possible.lv

RFID attacks
and
proxmark hands-on

@KirilsSolovjovs

About me

- Programming → sysad → networking
- IT security for the past 10+ y
- Owner and Lead Researcher at Possible Security
- Hacking and breaking things
  - http://kirils.org/
  - http://possiblesecurity.com/news/

Contents

- RFID basics
- RFID standarts
- Hacking tools
- Proxmark

+ Lots of demos

possible.lv

Let's get this out of the way: RFID vs NFC?

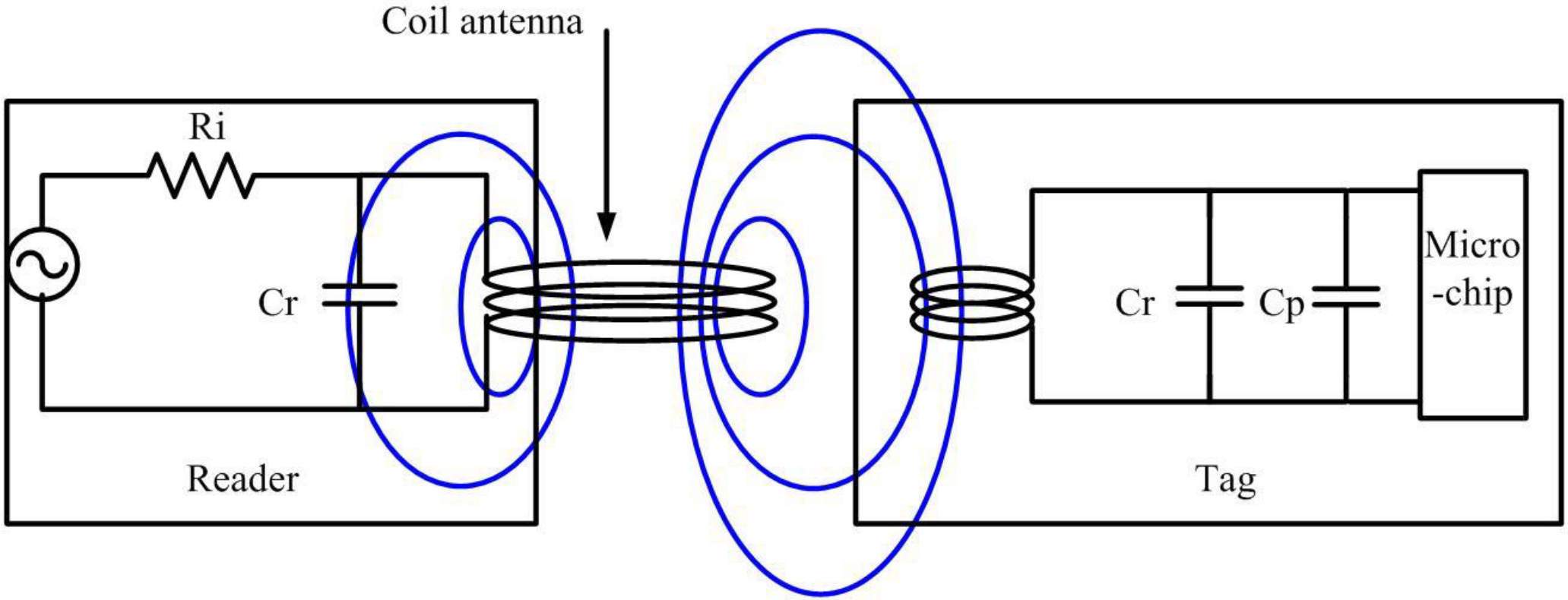
- NFC is a subset of RFID
  - 13.56MHz
  - ISO/IEC 14443
  - NFC device can be both a reader and a tag

RFID tag

- Microchip
- Antenna
- No power source

RFID

- Radio Frequency Identification



Typical RFID frequencies

possible.lv

- LF
- **125 kHz**
- 134.2 kHz
- …

- HF
- **13.56 MHz**
- …

RFID standards

- ISO/IEC 14443A
  - Mifare
- ISO/IEC 14443B
- ISO/IEC 15693

- em4xxx
- HID Global
  - iClass
  - Hitag2
  - Indala
- TI

Tools

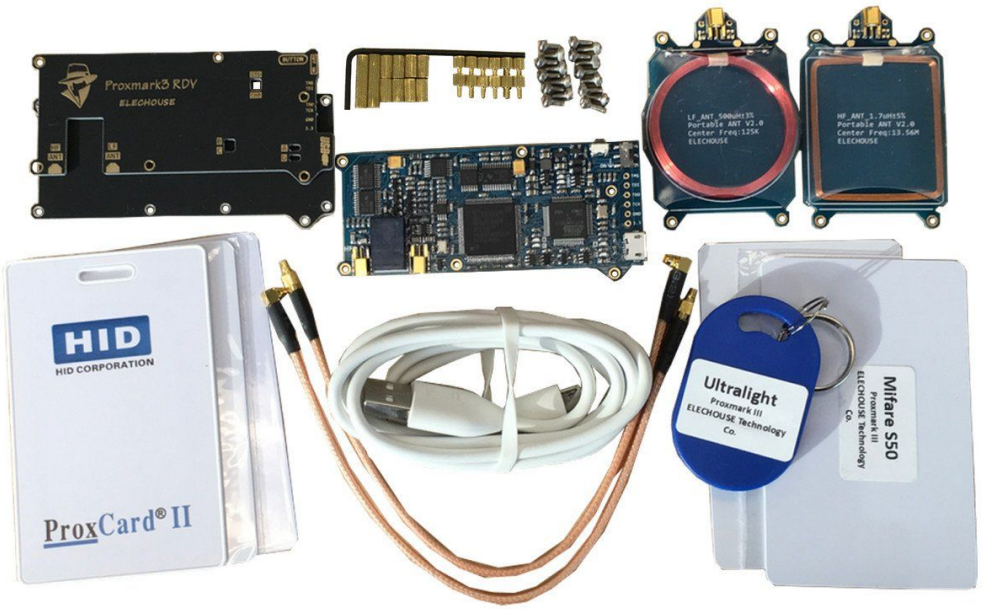
- RFID readers
- RFID duplication “gun”
- Frequency scanner
- BLEkey
- hackRF… ?
- Proxmark III !

possible.lv

Proxmark III

possible.lv

Proxmark III RDV 2 / 4



Wiegand interface

- Problematic for UID-based protocols

- BLEKey
  - Bluetooth connected UID sniffer / storage

Card cloning

- Duplicating contents of one card into another
- Often involves breaking some cryptography or defeating some other protection

Mifare Ultralight

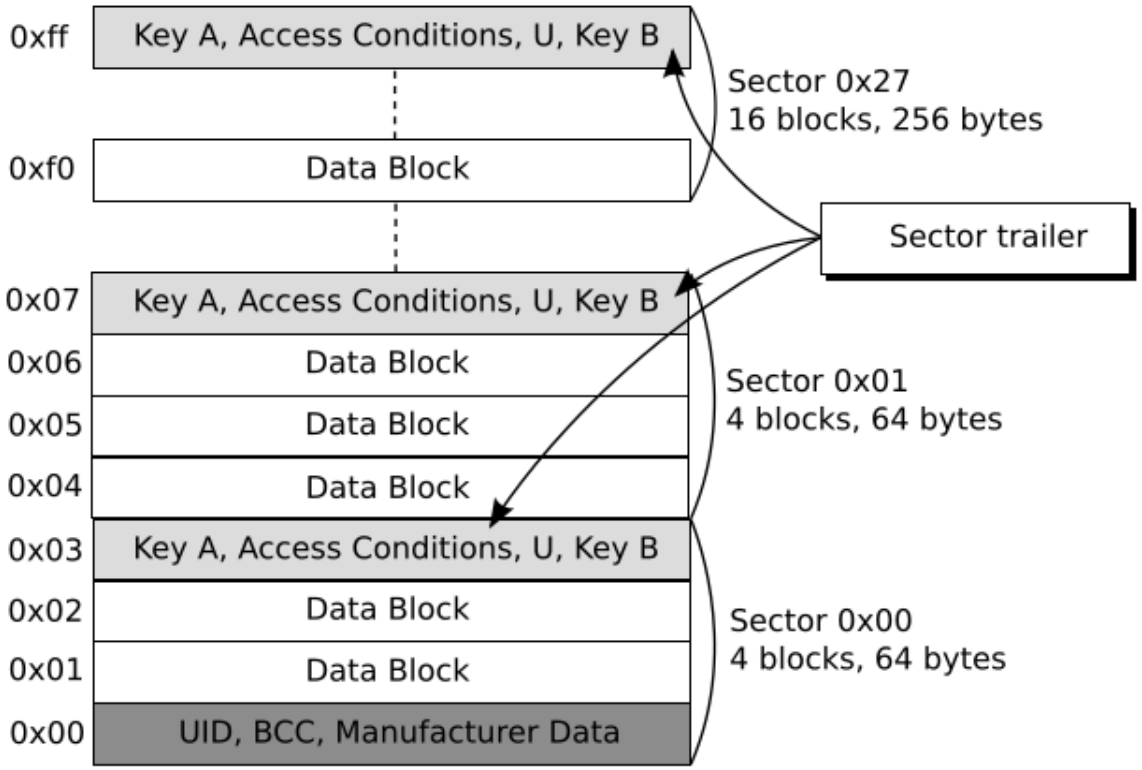
Byte Number	0x00	0x01	0x02	0x03	Page
Serial Number	SN0	SN1	SN2	BCC0	0x00
Serial Number	SN3	SN4	SN5	SN6	0x01
Internal / Lock	BCC1	Internal	Lock0	Lock1	0x02
OTP	OTP0	OTP1	OTP2	OTP3	0x03
Data Read/Write	Data0	Data1	Data2	Data3	0x04
Data Read/Write	Data4	Data5	Data6	Data7	0x05
Data Read/Write	Data8	Data9	Data10	Data11	0x06
Data Read/Write	Data12	Data13	Data14	Data15	0x07
Data Read/Write	Data16	Data17	Data18	Data19	0x08
Data Read/Write	Data20	Data21	Data22	Data23	0x09
Data Read/Write	Data24	Data25	Data26	Data27	0x0A
Data Read/Write	Data28	Data29	Data30	Data31	0x0B
Data Read/Write	Data32	Data33	Data34	Data35	0x0C
Data Read/Write	Data36	Data37	Data38	Data39	0x0D
Data Read/Write	Data40	Data41	Data42	Data43	0x0E
Data Read/Write	Data44	Data45	Data46	Data47	0x0F

MF0 U1 memory map

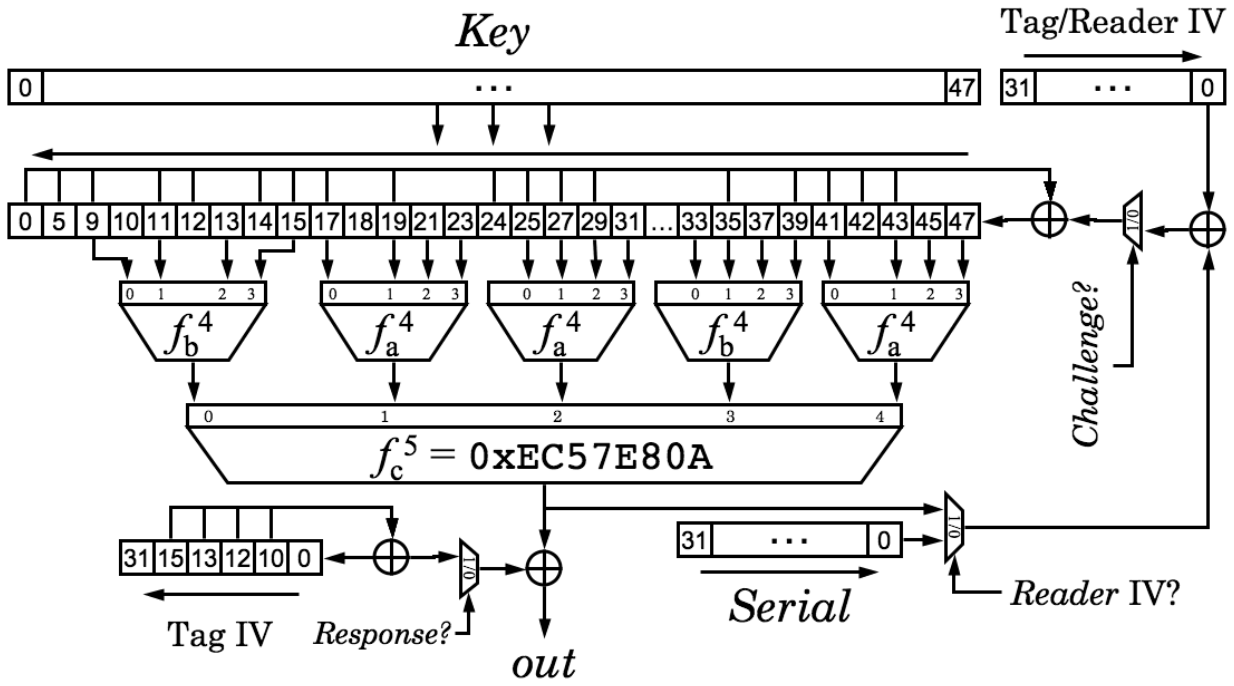
Remark: Bold frame indicates user area

Fig 4. Memory organization

Mifare Classic



Crypto1 Cipher

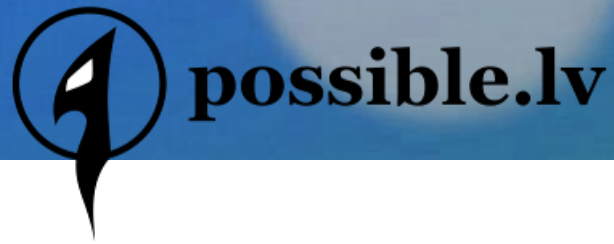


f_a^4 = 0x9E98 = (a+b)(c+1)(a+d)+(b+1)c+a

f_b^4 = 0xB48E = (a+c)(a+b+d)+(a+b)cd+b

Tag IV ⊕ Serial is loaded first, then Reader IV ⊕ NFSR

Proxmark III setup



- https://github.com/Proxmark/proxmark3/wiki/Kali-Linux

Proxmark III magic

- reading cards...
- attacks…
  - + mfkey

Proxmark III snooping