Security implications of DIY implants

Who am I?

- Alex Smith
- DIY cyborg/Grinder
- Biohack.me
- Cyberise.me

Warning: graphic content (blood)

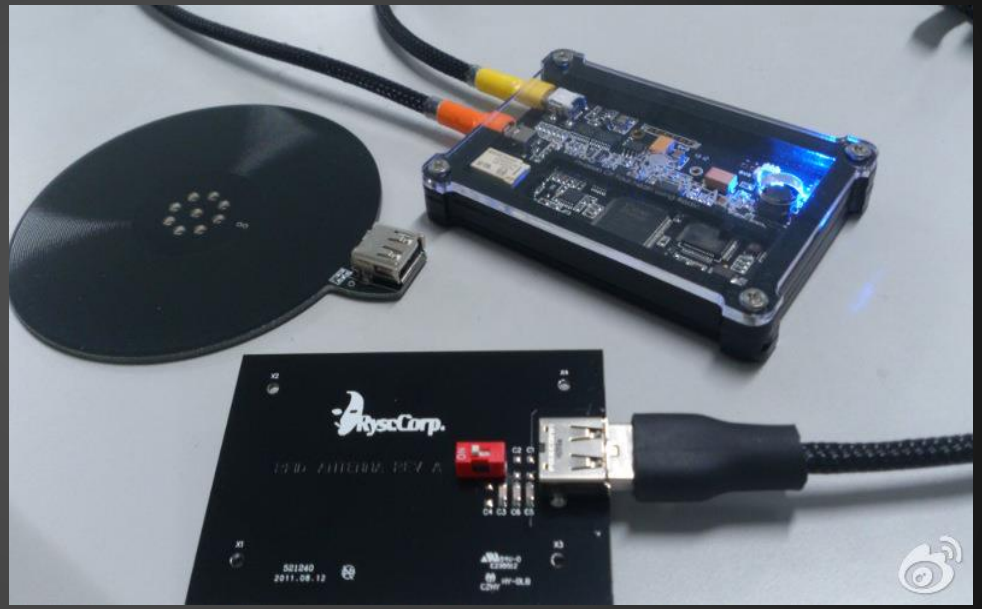
RFID Access cards

- Card frequencies
  - 125 kHz
  - 13.56 MHz
- LF Protocols
  - FDX
  - HID
  - Indala
  - EM4X

Low Frequency RFID Security

- (lack of) Crypto
- Proxmark3
- Rfidler
- handheld copier

- Cloning
- AT5577



RFID Implants

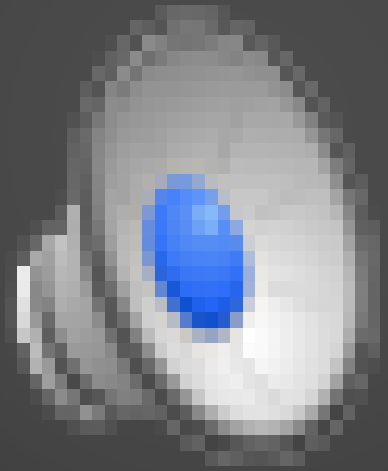
- Types
  - NFC
  - RFID
  - Sensor
- legality
  - DIY is fine
  - check your local laws

RFID Implants - Procedure

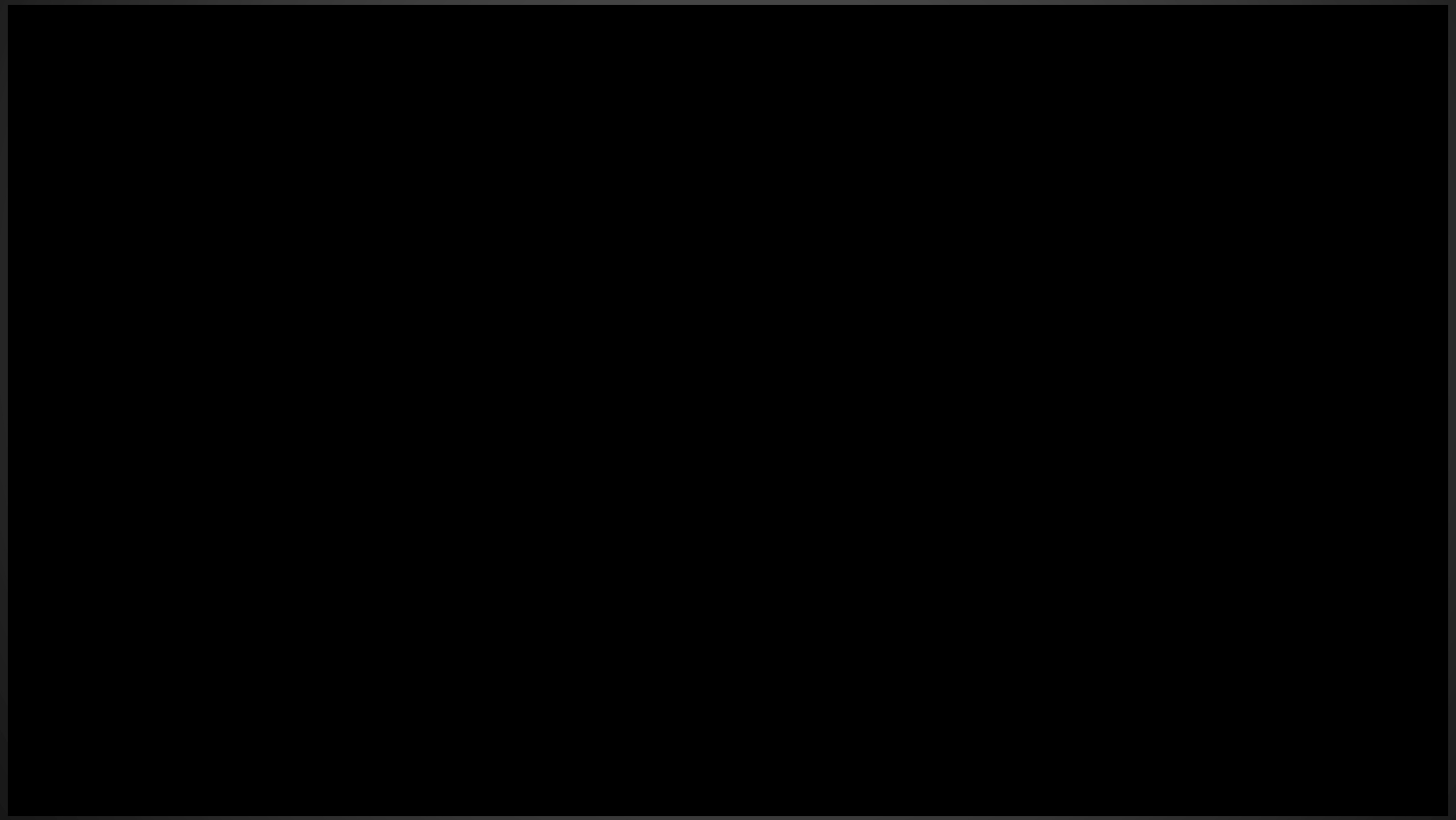
- Location
- Prep
- Injection
- Healing

- Safety
- Security

Implant video



Video of usage



Video of usage

Security Implications

- Concealed access
- Loss
- Theft

Demo of cloning card to implant

RFID Access cards

- Card frequencies
  - 125 kHz
  - 13.56 MHz
- HF Protocols
  - NFC
  - Mifare
  - iClass

Mifare Classic

- Attacks
- Cloning/Changeable UID cards
- Making implants

Mifare Classic attacks

- Snooping
- Brute force
- Cascade attack
- New analytical attack

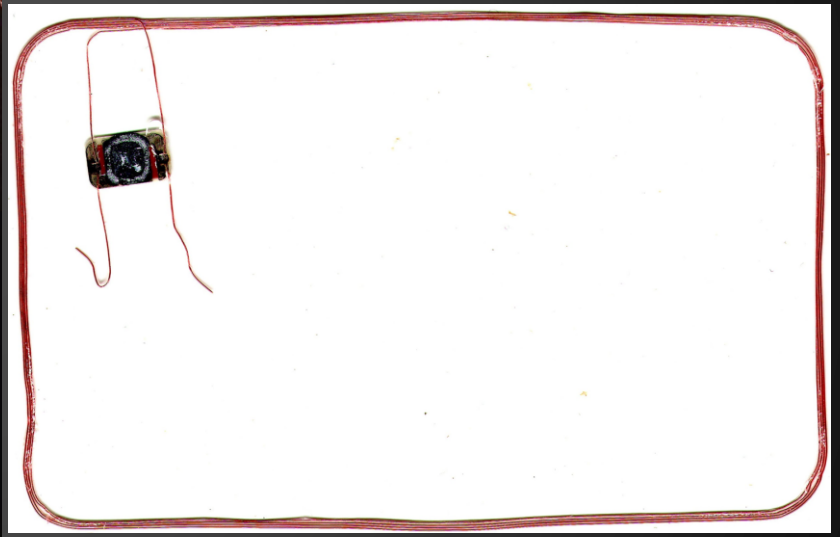
Cloning/Changeable UID cards

- Copying data
- “Magic” Mifare chips

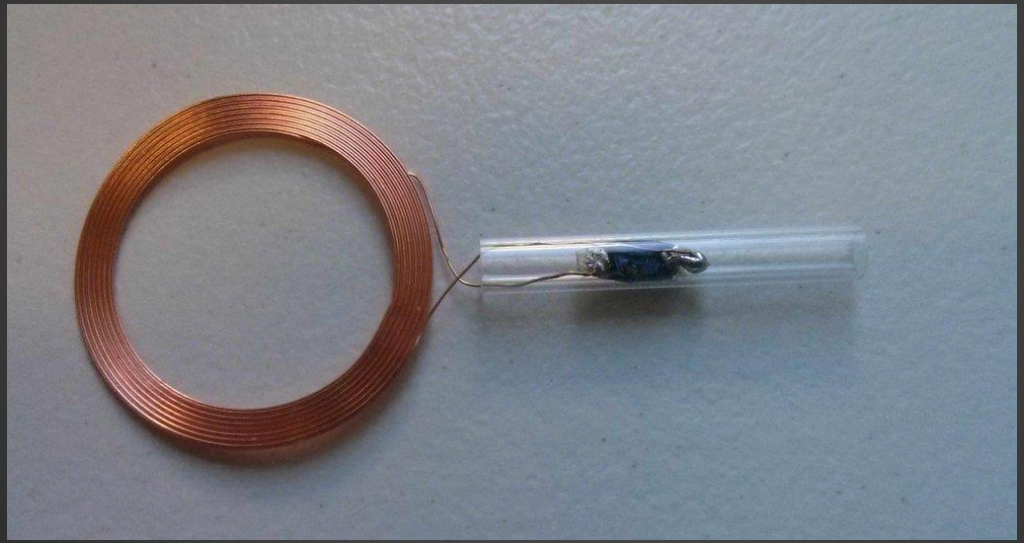
Mifare implants

- Hard coded UID Mifare implants
- Extracting chips
- Cutting chips to fit in capsules
- Antennas
- Sealing glass

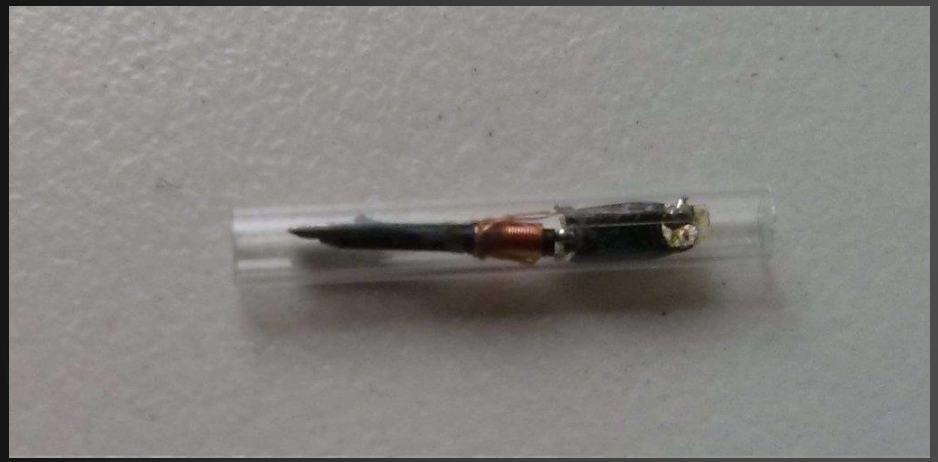
Extracting the chip

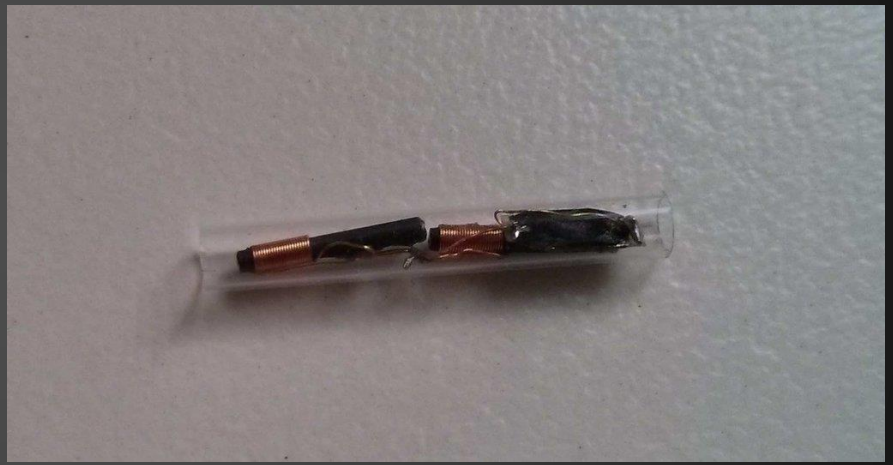


Reducing the size

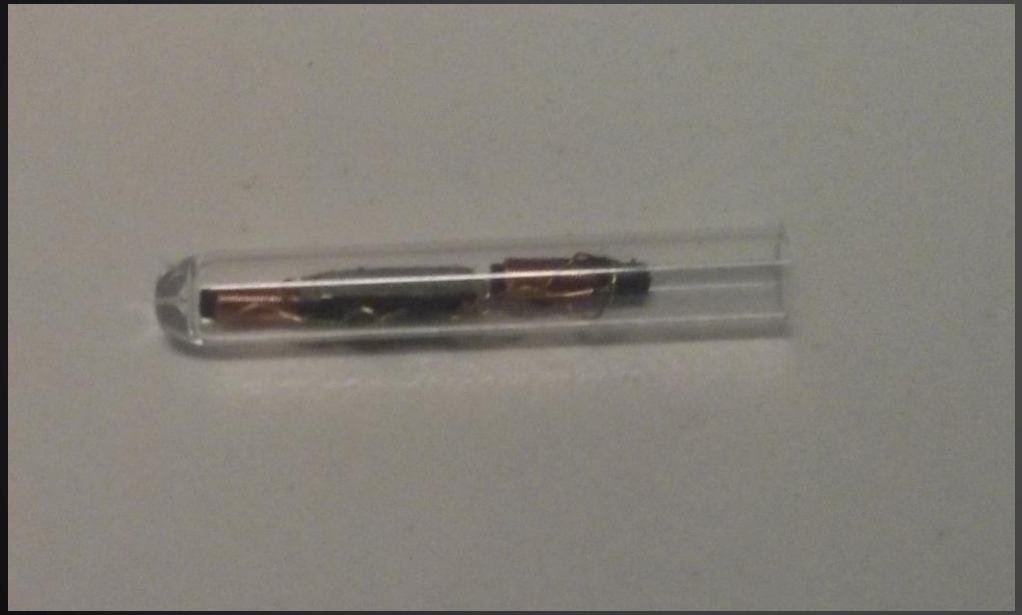


Antenna





Sealing capsule



Size scale

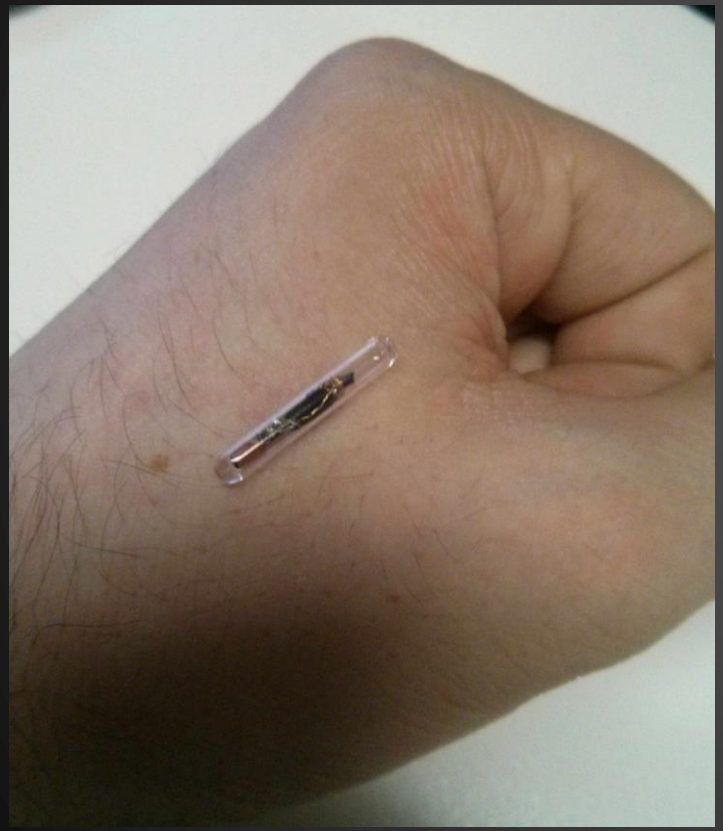

NORGE
5
5


UNITED STATES OF AMERICA
LIBERTY
QUARTER DOLLAR
IN GOD WE TRUST

Implant sizes

1.5x8mm
2x12mm
3x16mm

Finished implant



Demo of cloning card to implant

Security Implications

- Same as LF: concealed access/loss/theft

But also:

- Data infiltration/exfiltration
- Reader attacks

- Border crossing

Progress since DEFCON 23 (2015)

- Mifare Classic cloning
- Extracting IC and bioproofing

Future Goals

- UID changeable Mifare Ultralight (C) - easy, same process used for Mifare Classic ETA a couple of months
- Mifare DESFire - same as above
- Reduce implant size - medium difficulty, eta 1 year?
- Chip emulation - hard, probably at least a few years away

Questions