AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií

Bezpečnosť informačných technológií

Analýza bezpecnostnych kariet NFC a RFID - prakticka cast

Autor: **Tomáš Kiss**
ak. rok: **2022/2023 LS**

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

Github repozitár ku praktickej časti zo snímkami a videami:
https://github.com/TomasKiss18/Semestral-bit

Praktická analýza karty Mifare Classic:

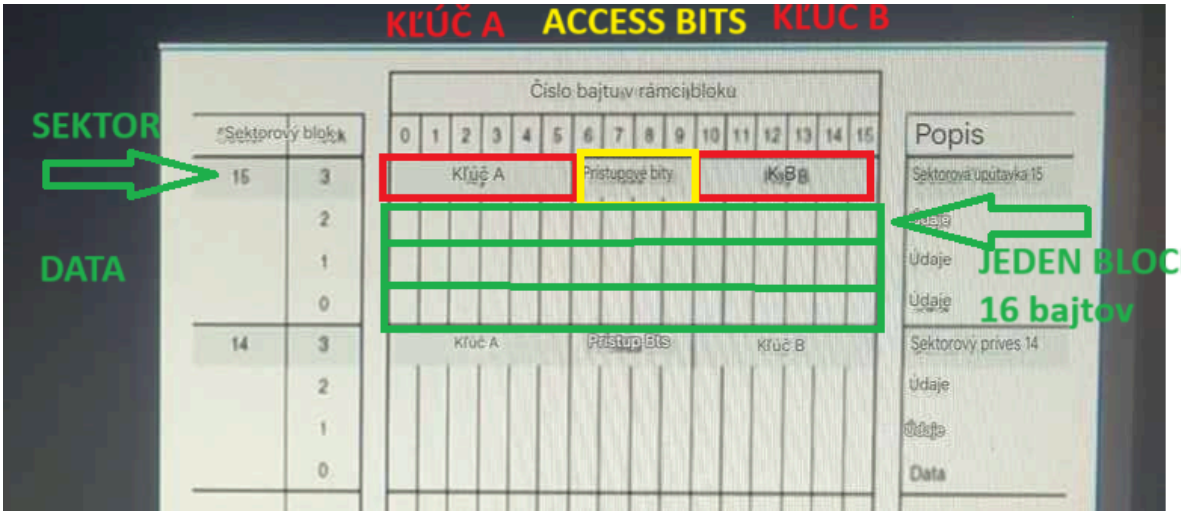
V rámci praktickej časti analýzy sme sa hlbšie pozreli na štruktúru **sektorov a blokov** na MIFARE Classic karte. Táto karta je rozdelená do viacerých sektorov, pričom každý sektor pozostáva zo **štyroch blokov** s veľkosťou **16 bajtov**. Sektory a bloky majú rôzne funkcie, ktoré môžeme rozdeliť nasledovne:

1. **Sektor a bloky**
    - **Sektor**: Základná jednotka organizácie dát na karte. Každý sektor obsahuje 4 bloky.
    - **Jeden blok**: Má veľkosť **16 bajtov** a môže ukladať buď dáta, alebo špecifické konfiguračné údaje.
    - **Dáta**: Bloky 0 až 2 (v sektore) sú väčšinou určené na ukladanie dát. Tieto bloky sa využívajú na zapisovanie alebo čítanie informácií, ktoré karta potrebuje prenášať.
2. **Sektor Trailer (Blok 3)**
    - Posledný blok každého sektora (blok 3) je špeciálny a nazýva sa **Sektor Trailer**.
    - Obsahuje:
        - **Kľúč A (Key A)**: Prvých 6 bajtov bloku. Používa sa na autentifikáciu pred prístupom k dátam v sektore.
        - **Access Bits**: 4 bajty určujúce prístupové práva jednotlivých blokov v rámci sektora. Definujú, či je možné bloky čítať, zapisovať, alebo ich zablokovať.
        - **Kľúč B (Key B)**: Posledných 6 bajtov. Kľúč B môže slúžiť na autentifikáciu alebo na ochranu Access Bitov pred modifikáciou.
3. **Access Bits**

- **Access Bits** sú mimoriadne dôležité pre riadenie bezpečnosti karty. Sú uložené v 4 bajtoch a určujú:
  - Prístup k jednotlivým blokom (čítanie, zápis, aktualizácia).
  - Práva na úpravu kľúčov A a B.
- Hodnoty Access Bitov sa zapisujú v binárnom tvare a ich nesprávne nastavenie môže spôsobiť stratu prístupu k dátam.

4. **Kľúče (Key A a Key B)**
   - **Key A** a **Key B** poskytujú dvojitú vrstvu ochrany. Pred prístupom k dátam je potrebná autentifikácia pomocou týchto kľúčov.
   - Kľúče sú unikátne pre každý sektor a môžu byť nakonfigurované pre rôzne úrovne prístupu.

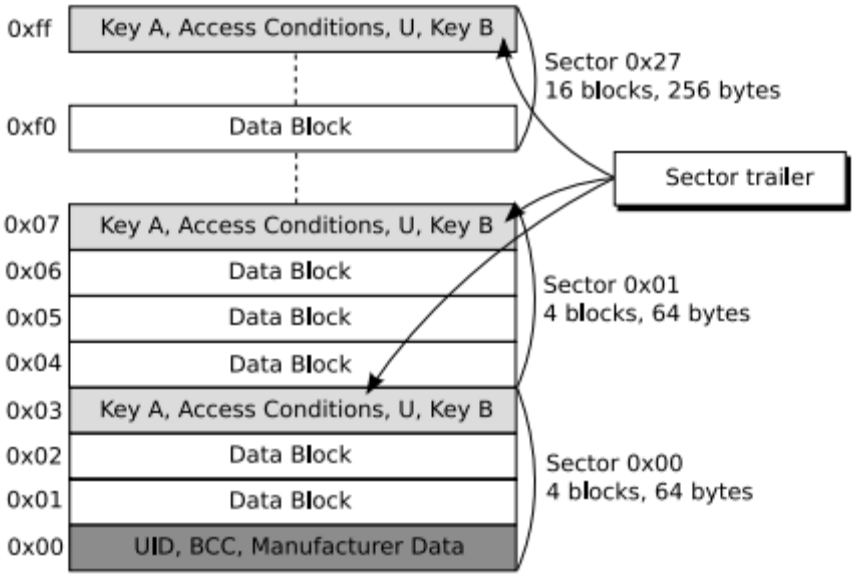
Aktívne rozdelenie:



[1]

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

Špecifikácia rozdelenia blokov karty **mifare Classic 4k Memory:**



[2]

Tiež tabuľka, ktorá poukazuje na jednotlivé časti karty.

Záver k analýze

Na základe týchto častí je možné lepšie pochopiť fungovanie MIFARE Classic karty a jej organizácie dát. Znalosť Sektor Trailer, Access Bitov a správna konfigurácia **Kľúča A** a **Kľúča B** sú kritické pre zabezpečenie informácií na karte a ich správne používanie.

Dôležité upozornenie pri praktickej časti:

Nakoľko sme mali k dispozícii len starú **neaktívnu Mifare Classic kartu ISIC(alebo novú avšak MIFARE DESfire)**, a nemali sme príslušnú funkčnú čítačku/bránu na overenie funkcionality, proces pri ktorom Flipper Zero dokáže čítačku detegovať (DETECT READER) sme **nemali možnosť aplikovať v praxi**. Navyše, s prelomenou kartou, ktorá je už **deaktivovaná** sa nedostaneme nikam.

ISIC karty

Mifare Classic

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

```
Filetype: Flipper NFC device
Version: 3
# Nfc device type can be UID, Mifare Ultralight, Mifare Classic, Bank card
Device type: Mifare Classic
# UID, ATQA and SAK are common for all formats
UID: E4 00 4B 3D
ATQA: 00 02
SAK: 18
# Mifare Classic specific data
Mifare Classic type: 4K
Data format version: 2
# Mifare Classic blocks, '??' means unknown data
Block 0: E4 00 4B 3D 92 98 02 00 E0 8E 18 D5 45 60 28 12
Block 1: 68 00 2A 97 C6 7F 47 28 02 07 3E 31 00 00 C1 00
Block 2: 49 4D 00 50 53 42 41 43 46 4E 4E 00 00 00 7A 00
Block 3: 53 3C B6 C7 23 F6 08 77 8F 69 ?? ?? ?? ?? ?? ??
Block 4: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
Block 5: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
Block 6: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
Block 7: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
Block 8: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 9: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block 11: 58 7E E5 F9 35 0F 08 77 8F 69 ?? ?? ?? ?? ?? ??
Block 12: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
Block 13: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
Block 14: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
```

Mifare DESfire

Zachytené UID ktoré som zamazal nakoľko karta je stále aktívna.

```
1  Filetype: Flipper NFC device
2  Version: 3
3  # Nfc device type can be UID, Mifare Ultralight, Mifare Classic, Bank card
4  Device type: Mifare DESFire
5  # UID, ATQA and SAK are common for all formats
6  UID: 04 2F [redacted] D8 69 [redacted]   ISIC UID
7  ATQA: 03 44
8  SAK: 20
9  # Mifare DESFire specific data                                  ISIC UID
10 PICC Version: 04 01 01 01 00 1A 05 04 01 01 01 04 1A 05 04 2F [redacted] D8 69 [redacted] B9 0C 10 41 90 10 20
11 PICC Free Memory: 1120
12 PICC Change Key ID: 00
13 PICC Config Changeable: true
14 PICC Free Create Delete: false
15 PICC Free Directory List: true
16 PICC Key Changeable: true
17 PICC Max Keys: 01
18 PICC Key 0 Version: 02
19 Application Count: 7
20 Application IDs: [redacted]
```

Emulácia karty Mifare DESfire:

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

Celé video: https://www.youtube.com/@tomaskiss2723/shorts

Skenovanie iných RFID kariet

Pri analýze a testovaní skenovania iných kariet sa nám podarilo oskenovať kartu zariadením flipper zero ktorá slúži na vstup do posilňovne. Všetky dáta boli prístupné (najmä potrebné UID zariadenia).

EM4100

```
1   Filetype: Flipper RFID key
2   Version: 1
3   Key type: EM4100
4   Data: 01 0D 7E 63 9A
5
```

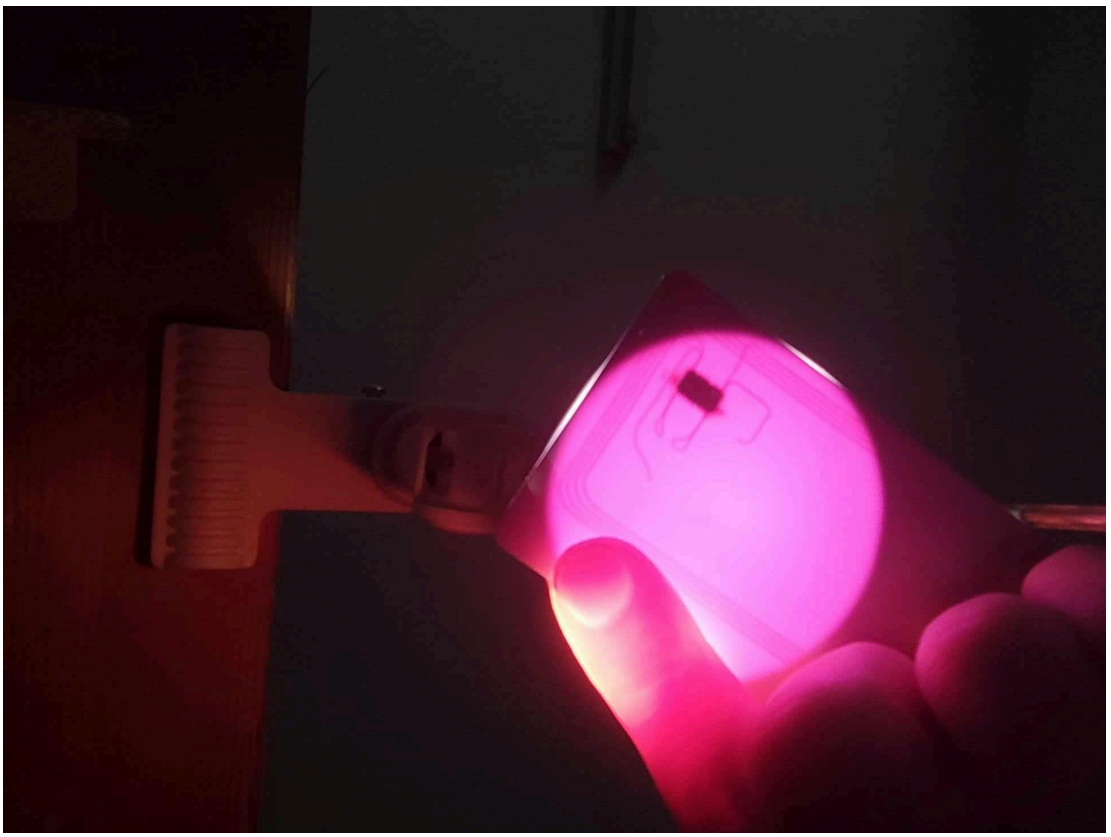
AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

Karty **EM4100** sú bezkontaktné RFID karty pracujúce na frekvencii **125 kHz**. Majú **jednoduchý formát** so **64-bitovým jedinečným identifikátorom (UID)**, ktorý je nemenný a slúži na identifikáciu. Karta neobsahuje žiadnu pamäť na zapisovanie dát, uchováva iba tento **fixný 10-miestny identifikátor**.

Jednoduchá fyzická karta.

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

DUAL LINE -čítačka kariet pri emulácii COMINFO s podporou bezpečnostných kariet DES 3DES, AES podľa špecifikacií karty celkom 128 overovacich klúčov 64 bit (alebo 64 kľúčov 128 bit)

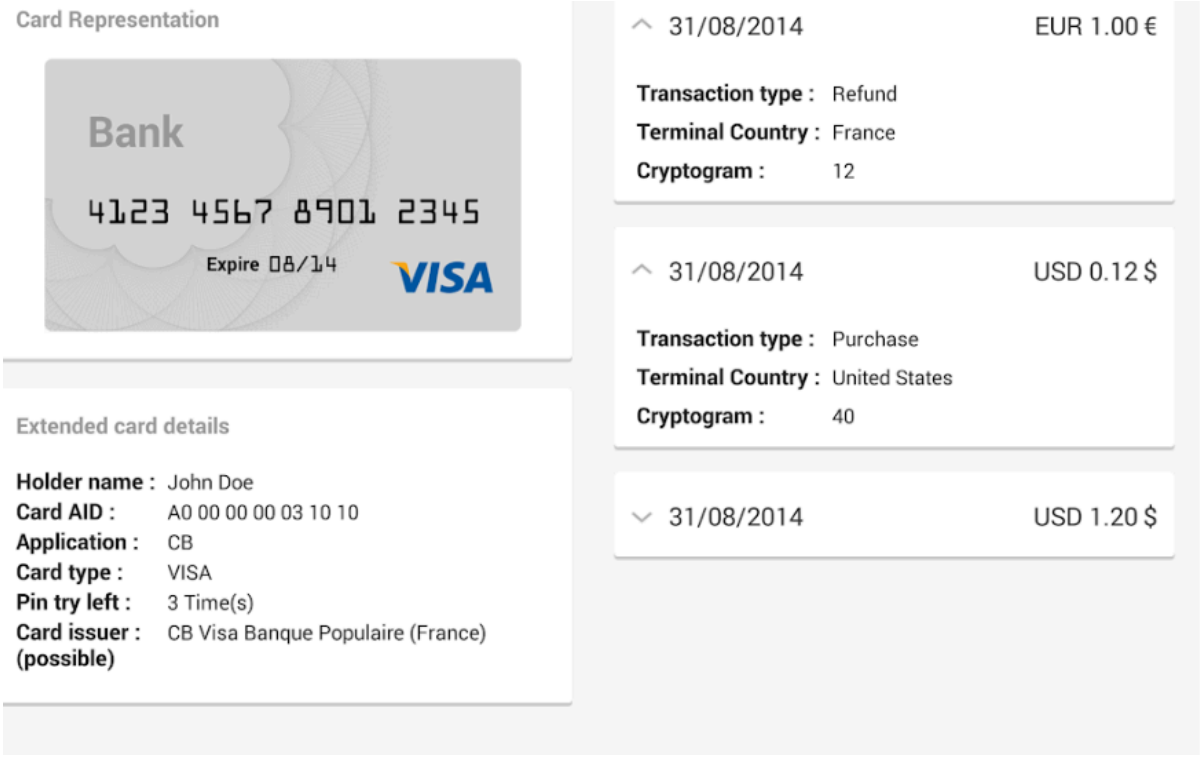


Karta presvietená lambou a môžeme vidieť jej samotné vnútro.

Skenovanie bankomatových kariet

Tento článok od firmy NETHEMBA [3] z roku 2015 sa venoval “too loud” kartám ktoré prezrádzali aj meno držiteľa čo je od zákona GDPR osobná informácia a je to hlboké

porušenie tohto zákonu. Screenshot:



Od roku 2015 prešli platobné karty významným vývojom v oblasti bezpečnosti, najmä v prípade NFC technológie. Moderné karty, ako napríklad **Visa**, implementujú pokročilé bezpečnostné mechanizmy, ktoré minimalizujú riziko neoprávneného čítania citlivých údajov. Na druhej strane, niektoré **Mastercard karty** stále vykazujú slabiny a môžu odhaliť základné platobné údaje, ako je **číslo karty** a **dátum expirácie**, pri pokuse o čítanie pomocou zariadení ako je **Flipper Zero**.

Visa a tokenizácia

Visa karty dnes často využívajú **tokenizáciu**, čo znamená, že údaje prenášané cez NFC sú dynamické a jednorazové. To znemožňuje útočníkovi získať použiteľné informácie na neoprávnené transakcie. Pri pokuse o čítanie Visa kariet môžu zariadenia jednoducho zobraziť informáciu, že dáta nie sú dostupné alebo sú chránené. Tento prístup je v súlade s modernými bezpečnostnými štandardmi, ako je EMV, a zabezpečuje, že NFC transakcie sú rovnako bezpečné ako tradičné čipové platby.

Mastercard a bezpečnostné slabiny

V prípade niektorých Mastercard kariet je situácia odlišná. Staršie alebo menej zabezpečené karty stále umožňujú čítanie statických údajov cez NFC rozhranie. Tieto údaje môžu zahŕňať číslo karty (PAN) a dátum expirácie, čo útočníkom otvára možnosť zneužitia na **online transakcie**, ktoré nevyžadujú CVV kód. Táto zraniteľnosť je často spojená so staršími implementáciami NFC technológie, ktoré nevyužívajú tokenizáciu alebo dostatočné šifrovanie.

Situácia v praxi

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

Ako je vidieť na obrázku, zariadenie **Flipper Zero** dokáže rozpoznať Mastercard kartu a získať základné informácie. Naopak, pokus o čítanie **Visa karty** zlyháva, pretože moderné Visa karty odmietajú poskytnúť akékoľvek dáta bez autentifikácie. Tento rozdiel ukazuje, ako sa bezpečnosť platobných kariet postupne zlepšuje, no zároveň upozorňuje na pretrvávajúce nedostatky v prípade niektorých starších technológií.

Záver

Aj keď sa bezpečnostné mechanizmy NFC platieb neustále vyvíjajú, je dôležité, aby používatelia vedeli o potenciálnych rizikách a ochrane svojich kariet. Moderné Visa karty sú dnes prakticky odolné voči neautorizovanému čítaniu, zatiaľ čo niektoré Mastercard karty môžu stále poskytovať citlivé informácie. Pri podozrení na zraniteľnosť je vhodné kontaktovať banku a požiadať o vydanie novej, bezpečnejšej karty.

Po novom však vnímam výrazné zlepšenie pri bankomatových kartách, obzvlášť tých od VISA Debit card - podla mojho názoru vhodnejšie ako Mastercard.

AIS ID: 110818
Meno a priezvisko: Tomáš Kiss

REFERENCIE

[1] - Zdroj:platforma YouTube https://www.youtube.com/watch?v=mSQkh7F__1w
Autor: Sanga Chidam (čas: 6.12. 18:00)
[2] - DE KONING GANS, Gerhard; HOEPMAN, Jaap-Henk; GARCIA, Flavio D. A practical attack on the MIFARE Classic. In: *International Conference on Smart Card Research and Advanced Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. p. 267-282.
[3] https://nethemba.com/sk/update-bezpecnostna-analyza-platobnych-nfc-kariet/