Hacking the Apple TV and Where your Forensic Data Lives

Presentation for:
Defcon 17
July 30, 2009
Kevin Estis
and
Randy “r3d” Robbins
DMCA Disclaimer

1. Digital Millennium Copyright Act

2. The authors of this presentation respects the intellectual property rights of others and is committed to complying with U.S. Copyright laws. Our policy is to respond to notices of alleged infringement that comply with the Digital Millennium Copyright Act. The Digital Millennium Copyright Act of 1998 ("DMCA") provides recourse for owners of copyrighted material who believe their rights under U.S. copyright law have been infringed on the Internet.

3. If you believe representations of your work has been copied or otherwise runs afoul of DMCA during this presentation that may constitute copyright infringement, please provide notice to our Designated Agent. The notice must include the following information as provided by the Digital Millennium Copyright Act, 17 U.S.C. 512 ( c ) (3):

   4. A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;

   5. Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site;

   6. Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material;

   7. Information reasonably sufficient to permit the service provider to contact the complaining party, such as address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted;

   8. A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law;

   9. A statement that the information in the notification is accurate and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

10. The Designated Agent for notice of copyright infringement claims may be reached as follows:


   12. Randy Robbins  randy.robbins[at]gmail[dot]com
Why Use the Apple TV?

Because it’s HOT...
Why Use the Apple TV?
Overview

1. What is the Apple TV?
2. How is it different?
3. How Does it Get Modified?
   - The Old Way
   - The New Way
4. Walkthrough Two Patchsticks
   - atvusb-creator
   - aTV Flash
5. Forensic Data

- Hardware Analysis from a Forensic Examiner Perspective
- Software Summary from a Forensic Examiner Perspective
- File Structures
- Basic Forensic Considerations
- General Forensic Considerations
  - Discovery
  - Investigations
  - Files (Almost) Always Modified
- Apple TV Files and Directories Important to Forensic Analysis
  - Basic Areas for User Data
  - Areas Where Most Data Resides
What is the Apple TV?
Overview

1. It is a Digital Media Player
2. Appliance made by Apple Computer based upon Mac OS X
   - Works with iTunes & iPhoto (plays what they do)
   - Built-in 802.11a/g/n
   - Uses Quicktime components to play media
   - Apple TV Operating System may be modified easily
How is it different?
How is it different?

1. Built on an open-source OS
   - *Darwin*, Berkeley Systems Distribution (BSD) Unix...the back-end of Mac OS X
   - Uses the Apple *Frontrow* application as the GUI

2. Does not have digital video recording (DVR) capabilities

3. Synchronizes content with iTunes and iPhoto
Darwin

1. Full kernel system for stability
2. Kernel extensions for feature extensibility
Frontrow

Default Menu for
ATV OS 1.1

Default Menu for
ATV OS 2.0.1
Apple TV and the iPhone

iPhone Remote
(Apple)

iPhone Remote
(Rowmote)
iTunes Store

Watchmen

A complex, multi-layered mystery adventure, "Watchmen" is set in an alternate 1985 America in which costumed superheroes are part of the fabric of everyday society, and the Doomsday Clock—which charts the USA's tension with the Soviet Union—moves closer to midnight. When one of his former colleagues is murder...

Movie Details
- Drama
- Released 2009
- 162 minutes
- 4.5/5 (271 Reviews)

Watchmen

Watchmen

Viewers Also Watched

Gran Torino

Summary
Add to Wish List

Actors
- Malin Akerman
- Billy Crudup
- Matthew Goode
- Carla Gugino
- Jackie Earle Haley
- Jeffrey Dean Morgan
- Patrick Wilson

Director
- Zack Snyder

Producers
- Lawrence Gordon
- Lloyd Levin
- Deborah Snyder
iTunes/iPhoto Sync

Synchronize content from iTunes and iPhoto

Firewalls, HIDS, and other security programs can make this a challenge...
How Does it Get Modified?
Two Ways to Modify

1. The Old Way
   - Remove the drive (void the warranty)
   - Copy over scripts/binaries manually
   - Generally more reliable but time consuming

2. The New Way
   - Point, click, modify
   - Sometimes stuff doesn’t install/work
The Old Way
Step 1: Make an Image

1. Remove drive and connect to my MacBook Pro via a USB-to-SerialATA cable
2. Image the drive with `dcfldd`
Step 2: Enable SSH

1. Enable “remote desktop” on MacBook Pro
2. Copy files to the Apple TV hard drive
Step 3: Enable VNC

1. Start VineVNC server on the MacBook Pro
2. Copy the needed files to the Apple TV hard drive
Step 4a: Enable kext

1. Patch the existing Apple TV OS kernel so that the watchdog service is disabled and kernel extensions re-enabled

2. Copy the patched kernel, the “enabler” file, and extensions to the Apple TV hard drive

```bash
[8] kevinstis@moonhack:Desktop% cp turbo_kext_enabler.bin /Volumes/OSBoot/hacks

[8] kevinstis@moonhack:/% cp -R /System/Library/Extensions/IODiskClass.kext /Volumes/OSBoot/System/Library/Extensions/

[8] kevinstis@moonhack:/% cp -R /System/Library/Extensions/IODiskClass.kext /Volumes/OSBoot/System/Library/Extensions/

[8] kevinstis@moonhack:/% cp -R /System/Library/Extensions/IODiskClass.kext /Volumes/OSBoot/System/Library/Extensions/
```
Step 4b: Enable kext

1. Put Apple TV hard drive back in Apple TV
2. Connect from MacBook Pro to Apple TV via SSH
3. Execute the kext enabler to start `kextload`
4. Use `kextload` to start USB drivers
Step 5: Verify USB Drive

Run `diskutil list` via SSH
Step 6: Use Only USB

1. Copy the data from the “default” location to the USB drive
2. Make a backup of the data located in the default location
3. Make a symbolic link from the default location to the new location

-bash-2.05b$ cp -R /mnt/Media/* /mnt/Scratch/Volumes/Multimedia/
bash-2.05b$ sudo mv /mnt/Media /mnt/Media.backup
Password:
bash-2.05b$ sudo ln -s /mnt/Scratch/Volumes/Multimedia /mnt/Media
Step 7: Install ATV

Install AwkwardTV via SSH

```
bash-2.05b$ sudo ./installme
Password:
installer: Package name is ATV Loader
installer: Installing onto volume mounted at /
installer: The install was successful.
```

![Screenshot of AwkwardTV installation](image)
Step 8: Install nitoTV

Install nitoTV via SSH

```bash
-bash-2.05b$ sudo ./installme
Password:
installer: Package name is nitoTV 0.2.6
installer: Installing onto volume mounted at /
installer: The install was successful.
Restarting Finder...
```
Step 9: Install Perian

- Manual installation (nitoTV install didn’t work)
- Lots of command line

Apple TV by default supports this:

Perian supports

- AVI, FLV, and MKV file formats
- MS-MPEG4 v1 & v2, DivX, 3ivX, H.264, FLV1, FSV1, VP6, H263i, VP3, HuffYUV, FFVHuff, MPEG1 & MPEG2 Video, Fraps, Windows Media Audio v1 & v2, Flash ADPCM, Xiph Vorbis (in Matroska), MPEG Layer II Audio
- AVI support for: AAC, AC3 Audio, H.264, MPEG4, and VBR
- MP3Subtitle support for SSA and SRT
Step 10: Rip/Download & Enjoy
Copy, Play
The New Way
Patchstick Summary

• Requires a USB drive
• Uses `boot.efi` from an existing Apple TV OS disk image
• Some version of bootable Linux
• Enable SSH and add `Finder.app` appliances (`*.frappliance`)
• Made for use by people with basic understanding of computers
aTV Flash - Overview

- Commercial patchstick ($49.95, includes 1-year of updates)
- Code has comments and subdirectories
- Mac and PC versions
- Installs a lot of applications others don’t
- Integrates with NitoTV (tracks Smart Installer and places “extras” in NitoTV App menu)
aTV Flash – Patchstick Setup

- Selects a USB drive
- Calls home to check for Internet connectivity
- Either download the update or tell it where the file exists
aTV Flash – Patchstick Setup

• Downloads the Apple TV OS Update

• Tell it what you want to do

• Done
aTV Flash – File Structure

- aTV Flash.app is the actual application
- A hidden subdirectory root is created; this is what is put on the thumbdrive
- Notice the directory structure of applications (including the .plist for CouchSurfer) and the latestXXXX.dmg at the bottom of the window
aTV Flash – Patchstick.sh
ATVUSB-Creator Overview

- ATVUSB-Creator creates an open-source patchstick.
- ATVUSB-Creator can also create a “Bootstick”...if you want to boot a Linux distro
- Windows and Mac versions
- Application is being actively developed and improved
- Adds SSH, File Utils, Software Menu, and XMBC/Boxee to Apple TV
ATVUSB-Creator - Patchstick Setup

• Locate a compatible USB thumb drive (not all are created equal)
• Determine appropriate /dev/<target-drive>
• Ensure the tools you want are selected
• Click “Create Using ->”…unless you are rolling your own “uber” ATV Recovery DMG
• In about two minutes, you have a handy-dandy ATV-USB Creator patchstick
ATVUSB-Creator - Patchstick Setup

- ATVUSB-Creator makes two partitions on the thumb drive
- Uses EFI to mount ATV drive and make modifications

Hum... wonder if you can edit "patchstick.sh" to add your own custom items
ATVUSB-Creator - Patchstick script

- ATVUSB-Creator mounts ATV hard drive in RW
- Creates some links and then searches for “install.sh” scripts
- Each “install.sh” configures and installs its package...
• Unplug and plug in the ATV...wait 2 minutes and `ssh frontrow@appletv.local`
Popular Applications
nitoTV - Overview

- Installed by almost all patchsticks
- Massive amount of functionality including mounting USB drives, viewing RSS feeds, and installation of 3rd-party applications
nitoTV - Overview

- Files menu will access USB drives
- Streams will access streaming audio/video feeds and play via mPlayer
nitoTV - Overview

- RSS menu will load RSS feeds you configure

- Although articles are limited to text only
nitoTV – Overview - Settings

- Most nitoTV functionality and benefit is on the back-end utilities
nitoTV – Overview - Settings

- nitoTV Smart Installer will not only go out and retrieve (most) of what you need it will automatically install components for you as long as the source files are present.
nitoTV – Overview - Settings

• nitoTV Utilities menu provides access to several sub-menus and scripts
• The reboot/shutdown scripts are most helpful since there is no other easy way
nitoTV – Overview - Settings

- **nitoTV Utilities – Services** menu provides access to enable/disable SecureShell, Apple Filing Protocol, and File Transfer Protocol

- **nitoTV Utilities – Console** provides read access to console logs
nitoTV Demo
Boxee Walk-through
Where Your Data Lives
What are the big ticket items?

- Hardware Analysis from a Forensic Examiner Perspective
- Software Summary from a Forensic Examiner Perspective
- File Structures
- Basic Forensic Considerations
  - General Forensic Considerations
  - Discovery
  - Investigations
  - Files (Almost) Always Modified
- Apple TV Files and Directories Important to Forensic Analysis
  - Basic Areas for User Data
  - Areas Where Most Data Resides
Hardware Analysis

- Small form factor and low noise (no fan)
- Has both 802.11n (which includes 802.11b and 802.11g backwards compatibility) and 10/100Base-T Ethernet abilities, so that either type of network connectivity may be utilized
- Video output from the device is processed via HDMI or component video, and audio output is processed via optical or RCA composite connections.
Software Summary

• By default, runs a modified version of the full Apple OS X operating system
• Built upon FreeBSD (a derivative of Berkeley Software Distribution Unix); very powerful and equally functional
• Capability to run the same programs and applications as other Linux/BSD servers
• Functionality for multiple video, audio, and picture formats already built-in
• Two primary variants of the Apple TV OS: version 1.0/1.1 and version 2.x (also known as Take 2); 2.x removed a lot of “unnecessary” applications
Software Summary

- GUID partition scheme, formatted as HFS+, and (by default) should have four separate disk partitions:
  - Extensible Firmware Interface [EFI]
  - Apple Recovery for system restores to factory original
  - OSBoot for the boot files
  - Media for the media files
OS takes advantage of the ability to use symbolic links (and even has some of the same links)
Basic Forensic Considerations

• Discovery
  – Conduct a wireless assessment to determine if wireless networking is allowing the device to communicate on the LAN or local WiFi networks.
  – The WAP being utilized may or may not belong to the individual being investigated and/or area being searched; information about all local WAP should be collected.
  – MAC addresses, IP addresses, and signal strength mapping can provide valuable data.
  – Remember USB drives, iPhones, and network file services (SMB/Samba, FTP, AFP, SSH).
Basic Forensic Considerations

• Investigations
  – Hard drive is has a GUID partition table formatted as HFS+; investigation workstation will need file system drivers for reading HFS/HFS+ drives
  – All OS X derivatives utilize Property List (.plist) files for configuration and some log data. Use OS X Property List Editor or another viewer capable of processing XML
  – OS X uses a database called NetInfo for storing some configuration data; normally accessed via NetInfo Manager in OS X prior to version 10.5 (Leopard) (possibly use NetInfo for Linux by PADL Software)
Files (Almost) Always Modified

- The ATV OS kernel must be patched to run kernel extensions (mach_kernel)
  - Located in /OSBoot/
  - Systems modified with patchsticks generally have copies of the original saved as mach_kernel.prelink.og
- New kernel extensions loaded into /OSBoot/System/Library/Extensions
- Secure Shell
  - SSHD into /Volumes/OSBoot/usr/sbin
  - Dropbear into /Volumes/OSBoot/usr/bin
Files and Directories Important to Forensic Analysis

- Most user data is located in:
  - `/Media/Scratch/Users/frontrow`

- However, your data is **EVERYWHERE**:
  - `/OSBoot/System/Library/Filesystems` - Used for file-system component applications, by default contains 2 items but may have user-added items (such as fusefs.fs for mounting shares via SSH).
  - `/OSBoot/System/Library/Frameworks` - by default has 49 items but users/3rd parties may have added more (such as AppleShareClient.framework for enabling AFS connections)
  - `/OSBoot/usr/libexec` - Contains executable libraries used by the OS, By default has 27 items but user/3rd party may place others (like sftp-server, etc.)
  - `/OSBoot/usr/sbin` - by default has 59 items but may contain others added by user/3rd parties like sshd
Files and Directories Important to Forensic Analysis

- `/Media/Photos/Pxx` - each folder will have a picture and a ‘thumbnail’ file for every photo synced with iPhoto.

- `/Media/Scratch/Library/Preferences/SystemConfiguration/autodiskmount.plist` - configuration data for disks to mount without user intervention, not present by default so it indicates the user utilizes removable disks

- `/Media/Scratch/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist` - configuration data for the Apple TV airport connection (includes list of known networks)

- `/Media/Scratch/private/var/run/resolv.conf` – contains DNS servers used to resolve DNS queries by the Apple TV (this file is configurable by the user).
Files and Directories Important to Forensic Analysis

• **Areas Where Most Data Resides**
  - Log information in .plist files and the Spotlight index; Spotlight can be hit or miss
    • `/OSBoot` partition contains some log files normally found in `/var/log` on a standard Apple OS X system
    • `/Media` partition has logs in `/var/log` generally different than `/OSBoot`
  - Generally, `/user/frontrow` has all 3rd party apps and data

• **Applications also track a LOT of data**
  - nitoTV places data in `\Media\Scratch\Users\frontrow\Library\Application Support\nito`
  - Boxee places a lot of data in `\Media\Scratch\Users\frontrow\Library\Application Support\BOXEE\`
Remnants of Data
Remnants of Data
Questions?