

Subverting satellite receivers for botnet and profit

Sofiane Talmat
Senior Security Consultant

Agenda

- The famous “who am I ?” slide
- The quest for the Control Word
- A series of “What could possibly go wrong ?”
- Questions ?

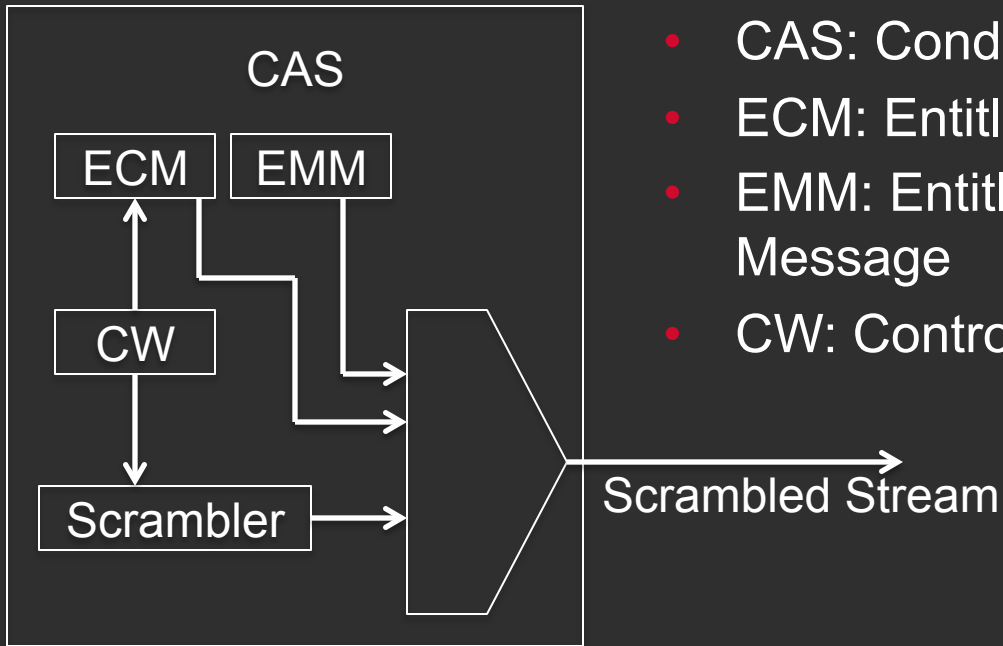
Who am I ?

- Senior security consultant at IOActive
- Like
 - Breaking things
 - Having fun with firmware and hardware
- Do not like:
 - Coffee
 - “Who am I ?” slides

The quest for the Control Word

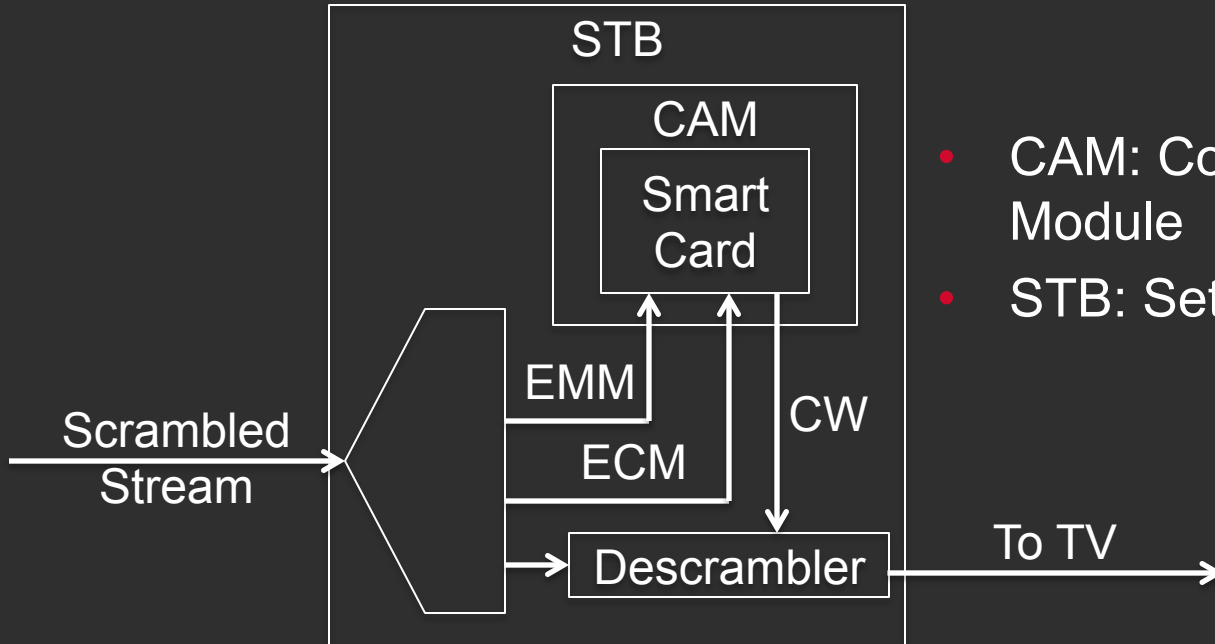


Scrambling



- 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 could possibly go wrong ?



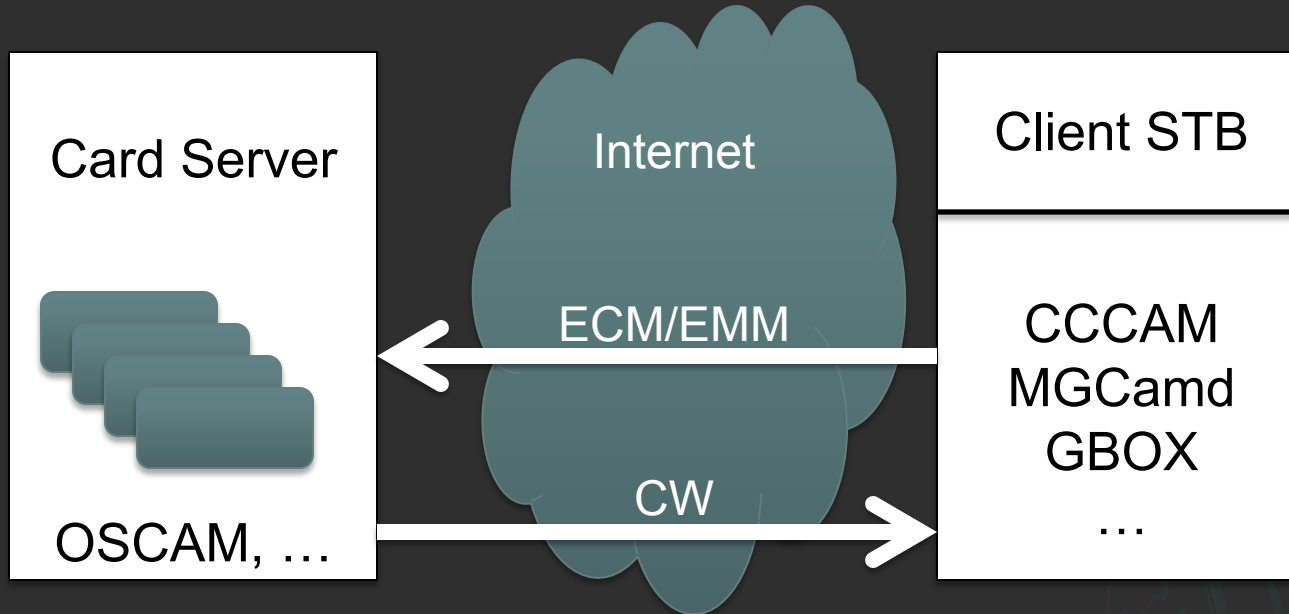
What made the difference ?

- 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 with CAS
 - Cloned smart cards
 - CAM
- Card Sharing
 - Protocol providers plugin
 - Internet connectivity
 - Satellite key sharing

Card sharing concept



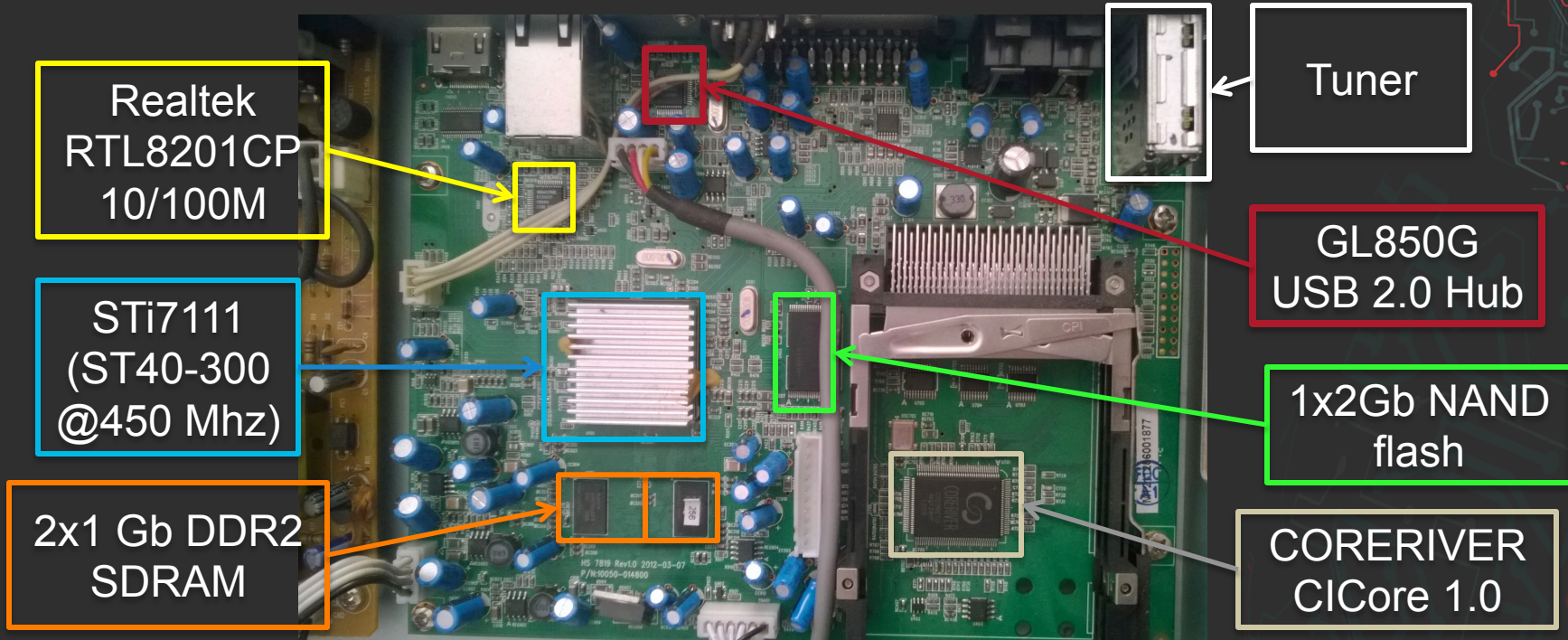
Components and Actors

- Card sharing plugins installed on STBs:
 - CCCAM, MGCAMD, NEWCAMD, GBOX, etc.
- Root provider :
 - Generally server hosted at home
- Reseller :
 - Generate keys and provide/install plugin
- End user :
 - Plugin running on STB

What could possibly go wrong ?



Teardown of an STB



Better than my graduation computer

- STi7111 (ST40-300 @450Mhz)
- ROM=256MB
- RAM= 256MB
- 10/100M Ethernet port
- 2 USB 2.0 ports
- 1 card reader
- 2 module reader (CI)
- HDMI – RCA – SPDIF

Are they vulnerable ?

- For all studied devices :
 - Internal design : Fail!
 - System update and upgrades : Fail!
 - OS protection : Fail!
 - Integrated software : Fail!

- Why ?
 - Because they are not designed to be secure

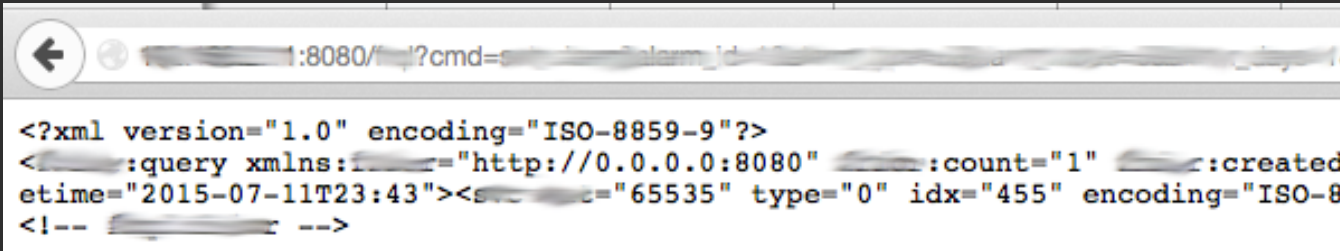
```
mov.l    #sub_40A560, r0    ; CODE XREF: sub_
mov.l    @(8,r14), r4
mov.l    @(h'C,r14), r5
jsr      @r0 ; sub_40A560
mov      r11, r6
bra      loc_409D34
cmp/pz   r0

-----
.align   h'20

mov.l    #strncmp, r1      ; CODE XREF: sub_
mov.l    #aCmd, r5        ; "cmd="
jsr      @r1 ; strncmp
mov      #4, r6
tst      r0, r0
bf/s     loc_409D86
```


Remotely exploitable ?

- YES :
 - But most of them are behind NAT
- How bad is that ? :
 - Accessing an STB means access to internal LAN



A screenshot of a web browser window showing an XML response. The address bar contains a URL with a port number 8080 and a query parameter 'cmd'. The XML content is as follows:

```
<?xml version="1.0" encoding="ISO-8859-9"?>
<[redacted]:query xmlns:[redacted]="http://0.0.0.0:8080" [redacted]:count="1" [redacted]:created
etime="2015-07-11T23:43"><[redacted]c="65535" type="0" idx="455" encoding="ISO-8
<!-- [redacted] -->
```


What could possibly go wrong ?



How does it work

- Root provider :
 - Provides reseller with access to card sharing server
 - Provides interface to create/manage accounts
 - Provides plugins to support protocols
- Reseller :
 - Create and manage accounts
 - Install plugins on end user STBs

The weakest link of the chain

- End user:
 - Installs plugins on his STB through USB key
 - Takes his STB to reseller to install the plugin
 - Download plugins from internet through the STB

What's wrong with that ?

- Root provider :
 - Unknown and proceeding from unknown location
- Reseller :
 - Unknown
 - Proceeding from specific countries (Legally in my country)
- End user:
 - Unaware about the problem
 - Always seeking free TV at any cost
 - Trusts internet

What could possibly go wrong ?



Overview

- Number of cards sharing subscribers joining IoT :
 - ~ 4 Millions in Algeria only / what about the world ?
- End user :
 - Unaware

Are we getting more ?



FOREVER HD 7819 PVR NANO Pro

In Démodulateurs FULL HD, New, Produits

Présentation Caractéristiques FAQ Mises à Jour Catalogue Galerie

- Récepteur Satellite 2e Génération **FULL HD 1080p** Linux Dual Core **CS + ENIGMA2**
- Connexion en mode **ETHERNET, WIFI** ou même **3G**
- Serveur Gratuit pour **394 jours (1an+1mois)** dans le meilleur serveur au monde

Ouvrant toutes les chaînes normales et Haute Définitions **HD** dans différents satellites

- Fonction **PAUSE** à l'abonnement pour ne pas perdre de jours ... Exclusivement sur les FOREVER
- Enregistrement des chaînes sur **USB / Disque dur Externe**

Free access to card sharing server for
394 days

What if ?

- A root provider deploys a plugin with backdoor
- A reseller deploys a plugin with backdoor
- Millions of end users installing them on their boxes
 - PS : Plugins will be running as root

Demo

OOPS ... Something went wrong.



Basic steps to build the 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

What will be the result ?

- A massive botnet based on rooted Linux boxes
- Unaware users about what's happening on their boxes
- Access to users and companies LAN
 - Yes some companies do have that in my country

Did this happen before ?

- Reported CCAM plugin in the wild with a backdoor :
 - Steal information from card sharing providers
 - Send information to an IP address

- Who could be :
 - Attackers stealing accounts
 - Service providers to counter attack card sharing

Challenges to mitigate that

- The bad thing :
 - You can not educate end user
 - End users don't care, they just want free TV
 - Not easy to put standards for piracy
- There is some light :
 - Some work is being done for hardening CW interception

Black Hat Sound Bytes

- Millions of Satellite TV receivers joined IoT without security design
- Card sharing providers can take control of satellite receivers
- End user is not aware and doesn't understand the risk

The background of the slide features a complex, abstract pattern of circuit board traces. The traces are rendered in shades of red and light blue against a dark grey background. The pattern is dense and intricate, resembling a high-density printed circuit board (PCB) layout. The traces form various geometric shapes, including lines, curves, and small circular nodes, creating a sense of depth and technical complexity.

Questions ?

Thank you

- My wife Amina
- Fernando Arnaboldi
- Carlos Hollmann
- Ahmed Mahfouz
- Abdelkader Mraiagh
- Hamza Tahmi