

IoT: Client Devices

Reversing: Image Analysis

So Far...

U-BOOT BOOT LOADER

- ▶ Version 1.1.4, built in late 2015

LINUX KERNEL

- ▶ Also built in late 2015

FILESYSTEM

- ▶ Squash-fs filesystem, late 2015

Extracting

NOW LET'S USE BINWALK TO EXTRACT THE FILES

- ▶ `binwalk -e -C extracted -M <imagename>`

WHAT DOES THIS DO?

- ▶ `-e`: extract the contents of the image
- ▶ `-C`: place the results in the 'extracted' subdirectory
- ▶ `-M`: recursively scan extracted stuff

```
[cclamb@ubuntu:~/Work/tplink/extracted/_hs110v1_us_1.0.7_Build_151016_Rel.24186.bin.extracted] $ ls
10300  10300.7z  _10300.extracted  1102C0.squashfs  439C  439C.7z  squashfs-root
[cclamb@ubuntu:~/Work/tplink/extracted/_hs110v1_us_1.0.7_Build_151016_Rel.24186.bin.extracted] $ binwalk ../../hs110v1_us_1.0.7_Build_151016_Rel.24186.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
15904	0x3E20	U-Boot version string, "U-Boot 1.1.4 (Oct 16 2015 - 11:22:22)"
15952	0x3E50	CRC32 polynomial table, big endian
17244	0x435C	uImage header, header size: 64 bytes, header CRC: 0xA2B5F4E6, created: 2015-10-16 03:22:22, image size: 38777 bytes, Data Address: 0x80010000, Entry Point: 0x80010000, data CRC: 0xFED80D4A, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: lzma, image name: "u-boot image"
17308	0x439C	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 112564 bytes
66240	0x102C0	uImage header, header size: 64 bytes, header CRC: 0x4D2B83AC, created: 2015-10-16 03:22:56, image size: 772570 bytes, Data Address: 0x80002000, Entry Point: 0x8019BF90, data CRC: 0xC849B1ED, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Kernel Image"
66304	0x10300	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 2238780 bytes
1114816	0x1102C0	Squashfs filesystem, little endian, version 4.0, compression: lzma, size: 2112689 bytes, 194 inodes, blocksize: 16384 bytes, created: 2015-10-16 03:25:36

```
cclamb — ssh -X 192.168.120.134 — 89x26
[cclamb@ubuntu:~/Work/tplink/hs110 $ strings -n 10 10300 > strings.out
[cclamb@ubuntu:~/Work/tplink/hs110 $ head strings.out
initcall_debug
Linux version 2.6.31--LSDK-9.2.0_U11.14 (yt@yangtao.localdomain) (gcc version 4.3.3 (GCC)
) #10 Tue Sep 8 15:36:13 HKT 2015
%s version %s (yt@yangtao.localdomain) (gcc version 4.3.3 (GCC) ) %s
plat_time_init
ar7240_serial_setup
ar7240_spi_flash_read_page
ar7240wdt_init
pause_on_oops
Od<2>BUG: recent printk recursion!
printk.time
[cclamb@ubuntu:~/Work/tplink/hs110 $ strings -n 10 439C > 439C-strings.out
[cclamb@ubuntu:~/Work/tplink/hs110 $ head 439C-strings.out
U-Boot 1.1.4 (Oct 16 2015 - 11:22:19)
ag7240_miiphy_write
ag7240_miiphy_read
ag7240_get_ethaddr
ag7240_mii_setup
reset - Perform RESET of the CPU
    Image Name:      %.*s
    Created:          %4d-%02d-%02d  %2d:%02d:%02d UTC
    Image Type:
Invalid OS
cclamb@ubuntu:~/Work/tplink/hs110 $
```

Strings

Seems to confirm binwalk results, but now we have a kernel version (released in 2009!)

```
[cclamb@ubuntu:~/Work/tplink/hs110 $ ls
10300      _10300.extracted  439C      439C-strings.out  squashfs-root
10300.7z   1102C0.squashfs   439C.7z   hex.out           strings.out
[cclamb@ubuntu:~/Work/tplink/hs110 $ cd squashfs-root/
[cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $ ls
bin  dev  etc  lib  linuxrc  mnt  proc  root  sbin  sys  tmp  usr
cclamb@ubuntu:~/Work/tplink/hs110/squashfs-root $
```

The filesystem

Take a look at squashes-root; it has a complete filesystem!