RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Fun with Proxmark3

SESSION ID: BR-R04A

Daniel Ayoub

Product Manager – IPS
Dell Network Security
@DanielAyoub

For educational purposes only. My views only, not of Dell. I did not create or contribute to the development of any of the hardware or software discussed.

Agenda

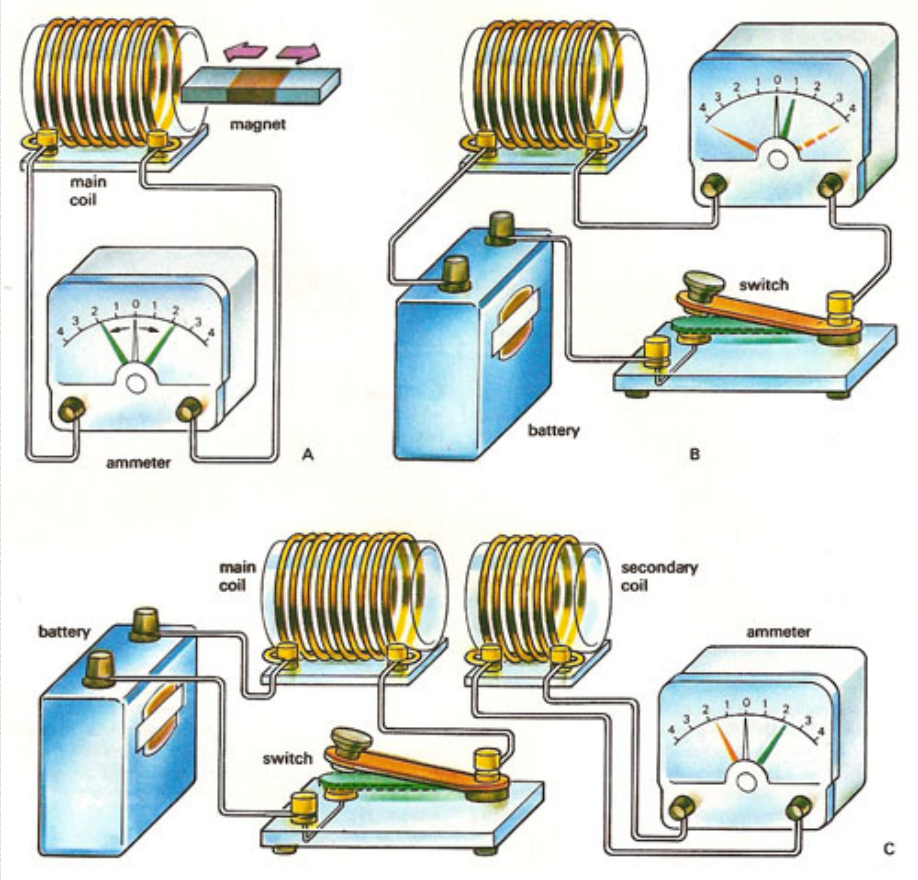
1. RFID primer
2. RFID authentication systems
3. Promark3
   - Read ID card
   - Simulate ID card
4. Risk overview and conclusion

The physics…

Electromagnetic Induction

The induced electromotive force in any closed circuit is equal to the negative of the time rate of change of the magnetic flux through the circuit.

-Faraday's Law 1831



http://www.daviddarling.info/encyclopedia/E/electromagnetic_induction.html
http://en.wikipedia.org/wiki/Electromagnetic_induction

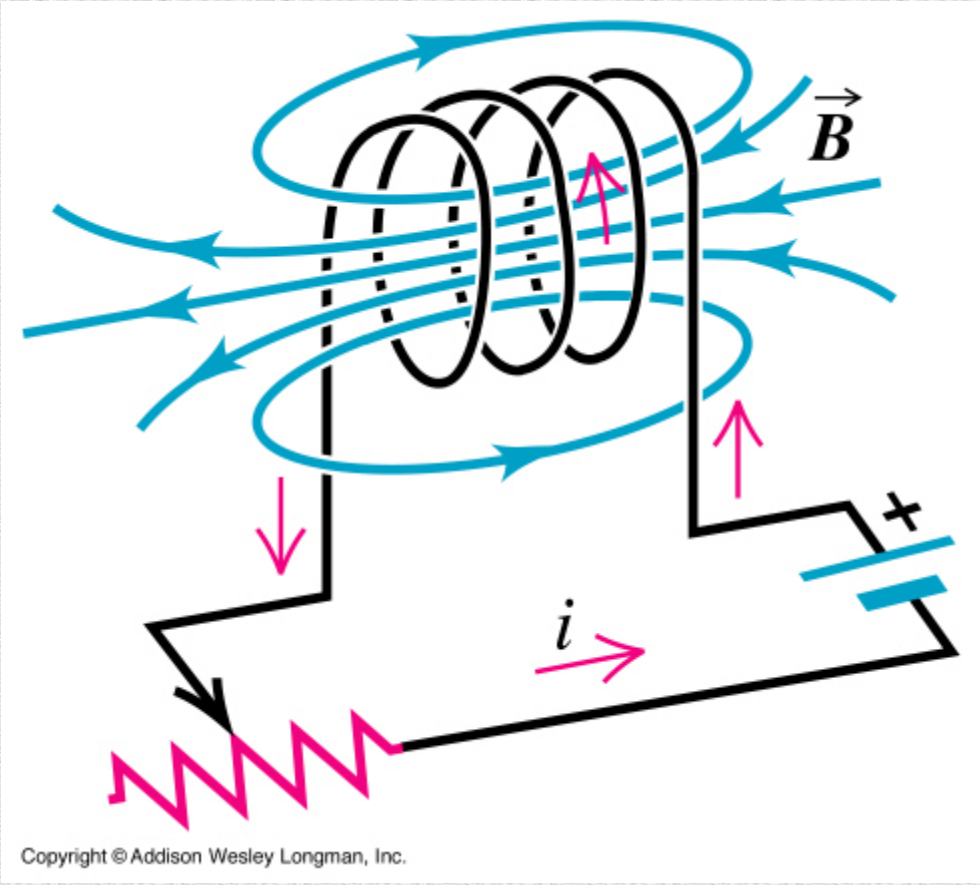
Faraday's Law

Practical Application

When a wire coil is exposed to magnetic field flowing in the direction 'B', an electric current is induced in the wire in direction 'i'.

The opposite is also true…

When an electric current in direction 'i' is sent through a wire coil, a magnetic field in the direction 'B' is generated.



http://www.physics.sjsu.edu/becker/physics51/induction.htm

RFID: Radio Frequency Identification

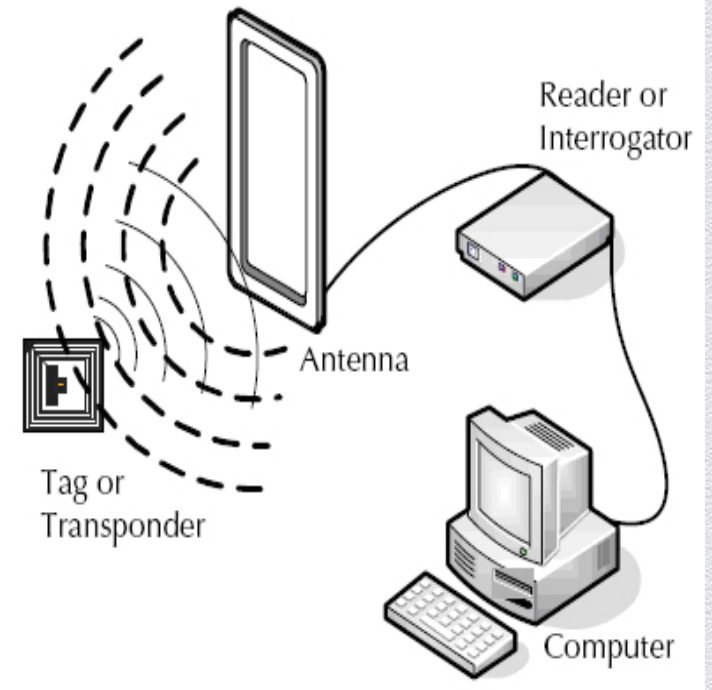
- Developed in 1970s
- Consists of microchip and an antenna
- Current generated by the antenna powers the chip
- Data about the RFID tag can be stored on the chip
- Remote readers can access this data
- There are many form factors of RFID circuits

Antenna

Chip

http://www.fidis.net/resources/deliverables/hightechid/int-d3700/doc/6/

Reading RFID Tags

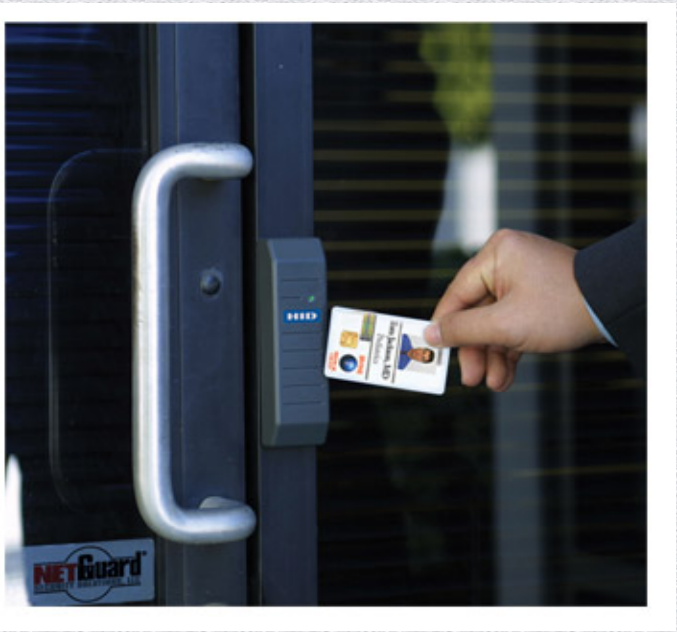


- Several standards for RFID tags
  - The modulation, protocols and microchip type are the main differences
- Different chips provide different levels of information storage and authentication
- Each reader and antenna are specially tuned for specific RFID tag types
- Software running on the computer is used to interpret the data and log the interaction
- Many modern cards rely on encrypted communications

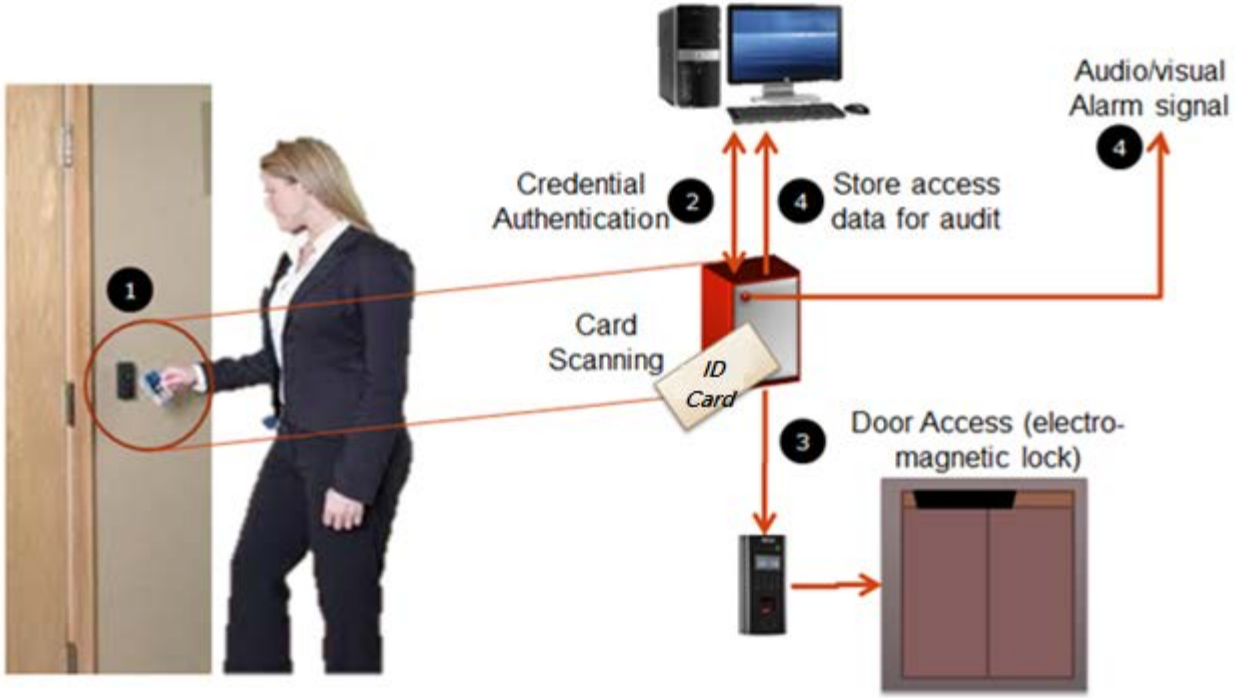
https://www.msasys.com/hardware/rfid-products/rfid-readers
http://www.epc-rfid.info/rfid

RFID Applications

RFID Access Control Systems



Access Control System



http://www.securespin.in/?page_id=169

ID Cards & Credentials

iCLASS® Seos™
State-of-the-art, SIO-enabled, high security smart card credentials for microprocessor cards and smartphones

iCLASS SE®
High security, SIO-enabled smart card credentials for iCLASS as well as MIFARE® technology and DESFire technology

pivCLASS®
pivCLASS Premium Security Dual interface Smart Card for FIPS201 deployments

iCLASS®
High frequency, secure contactless smart card credentials

ActivID® Authentication
Enables organizations to securely issue and manage smart card credentials

Crescendo®
High security hybrid smart card technology for converged physical and logical access control

FlexSmart®/ MIFARE®/ DESFire®
High frequency, secure contactless smart card credentials

HITAG
Low Frequency secure solution for contactless smart card credentials

HID Prox®
Low frequency, entry-level proximity cards for physical access control

Indala® Proximity
Low frequency entry-level proximity cards for physical access control

UltraCard®
Non-technology ID cards

LEGIC®
High Frequency, contactless smart card credentials

RFID Tag Types

- There are numerous standards, this vendor (HID) offers more than 10 different types of RFID based access cards.
- Different cards tend to be used for different purposes depending upon the level of authentication needed.
- Some cards even support things like FIPS201 and 3DES or AES encrypted communication for secure authentication.

http://www.hidglobal.com/product-display/cards-and-credentials

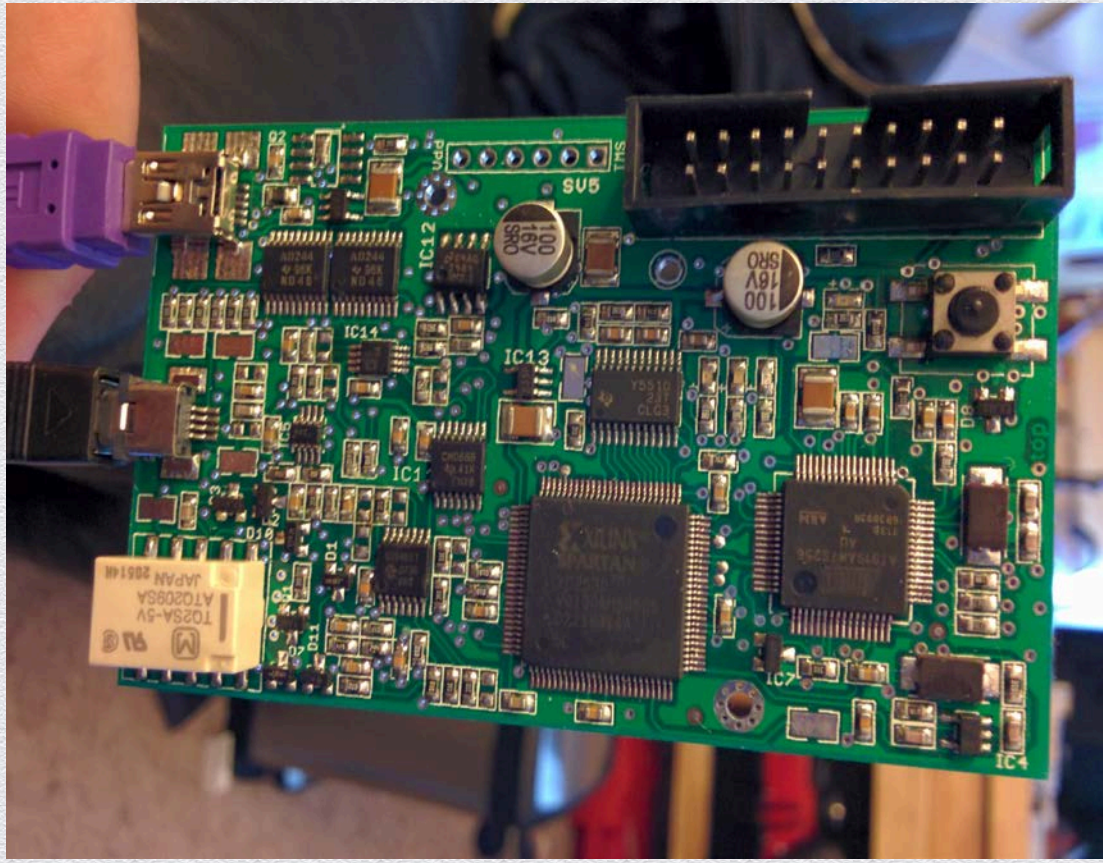
Breaking RFID

- Security researchers have been investigating RFID authentication technology for a number of years (5+).
- There are several examples of ‘broken’ RFID standards which are widely used (Mifare, iClass, Hitag2).
- Many attacks based on flaws in proprietary encryption and hashing protocols implemented by manufacturers.

http://www.youtube.com/watch?v=NW3RGbQTLhE
http://www.proxmark.org/forum/index.php
http://www.openpcd.org/OpenPCD_Passive_RFID_Project

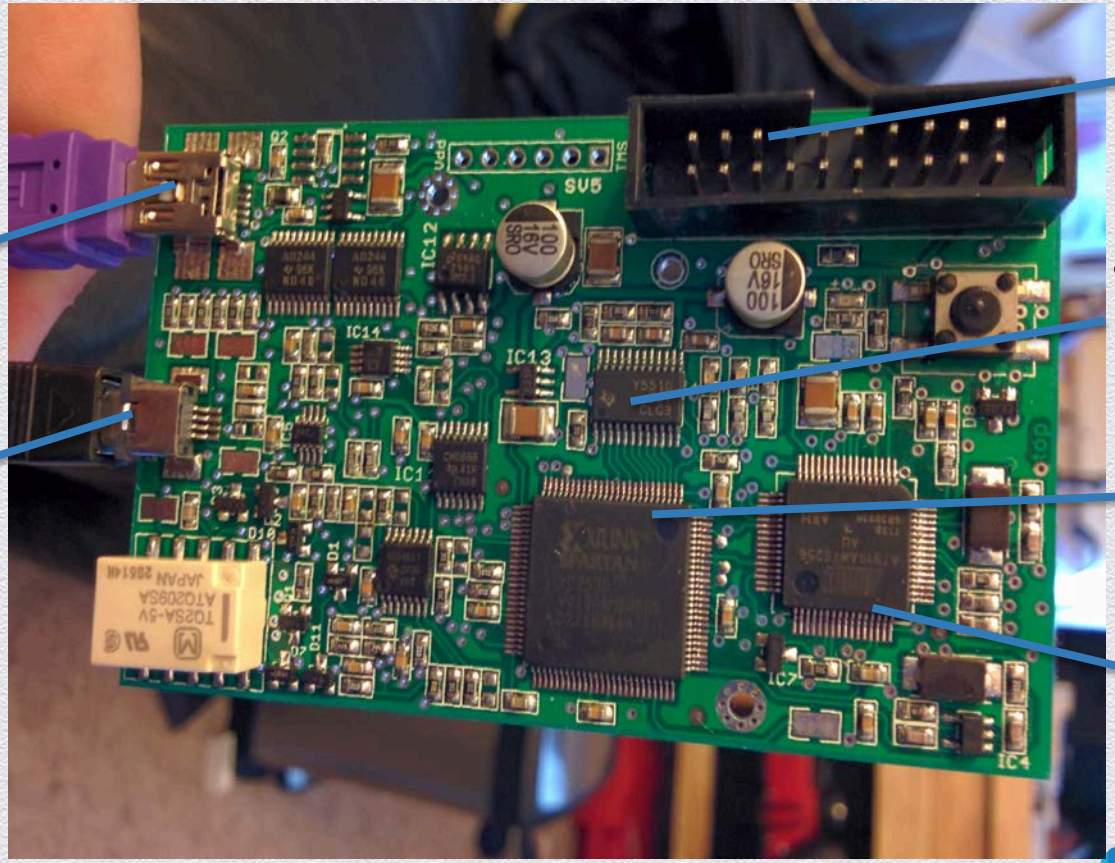
Proxmark3

- Developed in 2007 as a masters thesis project by Jonathan Westhues
- Designed to sniff, read, clone or emulate RFID cards; extensive support for numerous standards
- Device supported in Windows and Linux, originally command line interface however new point & click GUI recently released
- Uses FPGA to simulate card types



http://www.proxmark.org/proxmark

Proxmark3 Hardware



https://code.google.com/p/proxmark3/wiki/HardwareDescription

Proxmark3 Firmware

Bootrom

- Supports reflashing over USB
- Transfers execution to OS
- Safety in case OS is corrupted

FPGA

- Intermediate processing of RF signals
- Makes signals available for ARM

Operating System

- Communicates with client over USB
- Implements most of the Proxmark's functionality
- Most frequently updated

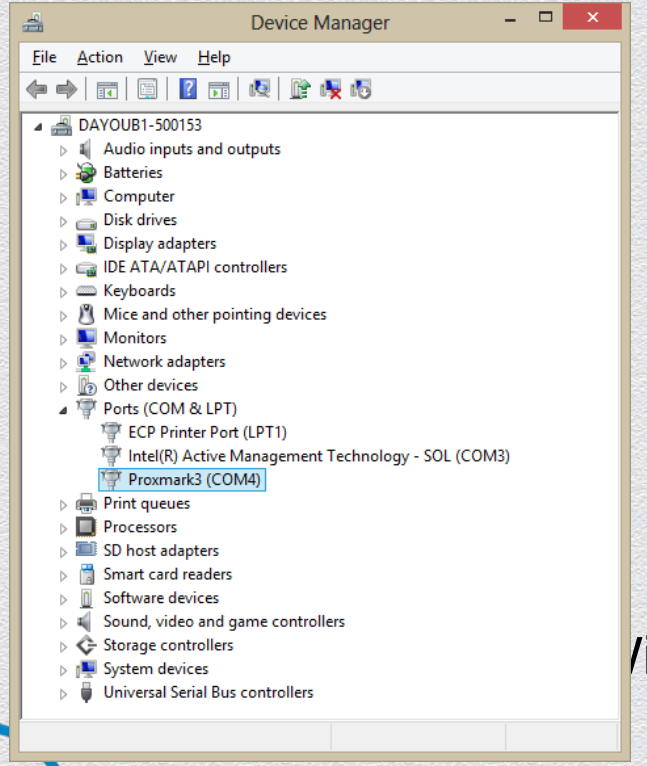
https://code.google.com/p/proxmark3/wiki/Compiling

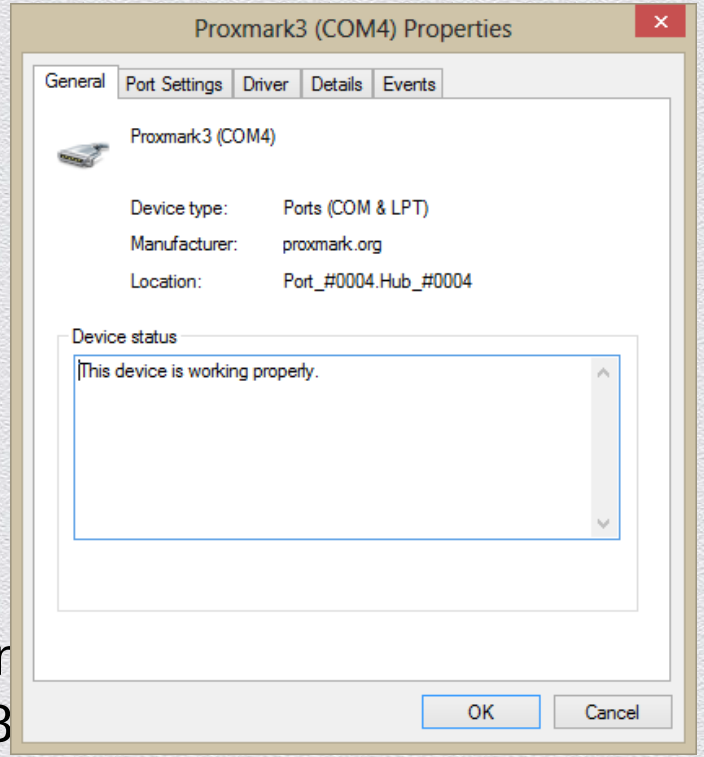
Proxmark3 Firmware Version

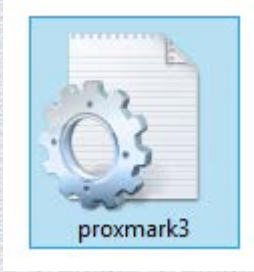
```
proxmark3> hw version
#db# Prox/RFID mark3 RFID instrument
#db# bootrom: svn 839 2013-12-05 07:11:23
#db# os: svn 839 2013-12-05 07:11:28
#db# FPGA image built on 2013/11/19 at 18:17:10
uC: AT91SAM7S256 Rev A
Embedded Processor: ARM7TDMI
Nonvolatile Program Memory Size: 256K bytes
Second Nonvolatile Program Memory Size: None
Internal SRAM Size: 256K bytes
Architecture Identifier: AT91SAM7Sxx Series
Nonvolatile Program Memory Type: Embedded Flash Memory
proxmark3>
```

Development is ongoing & has a very active community – the firmware version tested was less than 3 weeks old.

Proxmark3 Drivers

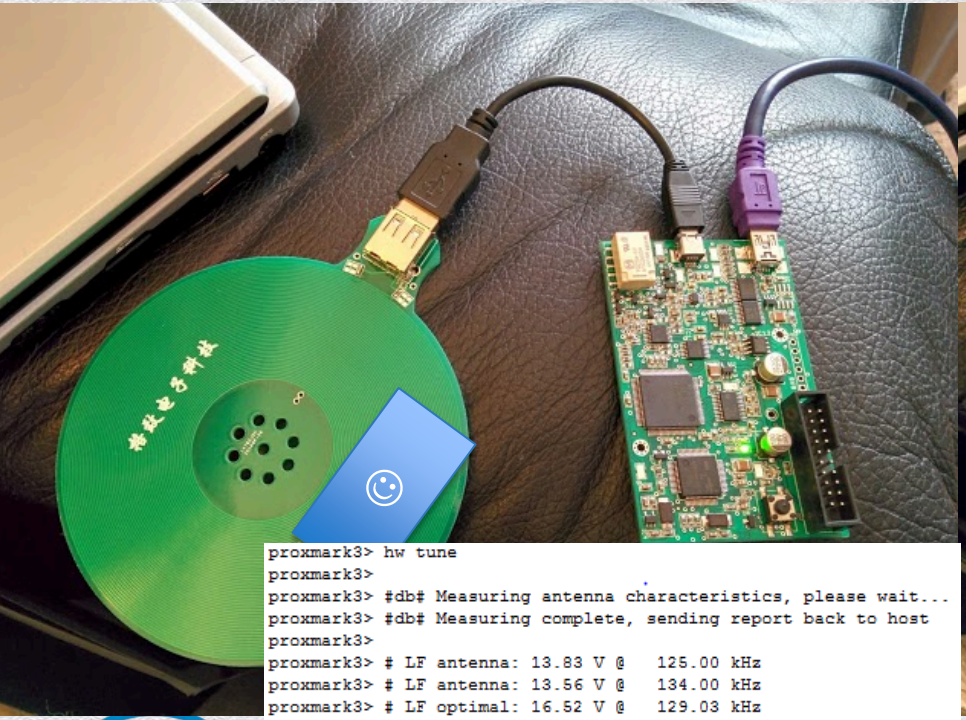




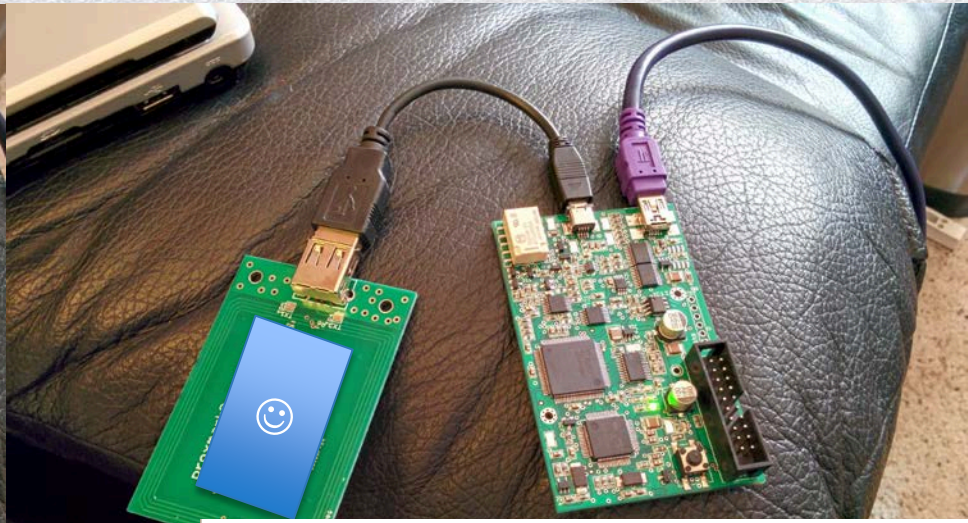


*Windows 8 not officially supported

Proxmark3 Antenna Types

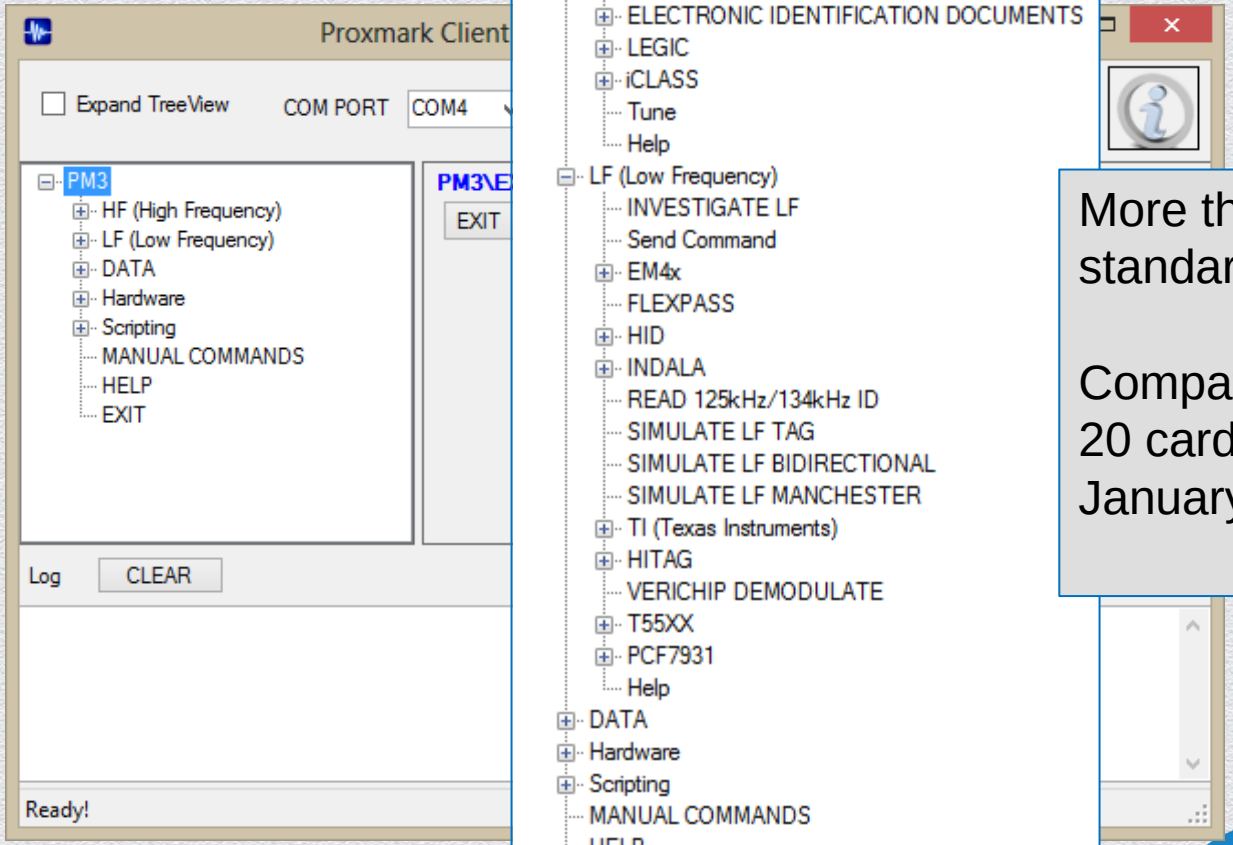


```
proxmark3> hw tune
proxmark3>
proxmark3> #db# Measuring antenna characteristics, please wait...
proxmark3> #db# Measuring complete, sending report back to host
proxmark3>
proxmark3> # LF antenna: 13.83 V @   125.00 kHz
proxmark3> # LF antenna: 13.56 V @   134.00 kHz
proxmark3> # LF optimal: 16.52 V @   129.03 kHz
proxmark3> # HF antenna:  0.23 V @    13.56 MHz
proxmark3> # Your HF antenna is unusable.
```



```
proxmark3> hw tune
proxmark3>
proxmark3> #db# Measuring antenna characteristics, please wait...
proxmark3> #db# Measuring complete, sending report back to host
proxmark3>
proxmark3> # LF antenna:  0.00 V @   125.00 kHz
proxmark3> # LF antenna:  0.00 V @   134.00 kHz
proxmark3> # LF optimal:  0.00 V @ 12000.00 kHz
proxmark3> # HF antenna: 10.67 V @    13.56 MHz
proxmark3> # Your LF antenna is unusable.
```

Proxmark3 Client GUI



- PM3
  - HF (High Frequency)
    - ISO14443A
    - ISO14443B
    - ISO15693
    - ELECTRONIC IDENTIFICATION DOCUMENTS
    - LEGIC
    - iCLASS
    - Tune
    - Help
  - LF (Low Frequency)
    - INVESTIGATE LF
    - Send Command
    - EM4x
    - FLEXPASS
    - HID
    - INDALA
    - READ 125kHz/134kHz ID
    - SIMULATE LF TAG
    - SIMULATE LF BIDIRECTIONAL
    - SIMULATE LF MANCHESTER
    - TI (Texas Instruments)
    - HITAG
    - VERICHIP DEMODULATE
    - T55XX
    - PCF7931
    - Help
  - DATA
  - Hardware
  - Scripting
  - MANUAL COMMANDS
  - HELP
  - EXIT

More than 15 different standards supported

Compatible with about 20 card types as of January 2014

Card Identification

Proxmark Client By El Gaucho De La Livida Palude

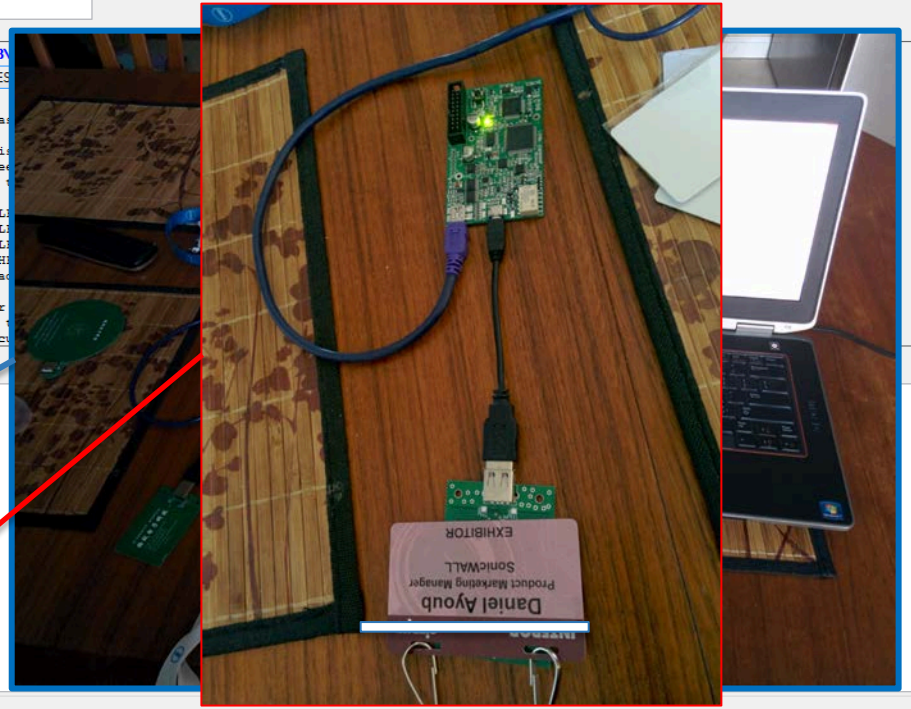
Expand TreeView COM PORT COM4 COMMAND TO SEND

- PM3
  - HF (High Frequency)
  - LF (Low Frequency)
  - DATA
  - Hardware
    - Detect Reader
    - FPGA Off
    - LCD
    - Read Flash Memory
    - Reset PM3
    - Drive LF antenna
    - Mux Settings
    - Tune
    - Version
    - Help
  - Scripting
  - MANUAL COMMANDS

Log CLEAR

```
proxmark3>
proxmark3> #db# Measuring antenna characteristics, please wait...
proxmark3> #db# Measuring complete, sending report back to host
proxmark3>
proxmark3> # LF antenna:  0.00 V @   125.00 kHz
proxmark3> # LF antenna:  0.00 V @   134.00 kHz
proxmark3> # LF optimal:  0.00 V @ 12000.00 kHz
proxmark3> # HF antenna: 10.83 V @    13.56 MHz
proxmark3> # Your LF antenna is unusable.
proxmark3> hw tune
proxmark3>
proxmark3> #db# Measuring antenna characteristics, please wait...
proxmark3> #db# Measuring complete, sending report back to host
proxmark3>
proxmark3> # LF antenna:  0.00 V @   125.00 kHz
proxmark3> # LF antenna:  0.00 V @   134.00 kHz
proxmark3> # LF optimal:  0.00 V @ 12000.00 kHz
proxmark3> # HF antenna:  6.77 V @    13.56 MHz
proxmark3> # Your LF antenna is unusable.
```

Ready!



Voltage drop indicated this is a HF card.

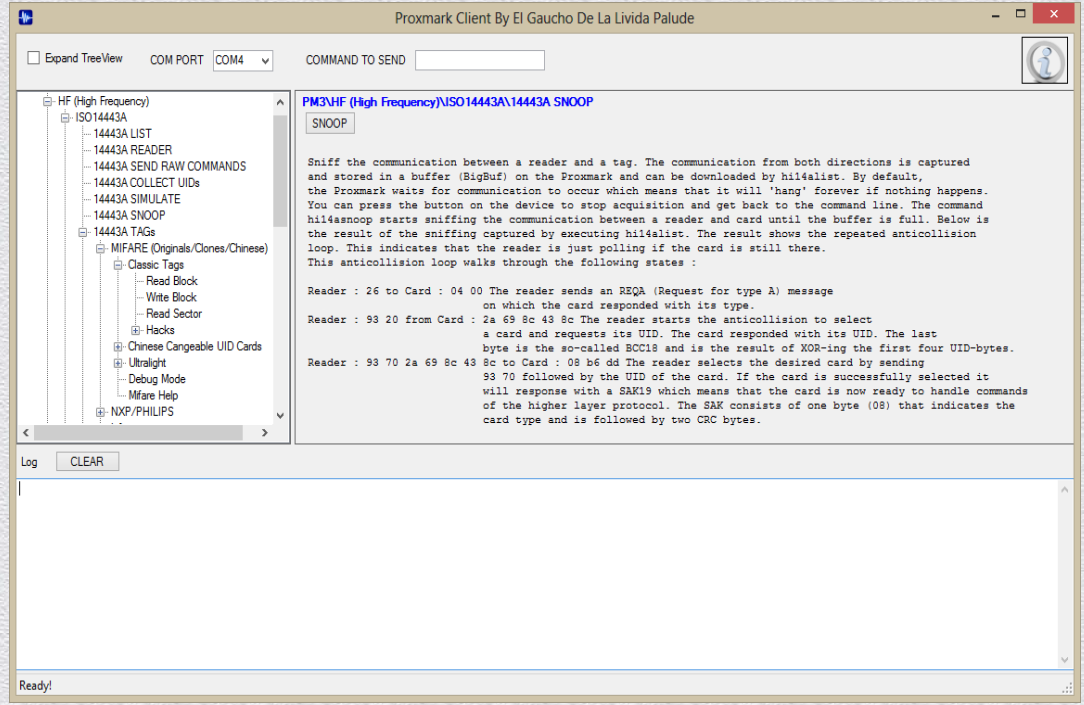
Next step it to try supported HF card ‘reader’ functions

Sometimes you know…

This manufacturer tell us exactly what kind of card it is. ☺

Snooping

- Objective is to observe interaction with a reader in order to capture enough data to derive the keys needed to encrypt communication
- Proxmark3 can also try to simulate a valid card in order to generate additional traffic
- Requires an attacker to get physically close to an entrance with his laptop (or android phone) and proxmark3
- Not all card types supported.

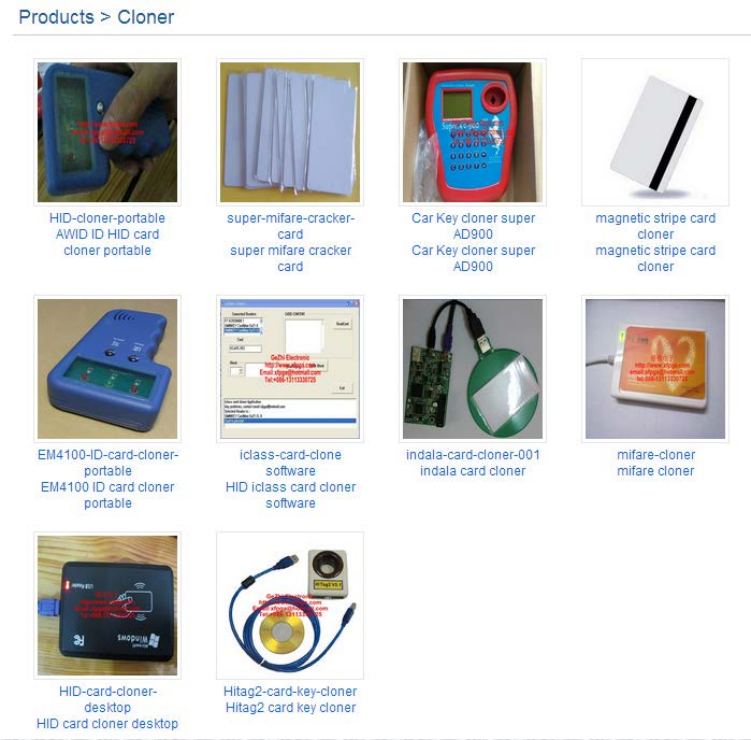


Simulating

- This is where the Proxmark3 shines.
- Not all card types can be simulated however many types can
- Functionality is very straight forward, can be used in situations where you do not even have the card
- Can also be used as part of a brute-force attack with a little scripting and imagination
- Proxmark3 supports some limited ‘stand-alone’ simulation modes that do not require a computer (can run on batteries)

Cloning

- Often requires specialized reader/writer equipment.
- Equipment is relatively cheap and easy to come by; software can also be purchased online to enable cloning for some cards.
- Proxmark3 capable of doing some card cloning but not all card types are supported, some vendors include master keys within their readers.
- There are several other RFID hacking devices in addition to PM3 available on the internet; many specialize in cloning



Putting it all together…

Proxmark Client By El Gaucho De La Livida Palude

Expand TreeView | COM PORT COM4 | COMMAND TO SEND

ISO15693
ELECTRONIC IDENTIFICATION DOCUMENTS
LEGIC
iCLASS
iCLASS List
iCLASS Snoop
iCLASS Simulate
iCLASS Reader
iCLASS Help
Tune
Help

PM3\HF (High Frequency)\iCLASS\iCLASS Snoop

SNOOP

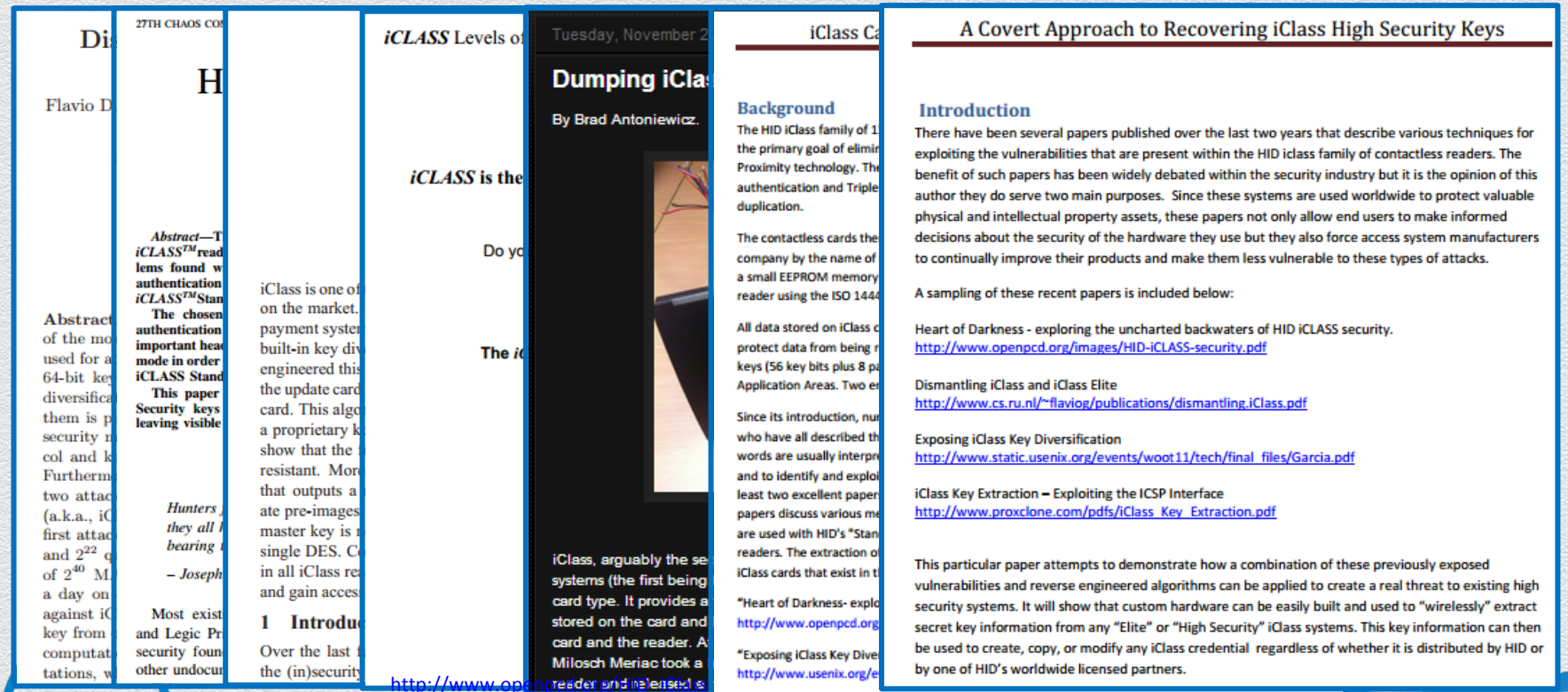
Log | CLEAR

```
proxmark3> hf iclass sim 0 [redacted]
--simtype:00 csn:[redacted]
proxmark3>
proxmark3> hf iclass snoop
proxmark3>
```

Ready!

This is a hobby. I don't have permission to proceed and I'd like to keep my job so this is where I stop.

Further iCLASS Attacks



http://www.openpcd.org/images/HID-iCLASS-security.pdf
http://www.cs.ru.nl/~flaviog/publications/dismantling.iClass.pdf
https://www.usenix.org/legacy/events/woot11/tech/final_files/Garcia.pdf
http://proxclone.com/pdfs/iClass_Cloner_rev0.pdf
http://blog.opensecurityresearch.com/2012/11/dumping-iclass-keys.html

MIFARE Attacks

- PM3
  - HF (High Frequency)
    - ISO14443A
    - ISO14443B
    - ISO15693
    - ELECTRONIC IDENTIFICATION DOCUMENTS
    - LEGIC
    - iCLASS
    - Tune
    - Help
  - LF (Low Frequency)
  - DATA
  - Hardware
  - Scripting
  - MANUAL COMMANDS
  - HELP
  - EXIT

- PM3
  - HF (High Frequency)
    - ISO14443A
      - 14443A LIST
      - 14443A READER
      - 14443A SEND RAW COMMANDS
      - 14443A COLLECT UIDs
      - 14443A SIMULATE
      - 14443A SNOOP
      - 14443A TAGs
        - MIFARE (Originals/Clones/Chinese)
          - Classic Tags
            - Read Block
            - Write Block
            - Read Sector
            - Hacks
          - Chinese Cangeable UID Cards
            - Write UID
            - Read Block
            - Write Block
            - Read Sector
            - Load Dump
            - Save Dump
            - Restore Corrupted Sector0Block0
          - Ultralight
            - Read Block
            - Write Block
            - Read Card
          - Debug Mode
          - Mifare Help
        - NXP/PHILIPS
          - NTAG203
        - Infineon
          - my-d move
      - 14443A Help

- 14443A TAGs
  - MIFARE (Originals/Clones/Chinese)
    - Classic Tags
      - Read Block
      - Write Block
      - Read Sector
      - Hacks
        - Test Block Keys
        - DARKSIDE ATTACK
        - NESTED ATTACK
        - SCRIPT - Automatic Mifare Crack
        - Dump Mifare Classic
        - Restore Mifare Classic
        - Sniff
      - SIMULATOR
        - Simulate
        - Clear Simulator
        - Get Memory Block
        - Set Memory Block
        - SCRIPT - Convert dumpdata.bin to .eml
        - Load (.eml)
        - Save To File (.eml)
        - Fill Simulator Memory
        - Print Keys

Detailed white papers are available to explain attack methodologies.

Threat Assessment

- Proxmark3 is a development platform capable of running customizable software, a skilled programmer could develop support for almost any RFID card type
- The amount of research that has been done in this field is overwhelming, breaking modern RFID systems is not ‘point and click’ but it can be done
- Most card types have already been broken or can be if someone writes the code
- Motivated attacker could use the proxmark3 to do a lot of damage
- Overall threat should be considered ‘medium-high’

감사합니다 Natick

Grazie Danke Ευχαριστίες Dalu Obrigado

Thank You Köszönöm

Tack

Спасибо Dank Gracias

谢谢 Merci Seé ありがとう