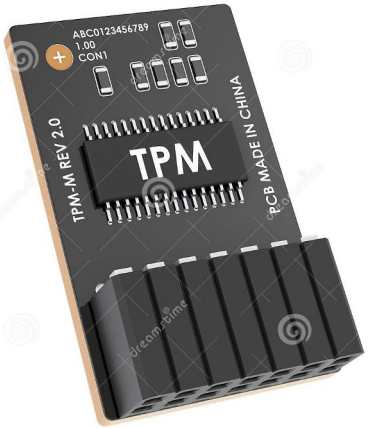
Trusted Platform Modules

By Haitham Al Eryani and Chirayu Agarwal

What is a Trusted Platform Module - C

Trusted Platform Module(TPM) is a computer chip(microcontroller) which helps to perform:-
cryptographic functions
provides security and privacy
generating and storing encryption keys

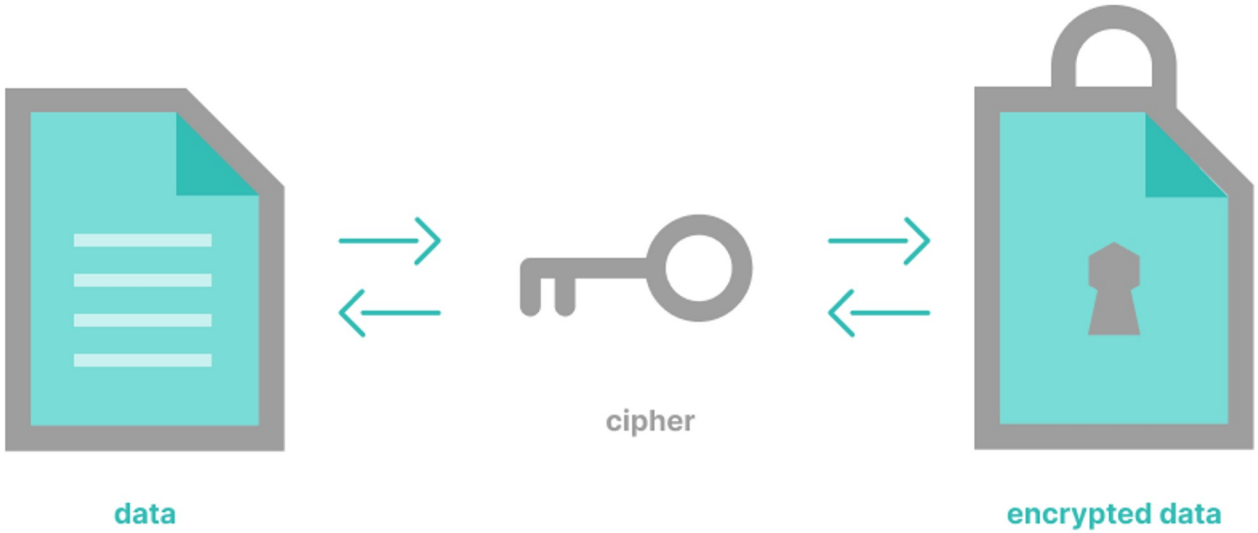


It is hardware based security so it cannot be easily tampered.

Trusted Computing Group (TCG) created TPM in 2003.
The current version is TPM 2.0, which is standardized under ISO/IEC 11889.

There are two main iterations of the TPM technology TPM 1.2 which supported RSA and SHA1 (which has later proven to be vulnerable) and TPM 2.0 which supports ECC and SHA256.

Function 1 - Shieldied Key Handling - C



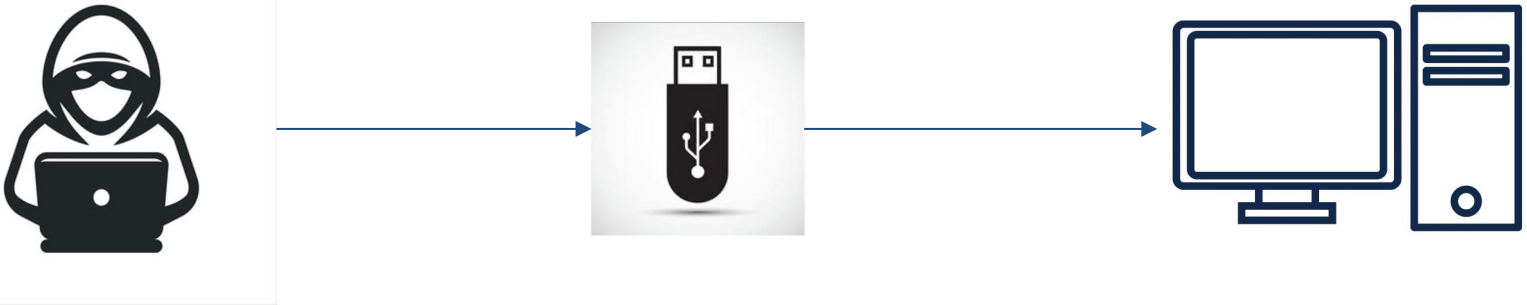
Function 1 - Shieldied Key Handling(Contd.)

TPM has it's own encryption key called **Storage Root Key.**
This key cannot be taken out of the TPM.

We have to provide the key to be encrypted to TPM.
It encrypts it using the storage root key.
This key can now be stored anywhere in the system or it can be stored in the TPM itself.
It can only be decrypted by TPM.

Every TPM consists of a different key.
The TPM which has encrypted the key can only decrypt it.

Function 2 - Measurement - C



Tells TPM to decrypt the encrypted key

Function 2 - Measurement - C

During the booting process of the computer,TPM checks the state of the computer and the state of the computer's environment. If the computer is in a trustworthy state (i.e. it has not been tampered with), it will operate normally. If not, it will not boot, meaning there is no way to access or extract any data from the computer.**It does so by comparing the current hash value with the last well known state hash value.**

Things that would trigger an untrustworthy state include:

- the computer hard drive has been placed into another computer (this is done to bypass or deactivate a password protected log-in),
- the computer is being booted and accessed remotely from an unauthorized source,
- the computer has been attacked by a software virus
- someone is using a brute-force attack to access the computer.

Function 3 - Attestation - H

- Verify data received is protected by a TPM.
- Verify the identity of the TPM that is providing us with data.

- Verification is done by a third party CA

- The attestation process involves two keys
  - Endorsement Key
  - Attestation Key
- Why do we have two keys?

Ultimate Goal = Proving that the EK and the AK are associated

Applications That Rely On TPMs - H

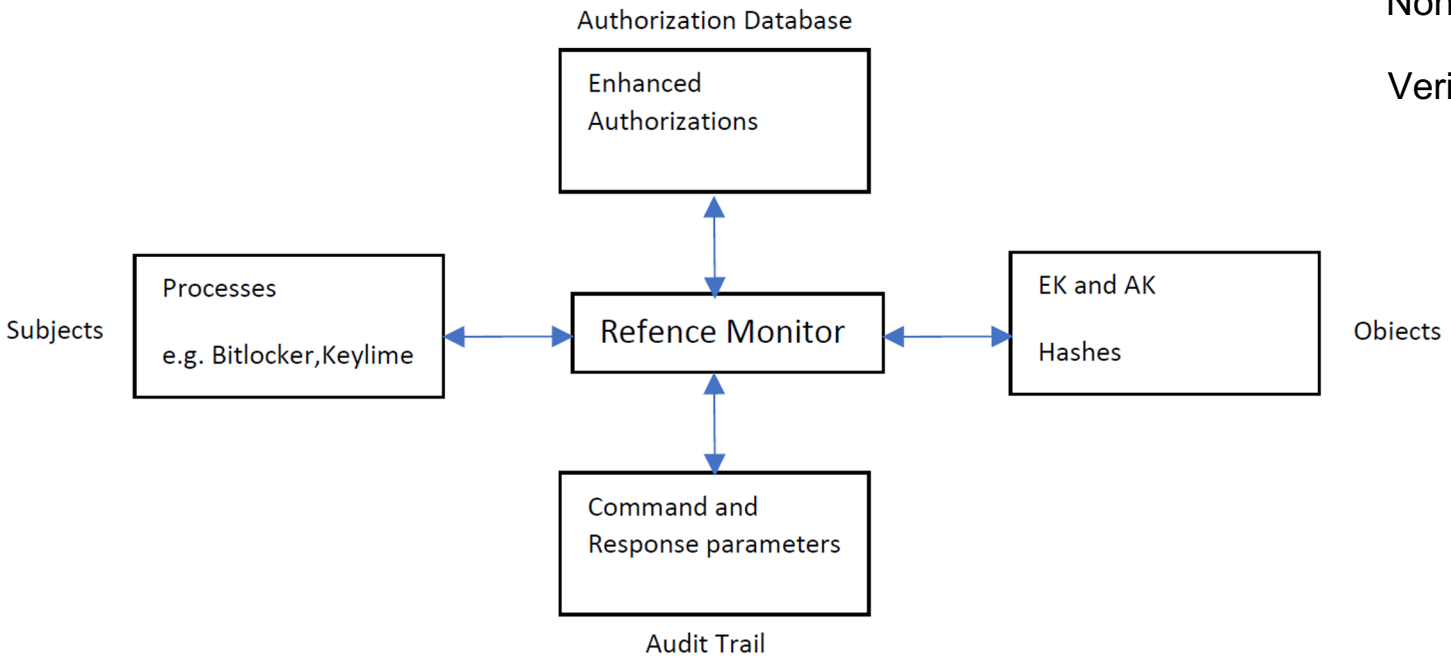
- Digital Right Management (DRM)
- Windows BitLocker
- Windows Defender Credential Guard
- Keylime

TPMs And The Reference Monitor - H

Tamper Proof

Non-Bypassable

Verifiable



TPMs And The Reference Monitor (Cont) - H

Tamper Proof - Protected from unauthorized alteration

Non-Bypassable - A subjects access to an object is controlled
Enhance Authorization

Verifiable - Do TPMs perform their function?
EAL4
Timing Attacks (FTPM on Intel Machines and STmicro T

TPM 2.0 PP Assurance leve

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

1

Augmentations -> EAL4+

Bibliography

Slide 3 - https://bit.ly/3QhHkZy
Slide 4 - https://bit.ly/3cKIj79
Slide 5 - https://bit.ly/3L1AdUt
Slide 7 - https://bit.ly/3QiKAEj
Slide 7 - https://bit.ly/3AQlCWW
Slide 9 - https://bit.ly/3enCw83
Slide 10 -https://bit.ly/3ehHovb
Slide 10 - https://bit.ly/3CXthp6
Slide 10 - https://bit.ly/3RoNbhq
Slide 10 - https://bit.ly/3KKsCJD