Sort of an adrenaline junkie
Outdoor day drinker
Romantically available
Hacker
Our Target
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
Previous Work

Pong on payment terminals$^1$
Previous Work

Tamper resistant bypasses and EMV protocol exploits$^2$
Previous Work

2015 Survey of POS attacks (90% use default PIN)
Previous Work

Breaches
Knee-Deep in the Dead
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
Warranty Voided!
Administrator Mode

Press 1 + 5 + 9

Enter pin

Massively increased attack surface!
### Diagnostic Info!

#### NAND FLASH

<table>
<thead>
<tr>
<th></th>
<th>MEGABYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>190.84</td>
</tr>
<tr>
<td>Used</td>
<td>23.10</td>
</tr>
<tr>
<td>Free</td>
<td>167.74</td>
</tr>
</tbody>
</table>

#### SDRAM

<table>
<thead>
<tr>
<th></th>
<th>MEGABYTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>104.32</td>
</tr>
<tr>
<td>Used</td>
<td>29.91</td>
</tr>
<tr>
<td>Free</td>
<td>74.40</td>
</tr>
</tbody>
</table>
Install Software Updates!
Software Update

Manual Interaction required unless using PAYware :(  

Updates must be signed prior to installation
Load Encryption Keys!
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>yes</td>
</tr>
<tr>
<td>Speed/Duplex</td>
<td>Auto</td>
</tr>
<tr>
<td>Mode</td>
<td>StaticIP</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.42.0.19</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.42.0.1</td>
</tr>
<tr>
<td>DNS1</td>
<td>10.42.0.1</td>
</tr>
<tr>
<td>DNS2</td>
<td></td>
</tr>
</tbody>
</table>

Manage Config Settings!
MOAR Config Settings!
File Manager!

Path: /proc/self

<table>
<thead>
<tr>
<th>Directory</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>auxv</td>
<td></td>
</tr>
<tr>
<td>cmdline</td>
<td></td>
</tr>
<tr>
<td>coredump_filter</td>
<td></td>
</tr>
<tr>
<td>cwd</td>
<td></td>
</tr>
<tr>
<td>environ</td>
<td></td>
</tr>
<tr>
<td>exe</td>
<td></td>
</tr>
<tr>
<td>fd</td>
<td></td>
</tr>
<tr>
<td>fdinfo</td>
<td></td>
</tr>
<tr>
<td>latency</td>
<td></td>
</tr>
<tr>
<td>limits</td>
<td></td>
</tr>
<tr>
<td>maps</td>
<td></td>
</tr>
<tr>
<td>mem</td>
<td></td>
</tr>
<tr>
<td>mountinfo</td>
<td></td>
</tr>
</tbody>
</table>
Exploit!!!
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
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
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!!
grrrrrrrrrrrrrrrrrsec

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...
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\textsuperscript{4}, RF\textsuperscript{5}, LED modulation\textsuperscript{6})
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
GREETZ!

Fareed Khattak

Mike Weber

Dean Jerkovich

samuslav

Richo

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

4.) 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