IMPROVING YOUR FIRMWARE SECURITY ANALYSIS PROCESS WITH FACT

Johannes vom Dorp
“Over nine million cameras and DVRs open to APTs, botnet herders, and voyeurs”

ZDNet; 2018-10-09

“Surveillance camera compromised in 98 seconds”

The Register; 2016-11-18
AGENDA

About Speaker  Motivation  About FACT  Live Case Study D-Link  FACT application  Q & A

Who am I?  Why am I here?  Why should you care?  Want an example?  How can you benefit?  Do you have questions?
About Speaker

Who am I?

- Graduated 2016 as M.Sc. in Computer Science
- Currently research assistance at Fraunhofer FKIE in Bonn, Germany
- Started doing hardware related work in 2015
- Also in 2015 wrote first LOCs for FACT (formerly FAF)
Motivation
Why am I here?

- For the french wine obviously
- Spread the word
  - FACT was open sourced in 2017 after 2 years development
  - Tool presentations at hardwear.io in 2017, BlackHat Asia & Europe in 2018
  - Currently at 262 Stars on GitHub
  - There's room to grow
- Interact with community to get feedback / improve on use cases
  - Has someone used it?
  - What would you want to do with it?
  - Is it important to have a christmas theme to use in december?
Typical firmware analysis process

I
Unpacking
About FACT
Why should you care?

Typical firmware analysis process

I  Unpacking

II  Tool-based information gathering
About FACT
Why should you care?

Typical firmware analysis process

I  Unpacking

II  Tool-based information gathering

III  Identifying obvious weaknesses
Typical firmware analysis process

- I Unpacking
- II Tool-based information gathering
- III Identifying obvious weaknesses
- IV Reverse Engineering
Firmware analysis process with FACT

I Unpacking

II Tool-based information gathering

III Identifying obvious weaknesses

IV Reverse Engineering
About FACT
Why should you care?

Firmware Analysis and Comparison Tool
About FACT
Why should you care?

- Idea (2015)
  - “Can we improve on binwalk?”
  - Automate as much of analysis process as possible
  - Make tool as extendable as possible

- Where are we today?
  - Still using binwalk for a lot of stuff
  - FACT slots in right beside and covers different use cases
About FACT
Why should you care?

- Whata unique about FACT
  - Combines various unpacking tools (sort of unique)
  - Runs analysis in automated and in parallel (sort of unique)
  - Visualize Results both as Summary for firmware and separate / detailed for each part (pretty unique)
  - Easily extendable with simple plugin system (pretty unique)
  - Store analysis results for (super unique)
    - Comparison
    - Statistic generation
Live Case Study D-Link

Want an example?

DEMO
FACT application
How can you benefit?
FACT application
How can you benefit?

- Hacker, Security Professional
  - What’s in my
    - Home router
    - Pentesting target
    - …
FACT application
How can you benefit?

- Hardware / Firmware Engineer
  - What can I learn about
    - Third party hardware / code
    - Components of other departments
    - Reuse of code base
FACT application
How can you benefit?

- Security Officer
  - What patchlevel do my assets have?
  - Is there vulnerable software in my assets?
  - Generate Statistics / Graphs for Management
FACT application
How can you benefit?

- Researcher
  - Develop new analysis / algorithm as plugin to scale evaluation
  - Generate large information corpus and produce statistics for it
FACT application
How can you benefit?
Thanks and Q & A
Do you have questions?

Key Takeaways
- Check [FACT] out, you might just improve some of your processes
- Automated simple – and some advanced – repetative tasks
- Gain a better understanding of Firmware through comparison and cross reference

Thanks for your attention !!

Don’t spare the hard hitting questions
About FACT

Why should you care?

- FACT architecture
  - Multilayered automated extraction
  - Purpose-driven analysis scheduling
  - Storage for querying, visualization
About FACT
Why should you care?

- Some useful analysis plugins
  - Linux-style FW
    - elf analysis (behavior tagging)
    - exploit mitigations (nx, canary, relro etc.)
    - cwe checker
    - source code analysis
  - Arbitrary FW
    - binwalk (yes, that binwalk)
    - crypto material
    - software components
    - (known vulnerabilities)
About FACT
Why should you care?

- Interfacing
  - Web UI
    - (Mostly) intuitive click-and-see interface
    - Full functionality exposed
    - Use for analysis, monitoring, querying, statistics
  - REST API
    - Most functionality exposed
    - Use for automation, repetitive tasks, integration

https://localhost/about