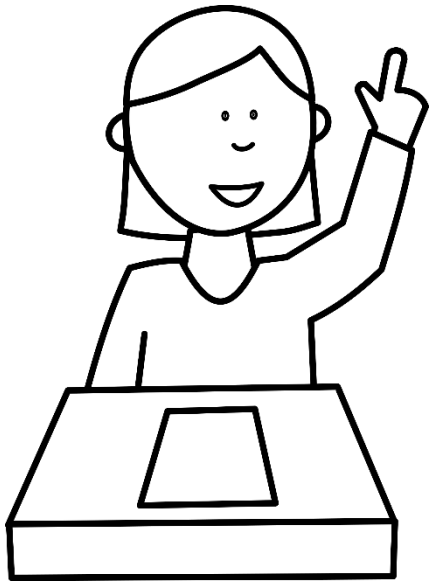
HANDS ON: SICHERHEITSLÜCKEN IN VERNETZTEN GERÄTEN AUFSPÜREN

Peter Weidenbach
peter.weidenbach@fkie.fraunhofer.de
Johannes vom Dorp
johannes.vom.dorp@fkie.fraunhofer.de

Vorstellungsrunde

Vorgehensweise

- Vorstellung von Kernpunkten des jeweiligen Themas
- Praktische Übungen
- Jederzeit Fragen stellen!
- Gemeinsame Abschlussdiskusion



Firmware - Aufbau und Betriebssysteme

- Embedded Devices sind vollwertige Computer mit:
  - CPU, Arbeitsspeicher, Festspeicher und Schnittstellen
  - Bootloader, Betriebssystem und Anwender-/Server-Software
    - Diese werden als Firmware bezeichnet
- Ein Gerät kann mehrere Embedded Devices beinhalten!

- Betriebssysteme mit Dateisystem
  - Linux
  - BSD
  - Windows
  - …
- Betriebssysteme ohne Dateisystem (Monolithen)
  - VxWorks
  - LynxOS*
  - FreeRTOS
  - …

*hat manchmal minimales Linux Dateisystem mit dem es Linux-Programme ausführen kann.

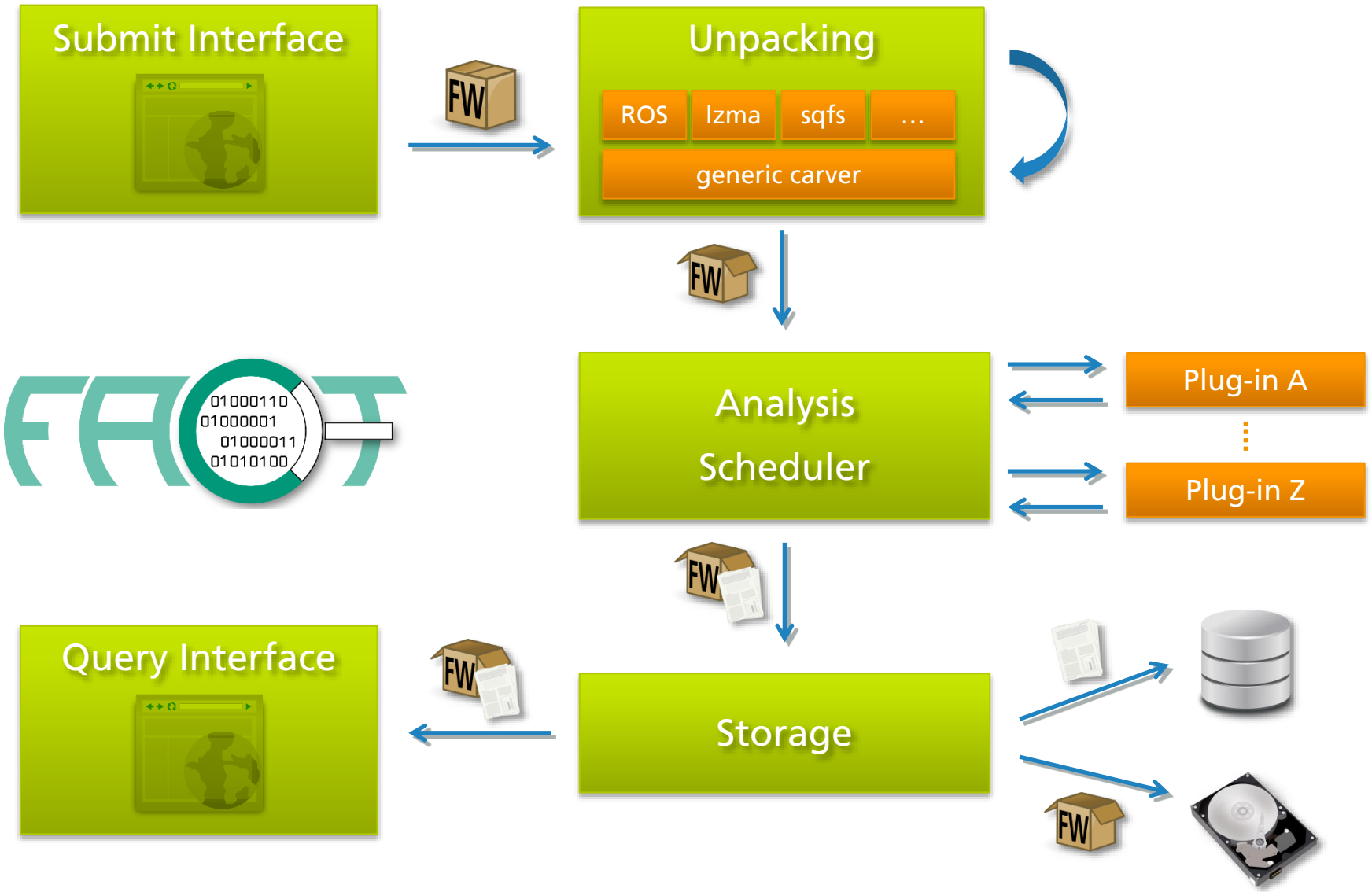
FIRMWARE ANALYSIS AND COMPARISON TOOL

- Open Source Firmware Analyse Plattform
  - Entwickelt von Fraunhofer FKIE
- Vereint diverse andere Open-Source-Analysewerkzeuge

GitHub

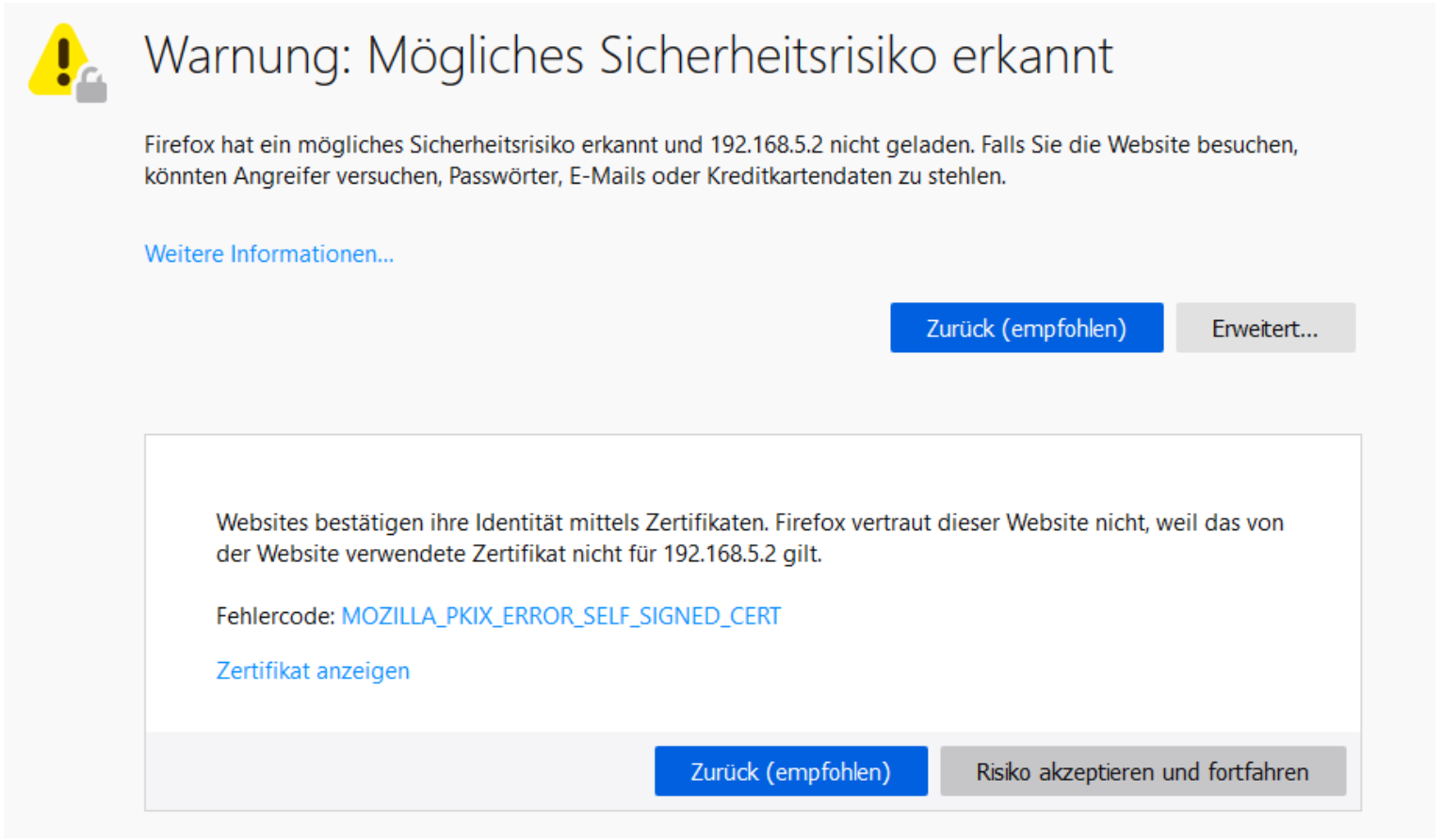
https://github.com/fkie-cad/FACT_core [1]

[1] GITHUB®, the GITHUB® logo design, OCTOCAT® and the OCTOCAT® logo design are exclusive trademarks registered in the United States by GitHub, Inc.


Submit Interface
FW
Unpacking
ROS
lzma
sqfs
…
generic carver
FW
FACT
01000110
01000001
01000011
01010100
Analysis
Scheduler
Plug-in A
Plug-in Z
FW
Query Interface
FW
Storage
FW

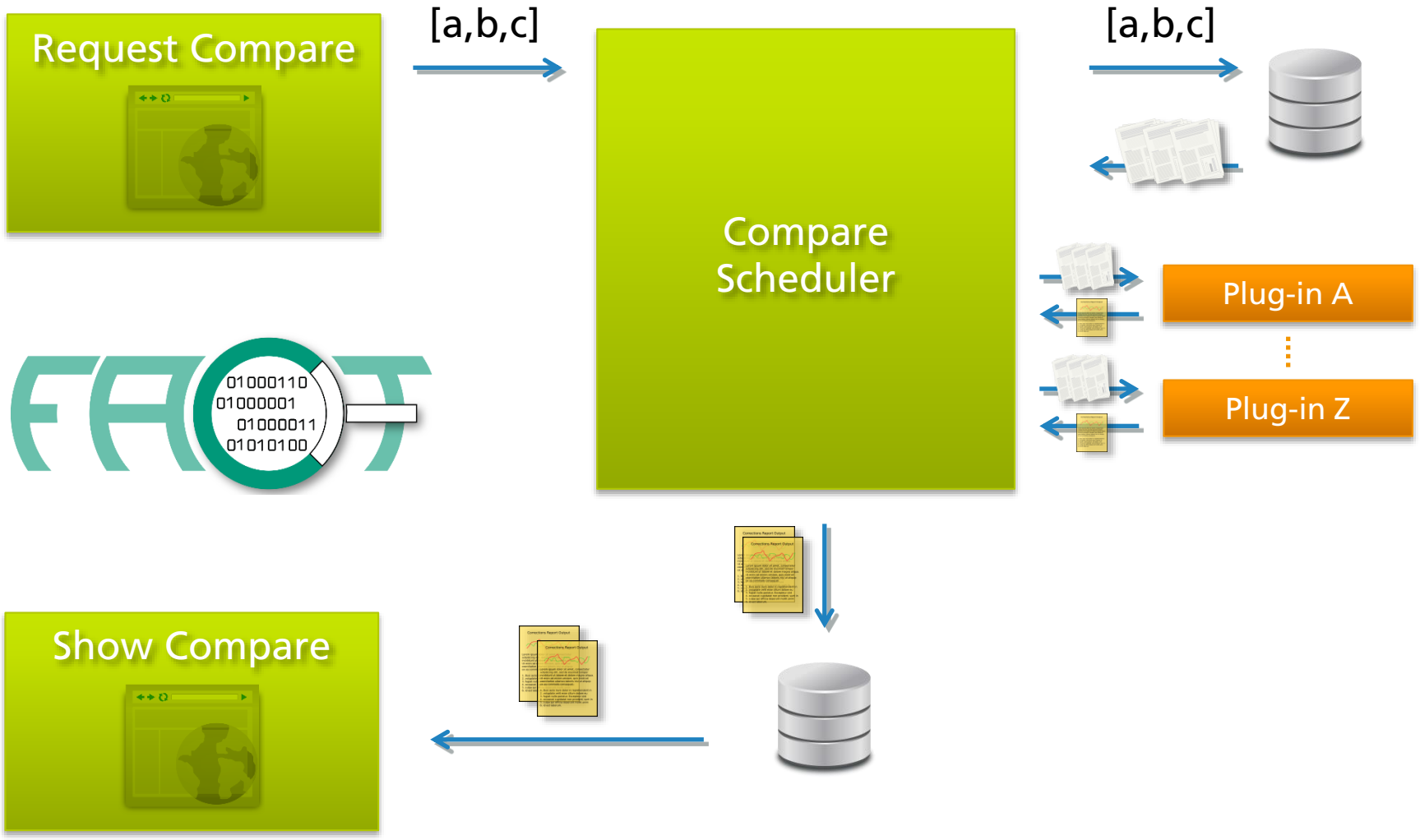
FACT TEST-System

- SSIDs:
  - FACT-A
  - FACT-B
  - FACT-C
- Passwort: FK1E!R0ck5
- FACT-Server: https://192.168.5.2



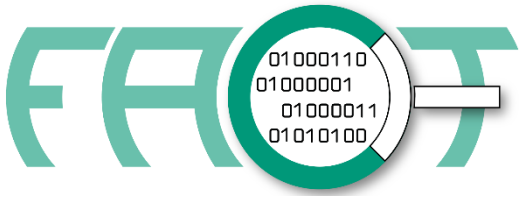
Hands On – „Statische Software-Erkennung“

- Führen die folgenden Analysen auf der Fritz!Box7490 und dem SRW2024 aus:
  - Software Detection
  - String Evaluator
- Welches Betriebssystem/Kernel Version wird verwendet?
- Welcher Web-Server kommt zum Einsatz?
- In welchen Dateien befinden sich Kernel und Web-Server?
- Welche Version hat der Web-Server?
- Welche Prozessor-Architektur treibt die Geräte an?


Request Compare
[a,b,c]
Compare Scheduler
[a,b,c]
Plug-in A
Plug-in Z
01000110
01000001
01000011
01010100
Show Compare

Hands On – „D-Link Bug-Fix“

- Vergleichen Sie die Firmware Versionen 2.02 und 2.03 des D-Link DWR-932(B1)
- Der Router enthielt einen offenen SSH-Wartungszugang mit festem Passwort
- Wie wurde diese Lücke vom Hersteller behoben?



Database Search

Binary Search

Hands On – „Alte Software“

- Linux Kernel 2.6.x wird seit 2014 nicht mehr mit Sicherheitsupdates versorgt
- Nutzen Sie die „Advanced Search“, um gefährdete Geräte in der Datenbank zu finden.

Hands On – „Abschlussdiskussion“

- Schauen Sie sich die Firmware der AVM Fritz!Box 7490 und des ASUS RT-AC5300 an.
- Basierend auf ihren Erkenntnissen: Für welchen Router würden Sie sich entscheiden.

Vielen Dank für Ihre Aufmerksamkeit.