Card Vulnerabilities

By: Ryan, Alan, James, and Jerry

How does RFID work?

- Electromagnetic fields to identify and track tags attached to objects
- Consists of tiny radio transponder, a radio receiver, and a transmitter
- When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data

Frequency Band	Range	Applications
LF (125–134 kHz)	~10 cm	Animal tracking, access control
HF (13.56 MHz)	~10–30 cm	Smart cards, NFC, payment
UHF (860–960 MHz)	~1–12 meters	Inventory, logistics, tolling
Microwave (2.45 GHz)	~1 meter	Specialized applications

Common Mitigations Strategies

- Encryption
  - scrambles the data on the card making it hard to read
- Mutual Authentication
  - ensure the tag and reader verify each other before exchange
- Access Control
  - limits which readers can interact with which cards
- RFID Blocking (Physical)
  - blocks card from transmitting signal
  - prevents cloning

Our project: MIFARE Classic Cards

- Employs a protocol compliant with parts 1–3 of ISO/IEC 14443 Type A, with an NXP proprietary security protocol for authentication and ciphering
- Easily readable and writable
- Uses Crypto-1 for encryption which is fully broken (brute force is not needed to decrypt)
- We want to design better access logic

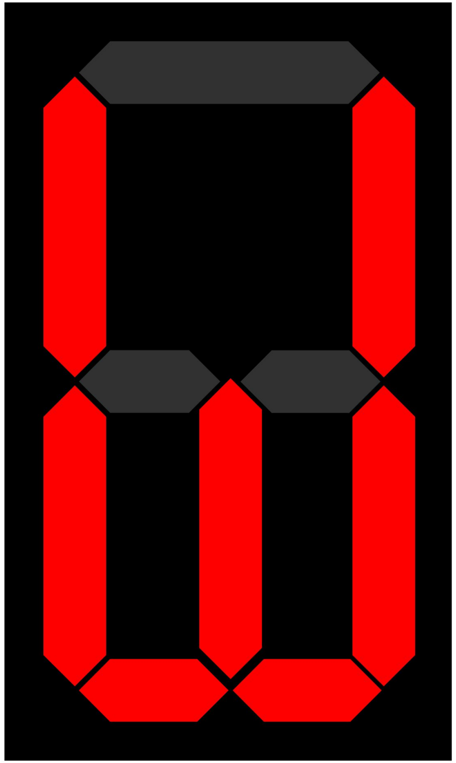
Attack Costs

- RFID Reader (ACR122U) – $56
  - – Sufficient for reading / cracking / writing / cloning Mifare Classic Cards
- Chinese UID Changeable Mifare Card – $2
  - With those cards an attacker is able to create a perfect clone of any Mifare Classic card (including UID)

Mitigation: Set Counter state

Rules

- Our counter is in alphabetical order
- From A to D, looping around
- We put our counter in one block section of the card
- We also record that counter in our database
- Everytime our guest swipe the card, the counter in the card and in the database will go next letter
- If they don't match each other, the card got cloned



Demo: Set Counter state

- Situation 1: Database=Counter=D

  Card is not getting cloned. Next time will be A

- Situation 2: Database=Counter=A

  Card is not getting cloned. Next time will be B

- Situation 3: Set Database=D Counter=B

  Mismatch Happen. Card is getting cloned

Mitigation: Timing / Clocking in and out

Overview

- For this mitigation we follow a running example of a company building that uses the MIFARE classic as a key for employees.
- We came up with a set of rules that will be implemented to prevent cloning attacks.

Clock in/out pt.2

Rules

- Only registered cards are accepted
- Employees must scan their card to enter and leave the building
  - this doubles as clocking in and out for convenience
- If an employee has clocked in, that same card signature cannot be used to clock in again without first clocking out
- Employees can only access the building during regular working hours
- For PTO or sick days, the card signature for that employee doesn’t work

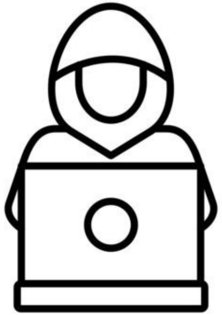
Example Usage for clock in/out

Scenario

- attacker clones an employees card and wants to access the building

Potential Outcomes

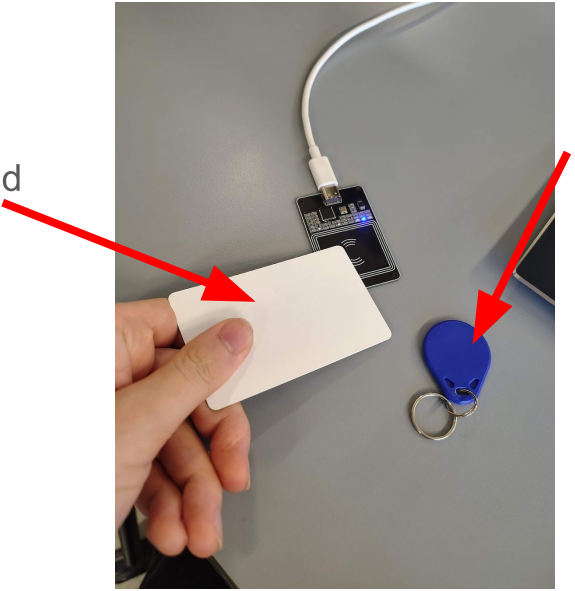
- the attacker arrives to the building before the employee, and when the employee tries to access the building, the system is alerted that the same card tried to access the building twice
- The attacker arrives after the employee and the system is alerted
- Attacker can only gain access undetected if the employee is no call, no show for the day



Mitigation: Two cards

Primary

- Holds a ciphertext that is encrypted by the key stored in the anchor



Anchor

- A random string is generated during write process
- This is used as the AES-ECB encryption key
- Neither primary or anchor data is stored anywhere in any database

Result: Cloning is far more difficult as Primary goes in wallet and Anchor goes on your keychain. No readable plaintext or pattern can be derived from dumping any one key.
- requires a custom tag reading script that accepts two tags to decrypt

Who uses these cards?

Check your pants

Mifare Classic Cards in use today

- Hotels, office building access, universities, theme parks
- Boston Charlie Card
- London Oyster Card
- Moscow Troika card
- Los Angeles Tap card

The MIFARE protocol takes 300ms to 500ms per tap

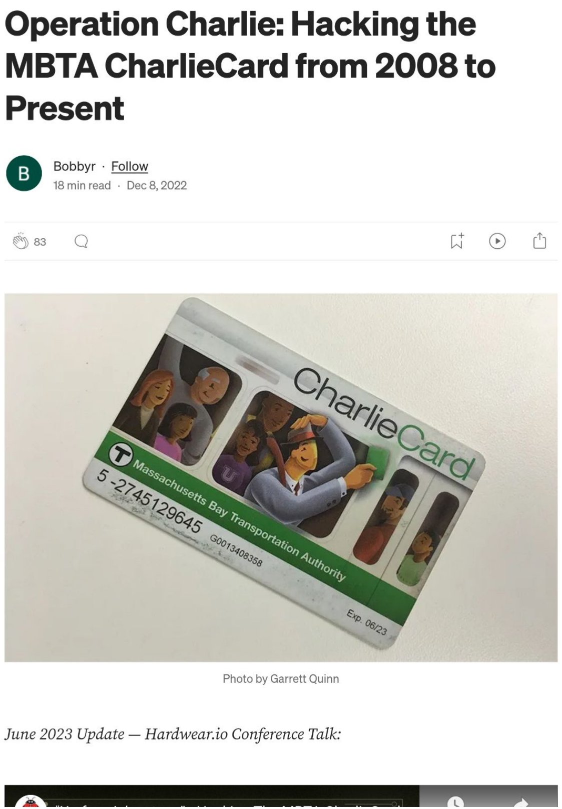
EMV (credit card tap) take ~500ms (can slow up the turnstiles)

mifare cards are really cheap

Most cities are transitioning to MIFARE DESFire EV1 which has real AES-128 encryption (ie brute force 2^128 operations to decrypt hidden blocks)

- or just switching to EMV like Boston, NYC, others

https://medium.com/@bobbyrsec/operation-charlie-hacking-the-mbta-charliecard-from-2008-to-present-24ea9f0aaa38



Operation Charlie: Hacking the MBTA CharlieCard from 2008 to Present

Bobbyr · Follow
18 min read · Dec 8, 2022

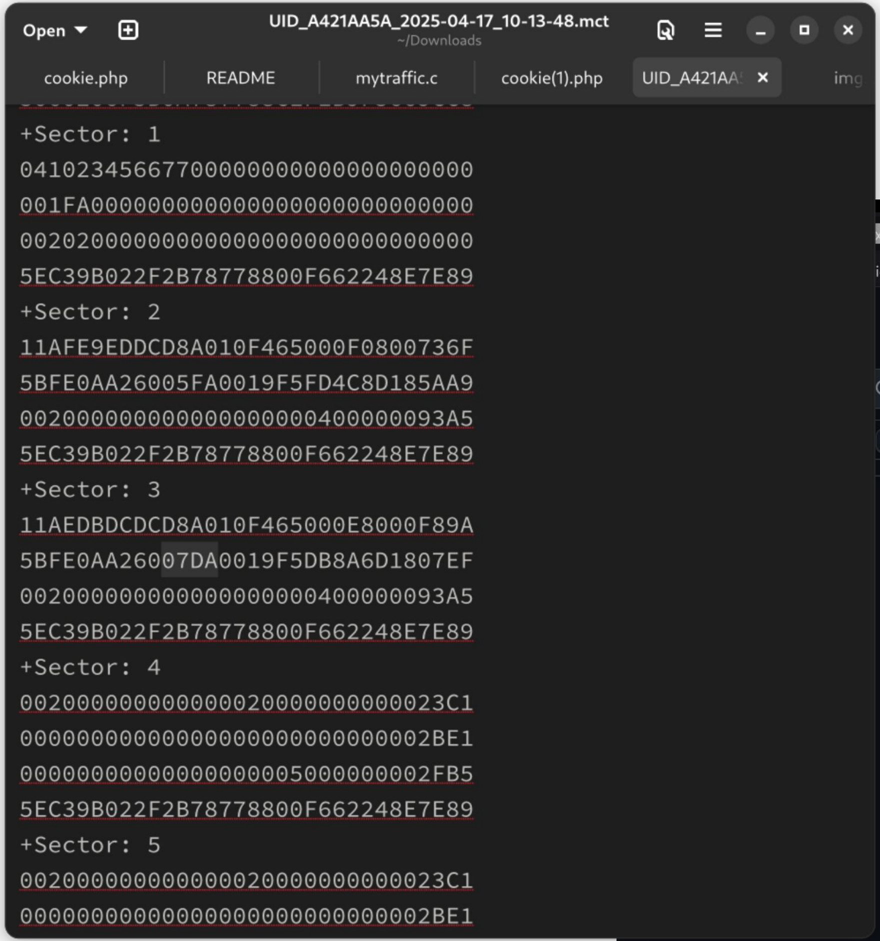
Photo by Garrett Quinn

June 2023 Update — Hardwear.io Conference Talk:

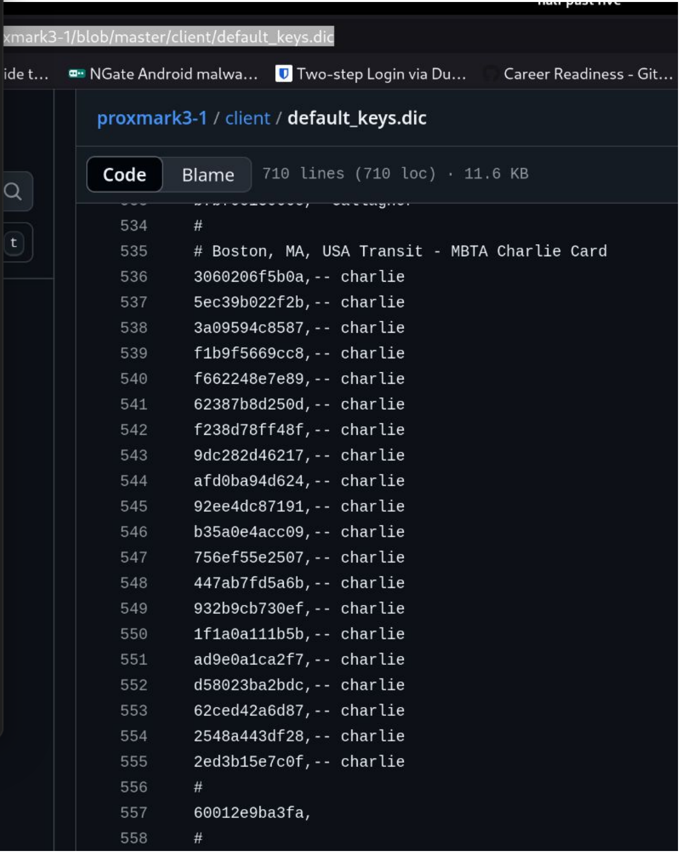
From Article:
“I am publicly disclosing that it is possible using only an Android phone to:

- **Have a replacement CharlieCard delivered to a listed address, without paying**
- **Provision a new CharlieCard with funds, without paying**
- **Steal anyone’s CharlieCard with a single physical tap of the card against a phone in a matter of seconds”**

0x07DA = 2010/2 = $10.05 on my charlie card



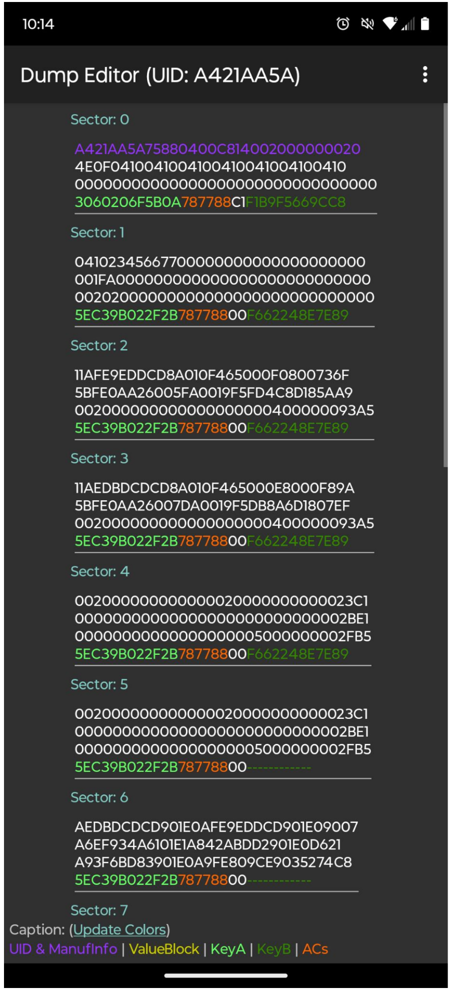
```
+Sector: 1
041023456677000000000000000000000
001FA0000000000000000000000000000
00202000000000000000000000000000
5EC39B022F2B78778800F662248E7E89
+Sector: 2
11AFE9EDDCD8A010F465000F0800736F
5BFE0AA26005FA0019F5FD4C8D185AA9
00200000000000000000400000093A5
5EC39B022F2B78778800F662248E7E89
+Sector: 3
11AEDBDCDCD8A010F465000E8000F89A
5BFE0AA26007DA0019F5DB8A6D1807EF
00200000000000000000400000093A5
5EC39B022F2B78778800F662248E7E89
+Sector: 4
0020000000000000200000000000023C1
0000000000000000000000000002BE1
00000000000000000005000000002FB5
5EC39B022F2B78778800F662248E7E89
+Sector: 5
0020000000000000200000000000023C1
0000000000000000000000000002BE1
```


xmark3-1/blob/master/client/default_keys.dic
ide t...
NGate Android malwa...
Two-step Login via Du...
Career Readiness - Git...
proxmark3-1 / client / default_keys.dic
Code
Blame
710 lines (710 loc) · 11.6 KB

```
#
# Boston, MA, USA Transit - MBTA Charlie Card
3060206f5b0a,-- charlie
5ec39b022f2b,-- charlie
3a09594c8587,-- charlie
f1b9f5669cc8,-- charlie
f662248e7e89,-- charlie
62387b8d250d,-- charlie
f238d78ff48f,-- charlie
9dc282d46217,-- charlie
afd0ba94d624,-- charlie
92ee4dc87191,-- charlie
b35a0e4acc09,-- charlie
756ef55e2507,-- charlie
447ab7fd5a6b,-- charlie
932b9cb730ef,-- charlie
1f1a0a111b5b,-- charlie
ad9e0a1ca2f7,-- charlie
d58023ba2bdc,-- charlie
62ced42a6d87,-- charlie
2548a443df28,-- charlie
2ed3b15e7c0f,-- charlie
#
60012e9ba3fa,
#
```

Android Cloning

- MIFARE Classic Tool in Play Store
- Can read MIFARE Classic RFID cards information using RFID on smartphones
- Tested on non Rooted Android device
- Can exploit this app for cloning
- Only need the decryption key. can be guessed or use a public key list like the charlie cards on GitHub



10:14

Dump Editor (UID: A421AA5A)

```
Sector: 0
A421AA5A75880400C814002000000020
4E0F0410041004100410041004100410
00000000000000000000000000000000
3060206F5B0A787788C1F1B9F5669CC8

Sector: 1
04102345667700000000000000000000
001FA000000000000000000000000000
00202000000000000000000000000000
5EC39B022F2B78778800F662248E7E89

Sector: 2
11AFE9EDDCD8A010F465000F0800736F
5BFE0AA26005FA0019F5FD4C8D185AA9
002000000000000000000400000093A5
5EC39B022F2B78778800F662248E7E89

Sector: 3
11AEDBDCDCD8A010F465000E8000F89A
5BFE0AA26007DA0019F5DB8A6D1807EF
002000000000000000000400000093A5
5EC39B022F2B78778800F662248E7E89

Sector: 4
002000000000000020000000000023C1
0000000000000000000000000002BE1
00000000000000000005000000002FB5
5EC39B022F2B78778800F662248E7E89

Sector: 5
002000000000000020000000000023C1
0000000000000000000000000002BE1
00000000000000000005000000002FB5
5EC39B022F2B78778800------------

Sector: 6
AEDBDCDCD901E0AFE9EDDCD901E09007
A6EF934A6101E1A842ABDD2901E0D621
A93F6BD83901E0A9FE809CE9035274C8
5EC39B022F2B78778800------------

Sector: 7
```

Caption: (Update Colors)
UID & ManufInfo | ValueBlock | KeyA | KeyB | ACs

Conclusion

- These cards are insecure and not possible to fully secure them
- Thus our mitigations are based on social engineering for different use cases of the cards
- MIFARE Classic Cards has been cracked and allows anyone to clone/copy those cards as demonstrated
- Solution is exchange all cards in circulation for more secure cards all approaches are workarounds
- MIFARE are cheap and reliable

Future Considerations:

- Finish implementing or expanding on mitigations
- Review real life cloning examples and evaluate risk (stolen wallets or proximity cloning)
- Test other MIFARE cards or other RFID cards

Thank You!