Eliminarea Slăbiciunilor Accesului bazat pe Smart Cards

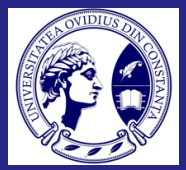
Masterand :
Gavrilă Doru

Coordonator lucrare :
Prof. univ. dr. Răcuciu Ciprian Iulian

Universitatea 'Ovidius' Constanța
Facultatea de Matematică și Informatică

2024

Cuprins



Ce sunt smart cardurile?

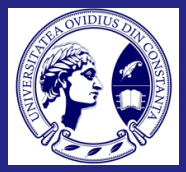
Smart cardurile (SC) sau cardurile cu circuit integrat(ICC) sunt carduri de plastic care includ un microcip sau un cip de memorie încorporat. Prin utilizarea cipurilor se poate stoca și procesa datele, din acest motiv cardurile cu cip sunt mai versatile și mai sigure în protecția datelor decât cardurile care folosesc banda magnetică.

Scurtă Istorie

1. În 1959 este inventat cipul (silicon integrated circuit), iar în 1967 inginerul german Helmut Grottup propune primele modele de carduri care integrează un cip. El propune două modele de integrare și comunicare: contact și contactless (primii pași în dezvoltarea cardurilor care folosesc tehnologia NFC sau RFID).

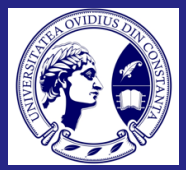
Scurtă Istorie

1. În 1959 este inventat cipul (silicon integrated circuit), iar în 1967 inginerul german Helmut Grottup propune primele modele de carduri care integrează un cip. El propune două modele de integrare și comunicare: contact și contactless (primii pași în dezvoltarea cardurilor care folosesc tehnologia NFC sau RFID).
2. Din punct de vedere al capacităților Smart Cardului, inovatorul francez Roland Moreno este recunoscut ca fiind părintele acestuia, propunând în 1974 un card capabil să stocheze date și să includă cel puțin o zonă de memorie protejată.



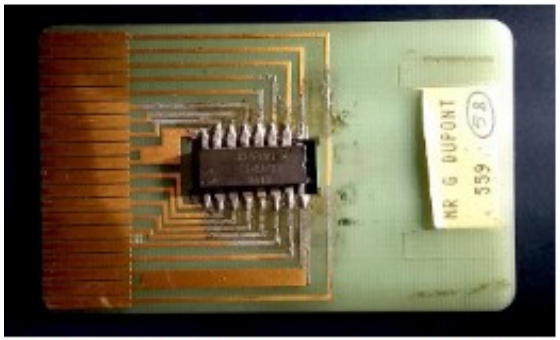
Scurtă Istorie

1. În 1959 este inventat cipul (silicon integrated circuit), iar în 1967 inginerul german Helmut Grottup propune primele modele de carduri care integrează un cip. El propune două modele de integrare și comunicare: contact și contactless (primii pași în dezvoltarea cardurilor care folosesc tehnologia NFC sau RFID).
2. Din punct de vedere al capacităților Smart Cardului, inovatorul francez Roland Moreno este recunoscut ca fiind părintele acestuia, propunând în 1974 un card capabil să stocheze date și să includă cel puțin o zonă de memorie protejată.
3. În zilele noastre putem întâlni de la carduri neprotejate până la carduri care integrează microprocesoare și respectă arhitectura von Neumann.



Scurtă Istorie

De la cardul propus de Roland Moreno la carduri cu microprocesor.



(a) The Roland Moreno smart card prototype

(b) Microprocessor smart card

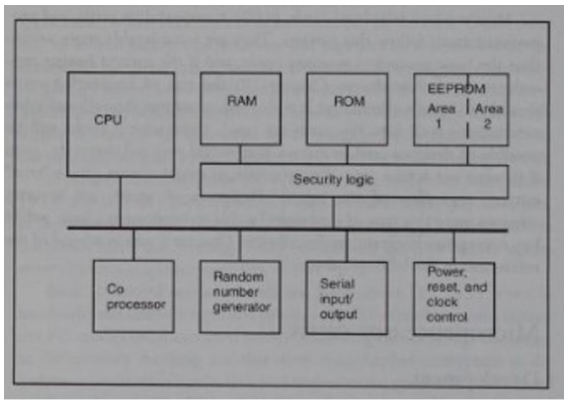


Figure 2.7: Smart card microprocesor architecture

Domenii de utilizare a smart cardurilor:

1. Domeniul Bancar : Carduri de debit sau credit.

Domenii de utilizare a smart cardurilor:

1. Domeniul Bancar : Carduri de debit sau credit.
2. Transport Public : bilete de calatorie sau abonamente

Domenii de utilizare a smart cardurilor:

1. Domeniul Bancar : Carduri de debit sau credit.
2. Transport Public : bilete de calatorie sau abonamente
3. Sănătate : cardul de sănătate

Domenii de utilizare a smart cardurilor:

1. Domeniul Bancar : Carduri de debit sau credit.
2. Transport Public : bilete de calatorie sau abonamente
3. Sănătate : cardul de sănătate
4. Comunicații : SIM cardul

Domenii de utilizare a smart cardurilor:

1. Domeniul Bancar : Carduri de debit sau credit.
2. Transport Public : bilete de calatorie sau abonamente
3. Sănătate : cardul de sănătate
4. Comunicații : SIM cardul
5. Documente administrative : Carte de identitate si pasaport

Domenii de utilizare a smart cardurilor:

1. Domeniul Bancar : Carduri de debit sau credit.
2. Transport Public : bilete de calatorie sau abonamente
3. Sănătate : cardul de sănătate
4. Comunicații : SIM cardul
5. Documente administrative : Carte de identitate si pasaport
6. Control Aces

Control acces

Controlul accesului reprezintă un concept esențial în securitatea informațiilor și protecția infrastructurii fizice a unei organizații. Prin controlul accesului, organizațiile pot proteja activele valoroase de accesul neautorizat și pot asigura confidențialitatea, integritatea și disponibilitatea datelor și resurselor.

De ce sunt folosite smart cardurile în controlul accesului?

Control accesul și Smart Carduri

Eficiență și Ușurință în Utilizare:

1. **Rapiditate:** Utilizatorului i se permite rapid accesul la resursele la care are drept.
2. **Ușurința de utilizare:** Prin folosirea cardurilor contactless, utilizatorul se autentifică prin apropierea cardului de cititor, fără un contact fizic.

Control accesul și Smart Carduri

Flexibilitate și Scalabilitate:

1. **Gestionare Ușoară:** Administratorii pot gestiona ușor drepturile de acces prin actualizări centralizate ale permisiunilor de pe carduri. În cazul pierderii unui card, accesul poate fi revocat imediat.
2. **Diferite cazuri de utilizare** Un singur smart card poate fi utilizat pentru multiple funcții, cum ar fi accesul la clădiri, autentificarea în rețele IT.
3. **Integrabilitate:** Smart cardurile pot fi integrate cu sisteme existente de securitate și de management al identității, oferind o soluție completă și eficientă.

Control accesul și Smart Carduri

Ușurința de monitorizare și Audit.
Datorită unicității UID-ului cardului se poate realiza:

1. Logare Evenimente
2. Detectare Anomalii

1. Pentru a reduce complexitatea sistemului de control acces firmele producătoare de sisteme utilizează ca principal mod de autentificare UID-ul.
2. UID (Unique Identifier) este un cod unic care este atribuit fiecărui smart card în timpul producției. Acesta servește ca un element fundamental în securitatea și gestionarea accesului, permițând identificarea unică a fiecărui card.
3. Sistemele de control acces bazate efectiv pe smart card sunt vulnerabile clonării smart cardului.

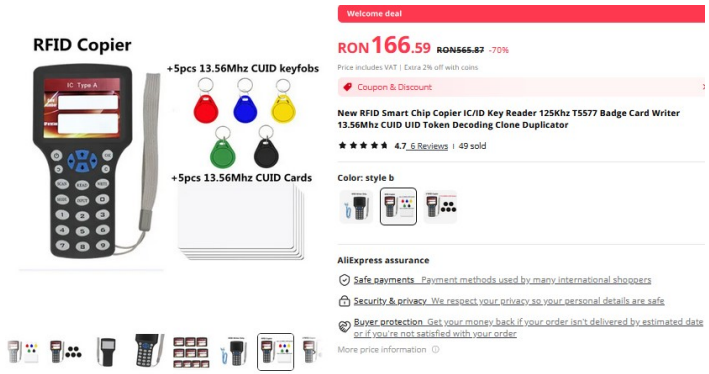
Cum funcționează

1. Stocare: UID-urile cardurilor autorizate sunt stocate într-o bază de date securizată.
2. Verificare: La fiecare accesare, sistemul verifică UID-ul cardului împotriva bazei de date pentru a valida accesul.
3. Monitorizare: Evenimentele de acces sunt înregistrate împreună cu UID-urile pentru monitorizare și audit.

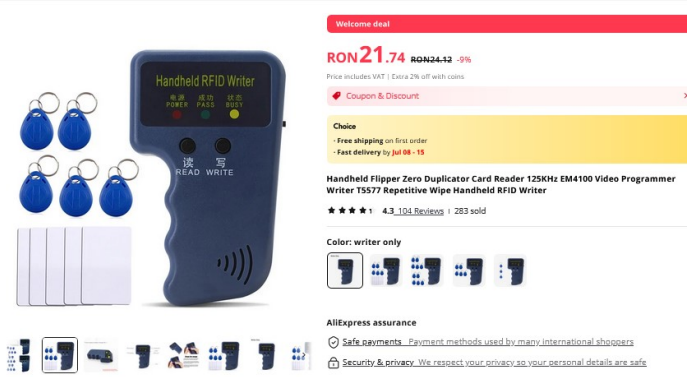
HF snd LF

- Pentru controlul accesului sunt folosite cardurile care operează pe HF (High Frequency) și LF (Low Frequency). Din punctul de vedere al frecvenței de operare, avem copiatoare dedicate sau hardware specializate pentru pentesting care pot citi, salva, emula și clona .

Dispozitive de clonare



(a) LF and HF



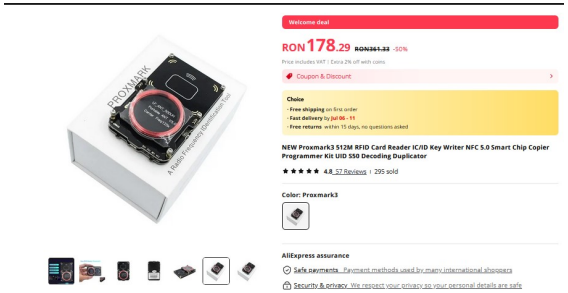
(b) Writer T5577

PRODUCT PARAMETERS

brand	iCopyKEY
name	Smart card key matching machine
model	iCopy X100
size	182*70*31MM
frequency	13.56MHz, 125KHz, 175KHz, 250KHz, 300KHz, 375KHz, 500KHz, etc.
Battery	4 AA dry batteries (bring your own)
interface	USB Type-C communication/power supply interface
power supply	5V 0.5A
Power consumption	Sleep standby <10uA
Product Shipping List	Host, manual, Type-C data cable, Type-C OTG adapter (gift)

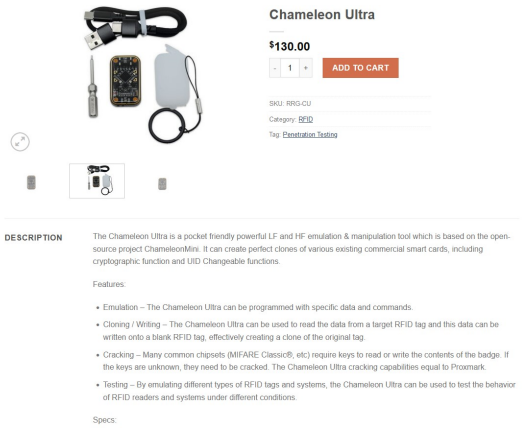
Type	ID	Interface	USB
Model Number	RP-SD	Origin	Mainland China
Read	EM / TK (EM4100 TK4100 etc) cards or keys	Write	EM4305 CETS557 T5577 5200 EM4205 etc cards or Keys
Built-in	individual LED lights and buzzer indicator, transceiver antenna	Power Supply	3V (2 x AAA battery)
Times	Read / Write > 20000 times	Type 1	RFID Duplicator Card Reader

Tool-uri pentru pentesting



(a) Proxmark

(b) Flipper Zero



(c) Cameleon Ultra

(d) HackRf One

Măsuri anticlonare caz Electra

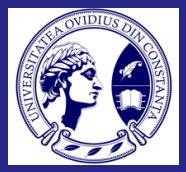
Firma românească de dispozitive de acces pe bază de carduri Electra a dezvoltat un sistem bazat pe carduri LF, care, în momentul în care cardul este citit, recepționează UID-ul și un cod.

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

[=] Note: False Positives ARE possible
[=]
[=] Checking for known tags...
[=]
[+] EM 410x ID 5600A583B4
[+] EM410x ( RF/64 )
[=] -------- Possible de-scramble patterns ---------
[+] Unique TAG ID      : 6A00A5C12D
[=] HoneyWell IdentKey
[+]     DEZ 8          : 10847156
[+]     DEZ 10         : 0010847156
[+]     DEZ 5.5        : 00165.33716
[+]     DEZ 3.5A       : 086.33716
[+]     DEZ 3.5B       : 000.33716
[+]     DEZ 3.5C       : 165.33716
[+]     DEZ 14/IK2     : 00369378034612
[+]     DEZ 15/IK3     : 000455277396269
[+]     DEZ 20/ZK      : 06100000100512010213
[=]
[+] Other              : 33716_165_10847156
[+] Pattern Paxton     : 1455014324 [0x56B9C1B4]
[+] Pattern 1          : 3352731 [0x33289B]
[+] Pattern Sebury     : 33716 37 2458548  [0x83B4 0x25 0x2583B4]
[+] VD / ID            : 086 / 0010847156
[=] ----------------------------------------------

[+] Valid EM410x ID found!

[=] Couldn't identify a chipset
```

(a) LF Card

```
] pm3 --> lf search

[=] NOTE: some demods output possible binary
[=] if it finds something that looks like a tag
[=] False Positives ARE possible
[=]
[=] Checking for known tags...
[=]
[+] EM 410x Short ID found on a 128b frame
[+]     Data after ID: 7C700000000   Code
[+]     Possibly an Electra (R0), 0x7C7 = 1991
[+]     Short ID details:
[+] EM 410x ID 03E8A955A1   UID
[+] EM410x ( RF/64 )
[=] -------- Possible de-scramble patterns ---------
[+] Unique TAG ID      : C01795AA85
[=] HoneyWell IdentKey
[+]     DEZ 8          : 11097505
[+]     DEZ 10         : 3903411617
[+]     DEZ 5.5        : 59561.21921
[+]     DEZ 3.5A       : 003.21921
```

(b) Electra Card



Continuare Electra

1. Nu se pot folosi alte taguri decât cele recomandate de Electra.
2. Clonarea cardurilor/scrierea trebuie să se facă cu un dispozitiv dezvoltat de firma Electra.

CARTELE DE ACCES			
1.	TAG.ELT.300		**Tag proximitate PROGRAMABIL, producție ELECTRA**, cu cod personalizare producător, posibilitate acordare a unui cod unic pe o scară de bloc, costuri reduse la vânzarea post-instalare **Instalațiile ELECTRA funcționează numai cu tag-uri ELECTRA !**

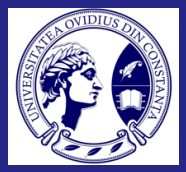
Doar că atât cu Flipper, cât și cu Proxmark, se poate clona pe un smart card T55xx dacă se modifică blocul 0, 3 și 4.

1. lf t55xx write -b 0 -d 00148080
2. lf t55xx write -b 3 -d 7E1EAAAA
3. lf t55xx write -b 4 -d AAAAAAAA

Adăugarea unei counter

O altă variantă ar fi să folosim un counter care se modifică în momentul utilizării cardului. Counterul pleacă de la 0 și este rescris la fiecare utilizare a cardului.
Se verifică counterul la fiecare utilizare și, dacă este egal cu valoarea din baza de date, se permite accesul.

1. Posibile erori la scriere datorită timpului scurt de menținere a cardului pe dispozitivul de citire/scriere.
2. Nu eliminăm clonarea, dar asigurăm un control.
3. Există posibilitatea ca persoana rău intenționată să poată intra. Aflăm după ce persoana de drept raportează că nu poate intra.



MIFARE Classic® EV1 1K - 4K

MIFARE asigură criptarea datelor folosind Crypto1, un algoritm de criptare dezvoltat de firma NXP pentru acest tip de carduri. Din 2009, acest algoritm nu este sigur, existând diverse moduri de atac implementate pe dispozitivele Proxmark, Chameleon și Flipper.

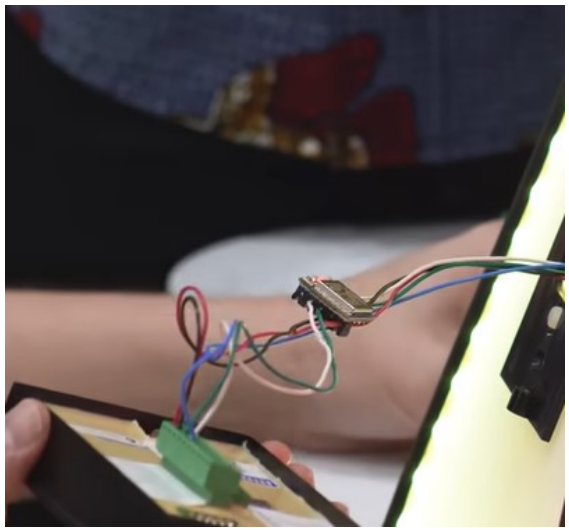
```
[usb] pm3 --> hf mf nested --1k --blk 0 -k 29BA8F5D03D1
[+] Testing known keys. Sector count 16
[+] Fast check found all keys

[+] found keys:

[+] -----+-----+--------------+---+--------------+----
[+]  Sec | Blk | key A        |res| key B        |res
[+] -----+-----+--------------+---+--------------+----
[+]  000 | 003 | 29BA8F5D03D1 | 1 | D64570A2FC2E | 1
[+]  001 | 007 | 29BA8F5D03D1 | 1 | D64570A2FC2E | 1
[+]  002 | 011 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  003 | 015 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  004 | 019 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  005 | 023 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  006 | 027 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  007 | 031 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  008 | 035 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  009 | 039 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  010 | 043 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  011 | 047 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  012 | 051 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  013 | 055 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  014 | 059 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+]  015 | 063 | FFFFFFFFFFFF | 1 | FFFFFFFFFFFF | 1
[+] -----+-----+--------------+---+--------------+----
[+] ( 0:Failed / 1:Success )
```

Figure 2.16: Proxmark Nested attack screenshot

Vulnerabilitațile Control Accesului

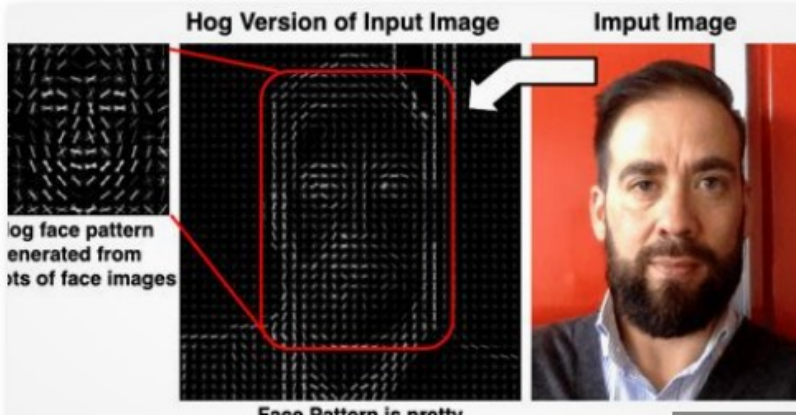
1. Pierdere sau Furt de Carduri
2. Împrumutare card
3. Inginerie Socială (see Figure 4a)
4. Interceptarea Comunicațiilor (see Figure 4b)

(a) Mantrap

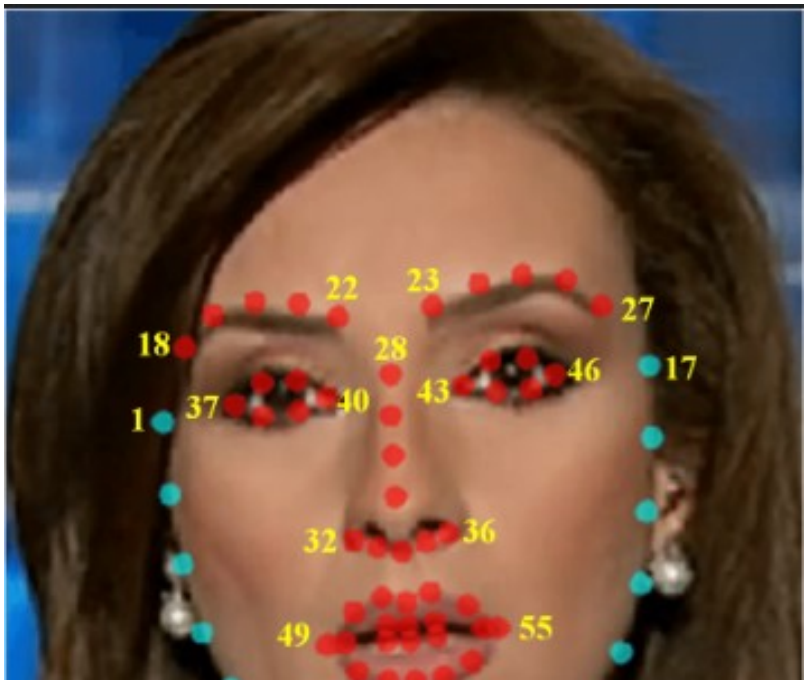


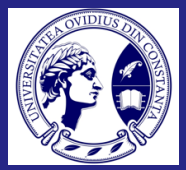
(b) ESP pentru colectare credentiale

Utilizarea MFA (autentificare multi-factor) Se păstrează smart cardurile și controlul accesului cum a fost descris anterior, la care se adaugă o verificare suplimentară bazată pe recunoaștere facială. Am utilizat HOG, fiind necesar ca în baza de date a sistemului să avem o poză a persoanei pentru ca sistemul să poată face recunoașterea.
Ca măsură de backup, în cazul în care nu se poate realiza recunoașterea facială, se trimite un cod de autentificare pe emailul persoanei. Codul trebuie să fie tastat într-o perioadă de timp limitată. În cazul în care, după expirarea timpului, codul nu a fost tastat, sistemul revine la starea inițială, iar persoana va trebui să parcurgă pașii de autentificare: prezentare card, recunoaștere facială și PIN, dacă nu se poate face recunoașterea facială.

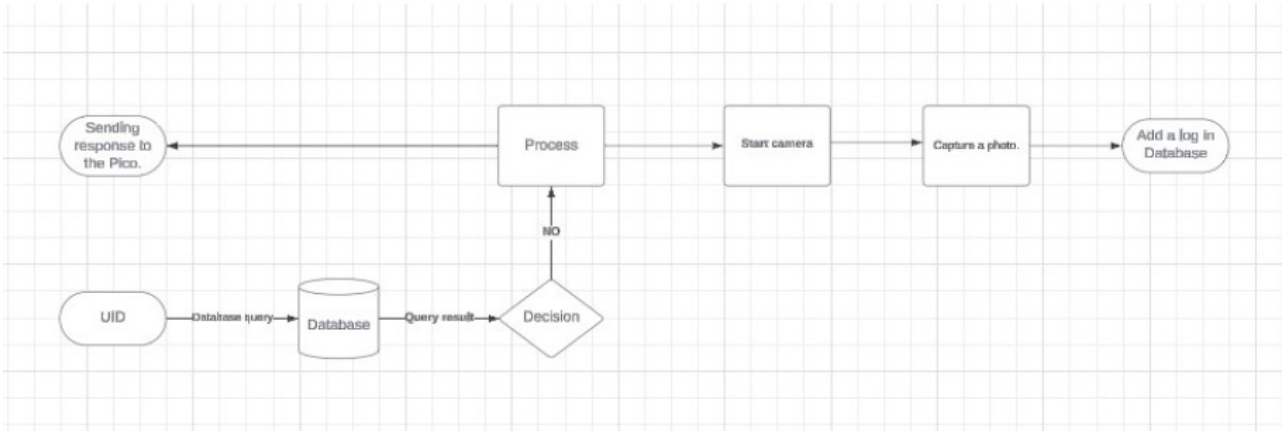


(a) Histogram of Gradients

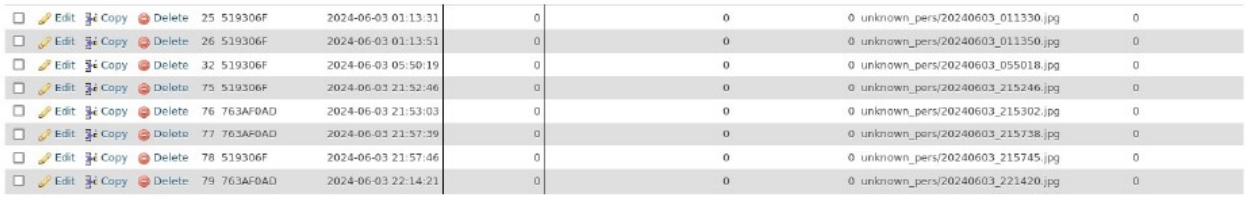




Cazul 1



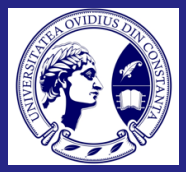
(a) Cazul 1



Edit	Copy	Delete	25	519306F	2024-06-03 01:13:31	0	0	0 unknown_pers/20240603_011330.jpg 0
Edit	Copy	Delete	26	519306F	2024-06-03 01:13:51	0	0	0 unknown_pers/20240603_011350.jpg 0
Edit	Copy	Delete	32	519306F	2024-06-03 05:50:19	0	0	0 unknown_pers/20240603_055018.jpg 0
Edit	Copy	Delete	75	519306F	2024-06-03 21:52:46	0	0	0 unknown_pers/20240603_215246.jpg 0
Edit	Copy	Delete	76	763AF0AD	2024-06-03 21:53:03	0	0	0 unknown_pers/20240603_215302.jpg 0
Edit	Copy	Delete	77	763AF0AD	2024-06-03 21:57:39	0	0	0 unknown_pers/20240603_215738.jpg 0
Edit	Copy	Delete	78	519306F	2024-06-03 21:57:46	0	0	0 unknown_pers/20240603_215745.jpg 0
Edit	Copy	Delete	79	763AF0AD	2024-06-03 22:14:21	0	0	0 unknown_pers/20240603_221420.jpg 0

(b) Database log

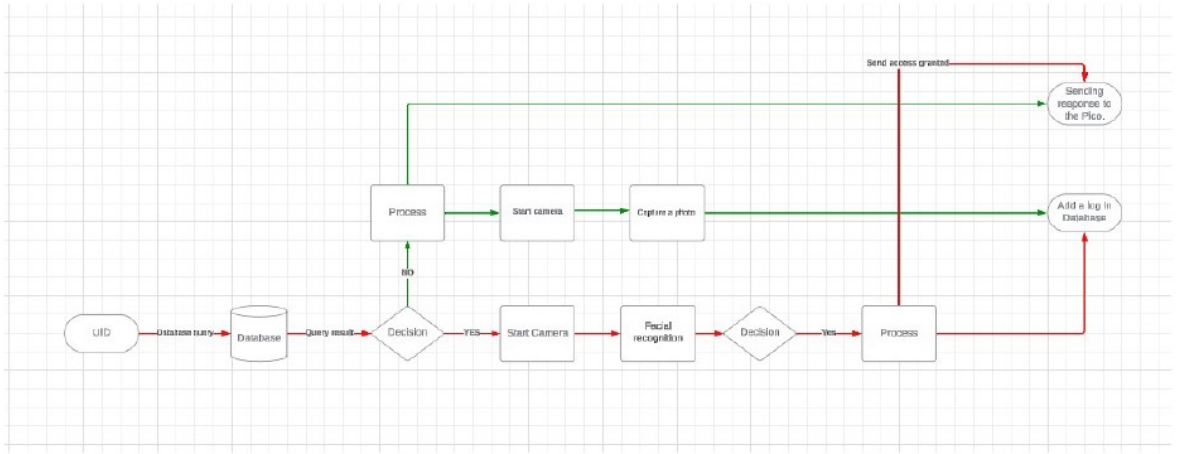
Click to watch the video case 1



Cazul 2

Case 2

Valid UID, the individual is the rightful holder of the card. This represents the ideal scenario.



(a) Flowchart Cazul 2

id	smart_card_uid	log_date	accepted_card	facial_recognition_successful	spoofing_detected	saved_image ▲ 1	email_sent	email_address
6	F3B1A31A	2024-06-02 15:37:53	1	1	0		0	
14	8958A46F	2024-06-02 22:04:57	1	1	0		0	
15	8958A46F	2024-06-02 22:11:05	1	1	0		0	

(b) Database log Cazul 2

Click to watch the video case 2

Cazul 3

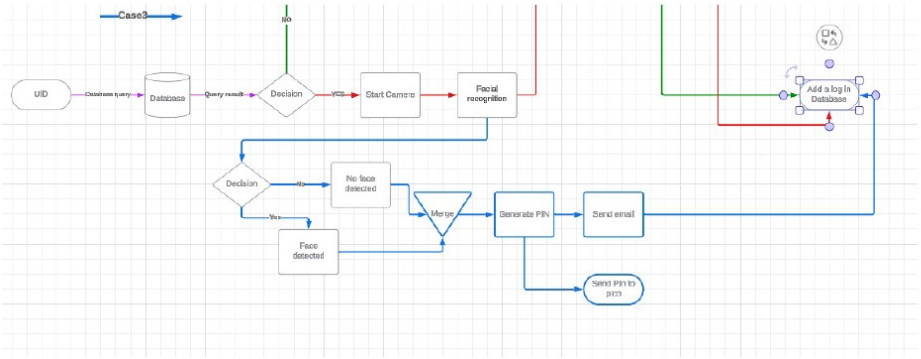
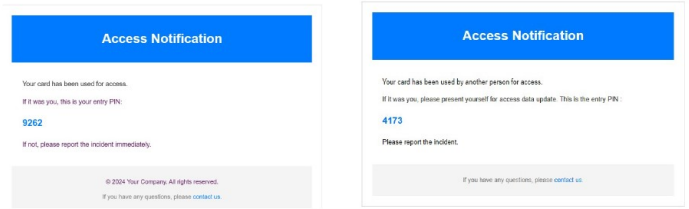


Figure: Flowchart Cazul 3



(a) No face detected (b) Face detected

17 8958A46F	2024-06-02 22:13:44	1	0	0
18 8958A46F	2024-06-02 22:14:46	1	0	0
19 8958A46F	2024-06-02 22:15:26	1	0	0 unknown_pers/202406C
	2024-06-02 22:22:51	0	0	0 unknown_pers/202406C

(a) Template emails (b) Database log

Figure: Examples of Email Templates and Database Logs

Click to watch the video case 3

1. Accesul bazat pe carduri inteligente este o metodă ieftină și comună de a asigura că persoanele care încearcă să intre într-o zonă administrativă au autorizația necesară. Vulnerabilitățile existente ale unui astfel de sistem, care se bazează exclusiv pe carduri inteligente, pot fi atenuate doar prin utilizarea unor carduri inteligente de nouă generație. Totuși, acest lucru crește costurile de implementare, inclusiv prețul cardului inteligent și complexitatea logicii sistemului. Chiar și cu aceste măsuri, eliminarea completă a vulnerabilităților nu este garantată. Cardurile inteligente pot fi pierdute sau clonate odată ce datele lor sunt obținute.

2. Un sistem bazat pe autentificare cu doi factori (2FA), cum ar fi recunoașterea facială sau un cod PIN trimis pe telefonul utilizatorului, poate atenua aceste vulnerabilități, făcând sistemul de control al accesului mai robust. În sistemul actual, am ales să trimitem un email persoanei