OWASP
Open Web Application Security Project

Firmware Analysis

By – Pratik Chotaliya

About Me

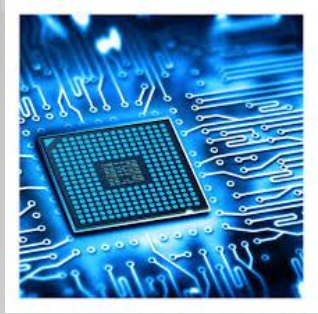
- Pratik Chotaliya
- Working as a Team Lead at AqmTechnologies.
- Interested in Exploit Writing | IOT.
- Twitter Handle - @PratikWhiteHat.

Topic to be Covered

- What is Firmware ?
- Usage of Firmware
- How to Obtain firmware for pen testers
- Firmware vulnerability analysis
- Analysing Firmware binaries
- Firmware file system types
- Squashfs
- Firmware extraction with binwalk
- Identifying hidden secrets.

Firmware

- Combination of all code running on the device.



- Almost all embedded devices.

- Consists of bootloader, kernel, file system and other resources.

Usage of firmware for PenTester

- Find hidden secrets – backdoor, passwords, Api keys, private certificates.
- Vulnerabilities in individual binaries.
- Emulate firmware binaries or firmware itself.
- By a competitor to understand and prepare a similar device.
- Creation of malicious firmware image.

How to obtain the firmware

- Vendor website, Support and community forums or Google search.
- Dumping it from the device's flash chip.
- Sniffing the update mechanism.
- Reversing mobile application or similar software reversing.

Downloading from Vendor website

https://support.dlink.com/ProductInfo.aspx?m=DIR-882-US

D-Link
Building Networks for People

TechSupport

Consumer | Business

Product Registration
Register your product to extend your free support from 30 days to 90 days

Warranty Document
Click here to see this product's warranty document.

DIR-882-US
AC2600 EXO MU-MIMO Wi-Fi Router

First Time Setting Up?
Check out our FAQs, Videos and Quick Install Guides

Contact Support
Get help by chat, email or phone

Downloads | FAQs | Videos

For access to the right downloads, please select the correct hardware revision for your device.

A

How to find the hardware version?

Type	Date		
WPA2 Security (KRACK) Patch (1.02B02 BETA)	02/09/18	Download	*Release Notes*
Firmware (1.20B06)	07/10/19	Download	*Release Notes*
Quick Install Guide (1.01 US)	05/16/18	Download	
User Manual (1.01 WW)	10/24/18	Download	
Datasheet (1.05 US)	11/13/18	Download	

D-Link | GPL Source Code | End-of-Life Policy | Terms of Use | Privacy | Contact Us

Firmware Vulnerability analysis

- Extract the firmware and look for specific component related security issues.
- Config files and hardcodes secrets.
- Attach it to a debugger and analyse.
- Reverse patches and diff two different versions of a firmware.

Analysing Firmware binaries

- Firmware binaries could have different extensions such as .bin/.img/.pkg or even come in a .zip package.

- Run strings and hexdump on it.

- What does a firmware actually contains?

File system types

- SquashFS
- CramFS
- JFFS2
- YAFFS2
- Ext2

SquashFs

- One of the most common file types in embedded devices.
- Could use utilities like unsquashfs and modified version of unsquashfs (with lzma decompression)
- Key thing is to identify the offset or where the file system start in the binary file.

Extracting SquashFS file system form Firmware

- Find out where is the squashFS header located in the firmware.
- Use dd to dump the contents.
- Unsquashfs to extract the squashfs file system.
- Use sasquatch – an extended version of the standard unsquashfs utility used to extract the file system.

Demo Time

Firmware Extraction with Binwalk

- Tool written by Craig Heffner (@devtty0).
- Extracts file system from firmware, performs decompressions, perform entropy analysis and different firmware's.
- Use Binwalk to extract file system from the D-Link Firmware.

Binwalk

- Binwalk firmware-name
- Binwalk –e firmware-name
- Binwalk –E firmware-name
- Binwalk –W first_file second_file

Identifying hidden secrets

- Extract the D-Link firmware.

❖Find the telnet credential form the firmware

Demo Time

Resources

- Binwalk Download link - https://github.com/ReFirmLabs/binwalk
- Attify OS - https://github.com/adi0x90/attifyos
- Firmware - https://firmware.center/

Any Questions

Thank You

- Security Folks.
- OwaspMumbai.
- Mr.Iot @Mr-IoT (Veerababu Penugonda)