Hacking Satellite TV receivers : Are those IoT devices secure ?

Sofiane Talmat
Security Consultant
IOActive®

Agenda

Introduction

Many things going wrong

Thank you

Why Satellite TV receivers ?

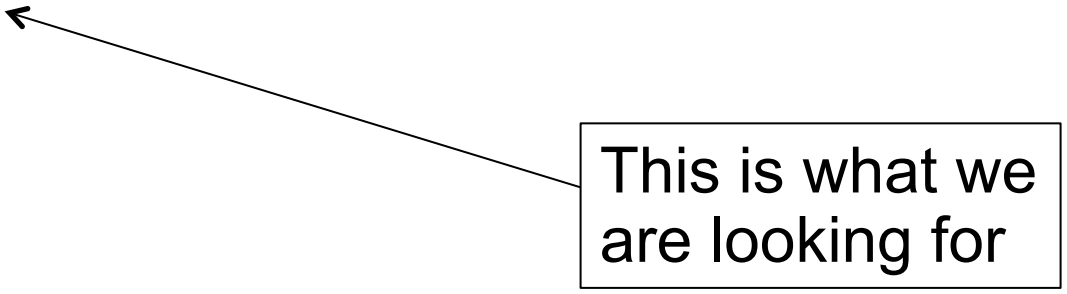
What is this all about ?

TV encryption scheme

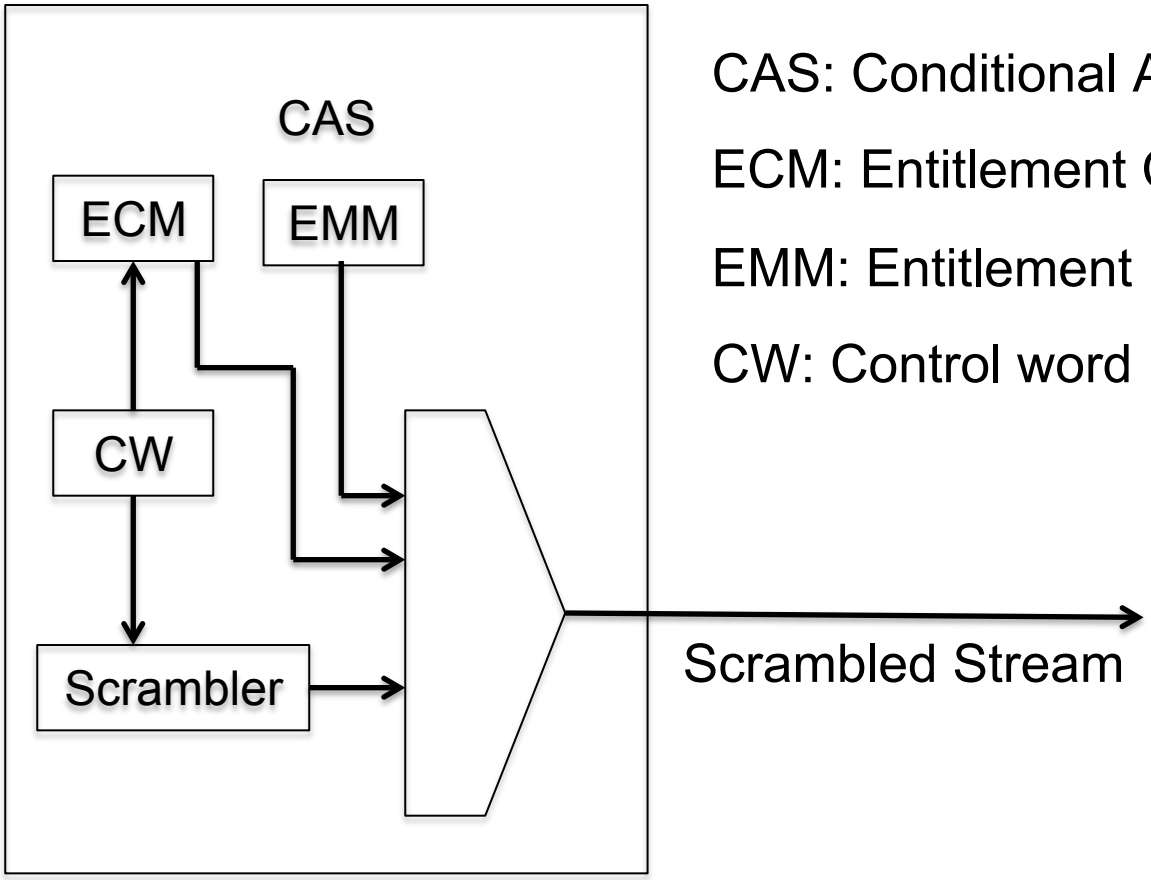
ECM : Entitlement Control Message

EMM : Entitlement Management Message

CW : Content encryption key



Scrambling



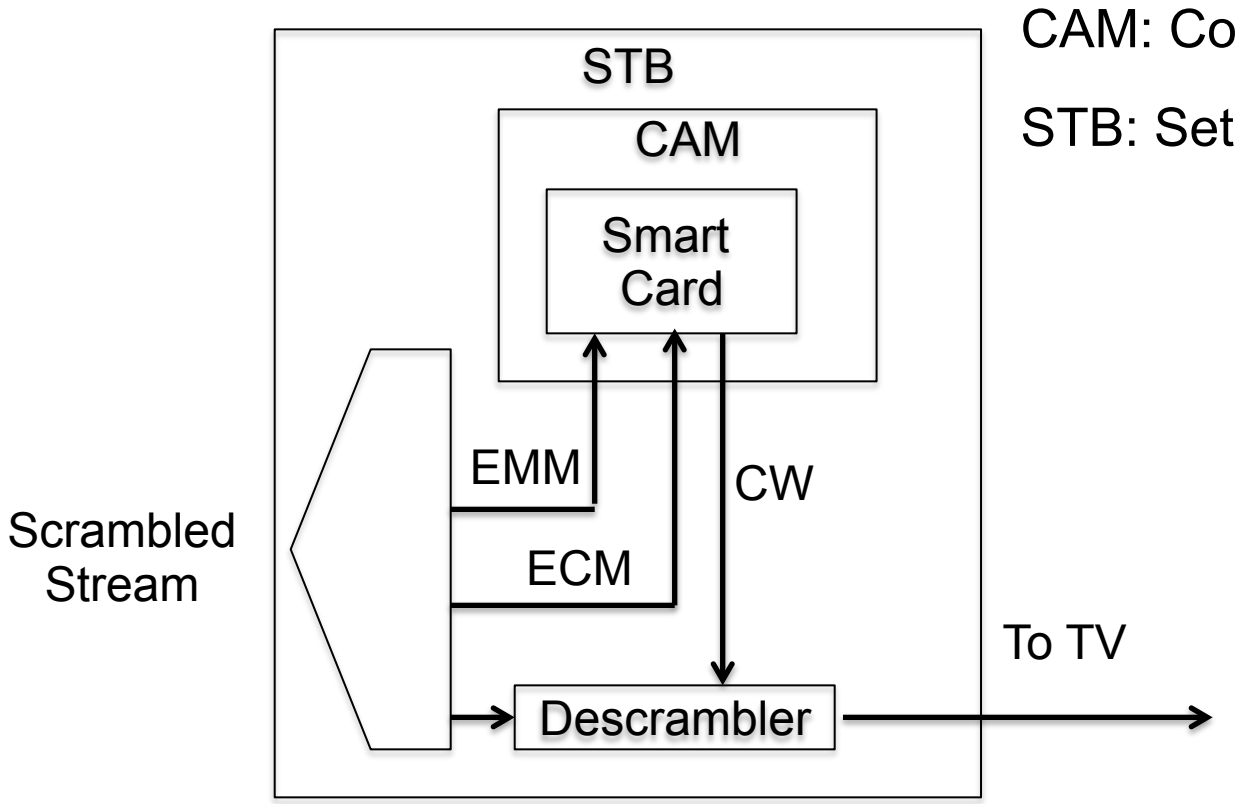
CAS: Conditional Access System

ECM: Entitlement Control Message

EMM: Entitlement Management Message

CW: Control word

Descrambling



CAM: Conditional Access Module

STB: Set Top Box

What made the difference ?

We used to have :

- Proprietary STBs
- One service provider per STB

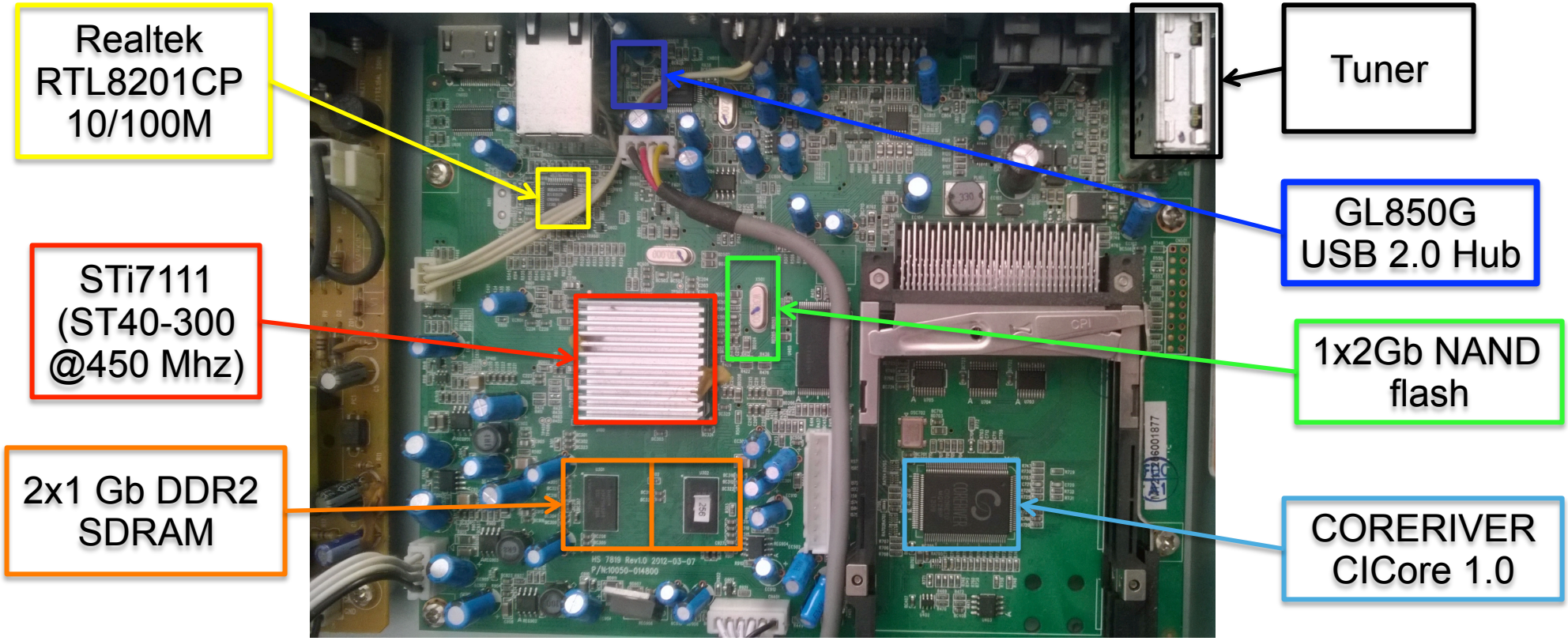
We now have :

- Open STBs
- Fully featured Linux boxes

Case study : Forever Nano Pro

Better than my graduation computer

Forever Nano pro : ~150 USD



Recap

STi7111 processor (St40 CPU @450Mhz)

ROM=256MB

RAM= 256MB

10/100M Ethernet port

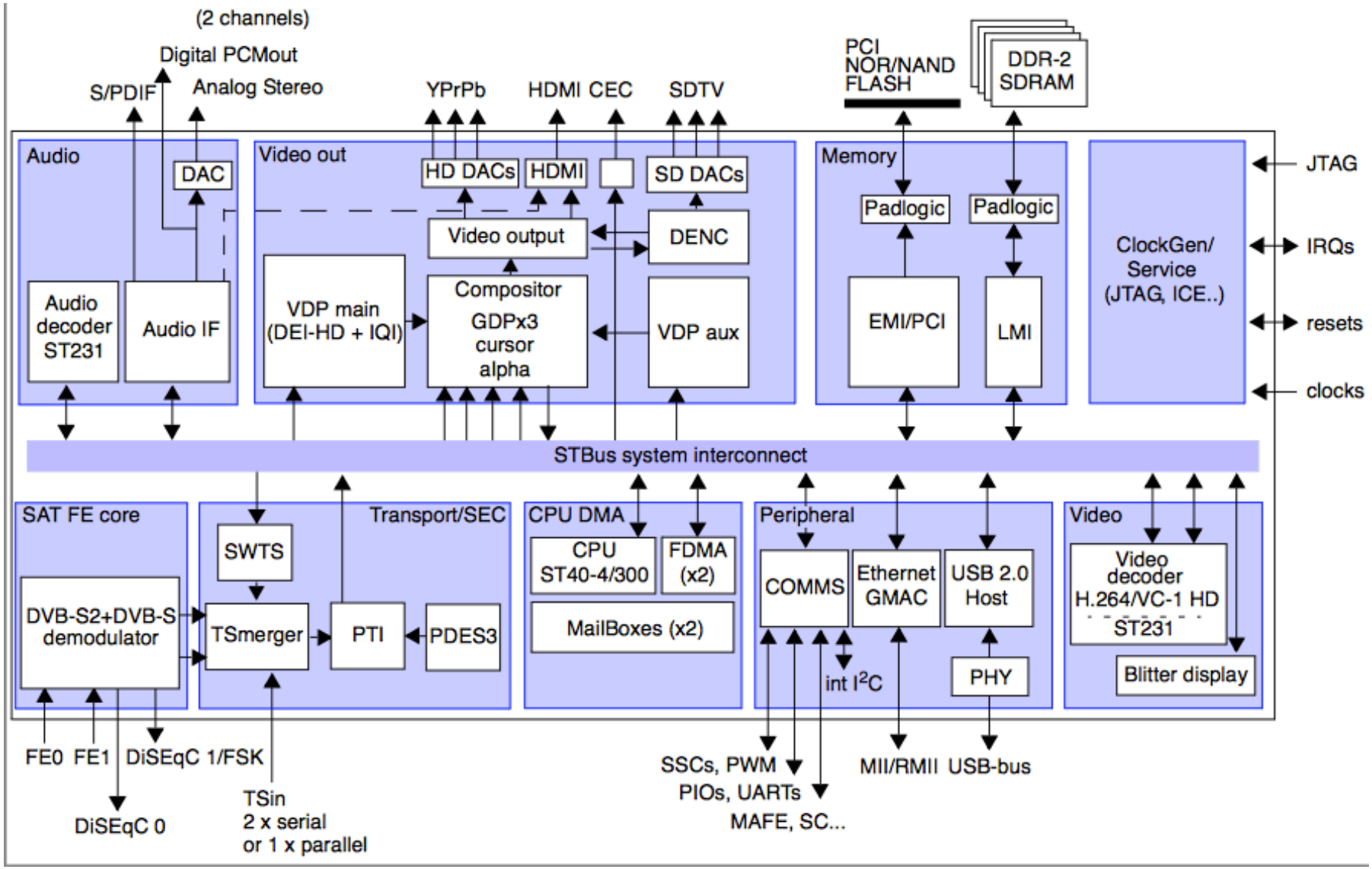
2 USB 2.0 ports

1 card reader

2 module reader (CI)

HDMI – RCA – SPDIF

Things getting easy



What could possibly go wrong ?

What bring STBs to IoT ?

What made the difference ?

We used to have :

- Proprietary STBs
- One service provider per STB

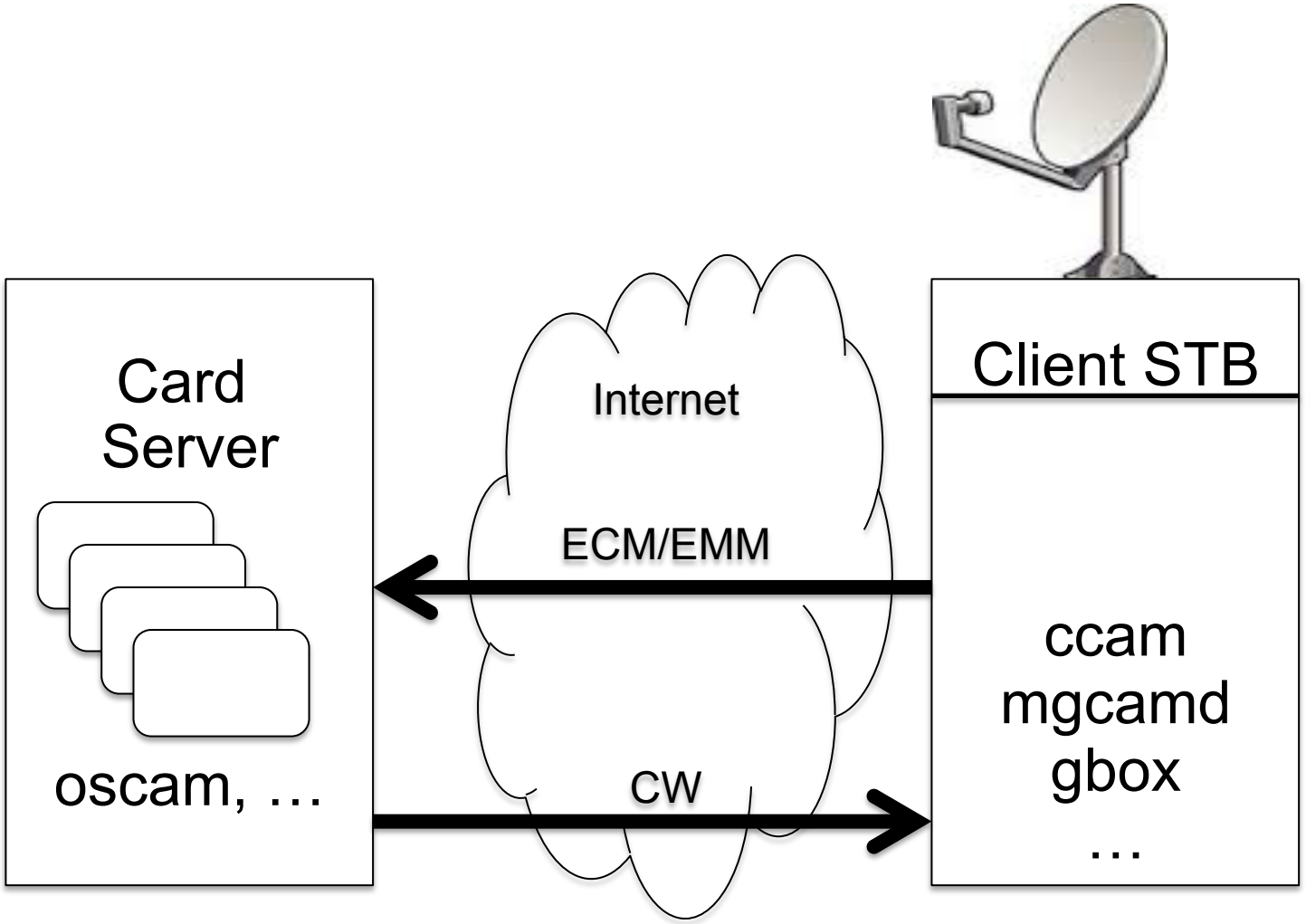
We now have :

- Open STBs
- Fully featured Linux boxes

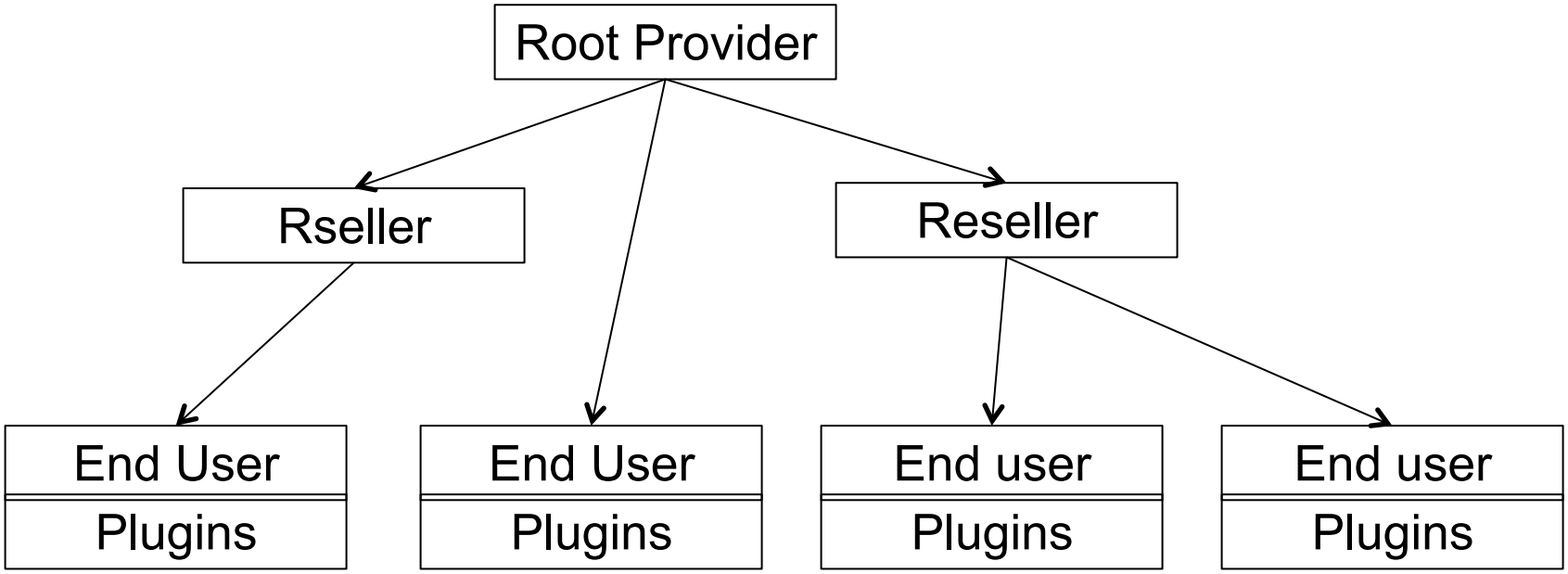
Attack evolution

- STB without CAS
  - Software emulator
- STB + CAS
  - Cloned smart cards
  - CAM
- Card Sharing
  - Protocol providers plugin
  - Internet connectivity
  - Satellite key sharing

Card sharing concept



Components and Actors



Components and Actors

Root provider :

- Generally server hosted at home

Reseller :

- Generate keys and provide/install plugin

End user :

- Plugin running on STB

Cardsharing plugins installed on STBs:

- cccam, mgcamd, newcamd, gbox, etc.: UNKNOWN origin

What could possibly go wrong ?

Vulnerabilities ?

Root account without password

Any other users ?

```
mail:*:9:11:mail:/var/spool/mail:
news:*:10:12:news:/var/spool/news:
operator:*:12:0:operator:/root:
games:*:13:100:games:/usr/games:
ftp:*:15:14:ftp:/home/ftp:
man:*:16:100:man:/var/cache/man:
nobody:*:65534:65534:nobody:/home:/bin/sh
sshd:*:74:74:sshd:/var/empty/sshd:/bin/false
httpd:*:75:75:httpd:/home/httpd:/bin/false
dnsmasq:*:75:75:dnsmasq:/var/lib/misc:/bin/false
dummy:3AQygx9M48HYU:0:0:dummy:/:/bin/ash
```

Rooting the devices

SH4 compiling options

Install gcc for SH4:

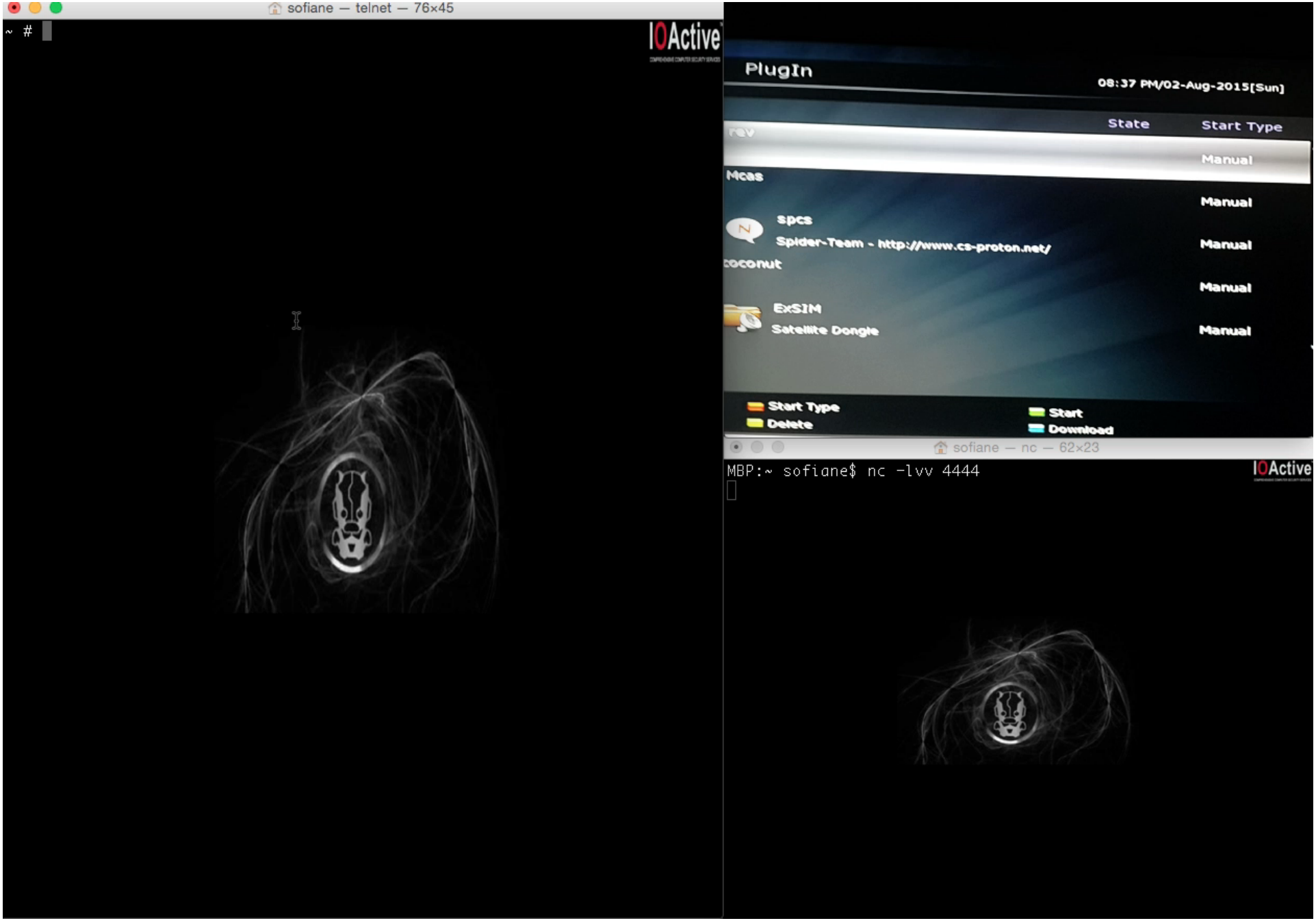
- Thanks to cross compiling tools

Qemu and SH4 debian image:

- SH4 vm

stLinux

- http://www.stlinux.com


sofiane — telnet — 76×45
~ #
IOActive
PlugIn
08:37 PM/02-Aug-2015[Sun]
State
Start Type
Manual
Mcas
Manual
spcs
Spider-Team - http://www.cs-proton.net/
Manual
coconut
Manual
ExSIM
Satellite Dongle
Manual
Start Type
Delete
Start
Download
sofiane — nc — 62×23
MBP:~ sofiane$ nc -lvv 4444
IOActive

Main processes

```
 423 root         0 SWN  [jffs2_gcd_mtd8]
 437 root      1892 S    telnetd
 443 root     11392 S    /usr/sbin/smbd -D -s /etc/samba/smb.conf
 445 root      1888 S    /usr/sbin/httpd -c /etc/httpd.conf
 475 root     11440 S    /usr/sbin/smbd -D -s /etc/samba/smb.conf
 515 root         0 SW<  [EMBXSHM-NewPort]
 516 root         0 SW<  [EMBXSHM-PortClo]
 517 root         0 SW<  [EMBXSHM-NewPort]
 518 root         0 SW<  [EMBXSHM-PortClo]
 521 root         0 SW<  [STFDMA_ClbckMgr]
 522 root         0 SW<  [STFDMA_ClbckMgr]
1310 root      1988 S    /usr/sbin/vsftpd /etc/vsftpd.conf
1311 root      1892 S    /bin/sh /etc/init.d/app_start start
1312 root      1200 S    /sbin/sys_func
1315 root      152m S    /root/bin/app
1318 root         0 DW<  [TUNER0]
```

Everything runs as root

No firewall

```
~ # netstat -anp | grep LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      395/smbd
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      1430/FRior
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      397/httpd
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      1248/vsftpd
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      389/telnetd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      395/smbd
```

Iptables config

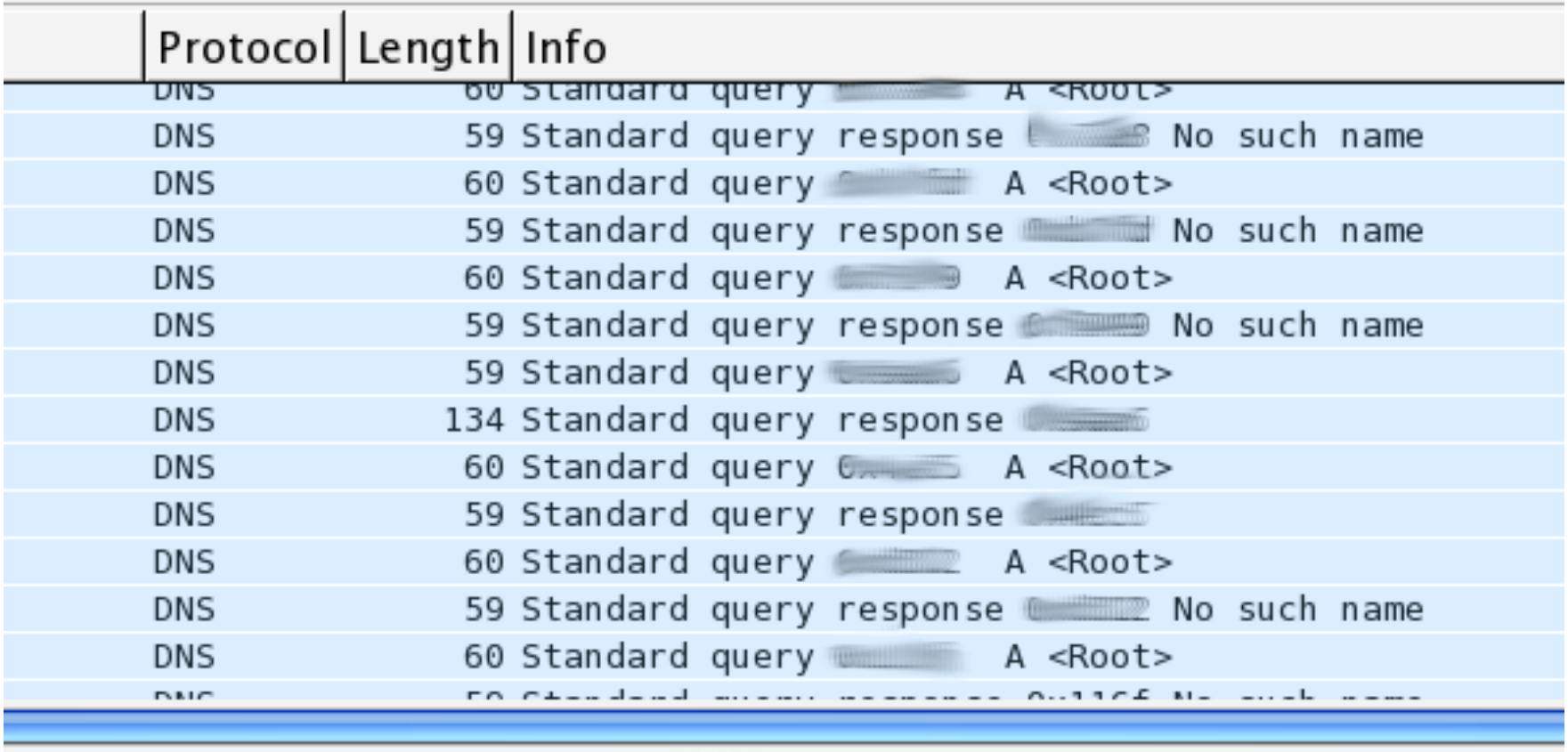
```
start() {
    echo Starting firewall: iptables.
    iptables-restore < /etc/firewall.conf
}
save() {
    iptables-save > /etc/firewall.conf
}

stop() {
    echo Stopping firewall: iptables.
    save
}
```

FTP config

```
226 Directory send OK.
ftp> cd /
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||51015|).
150 Here comes the directory listing.
drwxr-xr-x    8 0        0             544 Sep 27  2010 STORAGE
drwxr-xr-x    2 0        0            3784 Mar 29  2012 bin
drwxr-xr-x    3 0        0               0 Jan 01  1970 config
drwxrwxrwt    9 0        0            6940 Jan 01  2000 dev
drwxr-xr-x   13 0        0            4296 Nov 27  2012 etc
drwxr-xr-x    3 0        0             224 Apr 30  2009 home
drwxr-xr-x    6 0        0            5264 Oct 09  2012 lib
drwxr-xr-x    4 0        0             288 Jun 04  2006 mnt
drwxr-xr-x    2 0        0             160 Sep 08  2009 mnt1
dr-xr-xr-x  125 0        0               0 Jan 01  2000 proc
drwxr-xr-x    2 0        0             160 Oct 06  2009 ramdisk
drwxr-xr-x    4 0        0             288 Feb 07  2011 root
```

Network Activity



Protocol	Length	Info
DNS	60	Standard query [redacted] A <Root>
DNS	59	Standard query response [redacted] No such name
DNS	60	Standard query [redacted] A <Root>
DNS	59	Standard query response [redacted] No such name
DNS	60	Standard query [redacted] A <Root>
DNS	59	Standard query response [redacted] No such name
DNS	59	Standard query [redacted] A <Root>
DNS	134	Standard query response [redacted]
DNS	60	Standard query [redacted] A <Root>
DNS	59	Standard query response [redacted]
DNS	60	Standard query [redacted] A <Root>
DNS	59	Standard query response [redacted] No such name
DNS	60	Standard query [redacted] A <Root>

What could reversing FRior service


```
    nop
-------------------------------------------------------
    .align h'20

                                ; CODE XREF: sub_
    mov.l   #sub_40A560, r0
    mov.l   @(8,r14), r4
    mov.l   @(h'C,r14), r5
    jsr     @r0 ; sub_40A560
    mov     r11, r6
    bra     loc_409D34
    cmp/pz  r0
-------------------------------------------------------
    .align h'20

                                ; CODE XREF: sub_
    mov.l   #strncmp, r1
    mov.l   #aCmd, r5           ; "cmd="
    jsr     @r1 ; strncmp
    mov     #4, r6
    tst     r0, r0
    bf/s    loc_409D86
    mov     #h'FFFFFFFF, r0
    bra     loc_409C4E
    add     #2, r12
ction sub_409B60
```

Unauthenticated

- Check status, channel details, co
- View and set alarms
- View and edit service status
- Manage streaming to remote IP
- More, more, more, ….

Does it contain bugs ? : YES

What could possibly go wrong ?

System Updates

What about system update ?

Main firmware update

- Clear text protocol from internet
- No digital signature verification

Plugins and applications

- Clear text from internet
- No digital signature

Updated to the latest firmware

```
HD_PVR
=======
# busybox
BusyBox v1.14.2 (2012-03-1 15:08:37 KST) multi-call binary
Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
```

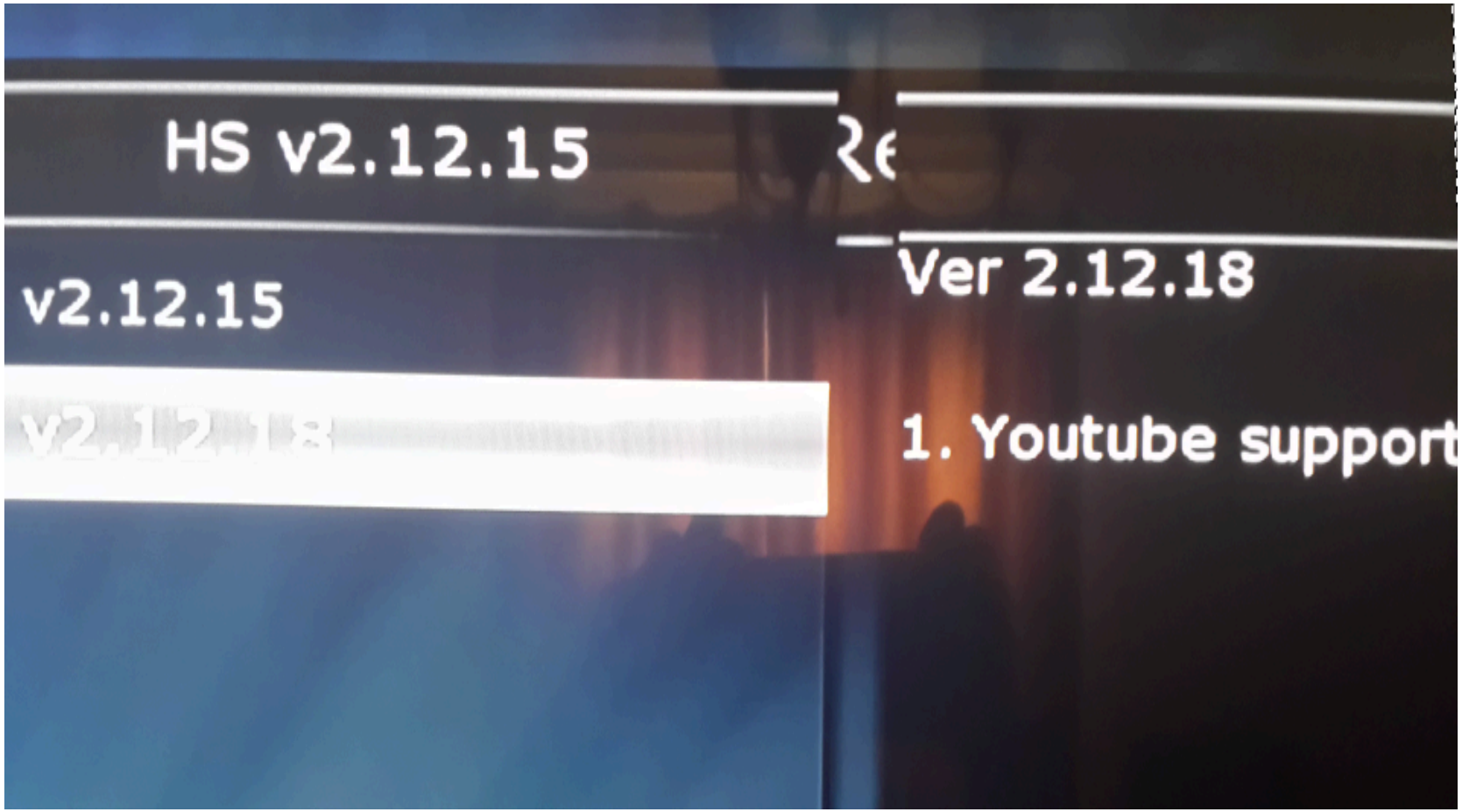
Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Ga
1	CVE-2011-2716	20		Exec Code	2012-07-03	2013-04-10	6.8	

The DHCP client (udhcpc) in BusyBox before 1.20.0 allows remote DHCP servers to execute arbitrary commands via TFTP_SERVER_NAME host name options.

Total number of vulnerabilities : 1 Page : 1 (This Page)

However they do fix some bugs ….



Miscellaneous

Internet connectivity support

- Integrated web browser
  - No support for HTTPS
- IPTV plugins applications
  - Remote SQL Injection

What could possibly go wrong ?

Put all this together

Overview

Internal Architecture and security

- Total Fail !

Cardsharing plugins installed on STBs:

- cccam/mgcamd/newcamd/gbox : UNKNOWN DEVLOPERS and Untrusted

Firmware upgrade and patching:

- Total Fail !

Main Actors :

- Unknown, untraceable and untrusted

Number of devices

Number of cards haring subscribers :

- ~ 4 Millions in Algeria only / what about the world ?

End user :

- Unaware

Manufacturers promoting card sharing

Free access to card sharing server for 394 days

Contacting vendor

Contact

Notre équipe s'engage à répondre à votre demande dans les plus brefs délais.

Votre nom (obligatoire)

Votre email (obligatoire)

Sujet

Votre message

Envoyer

Building a botnet

Building the plugin :

- Some C/C++ coding skills to build the plugin
- Thanks to cross compiling tools

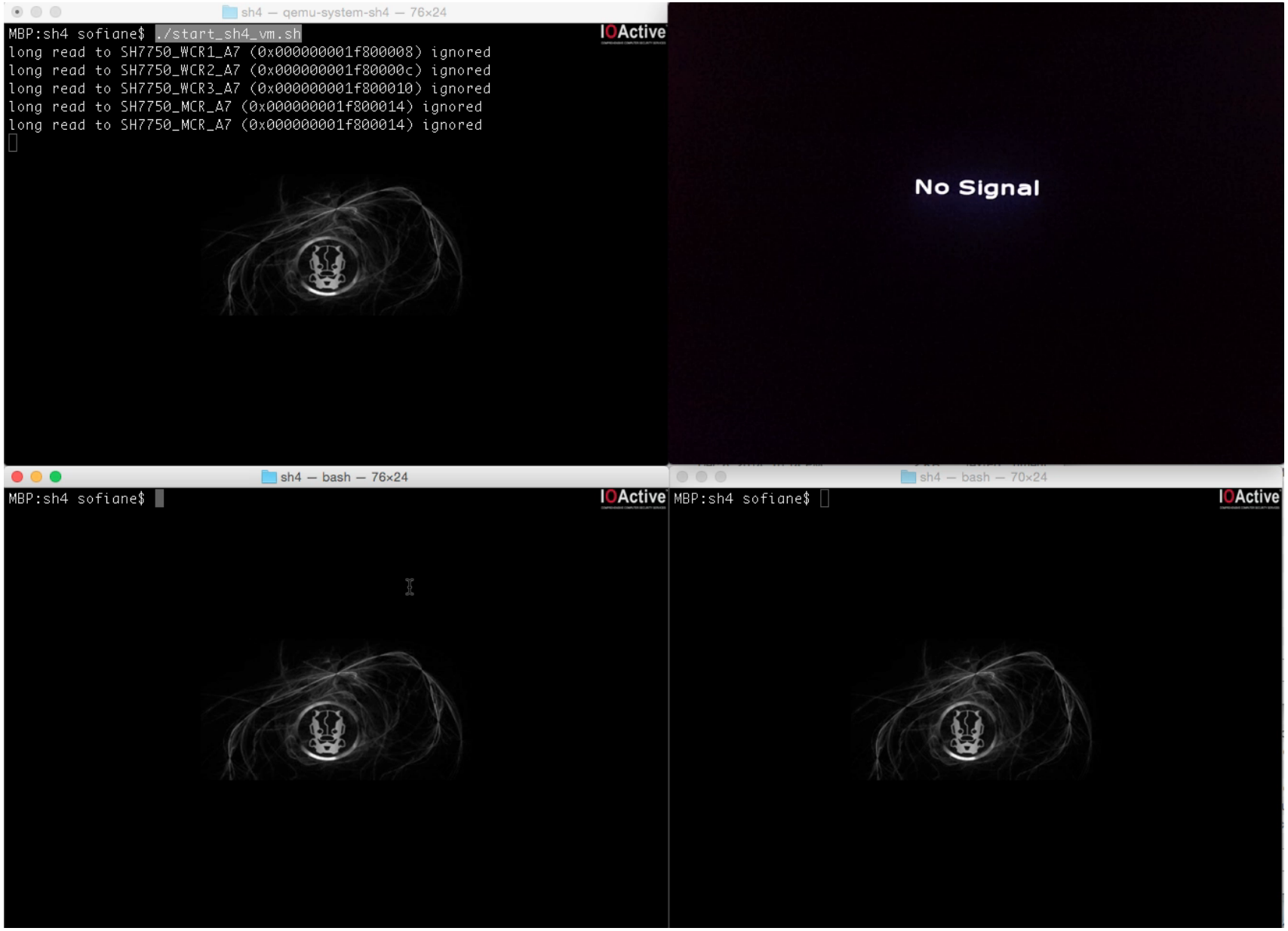
Hosting the service :

- Either host a card sharing server
- Or become a reseller
- Throw that on internet

End users/Resellers:

- They will come for you

Demo of a Backdoor



OOPS … Something went wrong.

Thank you