protected
 - Historically was BIOS (+ update signatures + write locks)
 - Intel Boot Guard/AMD Platform Security Processor inside CPU (signature of BIOS)



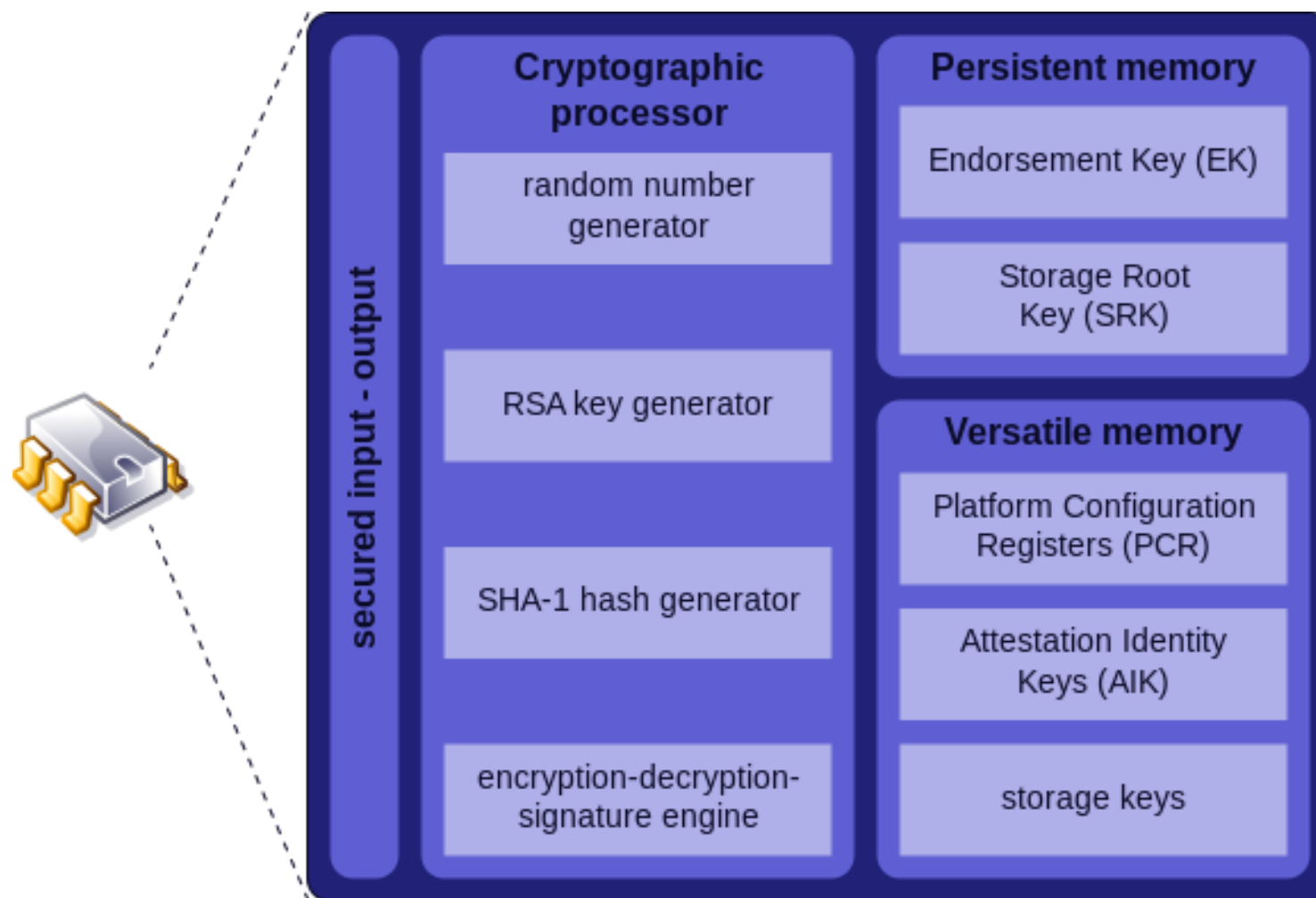
TRUSTED PLATFORM MODULE

TPM hardware

- Cryptographic smart card connected/inside to device
 - Secure storage, cryptographic operations...
 - (But not programmable JavaCard 😊)
- Physical placement
 1. Additional chip on motherboard (discrete dTPM: Infineon, STM, Nuvoton)
 2. Firmware module inside CPU (firmware fTPM: Intel, AMD)
 3. Incorporated in CPU/peripheral (integrated iTPM: Pluton)
 4. (Software TPM – for development and debugging)
- Accessed during boot time
 - “Measured” boot (TPM’s PCR registers)
 - BitLocker encrypted drive keys
- Accessed later (private key operation)



Trusted platform module

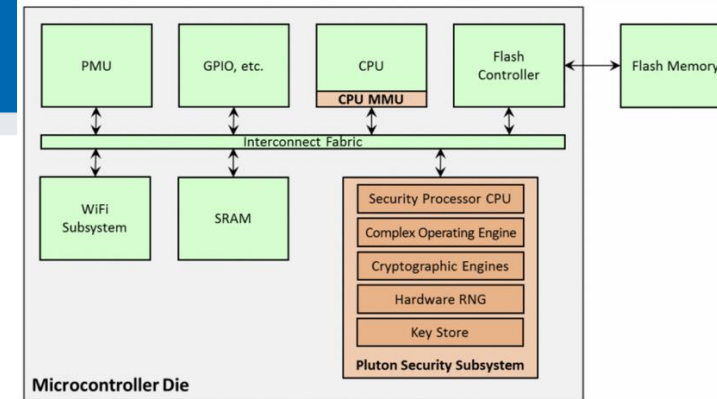


Author: Guillaume Piolle

Trusted Platform Module (TPM)

- ISO/IEC 11889 standard for secure crypto-processor
- Versions published by Trusted Computing Group
 - <https://trustedcomputinggroup.org>
 - TPM 1.2 (2003-2011)
 - TPM 2.0 (2013-now, not compatible with 1.2, but downgrade switch in BIOS)
- Tools to communicate with TPM
 - Windows: Microsoft PCPTool, TSS.MSR, Windows API
 - Linux: tpm_tools, tpm2_tools, GUI TPMManager

Pluton chip (iTTPM)



- Hardware chip inside AMD and Qualcomm CPU/SoC silicon die
 - Co-developed by Microsoft, AMD and Qualcomm (Intel not yet)
 - Similar functionality like Secure Enclave or ARM TrustZone
 - own on-chip RAM, ROM, RNG, cryptographic co-processors...
 - Only Microsoft signed firmware (Windows Update), downgrade protection
 - On non-Windows systems provides only generic TPM 2.0 (iTTPM)
- Used to implement TPM 2.0 functionality (integrated TPM => iTTPM)
 - But also more, design originally from Microsoft Xbox (DRM) and Azure Sphere
 - SHACK (Secure Hardware Cryptography Key) implementation
 - DICE (Device Identifier Composition Engine) implementation
 - Robust Internet of Things (RIoT) specification compliance

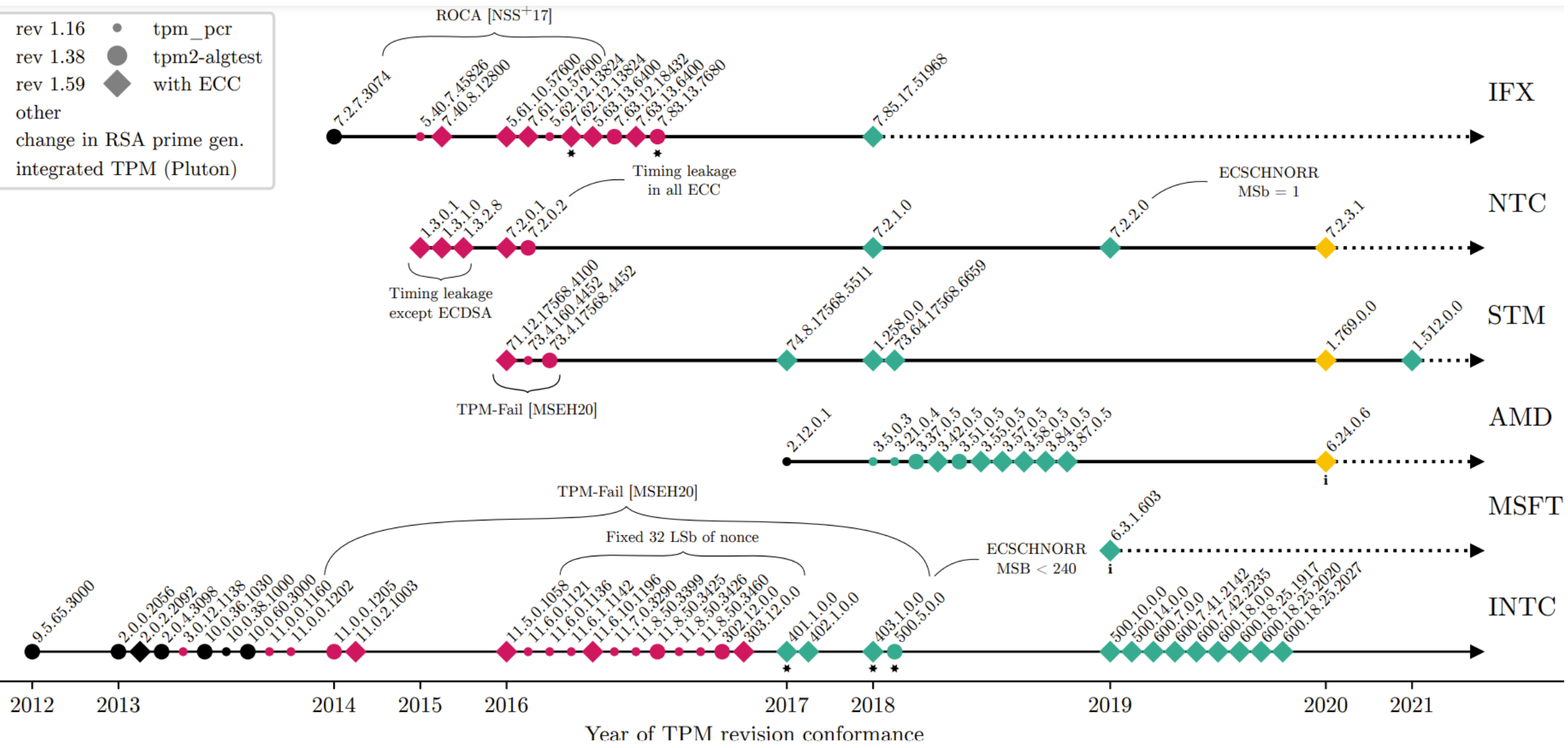
TPM ALG TEST PROJECT

TPM analysis (TPMAIgTest project)

- TPMAIgTest data collection tools
 - AMD, Intel, Infineon, Nuvoton, STM (total 80 TPM versions)
 - FI MU computers, compatibility testing cluster, community submissions
 - <https://github.com/crocs-muni/tpm2-algtest>
- 1. Algorithmic and performance support
- 2. Properties of cryptographic material (RSA and ECC keypairs)
 - Frequency of changes in cryptographic library
- 3. Properties of Endorsement keys (on-chip or injected)
- 4. Analysis of randomness data (GetRandom(), ECC keys and nonces...)

Type	Properties	#
Persistent	System info	—
	TPM capabilities	—
	Algorithm performance	1000x
	Anonymized endorsement keys	2B+2B
Temporal	PCR ₀ –PCR ₂₃ values	—
	RSA & ECC on-chip gen. keys	1000x
	RSA & ECC signatures, nonces	1000x
	Random data	512kB

- rev 1.16
- rev 1.38
- rev 1.59
- other
- tpm_pcr
- tpm2-algtest
- ◆ with ECC
- ★ change in RSA prime gen.
- i integrated TPM (Pluton)



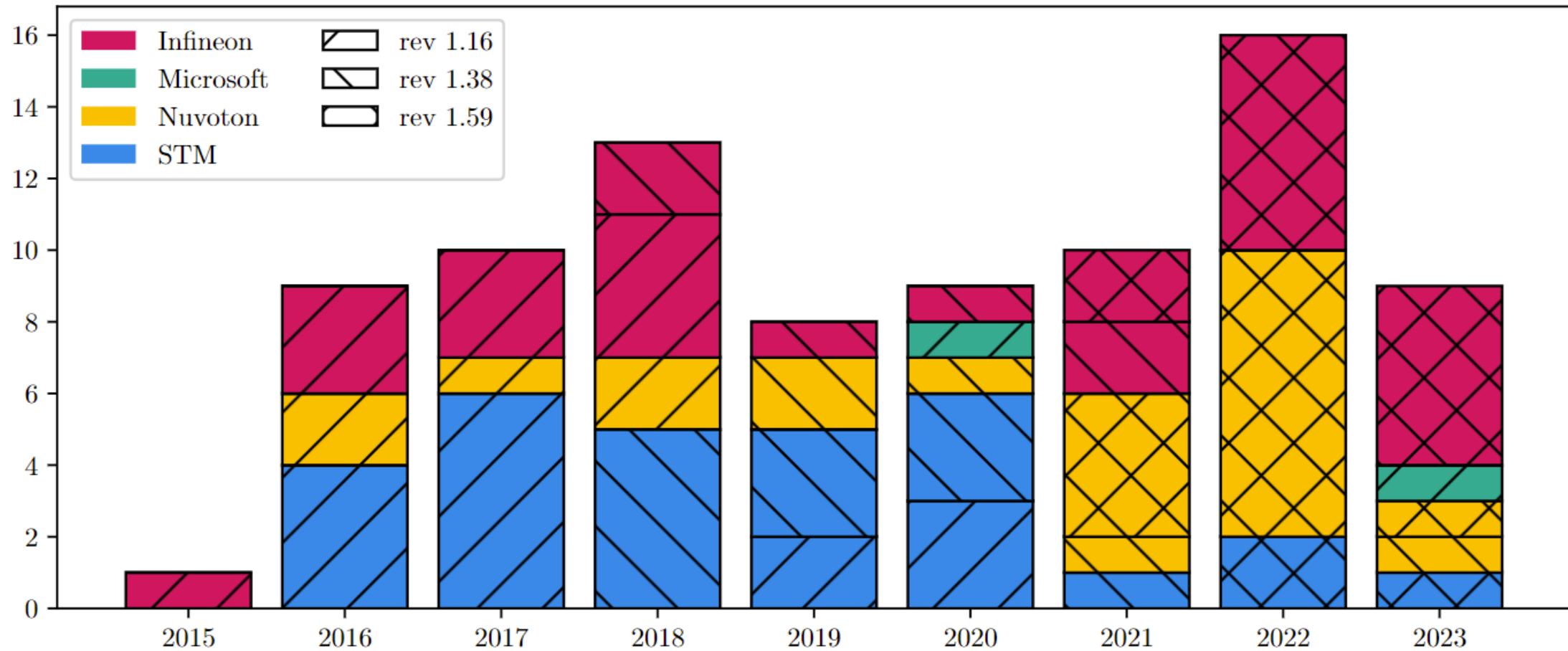


Figure 1: Number of TPM 2.0 certificates issued to vendors by year. The specification revision the certified TPM complies with is shown with a bar pattern.

TPM 1.2 vs. TPM 2.0

- TPM 2.0 introduced algorithm flexibility (no longer fixed SHA-1)
 - If (some) algorithm is broken, no need to create “TPM 3.0”
- TPM 2.0 often supports legacy API 1.2 (switch in BIOS)
- TPM 2.0 seems to focus on IoT-like devices (support TLS)

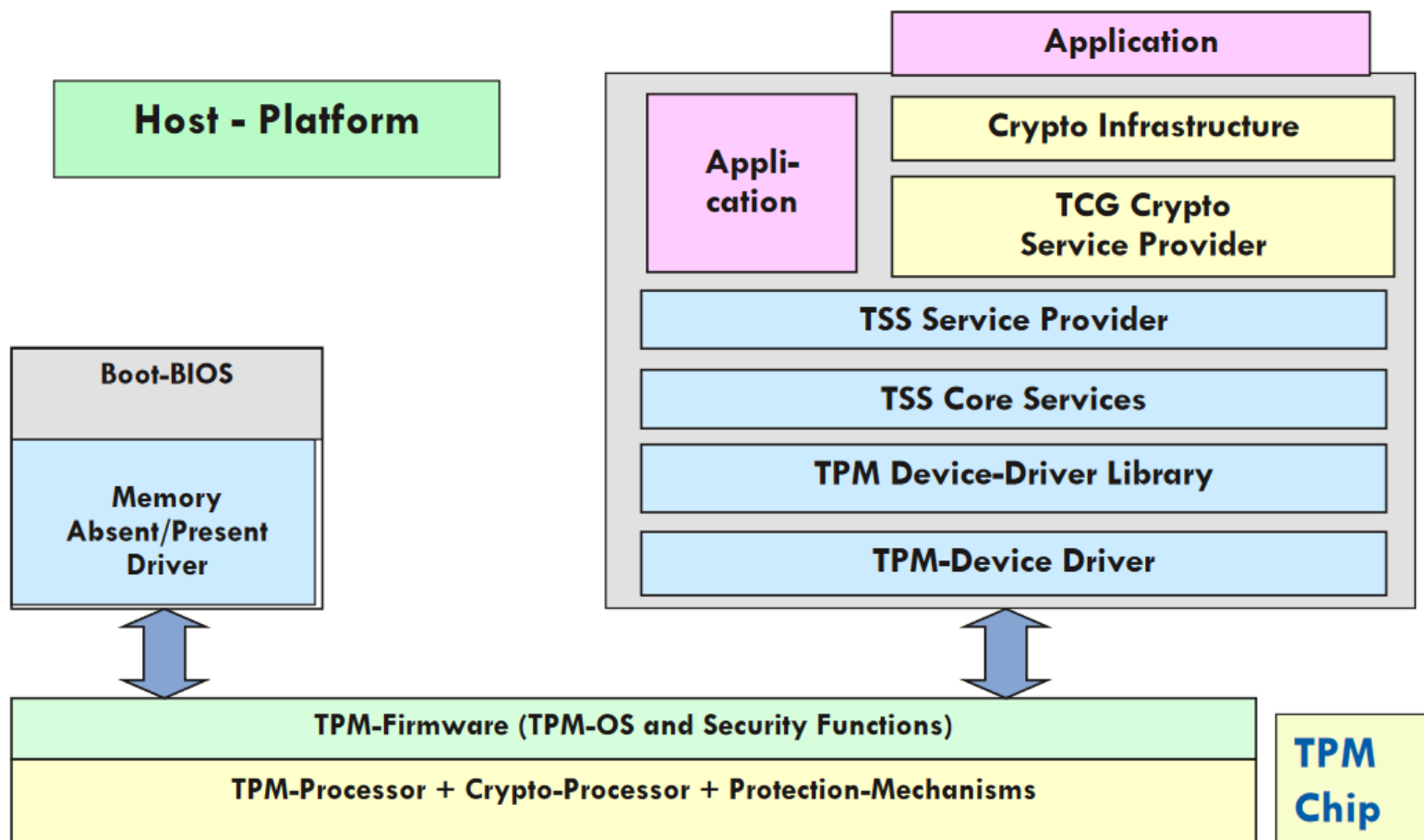
	TPM 1.2	TPM 2.0
Algorithms	SHA-1, RSA	Agile (such as SHA-1, SHA-256, RSA and Elliptic curve cryptography P256)
Crypto Primitives	RNG, SHA-1	RNG, RSA, SHA-1, SHA-256
Hierarchy	One (storage)	Three (platform, storage and endorsement)
Root Keys	One (SRK RSA-2048)	Multiple keys and algorithms per hierarchy
Authorization	HMAC, PCR, locality, physical presence	Password, HMAC, and policy (which covers HMAC, PCR, locality, and physical presence).
NV RAM	Unstructured data	Unstructured data, Counter, Bitmap, Extend

https://en.wikipedia.org/wiki/Trusted_Platform_Module

Security functions provided by TPM-based systems

- I. “Measured” boot with remote attestation
 - Provide signed log of what executed on platform (PCR)
- II. Storage of keys (disk encryption, private keys...)
 - Can be additionally password protected
- III. Binding and Sealing of data
 - Encryption key wrapped by concrete TPM’s public key
- IV. Platform integrity
 - Software will not start if current PCR value is not right

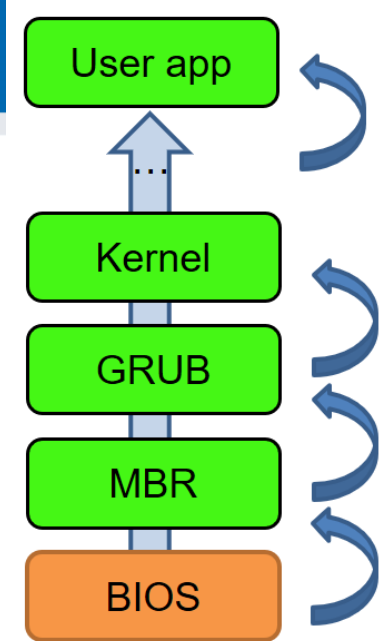
TPM Trusted Software Stack




Infineon, http://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf

TPM PCR

- Platform Configuration Register (PCR)
- Measurement cumulatively stored in PCR
 - measurement = $\text{SHA1}(\text{next block to execute})$
 - $\text{PCR}[i] = \text{SHA1}(\text{PCR}[i] \mid \text{new_measurement})$
 - Current block measure & store next before passing control
- PCR cannot be erased until reboot
 - Every part that was executed is stored
 - Possible to perform after-the-fact verification what executed
- Idea: boot what you want, but PCR will hold trace
- Multiple PCRs to support finer grained reporting



Remote attestation of platform state

- So you measured your boot. How to prove your state to remote party?
- Idea:
 1. Take current PCR values (stored inside TPM)
 2. Sign it by TPM's attestation private key (AIK), (all inside TPM)
 3. Send signed PCR values + TPMLog from computer to remote party
 4. Remote party holds public key and can verify signature => trust in authenticity of PCR values

Remote attestation of platform state

- Apps running on your computer measured in PCRs
- Your TPM contains unique Endorsement key
- You can generate Attestation key inside TPM (AIK)
 - And sign AIK by Endorsement key (inside TPM)
- You can sign your PCRs by AIK (inside TPM)
- Remote party can verify signature on AIK key
 - Using public key of Endorsement key
- Remote party can verify signature on PCRs
 - Using public key of AIK key
- Remote party now knows “what” you are running

Remote attestation

- Multiple PCRs to support finer grained reporting
 - not just single cumulative value
- Multiple PCRs available
 - BIOS, ROM, Memory Block Register [index 0-4]
 - OS loaders [5-7], Operating System [8-15]
 - Debug [16], Localities, Trusted OS [17-22]
 - Application specific [23]
- What is PCR measurement good for?
 - PCR content can be signed by TPM's private key and exported
 - List of applications claimed to be executed (=> PCR expected value can be recomputed by remote party)
 - => Remote attestation

Platform attestation – PCR registers

```

<PlatformAttestation size="30591">
  <Magic>PADS<!-- 0x53444150 --></Magic>
  <Platform>TPM_VERSION_12</Platform>
  <HeaderSize>28</HeaderSize>
  <PcrValues size="480">
    <PCR Index="0">8cb1a2e093cf41c1a726bab3e10bc1750180bbc5</PCR>
    <PCR Index="1">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
    <PCR Index="2">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
    <PCR Index="3">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
    <PCR Index="4">68fffb7e5c5f6e6461b3527a0694f41ebd07e4e1</PCR>
    <PCR Index="5">8e33d52190def152c9939e9dd9b0ea84da25d29b</PCR>
    <PCR Index="6">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
    <PCR Index="7">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
    <PCR Index="8">00000000000000000000000000000000000000000000</PCR>
    <PCR Index="9">00000000000000000000000000000000000000000000</PCR>
    <PCR Index="10">00000000000000000000000000000000000000000000</PCR>
    <PCR Index="11">b2a83b0ebf2f8374299a5b2bdfc31ea955ad7236</PCR>
    <PCR Index="12">7c84e69cd581eefd7ebe1406666711fd4fda8aa8</PCR>
    <PCR Index="13">01788a8a31f2dafcd9fe58c5a11701e187687d49</PCR>
    <PCR Index="14">26cda47f1db41bedc2c2b1e6c91311c98b4e2246</PCR>
    <PCR Index="15">00000000000000000000000000000000000000000000</PCR>
    <PCR Index="16">00000000000000000000000000000000000000000000</PCR>
    <PCR Index="17">ffffffffffffffffffffffffffffffffffffffffffffffff</PCR>
    <PCR Index="18">ffffffffffffffffffffffffffffffffffffffffffffffff</PCR>
    <PCR Index="19">ffffffffffffffffffffffffffffffffffffffffffffffff</PCR>
    <PCR Index="20">ffffffffffffffffffffffffffffffffffffffffffffffff</PCR>
    <PCR Index="21">ffffffffffffffffffffffffffffffffffffffffffffffff</PCR>
    <PCR Index="22">ffffffffffffffffffffffffffffffffffffffffffffffff</PCR>
    <PCR Index="23">00000000000000000000000000000000000000000000</PCR>
  </PcrValues>

```

TPM platform info

- Provides information about your platform state
- Included in PCR12 (Operating System information)

<PlatformCounters>

<OsBootCount>44</OsBootCount>

<OsResumeCount>2</OsResumeCount>

<CurrentBootCount>0</CurrentBootCount>

<CurrentEventCount>66</CurrentEventCount>

<CurrentCounterId>179136858</CurrentCounterId>

<InitialBootCount>0</InitialBootCount>

<InitialEventCount>64</InitialEventCount>

<InitialCounterId>179136858</InitialCounterId>

</PlatformAttestation>

Reboot =>

<PlatformCounters>

<OsBootCount>45</OsBootCount>

<OsResumeCount>0</OsResumeCount>

<CurrentBootCount>0</CurrentBootCount>

<CurrentEventCount>67</CurrentEventCount>

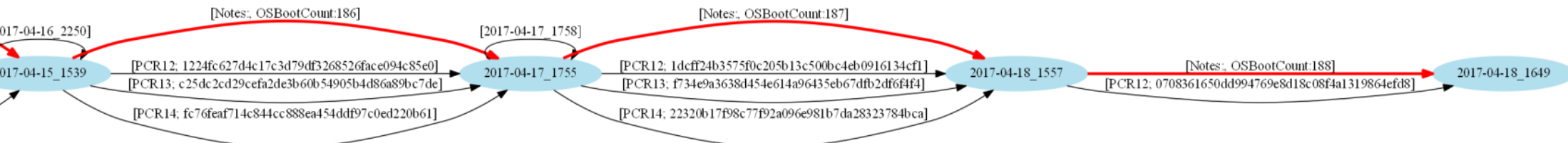
<CurrentCounterId>179136858</CurrentCounterId>

<InitialBootCount>0</InitialBootCount>

<InitialEventCount>67</InitialEventCount>

<InitialCounterId>179136858</InitialCounterId>

</PlatformAttestation>



TRUSTED BOOT – REAL IMPLEMENTATIONS



Verified boot - Chromium OS

- Starts with read-only part of firmware/BIOS (root of trust)
 - Cannot be forged, but also cannot be not updated
 - Contains permanently stored root RSA public key
- “Verified” boot strategy is used
 - Verifies that all executed code is from Chromium OS source tree
 - Code signatures verified by (shorter) keys signed by root key
 - speed tradeoff + possibility to update compromised keys
- Does not completely prevent user to boot other OSes
 - Developer mode turned on => signature on kernel not checked
 - TPM is used to provide mode reporting (normal/devel/recovery)
- <https://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot>
- <https://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot-crypto>



Chromium OS uses of TPM

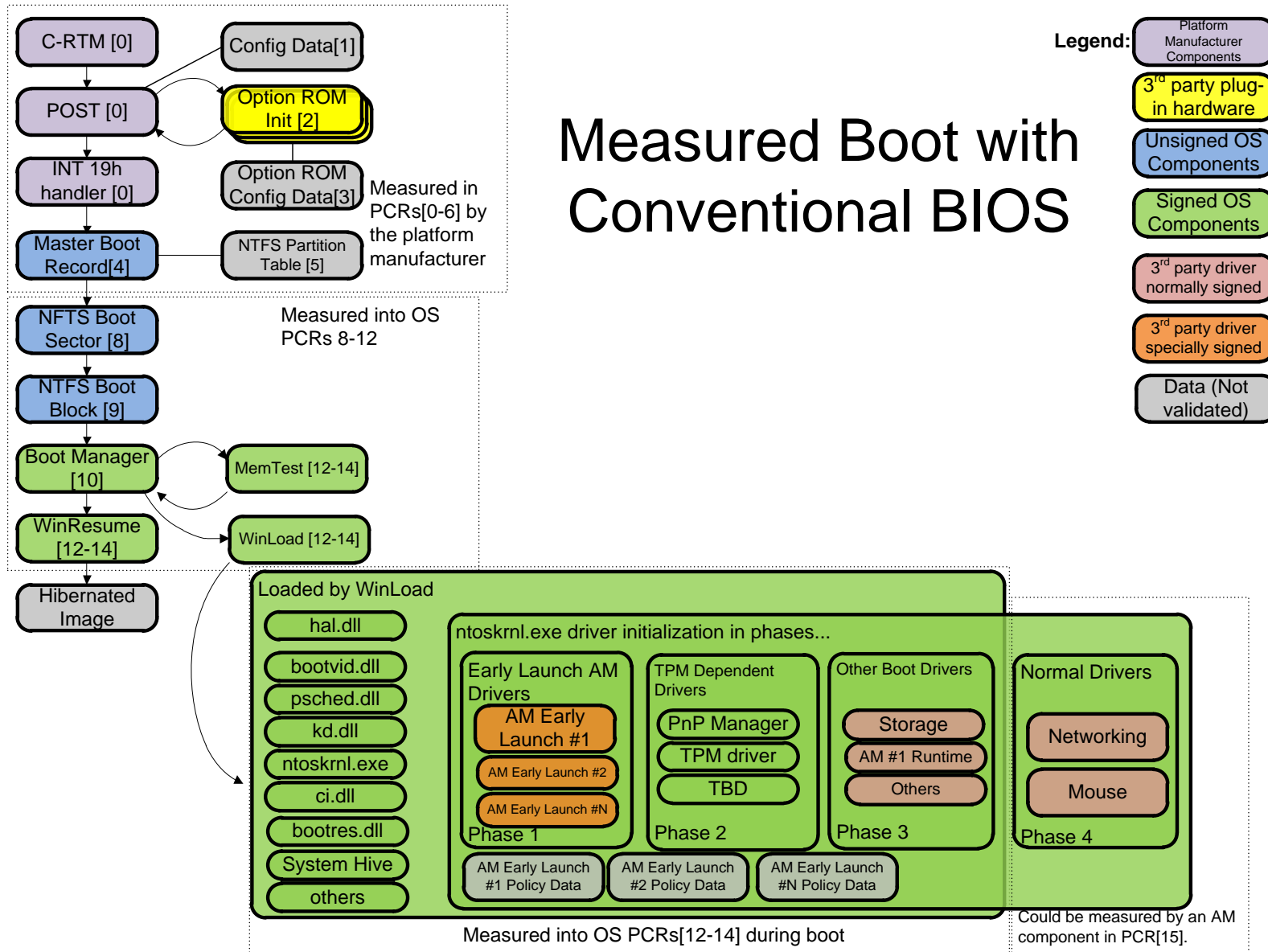
- Limited remote attestation (PCR[0] used)
 - to store developer and recovery mode switches
- Prevent rollback attack
 - Prevented by strictly increasing version of key & firmware
 - Version is written in TPM's NV RAM location, only read-only firmware can update this location
 - Key version prevents update to older (compromised) key
 - Firmware version prevents update to vulnerable firmware
- Store selected user's private keys (secure storage)
- Wrap selected disk encryption keys by TPM's system key
- <https://www.chromium.org/developers/design-documents/tpm-usage>

Secured and Trusted Boot

UEFI SECURE BOOT

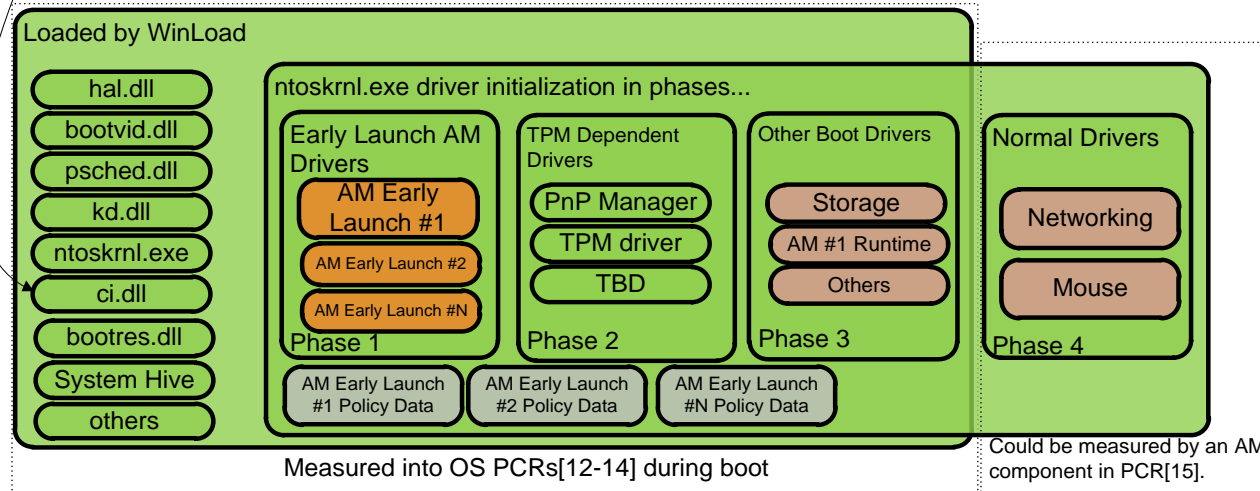
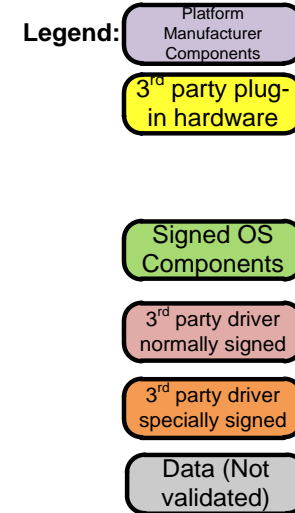
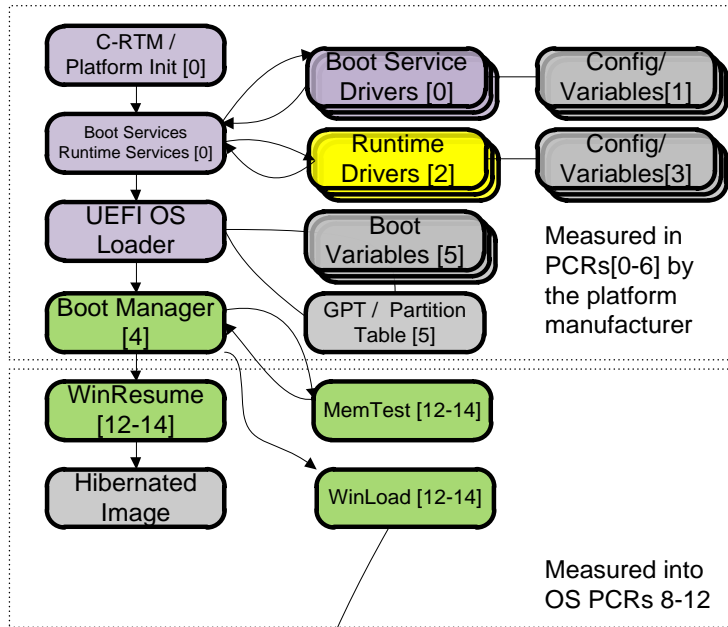
UEFI secure boot principles

- Platform key (RSA 2048b, PK) for authentication of platform owner
 - Key exchange keys (KEKs) for authentication of other components (drivers, OS components...)
1. “Setup” mode – platform key (PK) is not loaded yet
 - Everybody can write its own platform key (become owner)
 - Once PK is written, switch to “user” mode
 2. “User” mode
 - New keys (PKs, KEKs) can be written only if signed by PK
 - New software components loaded only if signed by KEKs



Microsoft, Secured Boot and Measured Boot: Hardening Early Boot Components Against Malware

Measured Boot with UEFI

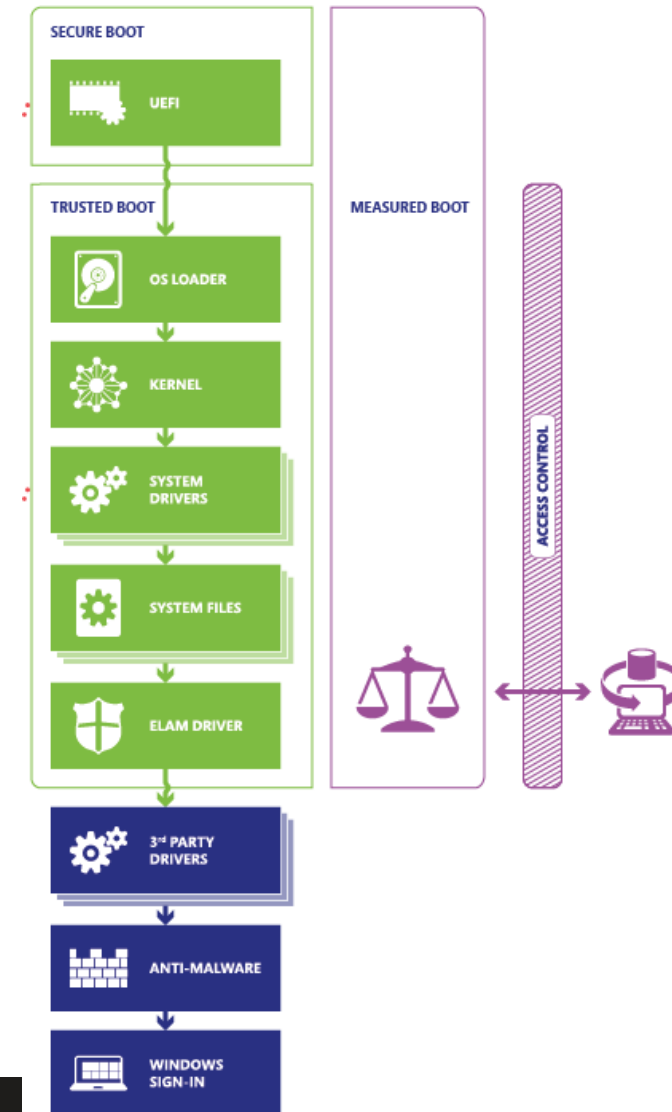


Secured and Trusted Boot

WINDOWS 8/10/11 TRUSTED BOOT

Windows 8/10 trusted boot

- Certified Windows 8/10/11 devices have trusted boot by default
 - “Verified” boot used (UEFI+OS sign)
 - “Measured” boot used (TPM)
- TPM PCRs used for measurements
- TPM used for keys protection
 - BitLocker disk encryption key
 - ROCA CVE-2017-15361 is relevant
 - If Infineon TPM used, patch!



Usage of TPM in BitLocker (disk encryption)

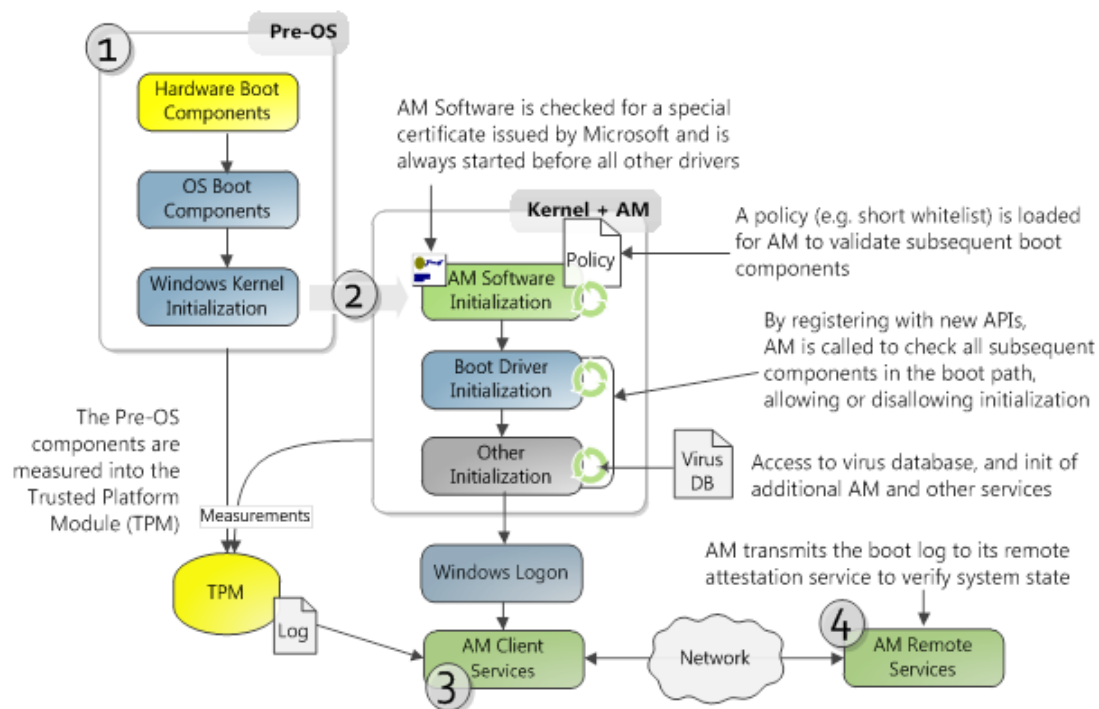
- Source of Volume Master Key (VMK)

Source	Identifies	Security	User Impact
TPM only	What it is	Protects against software attacks, but vulnerable to hardware attacks.	None
TPM + PIN	What it is + What you know	Adds protection against most hardware attacks as well.	User must enter PIN each boot
TPM + USB key	What it is + What you have	Fully protects against hardware attacks, but vulnerable to stolen USB key.	User must insert USB key each boot
TPM + USB key + PIN	What it is + What you have + What you know	Maximum level of protection.	User must enter PIN and insert USB key each boot
USB key only	What you have	Minimum level of protection for systems without TPM, but vulnerable to stolen key.	User must insert USB key each boot

M. Russinovich et. al., Windows Internals Part 2, 6th Edition

Windows 8/10 – secure boot process

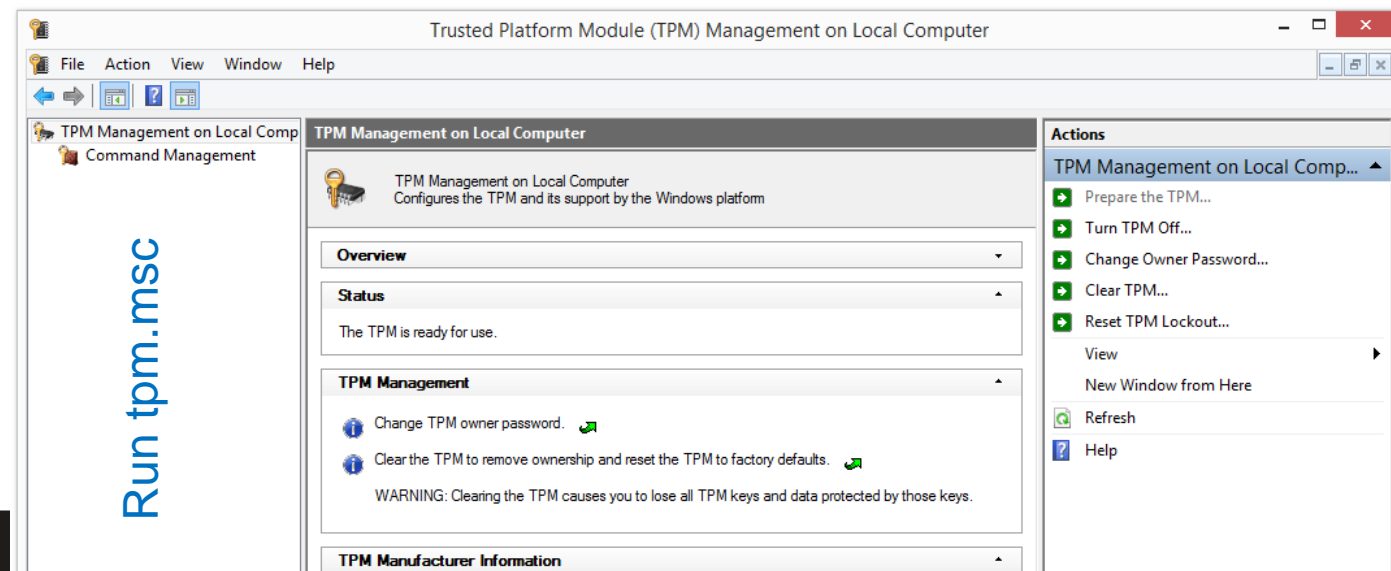
- Certified Windows 8/10 devices must have secure boot enabled by default



Microsoft, Secured Boot and Measured Boot: Hardening Early Boot Components Against Malware

TPM owner password

- You “own” TPM if you can set owner password
 - One owner password per single TPM
- Password set during TPM initialization phase
 - can be repeated, but content is erased
- Password protected storage of keys (Bitlocker...)



A configuration change was requested to clear this computer's TPM
(Trusted Platform Module)

WARNING: Clearing erases information stored on the TPM. You will
lose all created keys and access to data encrypted by these keys.

Press YES to clear the TPM

Press NO to reject this change request and continue

Do you accept the change?

[Yes]

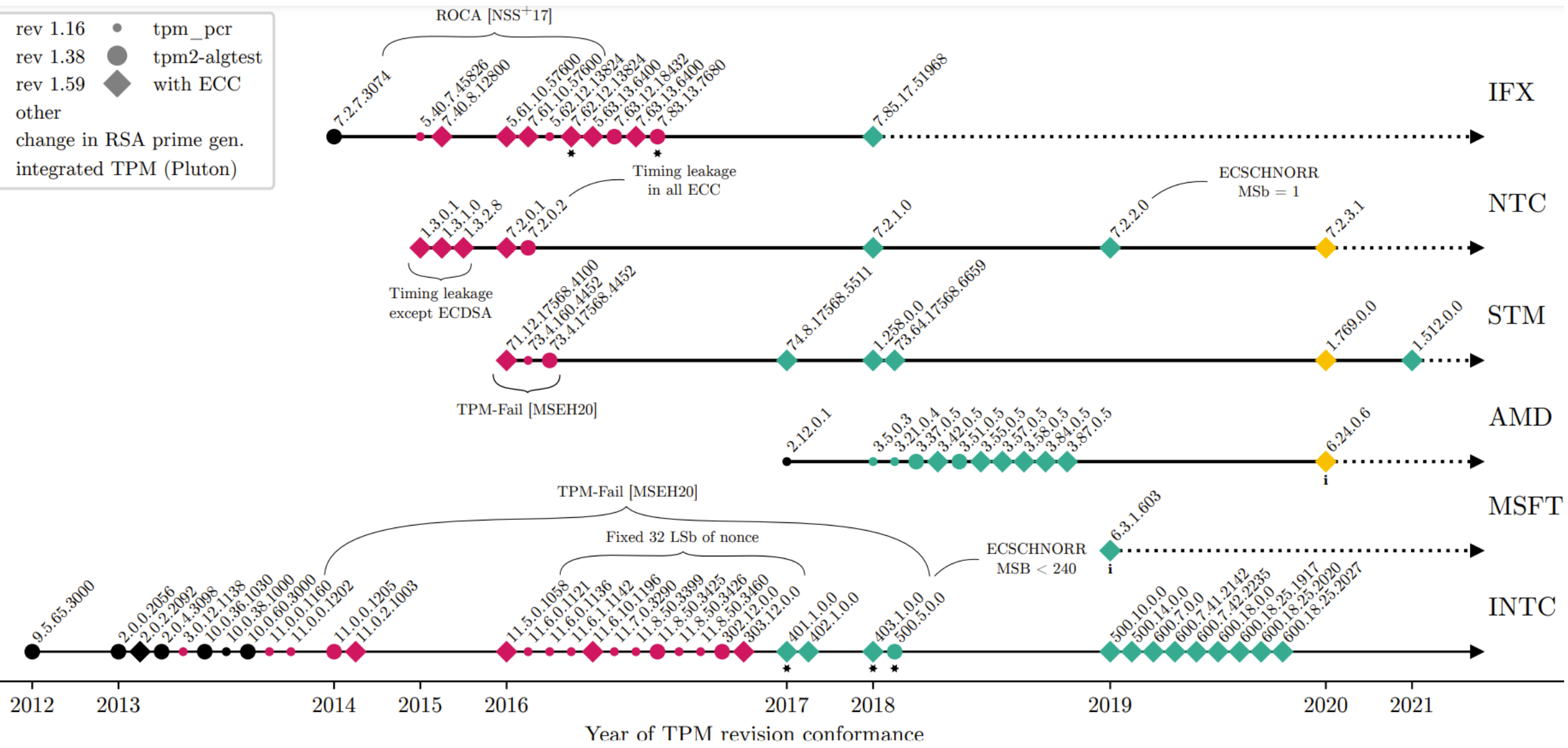
[No]

ATTACKS AGAINST TPM

Attacks against systems with TPM

- Physical attacks
 - Sniffing, side-channels, fault induction...
- Design/reference implementation weaknesses
 - Buffer overflow in packet handling [2023], updated specification January 2024
 - *“Revision 98 Added parameter to MemoryMove(), MemoryCopy(), and MemoryConcat() to make sure that the data being moved will fit into the receiving buffer.”*
- Attacks against cryptographic implementations
 - ROCA [2017, CRoCS], RSA factorization (Infineon)
 - TPM-Fail vulnerability [2020], ECDSA nonce timing dependency (STM, Intel)
 - TPMScan vulnerabilities [2024, CRoCS]
 - Fixed low 4 bytes of ECDSA nonce, (older Intel fTPM)
 - TPM-Fail-like nonce timing in other algorithm than ECDSA (Nuvoton)

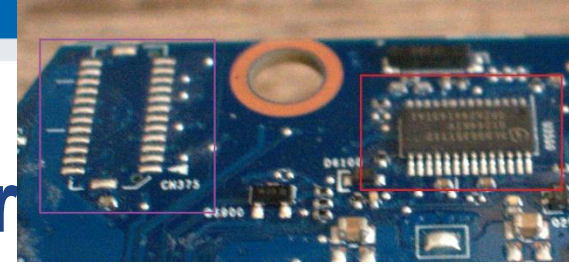
- rev 1.16
- rev 1.38
- rev 1.59
- other
- tpm_pcr
- tpm2-algtest
- ◆ with ECC
- ◆ with ECC
- ★ change in RSA prime gen.
- i** integrated TPM (Pluton)



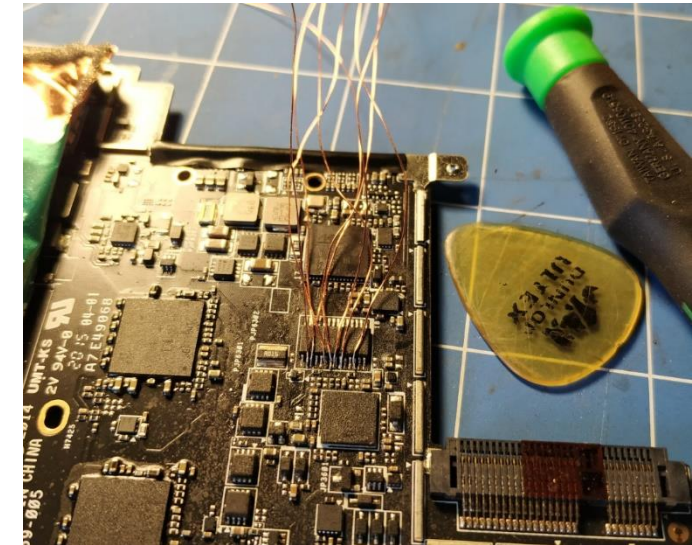
Research paper

- Paper written by CROCS and NUKIB [CHES'24]
 - https://crocs.fi.muni.cz/papers/tpm_ches2024
- Several ECC nonce-related vulnerabilities discovered
 - Known vulnerabilities by TPM-Fail (2019) – Intel, STM, Nuvoton
 - Few topmost bits leaked via timing, ~1000s signatures to recover key
 - Previously unreported vulnerabilities in ECSCHNORR and ECDAEA
 - inconsistent testing and reporting
- New serious vulnerability in older Intel fTPMs 11.5.0.1058-303.12.0.0
 - Lowest bytes of nonces of ECDSA and ECSCHNORR fixed to 0x00000001
 - Only nine signatures required to extract private key, no need for active observation
 - Fixed in 400.x versions, but not publicly disclosed

Attack: Sniffing commands/keys for BitLocker



- Nice writeup how to sniff BitLocker key when send from TPM to OS, then decrypt disk image
 - <https://pulsesecurity.co.nz/articles/TPM-sniffing>
- fTPM and iTPM does not have exposed bus



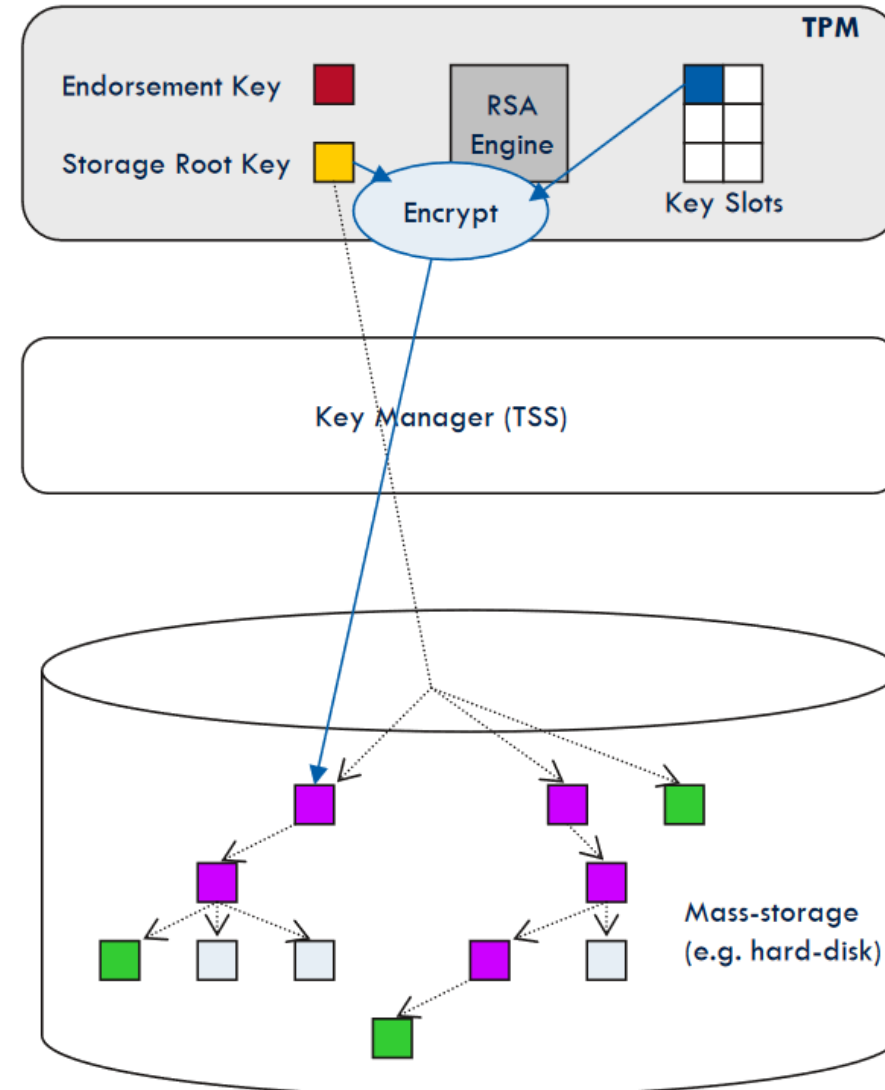
BASIC COMPONENTS

TPM keys

- Endorsement key (EK)
 - Generated during manufacturing, permanent
 - Remain in TPM device during whole chip lifetime
- TPM Storage Root Key (SRK)
 - Generated by use after taking ownership
 - New Storage root key can be generated after TPM clear
 - Used to protect TPM keys created by application
- Various delegate keys
 - Separate keys signed/wrapped by EK, SRK...
 - Application can generate and store own keys
 - Good practice: do not have single key for everything

TPM storage keys

- Application keys encrypted under SRK
- Exported as protected blob
- Stored on mass-storage
- If needed, decrypted back and placed into slot
- Key usable until removed



http://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdf

TPM policy

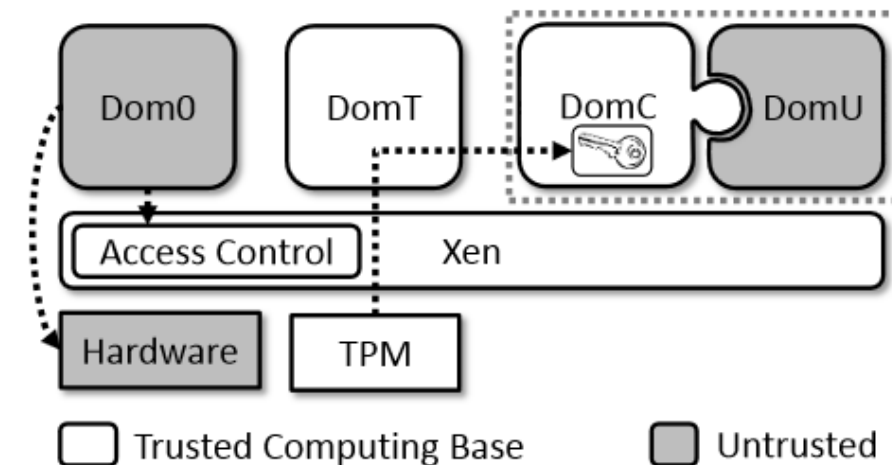
- TPM releases secret only when PCR contains particular value
- Enforcement even in measured-only mode
 - Key is not released if unexpected component was started (started => is included in measurements)
- Conditions can use ANDs and ORs
- How to handle policy updates?
 - Change policy of state only from already valid state

Programming with TPM

- The TPM Software Stack from Microsoft Research (C++, Java, C#, Python)
 - <https://github.com/Microsoft/TSS.MSR>
- tpm2-tools
 - Open-source TPM stack for Linux and Windows
 - <https://github.com/tpm2-software/tpm2-tools>

Usage of TPM in cloud-computing

- Combination of virtualization and trusted computing
 - Modified Xen hypervisor used to make standard TPM available for secret-less virtual machine
 - Results in significant decrease in the size of trusted computational base (TCB)
- Several different implementations
 - E.g., Red Hat keylime <https://github.com/keylime/>



<http://bleikertz.com/research/acns2013.pdf>

DYNAMIC ROOT OF TRUST

Static Root of Trust Measurement (SRTM)

- Start trusted immutable piece of firmware
 - E.g., BIOS loader or Intel Boot Guard
- Initiates measurement process
 - Integrity of every next component is added to TPM's PCRs
 - Start → BIOS → PCI EEPROM → MBR → OS ...
- But do we need to start (trusted boot) only after reboot?
 - Takes relatively long time
 - Can we execute the same process, but dynamically?
 - Can we exclude long chain (BIOS, PCI...)?
 - Long chain => large Trusted Computing Base (TCB)!

Dynamic Root Trust Measurement (DRTM)

- Launch of measured environment at any time
 - “Late lunch” option
 - No need to reset whole platform
 - Can be also terminated after some time
- Measurement process similar to static root of trust
 - Application trust chain executed from dynamic root
- Implementation of DRTM
 - Intel’s TXT (not used much in practice, server CPUs typically)
 - Intel’s SGX (all Skylake processors and newer, from 2015)

Intel's Trusted Execution Technology

- Intel's TXT uses a processor-based root of trust
 - Option given in TCG specifications
- Goal: shorten chain of trust
 - Run specific program in verified/trusted chain without restart
- Goal: provide independent root of trust (CPU-based)
 - Processor isolates memory of Measured Launched Environment (MLE) from other processes
- Intel's TXT still uses TPM to store measurements
- <http://www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf>
- Outdated, abounded in favor of SGX

Intel's TXT issues

1. TXT still relies on BIOS provided code (SMM)
 - TXT-started chain can be compromised by forged BIOS
 - Hard to patch (design decision, not implementation bug)
 - Proposed defence by hardening and sandboxing SMM
2. Bugs in TXT implementation
 - Memory corruption, misconfiguring VT-d ...
 - Can be fixed after discovery
3. Bugs in processing residual state of pre-TXT lunch
 - Maliciously modified ACPI tables
 - Can be fixed after discovery

tboot – open-source implementation

- Pre-kernel/VMM module
- Based on Intel's Trusted Execution Technology
- Performs a measured and verified launch of an OS kernel/VMM
- <http://sourceforge.net/projects/tboot/>

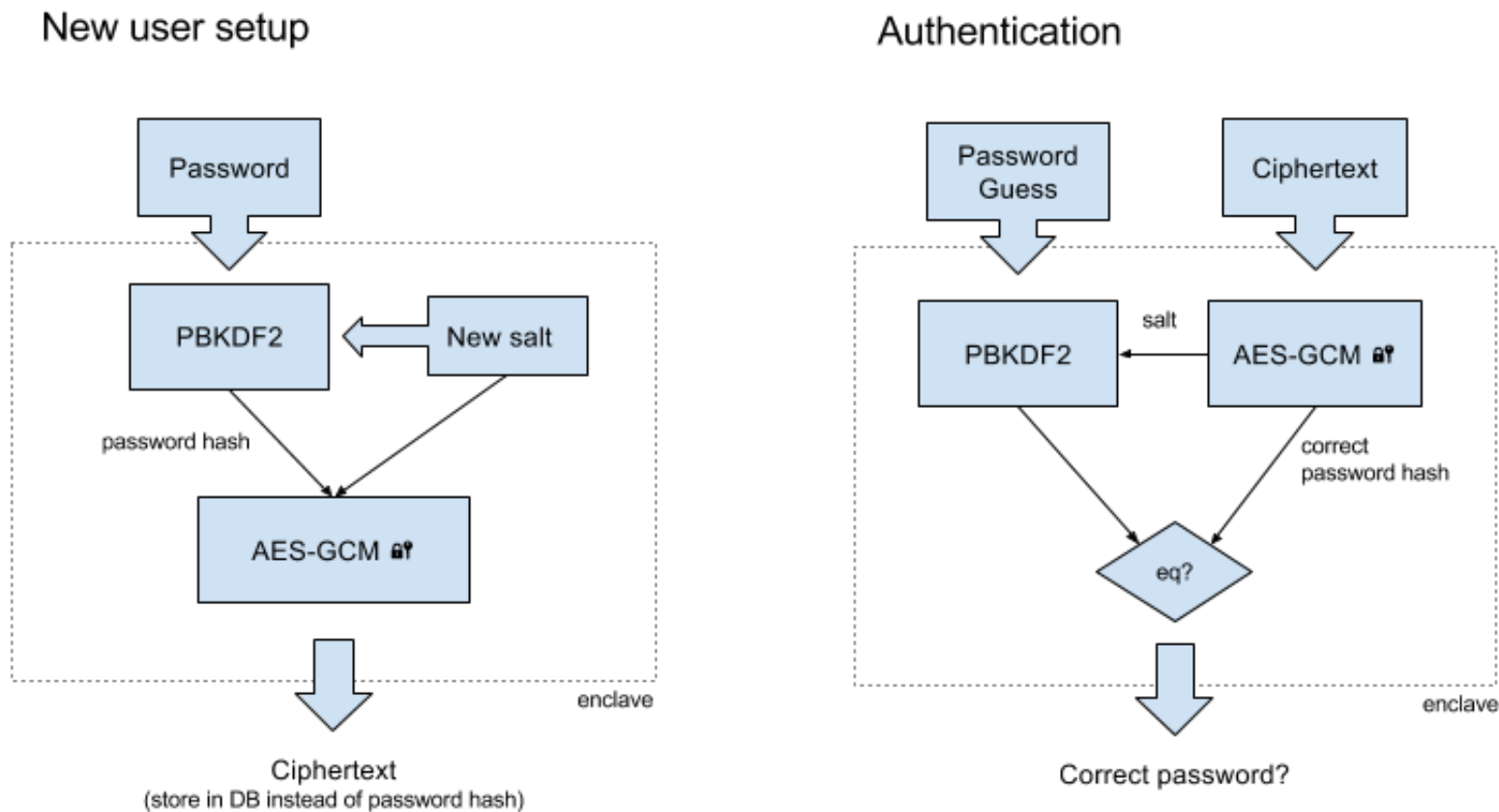
Intel's SGX : Security enclave

- Intel's Software Guard Extension (SGX)
 - New set of CPU instructions intended for future cloud server CPUs
- Protection against privileged attacker
 - Server admin with physical access, privileged malware
- Application requests private region of code and data
 - Security enclave (4KB for heap, stack, code)
 - Encrypted enclave is stored in main RAM memory, decrypted only inside CPU
 - Access from outside enclave is prevented on CPU level
 - Code for enclave is distributed as part of application
- Trusted Computing Base significantly limited! 😊
 - But proprietary Intel code inside CPU ☹️

Intel's SGX – some details

- EGETKEY instruction generates new enclave key
 - SGX security version numbers
 - Device ID (unique number of CPU)
 - Owner epoch – additional entropy from user
- EREPORT instruction generates signed report
 - Local/remote attestation of target platform
- Debugging possible if application opt in
- Enclave cannot be emulated by VM

SGX hardened password verification



<https://jbp.io/2016/01/17/using-sgx-to-hash-passwords/>

Intel SGX is/was very active research area

- Many small enclaves to cover whole program
 - User-annotated code split into many enclaves (“microns”)
 - Secure interaction between microns (attest, auth. encryption)
 - Tor, H2O, FreeTDS and OpenSSL successfully transformed
 - 2685, 154, 473 and 307 LOC changes required respectively
 - TCB only 20KLOC, PANOPLY specific overhead 24%
- Memory randomization of code inside enclave
 - SGX program modified with custom LLVM compiler
 - Added in-enclave loader for ASLR & swDEP (2703 LOC)
 - Code&data split into 32/64B units randomized separately
- Full library OS based on SGX (Haven, Graphene-SGX)

Recent attacks against SGX

- SGX is not a silver bullet
- Vulnerable to side-channels
 - Attacker with physical access explicitly excluded from attacker model
 - Impacted by Spectre attack (2017)
 - <https://github.com/llds/spectre-attack-sgx>
 - <https://github.com/osusecLab/SgxPectre>
 - Impacted by Foreshadow attack (CVE-2018-3615) <https://foreshadowattack.eu/>
 - Reading out attestation private key
- Bugs of enclave code are still problem (developer)
- Not everything is running inside enclave (other code, user input...)

Programming with Intel's SGX

- Intel SGX SDK
 - <https://software.intel.com/en-us/sgx-sdk>
 - 6th generation core processor (or later) based platform with SGX enabled BIOS support
- Example: Hardened password hashing
 - <https://jbp.io/2016/01/17/using-sgx-to-hash-passwords/>
 - <https://github.com/ctz/sgx-pwencclave>
- More SGX info
 - <http://theinvisiblethings.blogspot.cz/2013/08/thoughts-on-intels-upcoming-software.html>
 - <http://theinvisiblethings.blogspot.cz/2013/09/thoughts-on-intels-upcoming-software.html>

Intel SGX deprecated on non-server CPUs (end 2021)

- Intel deprecated technology for the newest non-server CPUs
 - Still present in server CPUs, utilized by Azure confidential computing...
- Not completely clear reasons so far
 - Possibly mix of many past attacks which cannot be fixed without changing the architecture significantly (and breaking compatibility)
- <https://community.intel.com/t5/Intel-Software-Guard-Extensions/Intel-SGX-deprecated-in-11th-Gen-processors/m-p/1351848>
- <https://edc.intel.com/content/www/us/en/design/ipla/software-development-platforms/client/platforms/alder-lake-desktop/12th-generation-intel-core-processors-datasheet-volume-1-of-2/001/deprecated-technologies/>

TRUSTED COMPUTING - CRITIQUE

Trusted Computing (TC) - controversy

- For whom is your computer trusted?
 - Secure against you as an owner?
- Is TC preventing users to run code of their choice?
 - Custom OS distribution?
 - Open OEM system – locked on first installation
 - Physical switch to unlock later
- Why some people from *Trusted Computing* consortium think that Trustworthy Computing might be better title?

Trusted computing - controversy

- R. Anderson, 'Trusted Computing' FAQ (2003)
 - <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>
- J. Edge, UEFI and "secure boot"
 - <http://lwn.net/Articles/447381/>
- R. Stallman, Can You Trust Your Computer?
 - <https://www.gnu.org/philosophy/can-you-trust.html>
- Selected problems addressed in current designs

Quo Vadis, TPM?

- ~2004: Started with primarily aim at DRM enforcement (TPM 1.2)
 - Some adoption, but also controversy, unclear future
- ~2013: TPM 2.0 significantly renewed interest and scope of use
 - Wide hardware support via certified dTPMs (Infineon, Nuvoton, STM) and non-certified fTPMs (Intel, AMD)
 - Microsoft Windows 11 requires TPM presence (measured boot, Bitlocker)
 - Linux systemd rapidly adds measured boot https://systemd.io/TPM2_PCR_MEASUREMENTS/
- ~2017: Support for TPM-based functions more common
- ~2022: Pluton chip (Microsoft + AMD & Qualcomm), iTPM
 - iTPM implementation (certification in progress), difficult to sniff TPM bus
 - Directly updatable via Windows Update

Summary

- Two principal solutions for trusted boot
 - Verified boot (signatures) and Measured boot (PCR+RA)
- Start from clean (and trusted) point
 - Allow only intended software to run
 - Or prove what actually executed
- Additional hardware inside motherboard / CPU provides wide range of new possibilities (TPM)
- Size of Trusted Computing Base matters (TPM/SGX)
- Controversy about implication of trusted boot
 - Who owns and control target platform