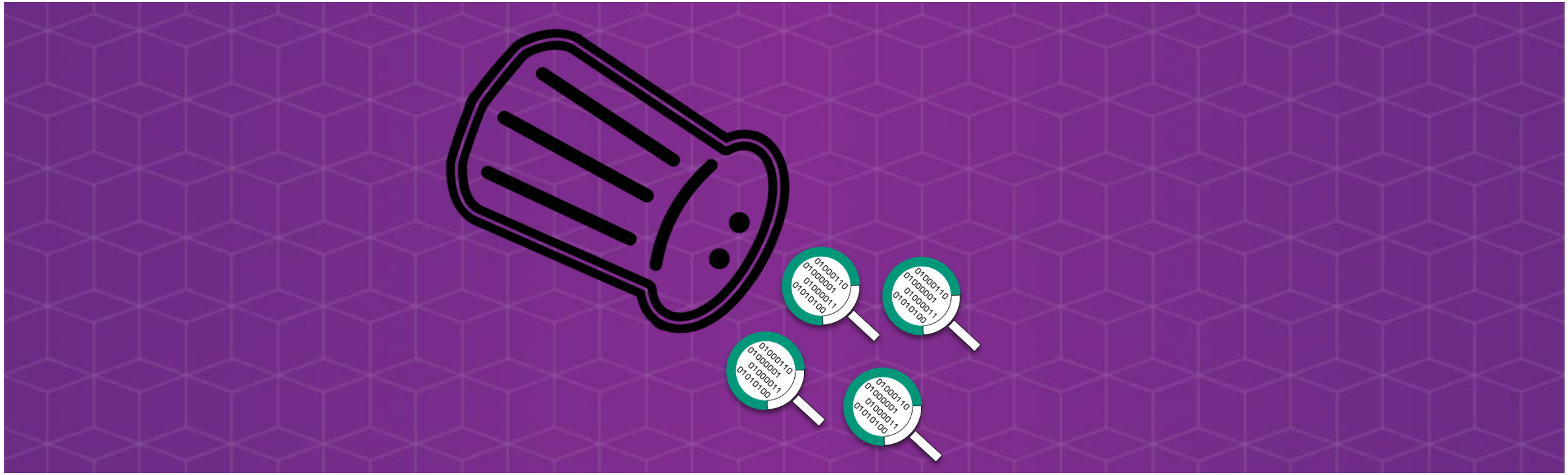
IMPROVING YOUR FIRMWARE SECURITY ANALYSIS PROCESS WITH FACT

Johannes vom Dorp

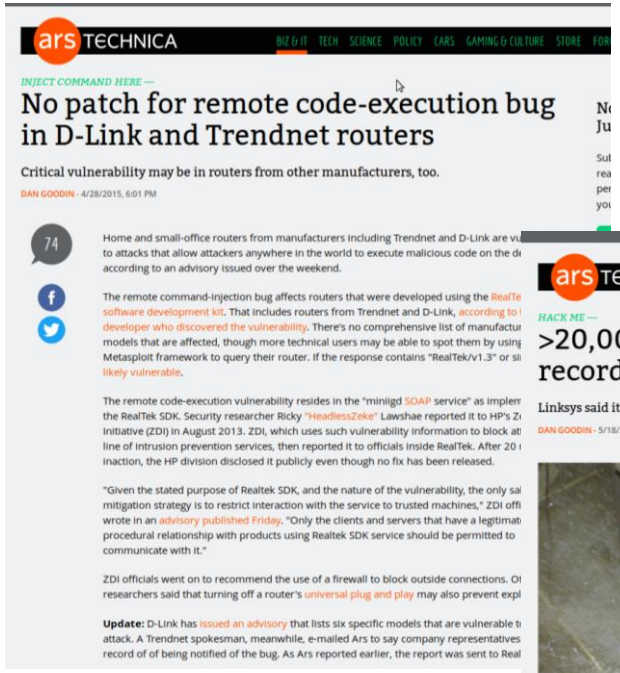
@FAandCTool

@jovomdorp



"Over nine million cameras and DVRs open to APTs, botnet herders, and voyeurs"

ZDNet; 2018-10-09


ars TECHNICA

INJECT COMMAND HERE —

No patch for remote code-execution bug in D-Link and Trendnet routers

Critical vulnerability may be in routers from other manufacturers, too.

DAN GOODIN - 4/28/2015, 6:01 PM

74

Home and small-office routers from manufacturers including Trendnet and D-Link are vu to attacks that allow attackers anywhere in the world to execute malicious code on the de according to an advisory issued over the weekend.

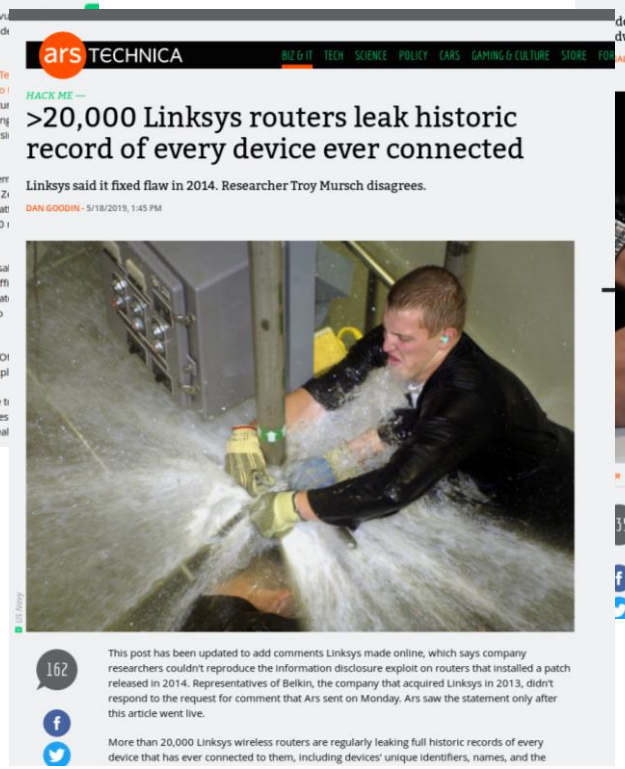
The remote command-injection bug affects routers that were developed using the RealTe software development kit. That includes routers from Trendnet and D-Link, according to t developer who discovered the vulnerability. There's no comprehensive list of manufactur models that are affected, though more technical users may be able to spot them by using Metasploit framework to query their router. If the response contains "RealTek/v1.3" or sli likely vulnerable.

The remote code-execution vulnerability resides in the "miniigd SOAP service" as implem the RealTek SDK. Security researcher Ricky "HeadlessZeke" Lawshae reported it to HP's Z Initiative (ZDI) in August 2013. ZDI, which uses such vulnerability information to block att line of intrusion prevention services, then reported it to officials inside RealTek. After 20 inaction, the HP division disclosed it publicly even though no fix has been released.

"Given the stated purpose of Realtek SDK, and the nature of the vulnerability, the only sa mitigation strategy is to restrict interaction with the service to trusted machines," ZDI offi wrote in an advisory published Friday. "Only the clients and servers that have a legitimat procedural relationship with products using Realtek SDK service should be permitted to communicate with it."

ZDI officials went on to recommend the use of a firewall to block outside connections. O researchers said that turning off a router's universal plug and play may also prevent expl

Update: D-Link has issued an advisory that lists six specific models that are vulnerable t attack. A Trendnet spokesman, meanwhile, e-mailed Ars to say company representatives record of of being notified of the bug. As Ars reported earlier, the report was sent to Real


ars TECHNICA

HACK ME —

>20,000 Linksys routers leak historic record of every device ever connected

Linksys said it fixed flaw in 2014. Researcher Troy Mursch disagrees.

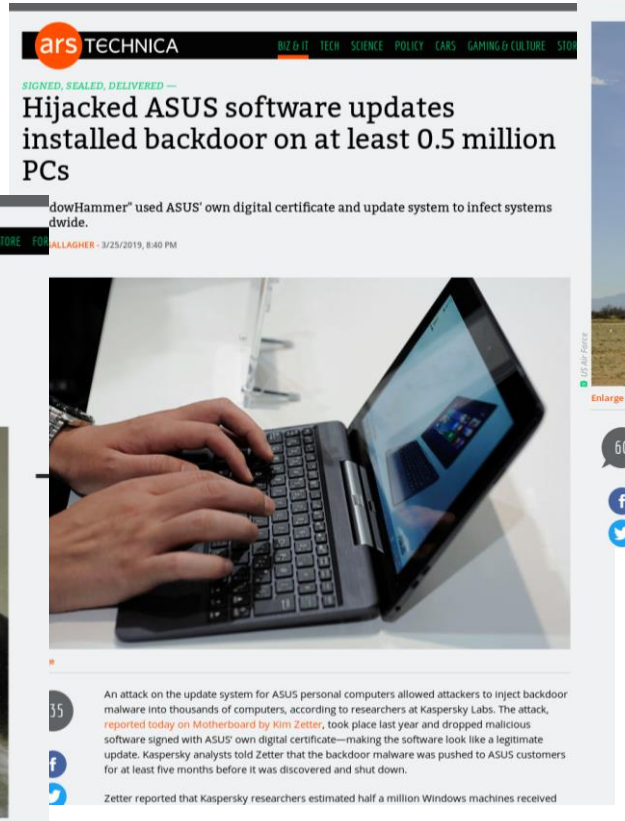
DAN GOODIN - 5/18/2019, 1:45 PM

US Navy

162

This post has been updated to add comments Linksys made online, which says company researchers couldn't reproduce the information disclosure exploit on routers that installed a patch released in 2014. Representatives of Belkin, the company that acquired Linksys in 2013, didn't respond to the request for comment that Ars sent on Monday. Ars saw the statement only after this article went live.

More than 20,000 Linksys wireless routers are regularly leaking full historic records of every device that has ever connected to them, including devices' unique identifiers, names, and the


ars TECHNICA

SIGNED, SEALED, DELIVERED —

Hijacked ASUS software updates installed backdoor on at least 0.5 million PCs

dowHammer" used ASUS' own digital certificate and update system to infect systems dwide.

ALLAGHER - 3/25/2019, 8:40 PM

US Air Force

35

An attack on the update system for ASUS personal computers allowed attackers to inject backdoor malware into thousands of computers, according to researchers at Kaspersky Labs. The attack, reported today on Motherboard by Kim Zetter, took place last year and dropped malicious software signed with ASUS' own digital certificate—making the software look like a legitimate update. Kaspersky analysts told Zetter that the backdoor malware was pushed to ASUS customers for at least five months before it was discovered and shut down.

Zetter reported that Kaspersky researchers estimated half a million Windows machines received


ars TECHNICA

FIREWALLS ON FIRE —

Cisco drops a mega-vulnerability alert for VPN devices [Updated]

By using "crafted XML," attacker could take over routers, security gateways.

SEAN GALLAGHER - 1/30/2018, 6:12 PM

Enlarge

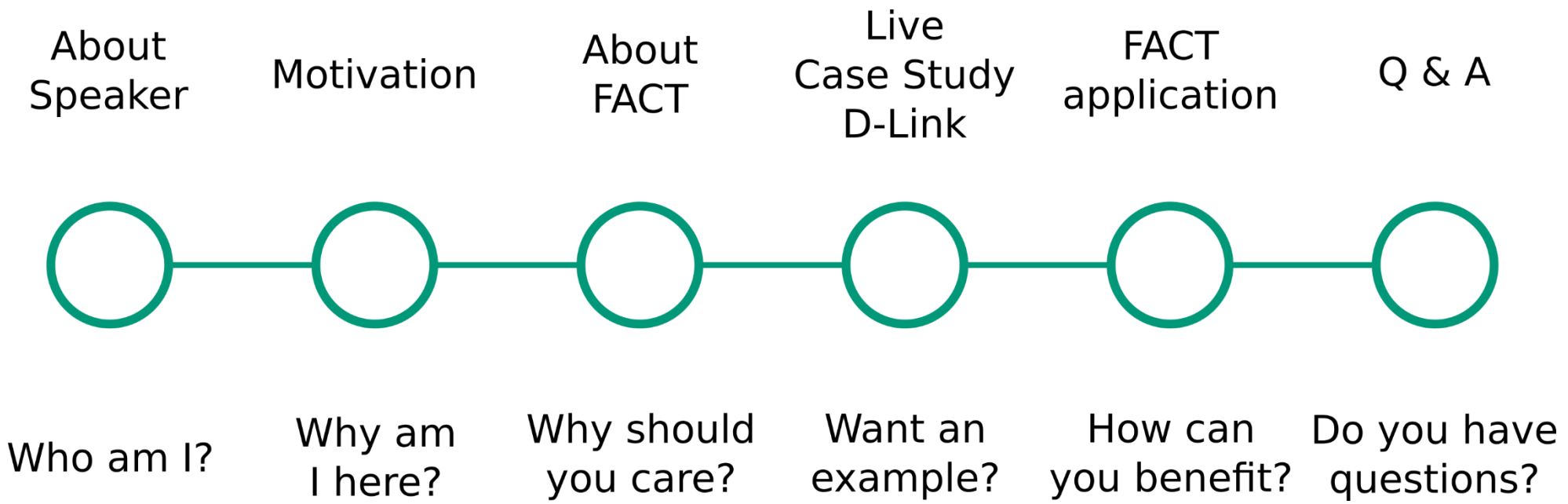
60

On January 29, Cisco released a high-urgency security alert for customers using network security devices and software that support virtual private network connections to corporate networks. Firewalls, security appliances, and other devices configured with WebVPN clientless VPN software are vulnerable to a Web-based network attack that could bypass the devices' security, allowing an attacker to run commands on the devices and gain full control of them. This would give attackers unfettered access to protected networks or cause the hardware to reset. The vulnerability has been given a Common Vulnerability Scoring System rating of Critical, with a score of 10—the highest possible on the CVSS scale.

"Surveillance camera compromised in 98 seconds"

The Register; 2016-11-18

AGENDA



About Speaker

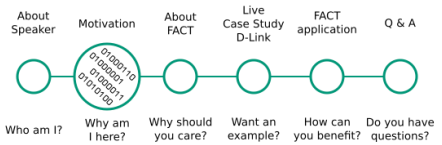
Who am I?

- 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)

Fraunhofer FKIE

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
  - Theres 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?

About FACT

Why should you care?

Typical firmware analysis process

I

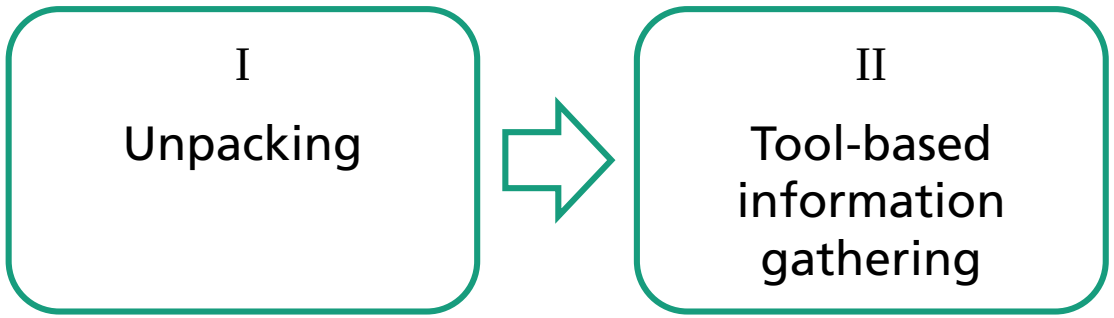
Unpacking

Fraunhofer FKIE

About FACT

Why should you care?

Typical firmware analysis process



Fraunhofer FKIE

About FACT

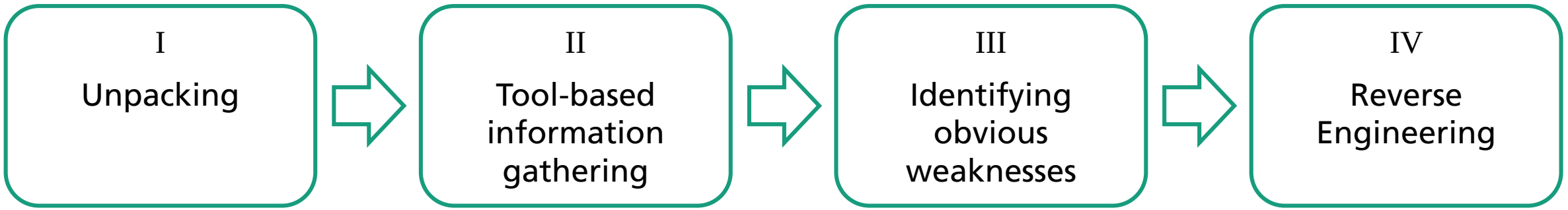
Why should you care?

Typical firmware analysis process

About FACT

Why should you care?

Typical firmware analysis process



About FACT

Why should you care?

Firmware analysis process with FACT

I
Unpacking

II
Tool-based information gathering

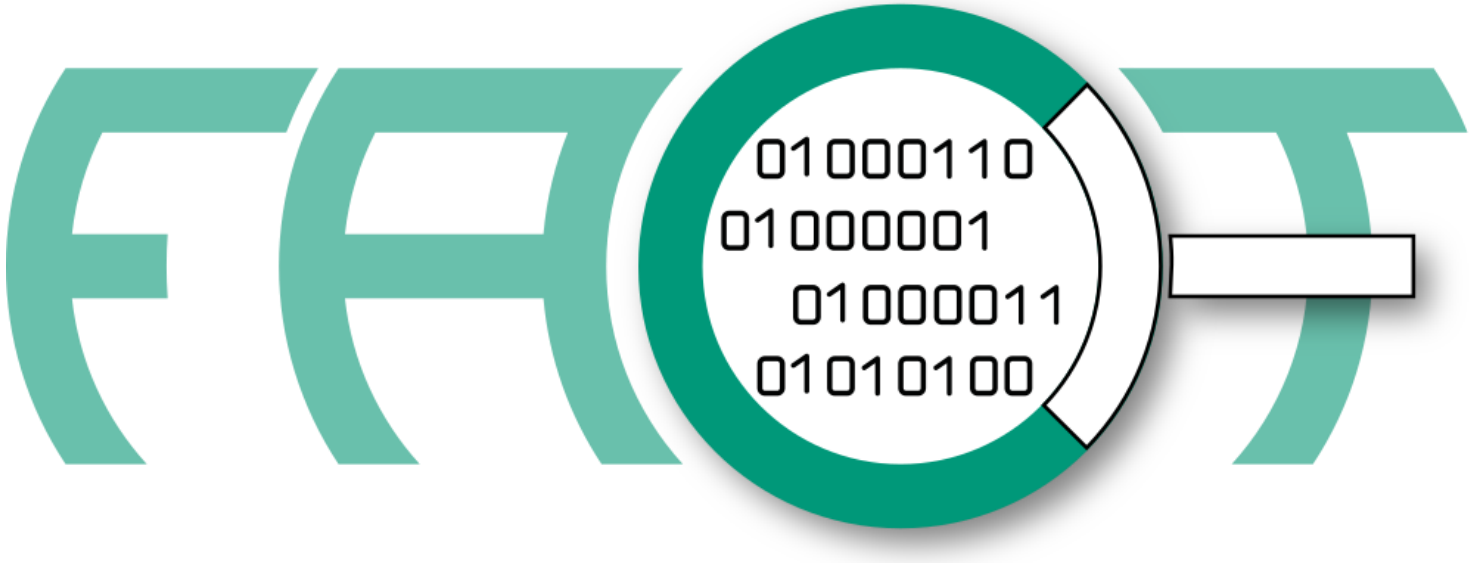
III
Identifying obvious weaknesses

IV
Reverse Engineering

Fraunhofer FKIE

About FACT

Why should you care?

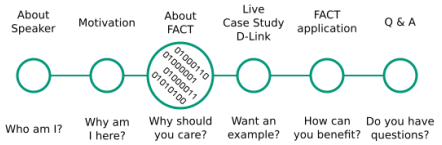


Firmware Analysis and Comparison Tool

Fraunhofer FKIE

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

Fraunhofer FKIE

About FACT

Why should you care?

- Whats 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 seperate / 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

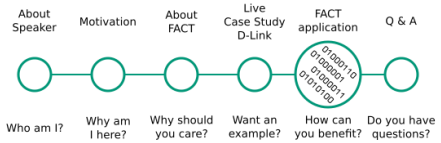
Want an example?

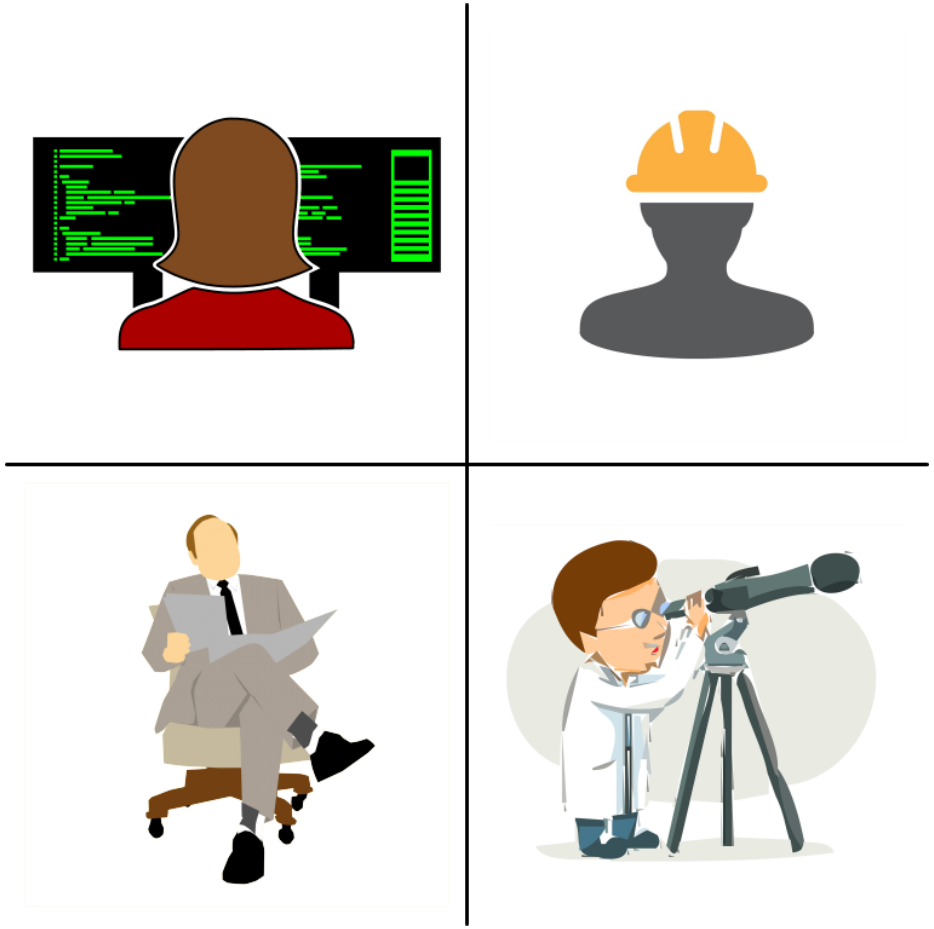
DEMO

Fraunhofer FKIE

FACT application

How can you benefit?

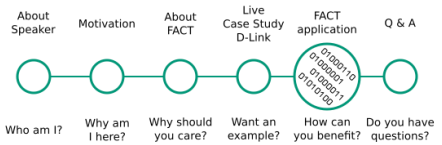




Fraunhofer FKIE

FACT application

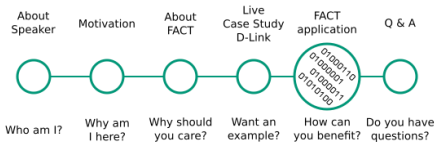
How can you benefit?



- Hacker, Security Professional
  - What's in my
    - Home router
    - Pentesting target
    - …

FACT application

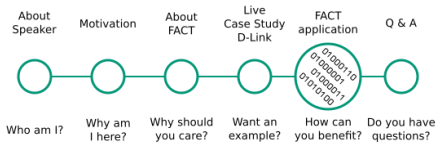
How can you benefit?



- 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?

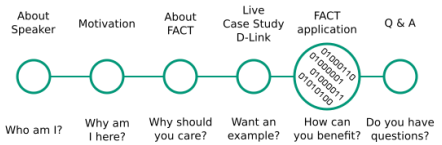


- Security Officer
  - What patchlevel do my assets have?
  - Is there vulnerable software in my assets?
  - Generate Statistics / Graphs for Management

Fraunhofer FKIE

FACT application

How can you benefit?

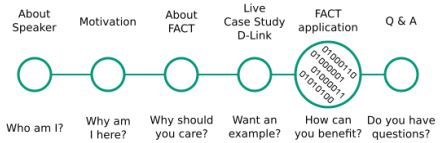


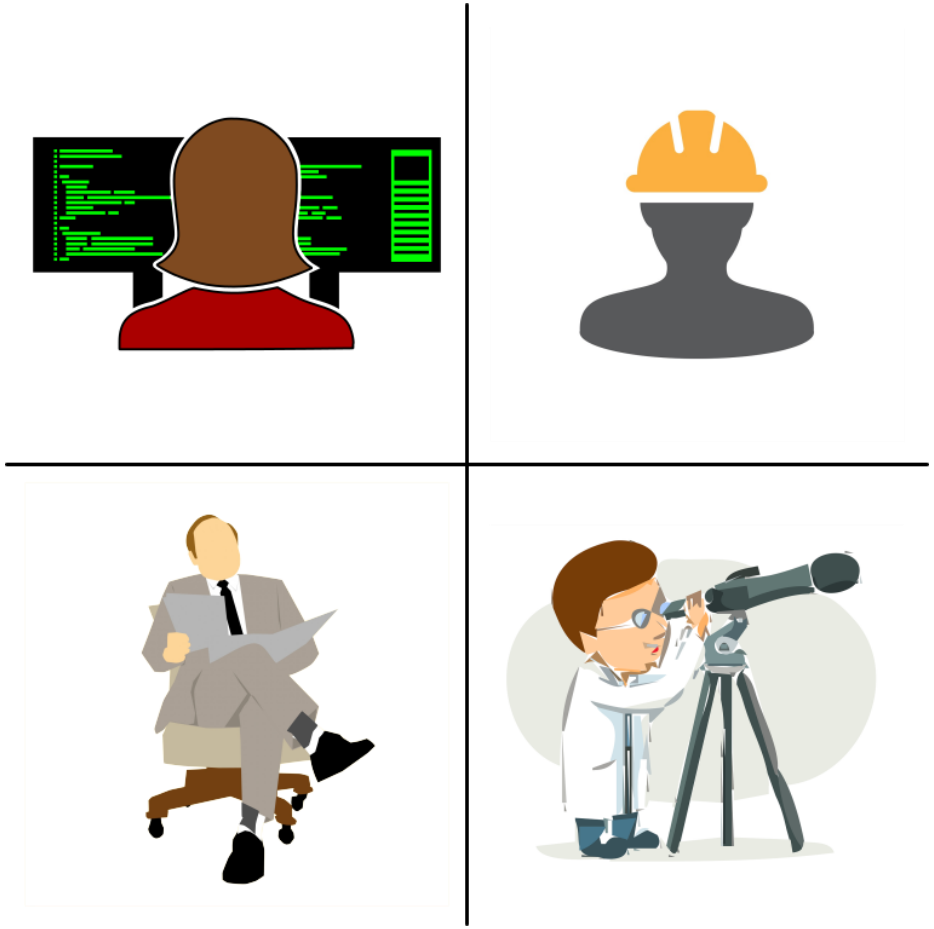
- Researcher
  - Develop new analysis / algorithm as plugin to scale evaluation
  - Generate large information corpus and produce statistics for it

Fraunhofer FKIE

FACT application

How can you benefit?

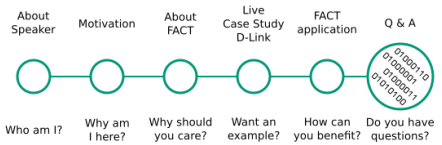




Fraunhofer FKIE

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

@FAandCTool

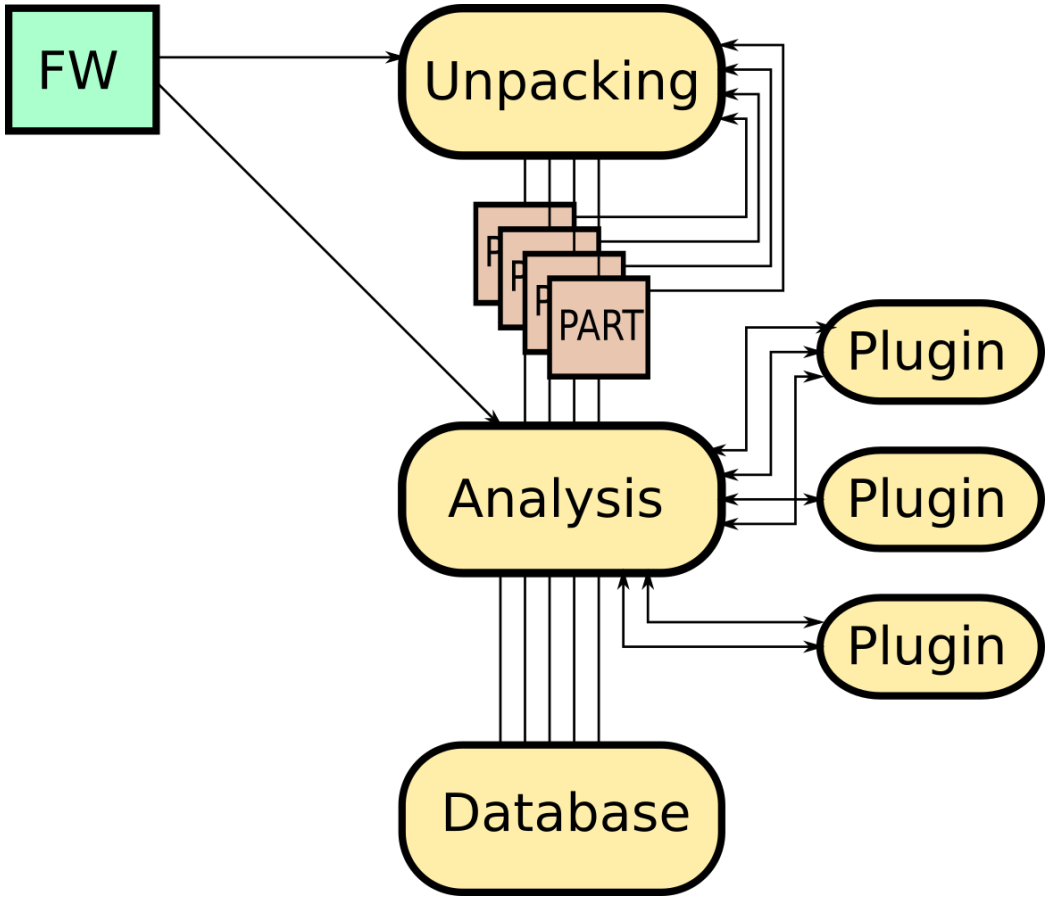
@jovomdorp

Fraunhofer FKIE

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)

- base64 decoder
- binwalk
- cpu architecture
- crypto material
- cwe checker
- elf analysis
- exploit mitigations
- file system metadata
- init systems
- ip and uri finder
- known vulnerabilities
- malware scanner
- printable strings
- qemu exec
- software components
- source code analysis
- string evaluator
- tlsh
- users and passwords

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

{ REST }