Sigurnost operacijskih sustava i aplikacija

Trusted Platform Module

Ivan Cvrk, 28.3.2025

Pregled predavanja

- Pitanja za ispite
- Motivacija
- Sklopovski i programski TPM
- Generiranje i pohrana ključeva
- Potvrda stanja sustava
- Identifikacija korisnika i uređaja
- Dodatne mogućnosti sklopa TPM 2.0

Pitanja za ispite

1. Nabrojite najmanje tri namjene za koje možemo koristiti TPM.
2. Kako TPM osigurava integritet podataka tijekom pokretanja sustava?
3. Koje su glavne značajke TPM-a kojima se štite kriptografski ključevi?
4. Kako TPM omogućuje sigurnu autentifikaciju uređaja i korisnika, te gdje je to korisno?
5. Opišite scenarij u kojem bi TPM mogao spriječiti neovlašteni pristup osjetljivim podacima na računalu.

Motivacija

- Problem identifikacije
  - Trebamo udaljenu potvrdu identiteta uređaja i korisnika.
  - Potreba za više identiteta bez mogućnosti korelacije.
- Gdje trebamo identifikaciju
  - **VPN autentifikacija uređaja i korisnika prije odobrenja pristupa mreži** - samo autorizirane osobe na uređajima u vlasništvu organizacije smiju pristupiti mreži.
  - **Autentifikacija korisnika banci i autorizacija transakcija –** pristup bankarskim aplikacijama moguć samo s odobrenih uređaja uz autorizaciju transakcija pomoću biometrije.

Motivacija

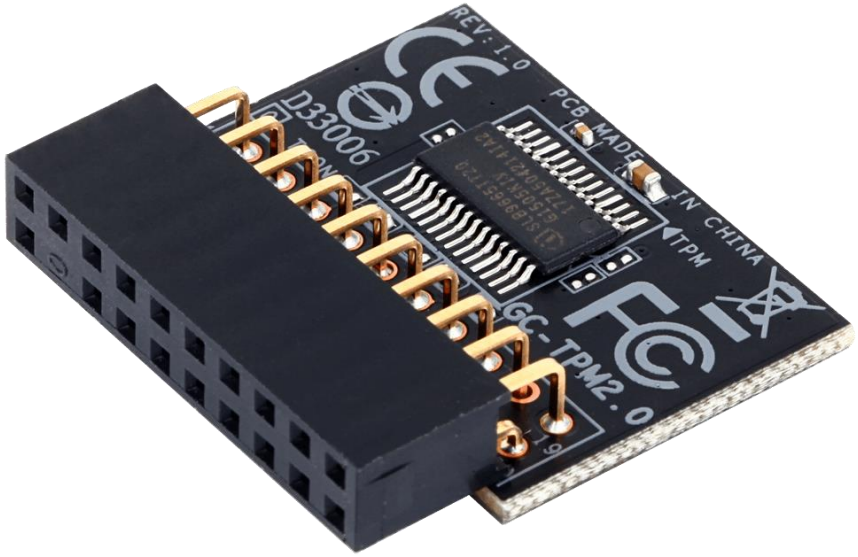
- Problem šifriranja
  - Šifrirani podatci su sigurni koliko i kriptografski ključevi.
  - Potreba za **sigurnom pohranom ključeva** otpornom na programske napade.
  - Sklopovska zaštita lozinki od napada rječnikom.
  - Biometrijska zaštita kriptografskih ključeva.
- Gdje koristimo šifriranje
  - šifriranje cijelog diska
  - šifriranje pojedinih datoteka
  - šifriranje kolačića u web pregledniku

Motivacija

- Problem provjere stanja sustava
  - U velikim korporativnim sustavima potrebno je pratiti stanje i rad uređaja u sustavu.
  - Samo ovlaštene promjene sustava se smiju dogoditi.
  - Moramo biti sigurni da nam komprimirano računalo lažno ne javlja da je sve u redu.
- Primjena
  - **Samo odobren operacijski sustav može dešifrirati disk** - zaštita od krađe laptopa, pokretanje drugog operacijskog sustava s USB-a i dešifriranje diska.
  - Samo računalo u ispravnom stanju smije pristupiti VPN mreži.

Trusted Platform Module - TPM

- TPM je sigurni kriptoprocesor – mikroprocesor za obavljanje kriptografskih operacija



Slika 1: sklop TPM 2.0

Sklopovski i programski TPM

Sklopovska inačica - TPM

- Pogodan za sustave koji se pokreču na fizičkom sklopovlju.
- Otporan na programske napade i fizičku zloupotrebu.
- Potpuna izolacija od ostatka sustava.
- Nešto sporiji od programske inačice ali sigurniji.

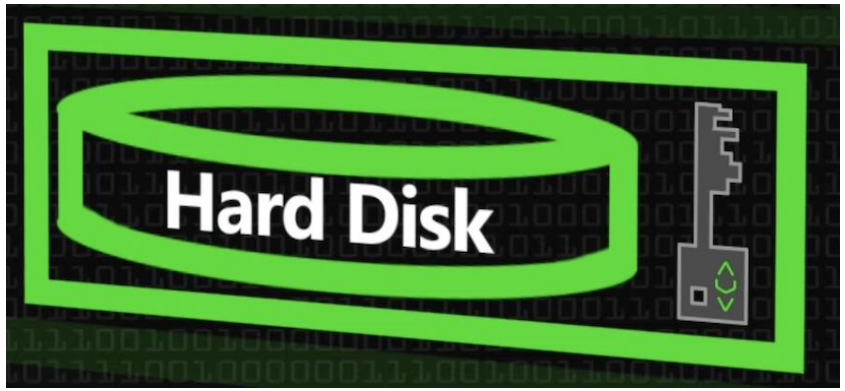
Programska inačica - TPM

- Pogodan za primjenu u virtualnim strojevima i okruženjima čiji sigurnosni model ne uključuje fizičku zloupotrebu.
- Domaćin ili hipervizor emulira sklopovlje.
- Sigurnost u potpunosti ovisi o sigurnosti domaćina te je ranjiv na programske napade na domaćina.
- Često brži od sklopovske inačice.
- Moguće je instalirati emulator TPM sklopovlja i bez virtualnih mašina.

Generiranje i pohrana ključeva

Primjer: Šifriramo disk, gdje spremiti ključ?

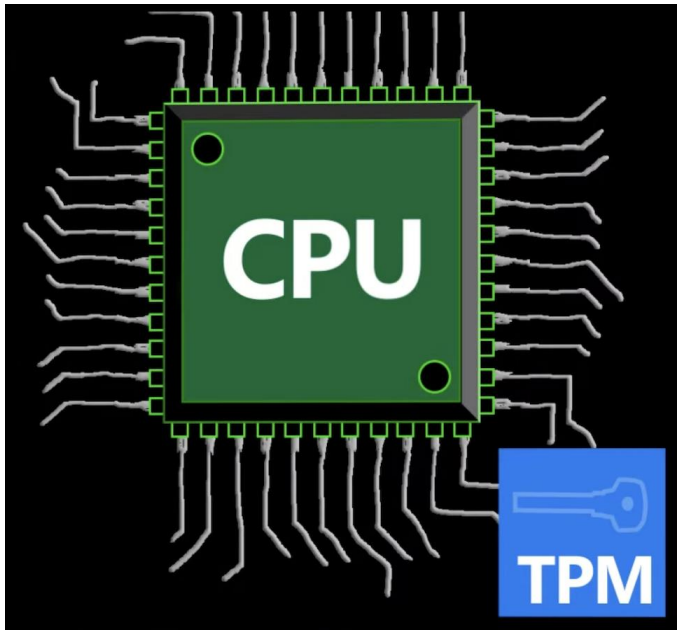
- Samo lozinke nisu dovoljne za generiranje ključa - **napad rječnikom**. Što čovjek može zapamtiti, računalo može pogoditi!
- Ako šifriramo ključ drugim ključem, gdje spremiti drugi ključ?



Slika 2: "Nezaštičen kriptografski ključ pohranjen pored kriptirane particije na tvrdom disku"

Generiranje i pohrana ključeva

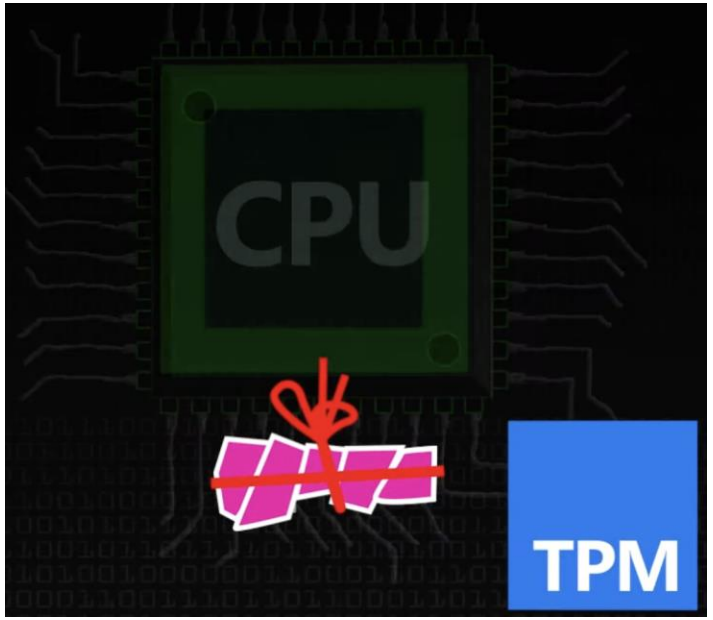
- TPM ima privatni ključ koji nije moguće pročitati.
- Taj ključ je zapravo velik nasumičan broj iz kojeg je moguće generirati više vrsta ključeva, npr. simetrični, asimetrični, AES128, RSA2048, ECC256, …
- Funkcija za generiranje ključeva (KDF, engl. key derivation function) je deterministička.



Slika 3: "TPM sklop sa skrivenim privatnim ključem nedostupnim procesoru"

Generiranje i pohrana ključeva

- TPM može generirati nove ključeve - ima ugrađen RNG
- Možemo tražiti TPM da zapakira naš ključ tako što ga kriptira svojim privatnim ključem.
- TPM je mogao umjesto ključa kriptirati cijeli disk, no to nije efikasno, programska implementacija je brža.
- KEK (engl. key encryption key) je mehanizam koji koristi BitLocker



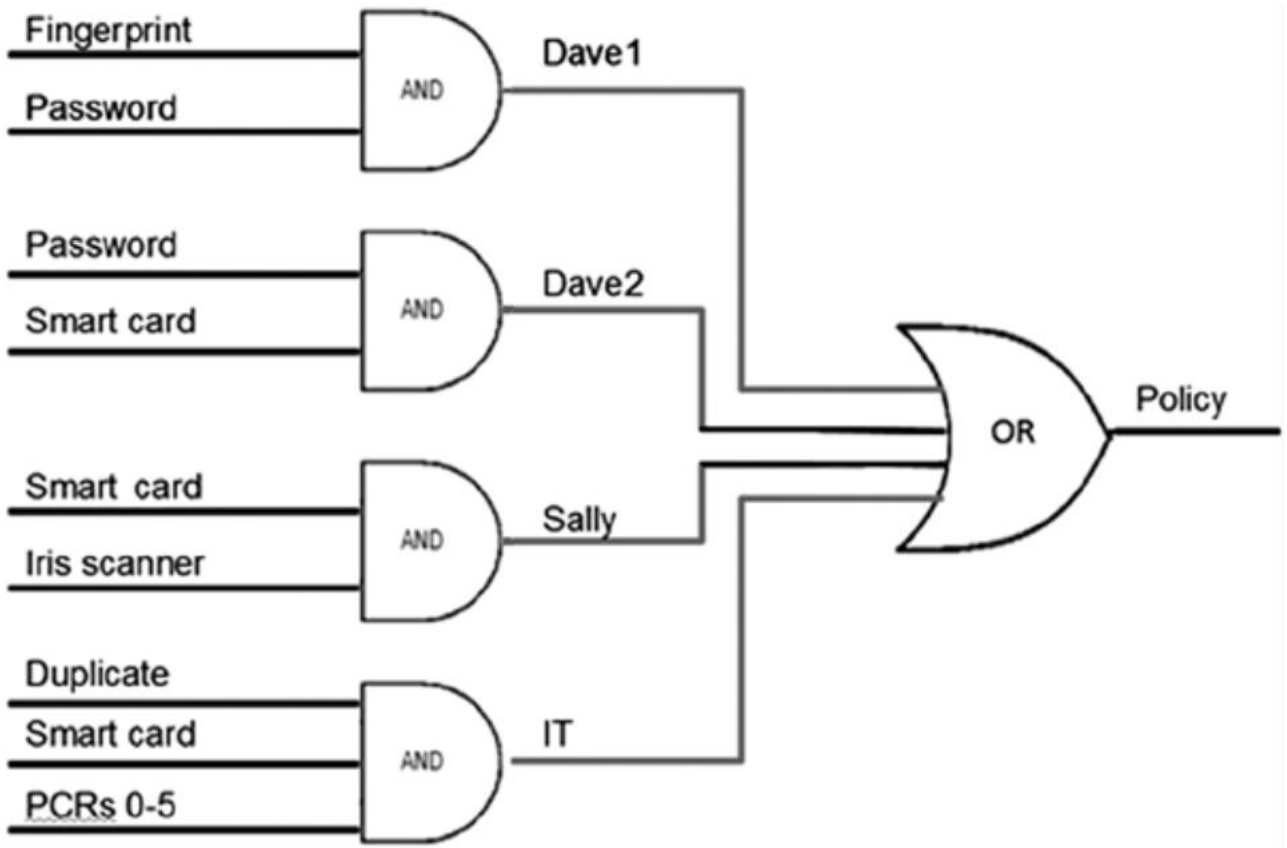
Slika 4: "TPM je zapakirao kriptografski ključ koji sada može biti sigurno pohranjen na tvrdom disku"

Generiranje i pohrana ključeva

- Moguće postaviti razna ograničenja pod kojima će TPM otpakirati ključ
  - pokrenut verificiran sustav
  - biometrijska mjerenja (otisak prsta, lice...)
  - geografska lokacija (GPS)
  - vrijeme
  - očitanje pametne kartice
  - lozinka
- Hardverska zaštita od napada rječnikom
  - minimalno vrijeme između dva pokušaja

Slika 5: "Kombinacija uvjeta mora biti zadovoljena kako bi TPM pristao otpakirati ključ"

Generiranje i pohrana ključeva



Slika 6: "Primjer složene politike za autorizaciju pristupa u TPM-u"

Generiranje i pohrana ključeva

- **Ograničeni ključevi za dešifriranje** (engl. restricted decryption keys)
  - Ključevi koje generiramo unutar TPM-a.
  - Moguće ih je koristiti samo za dešifriranje.
  - Ne vraćaju rezultat dešifriranja, već rezultat ostaje sigurno pohranjen u TPM memoriji.
  - Koriste se za izgradnju hijerarhije ključeva.
  - Još se zovu SK (engl. storage keys)
- Nismo ograničeni samo na jedan tajni ključ unutar TPM-a - olakšano upravljanje skupovima ključeva za istu namjenu.
- Primarni ključevi kriptiraju SK koji kriptiraju ostale ključeve.

Generiranje i pohrana ključeva

- Hijerarhije entiteta (TPM 2.0)
  - **Platform hierarchy**: Hijerarhija pod kontrolom proizvođača platforme, a koristi ju kod u ranoj fazi pokretanja sustava. Npr. za validaciju certifikata proizvođača tijekom nadogradnje, UEFI, sigurno pokretanje sustava...
  - **Storage hierarchy**: Hijerarhija pod kontrolom vlasnika platforme, koristi se proizvoljno kako je to odredio npr. IT odjel organizacije. Moguće dodavanje ključeva iz aplikacija. Npr. ključ za šifriranje diska, VPN ključevi, ključevi za upravitelj lozinkama...

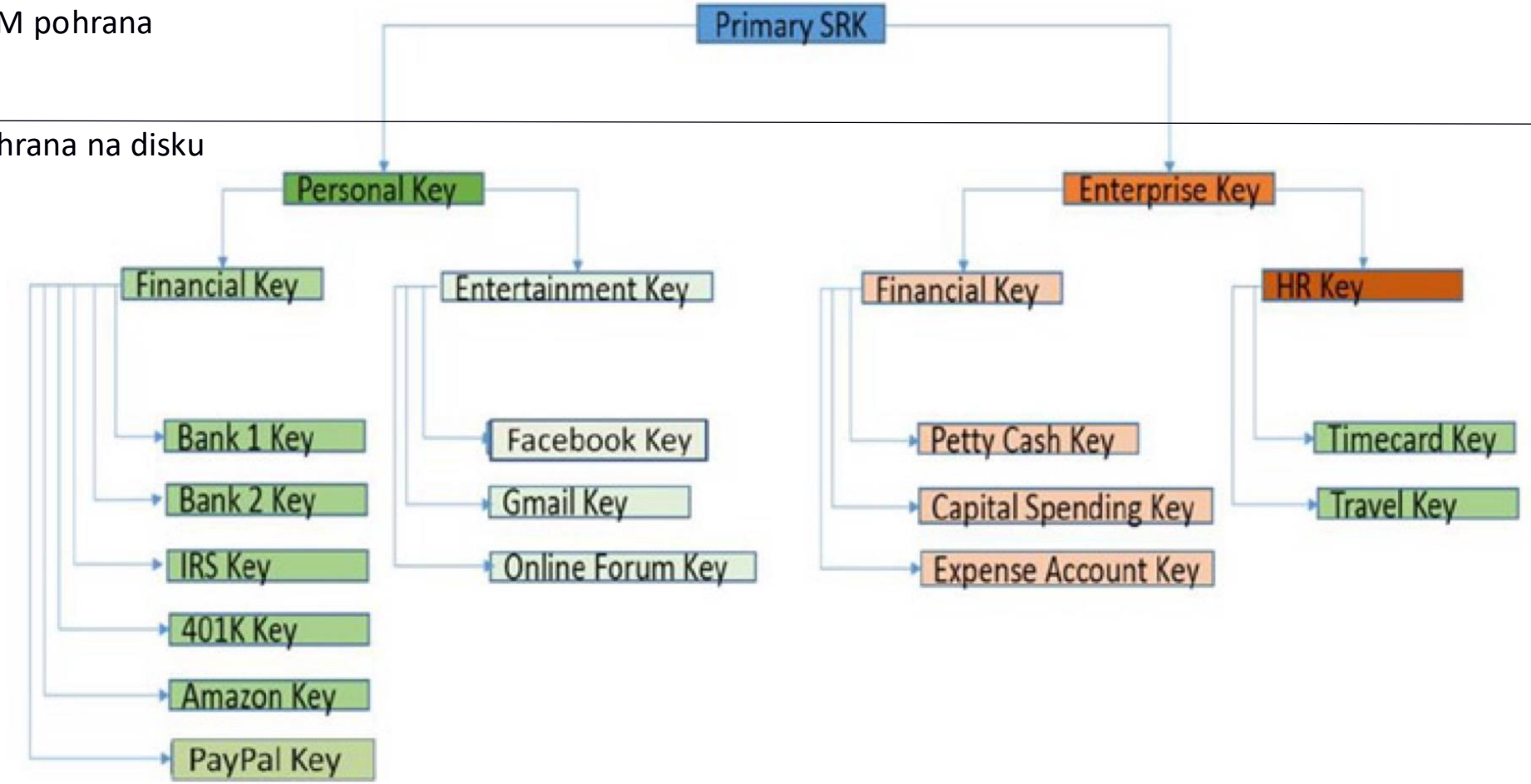
Generiranje i pohrana ključeva

- Hijerarhije entiteta (TPM 2.0)
  - **Endorsement hierarchy –** Hijerarhija za sigurno pohranjivanje podataka koji zahtijevaju zaštitu privatnosti. Konkretno, ključevi za identifikaciju uređaja i korisnika. Iz identifikacijskih ključeva se ne bi smjelo moći saznati da pripadaju istom TPM sklopu.
- Kod izgradnje hijerarhije potrebno je pohraniti samo korijenski ključ na TPM, zapravo sjeme ključa, a ostali ključevi mogu se kriptirati i pohraniti na disk.
- Moguće je imati više primarnih ključeva za istu hijerarhiju.

Generiranje i pohrana ključeva

TPM pohrana

Pohrana na disku



Slika 7: primjer hijerarhije ključeva za pohranu

Generiranje i pohrana ključeva

- Slika 6 pokazuje primjer hijerarhije ključeva, konkretno to je *storage hierarchy,* a sadrži korisnički definirane ključeve.
- Vlasnik platforme upravlja primarnim ključem, te je kreirao dvije glavne grane – osobni i poslovni ključevi.
- Svi ključevi, osim primarnog su šifrirani i **pohranjeni na disku** dok se ne koriste.
- **Samo listovi mogu šifrirati i dešifrirati proizvoljne podatke.**
- Potrebno je uvijek dešifrirati sve ključeve od korijena da bi se dohvatio ključ u listu hijerarhije.

Generiranje i pohrana ključeva

- Ključeve je moguće **duplicirati**, najčešće tako da se zapakiraju javnim ključem drugog TPM sklopa – ključevi ne mogu izaći iz originalnog TPM-a nešifrirani.
- Potrebno je unaprijed odrediti koji će se ključevi moći duplicirati i koja pravila moraju biti zadovoljena.
- Promjena sjemena primarnog ključa invalidira sve ostale ključeve u hijerarhiji.
- Uklanjanje jednog ključa iz hijerarhije invalidira svu njegovu djecu.

Generiranje i pohrana ključeva

- TPM kao zaštita ključeva
  - Generira kriptografski sigurne ključeve.
  - Ključevi nikad ne napuštaju sigurno okruženje TPM-a u dešifriranom stanju.
  - Kriptografske operacije koje koriste zaštićene ključeve moguće je obavljati isključivo unutar TPM-a koji je otporan na programske napade.
  - Ključevi su zaštićeni naprednim autorizacijskim sustavom koji se nalazi unutar TPM-a čime je on isto otporan na programske napade.

Potvrda stanja sustava

- NVRAM (engl. non-volatile random access memory) - memorija koja se ne mijenja između ponovnog pokretanja računala.
- **PCR (engl. Platform Configuration Registers)** - prostor u NVRAM-u TPM čipa koji sadrži kriptografski sažetak mjerenja sustava tijekom pokretanja.
- PCR vrijednosti se ne mogu izbrisati, samo ažurirati korištenjem XOR operacije.
- PCR vrijednosti prate promjene u sustavu.

Potvrda stanja sustava

- Tijekom pokretanja sustava u raznim koracima uzima se kriptografski sažetak koda i konfiguracije koja će se sljedeća pokrenuti, te se ažuriraju PCR vrijednosti ako ima promjene.
- Lanac povjerenja - 24 PCR kriptografskih sažetaka, a neki od njih su:
  - CRTM (engl. core root of trust)
  - BIOS (engl. Basic Input/Output System)
  - MBR (engl. master boot record)
  - Statični dio operacijskog sustava
- Mogu se pratiti i druge vrijednosti, npr. koliko je puta sustav bio pokrenut.

Potvrda stanja sustava

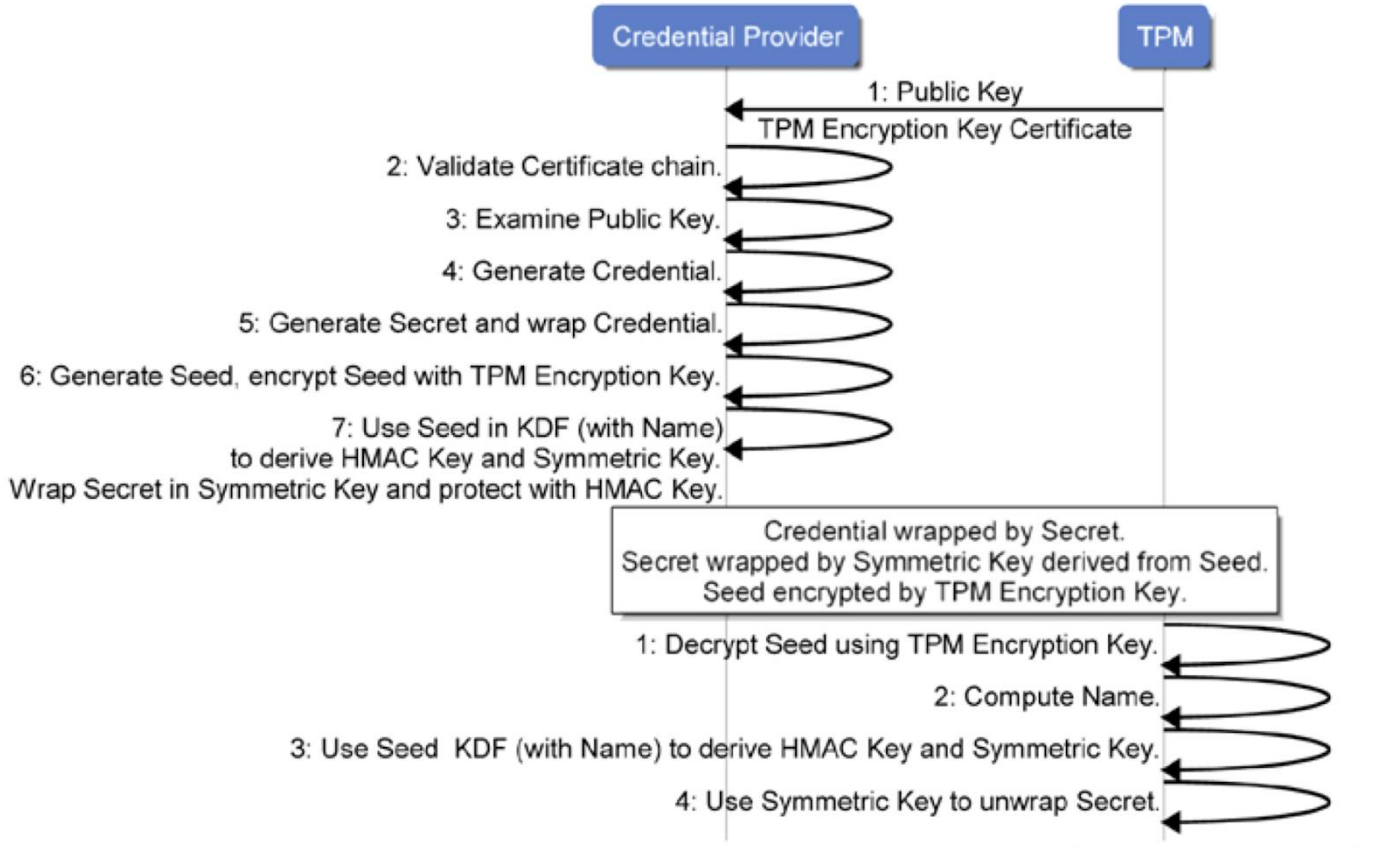
- PCR vrijednosti koriste se za **sigurno pokretanje sustava**.
- Moguće je tražiti predodređene vrijednosti u nekim PCR registrima kao korak autorizacije za korištenje nekih ključeva.
- PCR-ovi nisu ograničeni na kriptografske sažetke koda i konfiguracija, npr. mogu sadržavati kriptografski sažetak logova aplikacija kako bi se potvrdio njihov integritet.
- Status PCR vrijednosti može se pročitati iz TPM-a, a dodatno, TPM ih može potpisati dodijeljenim identifikacijskim ključem (AK, engl. attestation key).

Identifikacija korisnika i uređaja

- **AK (engl. attestation key)** - ključ koji služi za dokazivanje identiteta uređaja ili korisnika.
- AK ključeve najčešće izdaje CP (engl. credential provider) i potpisuje CA (engl. certificate authority). CP mora biti posebno prilagođen za TPM protokol.
- Nakon što su autorizacijski uvjeti AK ključa ispunjeni, TPM može iskoristiti ključ za potpisivanje poruke kako bi **dokazao identitet** dodijeljen tim ključem.

Identifikacija korisnika i uređaja

- Dodjelu identiteta radi *credential provider* korištenjem *"activating a credential"* protokola.
- Ako se ne šalje javni ključ TPM-a, onda treba napraviti *dokaz s nultim znanjem* za dokaz identiteta. Nije potreban CA.



Slika 8: sekvencijski dijagram protokola "activating a credential"

Dodatne mogućnosti sklopa TPM 2.0

- Podrška za velik broj kriptografskih algoritama.
- TPM kao certificirani kriptografski procesor pruža implementaciju najvažnijih kriptografskih algoritama za što ga izravno možemo koristiti kad ne želimo sami implementirati kriptografske algoritme, npr. za embedded programe ili npr. tijekom nadogradnje CRTM sustava kada CRTM sustav mora potvrditi potpis proizvođača kako bi izvršio nadogradnju.

Zaključak

- TPM je ključna sigurnosna komponenta u današnje vrijeme tehnologije te je neizostavan dio gotovo svakog računala, a posebno u institucionalnom i korporativnom okruženju.
- Vrlo moćan sigurnosni alat s gotovo neograničenim mogućnostima kada je u pravim rukama.
- Zbog svoje svestranosti i robusnosti, može biti iznimno težak za korištenje.

Literatura

[1] Will Arthur and David Challener. 2015. A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security (1st. ed.). Apress, USA. - PDF https://link.springer.com/book/10.1007/978-1-4302-6584-9

[2] TPM slika - https://www.gigabyte.com/Motherboard/GC-TPM20#ov

[3] Computerphile - https://www.youtube.com/watch?v=RW2zHvVO09g&t=572s

Dodatna literatura

[4] Debian PCR registri - https://uapi-group.org/specifications/specs/linux_tpm_pcr_registry/

[5] Trusted Computing Group stranica - https://trustedcomputinggroup.org/about/what-is-a-trusted-platform-module-tpm/

Hvala!