Másolásvédelem nyíltforrású eszközökhöz

Kovács Viktor
BME-AUT
MagiCom Kft.

Nincs tökéletes védelem!

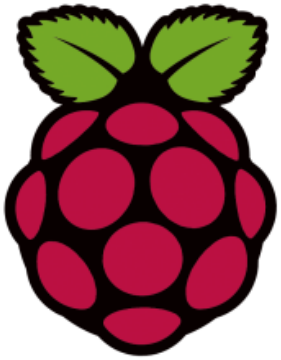
De egy kicsit megnehezíthető a támadás…

Miről is van szó?

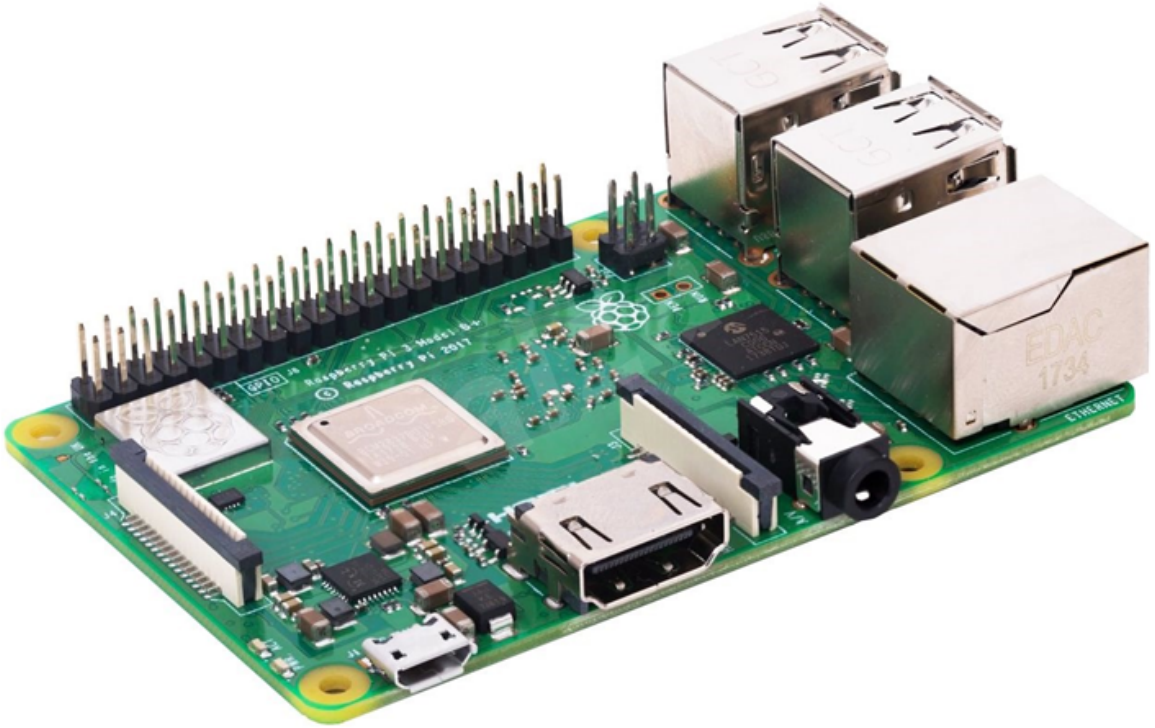
- Szoftvert fejlesztünk…
- A szoftver hardveren fut
- Az ügyfélnek oda kell adni az eszközt (hardver+szoftver)
- Nincs feltétlenül internetkapcsolat
- Sok példány
- Elegendő teljesítmény
- Legyen olcsó

Milyen hardvert használjunk?

Gyümölcsös piték



Raspberry Pi 3



SBC – Single Board Computer

- Nagyon olcsó
- Nagy teljesítmény
- Méretét, interfészeit tekintve **beágyazott**
- Bizonyos képességeit tekintve **PC**

- Cél: hobbi, tanulás, elronthatatlan, nyílt!

Más célokra is megfelel (?)

PC vs. beágyazott program

	PC	;yazott (mikrokontroller)
Terjesztés		
	•Digitális terjesztés, mint	· + szoftver együtt
		s szoftverfrissítés egyedileg
IP védelem		
	•Szoftver kulcs, aktivác	kiolvasható
	•(Speciális adathordozó)	ott külső memória
	•Hardver kulcs	emória
		emória hozzáférés tiltott

Probléma

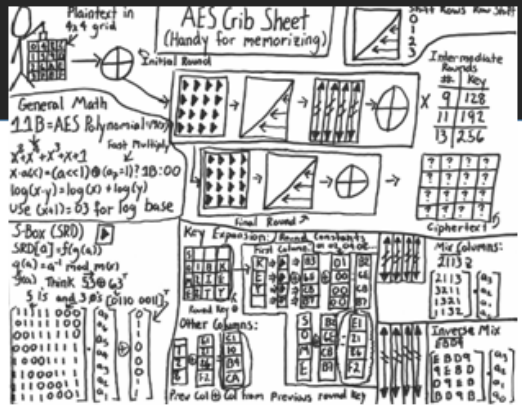
- A hardver nem egyedi
- A hardverrel együtt szállított kód nem védett
  - Az SD kártya kivehető és lemásolható, módosítható
- SD kártyán nem lehet biztonságosan kulcsokat tárolni
- Nincs RTC modul
- SBC – szerver kommunikáció nem megbízható

Feladat

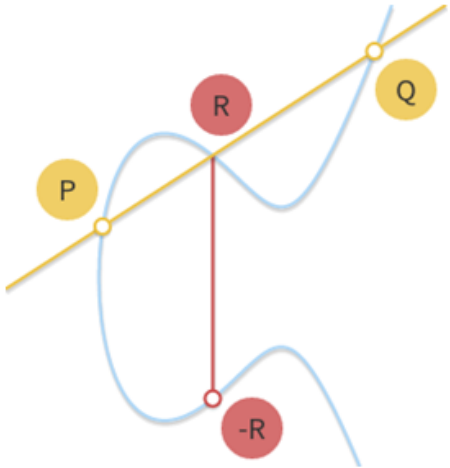
- Autentikáció
  - Kulcs tárolás
    - Fejben
    - Biometria
    - **Hardverben** – RSA token, **U2F, FIDO2, Yubikey**

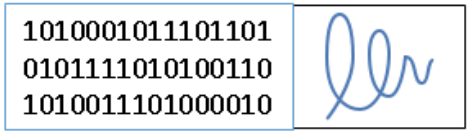
- Kommunikáció
  - Titkosított kommunikáció egy távoli szerverrel
  - Kulcs tárolás…

Kriptográfia



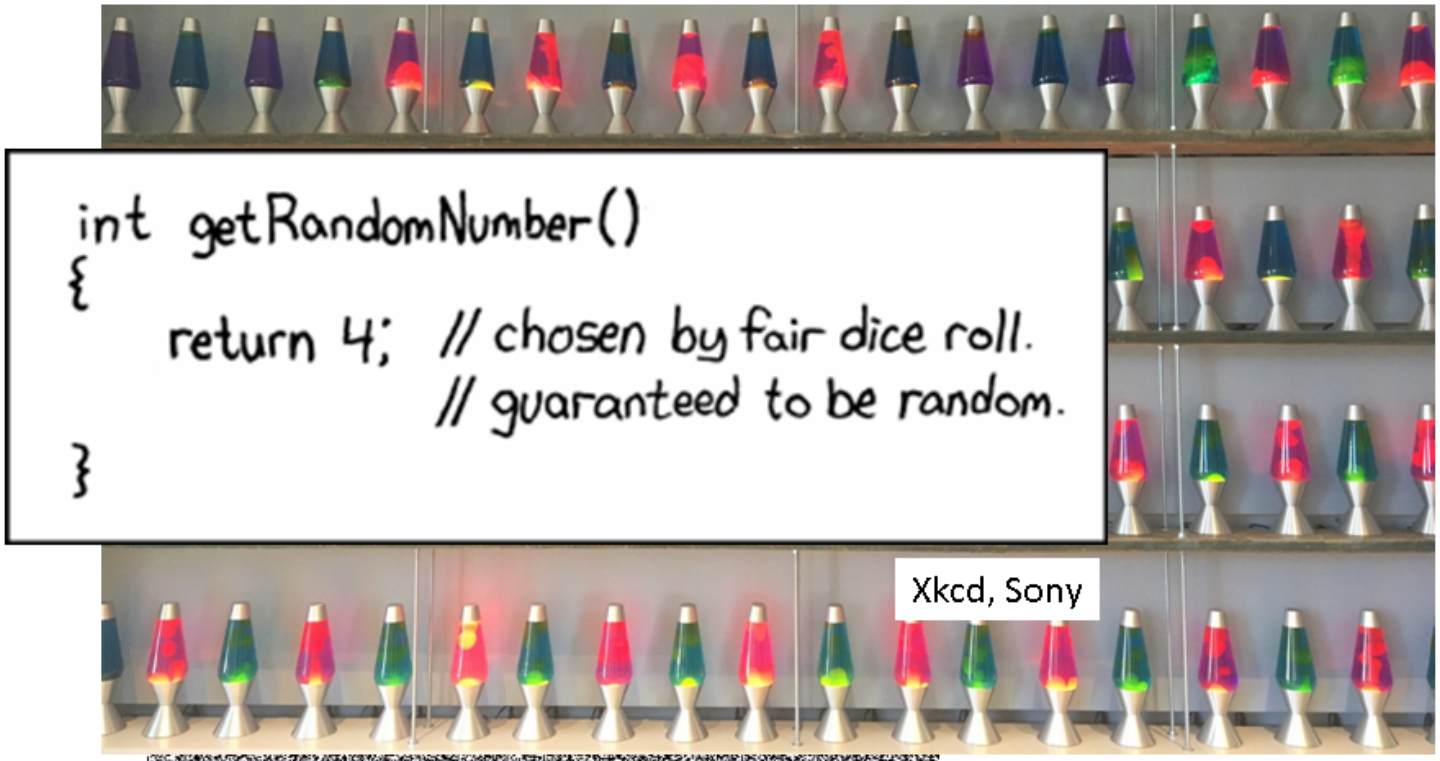
- Szimmetrikus
  - AES
    http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html
  - ChaCha20
- Publikus
  - RSA
  - ECC – Elliptic Curve Cryptography
  - Kulcscsere (Diffie-Hellman)
- Aláírás
  - ECDSA
  - Poly1305

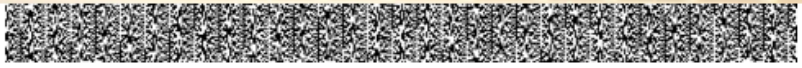




Véletlenszám generátor – RNG

- PRNG
- TRNG
- CSRNG
- CSPRNG





PHP rand() Windowson

Cloudflare: LavaRand

Elvárások

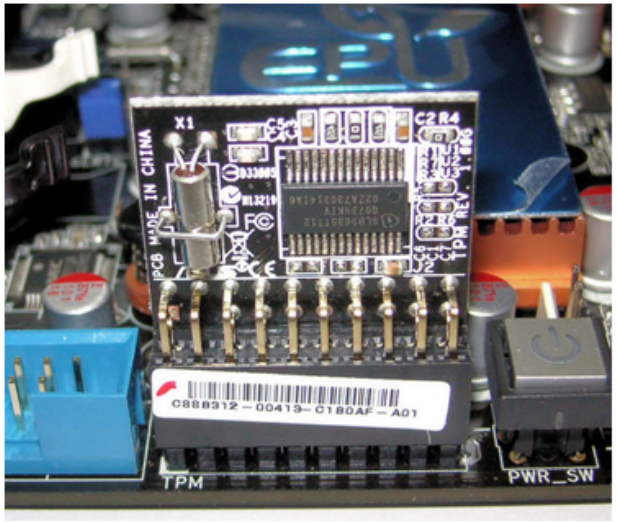
- Egyedi azonosító
- Kulcs tárolás
- Titkosítás
- Valódi véletlenszám generátor

Tökéletes védelem nincs,
de a támadás megnehezíthető

TPM

Trusted Platform Module

- Autentikáció
- Lemez titkosítás
- Secure Boot

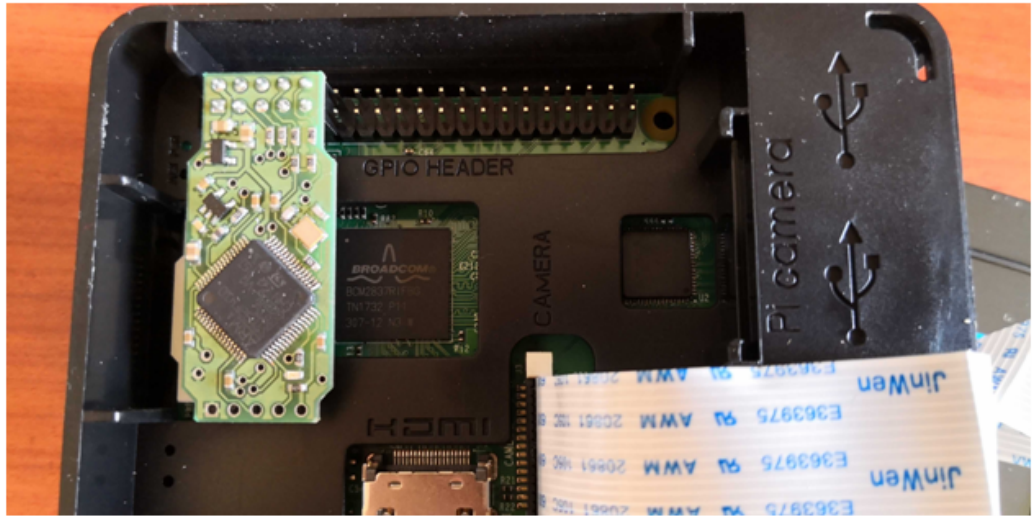


- TPM chip-ek (Infineon…)
- Apple T1, T2

Crypto modulok

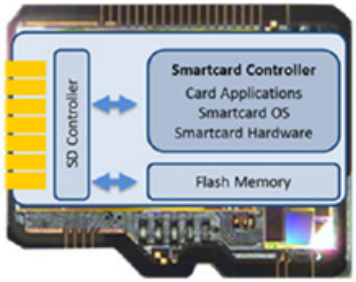
- ATECC sorozat – Zymbit

- Univerzális mikrokontrolleres – RPI-DRM
  - Egyedi azonosító
  - ECC alapú aláírás
  - Privát-publikus kulcs tárolás
  - Kulcs generálás
  - Kulcs hozzáférés beállítás
  - AES titkosítás
  - Titkosított kommunikáció
  - Véletlenszám generálás
  - Szoftverfrissítés
    - Bizonyos kritikus szoftver funkciók implementálhatóak itt



Speciális SD kártyák

- cgCard
  - 2 faktoros autentikáció
  - Titkosítás
  - TRNG
  - Blackberry, Android, Windows



- Swissbit
  - PKI
  - TRNG
  - Titkosítás

Esettanulmány

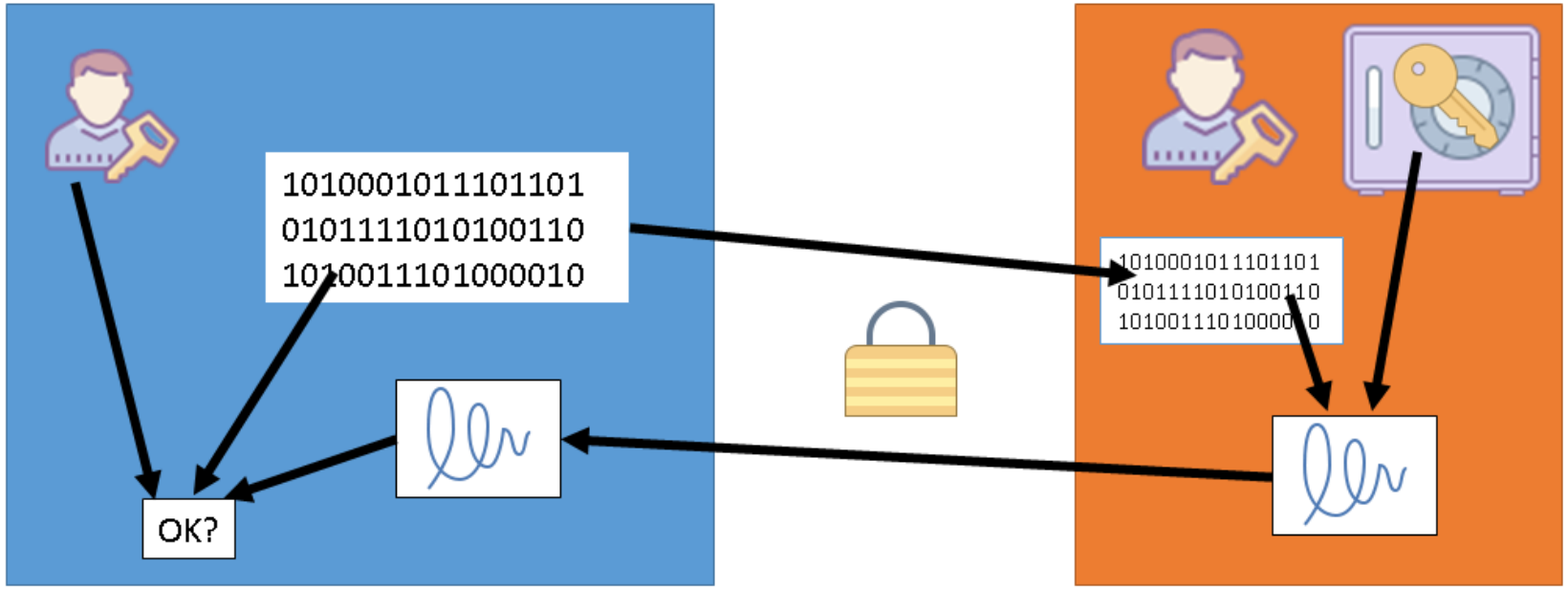
- Valósidejű képfeldolgozás kamerával (ATECC ☺)
  - Komoly számítási teljesítmény igény
- Hálózati kommunikáció a központtal
- Sok példány, olcsó
  - Raspberry PI 3
- „Demo” céljából kiadható
  - RPI-DRM modul

Köszönöm a megtisztelő figyelmet!

Kérdések?

Eredetiség ellenőrzés

- Aláírással - ECDSA



„Off-board” titkosítás