IoT Devices Fall Like Backward Capacitors

"That month Josh was forced to wear pants."

Joshua Wright
josh@counterhack.com
@joswr1ght
How Bad Are IoT Devices?

• How much time does it take to identify flaws and exploit IoT devices?
• What kind of tools and techniques are used?
• What are the implications of vulnerable IoT devices?
Linksys WVC80N Camera

- Basic 802.11n/wired home monitoring camera
- Popular on Amazon, 3-star rating
- Firmware last updated 6/2015 (v1.0.01)

"You can keep your video stream secure and private [...] by creating password-protected accounts."
Amazon.com product description
WVC80N Downloads

Hardware Version 1.0

Firmware
- Ver.1.0.01 build 01
- Latest Date: 06/09/2015
- Download 4 MB
- Release Notes

Setup Wizard
- Ver.v1.0
- Latest Date: 10/09/2009
- Download 76.3 MB
Yay for Binwalk!

```bash
$ binwalk DYRH08-510-100101.bin

<table>
<thead>
<tr>
<th>DECIMAL</th>
<th>HEXADECIMAL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>41492</td>
<td>0xA214</td>
<td>HTML document header</td>
</tr>
<tr>
<td>41695</td>
<td>0xA2DF</td>
<td>HTML document footer</td>
</tr>
<tr>
<td>42056</td>
<td>0xA448</td>
<td>HTML document footer</td>
</tr>
<tr>
<td>43175</td>
<td>0xA8A7</td>
<td>HTML document footer</td>
</tr>
<tr>
<td>142296</td>
<td>0x22BD8</td>
<td>gzip compressed data, maximum compression, from Unix, last modified: 2015-03-25 03:29:11</td>
</tr>
<tr>
<td>917504</td>
<td>0xE0000</td>
<td>Squashfs filesystem, little endian, version 3.0, size: 2871831 bytes, 470 i nodes, blocksize: 65536 bytes, created: 2015-03-25 05:32:37</td>
</tr>
<tr>
<td>4194226</td>
<td>0x3FFFFB2</td>
<td>Sercomm firmware signature, version control: 1, download control: 256, hardware ID: &quot;YRH&quot;, hardware version: 0x0, firmware version: 0x1, starting code segment: 0x0, code size: 0x7310</td>
</tr>
</tbody>
</table>

$ binwalk -e DYRH08-510-100101.bin

<table>
<thead>
<tr>
<th>DECIMAL</th>
<th>HEXADECIMAL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Firmware Spelunking

CGI-based HTTP management; main.cgi is the primary CGI, using symlinks to differentiate functionality.
This is an ancient Linux kernel, predating DEP and ASLR support. Yay4me!
Password Protection

The `.htpasswd` file is used for locally-added user accounts, common for simple web security.
Web Interface Navigation
"We won't be so easily fooled you evil hacker!" --Linksys
"I would like to retract my previous statement." --Linksys
LFI to Admin Credentials

The password is stored in plaintext, and is accessible using the LFI vulnerability.
Hopper App: $89

www.hopperapp.com
HTTP Basic Auth: REMOTE_USER

Get the remote username, `strncpy()` into 128 byte stack variable.
Like many embedded devices, this device uses Busybox for Unix utilities. This build includes a telnet daemon and a dead/unreachable function to start it.
• No DEP, stack protection, or ASLR
• Stack-based buffer overflow in login function
• Telnetd daemon and code to start
• Plaintext password storage

AM I BEING TROLLED?
Should I be wearing pants?
WVC80N Roundup

- Firmware + Binwalk + Firmware Spelunking for discovery
  - Ancient Linux kernel, old server components, htpasswd plaintext storage
- LFI exposing plaintext passwords
- Lots of software flaws, exploit dev in progress
- Time: 9 hours before Hopper, 8 hours on exploit dev to date.
Belkin WeMo Slow Cooker

- Slow cooker from Crock-Pot
- WiFi connectivity from WeMo
- Cloud and app controls from Belkin

"Sure, why not?" --me
WeMo App

- iOS and Android
- Adjust timer, temperature
- Firmware isn't accessible from Wemo site
  - Applied through mobile app
Easy iOS Packet Capture

iPhone 6s

- Capacity: 55.60 GB
- Phone Number: (401) 524-2911
- UDID: 2CF3C1F7B664DEC418C224124E107E4E31DCE9A8

iOS 9.1
Connect this iPhone using restore its software.

```
$ rvictl -s 2cf3c1f7b664dec418c224124e107e4e31dce9a8

Starting device 2cf3c1f7b664dec418c224124e107e4e31dce9a8 [SUCCEEDED] with interface rvi0

Password:

$ sudo tcpdump -n -i rvi0 -s0 -w wemoapp.pcap

tcpdump: WARNING: rvi0: That device doesn't support promiscuous mode 
(BIOCPROMISC: Operation not supported on socket)
tcpdump: listening on rvi0, link-type PKTAP (Packet Tap), capture size 262144 bytes
```
Firmware Retrieval

GET /wemo/NewFirmware.txt HTTP/1.1
Host: fw.xbcs.net
User-Agent: WeMo 1.13.2 rv:30080 (iPad; iPhone OS 8.4; en_US)
Connection: keep-alive
Accept-Encoding: gzip

HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=10
Content-Type: text/plain; charset=UTF-8
Date: Fri, 25 Sep 2015 18:52:05 GMT
Expires: Fri, 25 Sep 2015 18:52:15 GMT
Server: Apache/2.2.15 (Red Hat)
Content-Length: 23785
Connection: keep-alive

WeMoOpenWRTTransCROCKPOT
WeMo_WW_2.00.9898.PVT-OWRT-Jarden
c6acbc5a43758ee6581fbd8116df5eae
http://fw.xbcs.net/wemo/WeMo_WW_2.00.9898.OWRT_PVT_Jarden-trans.bin.pgp

WeMo Slow Cooker firmware release notes WW 9898 PVT
- Fixed a memory leak that can cause the WeMo device to not respond after a few days
- Fixed a separate memory leak that may occur over a long period of time
- Addressed an issue that may cause WeMo devices to get kicked off of an Airport Extreme router
- Adjusted the timing in which WeMo devices are recognized by the app, so they can be more easily discovered
- Fixed an issue where WeMo devices fail to setup due to long network passwords
- Fixed a rare case where WeMo device Wi-Fi connection may get interrupted
- Fixed an bug where sun-based rules times weren't changing over time
GPG Encrypted Firmware

$ ent WeMo_WW_2.00.9403.OWRT.PVT_Jarden-trans.bin.gpg
Entropy = 7.999860 bits per byte.

Optimum compression would reduce the size of this 4576005 byte file by 0 percent.

Chi square distribution for 4576005 samples is 881.96, and randomly would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bytes is 127.4915 (127.5 = random).
Monte Carlo value for Pi is 3.143080794 (error 0.05 percent).
Serial correlation coefficient is 0.000665 (totally uncorrelated = 0.0).

$
Firmware Decryption

First reported by Mike Davis/IOActive in February 2014. Still vulnerable today.

```
$ gpg -o WeMo_WW_2.00.9403.OWRT.PVT_Jarden-trans.bin -d WeMo_WW_2.00.9403.OWRT.PVT_Jarden-trans.bin.gpg
$ ent WeMo_WW_2.00.9403.OWRT.PVT_Jarden-trans.bin | grep Entropy
Entropy = 7.723884 bits per byte.
$ strings WeMo_WW_2.00.9403.OWRT.PVT_Jarden-trans.bin | head -2
MIPS OpenWrt Linux-2.6.21
```
Belkin Crock-Pot Platform

1. bash

```bash
$ ls lib/modules/
2.6.21/
$ cat etc/openwrt_release
DISTRIBUT_ID="OpenWrt"
DISTRIBUT_RELEASE="10.03"
DISTRIBUT_CODENAME="backfire"
DISTRIBUT_DESCRIPTION="OpenWrt Backfire 10.03"
$ file sbin/wemoApp
sbin/wemoApp: ELF 32-bit LSB executable, MIPS, MIPS32 version 1, dynamically linked (uses shared libs), corrupted section header size
```

No MIPS support in Hopper
IDA Pro

Instruction Set Overload
Qemu Emulation

$ sudo apt-get install build-essential libglib2.0-dev zlib1g-dev autoconf libtool
$ wget http://wiki.qemu-project.org/download/qemu-2.4.0.1.tar.bz2
$ tar xvf qemu-2.4.0.1.tar.bz2
$ cd qemu-2.4.0.1
$ ./configure --static && make && sudo make install

With a statically compiled Qemu, we can run executables in the firmware extract in debug mode.
Qemu and IDA Pro

Run with the "-g portNum" argument, Qemu accepts GDB-compatible remote debuggers to step through the target and watch mem/processor.
Running a cross-compiled binary with Qemu is possible, but not reliable. Crashes, obscure error messages and unpredictable behavior are common when emulating the platform.
All of This is Really Moot ...

Mode 52 = Cook on High
Because All Your WeMo Crock-Pot ...
No inherent CSRF protection. Add a little JavaScript to brute-force IP addresses.
Belkin WeMo Slow Cooker Roundup

- Firmware access through app packet sniffing
  - Firmware encrypted with key embedded in GPG file
  - Extracted firmware provides visibility into platform
- No authentication and no CSRF protection
- Time: 4 hours before IDA Pro, 33 frustrating hours on emulation of wemoApp, 30 minutes to CSRF

Don't make assumptions that the vendor does things in the way you expect
Why is this important to me?
$655 Billion

Worldwide market in 2014 for IoT devices representing 10.3 billion devices.

* Wall Street Journal, 6/3/2015
$1.7 Trillion

Anticipated 2020 worldwide market for IoT devices representing 29.5 billion devices.

* Wall Street Journal, 6/3/2015
The Internet
of Things
Hacking IoT

- We aren't covering novel techniques here
  - Nor are the mistakes novel
- Exploit development is still time-consuming
  - Often, fewer platform defenses
  - Other challenges with emulation, hardware
- Lots of flaws without exploit dev
- Today it is cameras and slow cookers
  - As our reliance grows on this connectivity, our exposure grows as well
Keep Applying Your Skills

- Linux skills for firmware analysis
- Network traffic and protocol analysis
- Web pen test against admin interfaces
- Exploit development against ARM, MIPS
- Mobile application analysis

If you thought these skills were in demand now, wait until we add 30 billion more devices that need security analysis.
Thank You

Joshua Wright
josh@counterhack.com
@joswr1ght