FTEC4004 TUTORIAL 8 RFID (IN)SECURITY

WANG Xianbo
xianbo@ie.cuhk.edu.hk

ABOUT THIS TUTORIAL

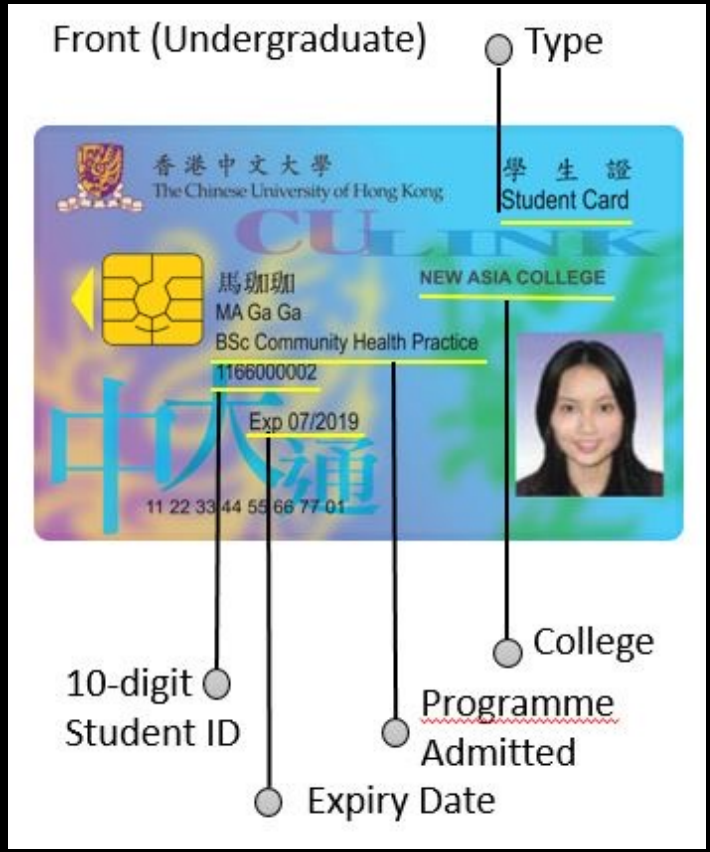
- We have learnt various smart card techniques in the lecture
- In this tutorial let's do something fun: RFID hacking
  - What kind of RFID tags are vulnerable?
  - What is required (hardware/software) to crack a card?
  - How to protect users/yourself.
- Disclaimer: this tutorial is for educational purpose only, do not attempt to break the law!

BASIC CONCEPTS

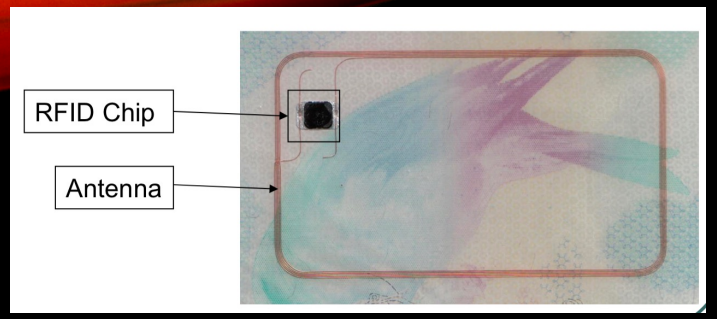
- RFID - Radio-frequency identification
- NFC - Near-field communication
  - HF (13.56MHz)
  - There are other cards/protocols working on LF (125 – 134 kHz)
- Contactless card & contact card
- Passive & Active

WE USE IT EVERYDAY

- Contactless: Mifare Classic/Plus
- Contact chip: MULTOS
- Does your CULINK have a contact chip?
- How many bytes for printed UID?
- Final question: **is CULINK secure?**



RFID CARDS


RFID Chip
Antenna


VISA
4000 1234 5678 9010
12/09
B. PARKER
MICHIGAN
ENHANCED DRIVER LICENSE
E 100 100 100 100
DOB 02-01-1977
ISS 02-01-2009
EXP 02-01-2013
JUNE SAMPLE
123 NORTH STATE ST.
LANSING, MI 48918-0000
Sex F
Hgt 504
Eyes BRO
Lic Type E,O
End NONE
Restrictions NONE
SAMPLE
DONOR
PASSPORT
United States of America

RFID STANDARDS

- ISO14443A: Mifare (NXP)
- ISO14443B: CryptoRF (Motorola/Atmel)
- ISO14443C: Felica (Sony)
- ISO14443D: (OTI)
- ISO14443E: (Cubic)
- ISO14443F: Legic (KABA)
- ISO15693: Tag-IT (Texas Instruments)

Different types of RFID transponders

Short range	Mid range	Long range
<= 15 centimeter	<= 5meter	Up to 500 meter
ISO 14443 A+B	ISO 15693	ISO 18000-xx
13.56 MHz, 125-134.2kHz	13.56 MHz, 125-135kHz	860-956 MHz (UHF) 2.4 GHz (Microwave) 5.8 GHz (Microwave)
E-field, magnetic field	EM-field	EM-field

HACKER'S ACTIONS

- Read – Unencrypted vs encrypted
- Clone – Read and write to new card
- Sniff – Eavesdropping, relay attack
- Emulate - Emulate card with devices

TOOLS – PHONE

NFC SUPPORTED PHONE = NFC READER

- MIFARE Classic Tool
- NFC Taginfo

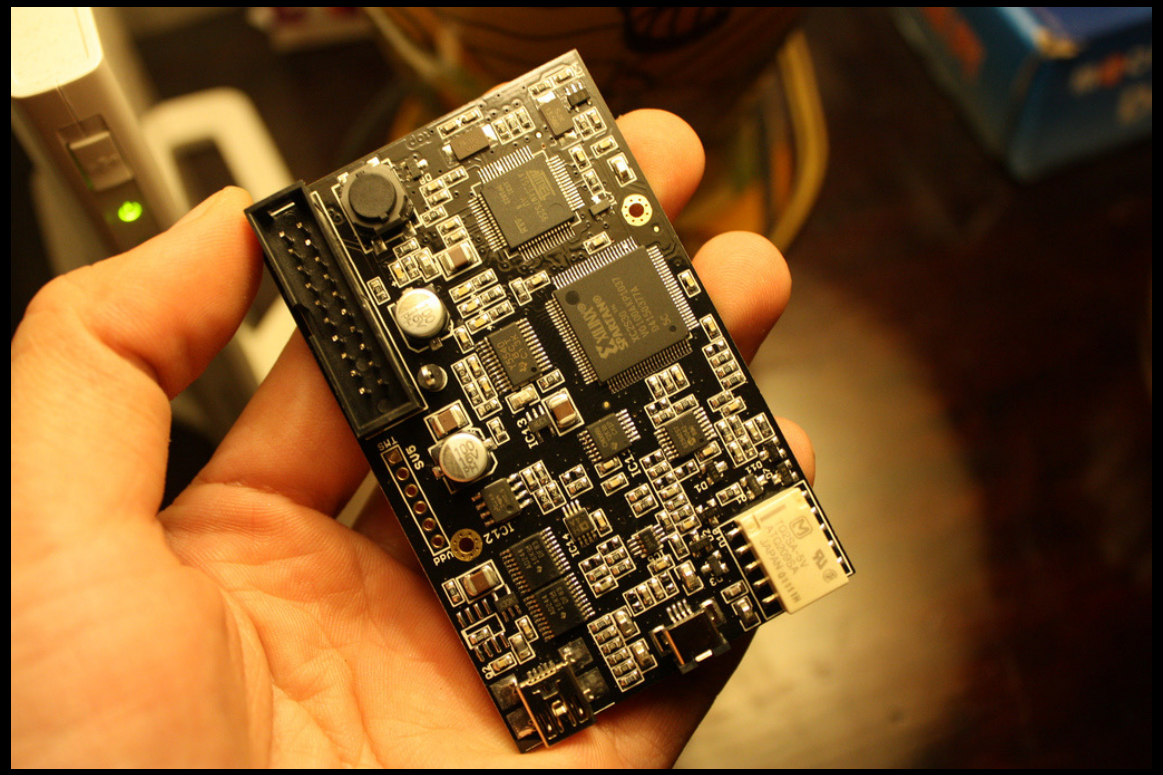
TOOLS - CARD READERS

- E.g. ACR122u
  - **Advanced Card Systems** Ltd (ACS), a Hong Kong company
  - Octopus reader
  - NXP PN532 chip, HF only
  - Cheap: 150 HKD

- Softwares
  - libnfc
  - RFIDiot
  - MFOC
  - miLazyCracker

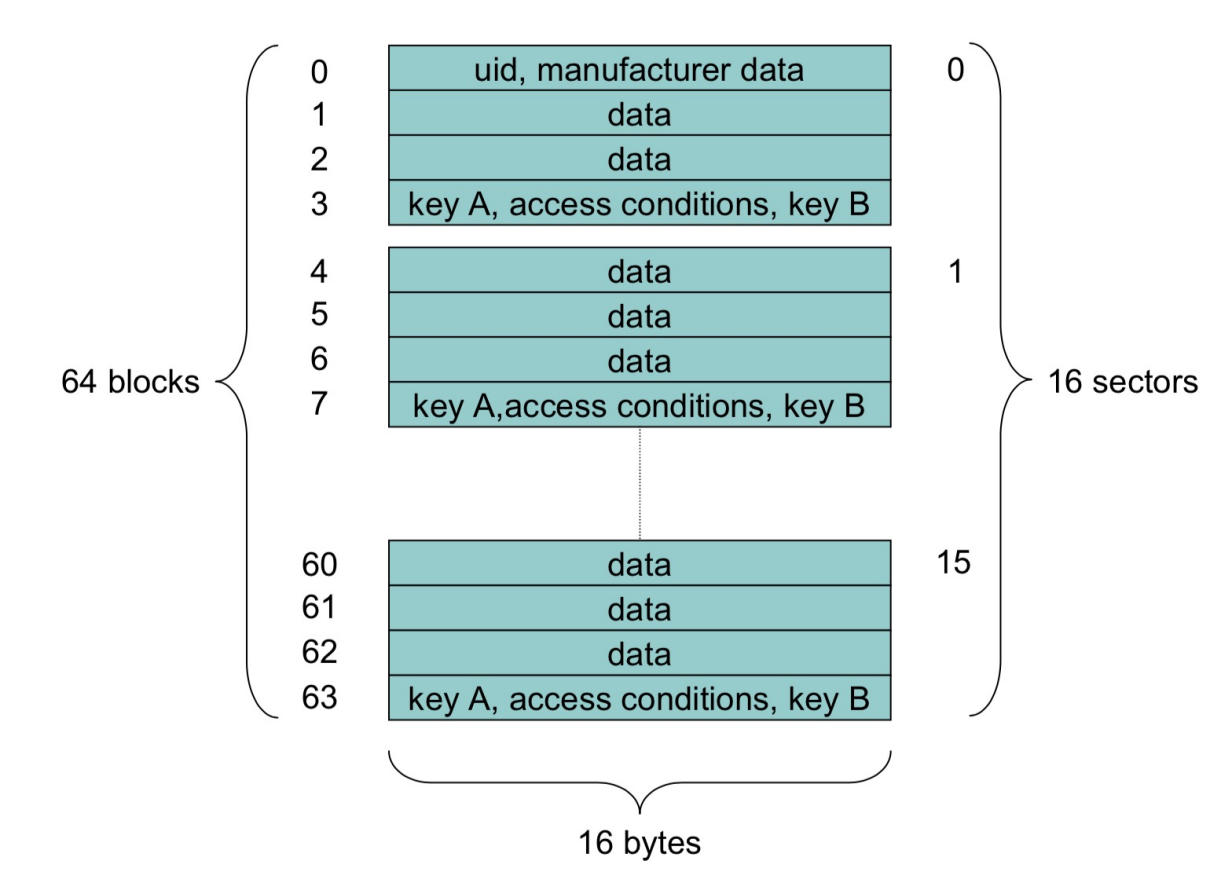
POWERFUL TOOL

- Proxmark3
  - HF and LF
  - Snoop communications
  - Emulate cards
  - Expensive: 1k+ HKD
  - Open-soruce hardware
  - Cheap now:
    - *China clones, 250HKD*



CASE STUDY – MIFARE CLASSIC

- Most widely used smart card
- Format
  - 16 sectors, each 4 blocks of 16 bytes
  - Data are encrypted
    - Two Key for access control
    - Key length: 48 bits (6 bytes)
  - UID (block 0) is readonly and public
    - Used as sole access control or identity in many cases
    - Some times printed on cards



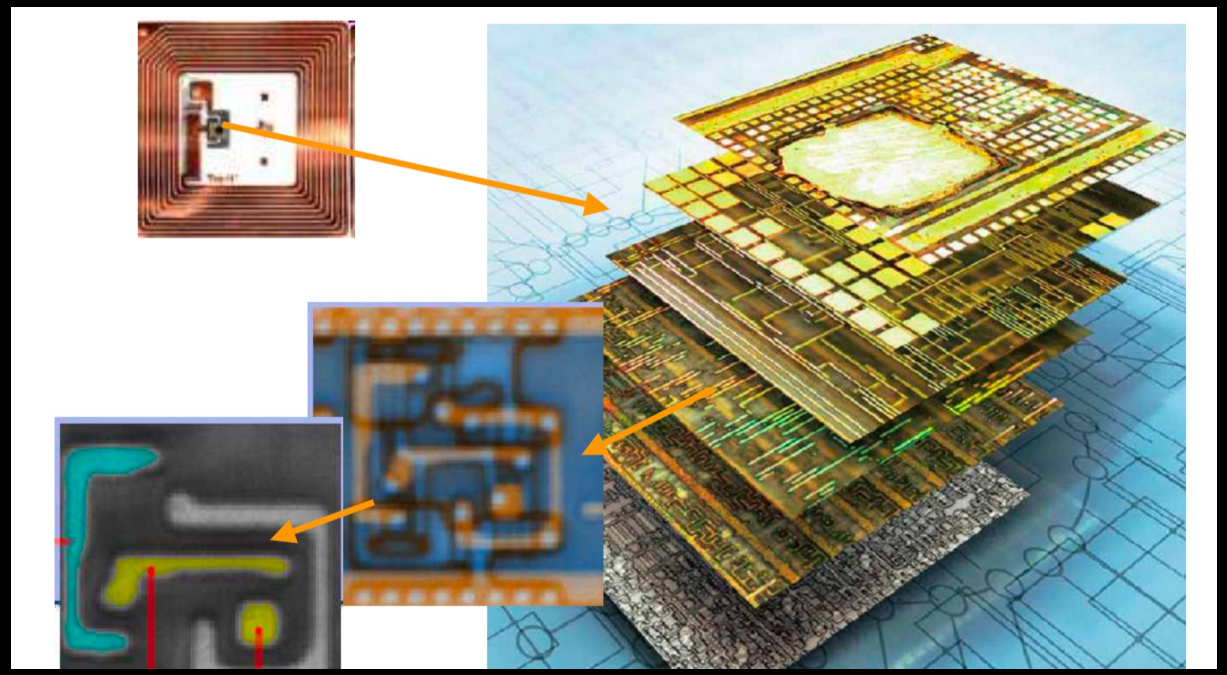
CASE STUDY – MIFARE CLASSIC

- Data communication

Step	Sender	Hex	Abstract
01	Reader	26	req type A
02	Tag	04 00	answer req
03	Reader	93 20	select
04	Tag	c2 a8 2d f4 b3	uid, bcc
05	Reader	93 70 c2 a8 2d f4 b3 ba a3	select(uid)
06	Tag	08 b6 dd	MIFARE 1K
07	Reader	60 30 76 4a	auth(block 30)
08	Tag	42 97 c0 a4	n_T
09	Reader	7d db 9b 83 67 eb 5d 83	$n_R \oplus ks1$, $a_R \oplus ks_2$
10	Tag	8b d4 10 08	$a_T \oplus ks_3$

CASE STUDY – MIFARE CLASSIC

- Hacker's favorite
  - (2008) Hardware reverse engineering
    - Custom encryption: Crypto-1
    - Sniff and decrypt attack
  - (2009) Nested Attack – MFOC tool
    - Know one key, crack all (10 sec)
  - (2009) Dark-Side Attack - MFCUK tool
    - Card-only attack (10 min)
  - (2015) HardNested Attack
    - Card-only attack (30 min)
  - A lot more …



MIFARE CLASSIC – ATTACK SCENARIOS

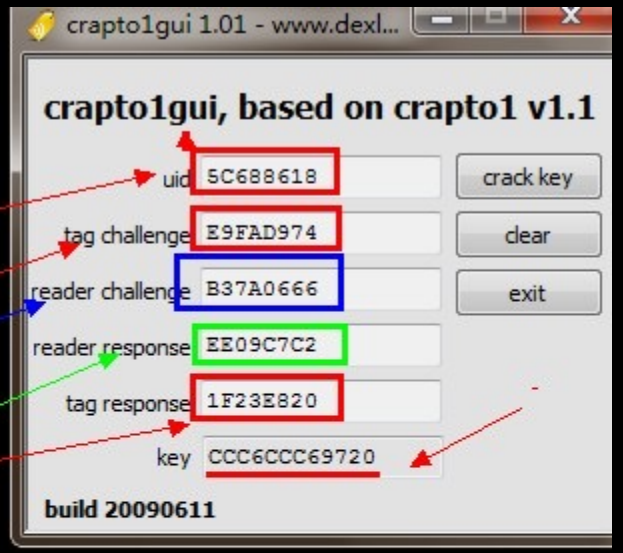
- Try default keys:

ffffffffff	a0a1a2a3a4a5
D3f7d3f7d3f7	aabbccddeeff
b0b1b2b3b4b5	000000000000
4d3a99c351dd	1a982c7e459a

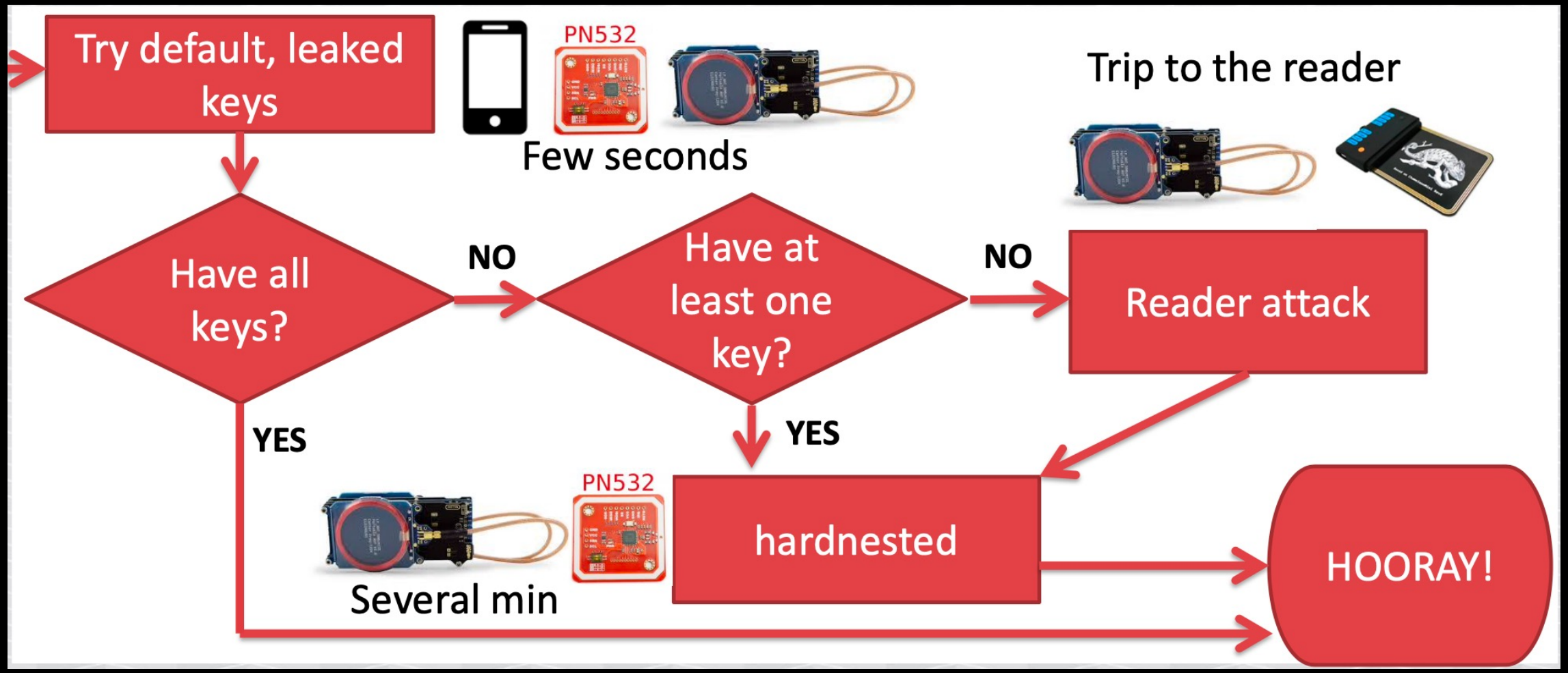
- Some keys are known -> Nested attack (MFOC) to recover the rest
- If no default key found, try Dard-Side Attack (MFCUK)
- If all not work -> sniff and decrypt

MIFARE CLASSIC – ATTACK SCENARIOS

```
proxmark3> hf 14a snoop
#db# cancelled_a
#db# maxBehindBy=4, Uart.state=0, Uart.byteCnt=0
#db# Uart.byteCntMax=20, traceLen=127, Uart.output[0]
proxmark3> hf 14a list
recorded activity:
 ETU      :rssi: who bytes
---------+----+----+-----------
 +      0:   0: TAG 04  00
 +    464:    :     93  20
 +     64:   0: TAG 5c  68  86  18  aa
 +   1240:    :     93  70  5c  68  86  18  aa  c6  2c
 +     64:   0: TAG 08  b6  dd
 +    704:    :     60  38  3e  c6
 +    112:   0: TAG e9  fa  d9  74
 +   1504:    :     b3  7a  06  66  ee  09  c7  c2      !crc
 +     64:   0: TAG 1f  23! e8  20
 +   1032:    :     40  62  ec  23      !crc
 +     64:   0: TAG 9a! 20  07  ff  60! 58! d4! 07! 04  c8! 56! 97! 3b! a4! 86  67! ca! 4e      !crc
 +   2464:    :     9e  da  78  b2      !crc
 +     64:   0: TAG 00! a1! dc  8b! 4c! b3  02! 6d  c4! 1b! ab  75! e7! 6c  d3  a8! a4  e5      !crc
 +   2464:    :     df  6e  0e  dc      !crc
 +     64:   0: TAG 4b! 62! f7! 87! e9  8c  8d  54  a1  e6  9c  9f! 77! 17  a2! f9! b9! 2f      !crc
 +   2464:    :     76  71  38  b0      !crc
 +     64:   0: TAG 8e! 83  73  07  e3  e3! a9! ec  24  a8! 8c  5e! 47! a5  46  bd  24! 4d!     !crc
 +   2464:    :     c5  b5  8f  a2      !crc
```



OVERALL ATTACK FLOW



MIFARE CLASSIC – ATTACK SCENARIOS

- After all data is decrypted and read
  - Clone to a blank card or emulate with proxmark3
  - Some situation require the change of UID
    - Chinese Magic Card: UID changeable, backdoor commands (￥1.00)
      - Supported by libnfc, proxmark3, etc

SECURITY ADVICE

- NXP (manufacturer of MIFARE cards) recommends upgrade existing MIFARE Classic systems and donnot use it in any security relevant application.
- Use RFID shield (really?)
- Don’t lend your card to untrusted.
- Don’t leak photo of your card.

DEMO TIME

REFERENCES

- Proxmark3: https://github.com/Proxmark/proxmark3
- Paper of Dark-Side attack: https://discovery.ucl.ac.uk/id/eprint/196096/1/196096.pdf
- Paper of HardNested attack: https://dl.acm.org/doi/abs/10.1145/2810103.2813641
- A 2018 practical gudie to hacking NFC/RFID: https://smartlockpicking.com/slides/Confidence_A_2018_Practical_Guide_To_Hacking_RFID_NFC.pdf