Fakulta informatiky a informačných technológií

Slovenská technická univerzita v Bratislave

Bezpečnosť informačných technológií

BIT - Analýza bezpečnostných kariet

Autor: Tomáš Kiss

Škola: FIIT STU

Ak. rok: 2024/25

1. Úvod

1.1. Cieľ projektu

Cieľom projektu bola analýza bezpečnostných kariet RFID a NFC(spolu s čítačkami) najmä v študentskom prostredí. Keďže študenti používajú na autentifikáciu do štátneho systému (na pridelenie dotácií za stravu) ako aj na vstup na rôzne miesta(knižnice alebo študijné centrá) **ISIC karty** (International student identity card), rozhodli sme sa hlbšie analyzovať tieto ale okrem iného aj iné karty typu RFID.

V projekte sme sa venovali analýze bezpečnostných vlastností ISIC kariet, ktoré prešli od staršej technológie **Mifare Classic** k novšej generácii **Mifare DESfire**. Nakoľko máme prístup ku starším typom kariet, keďže v tom čase sa ešte používali tie (Mifare Classic) - mohli sme prelamovať tie, avšak nakoľko sú už deaktívne nemali sme možnosť testovať im prislúchajúce čítačky.
Okrem ISIC kariet sme skúmali aj ďalšie karty typu RFID do miestnej posilnovni, zamerali sme sa na možné zraniteľnosti a metódy útokov.

Praktická časť pozostávala z testovania reálnych kariet pomocou zariadenia Flipper Zero, vrátane prelamovania Mifare Classic kariet využitím známych slabín šifrovacieho algoritmu CRYPTO1. Čo sa týka kariet Mifare DESfire, ich prelamovanie je v reálnom čase takmer nemožné. Tento typ kariet využíva pokročilé šifrovacie algoritmy, ako je AES (Advanced Encryption Standard) a 3DES (Triple DES), ktoré zvyšujú úroveň ochrany údajov. Mifare DESfire karty podporujú aj viacúrovňové overovanie a zabezpečenie, čo z nich robí veľmi robustné riešenie, ktoré sa považuje za odolné voči väčšine bežných útokov, vrátane tých, ktoré môžu byť vykonané pomocou zariadení ako Flipper Zero.

Napriek tomu, že prelamovanie Mifare DESfire kariet je veľmi náročné a prakticky neuskutočniteľné v reálnych podmienkach bez prístupu k šifrovacím kľúčom, sme sa v rámci praktickej časti snažili overiť, či sa tieto bezpečné karty skutočne používajú dostatočne bezpečne. Testovali sme, či sú využívané všetky šifrovacie metódy, ktoré karty ponúkajú, a či sa implementujú všetky možné mechanizmy ochrany proti zneužitiu. Zamerali sme sa na emuláciu týchto kariet a na testovanie ich schopnosti autentifikovať a zabezpečiť komunikáciu s čítačkami, ako aj na možnosť manipulácie so systémom v prípade zraniteľností v jeho implementácii.

Hlavným cieľom bolo identifikovať možné riziká, ktoré môžu ohroziť bezpečnosť študentských údajov a systému autentifikácie (impersonalizáciou) - potenciálnym predstieraním inej identity, a tiež navrhnúť opatrenia na ich minimalizáciu.

1.2. Význam analýzy bezpečnosti NFC kariet

Analýza bezpečnosti NFC kariet je kľúčová z dôvodu využitia kariet v každodennom živote, najmä na autentifikáciu, platby a prístupové systémy. V študentskom prostredí, kde sa NFC karty, ako napríklad ISIC používajú , môže narušenie bezpečnosti viesť k neoprávnenému prístupu, zneužitiu citlivých údajov. Identifikácia slabín a správne používanie je preto nevyhnutné na zlepšenie bezpečnosti a ochrany používateľov.

1.3. Prehľad technológií používaných v NFC kartách

V našom projekte sme sa(okrem iného) zamerali na dve najrozšírenejšie NFC technológie, a to **Mifare Classic** a **Mifare DESfire**, ktoré sa dnes bežne používajú v rôznych aplikáciách. Tieto karty sú základom pre mnoho služieb (elektronické peňaženky, prístupové systémy, ale aj pre školské a verejné služby). Typickým príkladom je **ISIC karta**, ktorá umožňuje študentom prístup k rôznym výhodám, ako je využívanie hromadnej dopravy, obedy v jedálňach, alebo vstup do miestností a študovní na školách. ISIC karta tak slúži ako univerzálny preukaz s viacerými funkciami v rámci verejnej a akademickej sféry. Bez nej je študent takpovediac "stratený".

Pre lepšiu prehľadnosť textu sme vytvorili HLAVNÉ POROVNANIE v tabuľke:

Vlastnosti	Mifare Classic	Mifare DESfire
Technológia	Staršia RFID technológia	Pokročilá RFID technológia
Kapacita úložiska dát	1 KB alebo 4 KB	Až do 8 KB
Bezpečnostné vlastnosti	Základná autentifikácia s kľúčmi A a B	Pokročilá autentifikácia s viacerými kľúčmi
Šifrovanie	Žiadne šifrovanie alebo slabé šifrovanie	Šifrovanie AES, 3DES
Protokoly	ISO/IEC 14443A	ISO/IEC 14443A/B, ISO/IEC 15693
Autentifikácia	Jednostupňová autentifikácia	Viacstupňová autentifikácia a šifrovanie
Bežné použitie	Prístupové systémy, doprava a vernostné karty	Bezpečné platobné systémy, prístupové systémy, univerzitné karty

Ku tabuľke prislúchajúci text:

1.3.1. Mifare Classic

- Ide o staršiu a jednoduchšiu technológiu, ktorá sa často používa v prístupových systémoch. Karty majú kapacitu 1 KB alebo 4 KB a údaje sú uložené v sektoroch, pričom každý sektor je rozdelený na bloky.
- Bezpečnosť je zabezpečená autentizačnými kľúčmi A a B, ktoré umožňujú prístup k rôznym blokom dát v rámci karty. Avšak, **Mifare Classic karty sú zraniteľné a bezpečnosť bola viackrát úspešne narušená** pomocou rôznych útokov, čo z nich robí menej bezpečnú voľbu pre citlivé aplikácie.
- Tieto karty používajú protokol ISO/IEC 14443 typu A [2], ktorý je štandardom pre RFID, ale aj tento protokol má svoje slabiny, ktoré môžu byť zneužité na získanie prístupu k údajom.

1.3.2. Mifare DESfire

- Mifare DESfire karty predstavujú **pokročilejšiu technológiu**, ktorá ponúka výrazne vyššiu úroveň bezpečnosti v porovnaní s Mifare Classic. Karty DESfire používajú **kryptografické algoritmy ako 3DES a AES**, čo zaručuje oveľa silnejšiu ochranu uložených dát a komunikácie medzi kartou a čítačkou.
- Tento typ kariet je vhodný pre aplikácie, ktoré vyžadujú vysokú úroveň ochrany, ako napríklad **bezkontaktné platby** alebo prístup do citlivých oblastí. Karty DESfire sú tiež schopné vykonávať **viacúrovňové autentifikácie** a podporujú **šifrovanie dát**, čo ich robí oveľa odolnejšími voči bežným útokom.

Preukaz ISIC sa používa tak, že na čip v preukaze si môže študent nahrať napríklad elektronickú peňaženku (električenku v MHD, vlakoch, autobusovej doprave...), ale aj na obedy v škole, prístupy do niektorých miestností, na plaváreň či do knižnice. [1] Zvyčajne túto aktivitu vykonávajú tretie strany ako napriklad:

[aktiváciu karty] - fakulty
[aktiváciu bezplatnej prepravy na železniciach v SR] - Železnice slovenskej republiky

[prístup do jedální alebo objektov internátov] - Terminál tretej strany pri objekte

2. Analýza problémovej oblasti a existujúcich riešení

Hypotéza pre MIFARE CLASSIC je takáto:

“ISIC karta využívajúca technológiu MIFARE Classic môže byť zneužitá v dôsledku známych zraniteľností v jej architektúre a slabosti šifrovacieho algoritmu CRYPTO1.**”**

Mifare Classic karty sú jedným z najrozšírenejších typov NFC kariet, používaných v prístupových systémoch, verejnej doprave či parkovacích službách. Hoci boli populárne pre svoju cenovú dostupnosť a jednoduchú integráciu, obsahujú vážne bezpečnostné nedostatky, ktoré umožňujú ich relatívne jednoduché prelomenie, napríklad pomocou zariadení ako **Flipper Zero**. Na toto je však priam nevyhnutné okrem zariadenia Flipper Zero mať potrebný fyzický prístup ku dvom veciam. Samotnej karte a čítačke ktorá túto kartu číta, aby mohol white hat hacker/ penetračný tester preukázať zraniteľnosť.

[3]

Hypotéza pre MIFARE DESfire je takáto:

“Zneužitie ISIC karty môže nastať v prípade jej naskenovania a emulácie, čím je držiteľ karty vystavený riziku pri strate alebo požičiavaní svojej karty.“

MIFARE DESfire karty predstavujú modernejšiu a bezpečnejšiu technológiu v porovnaní s Mifare Classic, najmä vďaka pokročilým šifrovacím mechanizmom, ako je AES. Napriek tomu, že prelomenie ich šifrovania je v reálnom čase prakticky nemožné, ich bezpečnosť stále závisí od implementácie systému a správania používateľov.

V praktickej časti sme úspešne preukázali, že **naskenovaním karty a jej následnou emuláciou** je možné vykonať **autentifikáciu na čítačke** a získať prístup do objektu internátov na Mlynskej doline. Okrem toho sme zistili, že je takýmto spôsobom možné opätovne čerpať **štátnu dotáciu na stravu**, čo môže naznačovať desynchronizáciu databáz alebo nedostatočné overovanie karty zo strany systému.

Tento fakt poukazuje na zraniteľnosť, ktorá môže nastať pri **stráte alebo neoprávnenom použití karty**, čím sa majiteľ karty vystavuje potenciálnemu riziku zneužitia. Naším cieľom bolo toto riziko preukázať eticky, použitím vlastnej karty a dodržaním všetkých zásad bezpečnostného testovania.

2.1. Historické pozadie a vývoj ISIC kariet

Firma v nedávnej dobe 5 a viac rokov udelovala Mifare Classic karty ale postupne (aspoň vysokoškolským študentom) začala vydávať robustnejšie(tým pádom aj drahšie) karty Mifare DESfire s bezpečnostnejšou kryptografiou a viac zabezpečenými a šifrovanými sektormi.

2.2. Bezpečnostné slabiny Mifare Classic (CRYPTO1 algoritmus)

Nebezpečenstvá algoritmu CRYPTO1

Algoritmus **CRYPTO1**, použitý v Mifare Classic kartách, bol navrhnutý ako proprietárne riešenie, pričom jeho dizajn bol pôvodne utajovaný a patentovaný. Paradoxne, práve **tajnosť algoritmu** zvýšila jeho riziko, pretože neprešiel nezávislou kryptografickou analýzou, ktorá je štandardnou praxou pre zabezpečené algoritmy. Reverzné inžinierstvo neskôr odhalilo niekoľko zásadných bezpečnostných nedostatkov:

1. Krátka dĺžka kľúča (48-bitový kľúč)

- Na šifrovanie používa CRYPTO1 iba **48-bitové kľúče**, čo je v porovnaní s modernými štandardmi, ako je **AES-128** alebo vyššie, extrémne nedostatočné.
- Útok hrubou silou (brute-force) je preto realizovateľný v krátkom čase s využitím moderného hardvéru, ako sú FPGA alebo zariadenia typu Flipper Zero. Tým je možné relatívne rýchlo získať kľúč a následne získať prístup k dátam na karte.

2. Slabé generovanie náhodných čísel (nonce)

- CRYPTO1 používa pseudonáhodné čísla (**nonce**) počas autentifikácie medzi kartou a čítačkou. Generovanie týchto čísel je však **predvídateľné** a opakovateľné.
- Táto slabina umožňuje tzv. **útoky opakovaním (replay attack)**. Útočník môže zachytiť komunikáciu medzi kartou a čítačkou, spätne analyzovať prenášané údaje a pomocou týchto údajov emulovať autentickú kartu. V prípade zariadenia Flipper Zero toto zariadenie priamo emuluje kartu a tvári sa ako karta samotná, zachytí kľúče ktoré čítačka pošle a neskôr je možné na základe poslaných kľúčov kartu prelomiť.

3. Nedostatočná ochrana pred útokmi postranných kanálov

- CRYPTO1 nevykonáva žiadne opatrenia na ochranu pred tzv. **útokmi z kanálov postranných informácií** (side-channel attacks).
- Tieto útoky zahŕňajú napríklad **analýzu elektromagnetického žiarenia**, ktoré karta generuje pri komunikácii, alebo **meranie spotreby energie** počas výpočtu autentifikácie. Na základe týchto fyzických meraní môže útočník získať **informácie o šifrovacom kľúči** alebo o prebiehajúcich operáciách.

3.1. Analýza

Vylepšenia v Mifare DESfire (AES šifrovanie)

a) Pokročilé šifrovanie

- **AES-128 (Advanced Encryption Standard):** Poskytuje silnú ochranu dát vďaka modernému šifrovaniu, ktoré je odolné voči bežným útokom.
- **3DES (Triple Data Encryption Standard):** Možnosť používať aj starší, ale stále bezpečný štandard šifrovania.
- Oproti slabému CRYPTO1 algoritmu (Mifare Classic) je DESFire prakticky imúnna voči známym útokom ako kryptoanalýza alebo útoky na slabé kľúče.

b) Bezpečná autentifikácia

- Využíva **vzájomnú autentifikáciu** (mutual authentication) medzi kartou a čítačkou, čím predchádza neoprávnenému prístupu.
- Podporuje rôzne bezpečnostné úrovne, vrátane šifrovania komunikácie medzi kartou a čítačkou.

c) Aplikácie na karte

- Karta umožňuje vytváranie až 28 samostatných aplikácií s nezávislými kľúčmi.
- Každá aplikácia môže obsahovať až 32 súborov, čo poskytuje vysokú flexibilitu na použitie pre rôzne účely (napr. lístky, prístupové kľúče, platby).

RFID je bezdrôtová, bezkontaktná technológia, ktorá používa elektromagnetické pole na identifikáciu čipov. Zvyčajne sa pri týchto technológiách bavíme o pasívnych tagoch/kartách. Spôsob, akým tieto karty fungujú, je ten, že **neobsahujú vlastný zdroj energie, ale aktivujú sa elektromagnetickým poľom generovaným čítačkou**. Toto elektromagenticke pole karta zachytí na anténe na ktorej sa naindikuje dostatocne malý prúd ktorý je schopný poháňať čip v čítačke ktorý už ďalej dokáže komunikovať s čítačkou.

Táto bezdrôtová komunikácia zjednodušuje používanie, no zároveň otvára priestor na rôzne typy útokov, ako je napríklad **odpočúvanie, emulácia alebo manipulácia s dátami**. Preto je dôležité používať moderné RFID/NFC technológie, ktoré implementujú bezpečné autentifikačné protokoly a šifrovanie, aby sa minimalizovalo riziko neoprávneného prístupu.

3.2. Popis vykonaných testov na Mifare Classic kartách

1. Brute-force útok na získanie kľúčov

Útočník priamo využije zariadenie **Flipper Zero** na útok brute force s predvolenými (defaultnými) kľúčmi, ktoré sú súčasťou jeho zoznamu na Flipperi. ->MENU ->NFC->READ

- Flipper Zero systematicky testuje **štandardné kľúče** pre jednotlivé sektory Mifare Classic karty, ktoré sú známe z verejných databáz a často sa používajú v implementáciách prístupových systémov.
- Tento proces prebieha bez potreby ďalšej prípravy alebo komunikácie s čítačkou – Flipper Zero pracuje priamo s kartou.

[5]

2. Získanie kľúčov

Flipper Zero iteratívne testuje kľúče na všetkých sektoroch karty. Ak sa kľúč zhoduje s tým, ktorý zabezpečuje daný sektor:

- **Autentifikácia je úspešná**, a Flipper Zero získa prístup k dátam uloženým v sektore.
- Vďaka slabinám algoritmu **CRYPTO1** a krátkej dĺžke kľúča (48 bitov) je tento proces **veľmi rýchly** a realizovateľný v krátkom čase.

3. Prístup k sektorom karty

Po úspešnom prelomení autentifikácie pre konkrétny sektor môže Flipper Zero:

- Prečítať obsah sektora, vrátane dát, ako sú **identifikátory, kredity** alebo **prístupové údaje**.
- Tento proces sa opakuje pre všetky sektory karty, až kým nie je zabezpečený **kompletný prístup** ku dátam.

Vidíme že nie ku všetkým dátam sa Flipper dostal:

sem_projekt > Isic_clasic_no_foto.nfc

```
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: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
```

Toto môže byť spôsobené aj samotným chýbajúcim elementom funkčnej čítačky (nakľko sme overovali starú kartičku ISIC)->

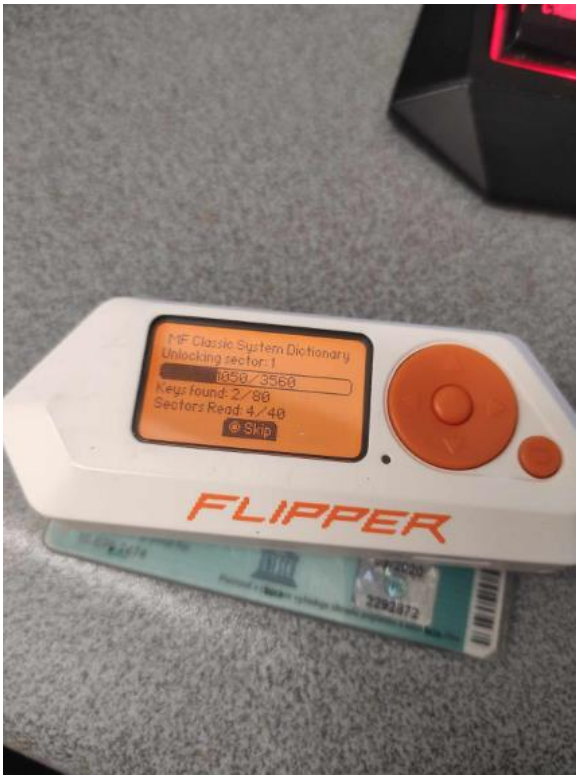
Dôležité upozornenie!

Nakoľko sme mali k dispozícii len starú **neaktívnu Mifare Classic kartu ISIC**, 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**, nie je možné získať prístup k reálnym systémom.

3.3. Použité zariadenia a nástroje

Pomocou slovníkových útokov v zariadení Flipper Zero sme sa snažili prelomiť niektoré sektory tejto Mifare CLASSIC karty ako je možné vidieť v nasledujúcom obrázku.

Tento útok vyzeral nasledovne ako zariadenie flipper postupne Brute Force metódou testovalo všetky dostupné kľúče nachádzajúce sa v slovníkovom útoku. Ilustračné obrázky sú nižšie.




```
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: ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
```

Ďalšou časťou bola emulácia aktívnej **novej a aktívnej** karty MIFARE DESfire kde sme testovali či Flipper umožní naskenovanie a dostatočne dobrú emuláciu na to aby sme cez bránu internátov prešli. A ako naznačuje zelené svetlo čítačky, emulácia bola úspešná. Viac vo videu tu: https://www.youtube.com/shorts/8yg_9dSLyC4

(Screenshot z videa)

3.6. Použitý software

Používali sme dodatočne doinštalovaný software s platformi github.

3.7 Aktuálne ISIC karty

Aktuálne vydávané ISIC karty už využívajú modernú technológiu Mifare DESFire, ktorá implementuje pokročilé bezpečnostné opatrenia, ako je šifrovanie pomocou algoritmu AES a robustné autentifikačné protokoly. Vďaka týmto technológiám je prelomenie karty prakticky nemožné žiadnym známym spôsobom, čo výrazne zvyšuje ochranu osobných údajov a bezpečnosť používateľov.

Napriek tomu sa v minulosti ukázali iné potenciálne bezpečnostné riziká spojené s používaním ISIC kariet. Jedným z nich bola možnosť neoprávneného prístupu do objektu Átriových domov, kde sa karta používala na otváranie dverí. Ďalším rizikom bolo zneužitie štátnej dotácie na jedlo v reštaurácii Eat&Meet, kde neboli dostatočne zavedené overovacie mechanizmy.

Útočník mohol napríklad naskenovať ISIC kartu inej osoby bez jej vedomia, čo mu umožnilo získať prístup k rovnakým výhodám. Tento scenár poukazuje na riziko spojené s nedostatočnou kontrolou používateľa pri overovaní v reštaurácii, kde sa využitie karty neoverovalo voči jej skutočnému majiteľovi. Tento problém je vážnym bezpečnostným rizikom, ktoré si vyžaduje doplnenie systému o dodatočné overovacie prvky, napríklad PIN kód, biometrické údaje alebo fotoidentifikáciu pri používaní kariet.
Viac o tomto na mojom Youtube kanály v shorts:
https://www.youtube.com/@tomaskiss2723/shorts

4 Výsledky analýzy

Donedávna boli **ISIC karty** vydávané prevažne len vo formáte Mifare Classic, avšak v súčasnosti prešli na bezpečnejší formát Mifare DESfire. Tento prechod predstavuje **významné zlepšenie bezpečnosti**, keďže karty Mifare DESfire ponúkajú **vyššiu ochranu údajov a silnejšie šifrovanie**, čo je dôležité pre moderné aplikácie využívajúce NFC technológie.

Mifare DESFire karty prinášajú zásadné vylepšenia v šifrovaní, správe aplikácií a kompatibilite s modernými systémami. Vďaka pokročilým bezpečnostným funkciám sú vhodné na citlivé aplikácie, ako sú platobné systémy, elektronické lístky či prístupové kľúče. Oproti Mifare Classic sú oveľa bezpečnejšie a odolné voči bežným útokom.

5. Záver

Projekt sa zaoberal analýzou bezpečnostných rizík spojených s používaním technológie Mifare v kartových systémoch a možnosťami ich zneužitia. V rámci analýzy sme identifikovali zraniteľnosti starších Mifare Classic kariet, ktoré sú vďaka slabému šifrovaciemu algoritmu CRYPTO1 náchylné na útoky, vrátane ich prelamovania pomocou zariadení ako Flipper Zero. Ukázali sme, že moderné Mifare DESFire karty implementujú výrazne bezpečnejšie mechanizmy, ako je šifrovanie AES a viacstupňová autentifikácia, čím eliminujú riziká spojené s prelomiteľnosťou samotnej karty.

Napriek technologickému pokroku sa však odhalili iné riziká spojené s procesmi overovania a používania ISIC kariet, ktoré nie sú dostatočne zabezpečené na úrovni systémov, ktoré tieto karty využívajú. Možnosť neoprávneného prístupu alebo zneužitia výhod, ako napríklad štátnej dotácie, upozorňuje na potrebu zlepšenia bezpečnostných kontrol pri autentifikácii používateľov.

Na základe týchto poznatkov projekt odporúča zavedenie dodatočných overovacích mechanizmov, ktoré by zabránili zneužitiu kariet tretími stranami. Tieto opatrenia by mohli zahŕňať overenie totožnosti prostredníctvom PIN kódu, biometrických údajov alebo integrácie so smartfónmi pre dodatočné overenie.

Projekt zároveň poukazuje na neustálu potrebu monitorovania a zlepšovania bezpečnostných štandardov, a to nielen na úrovni technológie kariet, ale aj v rámci celkového ekosystému, ktorý ich využíva. Týmto spôsobom možno zaistiť bezpečné a dôveryhodné používanie kartových systémov pre široké spektrum aplikácií.

6. Zoznam použitej literatúry

[1] - https://isic.sk/univerzitny-vysokoskolsky-preukaz-studenta-isic/

[2] - https://www.rfidcard.com/iso-iec-14443-identification-contactless-proximity-rfid-cards-standard/

[3] - https://cyberinitiative.org/talent-development/project-based-learning-program/flipper-zero--microsoft-project-based-learning-program.html

[4] Winston, Joy. "Evaluating Iot Device Security: Penetration Testing and Vulnerability Assessment with Flipper Zero." *Available at SSRN 4658141*.

[5] - 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.

[6] - Zdroj:platforma YouTube https://www.youtube.com/watch?v=mSQkh7F__1w
Autor: Sanga Chidam (čas: 6.12. 18:00)