WiMAX Hacking 2010

Pierce, Goldy, and aSmig
feat. sanitybit

DEFCON 18

Updated slides, code, and discussion at
https://groups.google.com/group/wimax-hacking

The Technology

- WiMAX: a broadband wireless Internet technology
- 802.16, similar to 802.11 (IEEE control)
- Competing with LTE
- Large network being deployed by Clearwire

Network Deployment

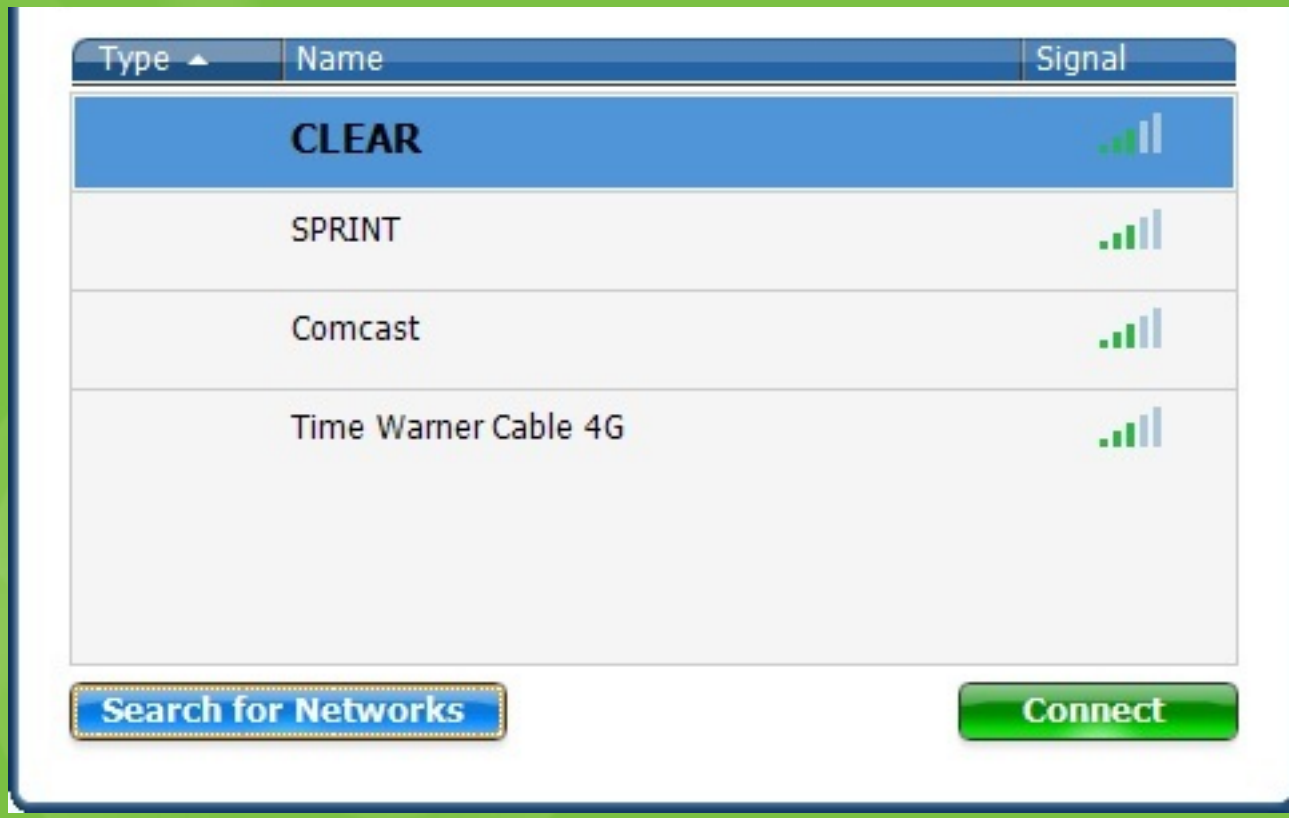
- Clear has the most widely deployed WiMAX network in the US, as such, it is the focus of our research efforts
- Currently deployed in 79 markets across 21 states
- An additional 22 markets are expected to be deployed in the next 3 months, including:

New York, NY	Denver, CO	Nashville, TN
Los Angeles, CA	Boston, MA	Minneapolis, MN
San Francisco, CA	Miami, FL	Philadelphia, PA

- Coverage planned for most major US cities by 2012
- Operates on frequencies in the 2.5-2.6 GHz range

Other Services using Clear's Network

- Time Warner Cable
  - Roadrunner Mobile
- Comcast
  - High-speed 2 go
- Sprint Nextel
  - 4G Service
  - HTC EVO



All of these services are placed onto the same physical network infrastructure, with small differences in provider portal pages

Official Clear coverage map taken from clear.com/coverage

Green = Current Market

Grey = Future Market (map does not show all of them)

Captive Portal Bypass

Last years vulnerability:

- OpenVPN over UDP/53

Their fix:

- Block large UDP/53 packets

Counter fix:

- OpenVPN over UDP/53, fragmented packets (1024 bytes)

OpenVPN Options to add:

tun-mtu 1500
mssfix 1024

Example OpenVPN Config

client
dev tun
proto udp
remote vpn.server.com 53
tun-mtu 1500
mssfix 1024
resolv-retry infinite
nobind
persist-tun
tls-client
ca ca.crt
cert vpn.server.com.crt
key client.key
dh dh2048.pem
keepalive 20 200
cipher BF-CBC
cipher AES-256-CBC
tls-remote vpngate
ns-cert-type server
route-delay 2
redirect-gateway def1
.....

Echo Peak Hardware & Software

- WiMAX gear from Intel
- www.linuxwimax.org
- 5150, 5350 are best supported
- Buy on eBay ($80)
- Get a USB-PCIe cradle ($40)
- PCIe cards **might** work in **some** thinkpads

Home Device Hard Hacks

CPEi25150

CPEi25750

Got root?

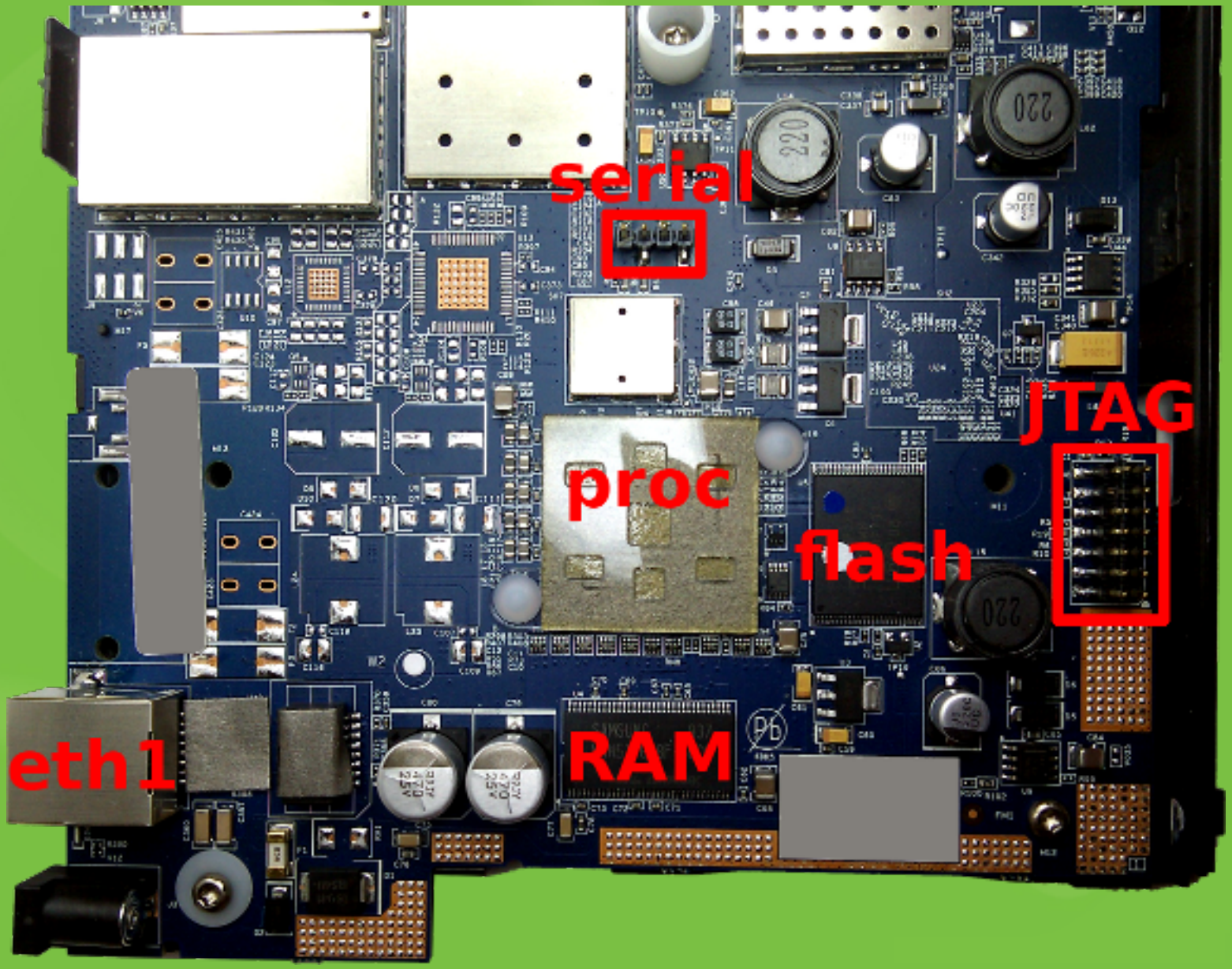
Home Device Specs

Motorola CPE 150/750

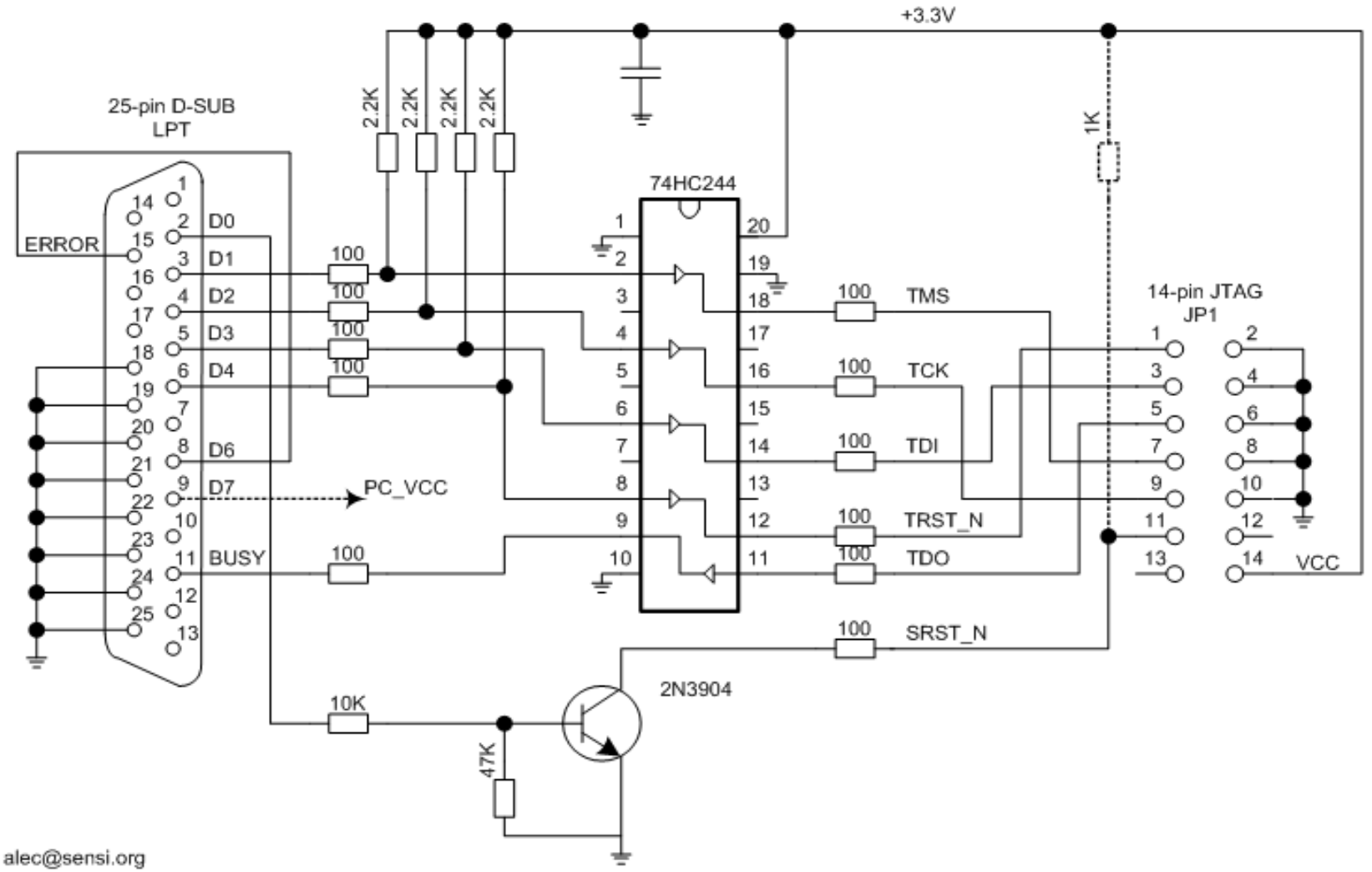
- 64MiB RAM
- 32MiB flash
- Beceem 802.16
- Texas Instruments TNETV1061
  - 213 MHz
  - MIPS32 4KEc
  - Chip debugging via EJTAG
  - Linux

Logic Probe

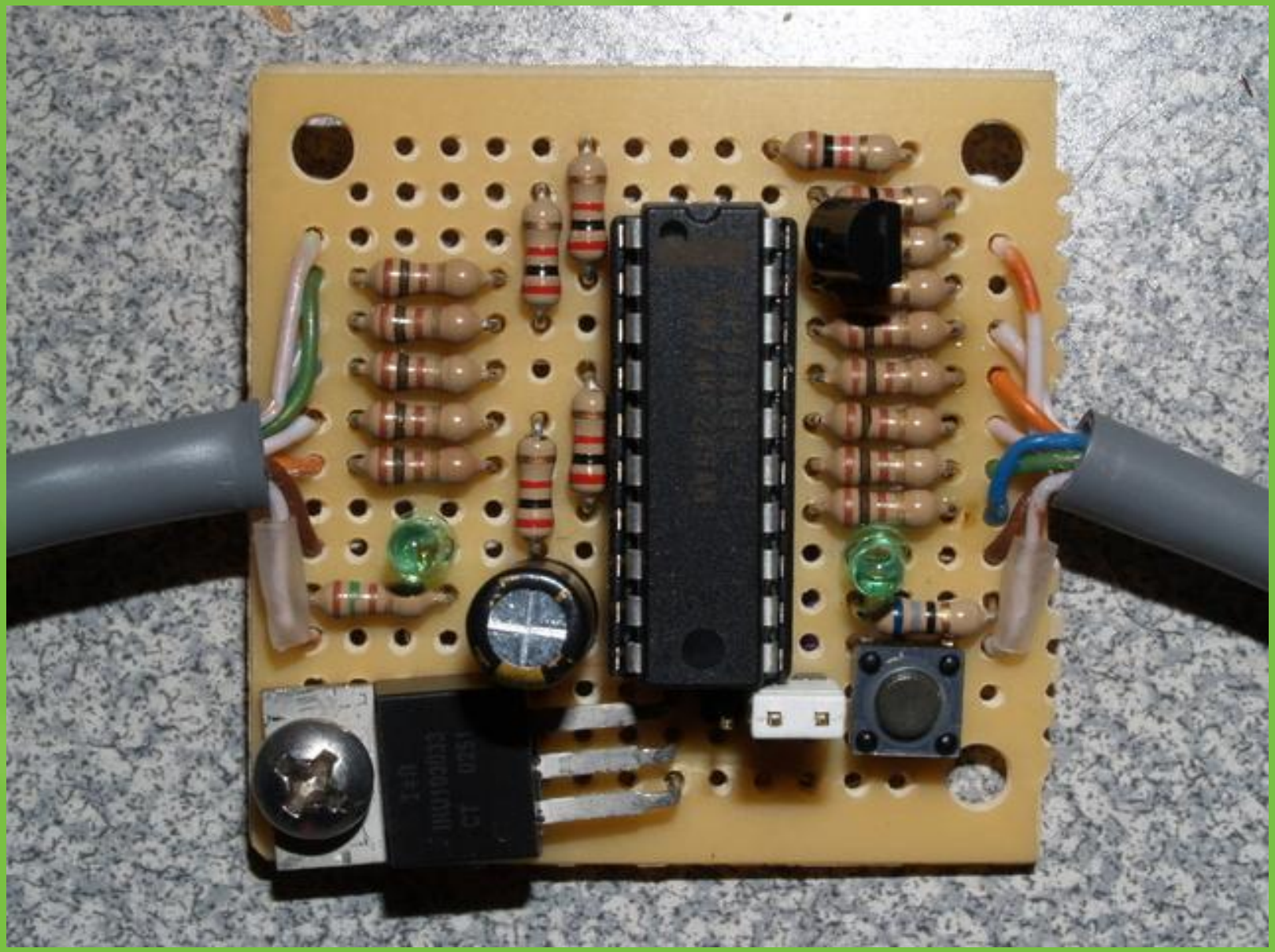
The magic wand of hardware hacking



CPE 150 (CPEi25150)



http://bit.ly/bqEBND



aSmig's first JTAG interface

B0011620: .....C.....TOOLS_USER.0.BOO
B0011640: TLOADER.0x90000000,0x90020000.IM
B0011660: AGE_A.0x90040000,0x90C40000.CONF
B0011680: IG_A.0x90C40000,0x90C60000.CONFI
B00116A0: G_B.0x90C60000,0x90C80000.IMAGE_
B00116C0: B.0x90CE0000,0x918E0000.FNE_CERT
B00116E0: S.0x90C80000,0x90CA0000.DEV_CERT
B0011700: S.0x90CA0000,0x90CC0000.FACTORY_
B0011720: DEF.0x90CC0000,0x90CE0000.JFFS2.
B0011740: 0x918E0000,0x92000000.RESET_CAUS
B0011760: E.0.PartNumber.SGDN5313AA.Produc
B0011780: tID.CPEi25725.HWRevision.REV.D.S
B00117A0: erialNumber.TS199X0YKY.HWA_1.00:
B00117C0: 23:EE:**:**:**.GATEWAY_MAC_ADDRE
B00117E0: SS.00:23:EE:**:**:**.FingerPrint
B0011800: .63F7FED52*****EB2E76B7F35B*****
B0011820: E1EC*****.HWA_0.00:24:A0:**:**:*
B0011840: *.FactoryProvision.Complete.CONS
B0011860: OLE_STATE.locked.....

Double-Take

B0011840: 5.FactoryProvision.Complete.CONS
B0011860: OLE_STATE.locked.....

Road map - Thanks bootloader!

BOOTLOADER	0x90000000	0x90020000
BootLoader Config	0x90020000	0x90040000
IMAGE_A	0x90040000	0x90C40000
CONFIG_A	0x90C40000	0x90C60000
CONFIG_B	0x90C60000	0x90C80000
FNE_CERTS	0x90C80000	0x90CA0000
DEV_CERTS	0x90CA0000	0x90CC0000
FACTORY_DEF	0x90CC0000	0x90CE0000
IMAGE_B	0x90CE0000	0x918E0000
JFFS2	0x918E0000	0x92000000

So what about the root?

Yeah, yeah.

/usr/bin/bd_chk

$ strings usr/bin/bd_chk
/lib/ld-uClibc.so.0
...
_end
/pstore/dbg_tools/bd_open2
CONSOLE_STATE
unlocked
Lock Serial Console
echo "unsetpermenv CONSOLE_STATE" > /proc/ticfg/env;
echo "setpermenv CONSOLE_STATE locked" > /proc/ticfg/env
CONSOLE_STATE not found

/pstore/dbg_tools/bd_open2

Magical debug tools file!

- CONSOLE_STATE is left alone
- file is executed on every boot!
  - change your passwords
  - re-crypt your keys
  - adjust your firewall
  - kill SNMPd

Shell Fun

ssh Admin@192.168.15.1 (Pass: Tools)

dbgcli> shell

BusyBox v0.61.pre (2009.09.14-12:29+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

export PATH=/bin:/sbin:/usr/bin:/usr/sbin

Now you can use tab complete for a list of system binaries.

There is too much information to cover here, but some highlights include access to iptables and the dbg/cpe cli tools.

Home Device Auth Bypass

There is a hidden administrative account on the home CPE device. We can use it to bypass the login on the web interface if the user changed the default.

login%3Acommand%2Fusername	router
login%3Acommand%2Fpassword	motorola

->

login%3Acommand%2Fusername	Admin
login%3Acommand%2Fpassword	Tools

Clear Mobile

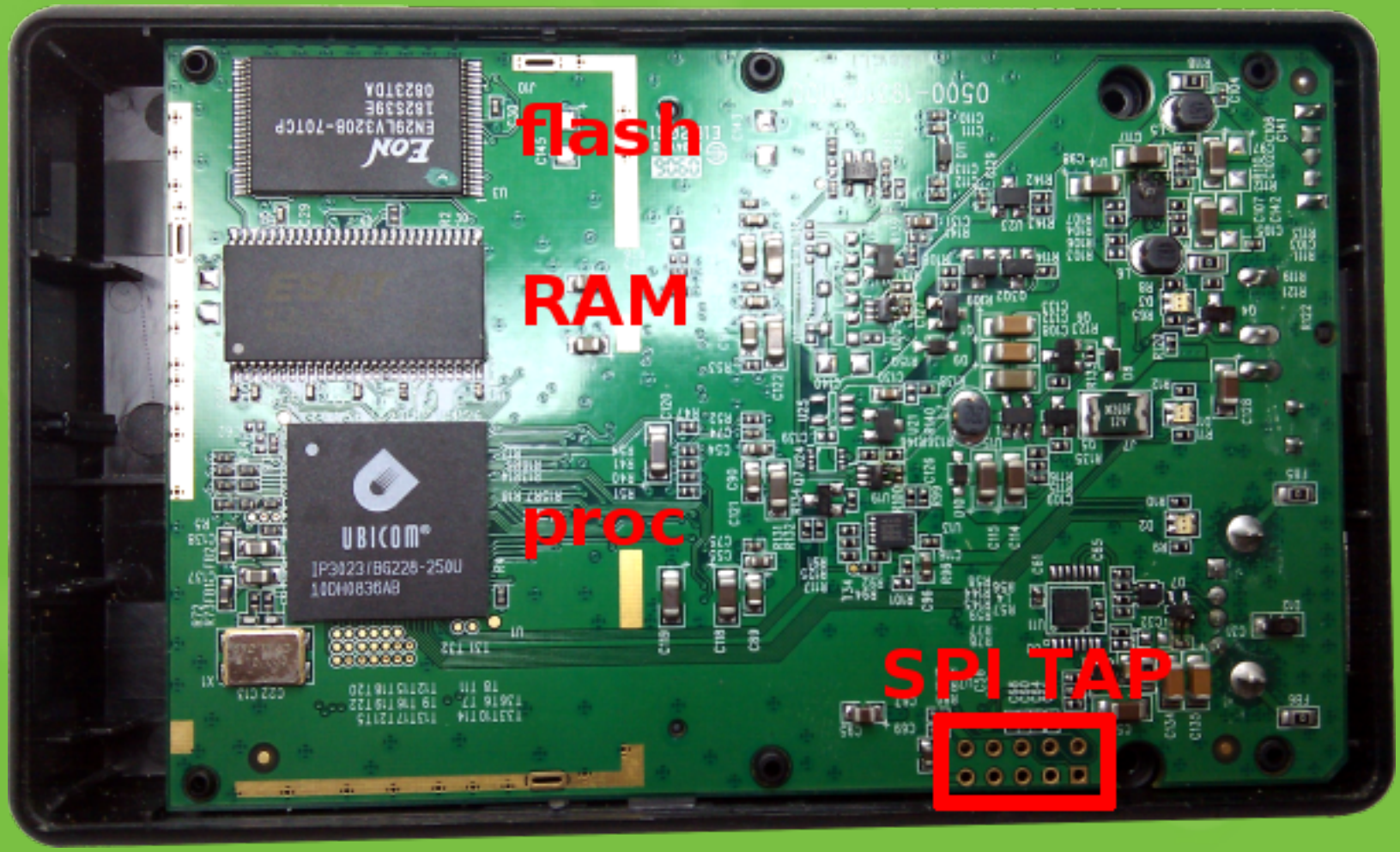
- Mobile 4g
- Mobile 3g/4g
  - sprint
- Clearspot
  - password is last three bytes in mac address

Clear Mobile Hard Hacks

Clear Spot

- 16MiB RAM
- 4MiB flash
- Mini PCI w/ Atheros WiFi card
- Ubicom IP3023 - MASI 250MHz
  - **M**ultithreaded **A**rchitecture for **S**oftware **I**/O
  - Chip debugging via proprietary SPI (not JTAG)
  - Proprietary instruction set
  - NOT Linux

Clear Spot



CradlePoint PHS300

It's only a 48 pin TSOP

SB5120 is good for something after all

- MIPS32
- EJTAG
- TTL UART

Clear "Stick" (USB Modem)

Mod and photo by Loki

HTC EVO

- sequans
- getprop/setprop
- Diagnostic apks
- WiMAX tether
- deactivated evo
- 2.1 (fresh or damage control)
- 2.2 cyanogen (toastcfh and maejrep)

Location Based Services

Service Types:

- Client/Server (AJAX) - "Where am I?"
  - http://developer.clear.com/ClearLocationDemo.html
- Server/Server (Parlay X) - "Where are they?"
  - x.509 cert & key required

Interfaces

- AJAX
  - Web browser friendly, uses Google Maps
- Parlay X
  - Uses SOAP specification, POSTed in XML format
  - Query by IP, MAC (phone number or e-mail)

Location Based Services (Parlay X)

Currently

- Location / Range are determined by tower and antenna

Current Accuracy: Predefined ranges (in meters)

- 160, 241, 321, 402, 482, 563, 643, 724, 804, 885, 965, 1126, 1448

Down the road

- Multiple towers used to increase accuracy of location and range
- No known ETA

Privacy Problems with LBS

- **Opt-IN is the DEFAULT**
  - Customer's have no option to Opt-OUT online
  - Registered and Unregistered devices are traceable
- **Who's Affected?**
  - **EVERYONE** that uses WiMAX
    - Clear, Sprint, Comcast, Time Warner, etc
- **How to Opt-OUT**
  - Contact the Engineering Department to have it disabled
  - This prevent's both AJAX and Parlay X queries
- **Random dead spots**

The Future

- Open source firmware
- OpenWRT on a home device
- 802.16m provides 100 Mbit/s mobile & 1 Gbit/s fixed
- Better privacy?

Mad Gr33tz
SophSec, Janus Privacy Solutions, Aardvark, Snoop Security, Lookout, xda-developers, theorie, rumple, tokiestar, iviatticus, i0n, osirisx11, caboose, and busticati everywhere.

Clearwire and Sprint Technical Development Resources
http://2md.hosted.panopto.com/CourseCast/Viewer/Default.aspx?id=1cd37bbb-d822-4637-bf18-2a254282e688

WiMAX Hacking Group
https://groups.google.com/group/wimax-hacking

AJAX LBS Demo
http://developer.clear.com/ClearLocationDemo.html

The insecurity is CLEAR