INTREPIDUS GROUP
MOBILE SECURITY

Raspberry Pi, Cars, and AppleTV

David Schuetz (@DarthNull)

DerbyCon 3.0

September 28, 2013

DERBYCON

Requisite Background

- Senior Consultant at Intrepidus Group
  - –Wholly owned by NCC Group
- Mobile app and OS testing and research
  - –I focus on iOS
  - –Others have more Android focus
    - Including three other guys presenting at this very con
- Also web app testing, pen testing, physical security reviews, etc.
- Interested in any of that? We’re also hiring! :)

Remember these?

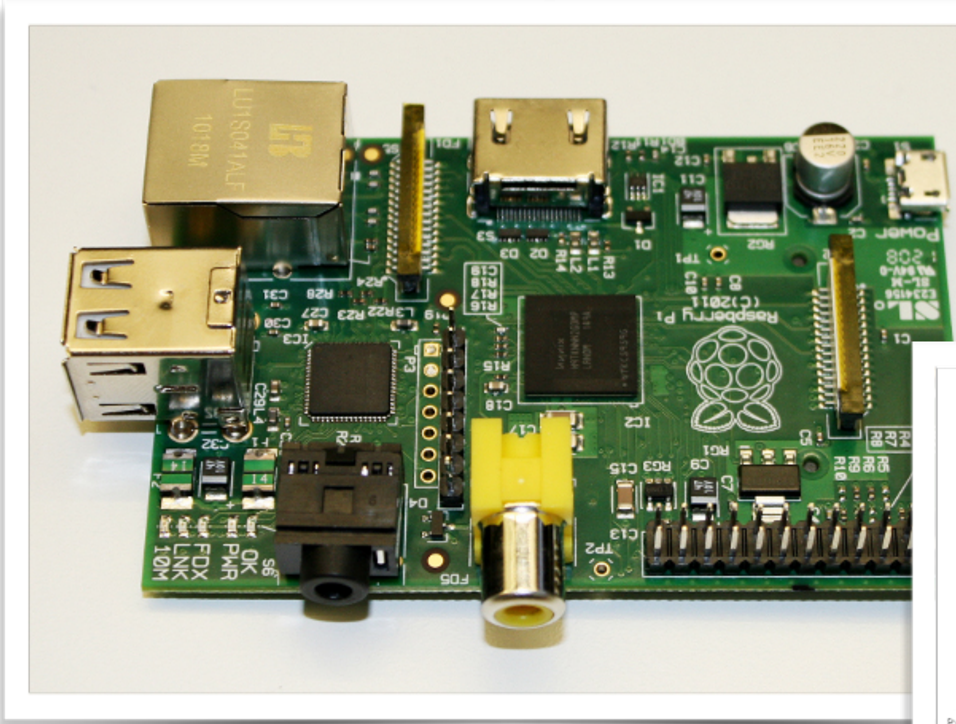
Nostalgia can't compete

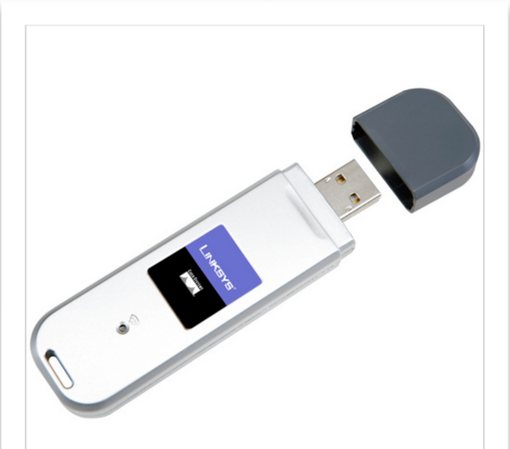
Minecraft in the Car

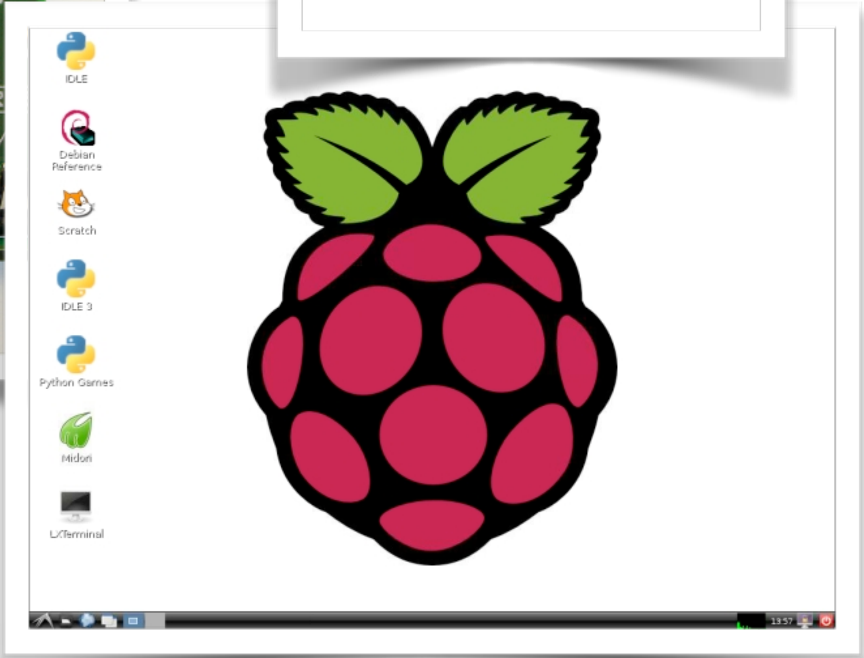
- My boys LOVE minecraft
- Just build, explore, tear down...
  - (and lately, shoot chickens)
- This past spring, had a great idea:
  - Let’s put an access point in the car!

- Then...I got a little feature crazy.
- Quick overview of some features
- Deep dive into integration with Apple TV

What do you need





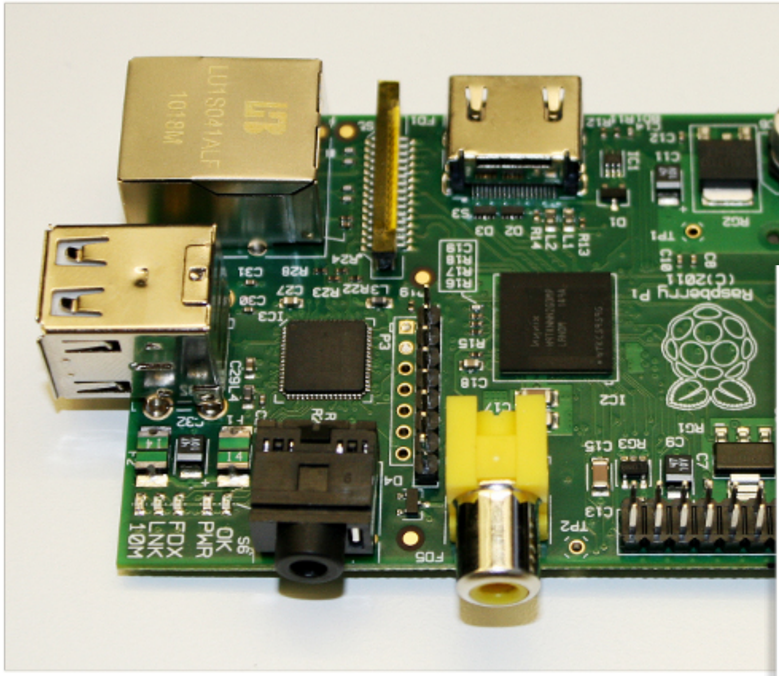


Software

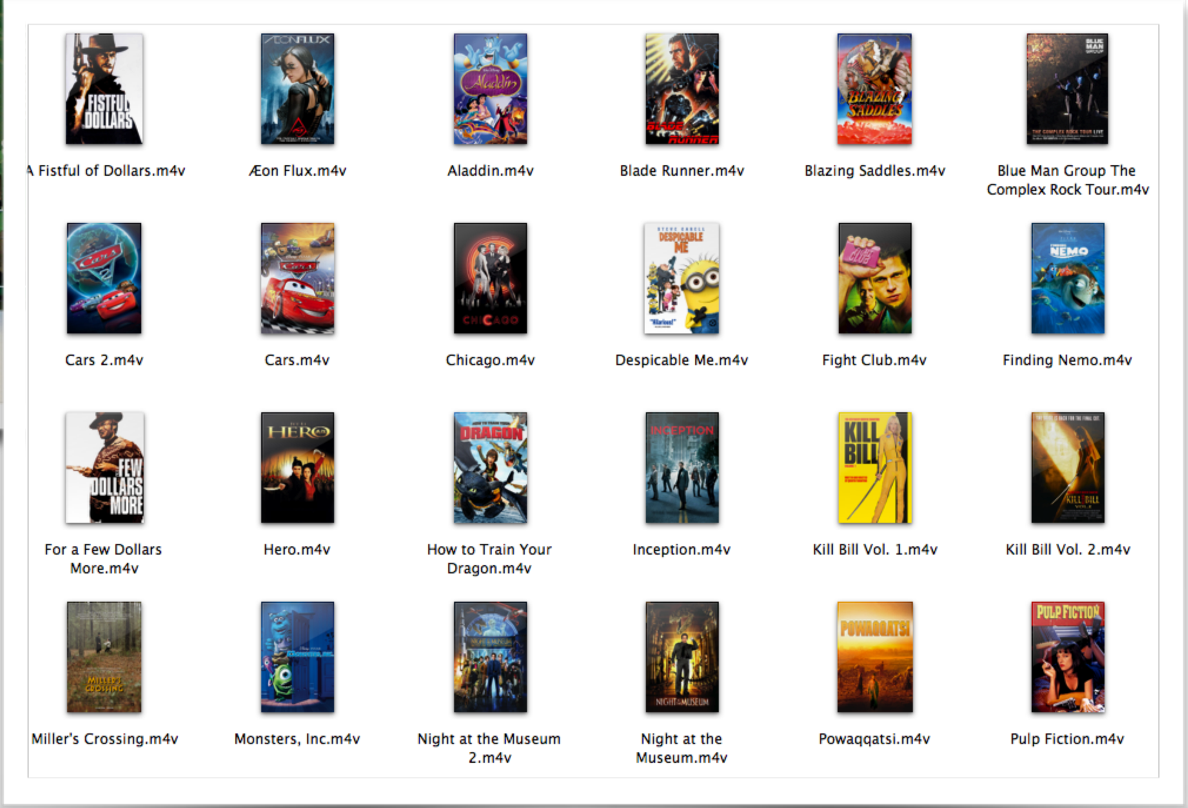
- Hardware:
  - –Logitech WUSB54GC
  - –By luck, had one in a drawer
- Software:
  - –iw: to verify your adapter will work
  - –udhcpd: to provide IPs for clients
  - –hostapd: set up access point
- Not worrying about NAT, FW, etc.
  - –For now, it’s a standalone (isolated) car network
- Step by step guides:
  - –learn.adafruit.com
  - –Pi-Point.co.uk

Tired of lugging DVDs?

Let's put movies on rPI



dlna®

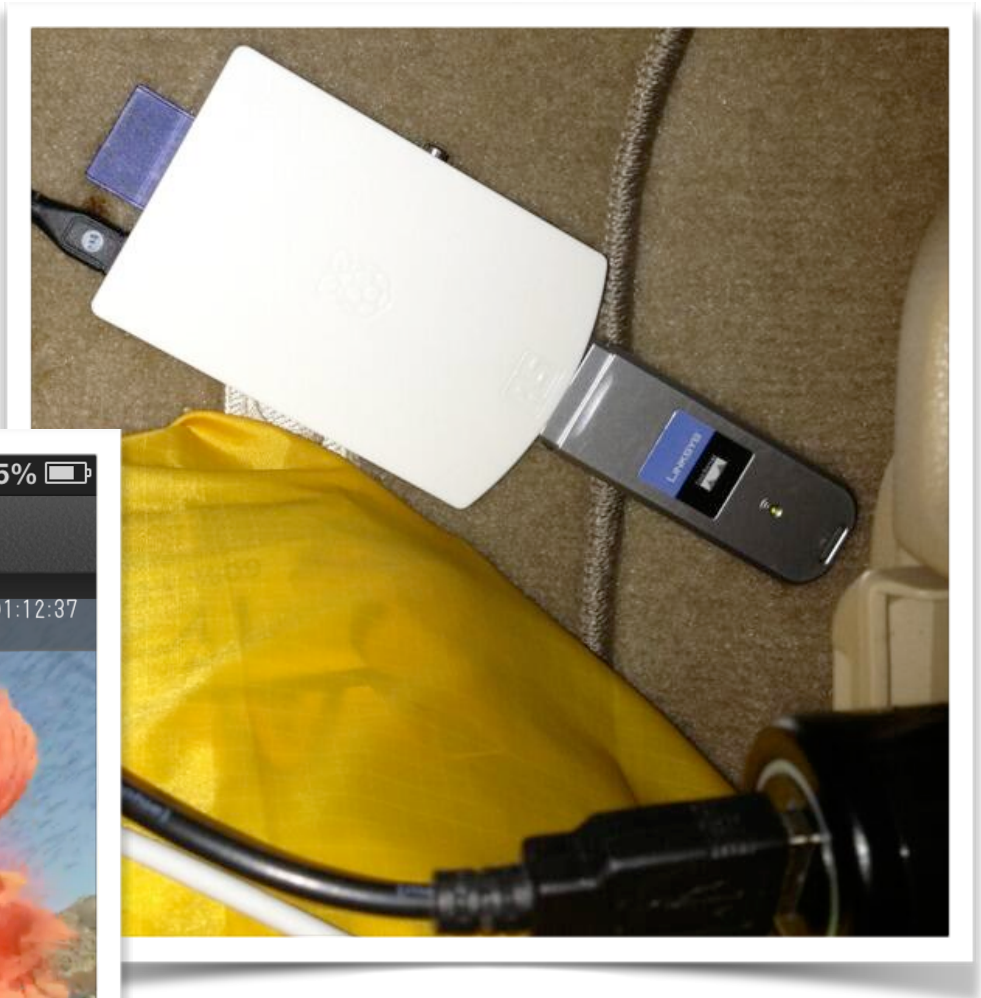


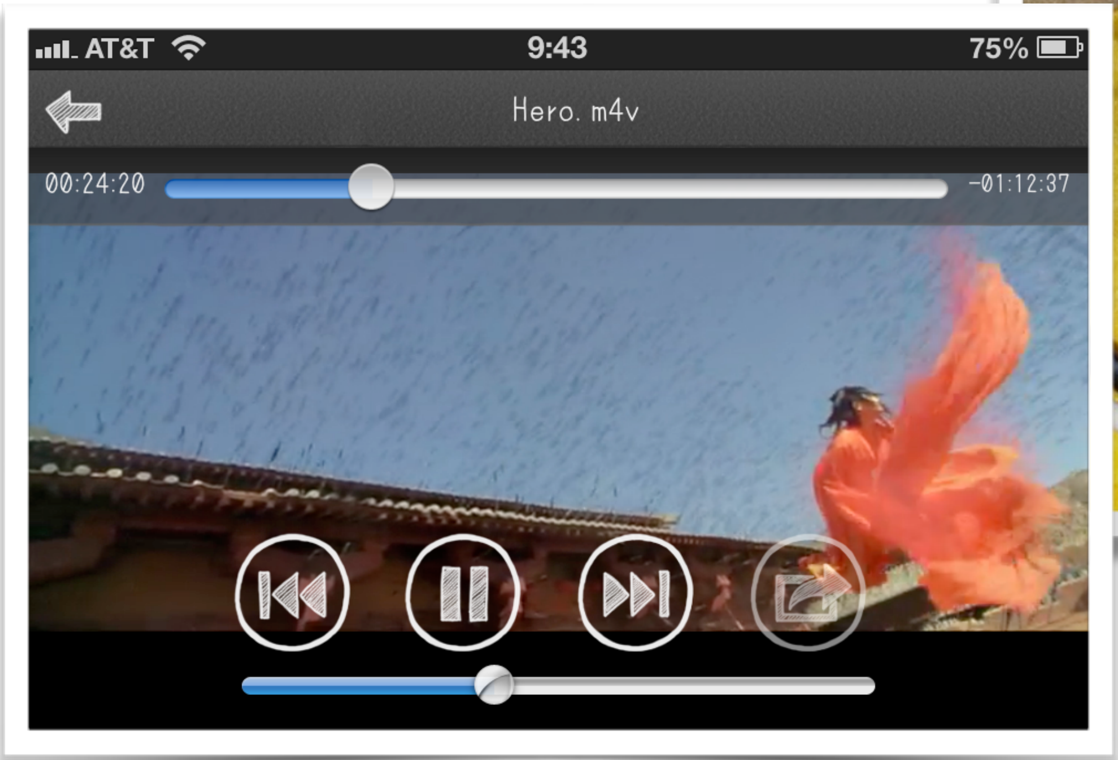
A Fistful of Dollars.m4v
Æon Flux.m4v
Aladdin.m4v
Blade Runner.m4v
Blazing Saddles.m4v
Blue Man Group The Complex Rock Tour.m4v
Cars 2.m4v
Cars.m4v
Chicago.m4v
Despicable Me.m4v
Fight Club.m4v
Finding Nemo.m4v
For a Few Dollars More.m4v
Hero.m4v
How to Train Your Dragon.m4v
Inception.m4v
Kill Bill Vol. 1.m4v
Kill Bill Vol. 2.m4v
Miller's Crossing.m4v
Monsters, Inc.m4v
Night at the Museum 2.m4v
Night at the Museum.m4v
Powaqqatsi.m4v
Pulp Fiction.m4v

Walk through sfwe

- minidlna: the DLNA server itself
- /etc/minidlna.conf: media folder, network address, etc.
- Content: Whatever your clients can display
  - –Using iOS devices -- m4v, etc. (Handbrake FTW)
- Clients: Whatever works
  - –All kinds of DLNA clients on iOS
  - –Most are... clunky.
  - –Should also work with DLNA TVs
    - But they might be a bit large for the car

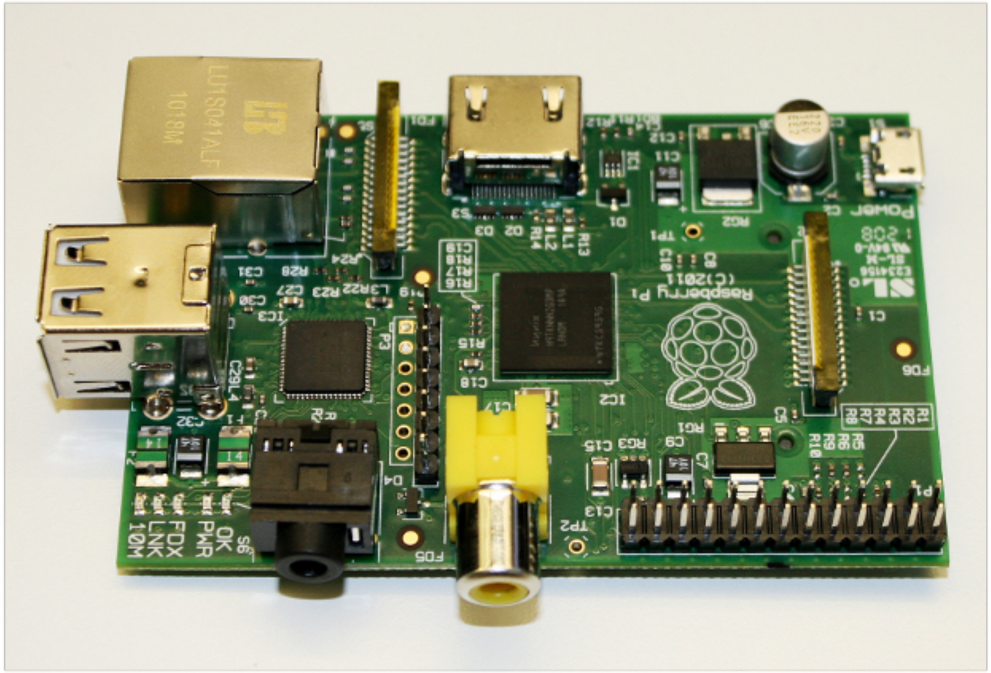
In Action!

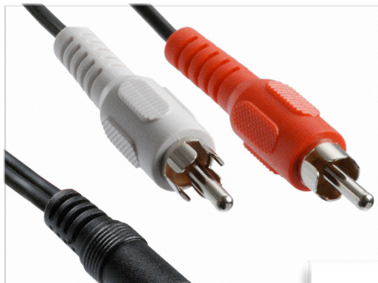




And when the battery dies?

Media player on rPI!





Not that simple...

- Several pre-built, dedicated images:
  - –OpenELEC
  - –Raspbmc
  - –XBian
- Fast, clean, simple
  - –Not as flexible -- replaces whole OS
- XBMC packages exist
  - –michael.gorven.za.net/raspberrypi/xbmc
- Control with XBMC web interface

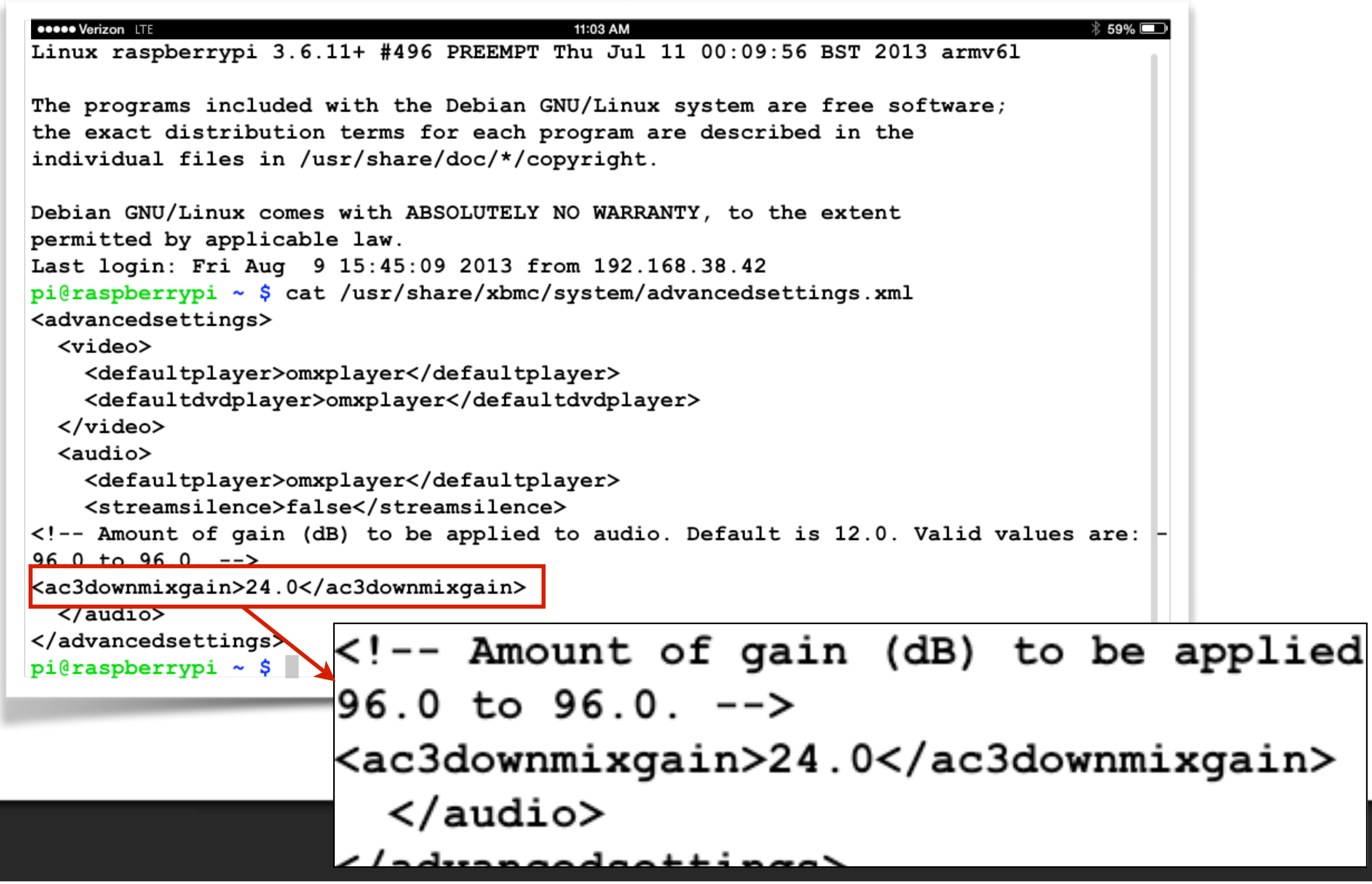
Metadata didn’t like

- XBMC grabs program info “live”
- Not the iTunes tags I painstakingly added
- Sometimes, VERY wrong.
- Reading iTunes tags is a royal pain
- Many old and unmaintained libraries
- During this work, settled on a pair of utilities
  - –But couldn’t get them running on the rPI

- Someone: Please fix this!

Very low volume

- Had to tweak mixdown parameters



```
Linux raspberrypi 3.6.11+ #496 PREEMPT Thu Jul 11 00:09:56 BST 2013 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Aug  9 15:45:09 2013 from 192.168.38.42
pi@raspberrypi ~ $ cat /usr/share/xbmc/system/advancedsettings.xml
<advancedsettings>
  <video>
    <defaultplayer>omxplayer</defaultplayer>
    <defaultdvdplayer>omxplayer</defaultdvdplayer>
  </video>
  <audio>
    <defaultplayer>omxplayer</defaultplayer>
    <streamsilence>false</streamsilence>
<!-- Amount of gain (dB) to be applied to audio. Default is 12.0. Valid values are: -
96.0 to 96.0. -->
<ac3downmixgain>24.0</ac3downmixgain>
  </audio>
</advancedsettings>
pi@raspberrypi ~ $
```

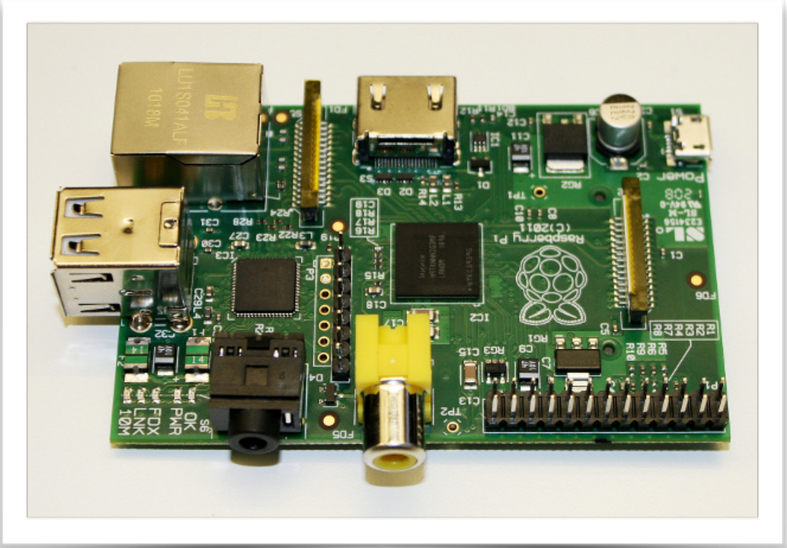
```
<!-- Amount of gain (dB) to be applied
96.0 to 96.0. -->
<ac3downmixgain>24.0</ac3downmixgain>
  </audio>
</advancedsettings>
```

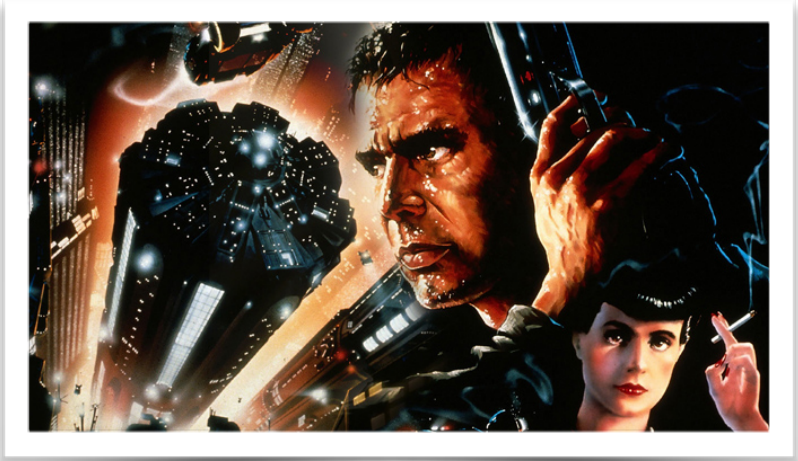
...and at the rental house?

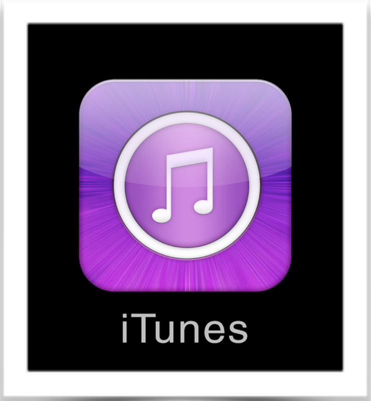
Bring the AppleTV!

- It’s small
- It’s got Netflix
- Many rental houses have WiFi
- But now I need to bring an iTunes server...

Let's put rPI on AppleTV

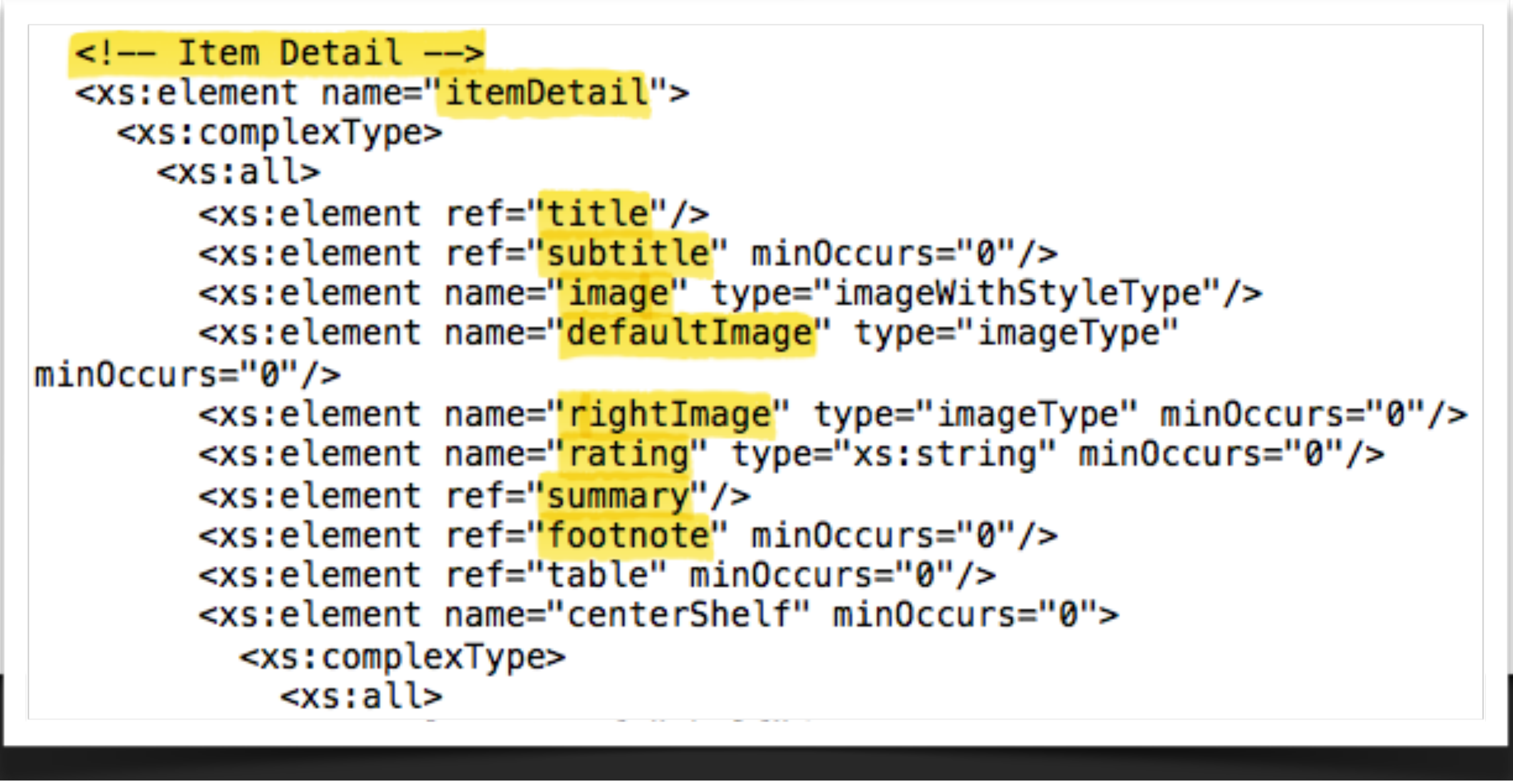






AppleTV Channels

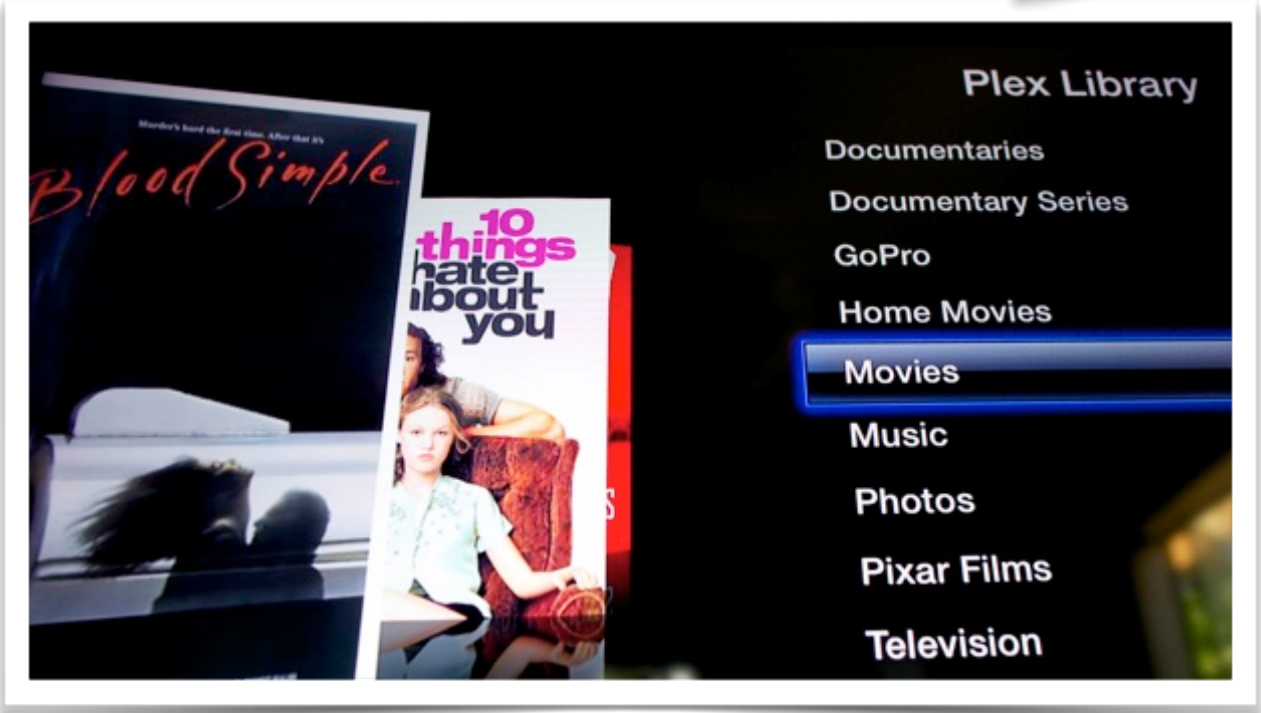
- Not compiled binaries
- Interface defined in XML
- Modified in JavaScript on client
- Fetched real time over the Internet



```
 <!-- Item Detail -->
 <xs:element name="itemDetail">
   <xs:complexType>
     <xs:all>
       <xs:element ref="title"/>
       <xs:element ref="subtitle" minOccurs="0"/>
       <xs:element name="image" type="imageWithStyleType"/>
       <xs:element name="defaultImage" type="imageType"
minOccurs="0"/>
       <xs:element name="rightImage" type="imageType" minOccurs="0"/>
       <xs:element name="rating" type="xs:string" minOccurs="0"/>
       <xs:element ref="summary"/>
       <xs:element ref="footnote" minOccurs="0"/>
       <xs:element ref="table" minOccurs="0"/>
       <xs:element name="centerShelf" minOccurs="0">
         <xs:complexType>
           <xs:all>
```

Sneaking in

- Point DNS to your server
- Intercept trailers.apple.com
- Send your own XML content
- Used by PlexConnect, others

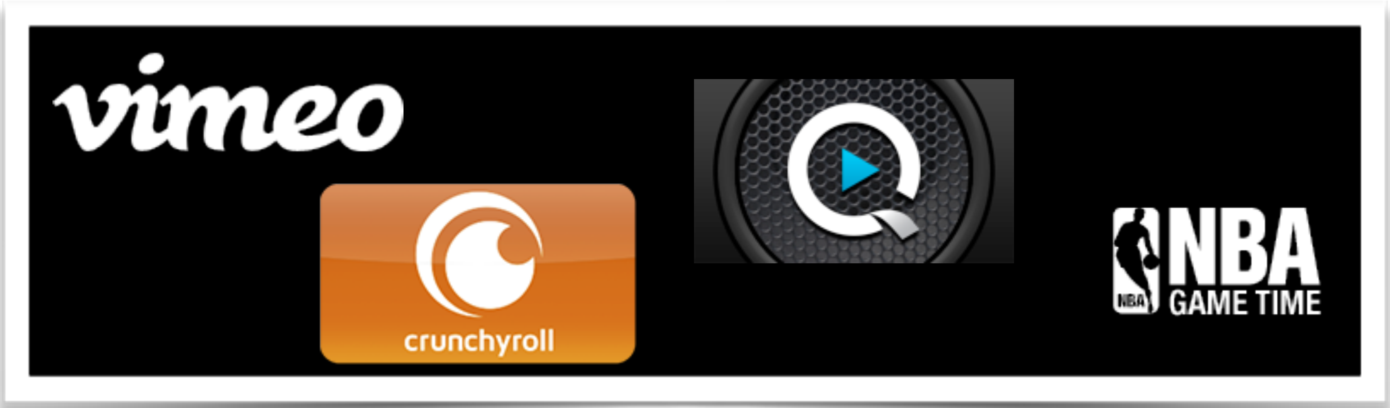


Some limitations

- Can't change the icon or name
- Only do this for one external app at a time
  - Unless you hijack additional channels
- Not great for externally hosted channels
- You lose the hijacked channel
  - I sorta like the Trailers app
- Changes by Apple can break it
  - Early September: changed to https for key files

Official Channels

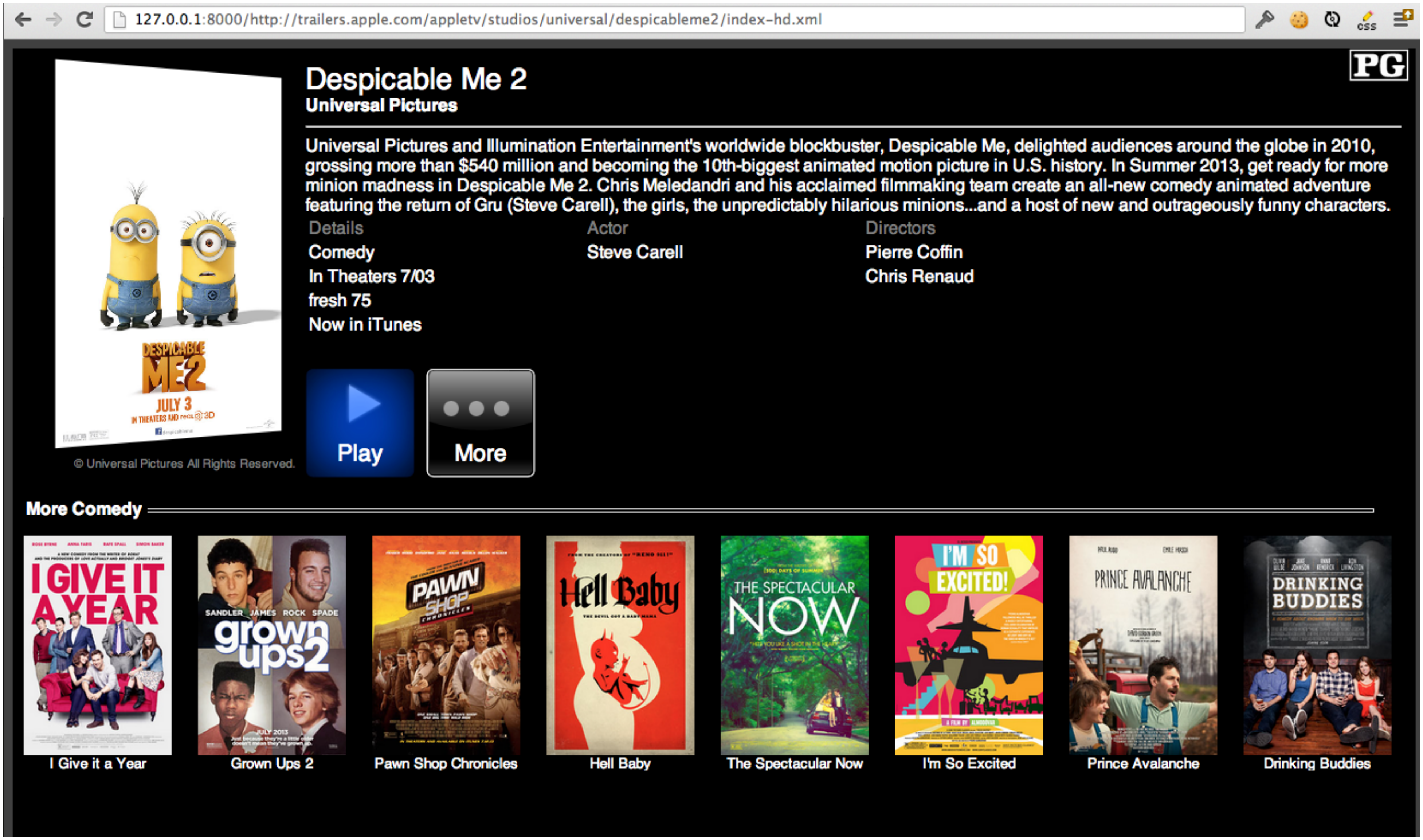
- Netflix, Vimeo, MLB, SkyNews, etc.
- Must be working directly with Apple
- Does Apple develop the apps?
- If not....
- ...how do they test their code?



Use a simulator?

- Not sure one exists
- But everything is in XML
- And I actually *like* XSLT (yes, I’m the one)
- So....now I can simulate AppleTV
  - Ugly “proxy” hack
  - Fetches remote pages
  - Applies XSLT, uses CSS for layout
  - Returns to browser
- Works in Chrome, better in Safari
- Should be a dedicated app

XML + XSLT = Hackalicious



127.0.0.1:8000/http://trailers.apple.com/appletv/studios/universal/despicableme2/index-hd.xml

PG

Despicable Me 2

Universal Pictures

Universal Pictures and Illumination Entertainment's worldwide blockbuster, Despicable Me, delighted audiences around the globe in 2010, grossing more than $540 million and becoming the 10th-biggest animated motion picture in U.S. history. In Summer 2013, get ready for more minion madness in Despicable Me 2. Chris Meledandri and his acclaimed filmmaking team create an all-new comedy animated adventure featuring the return of Gru (Steve Carell), the girls, the unpredictably hilarious minions...and a host of new and outrageously funny characters.

Details	Actor	Directors
Comedy	Steve Carell	Pierre Coffin
In Theaters 7/03		Chris Renaud
fresh 75		
Now in iTunes		

© Universal Pictures All Rights Reserved.

More Comedy

I Give it a Year · Grown Ups 2 · Pawn Shop Chronicles · Hell Baby · The Spectacular Now · I'm So Excited · Prince Avalanche · Drinking Buddies

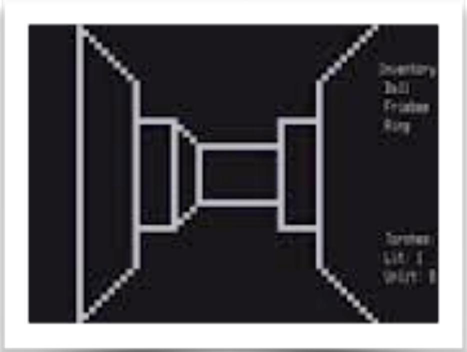
How do you test ON DEVICE?

- Even a perfect simulator is just a simulator
- Essential to test on the device itself
- Can you side-load apps via USB?
  - Direct filesystem upload would've been noticed
  - Profile-based install? MDM?
- Or maybe a hidden menu somewhere

- Let's get a jailbroken ATV and start hacking!

35 years of feature finding

- 1978: key combinations and algebra
- 1981: hexdump, disassembler, paper
- 1993: strings command and dwrites
- 2013: strings, IDA, mobileconfig

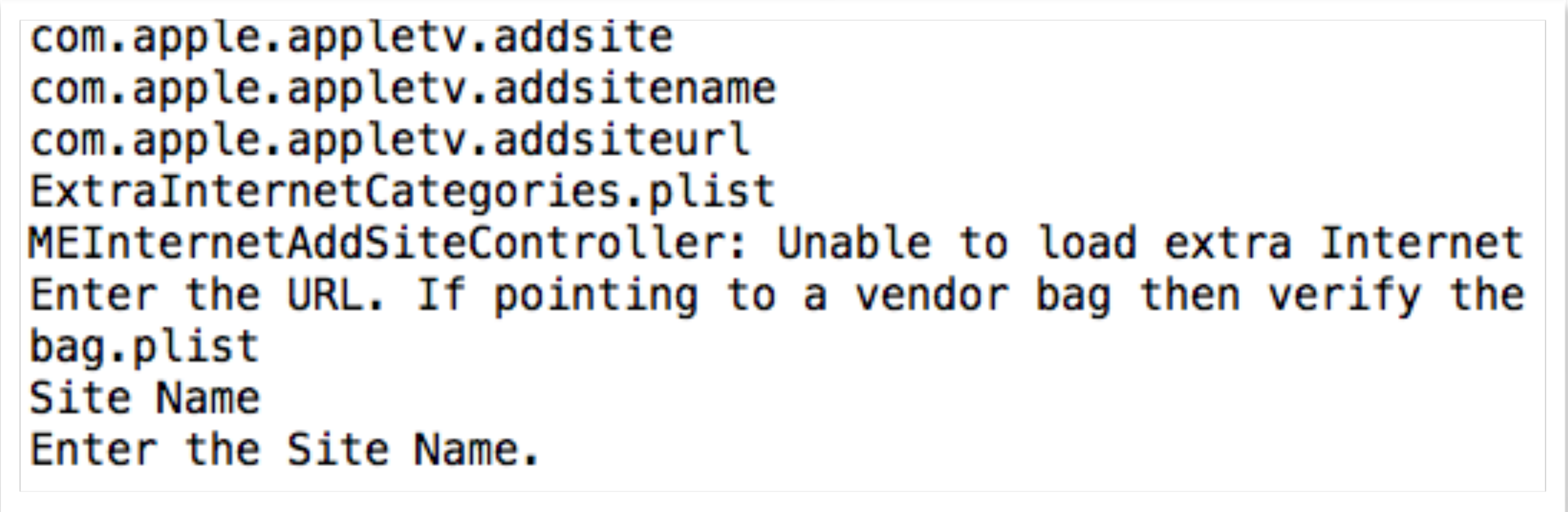


Close look at AppleTV

- Been working with iOS for a while now
- First time using a jailbroken AppleTV
- Plex hack inspired to dig deeper
- Looked closely at AppleTV.app
- Found quite a few neat tricks

Interesting Strings

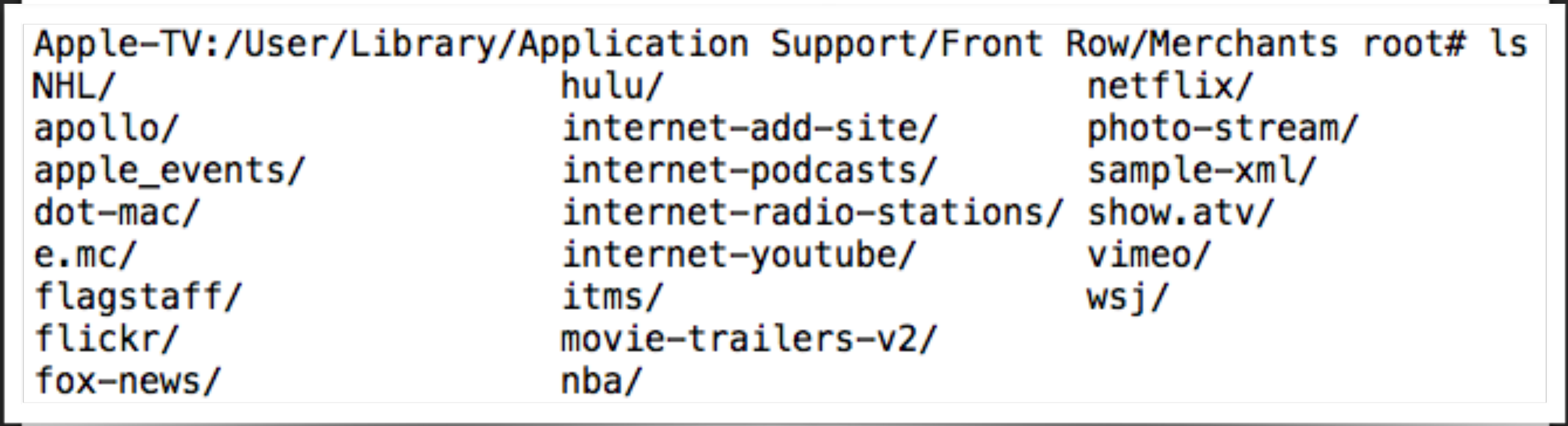
- EnableAddSite
- menu-title, menu-icon-url, root-url
- loaded-via-addsite
- AddProfile



```
com.apple.appletv.addsite
com.apple.appletv.addsitename
com.apple.appletv.addsiteurl
ExtraInternetCategories.plist
MEInternetAddSiteController: Unable to load extra Internet
Enter the URL. If pointing to a vendor bag then verify the
bag.plist
Site Name
Enter the Site Name.
```

Application Settings

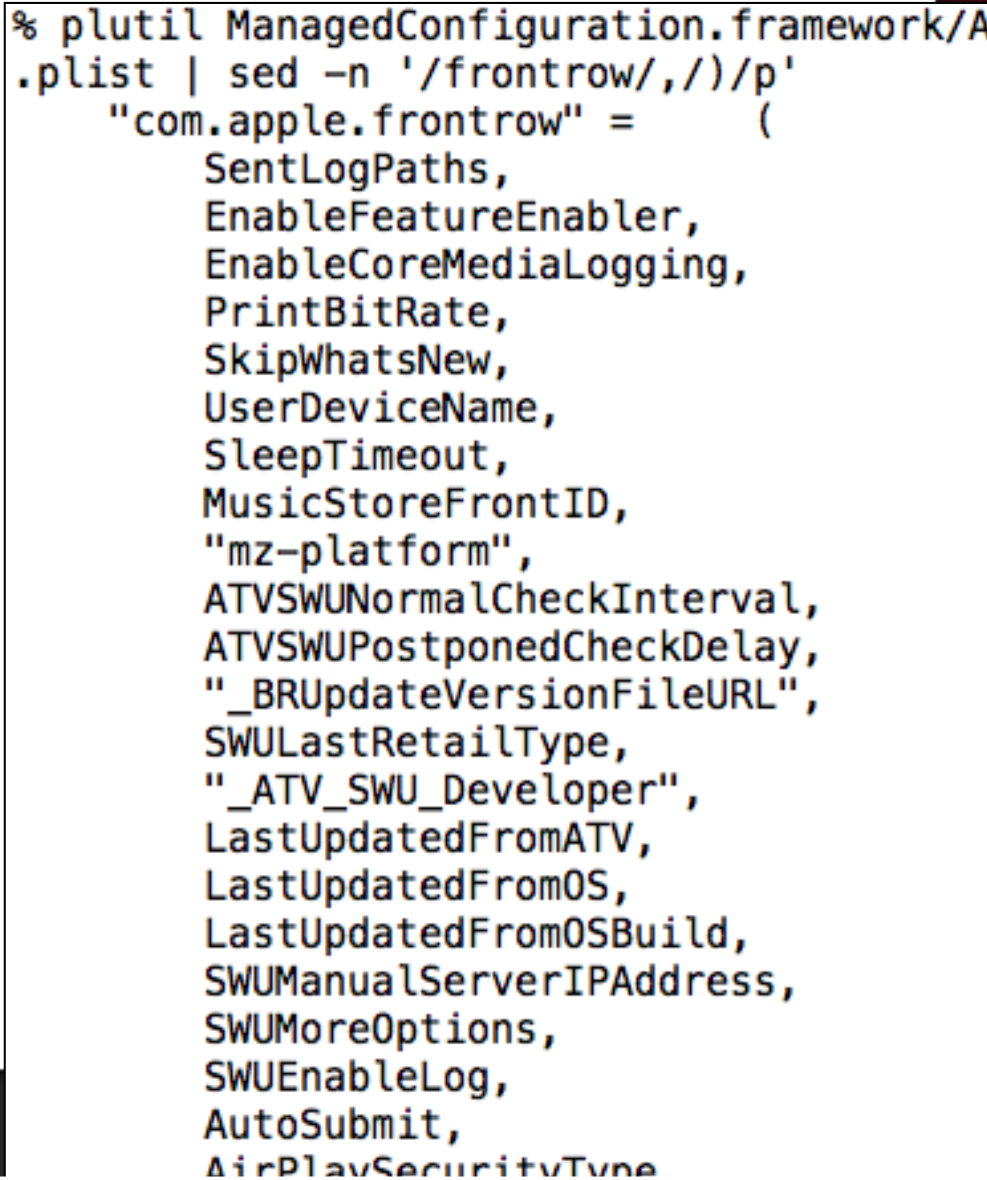
- Property list files
- Page templates, app preferences
- User credentials
- App history



```
Apple-TV:/User/Library/Application Support/Front Row/Merchants root# ls
NHL/                     hulu/                    netflix/
apollo/                  internet-add-site/       photo-stream/
apple_events/            internet-podcasts/       sample-xml/
dot-mac/                 internet-radio-stations/ show.atv/
e.mc/                    internet-youtube/        vimeo/
flagstaff/               itms/                    wsj/
flickr/                  movie-trailers-v2/
fox-news/                nba/
```

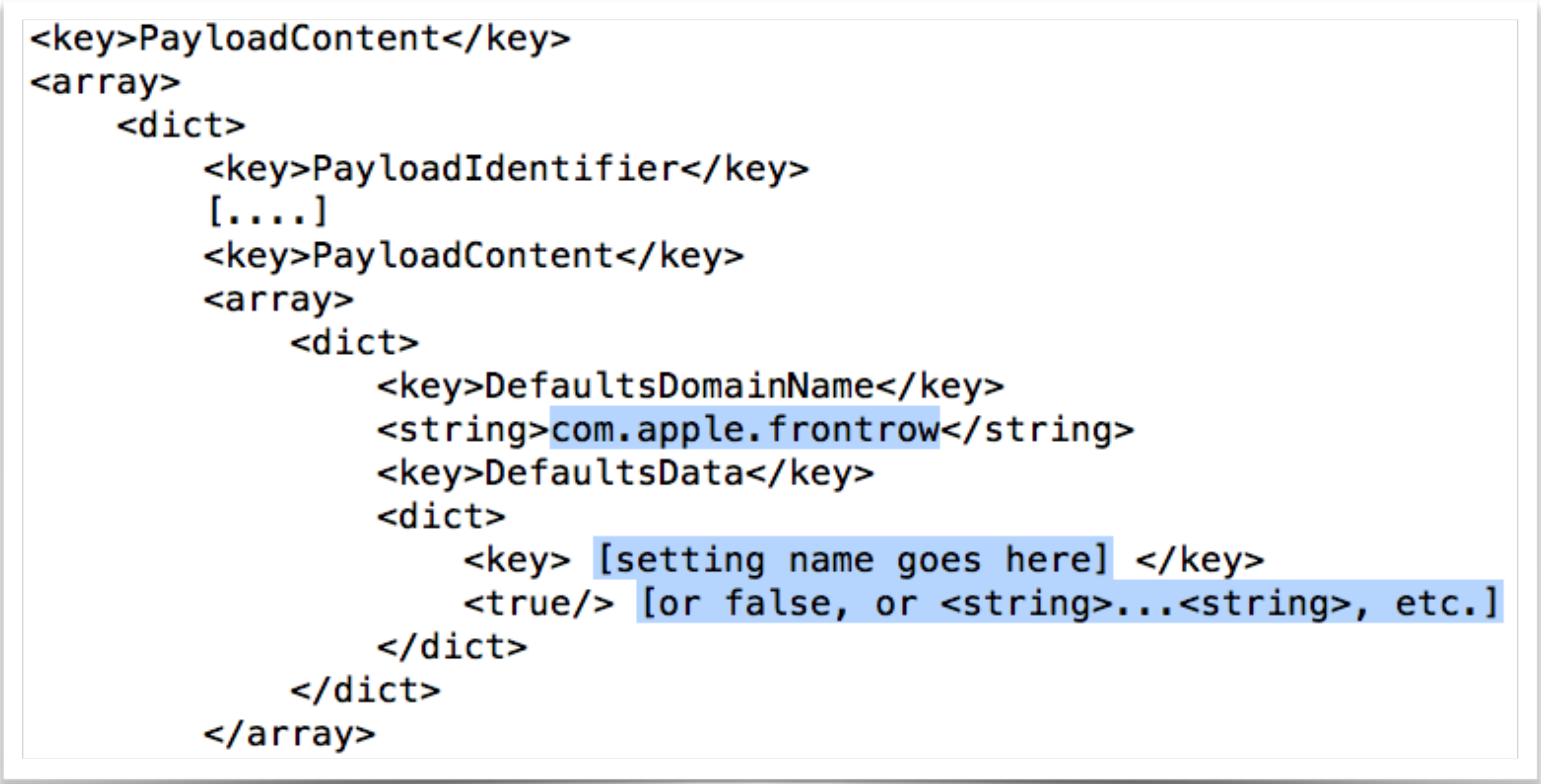
Config settings

- Managed.Configuration framework
  - –AllowedDefaults.plist
- EnableFeatureEnabler
- PrintBitRate
- UserDeviceName
- HSDiagnosticsEnabled
- EnableDPLogs



```
% plutil ManagedConfiguration.framework/A
.plist | sed -n '/frontrow/,/)/p'
    "com.apple.frontrow" =     (
        SentLogPaths,
        EnableFeatureEnabler,
        EnableCoreMediaLogging,
        PrintBitRate,
        SkipWhatsNew,
        UserDeviceName,
        SleepTimeout,
        MusicStoreFrontID,
        "mz-platform",
        ATVSWUNormalCheckInterval,
        ATVSWUPostponedCheckDelay,
        "_BRUpdateVersionFileURL",
        SWULastRetailType,
        "_ATV_SWU_Developer",
        LastUpdatedFromATV,
        LastUpdatedFromOS,
        LastUpdatedFromOSBuild,
        SWUManualServerIPAddress,
        SWUMoreOptions,
        SWUEnableLog,
        AutoSubmit,
        AirPlaySecurityType
```

Mobileconfig snippet

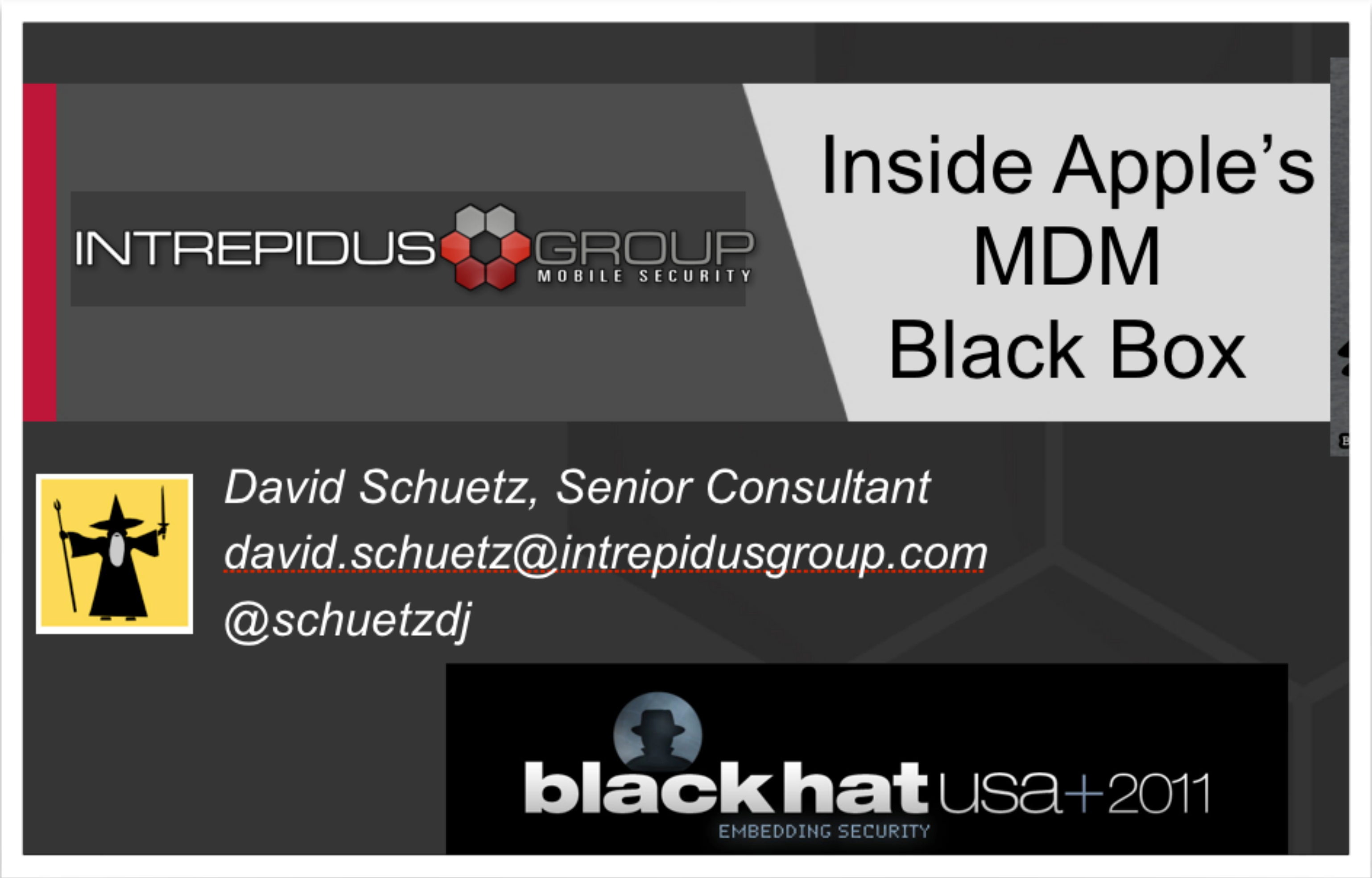


```
<key>PayloadContent</key>
<array>
    <dict>
        <key>PayloadIdentifier</key>
        [....]
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>DefaultsDomainName</key>
                <string>com.apple.frontrow</string>
                <key>DefaultsData</key>
                <dict>
                    <key> [setting name goes here] </key>
                    <true/> [or false, or <string>...<string>, etc.]
                </dict>
            </dict>
        </array>
```

Testing new settings

- Install profiles using Configurator app
  - –Power-on with USB connected
  - –Install profile
  - –Disconnect, reboot
- Lots of keys to try - this’ll take forever
- How else can we load a profile?

MDM, of course!



INTREPIDUS GROUP MOBILE SECURITY

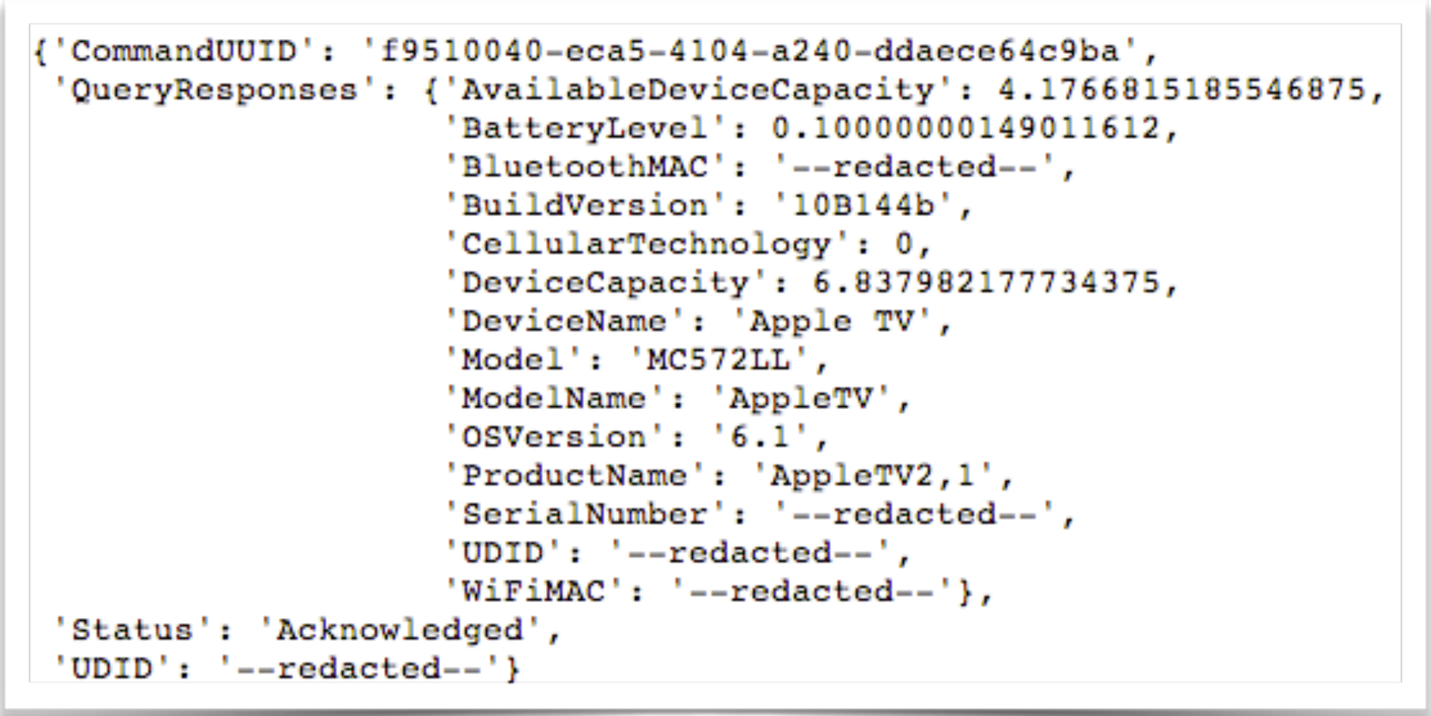
Inside Apple's
MDM
Black Box

David Schuetz, Senior Consultant
david.schuetz@intrepidusgroup.com
@schuetzdj

blackhat usa+2011
EMBEDDING SECURITY

Not supported

- Profile installed....
- ....but device wouldn't enroll
- Can manually force a poll of MDM server
- So rewrote my MDM server to fuzz profiles



```
{'CommandUUID': 'f9510040-eca5-4104-a240-ddaece64c9ba',
 'QueryResponses': {'AvailableDeviceCapacity': 4.1766815185546875,
                    'BatteryLevel': 0.10000000149011612,
                    'BluetoothMAC': '--redacted--',
                    'BuildVersion': '10B144b',
                    'CellularTechnology': 0,
                    'DeviceCapacity': 6.837982177734375,
                    'DeviceName': 'Apple TV',
                    'Model': 'MC572LL',
                    'ModelName': 'AppleTV',
                    'OSVersion': '6.1',
                    'ProductName': 'AppleTV2,1',
                    'SerialNumber': '--redacted--',
                    'UDID': '--redacted--',
                    'WiFiMAC': '--redacted--'},
 'Status': 'Acknowledged',
 'UDID': '--redacted--'}
```

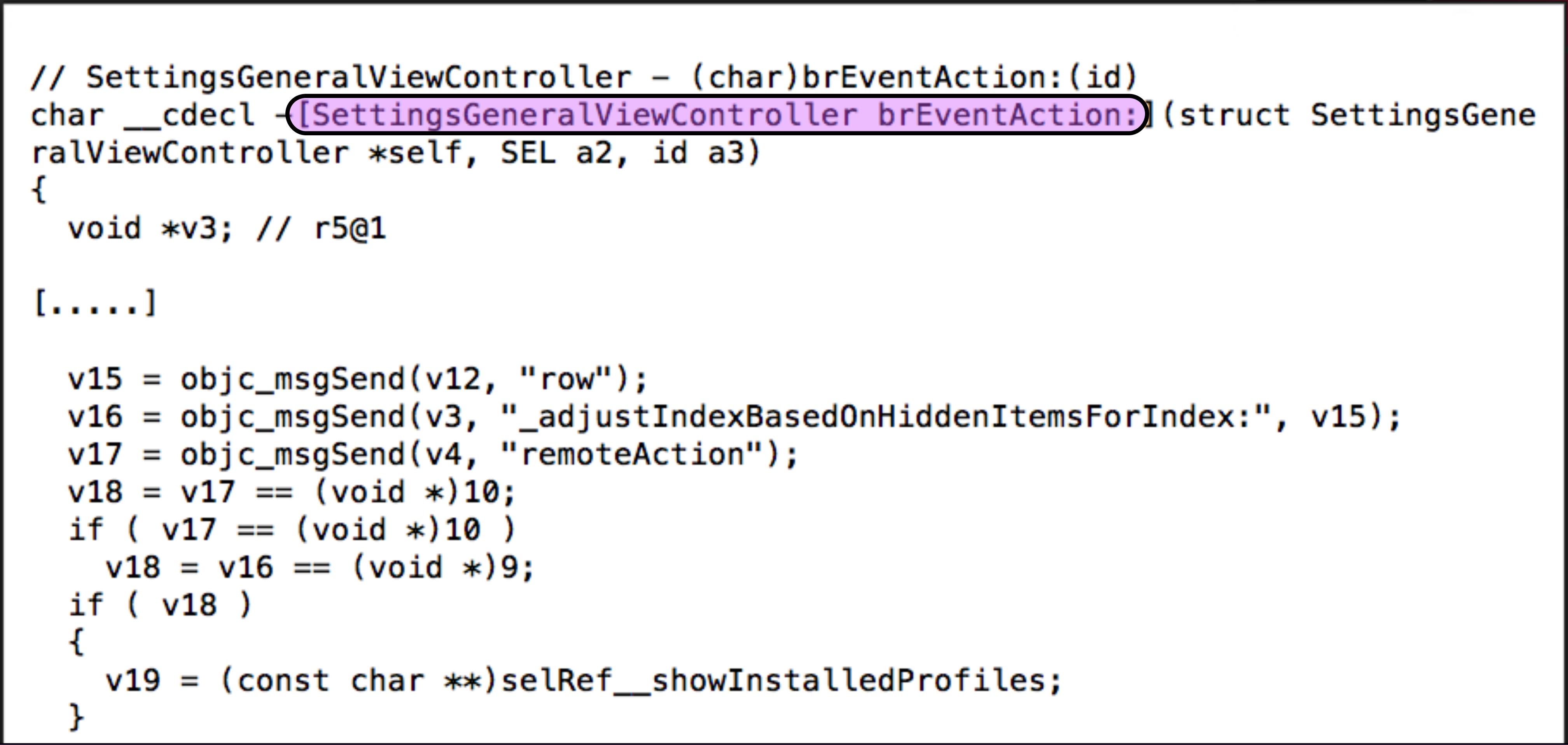
Fuzzer Engaged

- MDM sends new profile with each poll
- Changes key, iterates through values
  - That which doesn’t produce an error is interesting
- Fuzzing: Worked!
- Setting testing: Not so much.
  - AppleTV profile daemon is very forgiving
  - Hardly throws any errors
  - FreeMoviesForLife = True is accepted
    - (Doesn't do anything though)

Let's go IDA

- Dumped a 238 MB decompiled C file
- Slowed Sublime editor to a crawl
- Found some fun stuff

Hidden Remote Tricks

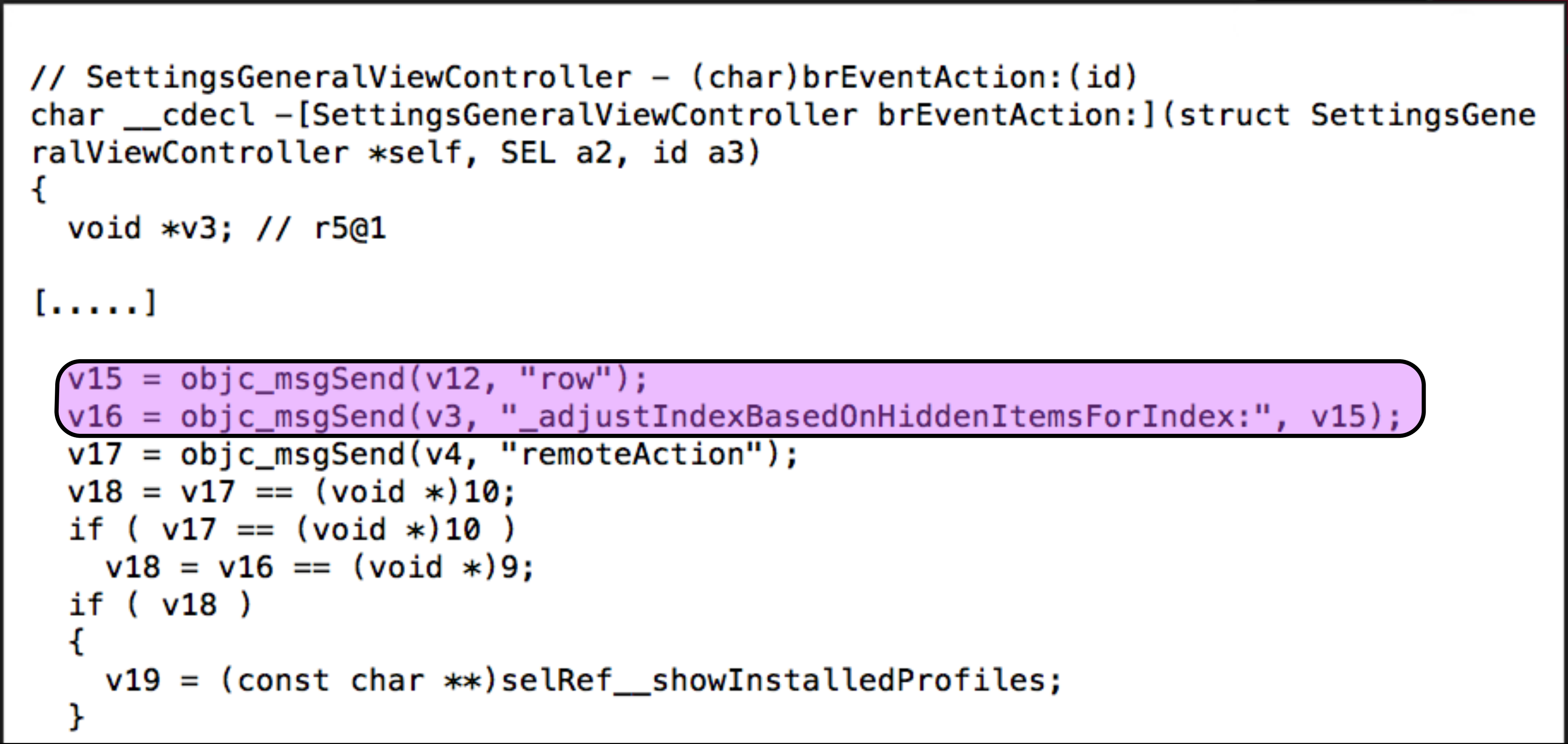


```
// SettingsGeneralViewController - (char)brEventAction:(id)
char __cdecl -[SettingsGeneralViewController brEventAction:](struct SettingsGene
ralViewController *self, SEL a2, id a3)
{
  void *v3; // r5@1

[.....]

  v15 = objc_msgSend(v12, "row");
  v16 = objc_msgSend(v3, "_adjustIndexBasedOnHiddenItemsForIndex:", v15);
  v17 = objc_msgSend(v4, "remoteAction");
  v18 = v17 == (void *)10;
  if ( v17 == (void *)10 )
    v18 = v16 == (void *)9;
  if ( v18 )
  {
    v19 = (const char **)selRef__showInstalledProfiles;
  }
```

SettingsGeneralViewController brEventAction

We’re in the General menu, and pushed a remote button

Hidden Remote Tricks

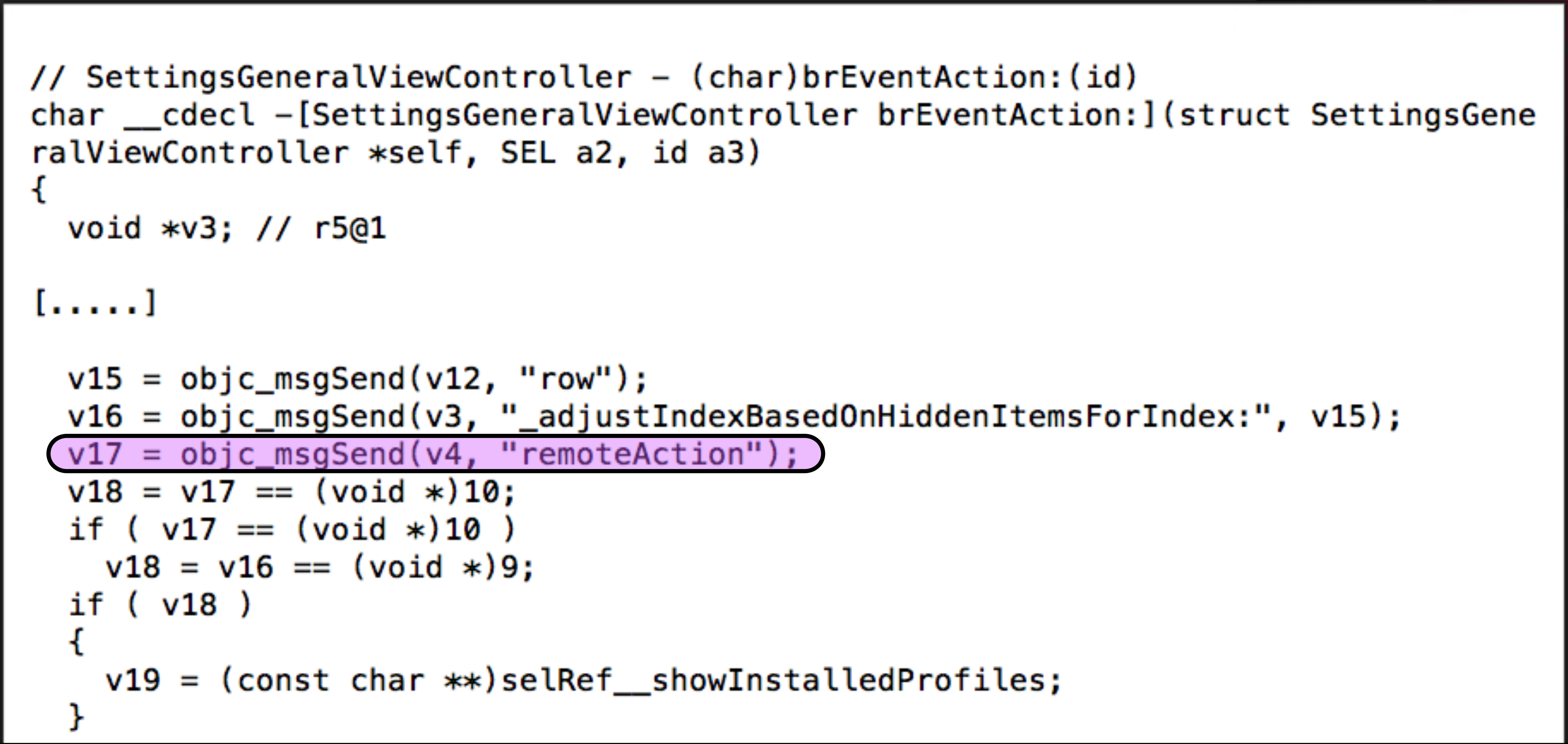


```
// SettingsGeneralViewController - (char)brEventAction:(id)
char __cdecl -[SettingsGeneralViewController brEventAction:](struct SettingsGene
ralViewController *self, SEL a2, id a3)
{
  void *v3; // r5@1

[.....]

  v15 = objc_msgSend(v12, "row");
  v16 = objc_msgSend(v3, "_adjustIndexBasedOnHiddenItemsForIndex:", v15);
  v17 = objc_msgSend(v4, "remoteAction");
  v18 = v17 == (void *)10;
  if ( v17 == (void *)10 )
    v18 = v16 == (void *)9;
  if ( v18 )
  {
    v19 = (const char **)selRef__showInstalledProfiles;
  }
```

Get the number of the item the cursor is on.

Adjust in case there are hidden menu items displayed.

Hidden Remote Tricks

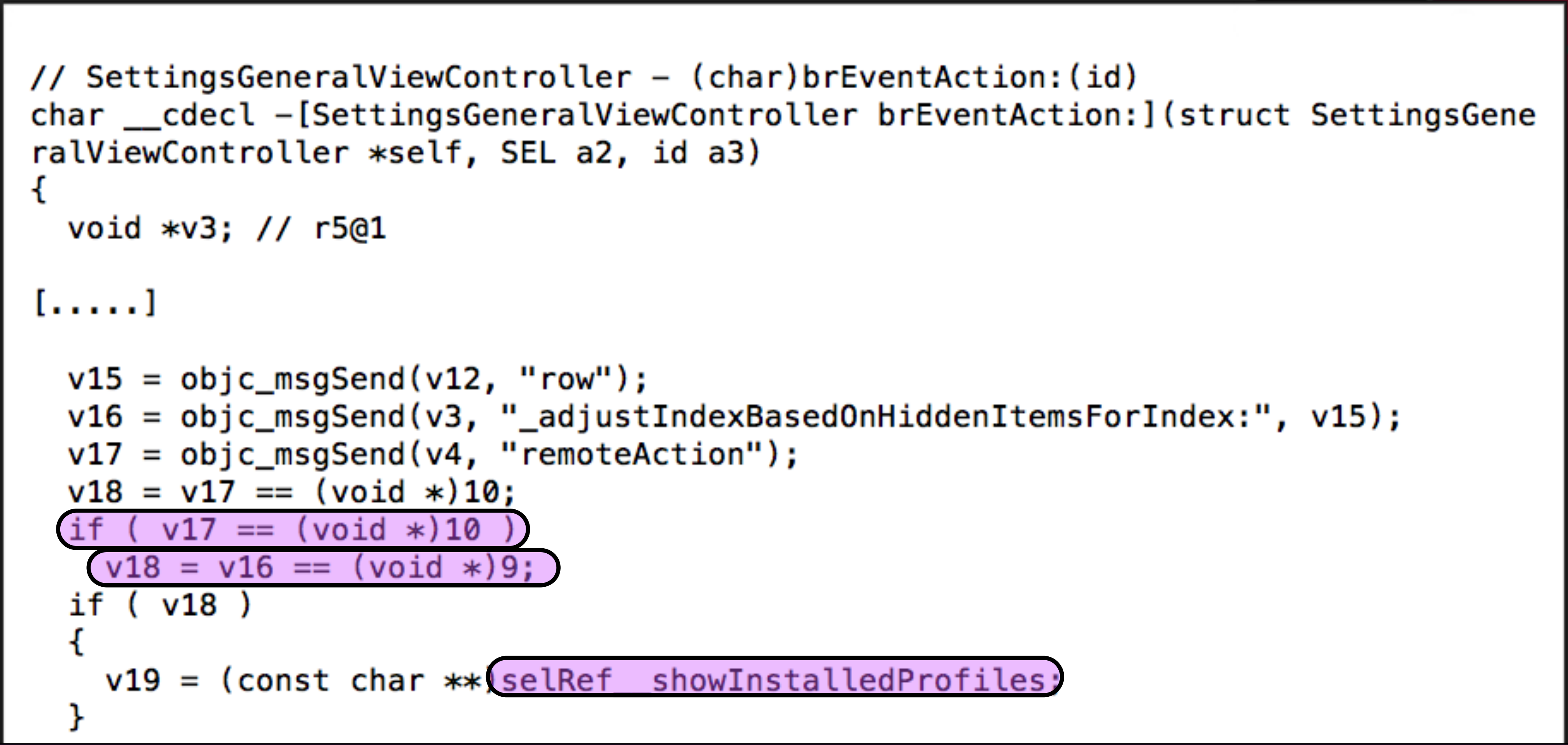


```
// SettingsGeneralViewController - (char)brEventAction:(id)
char __cdecl -[SettingsGeneralViewController brEventAction:](struct SettingsGene
ralViewController *self, SEL a2, id a3)
{
  void *v3; // r5@1

[.....]

  v15 = objc_msgSend(v12, "row");
  v16 = objc_msgSend(v3, "_adjustIndexBasedOnHiddenItemsForIndex:", v15);
  v17 = objc_msgSend(v4, "remoteAction");
  v18 = v17 == (void *)10;
  if ( v17 == (void *)10 )
    v18 = v16 == (void *)9;
  if ( v18 )
  {
    v19 = (const char **)selRef__showInstalledProfiles;
  }
```

v17 = [v4 remoteAction]

What did we just do?

Hidden Remote Tricks



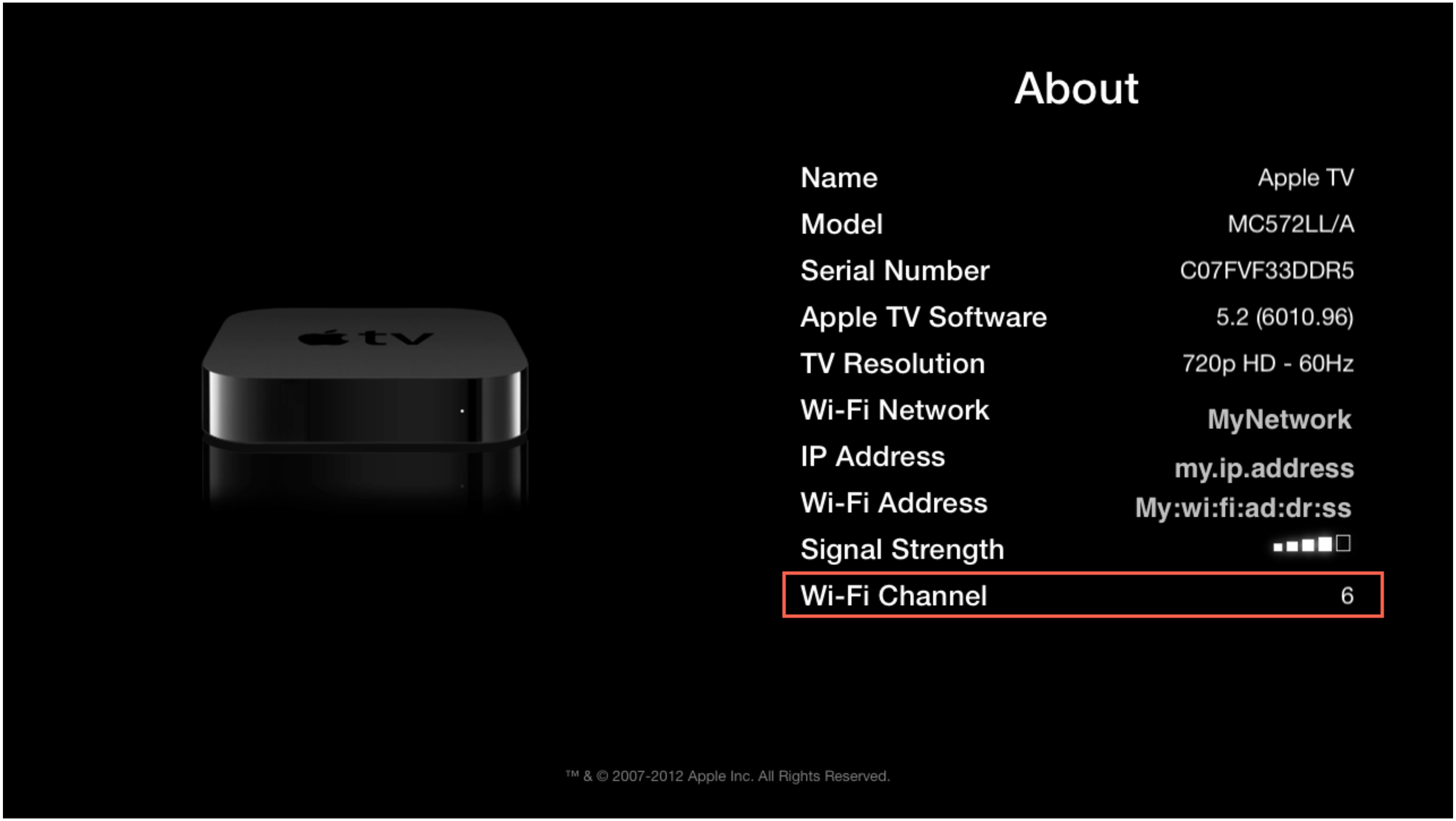
```
// SettingsGeneralViewController - (char)brEventAction:(id)
char __cdecl -[SettingsGeneralViewController brEventAction:](struct SettingsGene
ralViewController *self, SEL a2, id a3)
{
  void *v3; // r5@1

[.....]

  v15 = objc_msgSend(v12, "row");
  v16 = objc_msgSend(v3, "_adjustIndexBasedOnHiddenItemsForIndex:", v15);
  v17 = objc_msgSend(v4, "remoteAction");
  v18 = v17 == (void *)10;
  if ( v17 == (void *)10 )
    v18 = v16 == (void *)9;
  if ( v18 )
  {
    v19 = (const char **)selRef__showInstalledProfiles;
  }
```

if v17 (action) = 10 (“Play” button) ... and
v18 (current row) = 9 (“Send data to Apple” item)...
... then go to the “showInstalledProfiles” screen.

Hidden Remote Tricks

- SettingsAboutViewController
  - Using WiFi and remoteAction=3
    - toggleWiFiDetails
- SettingsGeneralViewController
  - Highlighted “About” item
    - remoteActions: 7, 7, 6, select: toggleRetailMode
  - Highlighted “Send Data to Apple” item
    - remote action 7: toggleShowInverseDeviceID
    - remote action 10: showInstalledProfiles

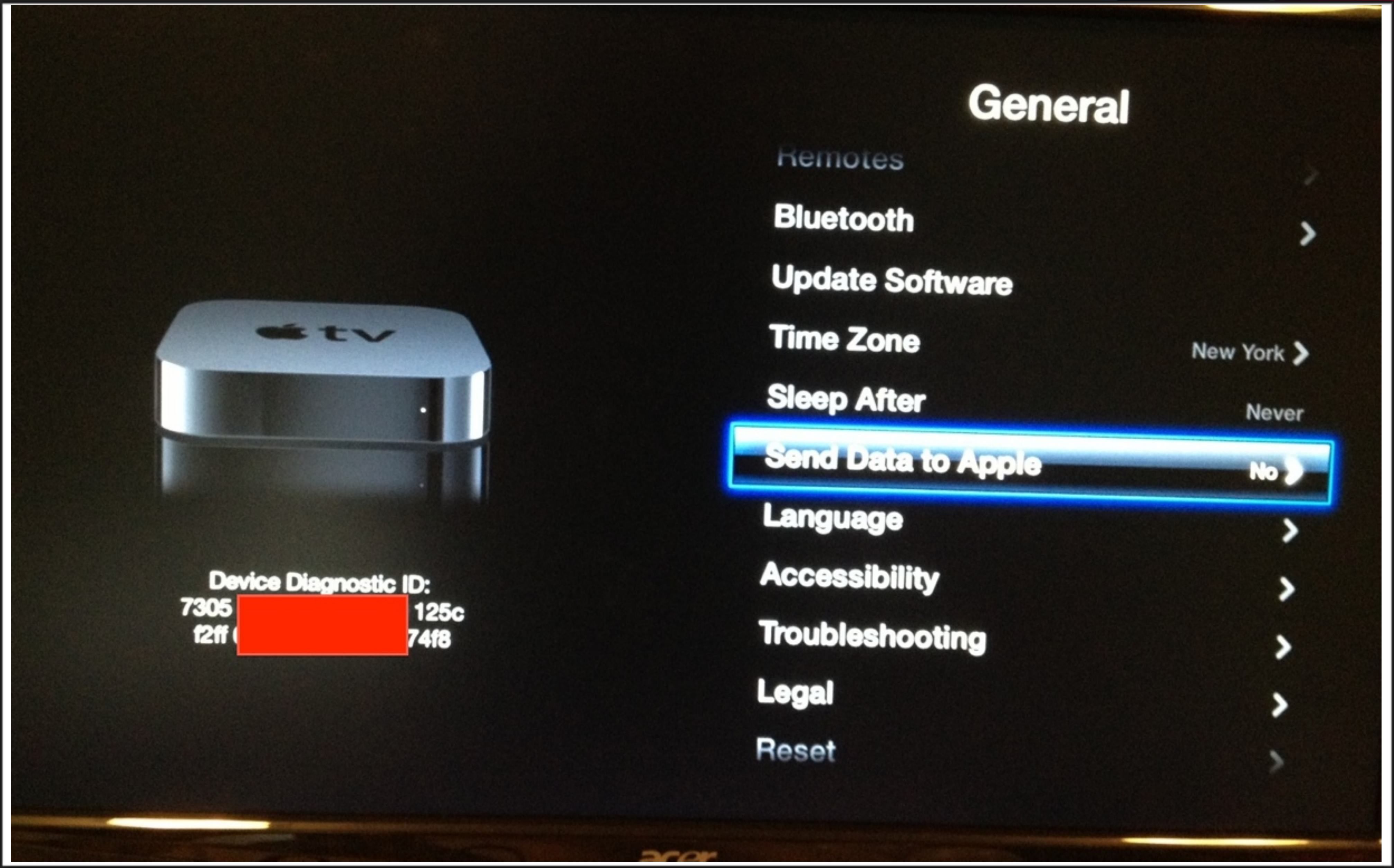
Up-arrow: Channel/BSSID



About

Name	Apple TV
Model	MC572LL/A
Serial Number	C07FVF33DDR5
Apple TV Software	5.2 (6010.96)
TV Resolution	720p HD - 60Hz
Wi-Fi Network	MyNetwork
IP Address	my.ip.address
Wi-Fi Address	My:wi:fi:ad:dr:ss
Signal Strength	▪▪■■□
Wi-Fi Channel	6

Right arrow: Diag ID



General

Remotes

Bluetooth

Update Software

Time Zone New York

Sleep After Never

Send Data to Apple No

Language

Accessibility

Troubleshooting

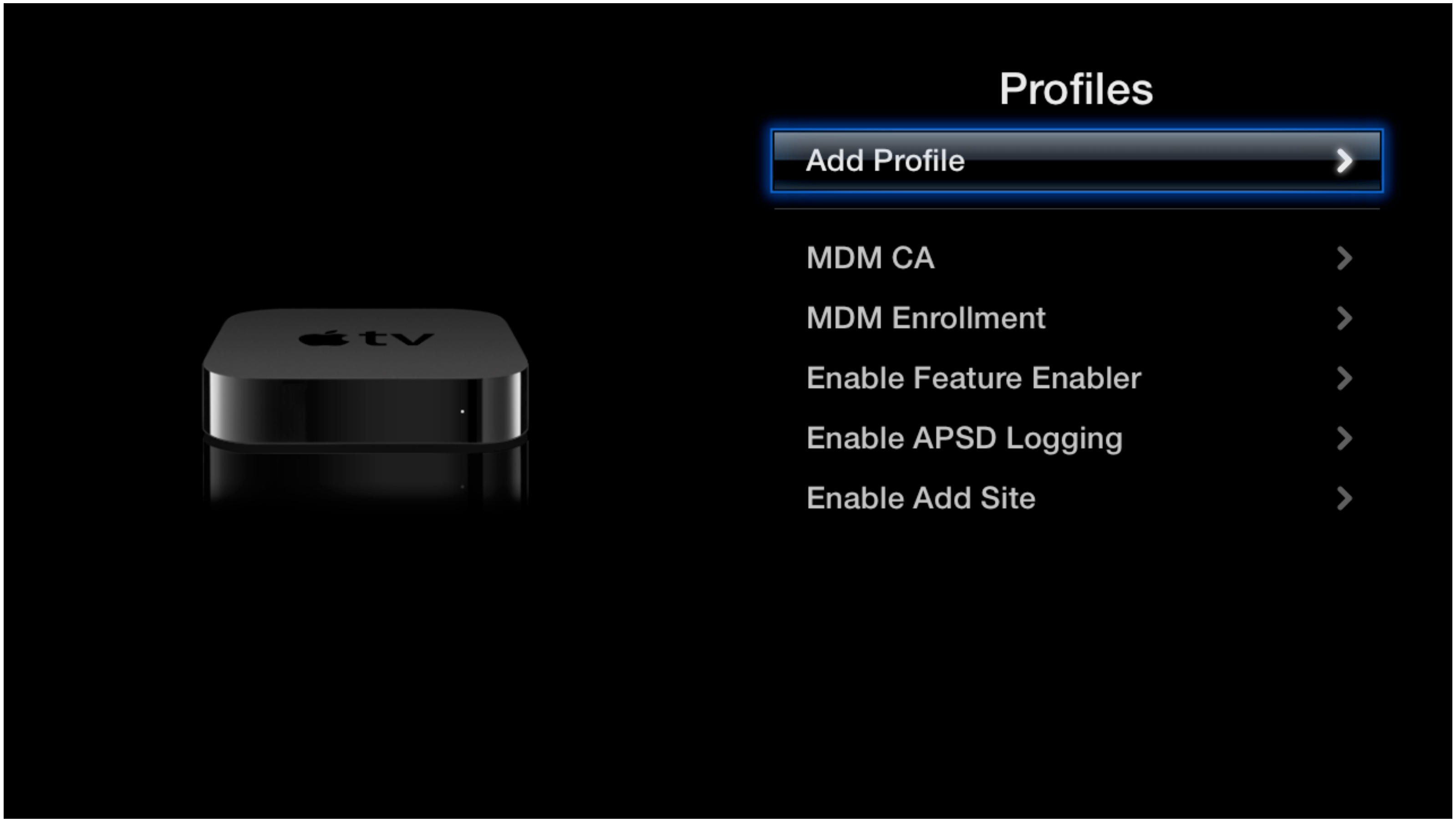
Legal

Reset

Device Diagnostic ID:
7305 [redacted] 125c
f2ff 74f8

Add Profile

- Highlight “Send Data to Apple”
- Hit “Play”



Profiles

Add Profile

MDM CA

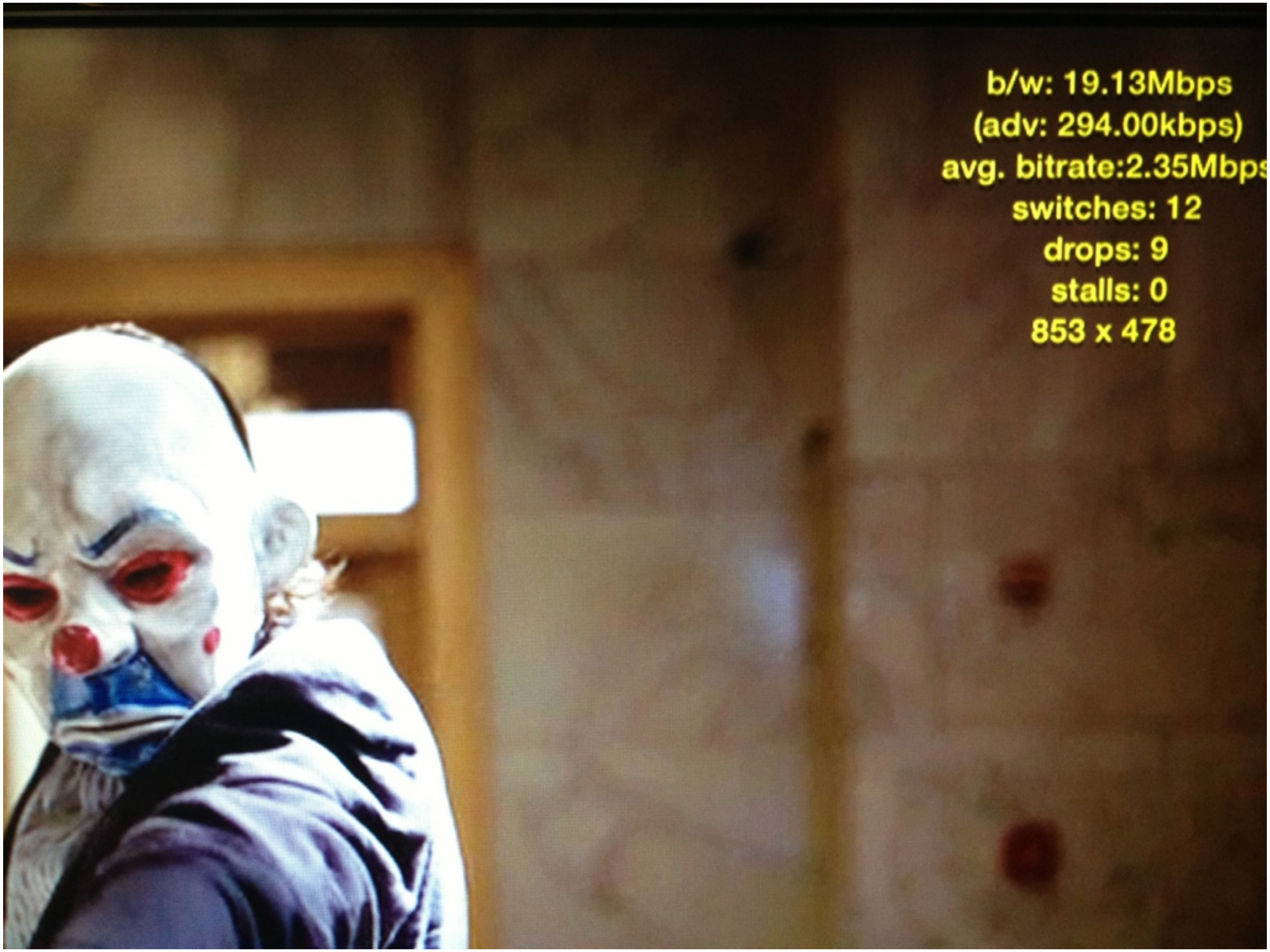
MDM Enrollment

Enable Feature Enabler

Enable APSD Logging

Enable Add Site

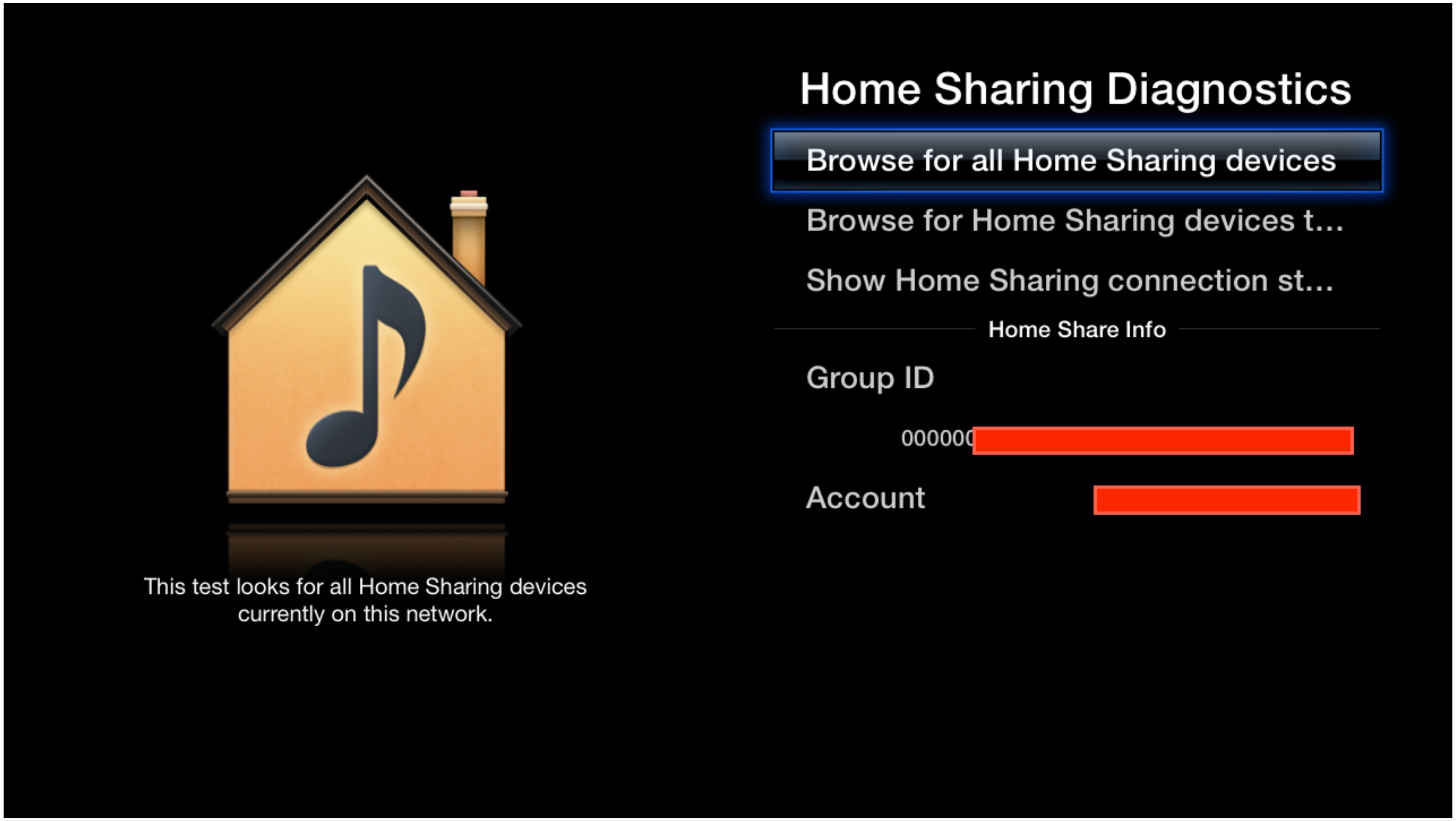
PrintBitRate = True



```
b/w: 19.13Mbps
(adv: 294.00kbps)
avg. bitrate:2.35Mbps
switches: 12
drops: 9
stalls: 0
853 x 478
```

Home Sharing Diagnostics

- HSDiagnosticsEnabled = True
- Menu appears in “Computers”



Home Sharing Diagnostics

Browse for all Home Sharing devices

Browse for Home Sharing devices t…

Show Home Sharing connection st…

Home Share Info

Group ID

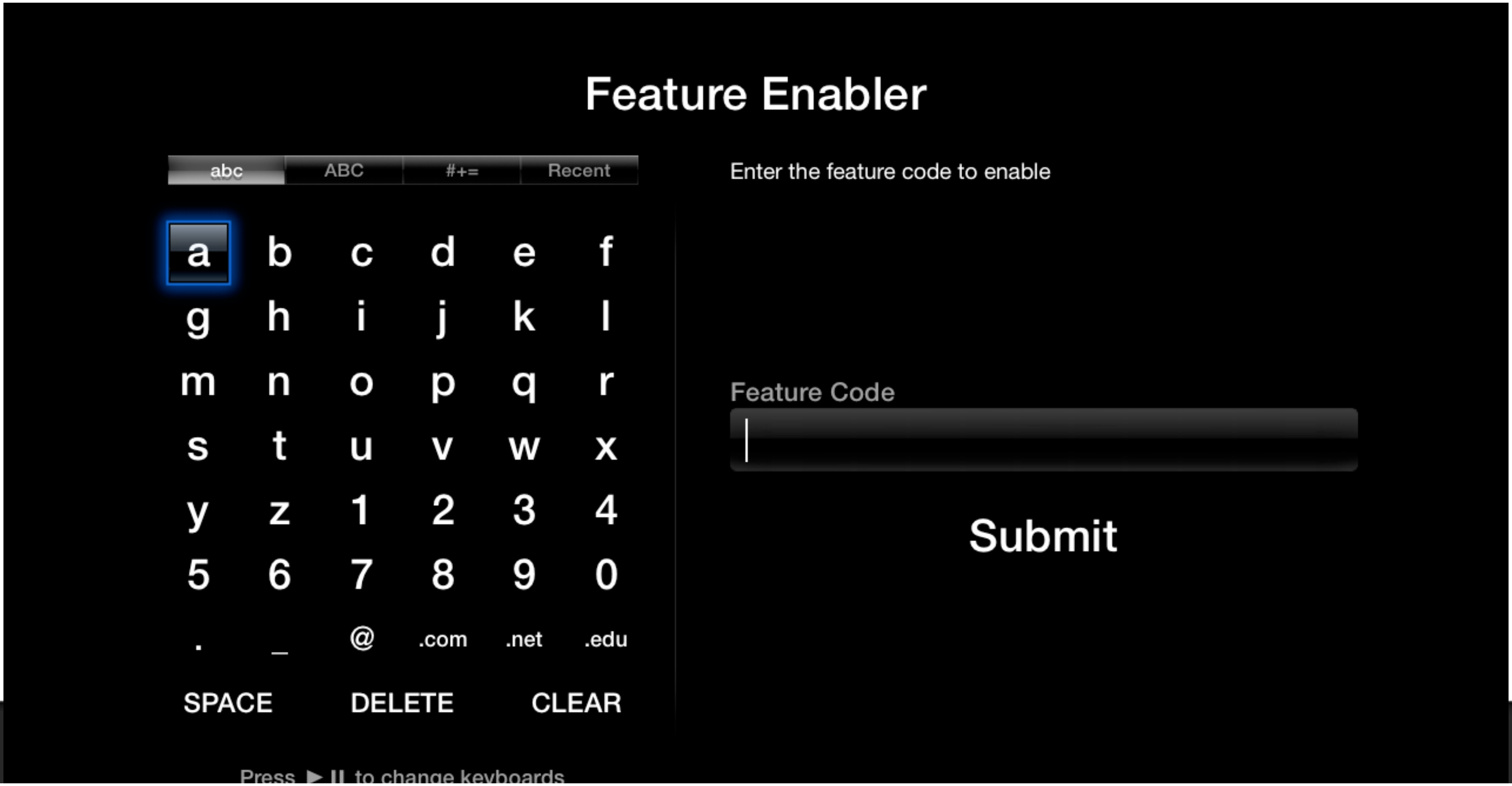
[redacted]

Account [redacted]

This test looks for all Home Sharing devices currently on this network.

EnableFeatureEnabler

- Some channels have a “Feature” code
- Maybe to preview new official channels?



Feature Enabler

Enter the feature code to enable

Feature Code

Press ▶ II to change keyboards

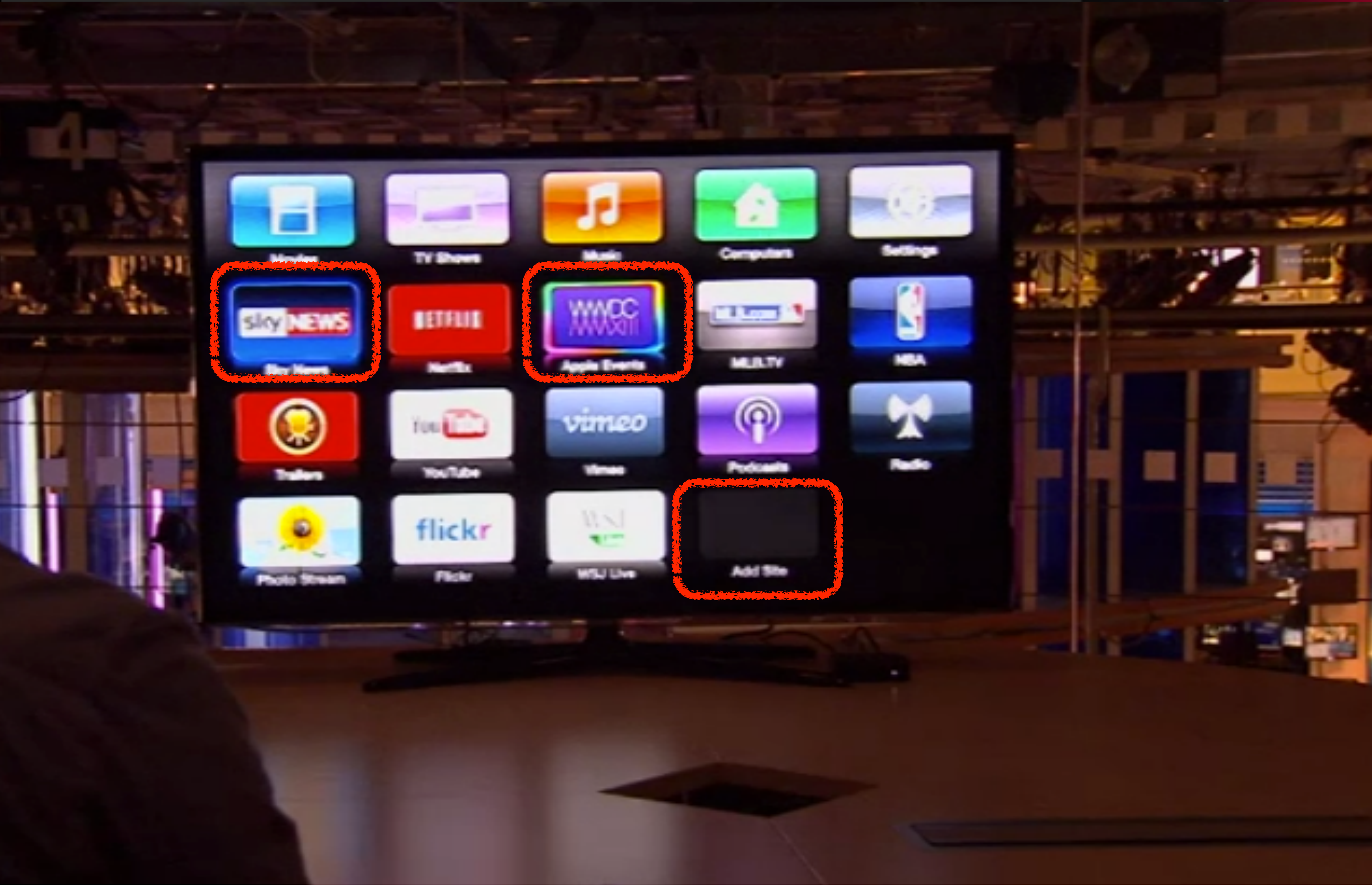
MITM Proxy

- Build a Wi-Fi configuration profile
  - iPhone Configuration Utility or Configurator
- Include an HTTP proxy
- Install (while still on wired ethernet)
- Unplug ethernet, now you’re MITM
- iTunes links break though
  - Tried bypassing certificate pinning
  - Haven’t yet tried fake “*.apple.com” certs
  - Breaks main screen -- hence load-and-switch

EnableAddSite

- But what does EnableAddSite do?
- Secret started leaking out:
  - SkyNews video from June 19
  - Announcing AppleTV app
  - Shows AppleTV screen, with:
    - WWDC app (so filmed in early to mid June)
    - SkyNews app
    - Something else interesting...

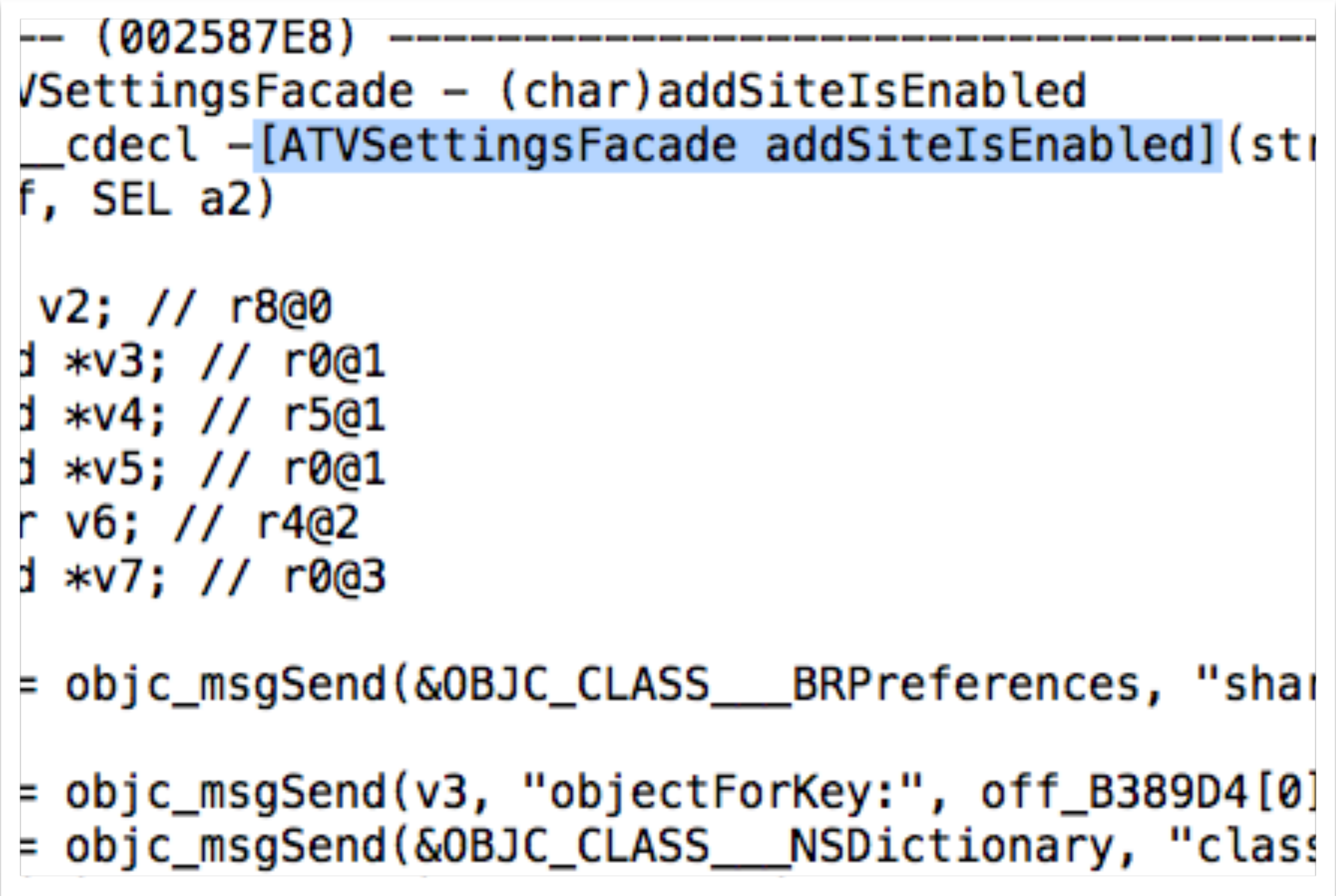
Sky news image



EnableAddSite

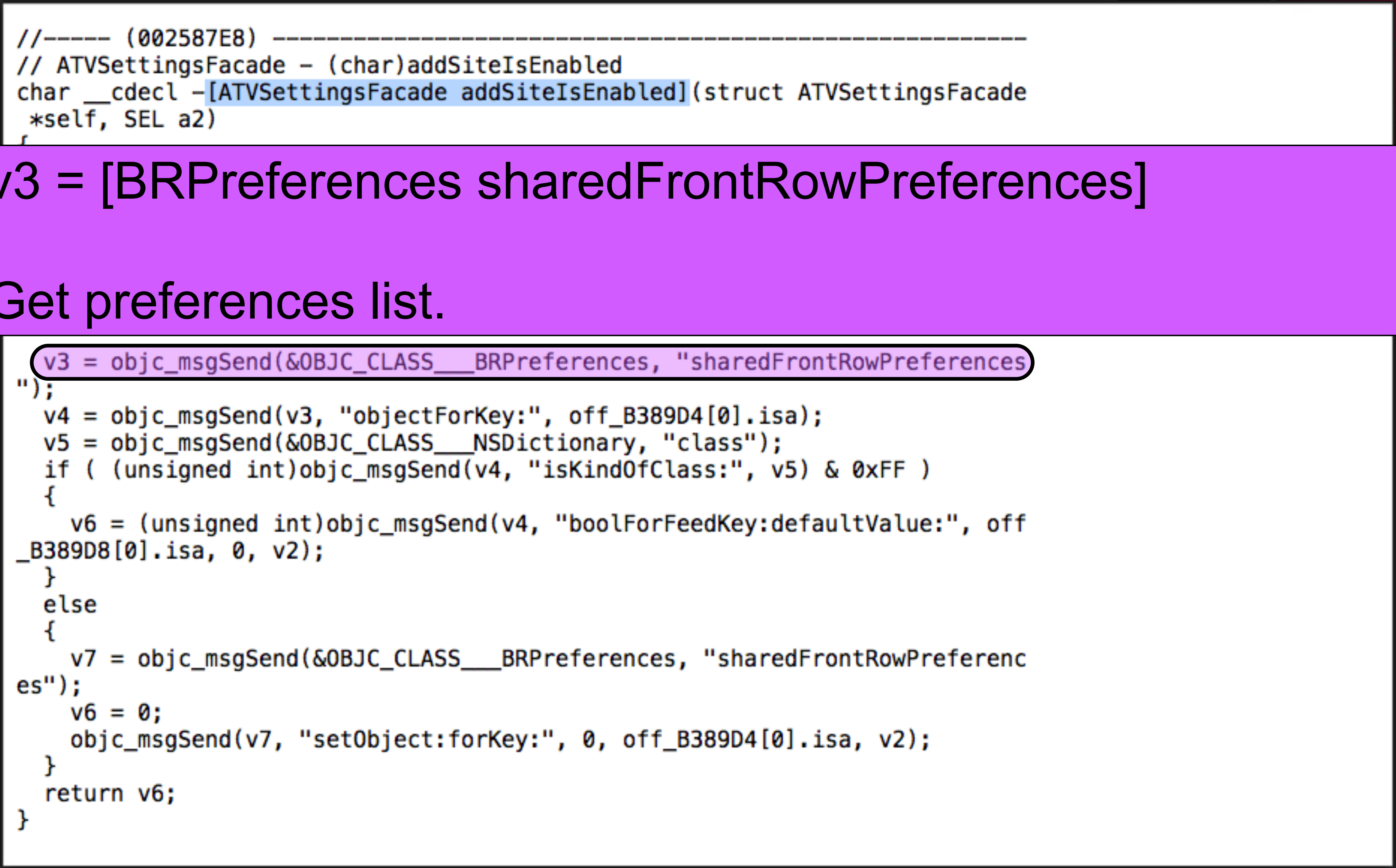
- Key by itself doesn’t work
- Something else is happening
- Where is the code that tests for that key...
- ...what could it be named.....?

Oh. There it is.



```
-- (002587E8) ------------------------------------
VSettingsFacade - (char)addSiteIsEnabled
__cdecl -[ATVSettingsFacade addSiteIsEnabled](str
f, SEL a2)

 v2; // r8@0
d *v3; // r0@1
d *v4; // r5@1
d *v5; // r0@1
r v6; // r4@2
d *v7; // r0@3

= objc_msgSend(&OBJC_CLASS___BRPreferences, "shar

= objc_msgSend(v3, "objectForKey:", off_B389D4[0]
= objc_msgSend(&OBJC_CLASS___NSDictionary, "class
```

What does it MEAN?!?



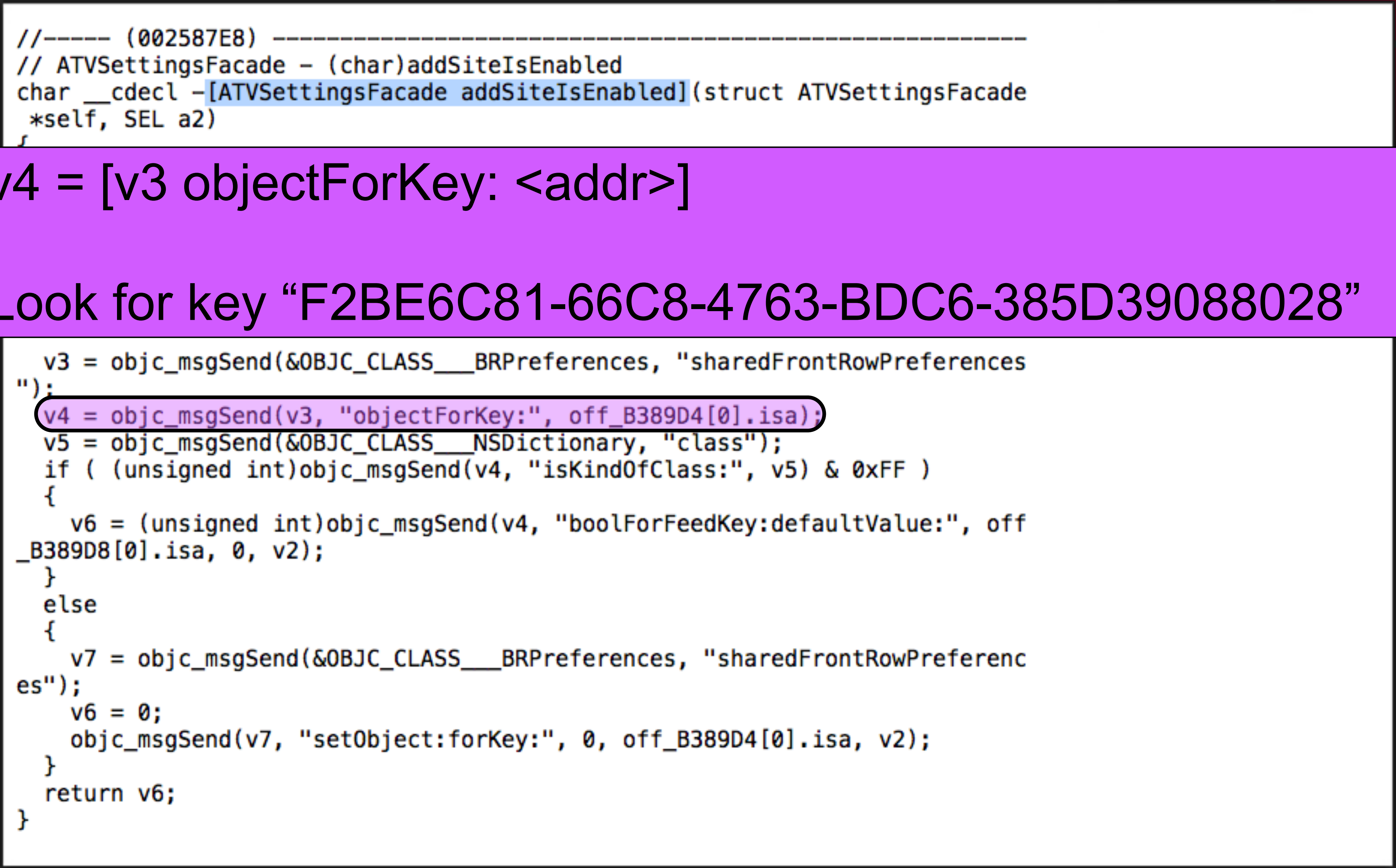
```
//----- (002587E8) --------------------------------------------------------
// ATVSettingsFacade - (char)addSiteIsEnabled
char __cdecl -[ATVSettingsFacade addSiteIsEnabled](struct ATVSettingsFacade
 *self, SEL a2)
{
```

v3 = [BRPreferences sharedFrontRowPreferences]

Get preferences list.

```
  v3 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferences
");
  v4 = objc_msgSend(v3, "objectForKey:", off_B389D4[0].isa);
  v5 = objc_msgSend(&OBJC_CLASS___NSDictionary, "class");
  if ( (unsigned int)objc_msgSend(v4, "isKindOfClass:", v5) & 0xFF )
  {
    v6 = (unsigned int)objc_msgSend(v4, "boolForFeedKey:defaultValue:", off
_B389D8[0].isa, 0, v2);
  }
  else
  {
    v7 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferenc
es");
    v6 = 0;
    objc_msgSend(v7, "setObject:forKey:", 0, off_B389D4[0].isa, v2);
  }
  return v6;
}
```

What does it MEAN?!?



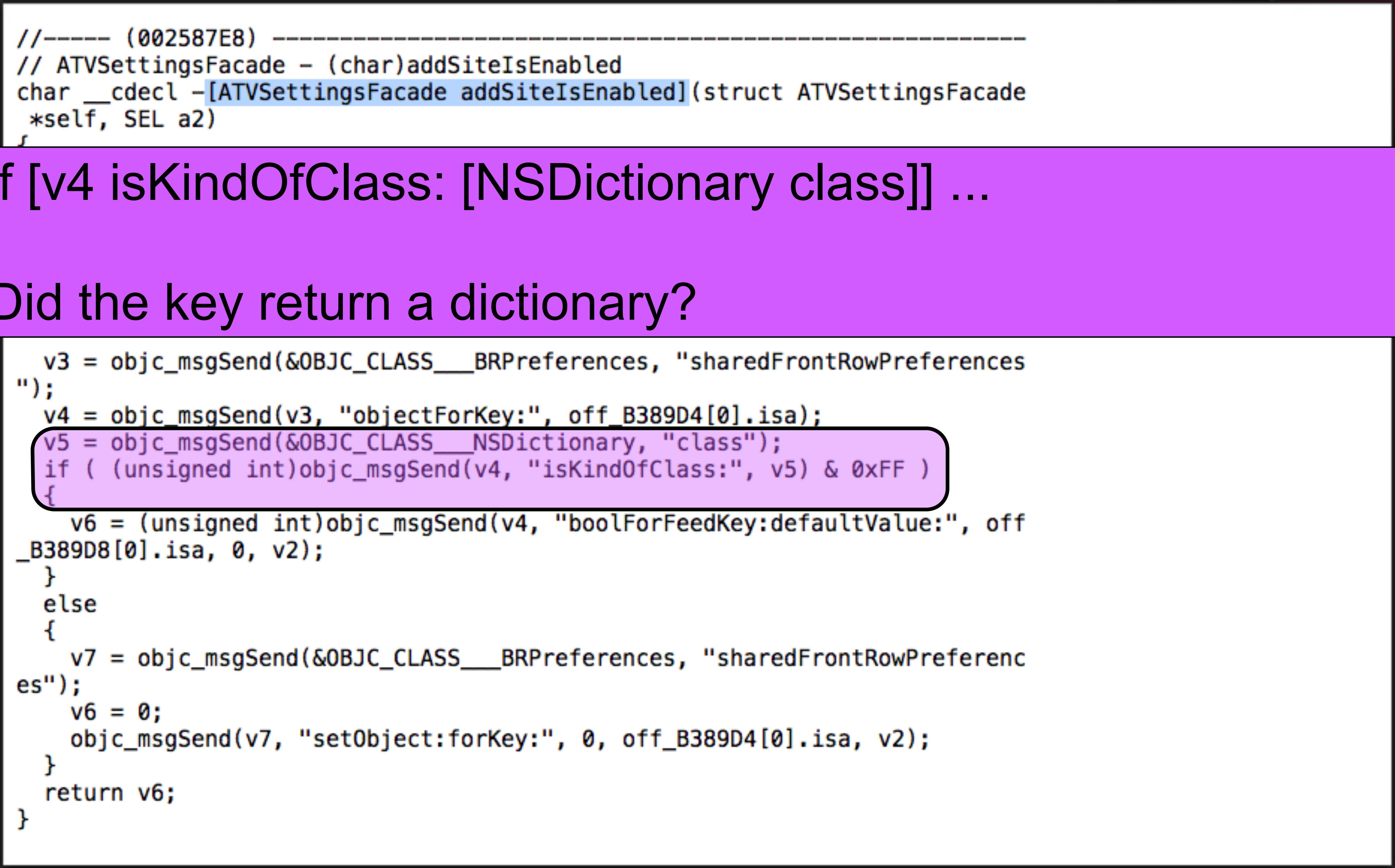
```
//----- (002587E8) --------------------------------------------------------
// ATVSettingsFacade - (char)addSiteIsEnabled
char __cdecl -[ATVSettingsFacade addSiteIsEnabled](struct ATVSettingsFacade
 *self, SEL a2)
{
```

v4 = [v3 objectForKey: <addr>]

Look for key “F2BE6C81-66C8-4763-BDC6-385D39088028”

```
  v3 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferences
");
  v4 = objc_msgSend(v3, "objectForKey:", off_B389D4[0].isa);
  v5 = objc_msgSend(&OBJC_CLASS___NSDictionary, "class");
  if ( (unsigned int)objc_msgSend(v4, "isKindOfClass:", v5) & 0xFF )
  {
    v6 = (unsigned int)objc_msgSend(v4, "boolForFeedKey:defaultValue:", off
_B389D8[0].isa, 0, v2);
  }
  else
  {
    v7 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferenc
es");
    v6 = 0;
    objc_msgSend(v7, "setObject:forKey:", 0, off_B389D4[0].isa, v2);
  }
  return v6;
}
```

What does it MEAN?!?



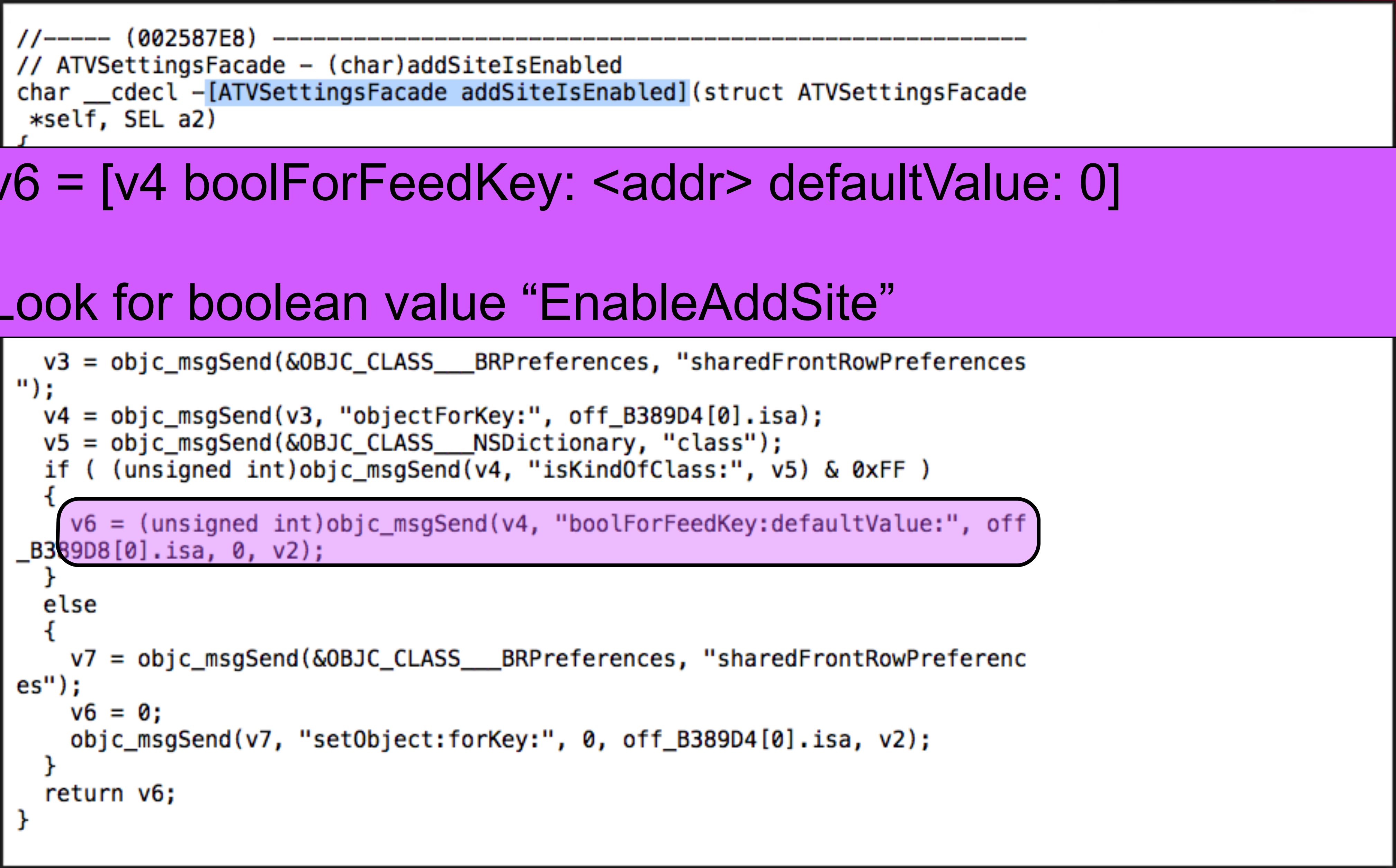
```
//----- (002587E8) --------------------------------------------------------
// ATVSettingsFacade - (char)addSiteIsEnabled
char __cdecl -[ATVSettingsFacade addSiteIsEnabled](struct ATVSettingsFacade
 *self, SEL a2)
{
```

if [v4 isKindOfClass: [NSDictionary class]] ...

Did the key return a dictionary?

```
  v3 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferences
");
  v4 = objc_msgSend(v3, "objectForKey:", off_B389D4[0].isa);
  v5 = objc_msgSend(&OBJC_CLASS___NSDictionary, "class");
  if ( (unsigned int)objc_msgSend(v4, "isKindOfClass:", v5) & 0xFF )
  {
    v6 = (unsigned int)objc_msgSend(v4, "boolForFeedKey:defaultValue:", off
_B389D8[0].isa, 0, v2);
  }
  else
  {
    v7 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferenc
es");
    v6 = 0;
    objc_msgSend(v7, "setObject:forKey:", 0, off_B389D4[0].isa, v2);
  }
  return v6;
}
```

What does it MEAN?!?



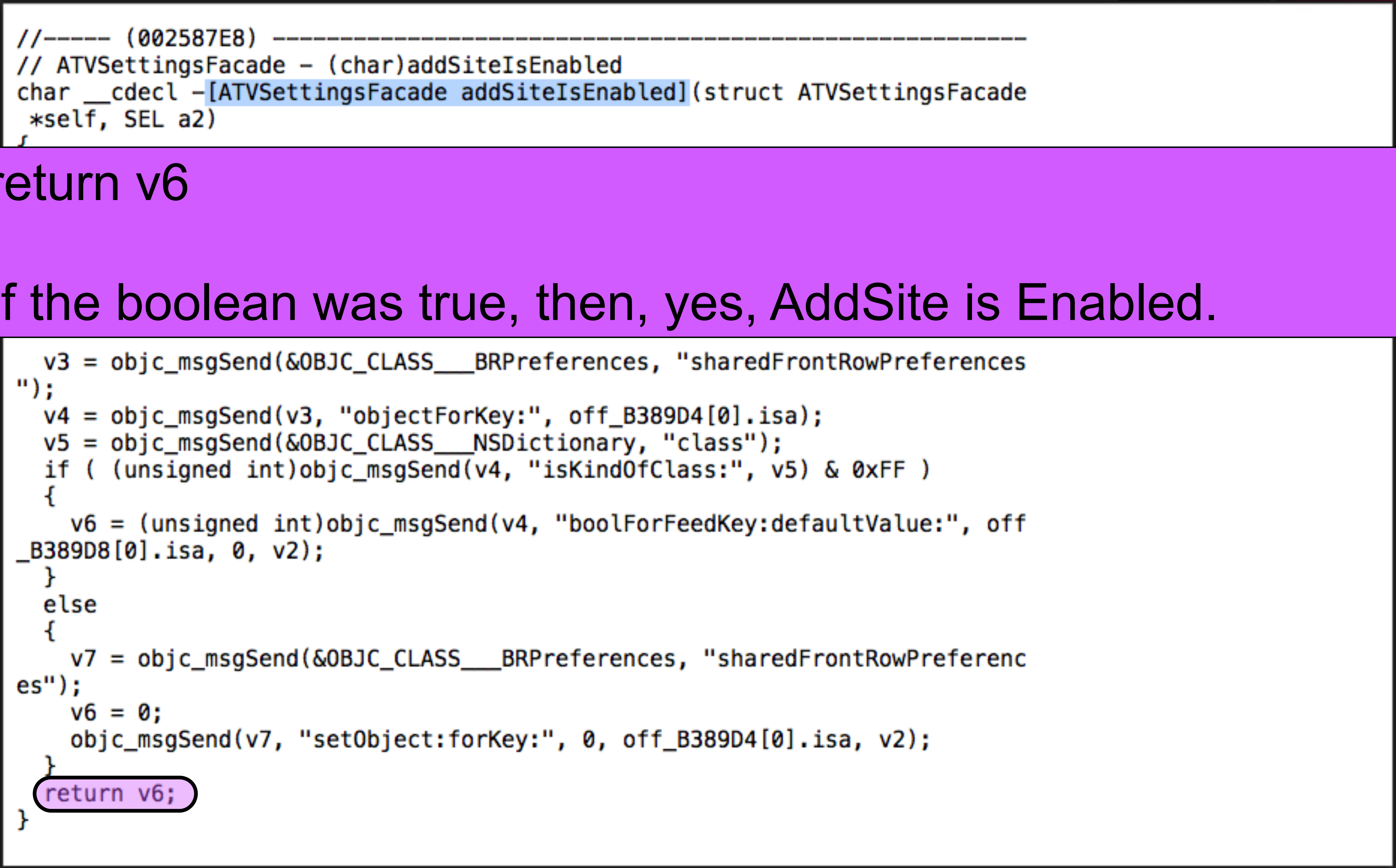
```
//----- (002587E8) --------------------------------------------------------
// ATVSettingsFacade - (char)addSiteIsEnabled
char __cdecl -[ATVSettingsFacade addSiteIsEnabled](struct ATVSettingsFacade
 *self, SEL a2)
{
```

v6 = [v4 boolForFeedKey: <addr> defaultValue: 0]

Look for boolean value “EnableAddSite”

```
  v3 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferences
");
  v4 = objc_msgSend(v3, "objectForKey:", off_B389D4[0].isa);
  v5 = objc_msgSend(&OBJC_CLASS___NSDictionary, "class");
  if ( (unsigned int)objc_msgSend(v4, "isKindOfClass:", v5) & 0xFF )
  {
    v6 = (unsigned int)objc_msgSend(v4, "boolForFeedKey:defaultValue:", off
_B389D8[0].isa, 0, v2);
  }
  else
  {
    v7 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferenc
es");
    v6 = 0;
    objc_msgSend(v7, "setObject:forKey:", 0, off_B389D4[0].isa, v2);
  }
  return v6;
}
```

What does it MEAN?!?



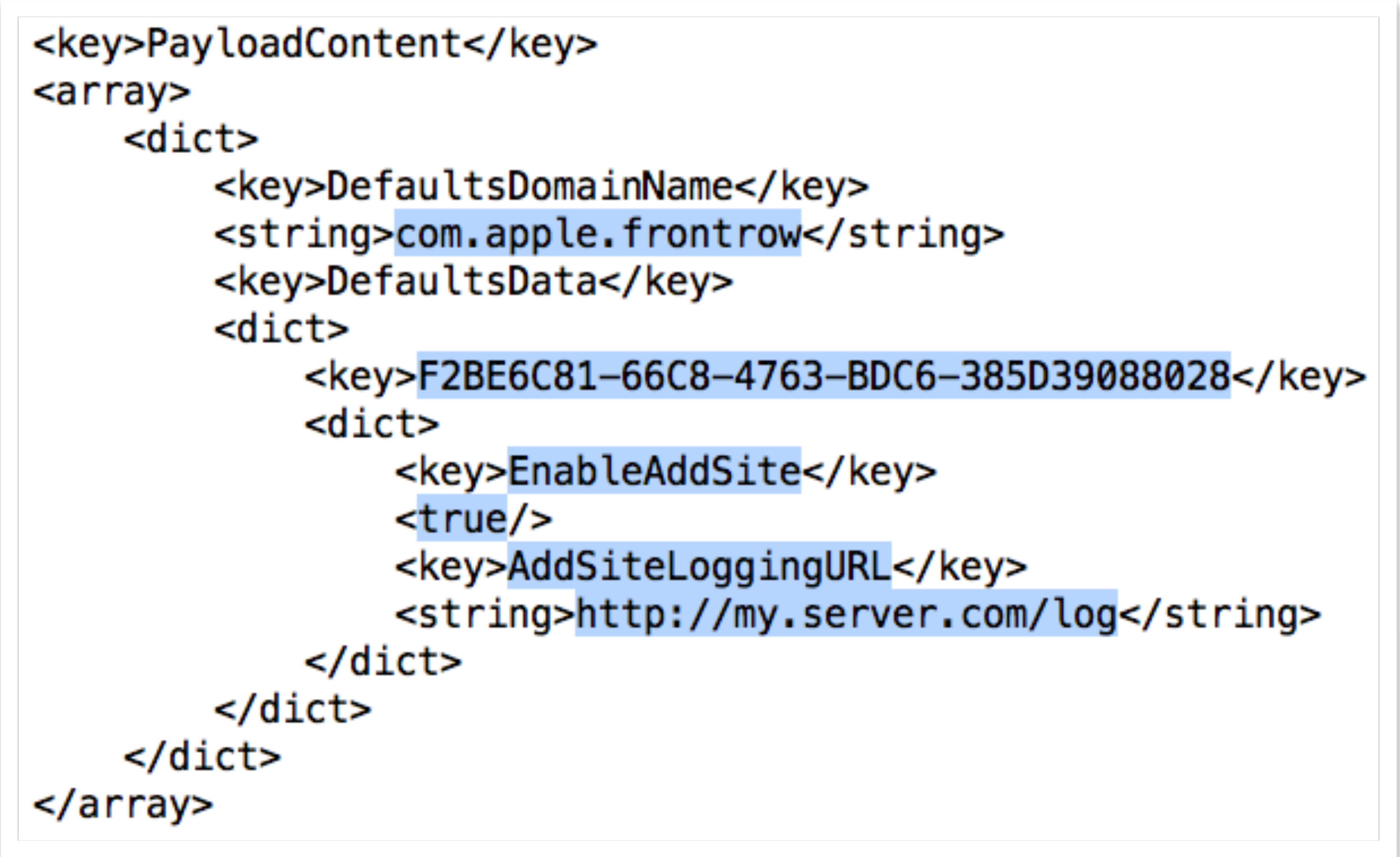
```
//----- (002587E8) --------------------------------------------------------
// ATVSettingsFacade - (char)addSiteIsEnabled
char __cdecl -[ATVSettingsFacade addSiteIsEnabled](struct ATVSettingsFacade
 *self, SEL a2)
{
```

return v6

If the boolean was true, then, yes, AddSite is Enabled.

```
  v3 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferences
");
  v4 = objc_msgSend(v3, "objectForKey:", off_B389D4[0].isa);
  v5 = objc_msgSend(&OBJC_CLASS___NSDictionary, "class");
  if ( (unsigned int)objc_msgSend(v4, "isKindOfClass:", v5) & 0xFF )
  {
    v6 = (unsigned int)objc_msgSend(v4, "boolForFeedKey:defaultValue:", off
_B389D8[0].isa, 0, v2);
  }
  else
  {
    v7 = objc_msgSend(&OBJC_CLASS___BRPreferences, "sharedFrontRowPreferenc
es");
    v6 = 0;
    objc_msgSend(v7, "setObject:forKey:", 0, off_B389D4[0].isa, v2);
  }
  return v6;
}
```

Mobileconfig snippet



```
<key>PayloadContent</key>
<array>
    <dict>
        <key>DefaultsDomainName</key>
        <string>com.apple.frontrow</string>
        <key>DefaultsData</key>
        <dict>
            <key>F2BE6C81-66C8-4763-BDC6-385D39088028</key>
            <dict>
                <key>EnableAddSite</key>
                <true/>
                <key>AddSiteLoggingURL</key>
                <string>http://my.server.com/log</string>
            </dict>
        </dict>
    </dict>
</array>
```

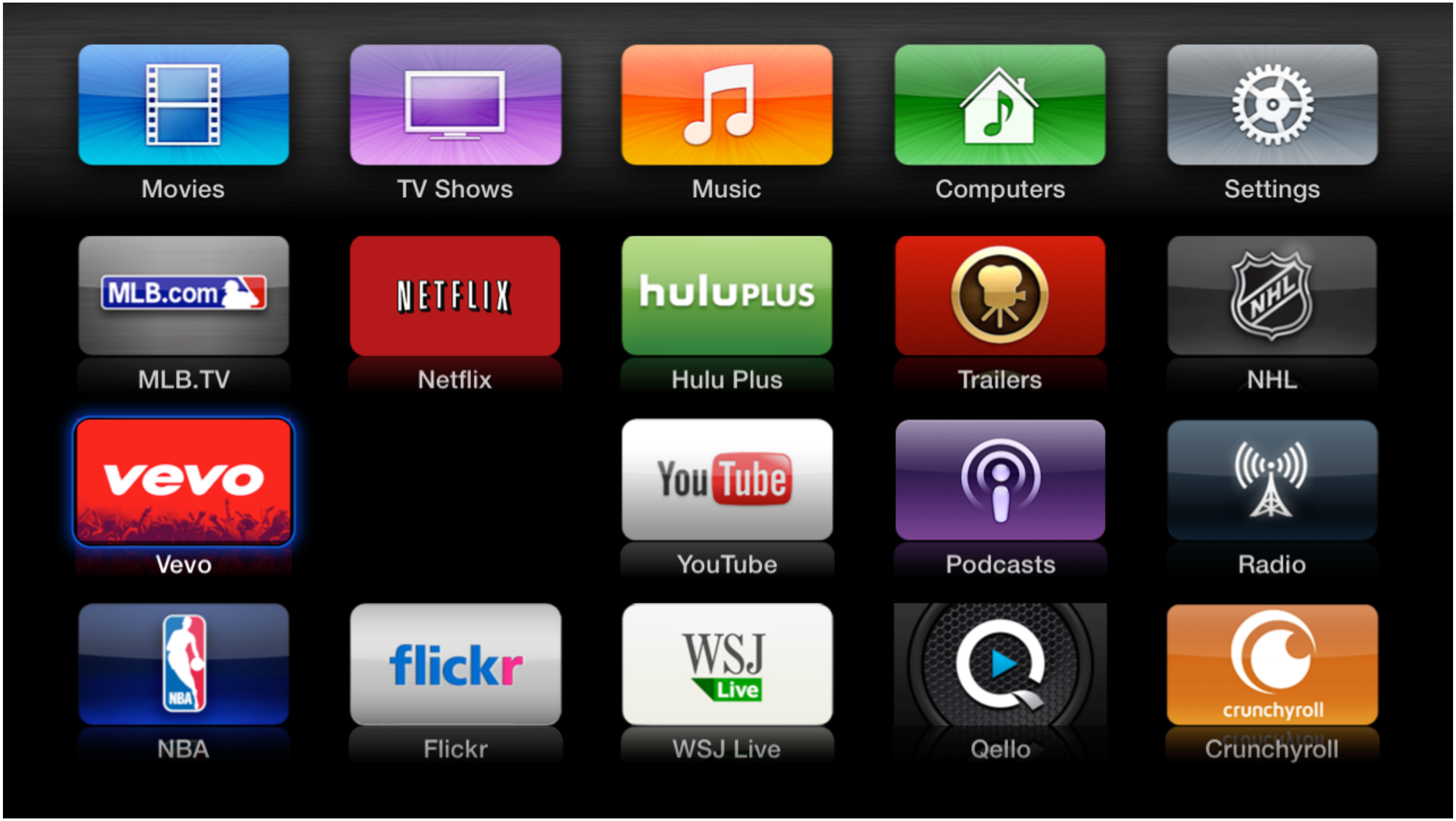
Adding a site

- After loading the profile, restart AppleTV
- Click on Add Site
- Enter a “vendor bag” (ends with bag.plist)
  - Or enter the app’s root URL and name individually
- Doesn’t have to be an app you developed...

Sneaking an early peak

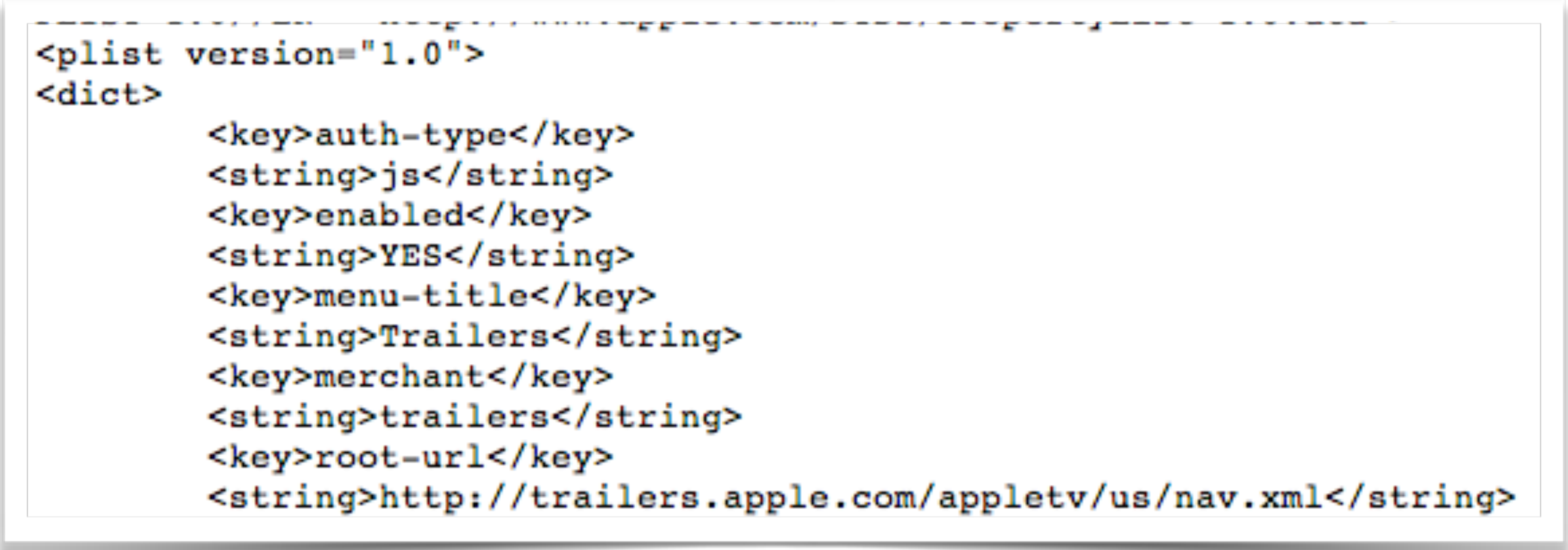
- August 21: Rumors of Vevo app on AppleTV
- Try multiple URLs:
  - –atv.vevo.com, appletv.vevo.com, etc.
  - –appletv.vevo.com gives a server error
  - –Add /bag.plist to URL - Success!
- Add to AppleTV
- Total elapsed time: Like a minute.

Loaded beta app



What is bag.plist?

- Property list file, defines the “app”
- Screensaver settings
- Menu title, merchant name, root URLs
- Examples: hunt for existing ATV feeds (trailers, Qello, etc.)

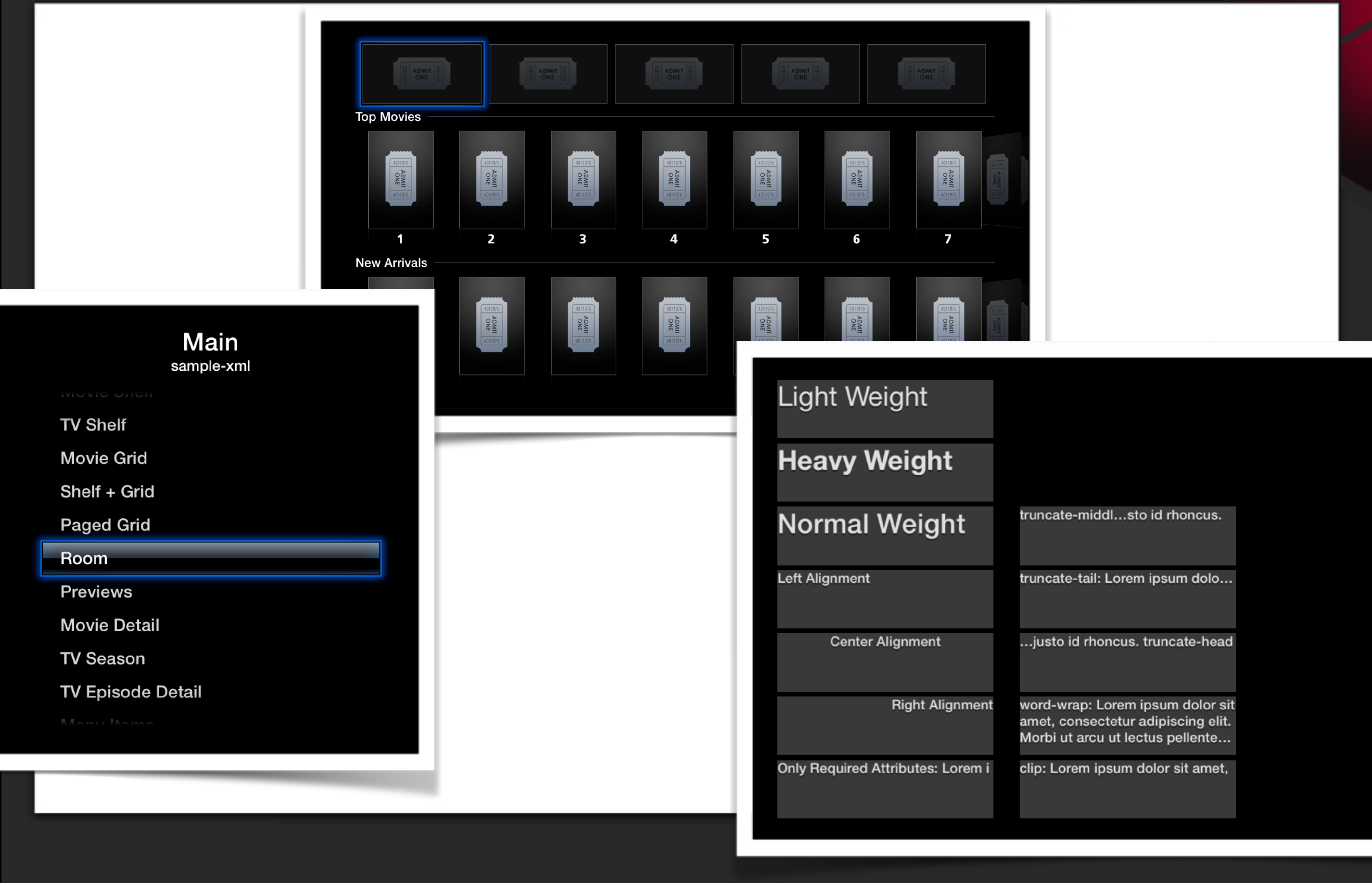


```
<plist version="1.0">
<dict>
        <key>auth-type</key>
        <string>js</string>
        <key>enabled</key>
        <string>YES</string>
        <key>menu-title</key>
        <string>Trailers</string>
        <key>merchant</key>
        <string>trailers</string>
        <key>root-url</key>
        <string>http://trailers.apple.com/appletv/us/nav.xml</string>
```

How is an app built?

- XSD schema on AppleTV filesystem
  - /Applications/AppleTV.app/atv.xsd
- Look at existing apps
  - Trailers app for example
- Google search for AppleTV and bag.plist
  - Found unfinished Fox News app
  - Linked to S3 copy of sample AppleTV app
  - Newer version in Plex forum

AppleTV sample-xml App



Light Weight

Heavy Weight

Normal Weight

truncate-middl...sto id rhoncus.

Left Alignment

truncate-tail: Lorem ipsum dolo...

Center Alignment

...justo id rhoncus. truncate-head

Right Alignment

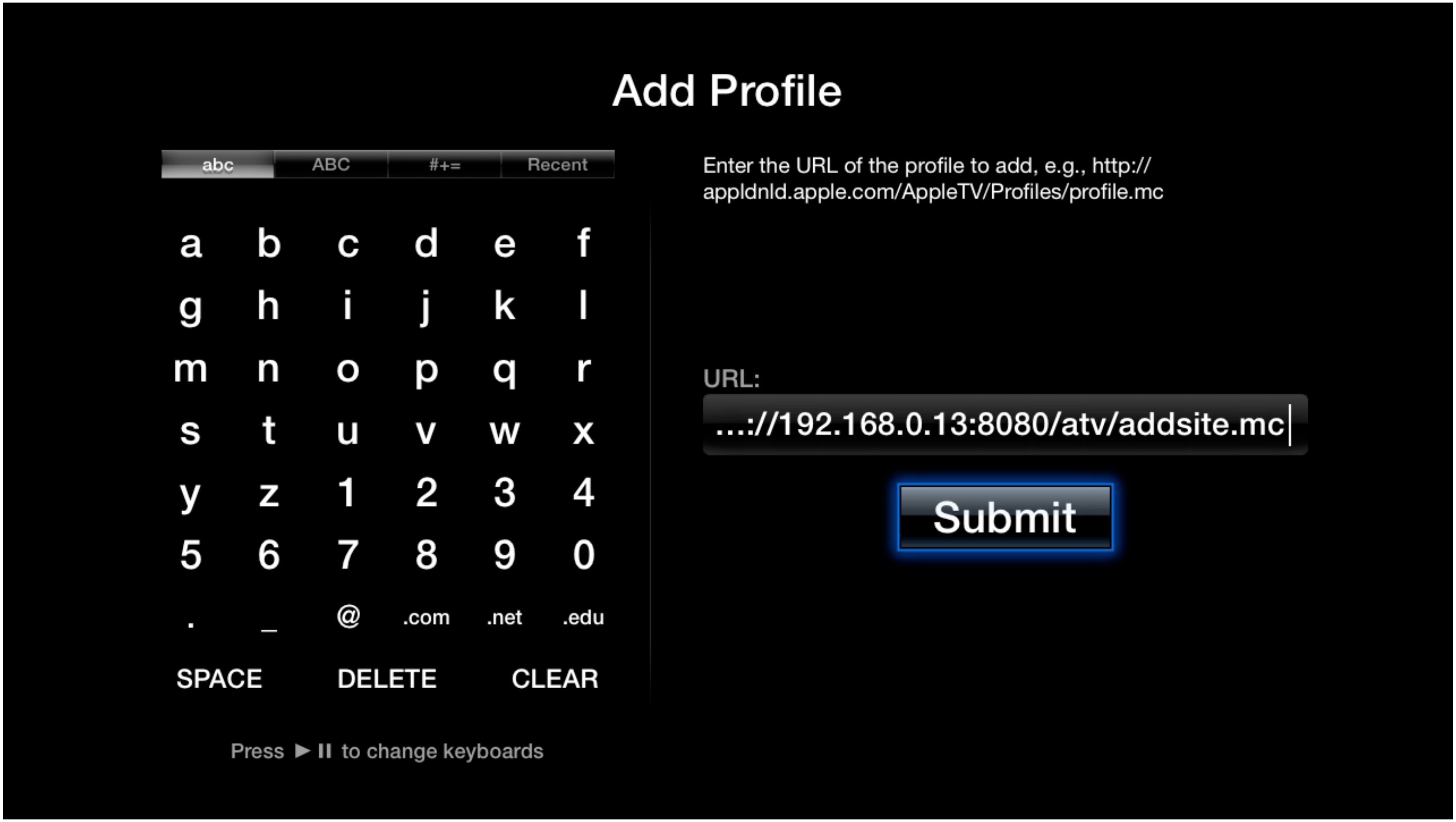
word-wrap: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi ut arcu ut lectus pellente...

Only Required Attributes: Lorem i

clip: Lorem ipsum dolor sit amet,

Demo

Demo: EnableAddSite

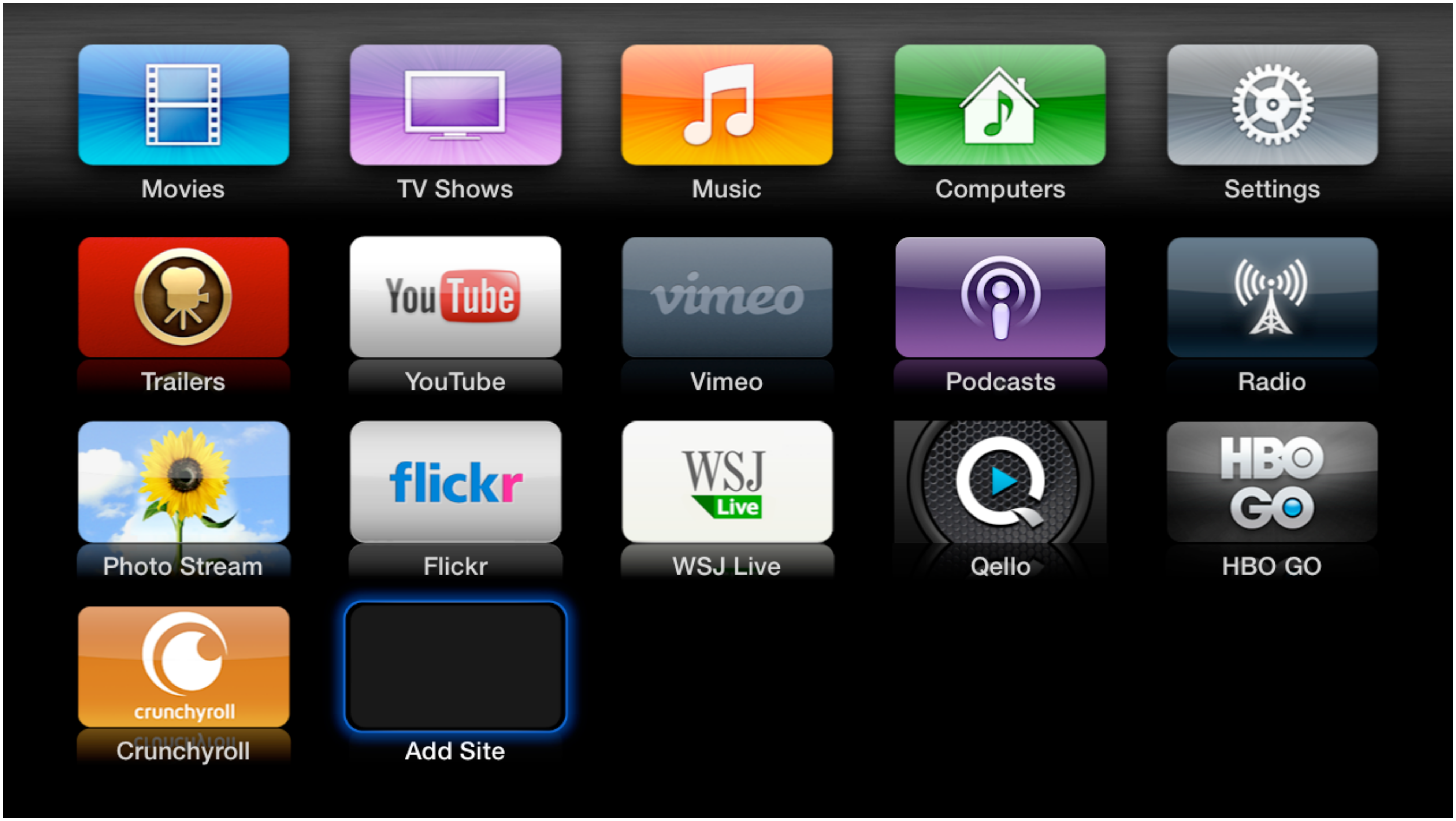


Add Profile

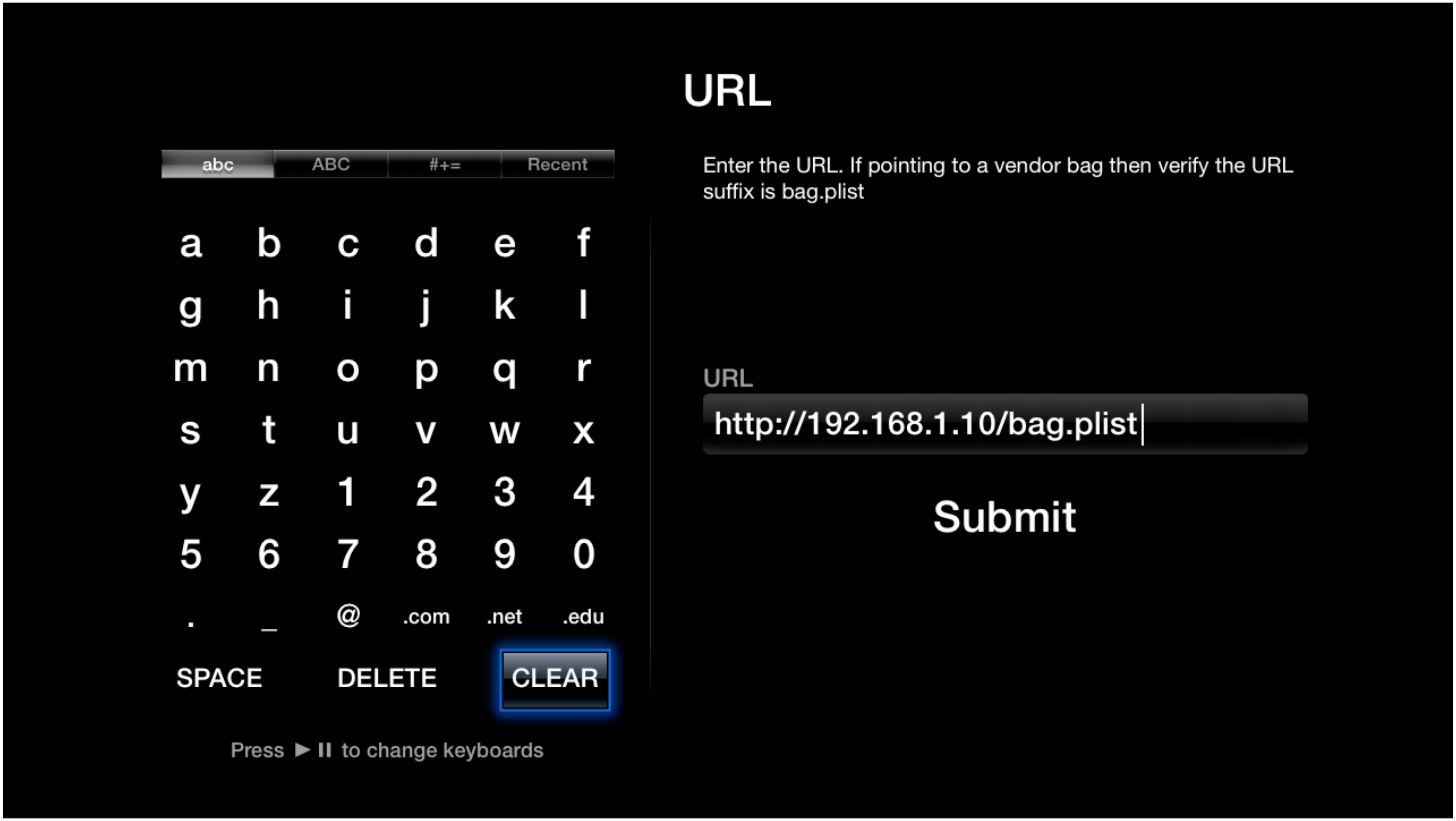
Enter the URL of the profile to add, e.g., http://appldnld.apple.com/AppleTV/Profiles/profile.mc

URL: ...://192.168.0.13:8080/atv/addsite.mc

Demo: Success!



Demo: Add new channel



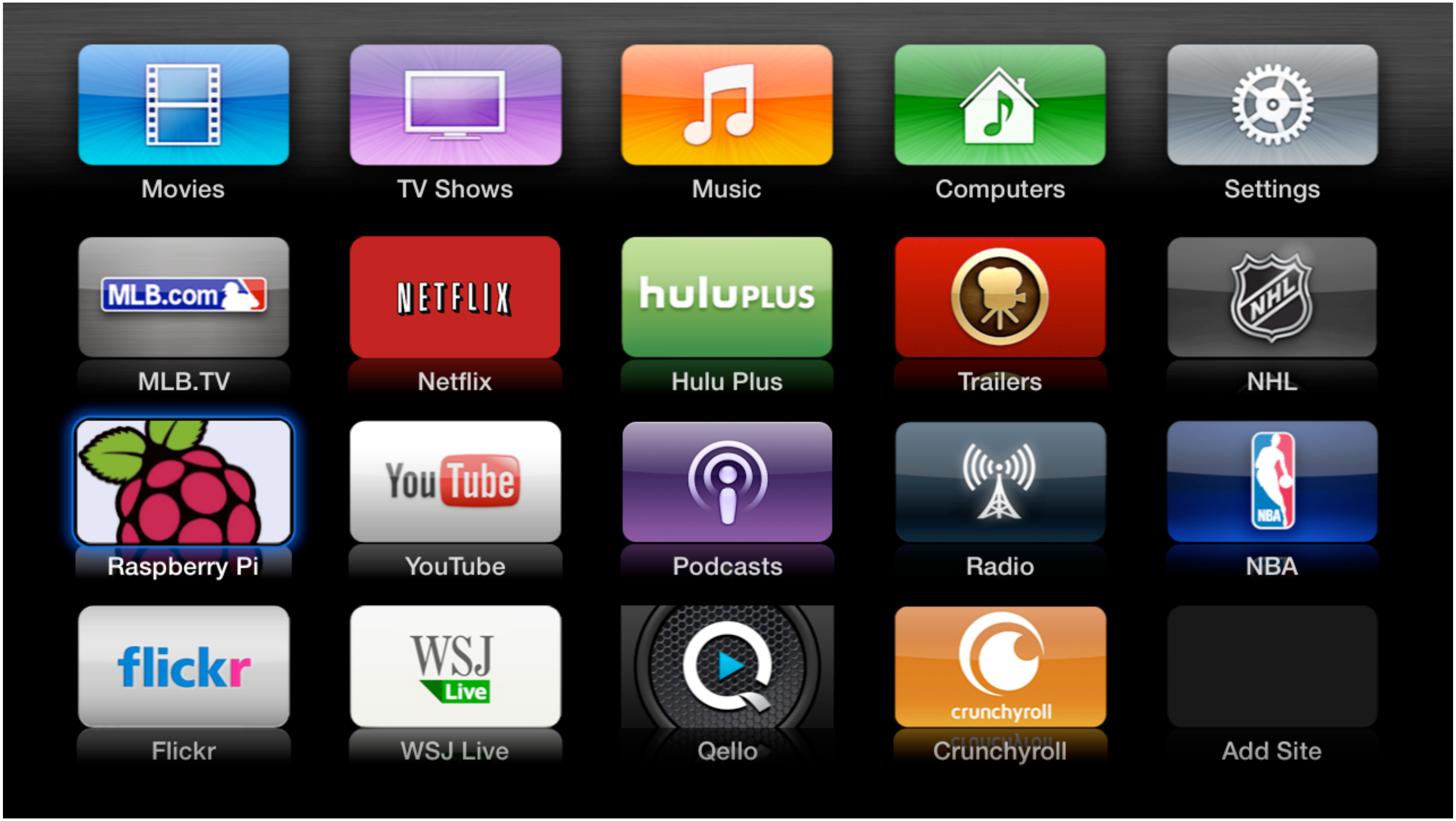
URL

Enter the URL. If pointing to a vendor bag then verify the URL suffix is bag.plist

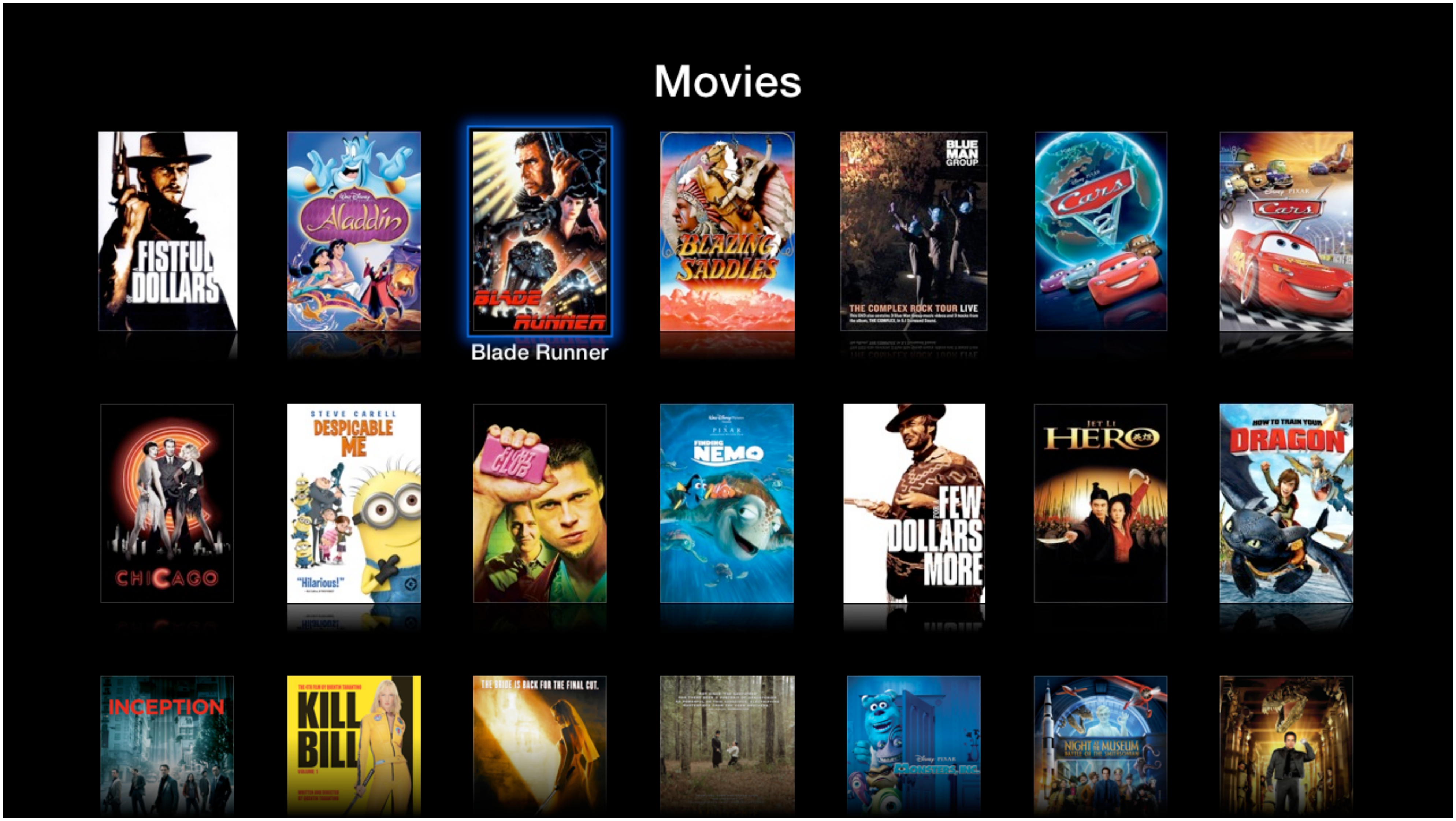
URL

http://192.168.1.10/bag.plist

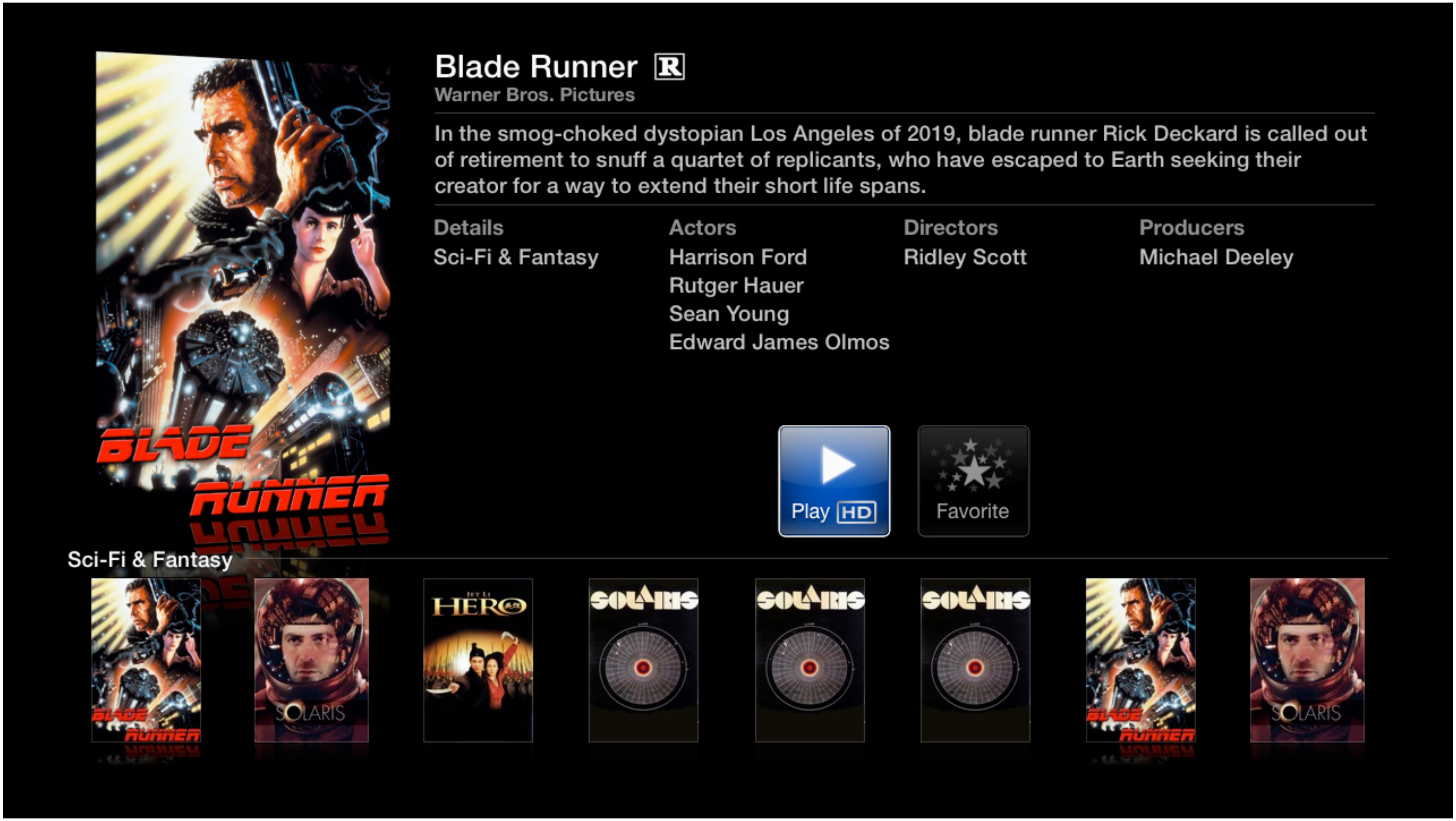
Demo: Success!



Demo: We got movies!



Demo: Movie Detail



Blade Runner R

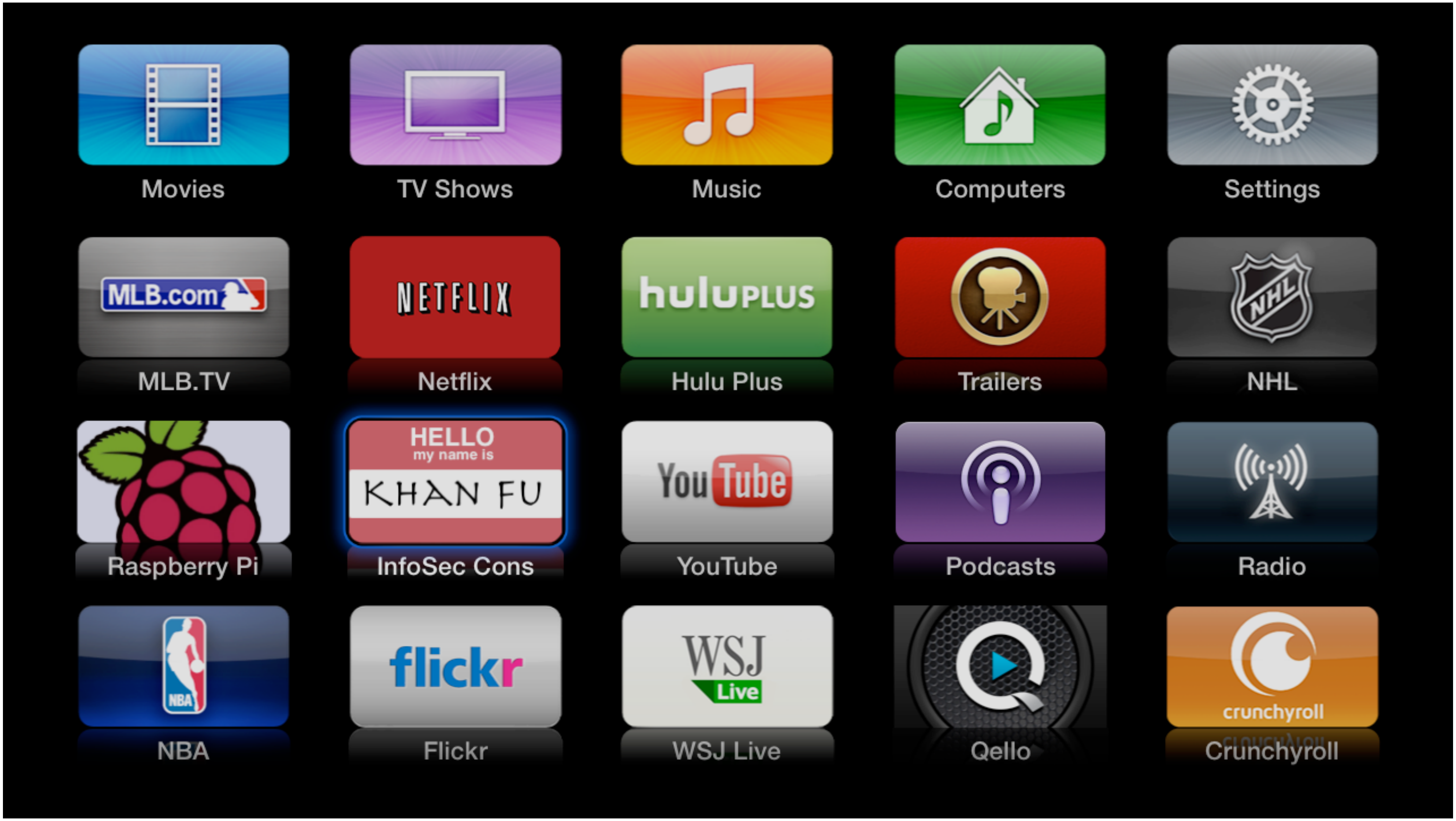
Warner Bros. Pictures

In the smog-choked dystopian Los Angeles of 2019, blade runner Rick Deckard is called out of retirement to snuff a quartet of replicants, who have escaped to Earth seeking their creator for a way to extend their short life spans.

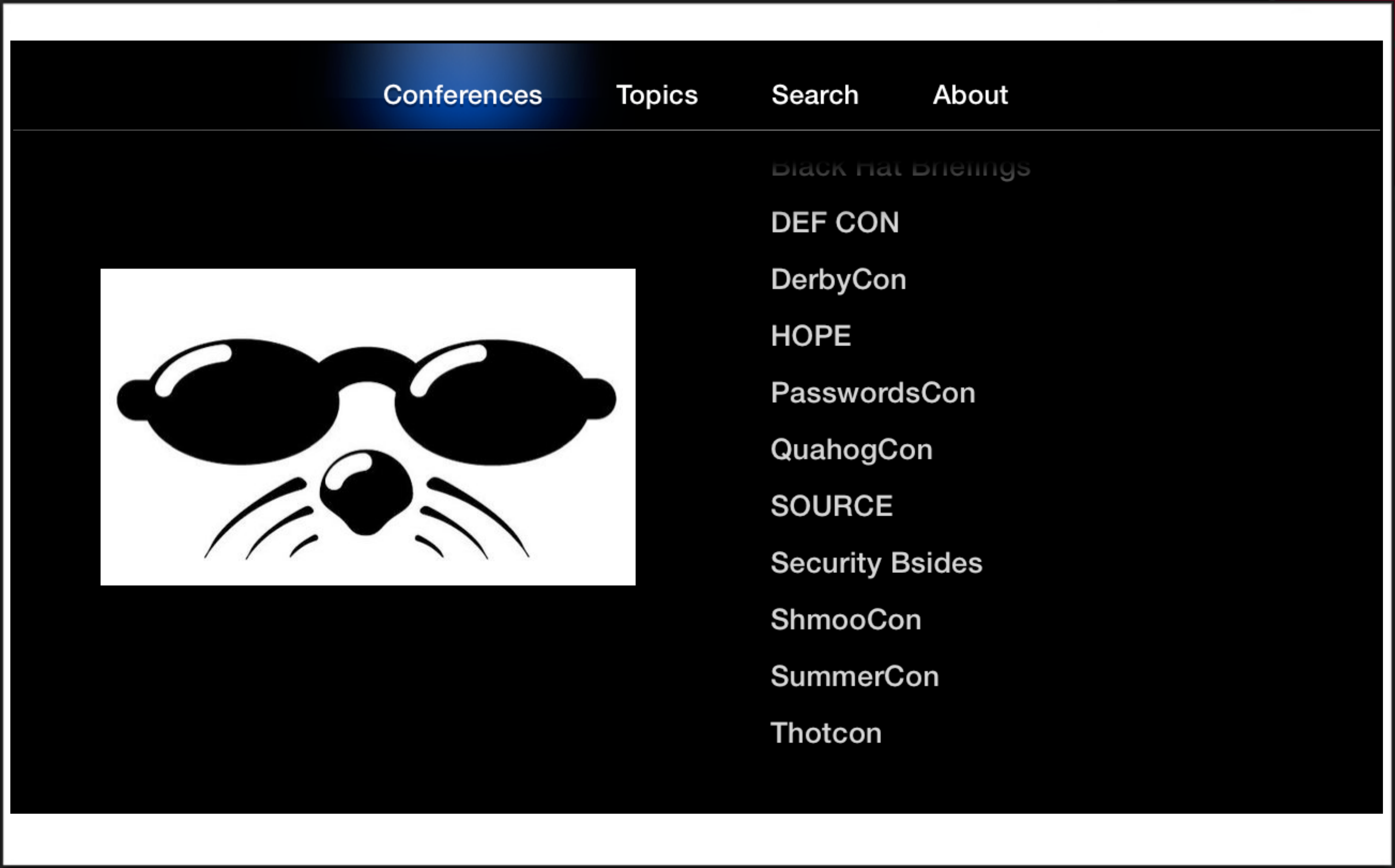
Details	Actors	Directors	Producers
Sci-Fi & Fantasy	Harrison Ford Rutger Hauer Sean Young Edward James Olmos	Ridley Scott	Michael Deeley

Demo: Not just movies

INTREPIDUS GROUP MOBILE SECURITY



Demo: Pick a conference



Black Hat Briefings

DEF CON

DerbyCon

HOPE

PasswordsCon

QuahogCon

SOURCE

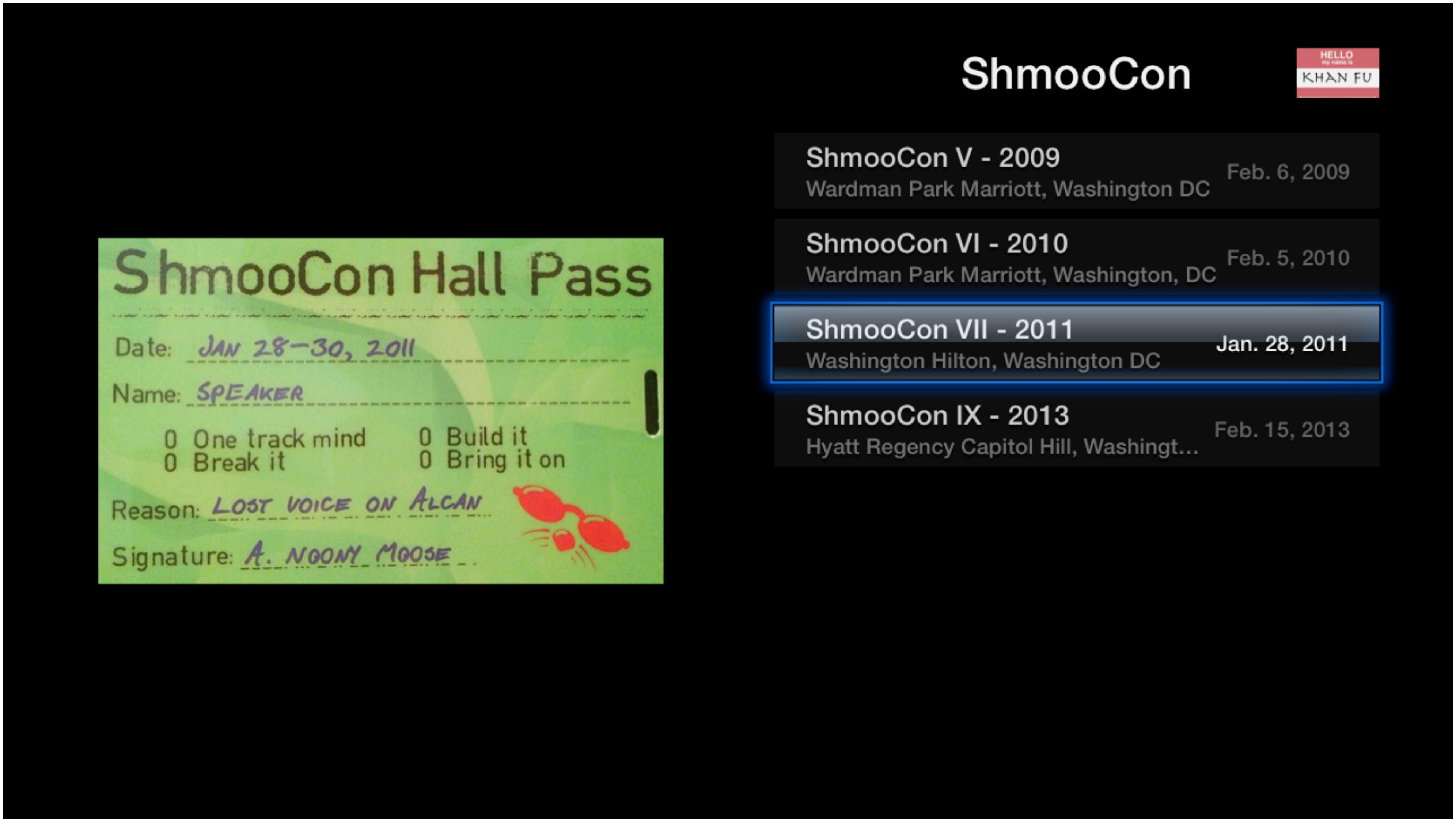
Security Bsides

ShmooCon

SummerCon

Thotcon

Demo: Pick a year



ShmooCon

ShmooCon V - 2009 Wardman Park Marriott, Washington DC	Feb. 6, 2009
ShmooCon VI - 2010 Wardman Park Marriott, Washington, DC	Feb. 5, 2010
ShmooCon VII - 2011 Washington Hilton, Washington DC	Jan. 28, 2011
ShmooCon IX - 2013 Hyatt Regency Capitol Hill, Washingt…	Feb. 15, 2013

ShmooCon Hall Pass

Date: JAN 28–30, 2011

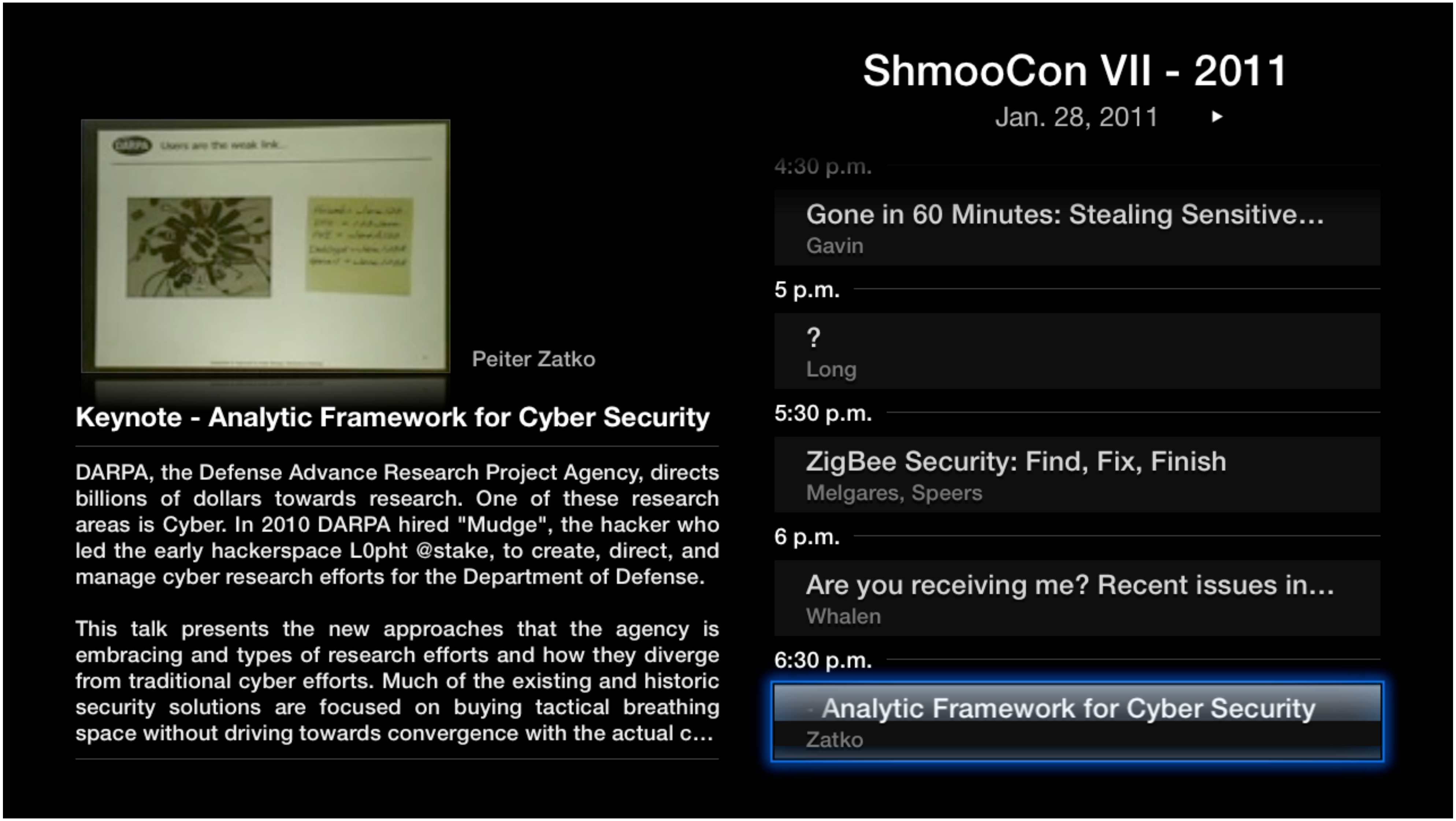
Name: SPEAKER

0 One track mind   0 Build it
0 Break it   0 Bring it on

Reason: LOST VOICE ON ALCAN

Signature: A. NOONY MOOSE

Demo: Talks and abstracts



ShmooCon VII - 2011

Jan. 28, 2011 ▸

Peiter Zatko

Keynote - Analytic Framework for Cyber Security

DARPA, the Defense Advance Research Project Agency, directs billions of dollars towards research. One of these research areas is Cyber. In 2010 DARPA hired "Mudge", the hacker who led the early hackerspace L0pht @stake, to create, direct, and manage cyber research efforts for the Department of Defense.

This talk presents the new approaches that the agency is embracing and types of research efforts and how they diverge from traditional cyber efforts. Much of the existing and historic security solutions are focused on buying tactical breathing space without driving towards convergence with the actual c…

4:30 p.m.

Gone in 60 Minutes: Stealing Sensitive…
Gavin

5 p.m.

?
Long

5:30 p.m.

ZigBee Security: Find, Fix, Finish
Melgares, Speers

6 p.m.

Are you receiving me? Recent issues in…
Whalen

6:30 p.m.

Analytic Framework for Cyber Security
Zatko

Limitations

- Can't remove channels
- Sometimes a little flaky
- Logging setting is chatty
  - General facility -- includes all apps
  - Might include credentials or other sensitive info
- Adding feeds is manual - can't push a profile
- Limited to AppleTV interface
  - Not a generic SDK
  - But still some control using JS -- see sample app
  - Weather Channel app uses custom layouts

Security concerns

- Log leakage
- All channels run in same context
  - Break out of js sandbox
  - Read credentials for other feeds
- Finding unreleased apps

What will Apple do?

- Good job. Have fun. Don't bitch if it breaks.
- D'oh. Next update will need a signed profile.
- Coming soon: an official channel store!

What DID Apple do?

- iOS 7 (ATV 6.0) released last week
- Gone:
  - AllowedDefaults.plist
- Looks like a lot of interesting bits added:
  - resource:// URL type
  - FeedResource.archive - app format?
  - Full Add Site Manager - Add, list, delete sites
  - Site Verification - perhaps to limit unauthorized use
  - Sounds awfully close to a “channel store” interface

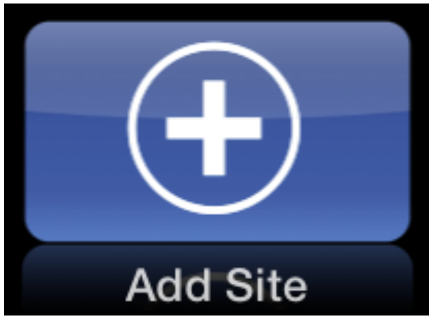
But does it still WORK?

- Not Yet.
  - sad panda. sad trombone. etc.
- All the custom profile-enabled settings broke
  - Not just Add Site
- Suspect it's a question of profile details
  - Was PayloadType: com.apple.frontrow
  - Now... ???

- Hopefully this shouldn't take community too long to figure out...

New icon!

- Just appeared on my 5.2 and 5.3 devices
- Was just a blank tile before
- Was there always a hook somewhere?
  - Apple just finally put the icon on their server
- Maybe finally getting ready for public channel management?



What will hackers do?

- Amazon Prime Video
  - Please?
- Educational Videos
  - NASA, Ted, etc.
  - Instructables, CBT
- Other networks
  - PBS, Discovery
- Chromecast clone

What's Next?

Future ideas

- Recognize home AP and bind there
  - Automatic sync
  - Built-in battery, automatic shutdown after sync
- Cellular hotspot
  - Service to all the kids' iPod-class devices
- Minecraft server :)

Improved Hardware

- Added 120 GB external SSD
- Better hardware
  - –Louder output volume
  - –Faster processor
  - –SATA
  - –On-board WiFI
- Hard to find mix of everything
  - –Especially SATA, and composite + HDMI video
  - –Opportunity for Yet-Another-Single-Board-System

Conclusion

- Fun little toy
- Used it on a couple of trips already
- rPI capable, but a little limited
- Excited about potential with AppleTV
- Really hope we see official (and DIY) channel store soon

Further Reading

- Intrepidus Group blog:
  - –http://intrepidusgroup.com/insight/2013/09/rpi-atv/
- Github Site:
  - –https://github.com/intrepidusgroup/rpi-atv

Thanks!