FACT-VIS: a visual tool for the analysis and security of firmware

SAPIENZA
UNIVERSITÀ DI ROMA

Facoltà di Ingegneria dell'Informazione, Informatica e Statistica

Master's degree in Engineering in Computer Science

A.Y. 2020-2021

Candidate: Valerio Longo 1655653

Advisor: Prof. Giuseppe Santucci

Co-Advisor: Dr. Simone Lenti

Introduction

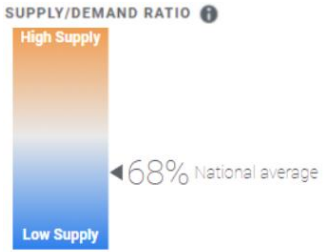
Firmware is **everywhere!**

All electronic systems needs it

- Domestic
- Healthcare
- Personal
- Military
- …

The spreading of IoT devices and COTS make easier the **diffusion of firmware** and with them **their vulnerabilities.**

This phenomena increased the need to perform firmware analysis, but this process **is not completely automatable!**



cyberseek.org

Lack of high technical skilled workforce which provide security and analyze the safety of firmware

OWASP Methodology

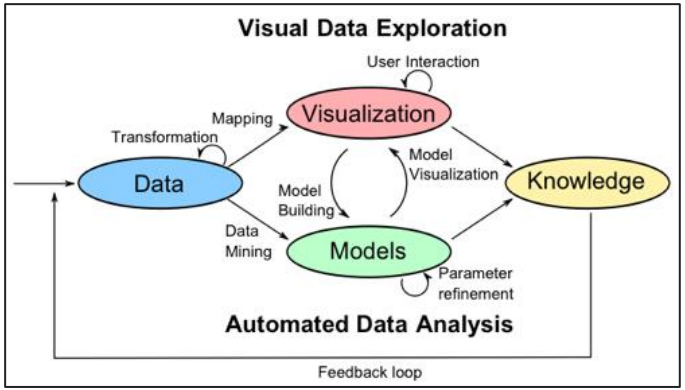
- A nine staged guide to tailor all domain's interested with conducting **firmware analysis**.

1. Information gathering and reconnaissance
2. Obtaining firmware
3. **Analyzing firmware**
4. **Extracting the filesystem**
5. **Analyzing filesystem contents**
6. Emulating firmware
7. Dynamic analysis
8. Runtime analysis
9. Binary Exploitation

- Automated
- Needs support for users

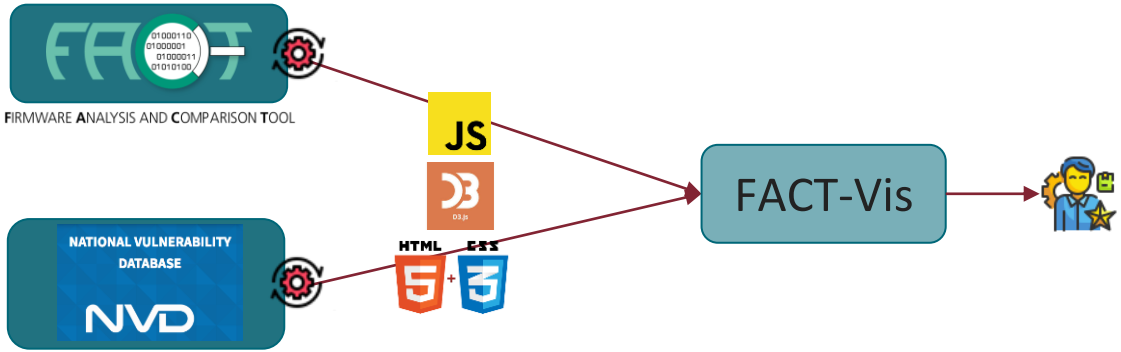
- Firmware security field requires the collaboration between **automatic tools and users**

- **Visual Analytics** connects the **human** cognitive capabilities with the **computer** computational power.



Our solution - FACT-Vis

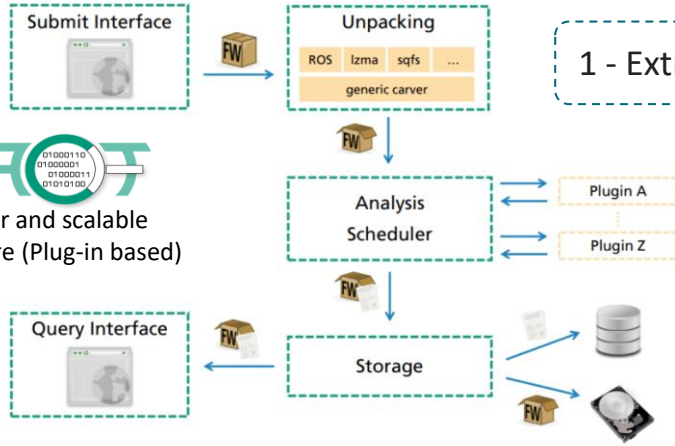
FACT-VIS: a visual tool able to support the 3 stages of the firmware analysis process



Aimed to assist a **large spectrum of users** into **support firmware analysis**, providing:

- General **overviews** of the firmware
- Specific **details** of firmware and its components
- **Report** to summarize the analysis process

FACT - NVD



Modular and scalable architecture (Plug-in based)

1 - Extraction — ***Unpacker***

2 - Analysis

Meta *info (file type, architecture, ..)*

Security *info (cracked credentials, mitigations, ..)*

3 - Report

GUI

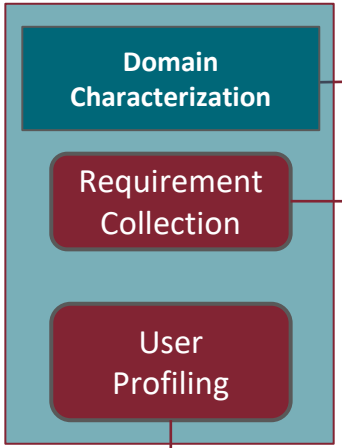
pdf ***report***

Collection of vulnerabilities and security flaws scored through the CVSS:

- Standard and public
- Prioritize risk providing both a general and specific metrics.
- Well describes how much dangerous a flaw is

Design process

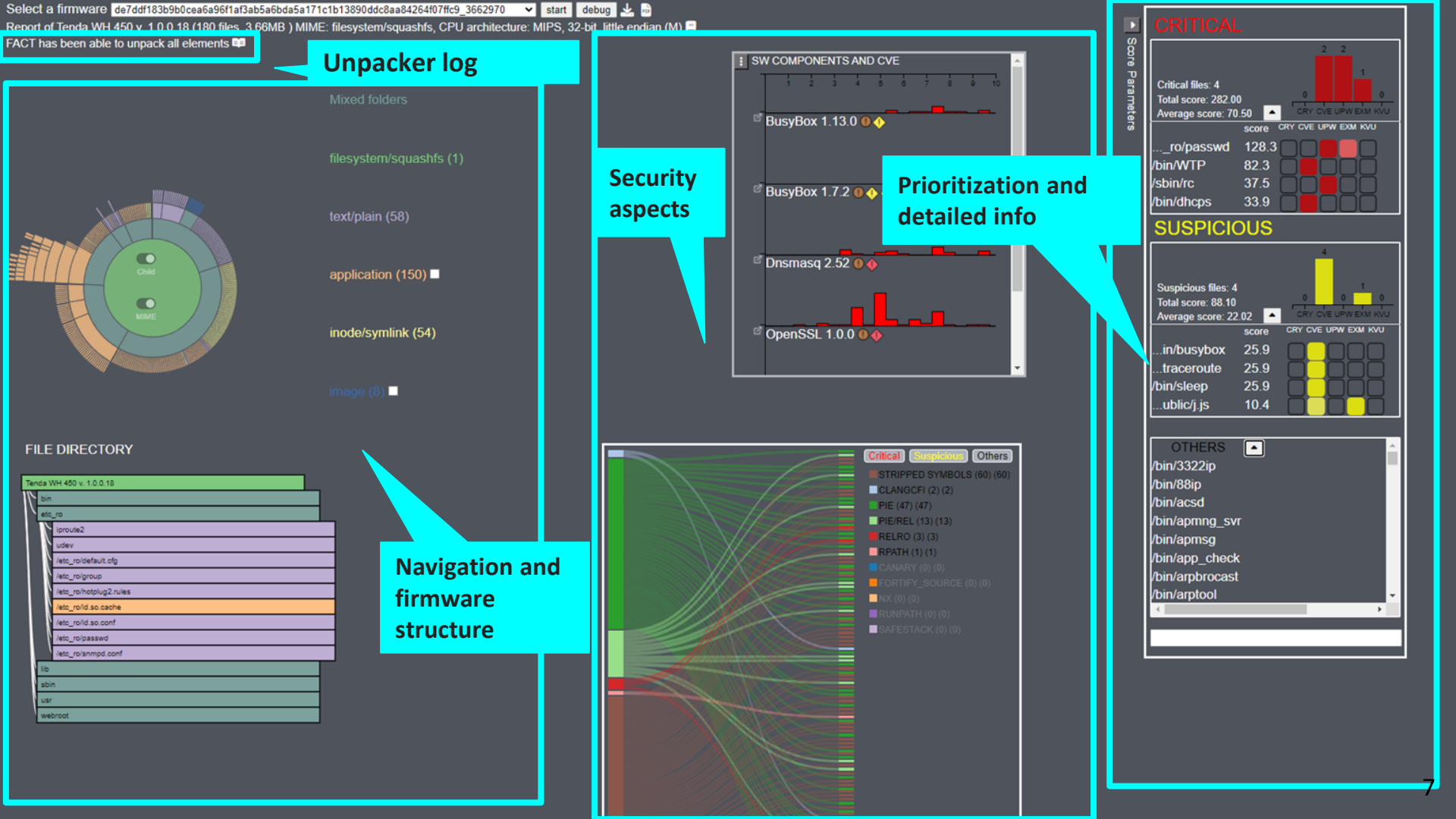
The nested model [1]: four nested layers which describe the path starting from the domain problem until the intuition of the actual solution.



Data/Task Abstraction → Design Conceptualization → Implementation: FACT-Vis

	ID	Description
Overview	R1	Capability to see the overview of the most critical file objects
	R2	Capability to see the overview of the firmware's status
Firmware	R3	Capability to analyze the firmware
	R3.1	Capability to see the overview of the firmware composition
	R3.2	Capability to maintain the focus only on certain aspects during the navigation of the firmware
File objects	R4	Capability to analyze generic file objects
	R4.1	Capability to analyze packed file objects
	R4.2	Capability to analyze security flaws associated to files objects
Report	R5	Capability to provide a concrete summary of the analysis done

[1] Interactive visual data analysis. 1st ed.

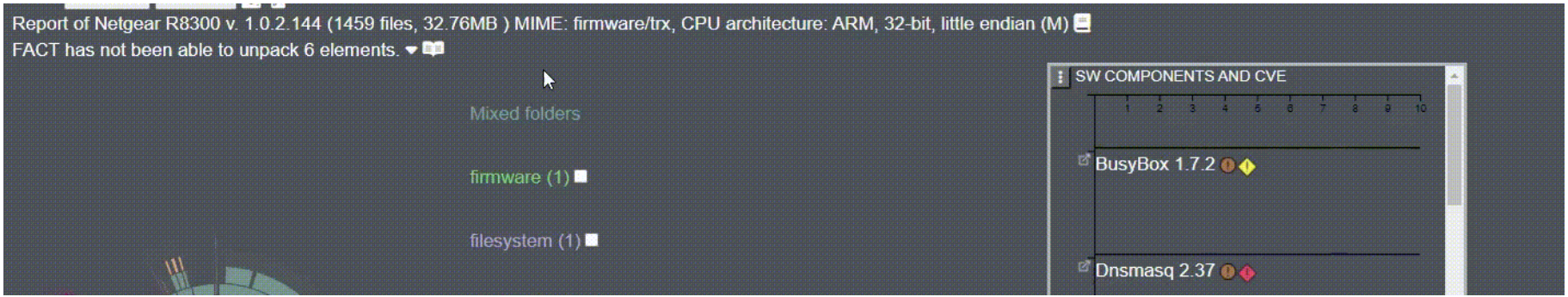

Select a firmware
de7ddf183b9b0cea6a96f1af3ab5a6bda5a171c1b13890ddc8aa84264f07ffc9_3662970
start
debug
Report of Tenda WH 450 v. 1.0.0.18 (180 files, 3.66MB) MIME: filesystem/squashfs, CPU architecture: MIPS, 32-bit, little endian (M)
FACT has been able to unpack all elements
Unpacker log
Mixed folders
filesystem/squashfs (1)
text/plain (58)
application (150)
inode/symlink (54)
image (8)
Child
MIME
FILE DIRECTORY
Tenda WH 450 v. 1.0.0.18
bin
etc_ro
iproute2
udev
/etc_ro/default.cfg
/etc_ro/group
/etc_ro/hotplug2.rules
/etc_ro/ld.so.cache
/etc_ro/ld.so.conf
/etc_ro/passwd
/etc_ro/snmpd.conf
lib
sbin
usr
webroot
Navigation and firmware structure
SW COMPONENTS AND CVE
BusyBox 1.13.0
BusyBox 1.7.2
Dnsmasq 2.52
OpenSSL 1.0.0
Security aspects
Critical
Suspicious
Others
STRIPPED SYMBOLS (60) (60)
CLANGCFI (2) (2)
PIE (47) (47)
PIE/REL (13) (13)
RELRO (3) (3)
RPATH (1) (1)
CANARY (0) (0)
FORTIFY_SOURCE (0) (0)
NX (0) (0)
RUNPATH (0) (0)
SAFESTACK (0) (0)
Prioritization and detailed info
Score Parameters
CRITICAL
Critical files: 4
Total score: 282.00
Average score: 70.50
CRY CVE UPW EXM KVU
score
.._ro/passwd 128.3
/bin/WTP 82.3
/sbin/rc 37.5
/bin/dhcps 33.9
SUSPICIOUS
Suspicious files: 4
Total score: 88.10
Average score: 22.02
CRY CVE UPW EXM KVU
score
...in/busybox 25.9
...traceroute 25.9
/bin/sleep 25.9
...ublic/j.js 10.4
OTHERS
/bin/3322ip
/bin/88ip
/bin/acsd
/bin/apmng_svr
/bin/apmsg
/bin/app_check
/bin/arpbrocast
/bin/arptool

Unpacker

The analysis process starts from the unpacking of the firmware.

Inform the user about the unpacking process and identifies which element has not been correctly unpacked

R4.1	Capability to analyze packed file objects



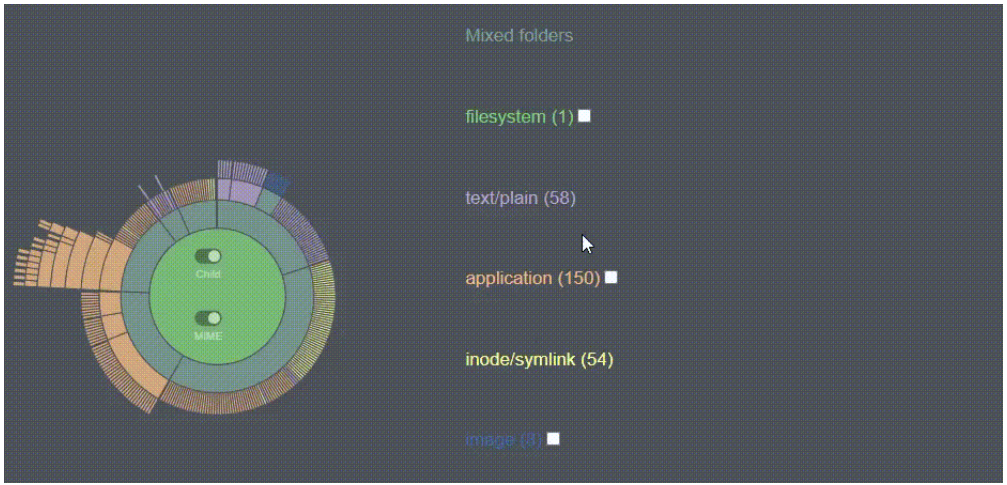
NOTE: this process is prone to errors, it can produce false positives or files with some garbage attached at the end → **need to alert the user**

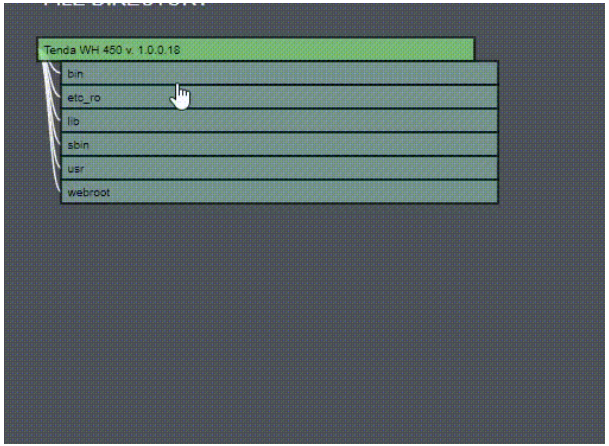
Firmware Navigation

After the extraction, the user need to explore the firmware

Overview and navigation must coexists in this phase, so we need two **synchronized** and **customizable visualization** according to the user needs

R3	Capability to explore the firmware
R3.1	Capability to see the overview of the firmware composition
R3.2	Capability to maintain the focus only on certain aspects during the navigation of the firmware



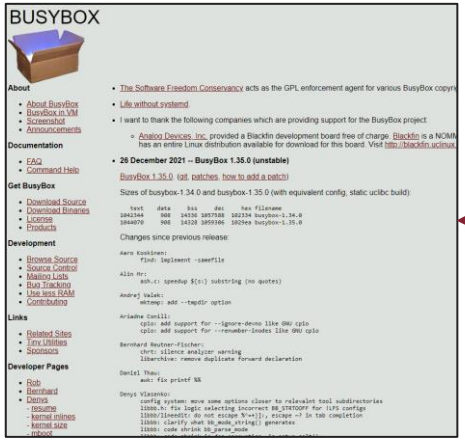


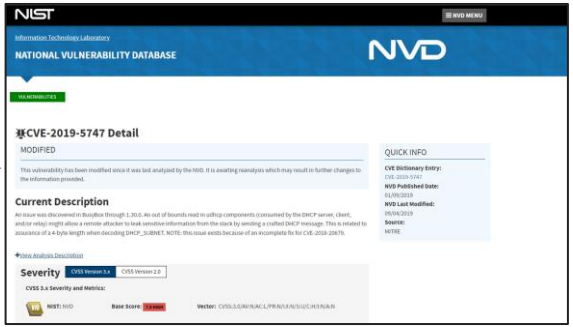
Software components and CVE

The user checks the sw component security aspects

Through cve external data sources and integration, each component shows its cve distribution according to different parameters

R2	Capability to see the overview of the firmware's status
R4.2	Capability to analyze security flaws associated to files objects



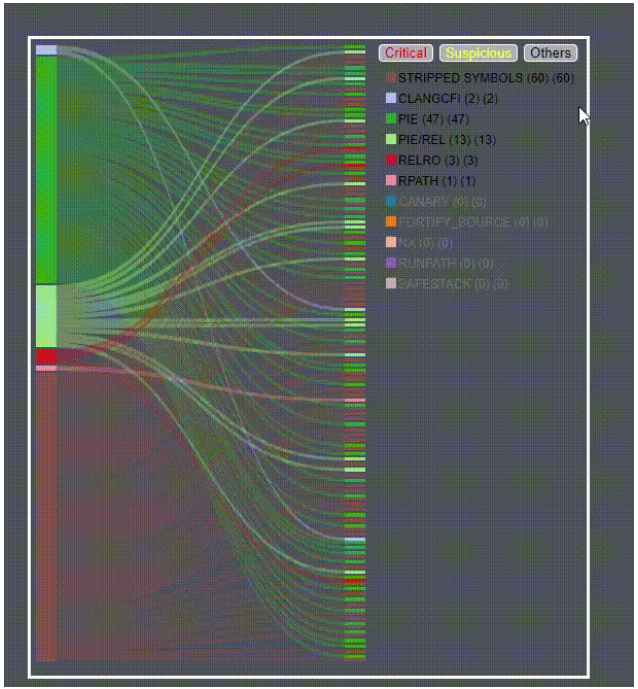


Exploit mitigation

The user checks the file objects security aspects

Bipartite Graph capable to inspect the security problems of a single file object and/or visualize the spread of security best practices

- Mitigations found in executable files encoded following the color set in the legenda.
- File objects in function of mitigations and vice versa



R2	Capability to see the overview of the firmware's status
R4.2	Capability to analyze security flaws associated to files objects

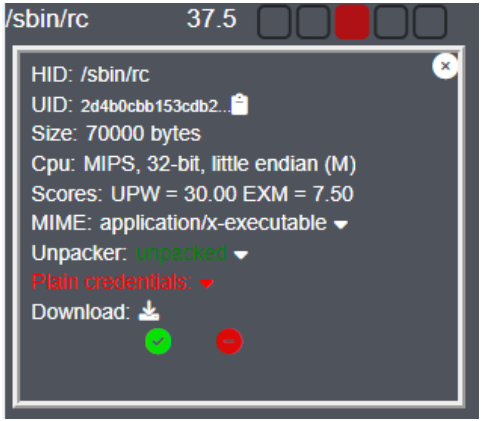
Rank Danger

Main goal is to prioritize the files based on their security aspects

FACT-Vis automatically categorize a file as **Critical** , **Suspicious** or **Other**

R1	Capability to see the overview of the most critical file objects

Each flaw is counted and weighted based on the user needs

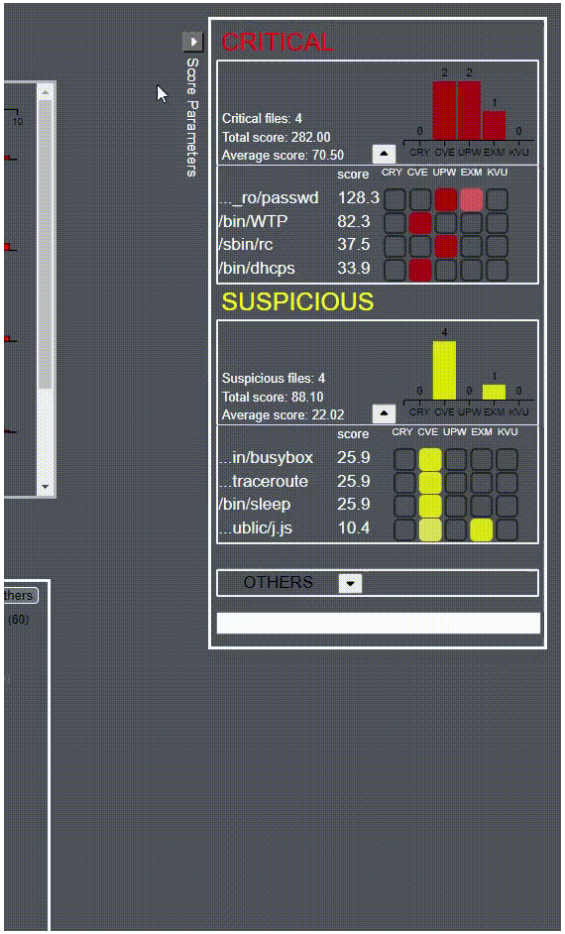


R2	Capability to see the overview of the firmware's status

Bar chart and score information

R4	Capability to analyze generic file objects

Technical data sheet and personal file information



Report

R5 Capability to provide a concrete summary of the analysis done

Report of Tenda WH 450 v. 1.0.0.18

Metadata

Vendor: Tenda
Name: WH 450
Size: 3662970 Bytes
Version: 1.0.0.18
device class: Misc
Total files: 180

File Types

application/x-executable : 89
text/plain : 58
inode/symlink : 54
application/x-sharedlib : 47
application/x-object : 13
image/gif : 5
image/png : 3
application/octet-stream : 1
filesystem/squashfs : 1

Exploit Mitigations

STRIPPED SYMBOLS: 60
PIE: 47
PIE/REL: 13
RELRO fully: 3
CLANGCFI: 2
RPATH: 1

Analysis of file objects

Critical Files

HID	Score	State
/etc_ro/passwd	128.3	Safe
/bin/WTP	82.3	Dangerous
/sbin/rc	37.5	Safe
/bin/dhcps	33.9	Safe

Suspicious Files

HID	Score	State
/bin/busybox	25.9	Safe
/sbin/traceroute	25.9	Safe
/bin/sleep	25.9	Dangerous
/webroot/public/j.js	10.4	Dangerous

Parameters

Parameter	Value
W_CRYPTO	30
W_CVE_CRIT	0.2
W_CVE_N_CRIT	0.1
SCORE_TYPE	base_score
W_USR_N_PWD	30
W_EXPLOIT	1.5
W_KNOWN_VULN	5
THRESHOLD	29

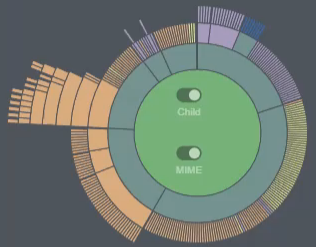
Software Components and CVE

ID	Name	CVE	Critical	Critical files	Suspicious Files
1	OpenSSL 1.0.0	72	true	true	false
2	Dnsmasq 2.52	22	true	true	false
3	BusyBox 1.13.0	13	true	false	true
4	BusyBox 1.7.2	13	true	false	true
5	jQuery 1.7	4	false	false	true

Select a firmware de7ddf183b9b0cea6a96f1af3ab5a6bda5a171c1b13890ddc8aa84264f07ffc9_3662970 start debug

Report of Tenda WH 450 v. 1.0.0.18 (180 files, 3.66MB) MIME: filesystem/squashfs, CPU architecture: MIPS, 32-bit, little endian (M)

FACT has been able to unpack all elements



Mixed folders

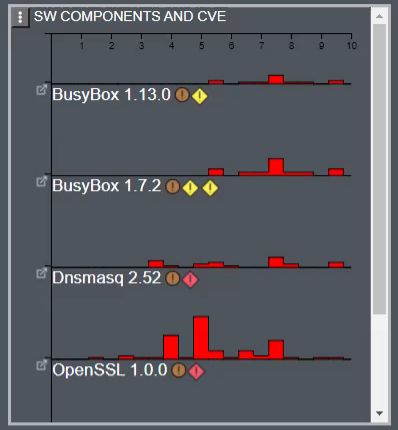
filesystem/squashfs (1)

text/plain (58)

application (150)

inode/symlink (54)

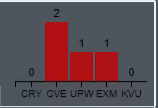
image (8)



Score Parameters

CRITICAL

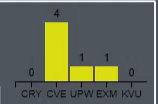
Critical files: 3
Total score: 196.50
Average score: 65.50



	score	CRY	CVE	UPW	EXM	KVU
/bin/WTP	82.3					
..._ro/passwd	80.3					
/bin/dhcps	33.9					

SUSPICIOUS

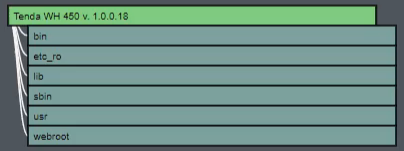
Suspicious files: 5
Total score: 113.60
Average score: 22.72

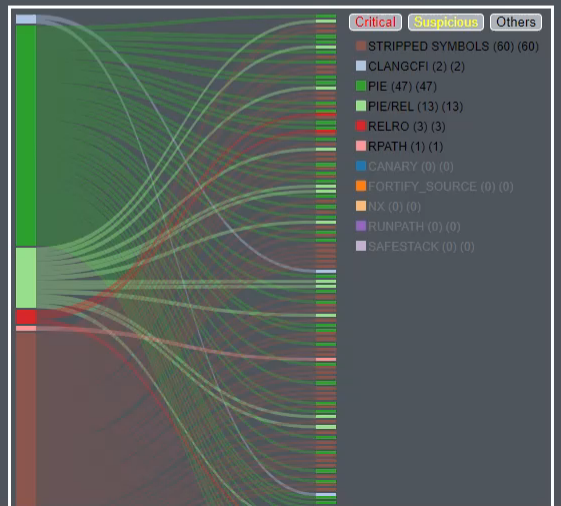


	score	CRY	CVE	UPW	EXM	KVU
...in/busybox	25.9					
...traceroute	25.9					
/bin/sleep	25.9					
/sbin/rc	25.5					
...ublic/j.js	10.4					

OTHERS

FILE DIRECTORY





Conclusion

FACT-Vis is designed to support wide range of users (from cyber-security equipes to hobbyists) in performing **firmware analysis,** enhancing FACT's power.

FACT-Vis is a **transverse project**, which connect two different fields of study: the firmware analysis and the visual analytics.

Future works:

- Investigate and master the OWASP stages considered
- Integrate FACT-Vis with other stages
- Consolidate FACT-Vis with the methodology
- Improve the system through user's feedback

SAPIENZA
UNIVERSITÀ DI ROMA

Thanks for your attention