UNLOCKING SECRETS OF PROXMARK3 RDV4.0

By Christian Herrmann (iceman)
TALK SUMMARY

- About us
- What is a Proxmark3?
- Presentations
- Previous generations
- Addressing these limitations
- Usage examples
- Q/A
Iceman

- RFID/NFC researcher
- Proxmark3 forum Administrator
- Maintainer of popular iceman forks
- Software priest at RRG
- Certified MCPD enterprise architect
Radio Frequency IDentification

...remember this...
PROXMARK3

First developed by Jonathan Westhues 2006.

Often referred to as the Swiss army knife of RFID research.

RFID security research tool for 125 kHz LF, 13.56 MHz HF and now also contact.

A versatile tool for RFID security research. It can be used to analyse and reverse engineer RF protocols deployed in billions of cards, tags, fobs, phones and keys.

The Proxmark3 operates in three modes. Sniffing mode, Card emulation Mode and Reader mode.
Previous work presented

Fran Brown at Blackhat 2013 - RFID hacking; Live free or RFID hard
https://www.youtube.com/watch?v=pNCeN1tZbAl

Craig Young at DEFCON 23 - Train your rfid RFID hacking tools
https://www.youtube.com/watch?v=kVMAqiJlQkI

Dennis Maldonado at DEFCON 25 - Real time RFID Cloning in the field
https://www.youtube.com/watch?v=kUduHlygbY8

Kevin Barker, Christian Herrmann at BlackAlps ’18 ..
https://www.youtube.com/watch?v=BBRE-bnNDKQ
Recent high profile practical applications

**Tesla model S key fob cloning.**
- Team of researchers at the KU Leuven university
  - Vehicle entry system has been upgraded since to mitigate this type of attack.
  - Proxmark3 RDV2 used, custom FPGA / ARM code used

**Assa Abloy’s VingCard vulnerability (Ghosts in the locks)**
F-Secure by Tomi Tuominen and Timo Hirvonen
- 140 millions door locks affected
- Later generation hardware installed.
- Proxmark3 RDV2 used, custom standalone mode
Previous generations

Lack of interface options.
Poor quality control.
Bulky - Large PCB’s & even larger antennas.
Clunky - Often requires weird leads / plugs.
Underwhelming RF performance.
Unreliable hardware revisions.
Partial solution.
Not suitable for covert operation.
Building a platform...

We wanted to build a hardware platform upon easy modifications could be added meanwhile still be backwards compatible with source code.

Not an super easy task...

Luckily we have a hardware design genius called Proxgrind
Addressing these limitations

Sexy!

Flexible RF interface.

LF / HF range improvements. 68% more power.

2Mbit flash memory.

7816 interface.

40% smaller form factor - Making it covert.

FPC for active antenna, UART and battery options

PVC Case.
Flexible RF interface

New mechanical design allows for easy antenna customisation.
2 Mbit Flash memory

Onboard SPI Flash memory
4 x 64Kb pages divided in to 16 x 4Kb sectors

- Offline simulation
- Offline dictionary
- Storage

New commands
- hf mf fchk m
- mem load m default_keys
- If t55xx deviceconfig
CONTACT ANALYSIS

ISO-7816 Contact analysis

With the new sc / emv commands, we can now do both contact and contactless analysis within the Proxmark3 client.

The following group of commands has now been adapted to take advantage of both interfaces.

New commands
- sc
- emv
CONTACT ANALYSIS

ISO-7816 Contact analysis

- Analyse chip & pin card
- SIM slot hidden under casing
- New commands

Full size extension adaptor
CONTACT ANALYSIS

SC commands

- sc info
- sc raw
  - r - skip response
  - a - active select
  - t - decode TLV

--- Smartcard Information -------

ISO768183 ATR : 3B 65 00 00 20 63 CB B7 20
look up ATR
pm3 --> sc raw d 00a404000e315041592e5359532e444446303100
received 3 bytes
A4 61 22
received 3 bytes
C0 6F 20 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 90 00
pm3 -->
CONTACT ANALYSIS

EMV commands

[usb] pm3 --> env
help          This help
exec          Executes PPSE. It selects 2PAY.SYS.DDF01 or 1PAY.SYS.DDF01 directory.
pse           Try to select all applets from applets list and print installed applets.
search        Select applet.
gpo           Execute GetProcessingOptions.
readrec       Read files from card.
genac         Generate ApplicationCryptogram.
challenge      Generate challenge.
intauth        Internal authentication.
scan           Scan EMV card and save it contents to json file for emulator.
test          Crypto logic test.
list           List ISO7816 history
roca           Extract public keys and run ROCA test
Bluetooth / Battery addon

Bluetooth over FPC
- HC-06 BT
- USART serial over BT
- 115200 baudrate

Battery
- 400 mHa LIPO
- 1h runtime HF
- 2h runtime LF

Full client support
- Adapted firmware / client to switch between USB or FPC

What’s missing?
Android / iPhone app of course.
Source code / ARM

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

FPGA
- Intermediate processing of RF signals
- Makes signals available to ARM

Operating System
- Communicates with client over USB
- Implements most of the Proxmark’s functionality
- Most frequently updated
Source code / Client

The Proxmark3 client is a strange place.

Like old school terminal window you find commands with subcommands groups.

pm3-> hf mf nested

But that would be too easy, so sometimes is one level, two, three levels.

Not to forget the parameters.

We have without hyphen, with hyphen and long params. All mixed up.

pm3 ->hf mf nested h
pm3->script run mifare_autopwn -h
pm3->emv select --help
Source code / transfers

Transfers between device and client is the old Usbcommand packages

544 bytes of size.
  - 3 u64 vars
  - 1 u8 byte[512]

Not good for Bluetooth slow transfers

Solution?

The NG command format. It has a variable length upto 512 bytes of data.

Read more:

Some four years ago @Holiman decided to add LUA script functionality into the Proxmark3 client.

/gl/client/lualibs
/gl/client/scripts

Glued into client with
/gl/client/scripting.c

/gl3->script run emul2dump -h

/gl3-> script list
14araw.lua
Legic_clone.lua
amiibo.lua
brutesim.lua
calc_di.lua
calc_ev1_it.lua
Calc_mizip.lua
calypso.lua
didump.lua
dumptoemul-mfu.lua
dumptoemul.lua
e.lua
emul2dump.lua
emul2html.lua
Full client vs Standalone

Proxmark3 has a lot of functionality implemented on the ARM side. However the MCU is too weak and too little memory available so all interesting attacks is implemented on client side.

This leads to the strange notion of how to replace the client. Short answer, you can... but... you need to reimplement all attacks/logic/fixes as it goes.

This means the standalone functions can only use what already is in ARM. The limits is already breaking the 256 Kb and entering the 512 Kb realm.

Solution?

- skip that and go for the full client support over BT :)
- Add a raspberry pie to control
- Use Android phone
Workshop tomorrow..

It will be a practical hands on experience.

You be playing with RDV4 and Blue shark

And learn how to make a standalone mode..
CONTACT ME

www.rfidresearchgroup.com

chris@rfidresearchgroup.com
More info

- www.proxmark.org/forum/index.php
- github.com/rfidresearchgroup/proxmark3
- github.com/proxmark/proxmark3
- www.proxmark.org/files/
Thank you!

Special thanks to Willok, Sentinel, Colin, Doegox & the proxmark community!

Thanks to proxgrind, dot.com, 0xFFFF