NAVAL GROUP

POWER AT SEA

INTRODUCTION AUX TRUSTED PLATFORM MODULES (TPMs)

Julien FRANCQ

Naval Cyber Laboratory

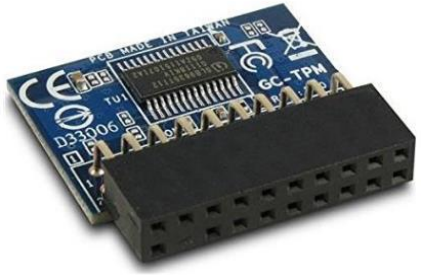
29/08/2020

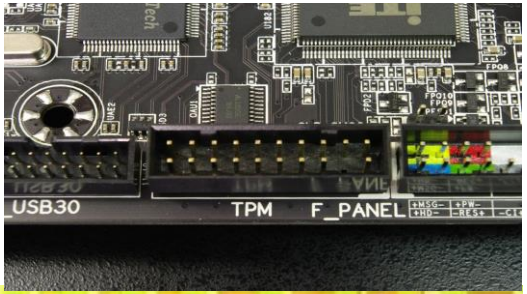
SOMMAIRE

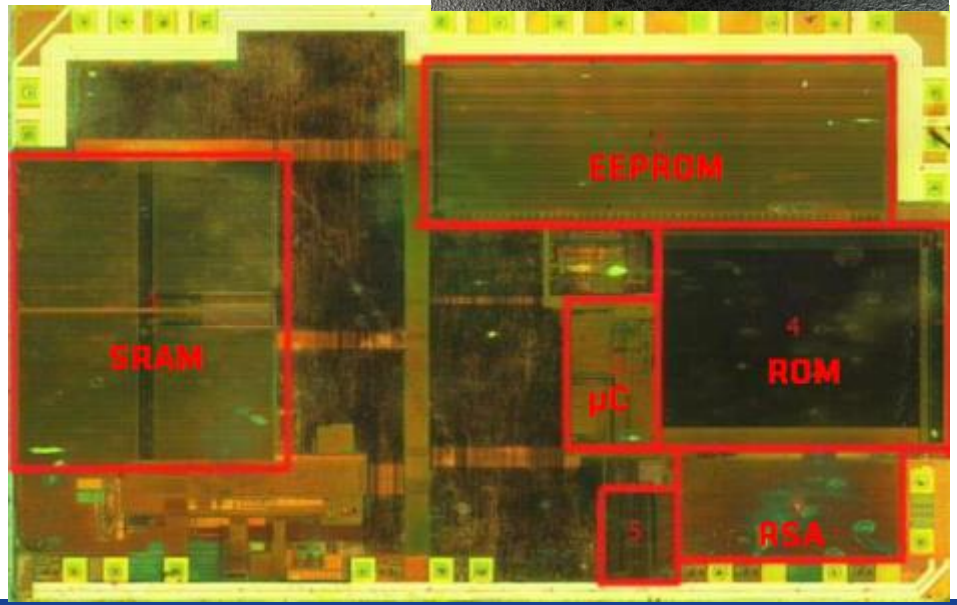
C’EST QUOI UN TPM ?

LES TPMs EN UNE SLIDE

- Composant du Trusted Computing
- Co-processeur cryptographique
- Gère des clés cryptographiques
- Contient des registres d'intégrité (Platform Configuration Registers, PCRs)
- Protégé contre les attaques physiques
- Enfoui au sein de la plateforme
- Composant passif

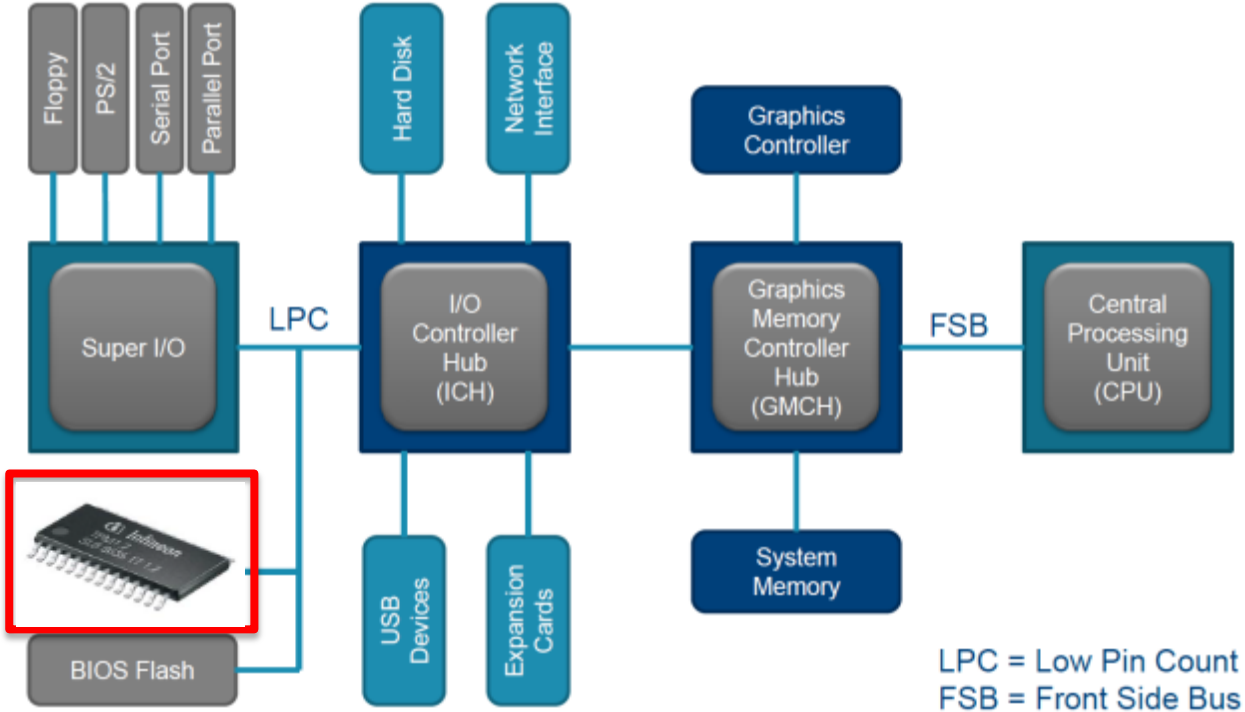






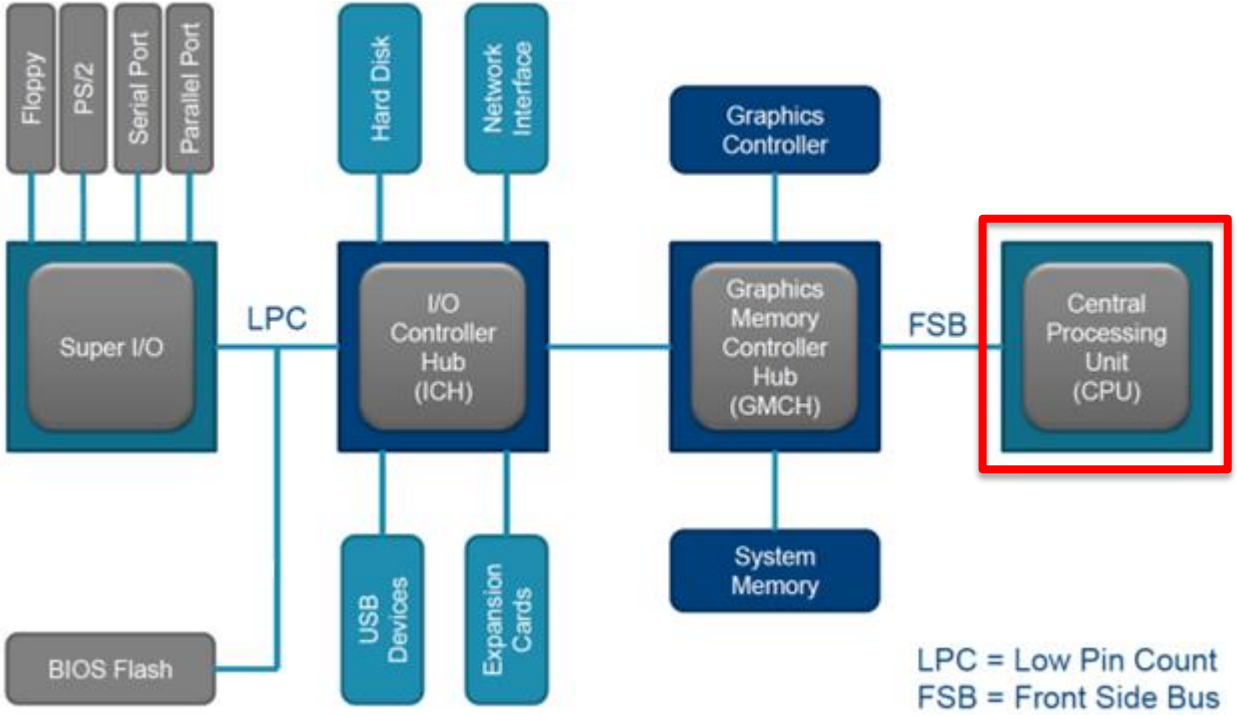
INTEGRATION D'UN TPM DANS UN PC

- TPM discret (dTPM) intégré dans la carte mère et disponible avant le boot de la machine



INTEGRATION D'UN TPM DANS UN PC

- Firmware TPM (fTPM) s'exécutant dans la zone de confiance du CPU
  - Trusted Execution Environment (TEE)



CHRONOLOGIE DU TPM

- 1999 : Trusted Computing Platform Appliance (TCPA) fondée par Compaq, HP, IBM, Intel, Microsoft (remplacé par le Trusted Computing Group - TCG)
- 2002 : spécifications du TPM 1.1b publiées
- 2003 : spécifications du TPM 1.2 publiées
- 01/2007 : TPM supporté par le logiciel de chiffrement de disque BitLocker sur Windows Vista
- 07/2007 : standard Mobile Trusted Module (MTM) 1.0 publié
- 03/2013 : spécifications du TPM 2.0 publiées
- Aujourd'hui : les TPMs sont présents sur la plupart des PCs et serveurs, et croissance soutenue (automobile, smart grids, Industrie 4.0, IoT, etc.)

FONCTIONNALITÉS DU TPM

- Authenticated/Measured/Trusted Boot
  - Logging des mesures de la séquence de boot
- Remote Attestation
  - Rapport de la séquence de boot à un tiers
- Gestion des clés cryptographiques
  - Contrôler l'usage et l'accès aux clés
  - Stockage scellé (sealing) : accès restreint aux clés suivant l'état de la plateforme
- Gestion des utilisateurs
  - Equilibre de l'intérêt des différentes parties (propriétaire de la plateforme, respect de la privacy des utilisateurs, etc.)
- Autres fonctionnalités
  - Générateur de nombres aléatoires, horloge, compteurs, etc.

MESURES ET PCRs

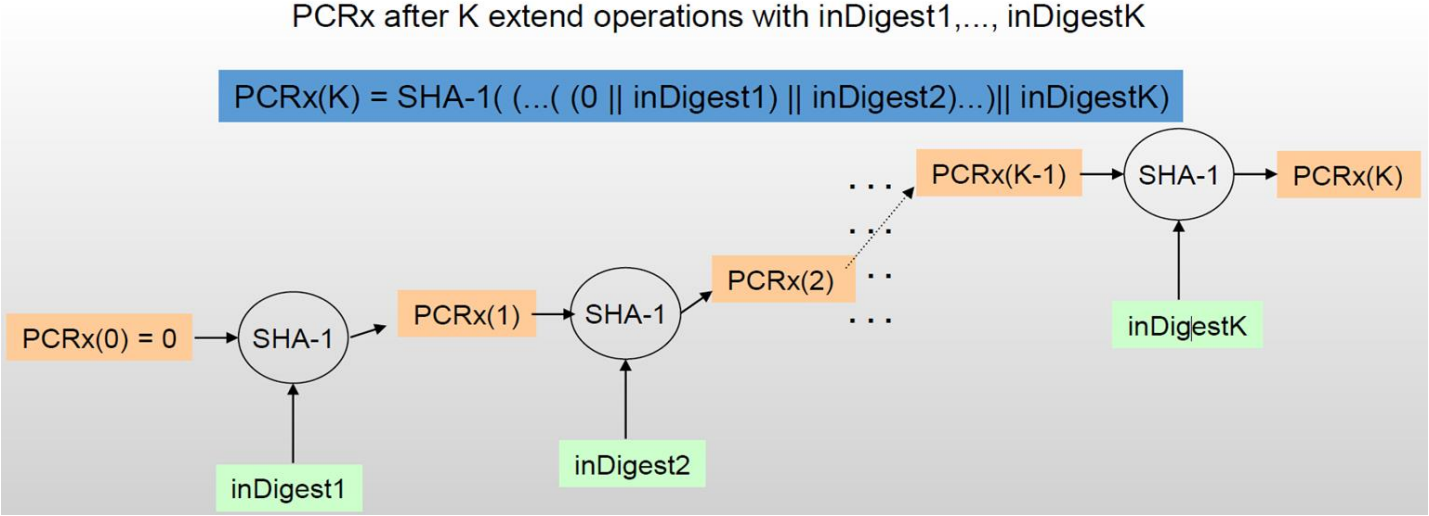
- Les PCRs stockent des mesures de manière sécurisée dans le TPM
  - 16/24 PCRs obligatoires dans les TPMs 1.2/2.0
  - Chacun contient 160/256 bits correspondant à un haché par SHA-1/256
  - Mapping des PCRs standard
  - Chaque PCR peut contenir en pratique un nombre illimité de mesures via des chaînes de hachage

- 2 types de PCRs :
  - Statiques : PCRs 1...16
  - Dynamiques : PCRs 17...24

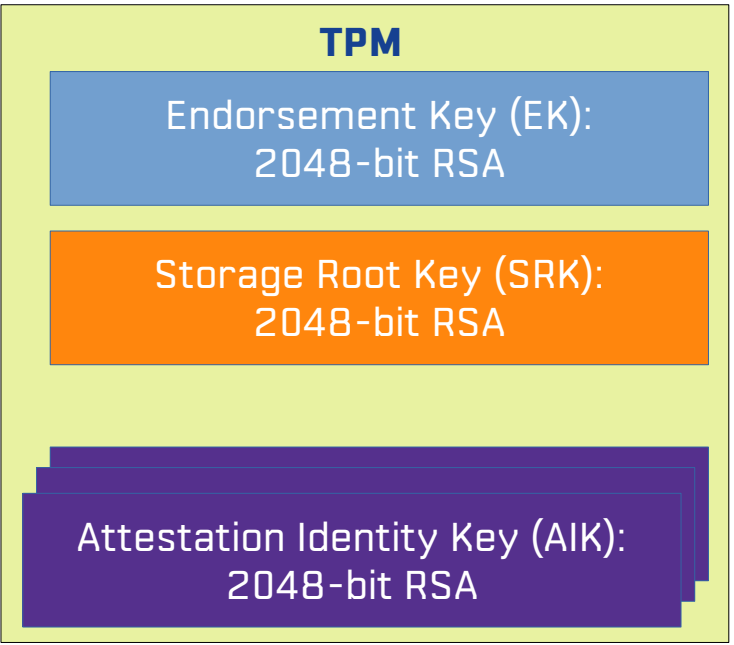
CHAINES DE HACHAGE

- PCRs initialisés au Reset Système
- PCRs peuvent seulement être « étendus » par 20/32 octets de données additionnelles inDigest dans une itération de SHA
- TPM2_PCR_Extend(PCR_{old}, inDigest) :

$$PCR_{new} = SHA(PCR_{old} \,||\, inDigest)$$



TPM : CLÉS ET CERTIFICATS

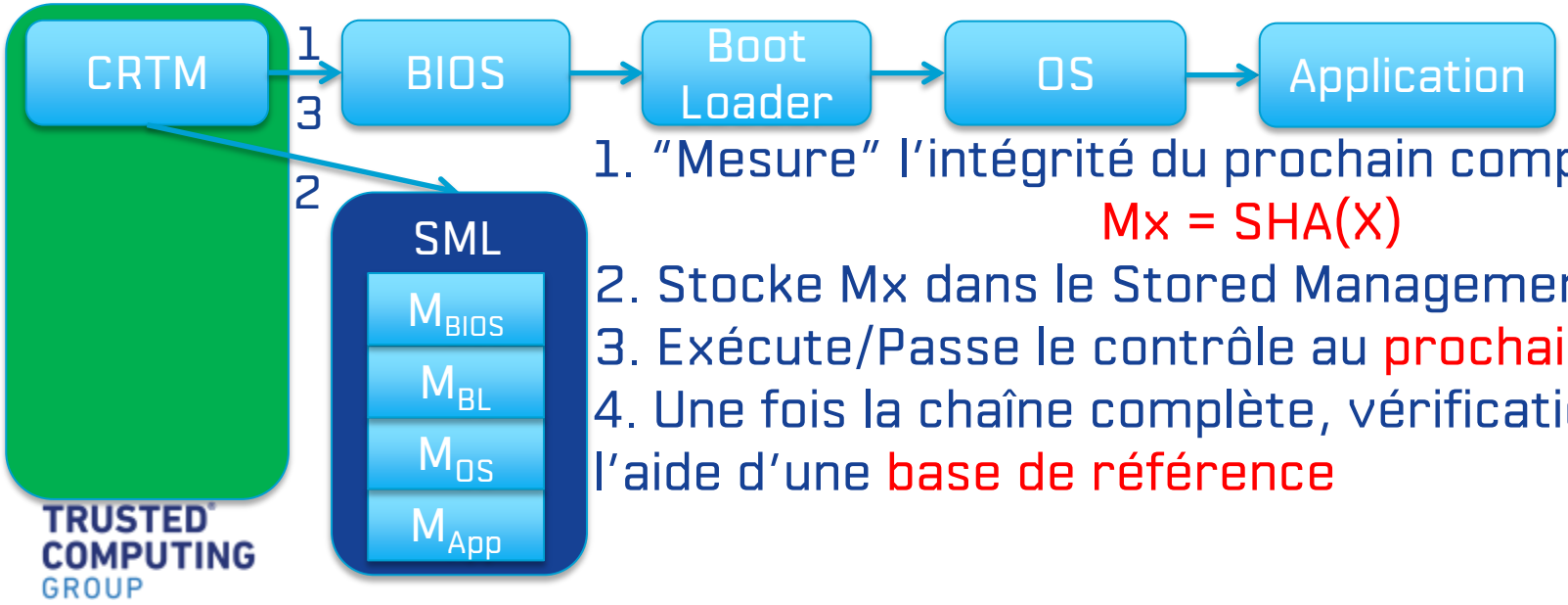


- Mémoire non-volatile d'un TPM limitée en taille
- Le TPM ne stocke donc que 2 clés cryptographiques permanentes
  - EK : clé constructeur
  - SRK : clé racine d'une hiérarchie de clés créé par le propriétaire de la plateforme
- AIK :
  - Pour l'authentification des rapports d'intégrité pour la Remote Attestation
  - Pseudonymes d'EK
  - Respect de la privacy des utilisateurs via une Privacy Certificate Authority (PCA)

APPLICATIONS DES TPMs

CHAÎNE DE BOOT (SANS TPM)

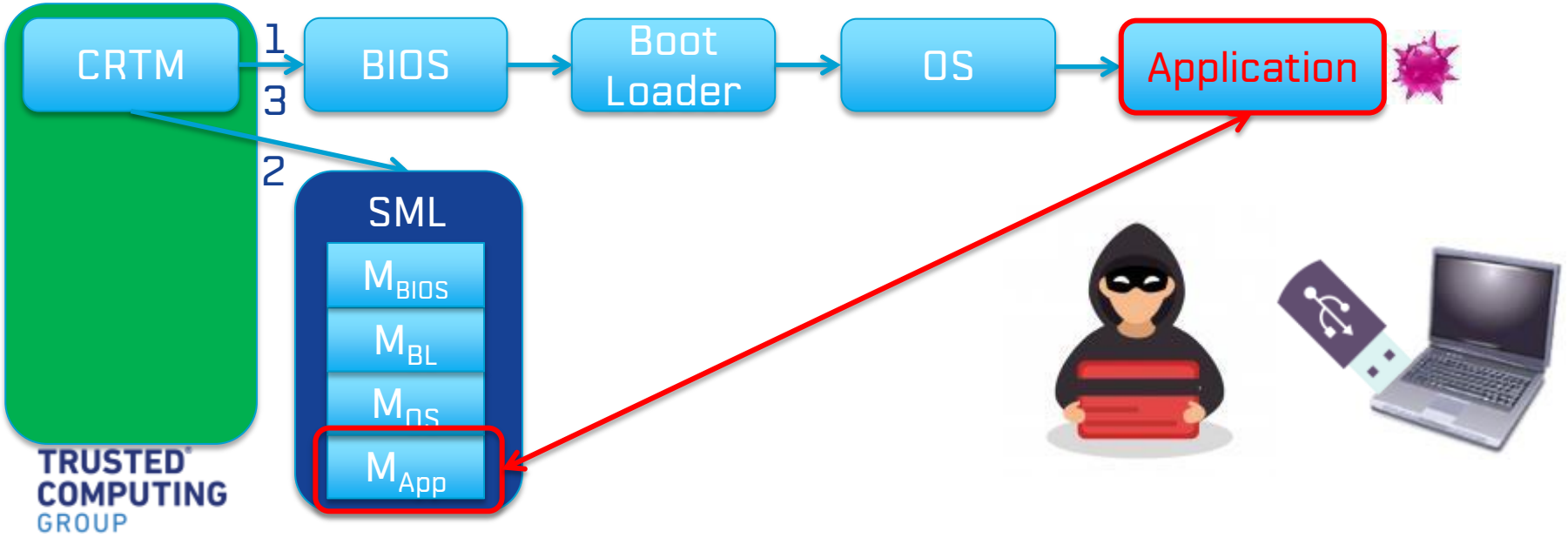
- Chaîne de boot transitive (« Measure then Execute »)
  - Chaque composant impliqué dans le boot est mesuré, et la mesure est envoyée dans un fichier de log



1. “Mesure” l’intégrité du prochain composant
   $Mx = SHA(X)$
2. Stocke Mx dans le Stored Management Log (SML)
3. Exécute/Passe le contrôle au prochain composant
4. Une fois la chaîne complète, vérification du SML à l’aide d’une base de référence

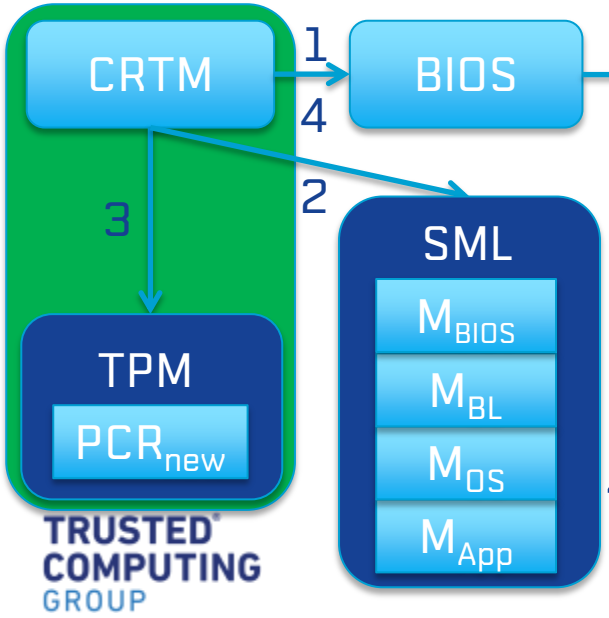
ATTAQUE « EVIL MAID » (POSSIBLE SANS TPM)

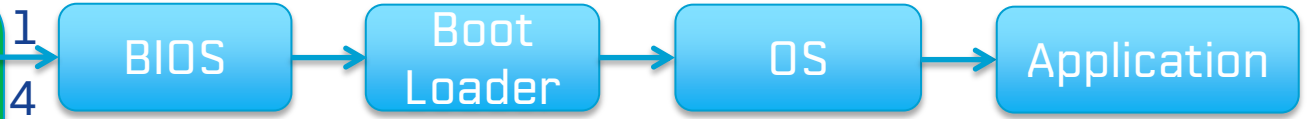
- Chaîne de boot transitive (« Measure then Execute »)
  - Chaque composant impliqué dans le boot est mesuré, et la mesure est envoyée dans un fichier de log



AUTHENTICATED BOOT

- Chaîne de boot transitive (« Measure then Execute »)
  - Chaque composant impliqué dans le boot est mesuré, et la mesure est envoyée à la fois dans les PCRs du TPM et dans un fichier de log





1. “Mesure” l’intégrité du prochain composant

$$Mx = SHA(X)$$

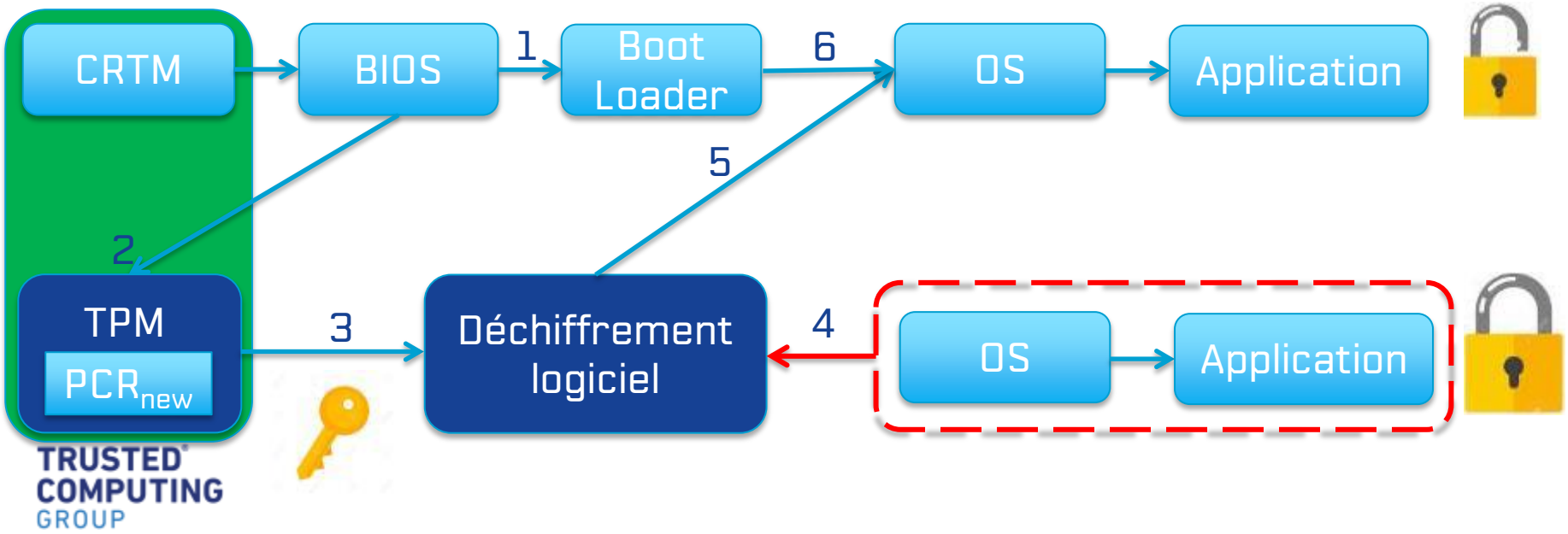
2. Stocke Mx dans le Stored Management Log (SML)
3. Etend Mx dans le PCR

$$PCR_{new} = SHA(PCR_{old} \,||\, Mx)$$

4. Exécute/Passe le contrôle au prochain composant
5. Une fois la chaîne complète, vérification du SML

SEALING

- Libération (dé-scellement) par le TPM d'une clé de déchiffrement des composants logiciels ultérieurs si les PCRs sont à la valeur attendue



QUELQUES APPLICATIONS A BASE DE TPMs

- Authenticated Boot (≠ Secure Boot)
  - Windows 8/10, KeyLime, McAfee ePolicy Orchestrator, Hyperviseurs (Hyper-V, vSphere, Google Cloud Platform, Xen, Open-CIT), etc.
- Remote Attestation
  - Wave Systems, Integrity Measurement Architecture (IMA), tboot, KeyLime, etc.
- Scellement
  - VPN
    - Strongswan, Cisco, etc.
  - Full-Disk Encryption
    - BitLocker (Windows), dm-crypt (Linux), CLIP OS (v5), etc.
  - File/Folder Encryption ((Open)PGP), E-mail (Thunderbird, Outlook, etc.), Web browser (IE, Firefox, Chrome)
- Authentification pour mise à jour du firmware
  - Google Nest
- Sécurisation cryptographie logicielle
  - FireEye HX, Stormshield Network Security (SN3100)

ATTAQUES SUR LES TPMs

POINT ATTAQUES SUR TPMs

Références attaques\TPMs vulnérables	Infineon (dTPM)	STMicro (dTPM)	Nuvoton (dTPM)	Intel (fTPM)	AMD (fTPM)
[KSP05] [WD11] [K07] [S07] [B18] Bus I²C, LPC	X	X	X		
[A19] BitLocker	X	X	X		
[T10] Reverse-Engineering	X	?	?		
[MSE+19] Timing Attack	?	X	?	X	
[NSS+17] ROCA (attaque crypto)	X				
[HSP+18] Sleep Mode	X	X	X		
Buffer Overflow					X

19 CVEs au total
Aussi : lien entre TPM virtuels (vTPMs) et dTPM pas garanti par tous les hyperviseurs, etc.

RESUME

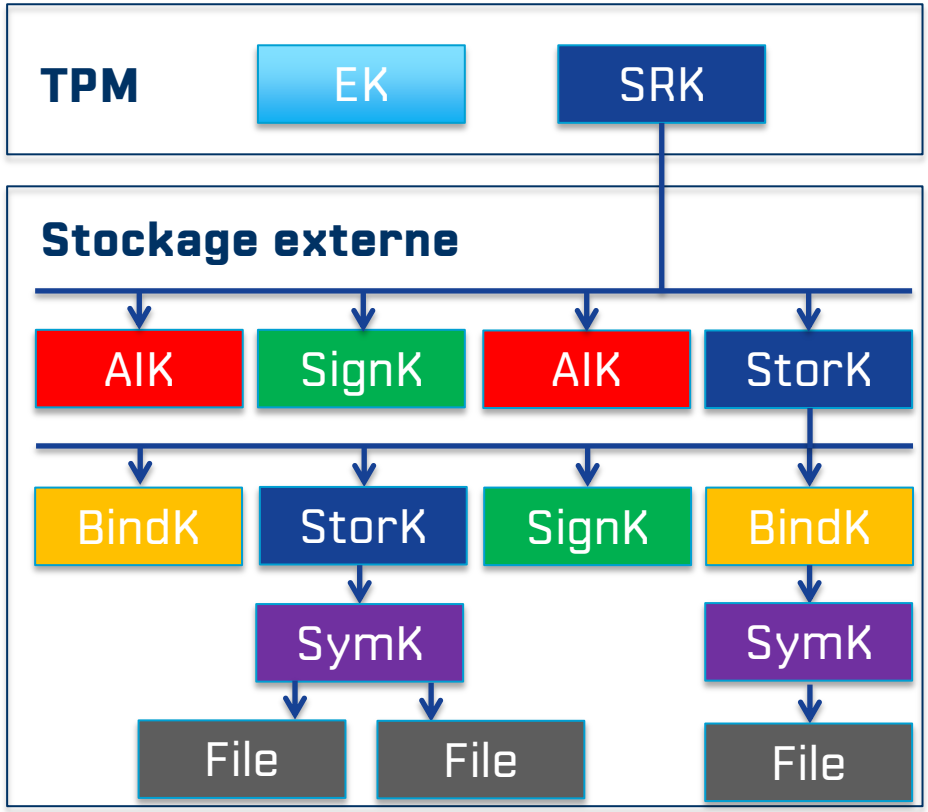
TAKE AWAY

- Un TPM dispose de plusieurs opportunités :
  - Il est présent à l'origine du boot, donc il a la vue complète sur ce dernier dès son « t=0 »
  - Ses rapports sur l'état de la plateforme sont de confiance
  - Il peut libérer des objets (ex. : clés) suivant cet état
  - Il peut contribuer à sécuriser de la crypto logicielle (stockage matériel des clés, meilleure entropie des nombres aléatoires, etc.)
- Malgré ses réelles qualités, peu de TPMs sont réellement utilisés…
- …mais ça ne va pas durer
- Disclaimers :
  - Un TPM n'est pas une baguette magique
  - Un TPM peut aussi être attaqué
  - Détournement des TPMs ?


NAVAL
GROUP

ANNEXES

HIÉRARCHIE DES CLÉS D'UN TPM



- Un nombre illimité de clés peuvent être stockées en externe
- Les Storage Keys (**StorK**) protègent les autres types de clés
  - Attestation ID Keys (**AIK**)
  - Binding Keys (**BindK**)
  - Signing Keys (**SignK**)
  - Symmetric Keys (**SymK**)
- Toutes les clés et données (**Files**) indirectement protégées par la SRK
- Attributs : mots de passe, scellement, etc.

REMOTE ATTESTATION

- Chaîne de boot transitive (« Measure then Execute »)
  - Chaque composant impliqué dans le boot est mesuré, et la mesure est envoyée à la fois dans les PCRs du TPM et dans un fichier de log