Trusted Platform Modules: Introduction and Shortcomings

Bc. Ondřej Ondryáš

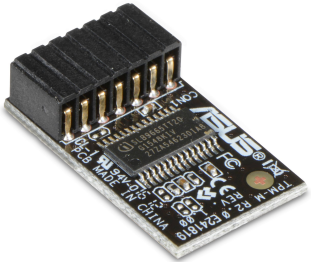
16. dubna 2024

- Prosazování chování
- Důvěra a důvěryhodnost
  - Očekávané chování
  - Predikovatelné chování
- Trusted Computing Group (TCG)
- Důvěryhodná výpočetní báze (TCB)
- Trusted Platform Module (TPM)

TRUSTED® COMPUTING GROUP

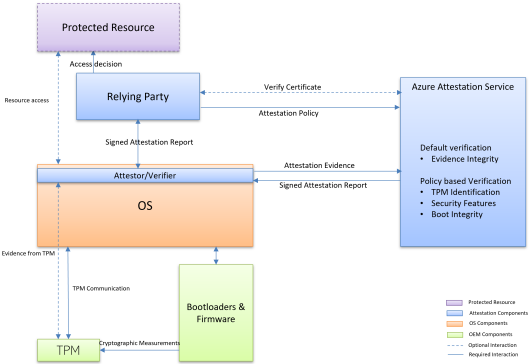
Trusted Platform Module

- Fyzická komponenta oddělená od zbytku systému
- Pomáhá vytvořit TCB
- Kryptografická primitiva, bezpečnostní funkce
- Různé realizace
  - dTPM, iTPM, fTPM, vTPM, . . .



Funkce TPM

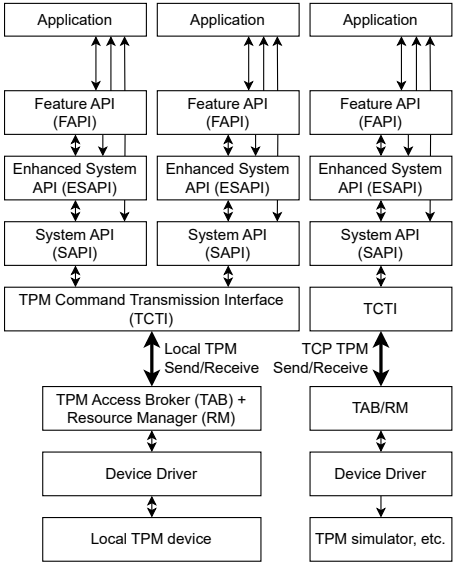
- Náhodná čísla
- Identifikace a autentizace zařízení
- *Device attestation* – ověřování integrity zařízení
  - Platform Configuration Registers
  - Remote attestation
  - Direct anonymous attestation
- Správa kryptografických klíčů
  - Binding/Wrapping
  - Sealing
- Kryptografické operace – šifrování, podepisování



Zdroj: learn.microsoft.com/en-us/azure/attestation/tpm-attestation-concepts

Použití TPM

- The TPM Software Stack
- Vrstvy abstrakce
- Další implementace



Problémy TPM

- Extrémně komplikované specifikace
- Nedostatek zdrojů pro začátečníky
- Nevhodný stav knihoven
- Zranitelnosti

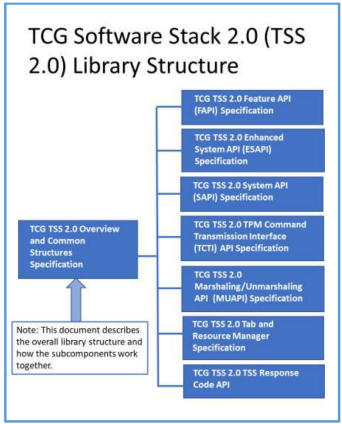
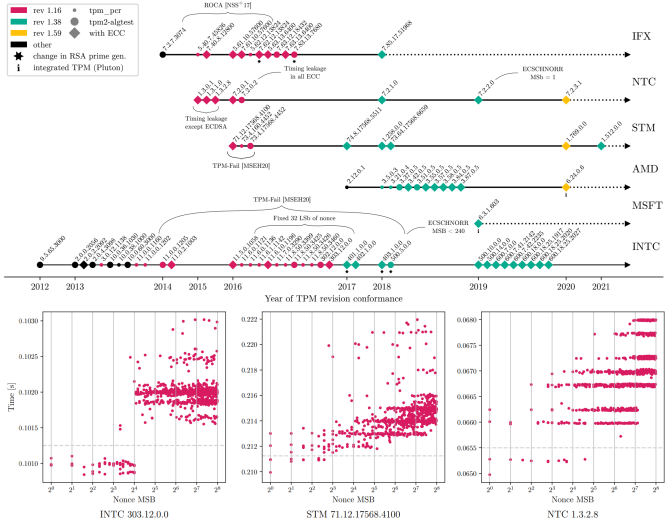


Figure 1: TSS 2.0 Specification Library

Zranitelnosti TPM

- Specifikace
- Fyzické útoky (fTPM)
- Postranní kanály (fTPM)
- Útoky na sběrnici (dTPM)
- Útoky na implementaci!
  - Navzdory certifikacím!
  - TPM-Fail, ROCA, ...
- Problémy použití :)



Zdroj: P. Švenda, "TPMScan: A wide-scale study of security-relevant properties of TPM 2.0 chips", TCHES, březen 2024.