Odolnost kryptografického HW s ohledem na nasazení

Vašek Lorenc, Vašek Matyáš

XVIII. konference EurOpen

Fakulta informatiky
Masarykova univerzita
Brno

Obsah přednášky

Autentizační techniky

- *„něco, co znám“*
  - tajná informace (hesla, PIN, . . .)
- *„něco, co jsem“*
  - biometriky (otisky prstů, rozpoznání hlasu, . . .)
- *„něco, co mám“*
  - token (pečeť, prsten, klíč, čipová karta, USB zařízení)
- + možné kombinace (dvoufaktorová autentizace, . . .)
- každá technika má své klady i zápory

Kryptografický HW

- mikrokontrolery
  - procesor, paměť (RAM i ROM), řadiče pro I/O operace, časovač
- čipové karty
  - paměťové – vhodné pro ukládání dat,
  - procesorové – procesor schopný ochránit přístup k datům; vlatní OS a aplikačním softwarem,
  - kryptografické – procesorová se speciálním koprocesorem pro vykonávání kryptografických operací,
- hardwarové bezpečnostní moduly (HSM)
  - specializované, vysoká odolnost vůči útočníkům, TRNG
- rozdíly v cenách, schopnostech a míře bezpečí

Kryptografický HW

- mikrokontrolery
  - procesor, paměť (RAM i ROM), řadiče pro I/O operace, časovač
- čipové karty
  - paměťové – vhodné pro ukládání dat,
  - procesorové – procesor schopný ochránit přístup k datům; vlatní OS a aplikačním softwarem,
  - kryptografické – procesorová se speciálním koprocesorem pro vykonávání kryptografických operací,
- hardwarové bezpečnostní moduly (HSM)
  - specializované, vysoká odolnost vůči útočníkům, TRNG
- rozdíly v cenách, schopnostech a míře bezpečí
- *odpovídá však cena skutečně poskytovanému bezpečí?*

Bezpečnost kryptografického HW

- fyzická bezpečnost
  - překážka umístěná kolem počítačového systému za účelem ztížení neautorizovaného fyzického přístupu k tomuto počítačovému systému
- odolnost vůči narušení
  - vlastnost části systému, která je chráněna proti neautorizované modifikaci způsobem zajišťujícím podstatně vyšší úroveň ochrany než ostatní části systému
- zjistitelnost narušení
  - systém, u kterého jakákoliv neautorizovaná modifikace zanechává zjistitelné stopy
- detekce narušení
  - automatické zjištění pokusu o narušení fyzické bezpečnosti
- odpověď na narušení
  - automatická akce provedená chráněnou částí

Útoky na kryptografický HW

- lokální útoky
  - útočník má kartu fyzicky v držení
  - typy lokálních útoků:
    - invazivní
    - semi-invazivní
    - neinvazivní
- vzdálené útoky
  - softwarové útoky, možno provádět na dálku
  - zneužití i automatizovanými prostředky (viry, boti)

Invazivní útoky

1. zbavení ochranného pouzdra
   - mechanicky nebo za pomoci chemických roztoků
2. reverse engineering
   - nejnáročnější část, vysoké nároky na vybavení i znalosti útočníka
3. použití mikrosond
   - čtení hodnot na sběrnici, ovlivňování chování obvodu
4. modifikace čipu
   - upravení čipu dle záměru útočníka

- nároky na vybavení útočníka zpravidla vysoké, podobné výrobci
- elektronové mikroskopy, speciální mikrosondy

Neinvazivní útoky

1. indukce chyb během výpočtu
   - napájecí napětí, hodinový signál, reset signál elektrické pole, teplota
   - snaha změnit data v registrech nebo přeskočit instrukci
2. časová analýza
   - různé větve programu trvají různě dlouho, stejně tak operace nad různými operandy
   - průběhu DESu, násobení, umocňování – vliv optimalizací
3. výkonová analýza
   - různý odběr proudu při sčítání/násobení, zapisování 0 a 1, ...
   - jednoduchá výkonová analýza (*simple power analysis*)
   - rozdílová výkonová analýza (*differential power analysis*)

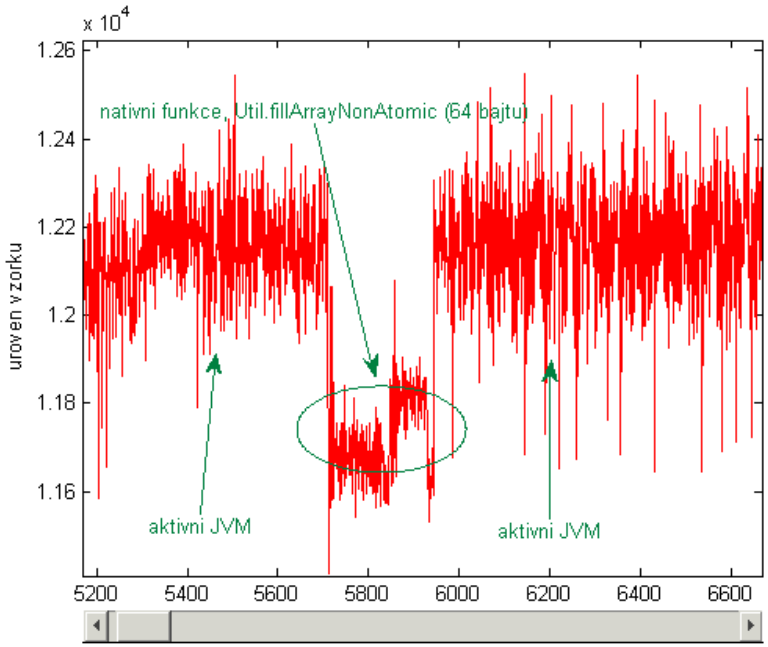
- analýza zařízení vnějším pozorováním jeho chování
- většinou nezjistitelné!

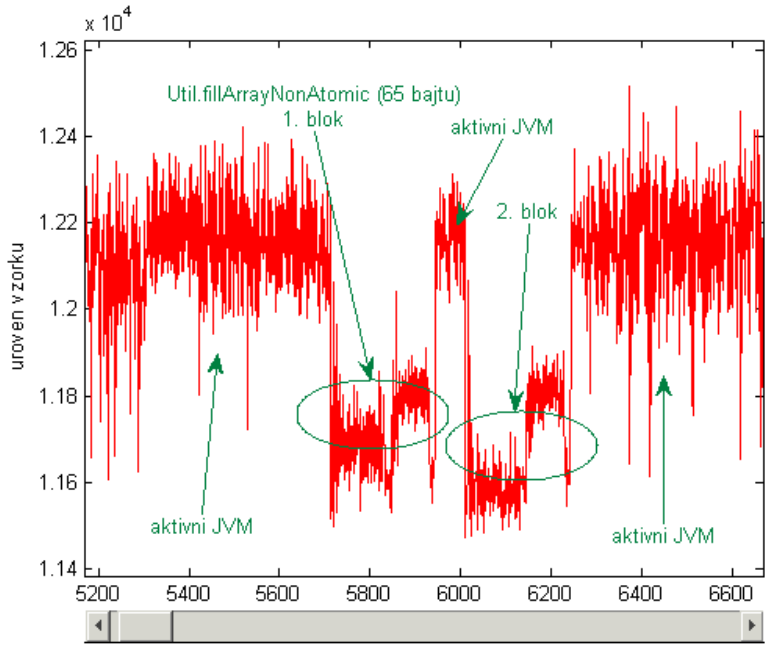
Neinvazivní útoky

časová analýza

Průběh zápisu pole do paměti:

- karta zapisuje po 64 bitech
- rozdíl mezi zapsáním 64 bitů a 65 bitů

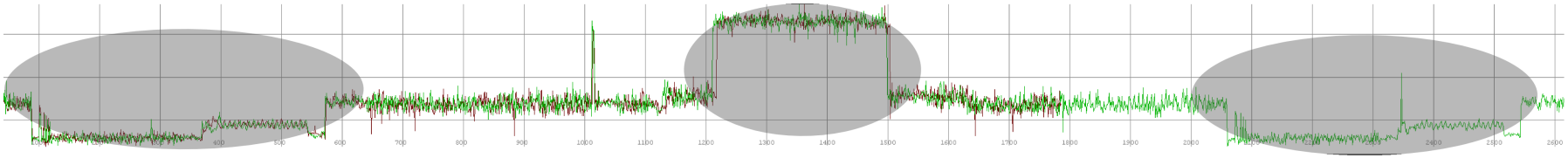




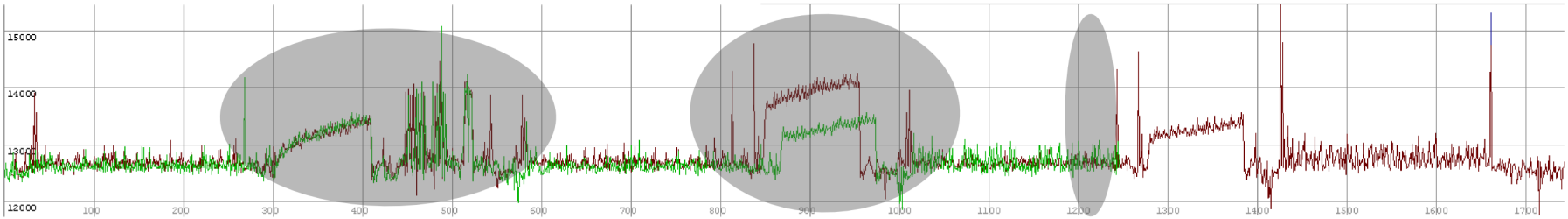
Neinvazivní útoky

SPA/DPA – verifikace PINu

- správná implementace: sniž čítač → ověř PIN [→ *zvyš čítač*]



- zranitelná implementace: ověř PIN [→ *sniž čítač*]



Semi-invazivní útoky

- útoky zejména na mikrokontrolery
- nedochází ke zničení čipu
- používané techniky
  - laserové paprsky
  - kvalitní fotografické blesky
  - elektromagnetická pole
  - ...
- datové remanence RAM pamětí
  - podchlazení a zjištění obsahu paměti odpojené od zdroje
  - s pokročilou technikou nevymizelo!

Vzdálené útoky

často využívají poznatků získaných při fyzických útocích

1. útoky na klíče,
   - využívá vztahy mezi klíči, zajištění kompatiblity, zálohy
2. nedostatečná kontrola parametrů,
   - decimalizační tabulka, odvození části PINu, hledání kolizí,
3. nevynucení politiky,
   - zneužívání API bez bezpečnostní politiky (PKCS #11),
4. útoky na USB rozhraní tokenů

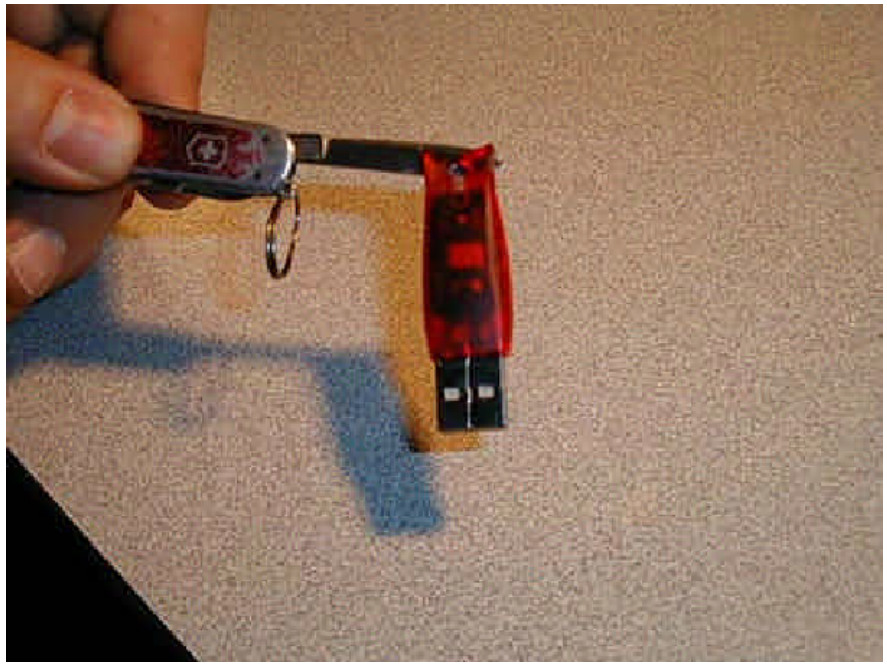
K čemu je to dobré?

Studie @stake útoku na zařízení:

- Alladin eToken
- iKey 1000
- iKey 2000

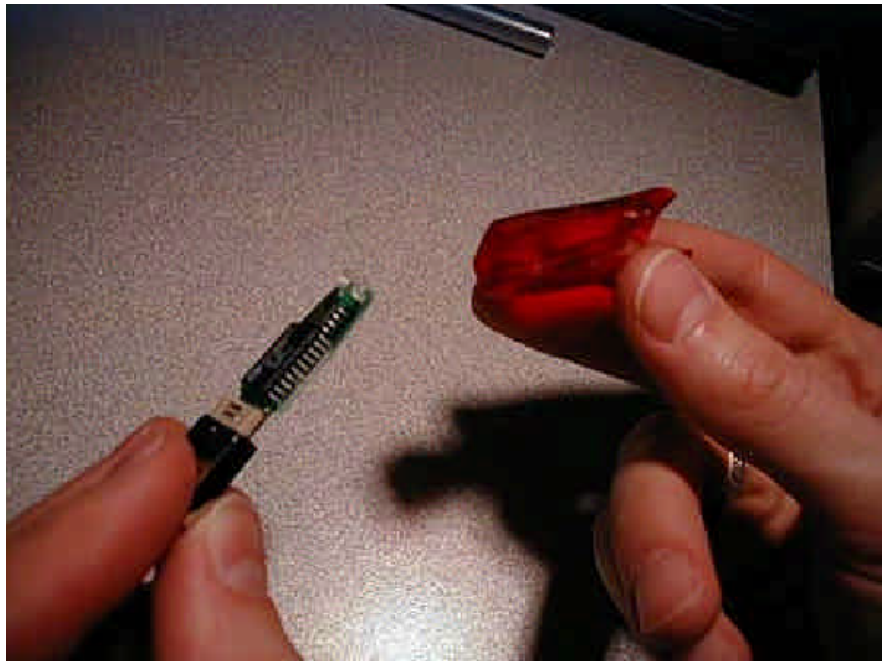
Alladin eToken R1

příprava vzorku



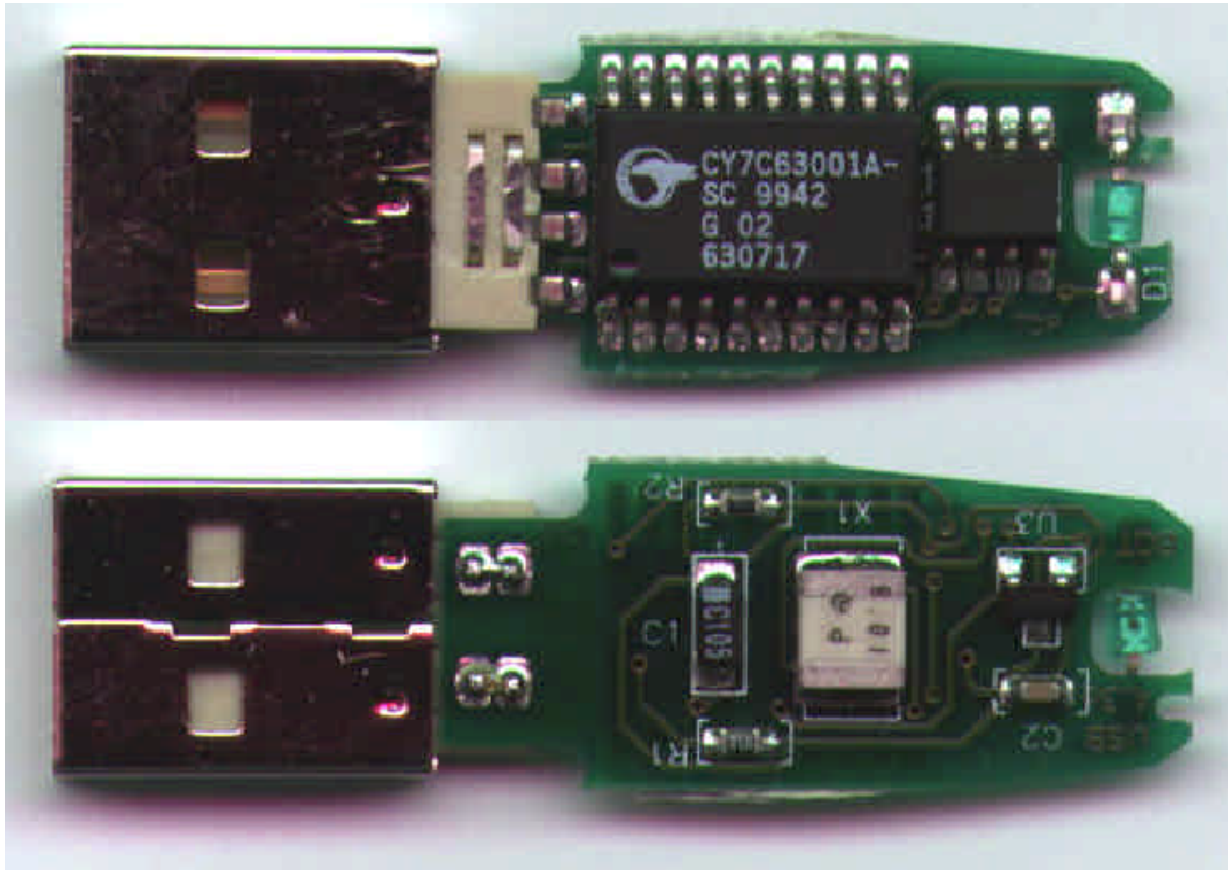
Alladin eToken R1

příprava vzorku (2)



Alladin eToken R1

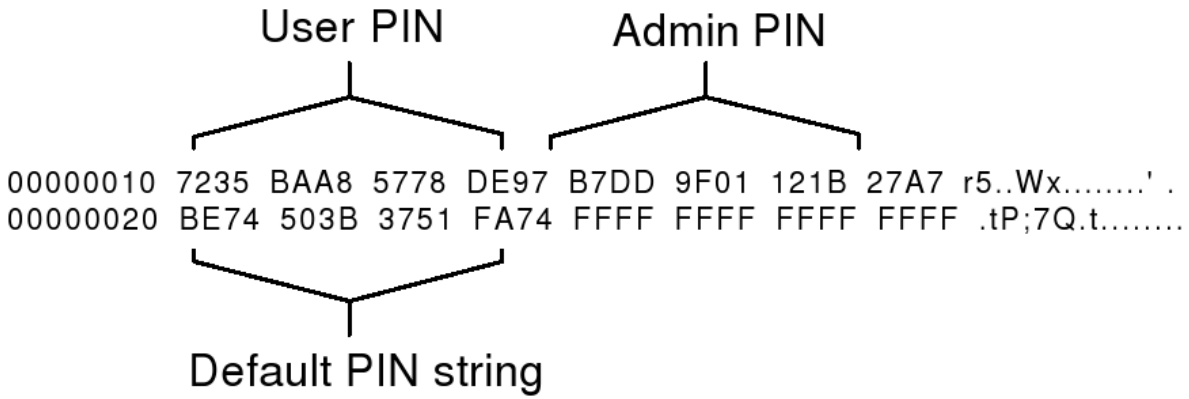
detail, analýza zařízení



Alladin eToken R1

práce s EEPROM pamětí

- s volně přístupnou EEPROM pamětí je možné ji celou přečíst
- mapa paměti
- uložení PINů



- .. i jejich možný přepis

```
00000010 BE74 503B 3751 FA74 B7DD 9F01 121B 27A7 .tP;7Q.t.....' .
00000020 BE74 503B 3751 FA74 FFFF FFFF FFFF FFFF .tP;7Q.t.....
```

Alladin eToken R1

shrnutí

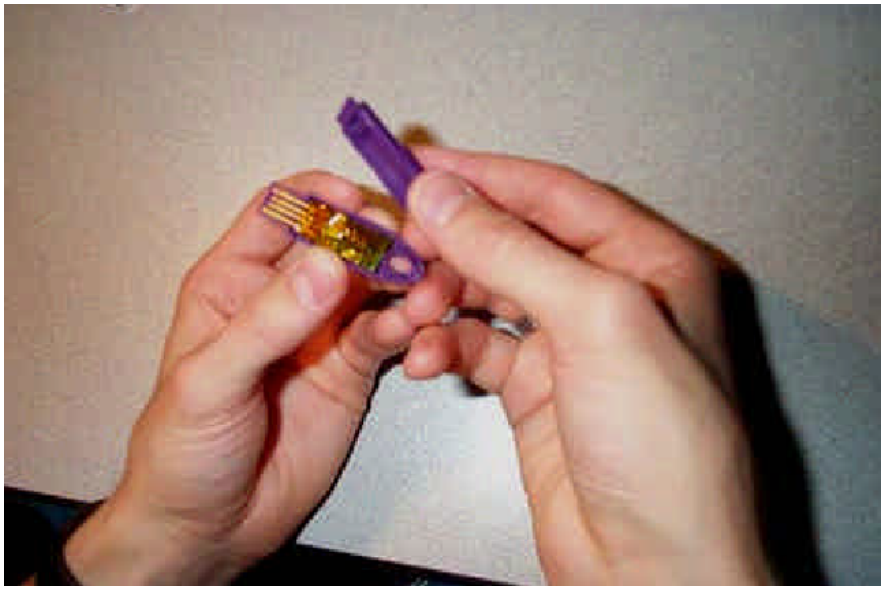
- odstranění prvního obalu relativně snadné (lepidlo)
- žádná další ochrana, obvod snadno analyzovatelný
  - EEPROM volně dostupná!
- snadno zjistitelný způsob uložení PINu v paměti

Rainbow Technologies iKey 1000/2000

příprava vzorku

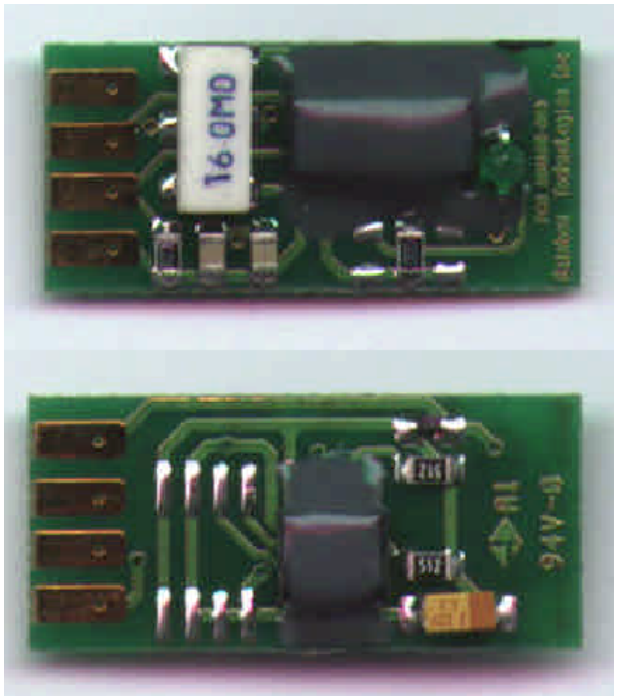
Rainbow Technologies iKey 1000/2000

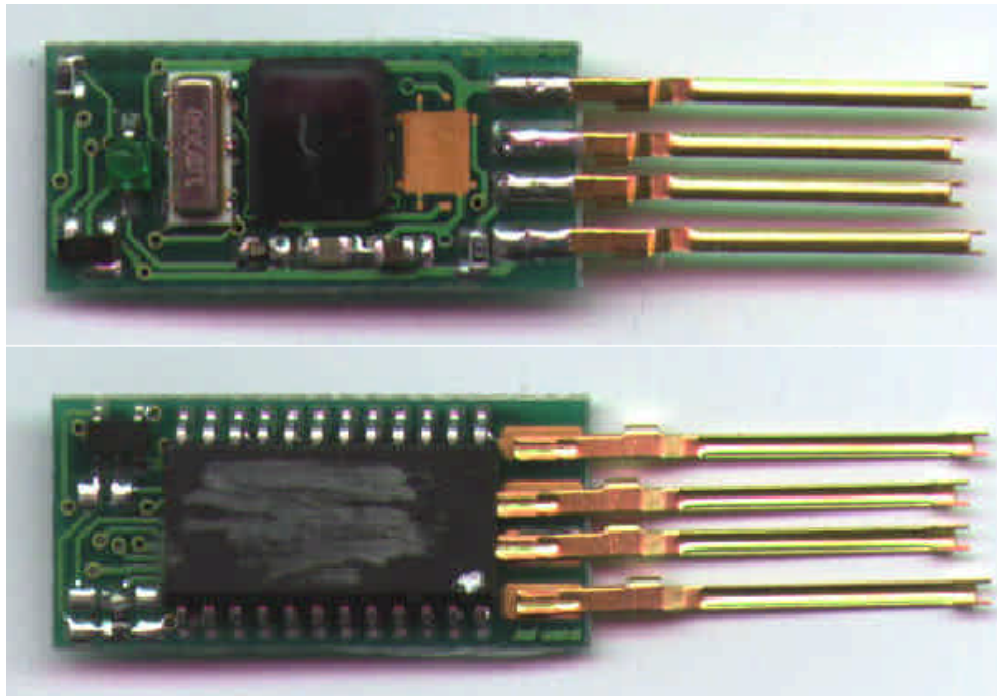
příprava vzorku (2)



Rainbow Technologies iKey 1000/2000

detail, analýza zařízení





Rainbow Technologies iKey 1000/2000

uložení hesla

- jedno heslo pro přístup k datům
- zařízení obdrží jen MD5 hash hesla
- interní uložení se však liší:

- stačí však pár pokusů...

Rainbow Technologies iKey 1000/2000

shrnutí

- odstranění prvního obalu triviální
- snaha o matení útočníka, obrana čipů (zalití do epoxidu)
- modulární výroba, nepotřebné součásti
  - přístup k EEPROM!
- nedokonalý způsob práce s uložením hesla

Možné softwarové útoky

- USB útoky
  - nevalidní pakety
  - nedokumentované příkazy
- útok na délku hesla
  - 8bitový procesor zvládne porovnat jen jeden znak v jednom průchodu..
- shrnutí, doporučení

Klasifikace útočníků

- 0 *(script kiddies)*
  - využívají volně dostupné nástroje a zveřejněné zranitelnosti
- 1 *(clever outsiders)*
  - inteligentní útočníci bez dostatku informací o systému
- 1.5
  - útočníci hledající i nové slabiny (např. specializovaná univerzitní pracoviště provádějící výzkum v dané oblasti)
- 2 *(knowledgeable insiders)*
  - jedinci nebo týmy s nákladným vybavením, schopni provést analýzu v dostatečném čase
- 3 *(funded organizations)*
  - vysoce kvalifikované týmy, běžně nedostupná zařízení; vyvíjejí komplexní útoky za pomocí nejnovějších analytických nástrojů (např. NSA)

Odolnost HW

Invazivní útoky:

Typ útoku	Mikrokont.		Čipové karty		HSM	
	út.	čas	út.	čas	út.	čas
preparace čipu	≥ 1	hod.	≥ 1	hod.	≥ 3	měs.
rekonstrukce a analýza čipu	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
testování čipu s využitím mikrosond	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
čtení paměti nebo modifikace čipu	$\geq 1,5$	dny	≥ 2	dny	≥ 3	měs.

Odolnost HW

Semi-invazivní útoky:

Typ útoku	Mikrokont.		Čipové karty		HSM	
	út.	čas	út.	čas	út.	čas
UV záření	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
ozáření CMOS tranzistorů	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
mikrovlnné radiace	$\geq 1,5$	dny	–	dny	≥ 3	měs.
chybová analýza	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.

Odolnost HW

Neinvazivní útoky:

Typ útoku	Mikrokont.		Čipové karty		HSM	
	út.	čas	út.	čas	út.	čas
výkonová analýza	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
časové útoky	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
diferenciální elektromagnetická analýza	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
datové remanence	$\geq 1,5$	dny	$\geq 1,5$	dny	≥ 3	měs.
reverse engineering	≥ 1	týd.	≥ 1	týd.	≥ 1	měs.

Otázky?

Děkuji za pozornost. . .