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

CAS

ECM  EMM

CW

Scrambler

Scrambled Stream
Descrambling

- CAM: Conditional Access Module
- STB: Set Top Box

Scrambled Stream → Descrambler → To TV
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?
3.1 Services

Teardown of an STB

- Realtek RTL8201CP 10/100M
- STi7111 (ST40-300 @450 Mhz)
- 2x1 Gb DDR2 SDRAM
- 1x2Gb NAND flash
- CORERIVER CICore 1.0
- Tuner
- GL850G USB 2.0 Hub
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
Remotely exploitable?

- YES:
  - But most of them are behind NAT

- How bad is that?:
  - Accessing an STB means access to internal LAN
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?

Free access to card sharing server for 394 days
What if?

• A root provider deploys a plugin with a backdoor.

• A reseller deploys a plugin with a backdoor.

• Millions of end users installing them on their boxes.
  - PS: Plugins will be running as root.
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
Questions ?
Thank you

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