SmartCard Security

MiFare Case

Charles GUILLEMET

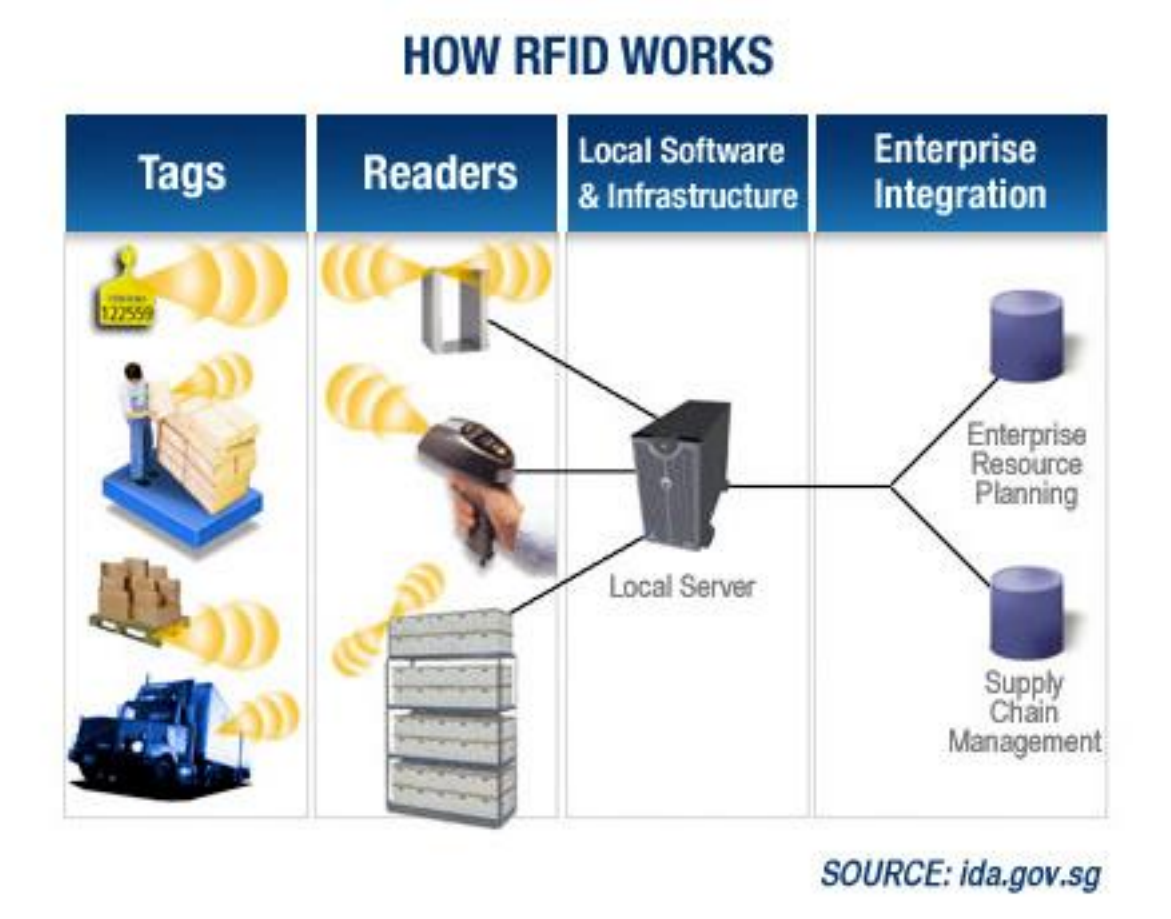
Mifare - Disclaimer

Cracking Mifare is

Illegal

- The objective is to give an example of bad choices in designing security system
- This research has been done in my freetime

MIFARE example



Mifare use

- Widely used
  - Authentication:
    - Vigik system
    - access control
  - Transportation:
    - Oyster card (London)
    - IstanbulKart
    - …

Mifare Design

- Designed by NXP (Holland)
  - (old Philips Electronics)
- Use the 14443 Type A for communication
- Cheap circuit (few cents)
- Licensed

Mifare Design

- « Cryptography »:
  - Invented and maintained by NXP Semiconductor
  - Security by obscurity

  This always fails: this time again

  - Name of the algorithm: Crypto1

- More then 4 billions cards produced !

  Several hundreds of millions still used

Mifare Security

- UID read only
- Mutual Authentication
- Crypto1 secrecy
- Hardware only implementation

Mifare Structure

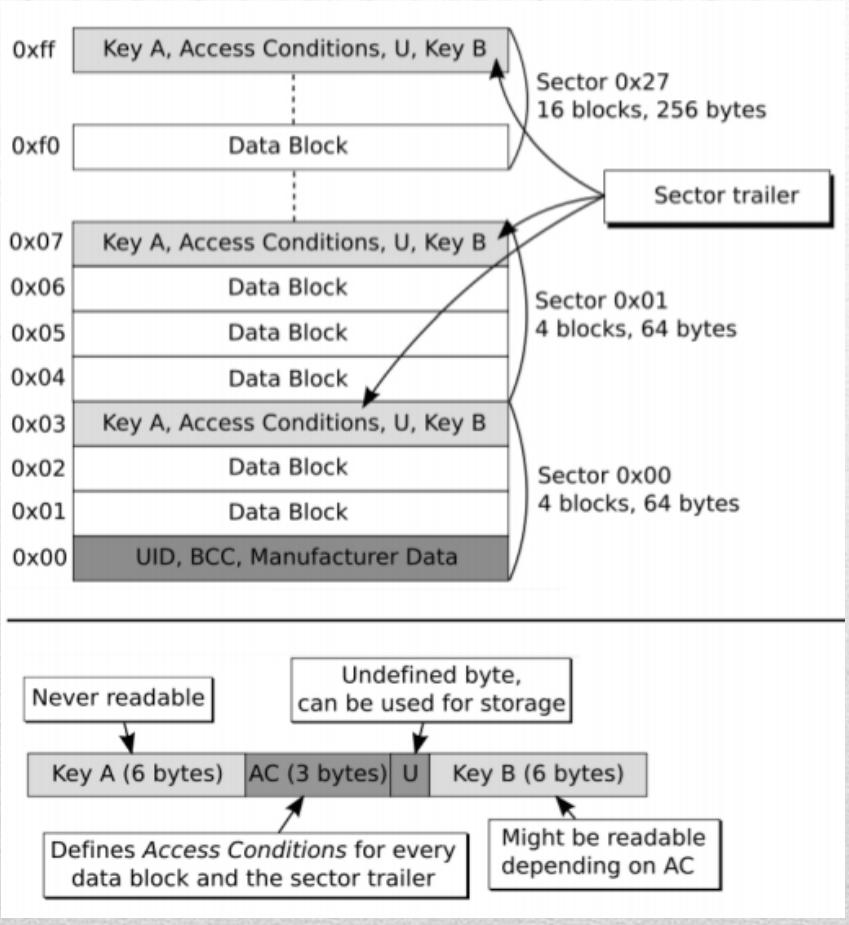
- Sectors of 4

16-byte blocks (1K)

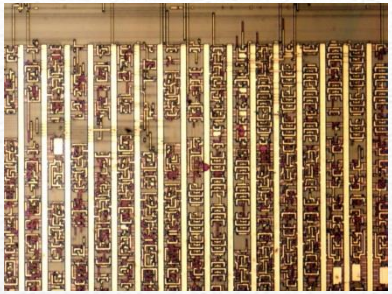
- 1st block contains

UID, BCC and Data from the manufacturer

- Last block contains keys and access rights



Mifare reversed



- Partially reversed in 2007 by 2 german researchers
  - Crypto1 partially reversed
  - Weakness found
- 2008 : Radbond university fully reversed
- NXP tried to stop the discolosure of the article by judicial process
- The court allowed the disclosure

Mifare fully reversed

- Radbond university published the full specification of Crypto-1 as open source
- Since then, LOT of attacks found

Mifare Security

- Reverse engineering on the circuit himself
- Acids and microscope

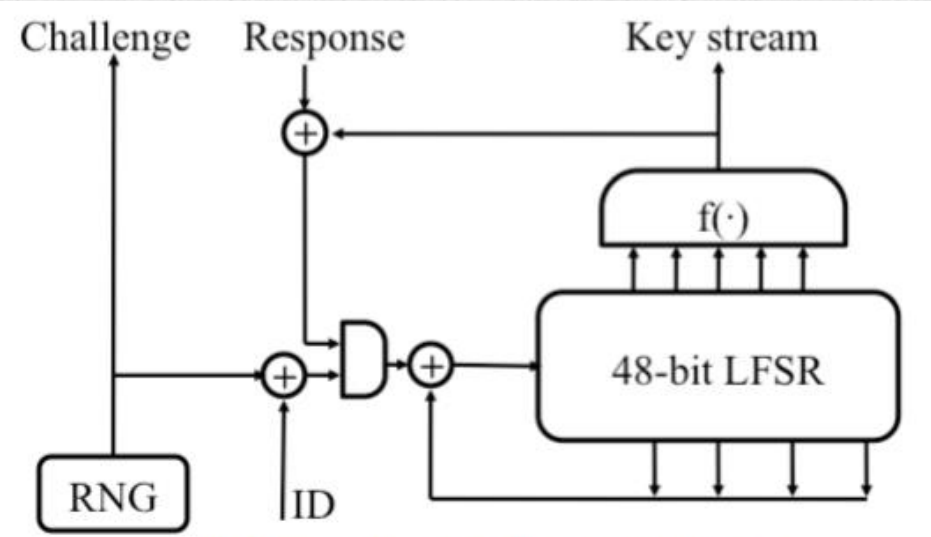
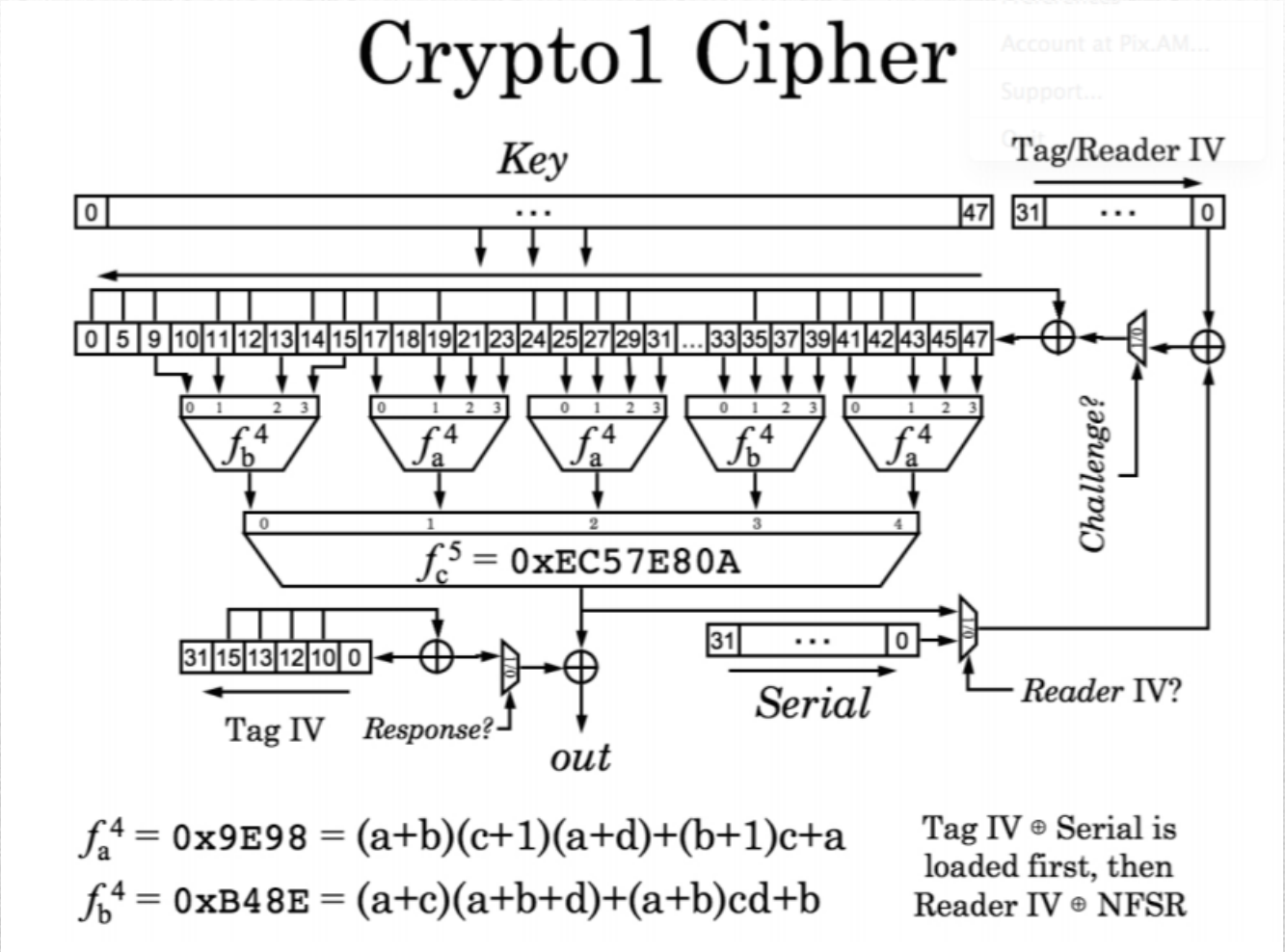
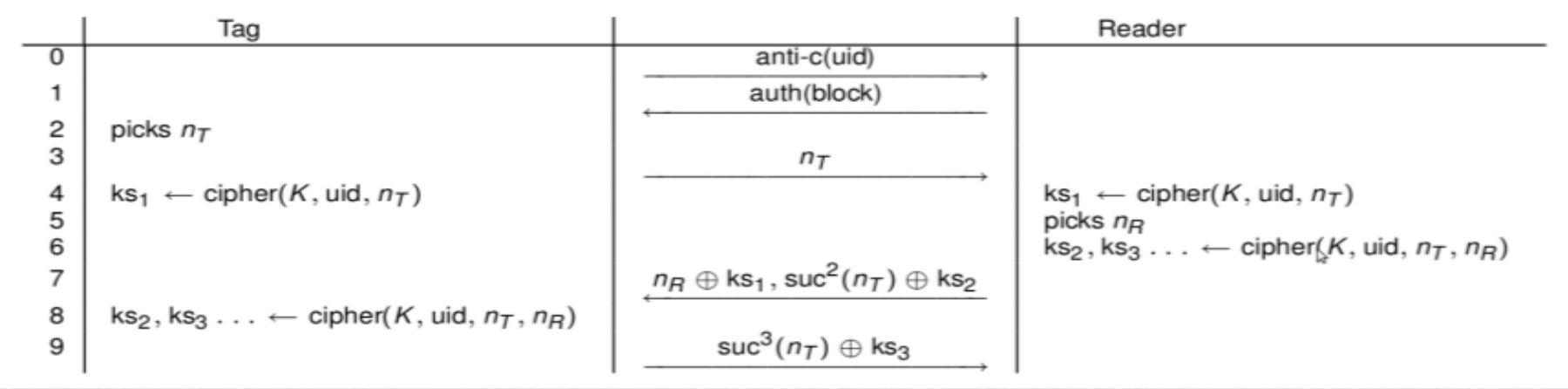


Figure 2: Crypto-1 stream cipher and initialization.

Mifare security : Crypto1



Mifare Security



- Nt, Nr -> nonces picked by tag and reader
- ks1, ks2 and ks3 -> key stream generated by cipher (96
- bits total and 32 bits each).
- suc2(Nt) or {Ar} and suc3(Nt) or {At} -> bijective functions

Mifare Security

- Keys with only 48 bit of length (Brute-force feasible – with FPGA aprox. 10h to recover one key)

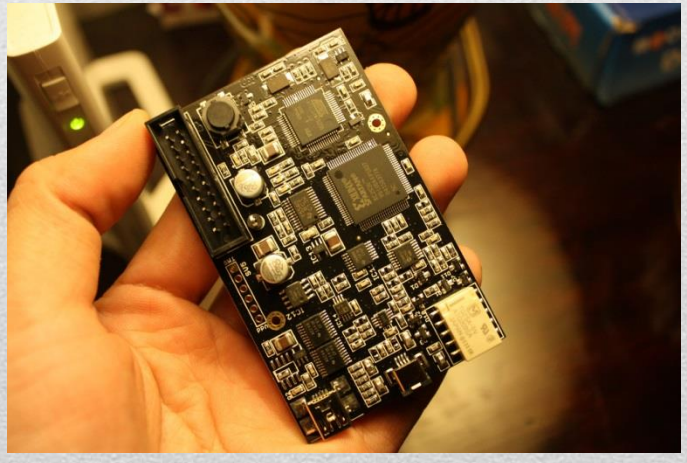
YES : 48 bits

- The LFSR (Linear Feedback Shift Register) used by RNG is predictable (constant initial condition).
  - Each random number only depends of the quantity of clock cycles between: the time when the reader was turned up and the time when the random number is requested.

- Since an attacker controls the time of protocol, he is able to control the generated random numbers and that way recover the keys from communication.

Mifare Security

- Attacks: Proxmark3
  - Open source Design and Embedded software
- Sniffing
  - Needs a valid card and reader communication
  - Able to retrieve keys of blocks involved
- Replay
- Emulation



Mifare Security

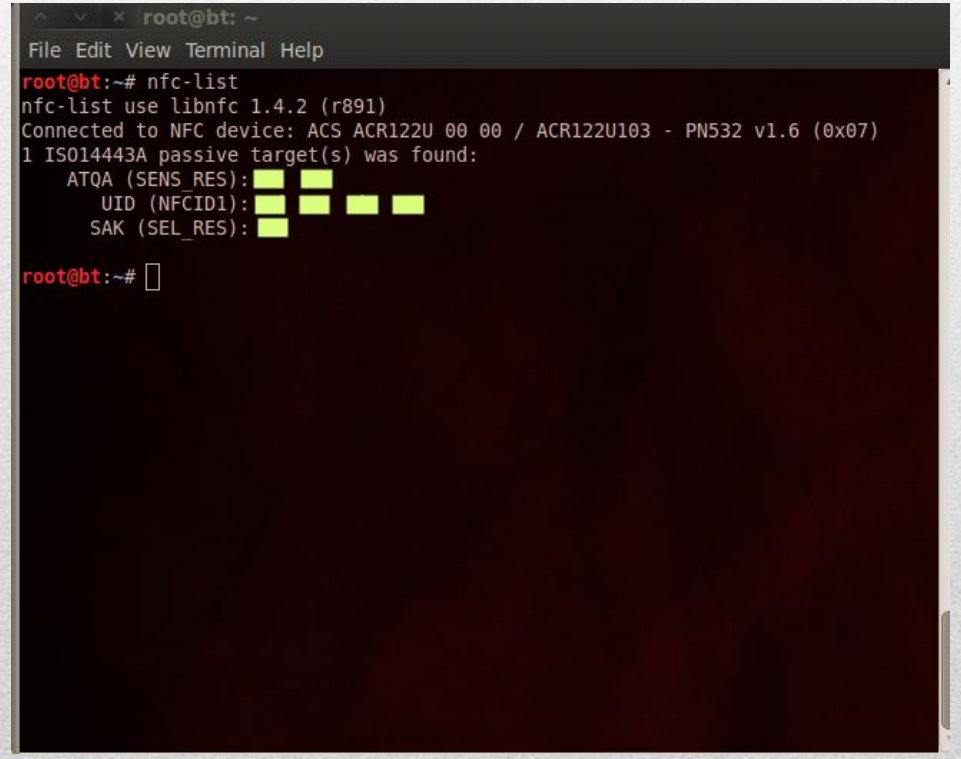
- Attacks: MF Tools
  - Card only attack
  - MFOC + MFCUK (2009) (DarkSide and Nested)
- Nested : knowing 1 key !
  - Authenticate to the block with default key and read tag's Nt (determined by LFSR)
  - Authenticate to the same block with default key and read tag's Nt' (determined by LFSR) (this authentication is in an encrypted session)
  - Compute “timing distance” (number of LFSR shifts) Guess the next Nt value, calculate ks1, ks2 and ks3 and try authenticate to a different block.

MIFARE : Attack Steps

- Initially utilize the MFOC tool to test if the card utilize any default keys. (around 1 minute)
- If the card utilizes any of default keys the MFOC tool will perform the Nested attack utilizing.
- If the card haven’t use any of the default keys, utilize the MFCUK to recover at least one key from any sector of card (few minutes)

MIFARE : Attack Steps

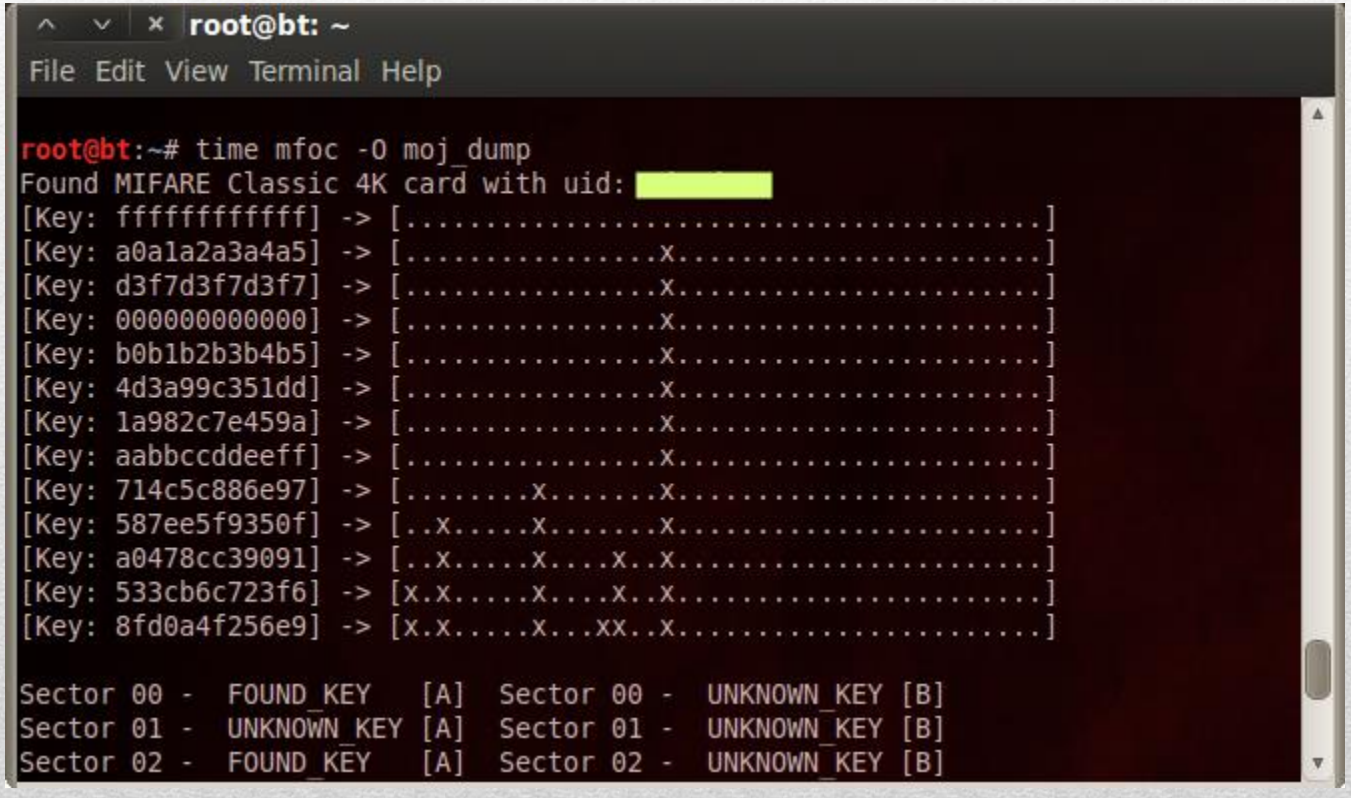
mfoc / libnfc available in official repos



MIFARE : Attack Steps

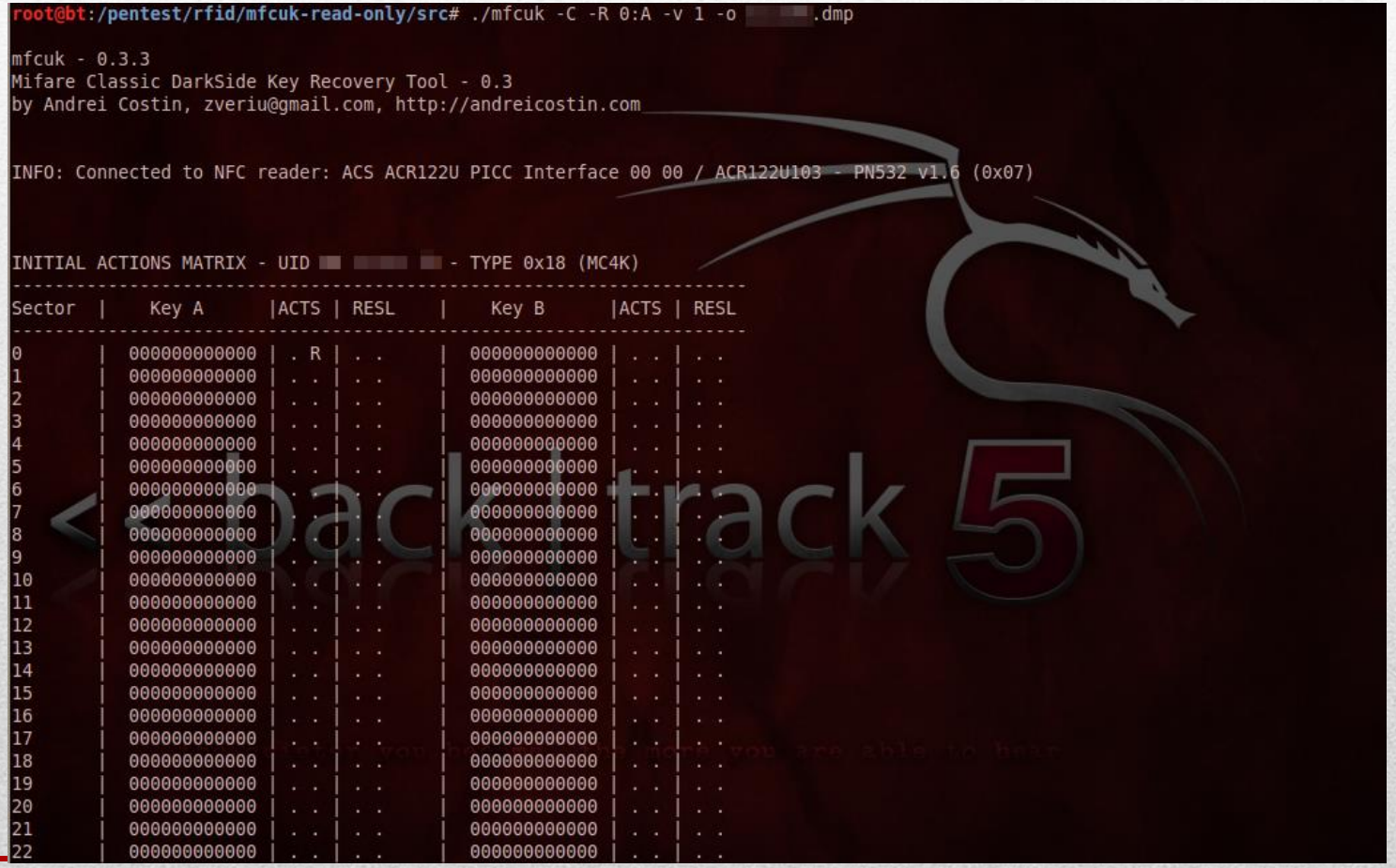
- mfoc tries first the default keys

(Most of the time, unused sector have default keys)

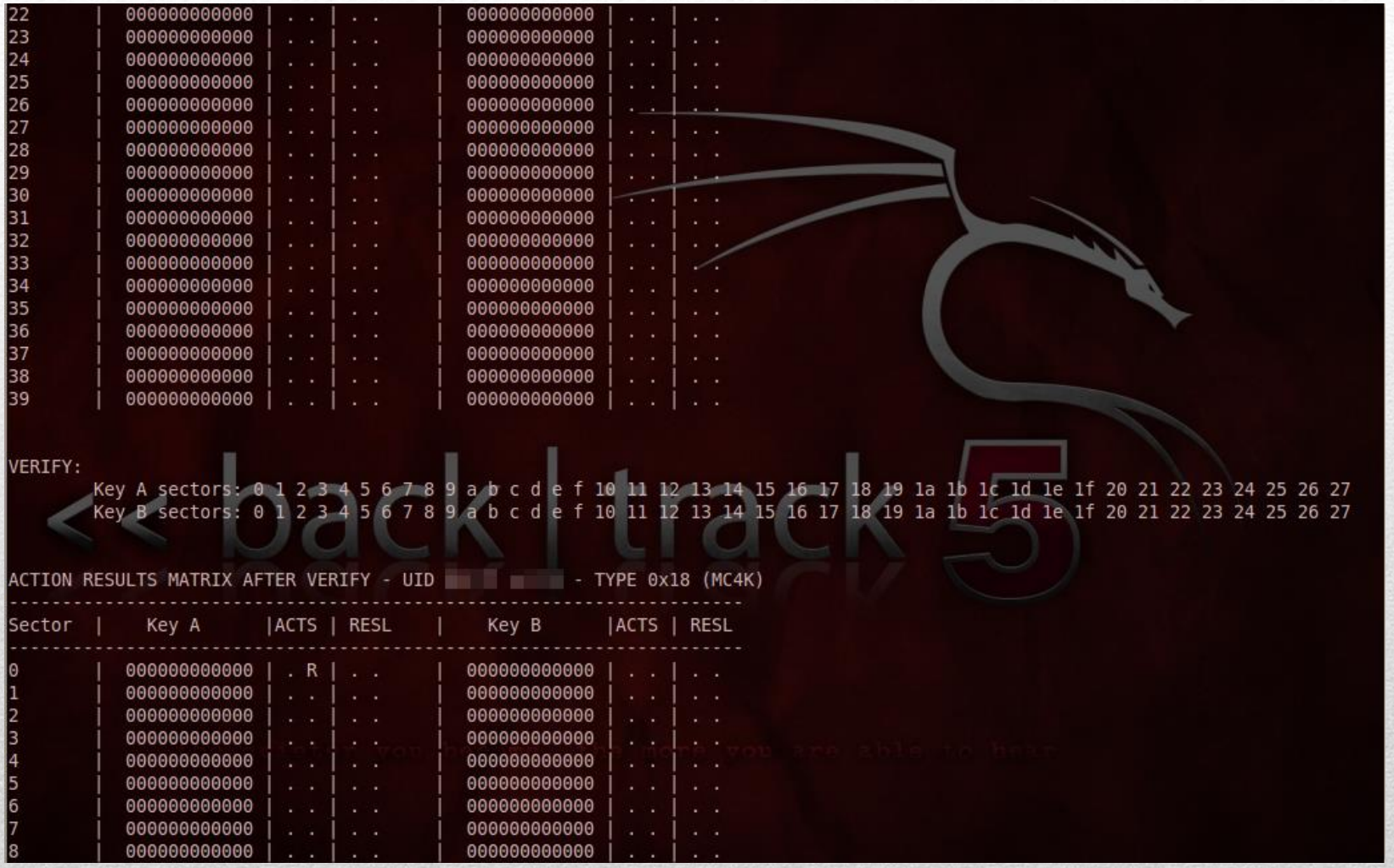


MIFARE : Attack Steps

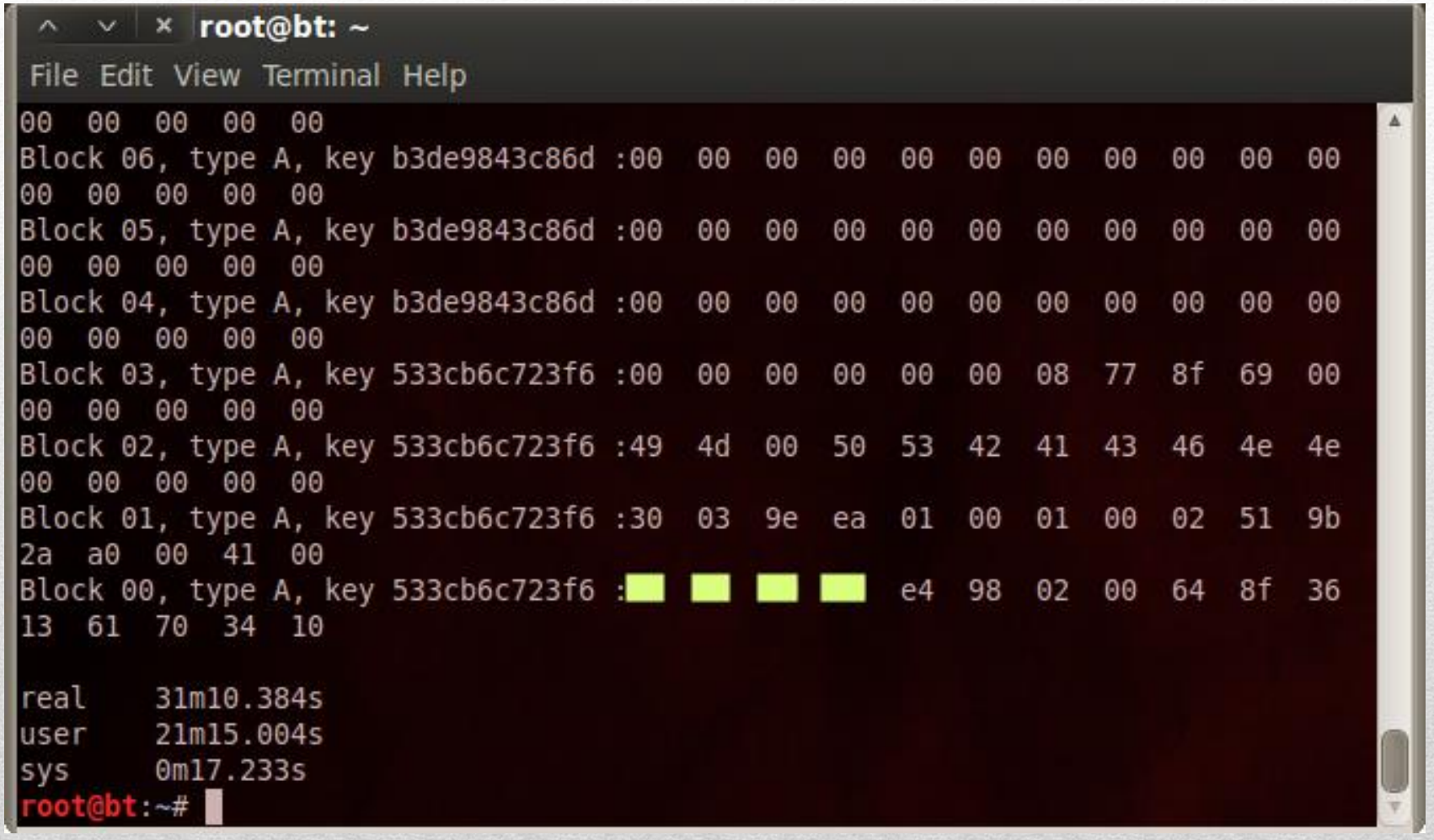
- mfcuk



MIFARE : Attack Steps



MIFARE : Attack Steps



MIFARE : Attack Steps

- Needed:
  - Tag reader: ~30euros
  - UID writable Mifare Tags (Chinese tag): ~2euros
- Few minutes
- Can clone ANY MIFARE classic tag
- Once the key is discovered, it’s possible to read any token within few ms

Mifare use

- Still widely used
  - Authentication:
    - Vigik system: still used
      - Default keys on unused sector
      - One sector used

      => the key is on the picture
    - access control: still used

  - Transportation:
    - Oyster card (London)
      - System changed due to fraud
    - IstanbulKart
      - System changed due to fraud

Mifare - Disclaimer

Cracking Mifare is

Illegal

Security by obscurity always fails

References

Freely inspired from

- Card-Only Attacks on MiFare Classic or How to Steal Your Oyster Card and Break into Buildings Worldwide (Nicolas Courtois)

- Hacking Mifare Classic Cards (Márcio Almeida)

- Practical Attacks on the MIFARE Classic by Wee Hon Tan (wht08)

- proxmark3 : http://www.proxmark.org/

- nfc-tools : http://nfc-tools.org/