Projektziel

FiBack zielt auf das (teil-)automatisierte **Auffinden von** (un)beabsichtigt eingebauten **Backdoors** in IT-Komponenten (Software von Drittanbietern, Appliances, IoT-Geräte) ab.

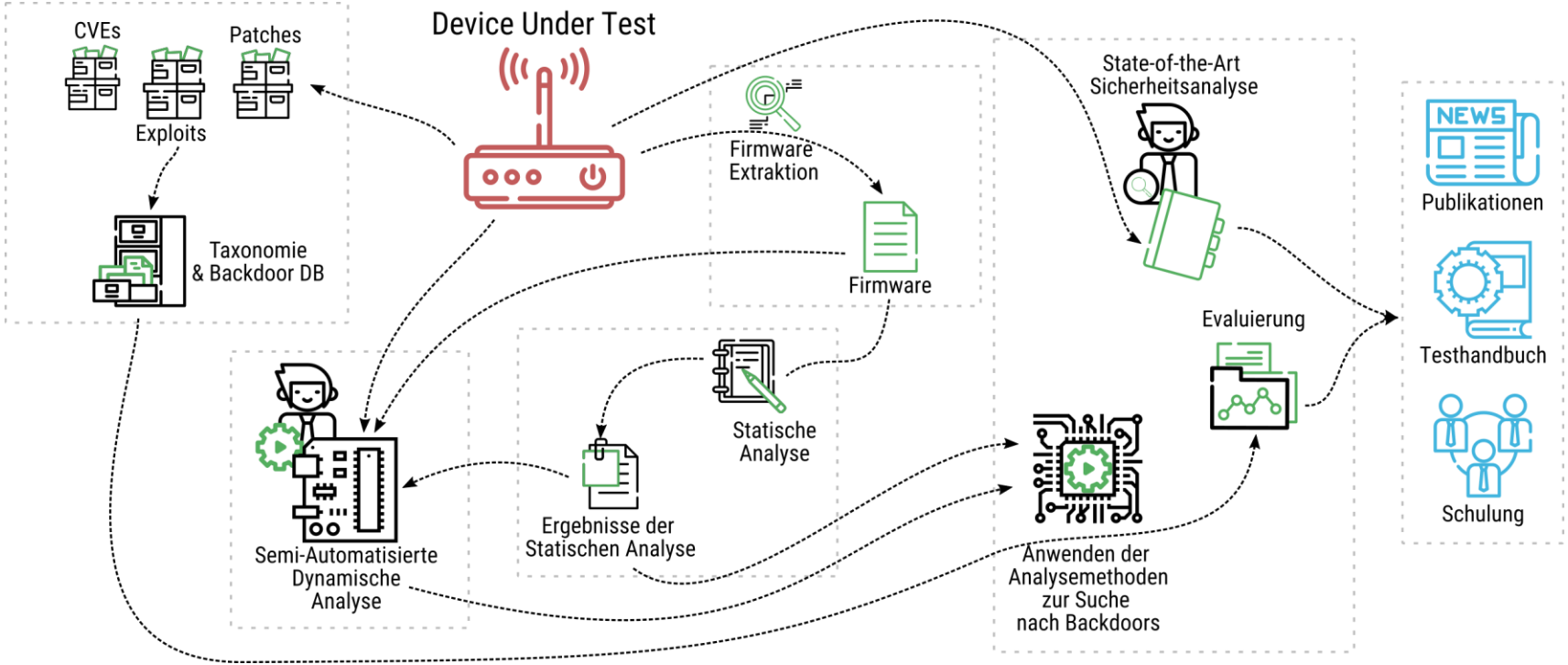
Backdoor

- Ermöglicht es Angreifer:innen unberechtigten Zugang zu geschützten Funktionen eines Systems zu erlangen
- Kann absichtlich oder unabsichtlich in ein System eingebaut sein

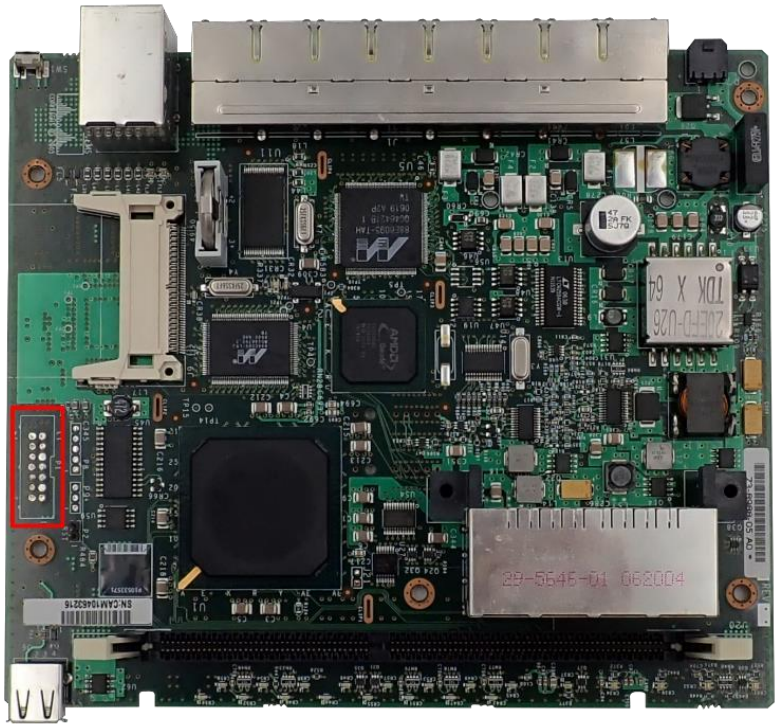
Forschungsfragen

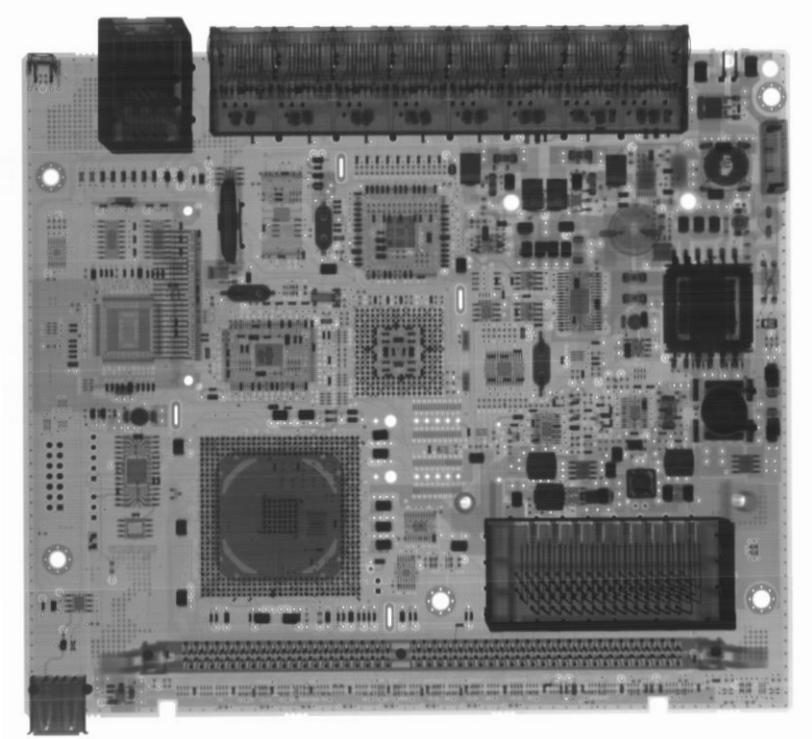
- Was ist ein Backdoor?
- Wie kommt man an die Firmware?
- Wie kann die Firmware effizient analysiert werden?
- Welche Möglichkeiten zur Identifikation von Backdoors gibt es?
- Welcher Grad an Automatisierung kann für ein Analysesystem erreicht werden?
- Wie zielsicher können Backdoors identifiziert werden?

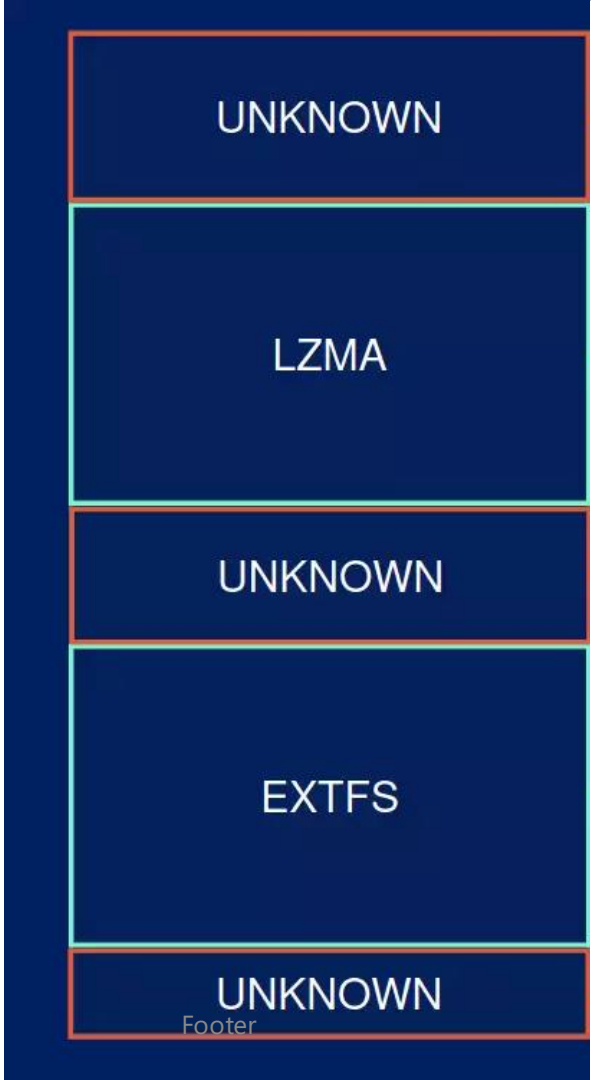
Methodologie

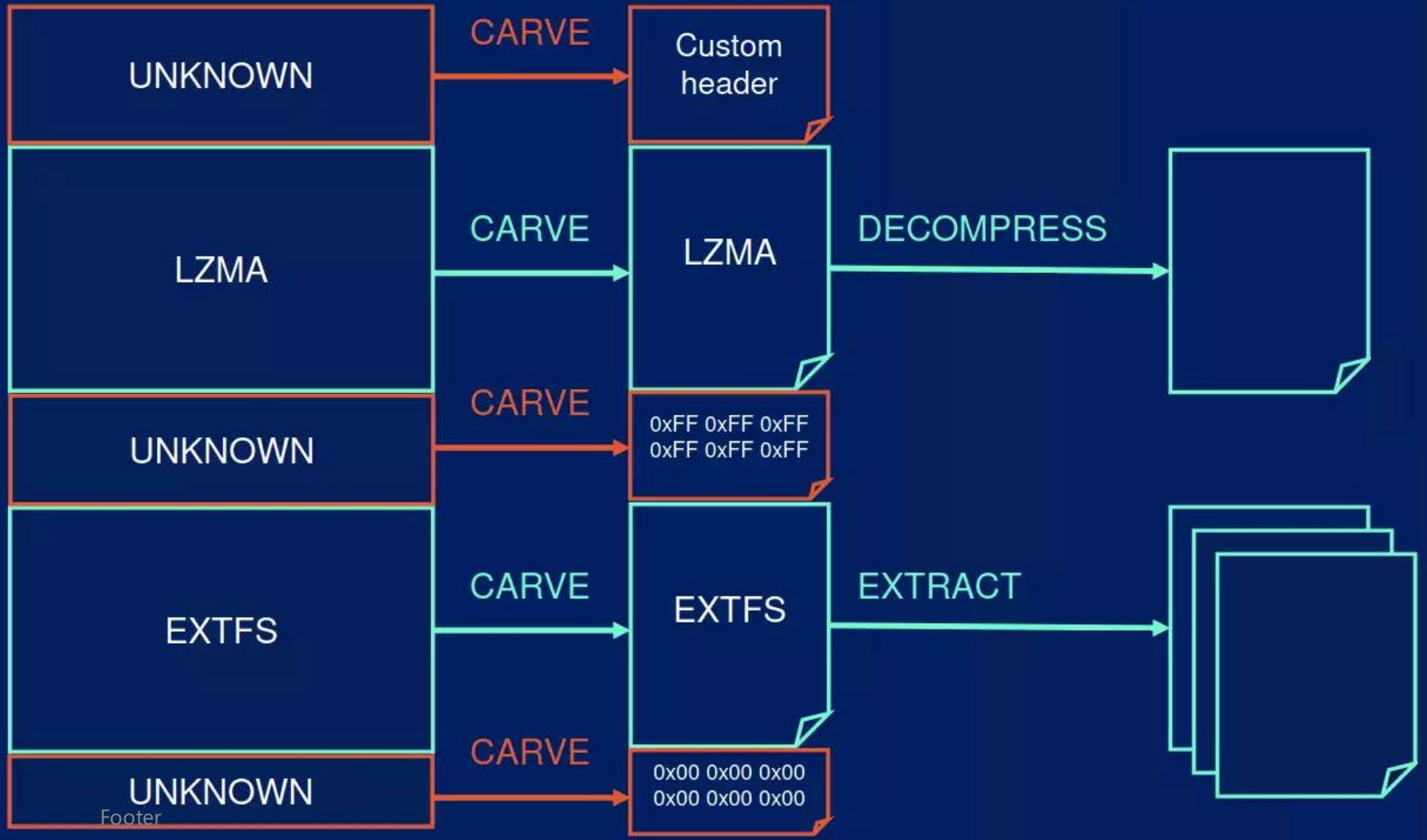


Hardware Analyse & Firmware Extraktion






UNKNOWN
LZMA
UNKNOWN
EXTFS
UNKNOWN

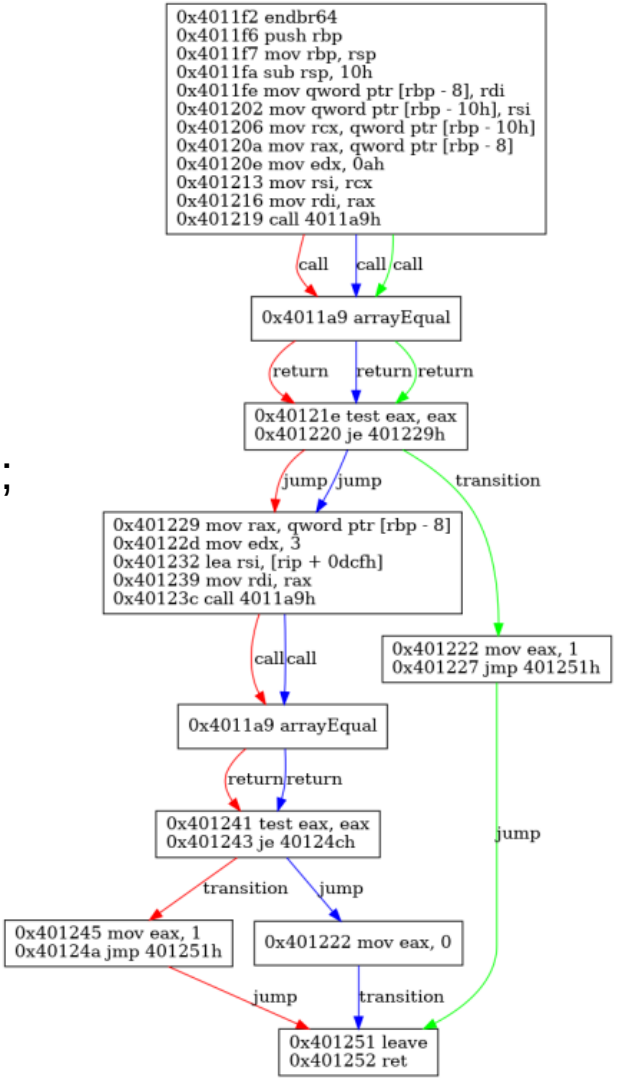

UNKNOWN
CARVE
Custom header
LZMA
CARVE
LZMA
DECOMPRESS
UNKNOWN
CARVE
0xFF 0xFF 0xFF 0xFF 0xFF 0xFF
EXTFS
CARVE
EXTFS
EXTRACT
UNKNOWN
CARVE
0x00 0x00 0x00 0x00 0x00 0x00

Firmware Aufbereitung: *unblob*

- genaue, schnelle und benutzerfreundliche Extraktionssuite
- unterstützt mehr als 30 verschiedene Archiv-, Komprimierungs- und Dateisystemformate
- verwendbar als Python Bibliothek
- veröffentlicht als Open-Source Tool unter der MIT-Lizenz: https://www.unblob.org
- Erfolgreich auf „Hacker“-Konferenzen präsentiert

Firmware Analyse & Suche nach Backdoors

```
bool check_password(int a0, int a1) {
    int v1, v2;
    if(arrayEqual(a0, a1, 10, a1, v1, v2, a1, a0)) return true;
    if(arrayEqual(a0, "pwd" 3)) return true;
    return false;
}
```



Validierung der entwickelten Methoden

- Experimentellen Suche nach Backdoors
  - Kritische Schwachstellen in mehreren WAGO Produkten
  - Responsible Disclosure Prozess
  - Security Advisory: https://onekey.com/blog/security-advisory-wago-unauthenticated-remote-command-execution/

Workshops & Wissenstransfer

- Wissenstransfer an das BMLV am Ende des Projekts in Form von Workshops
  - *unblob*
  - Erarbeitete Methoden für statische und dynamische Analysen

Zusammenfassung

- Backdoor ≠ Backdoor
  - unterscheiden sich stark
  - geplant oder ungeplant in IT-Komponenten enthalten

- Ergebnisse Forschungsprojekt
  - *unblob* wichtiges neues Tool für Firmwareaufbereitung
  - kritische Schwachstellen identifiziert
  - Wissenstransfer der erarbeiteten Methoden an das BMLV