Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Hacking The Stars

A Fuzzing Based Security Assessment of CubeSat Firmware

Berlin, 22.05.2023

Motivation

- Steigende Zahl von Satelliten
- Wenig Forschung zu deren IT-Sicherheit

Motivation

- Steigende Zahl von Satelliten
- Wenig Forschung zu deren IT-Sicherheit
- Fokus bisher: Bodenstationen

ESA OPS-SAT Mission

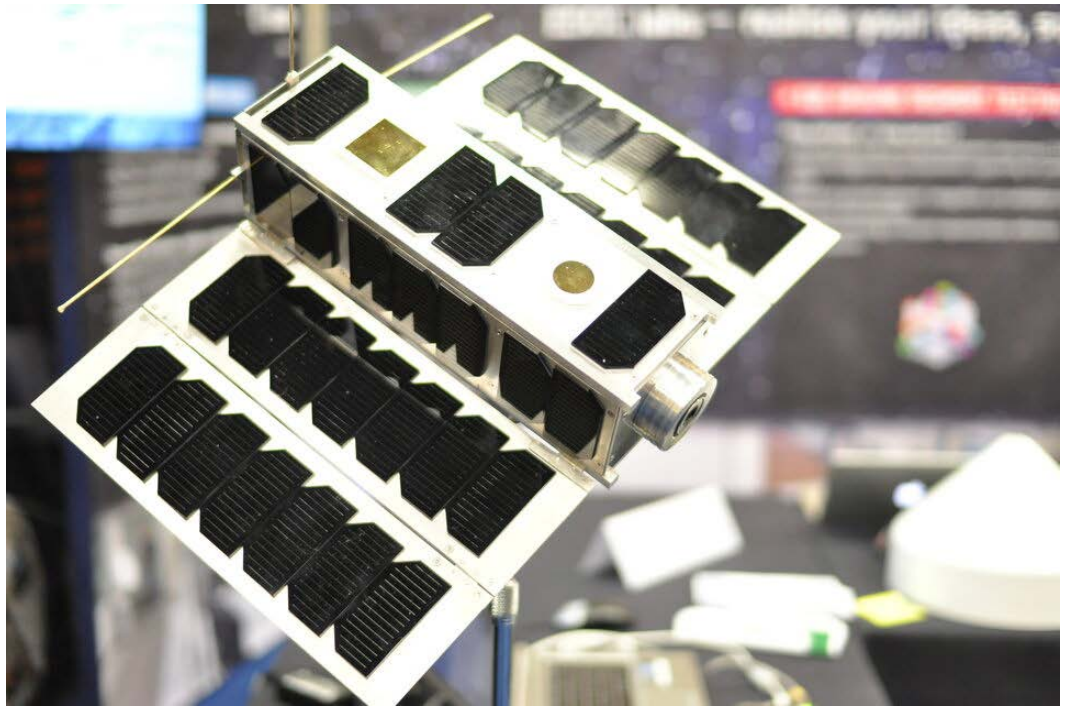


Bild: ESA

- Experimenteller Satellit (CubeSat)
- Test neuer Verfahren zur Missionskontrolle
- Offen für „jeden“

OPS-SAT Aufbau

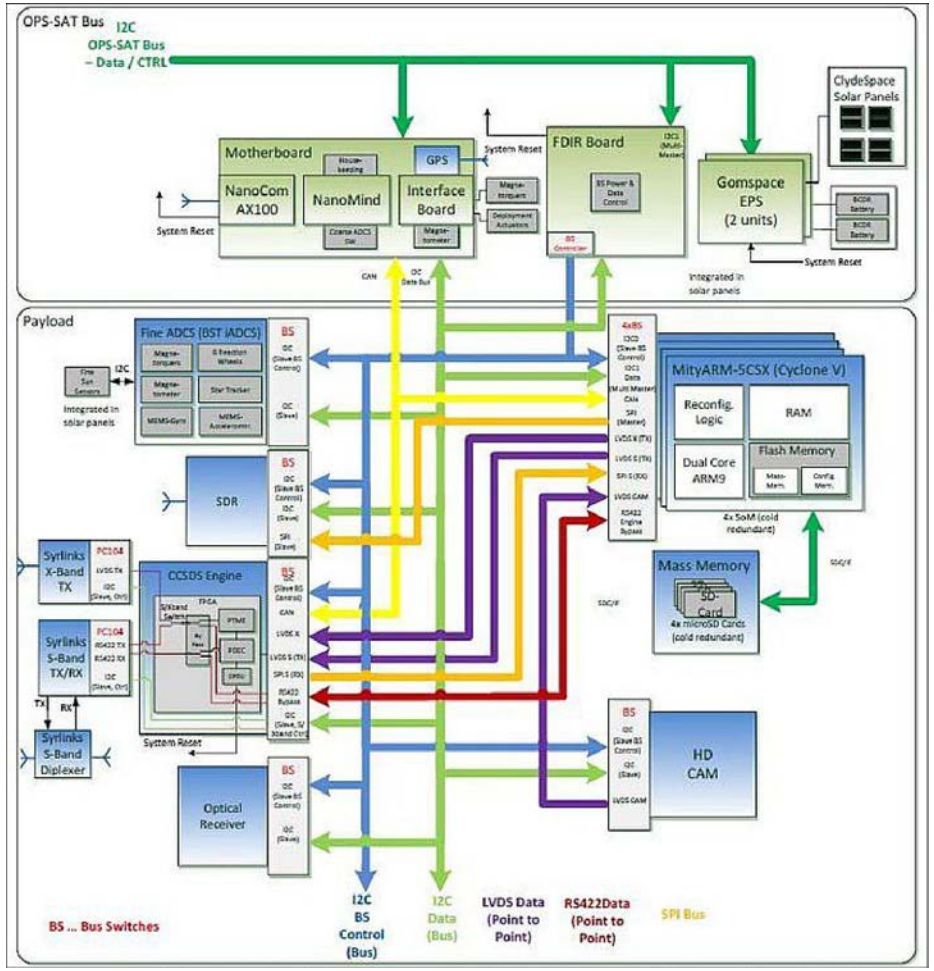


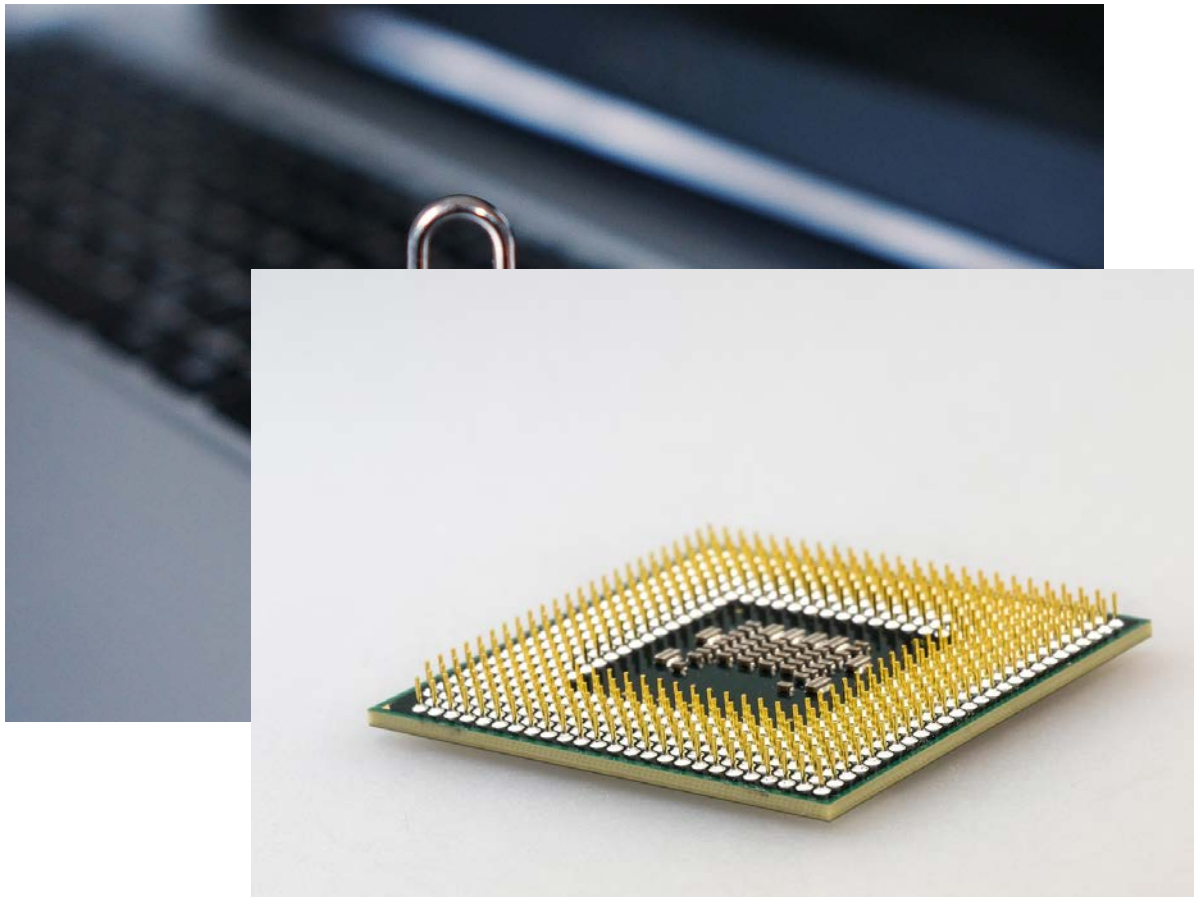
Bild: ESA

- Satellite-Bus zur Missionskontrolle
- Experimental-Plattform (Payload)
  - Kamera
  - GPS
  - Antennen
  - Laser-Kommunikaiton

Ziel

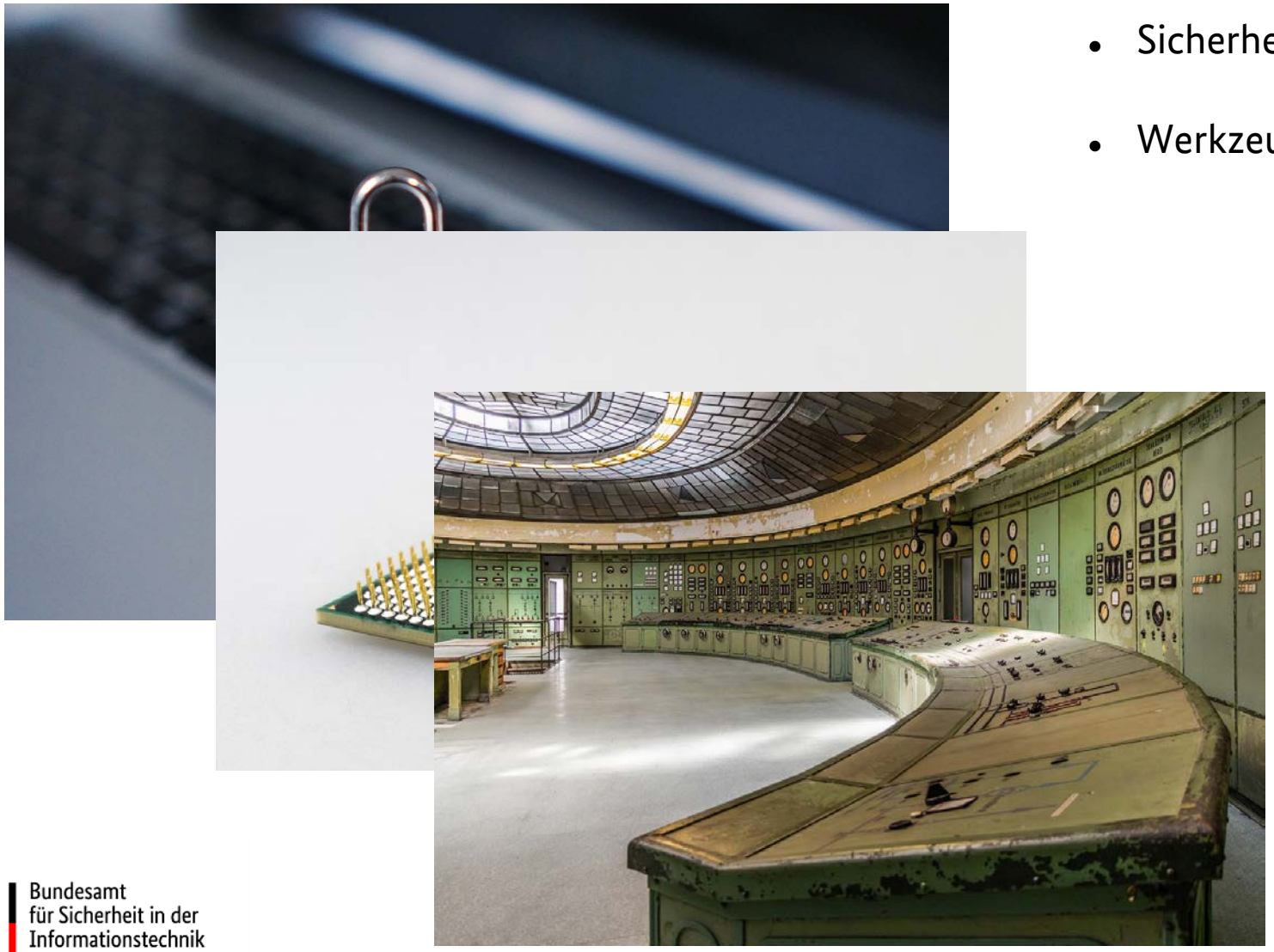
- Sicherheitsanalyse der OPS-SAT Firmware
- Werkzeug: Fuzzing

Ziel



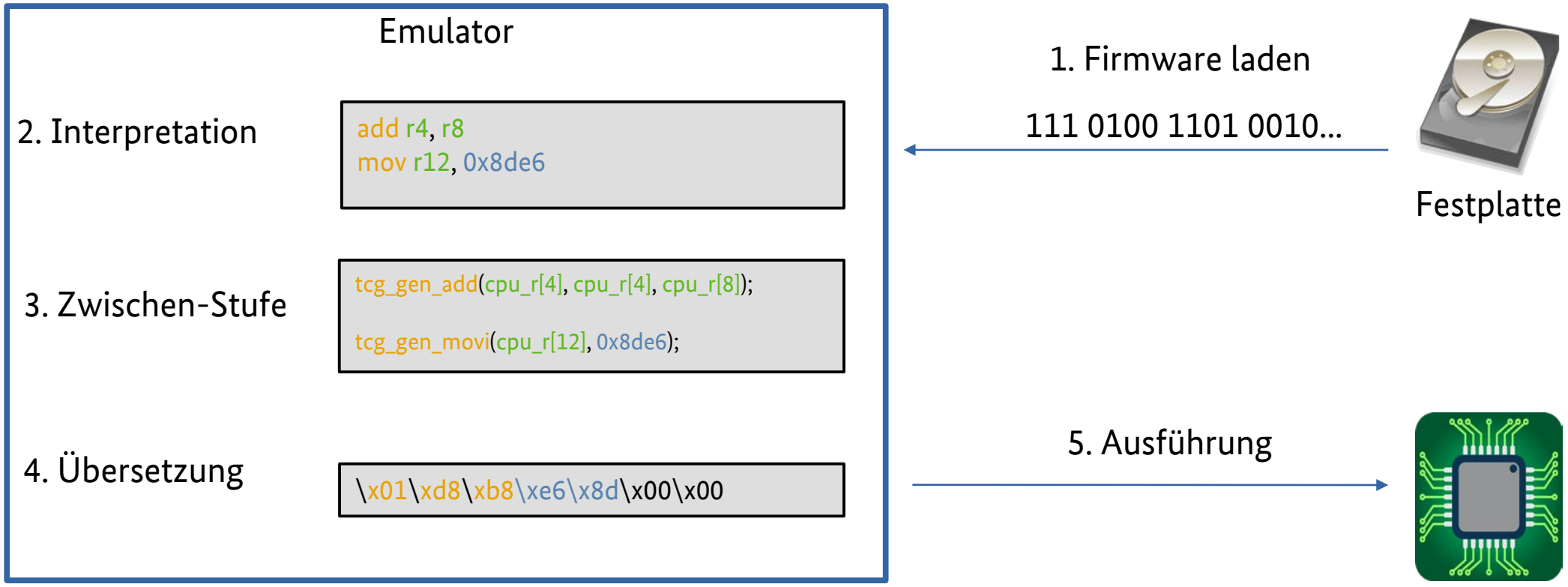
- Sicherheitsanalyse der OPS-SAT Firmware
- Werkzeug: Fuzzing

Ziel

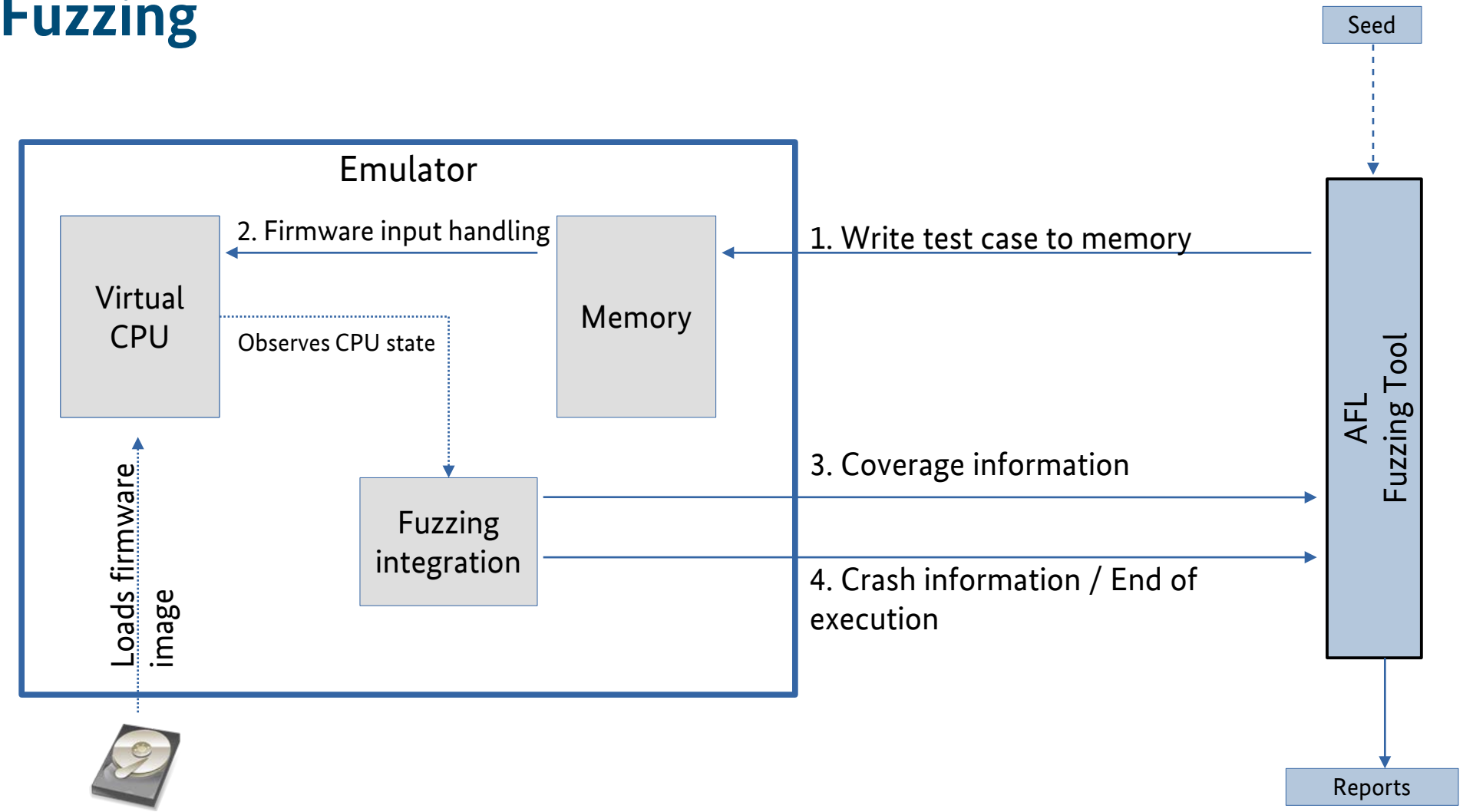


- Sicherheitsanalyse der OPS-SAT Firmware
- Werkzeug: Fuzzing

Firmware Emulation



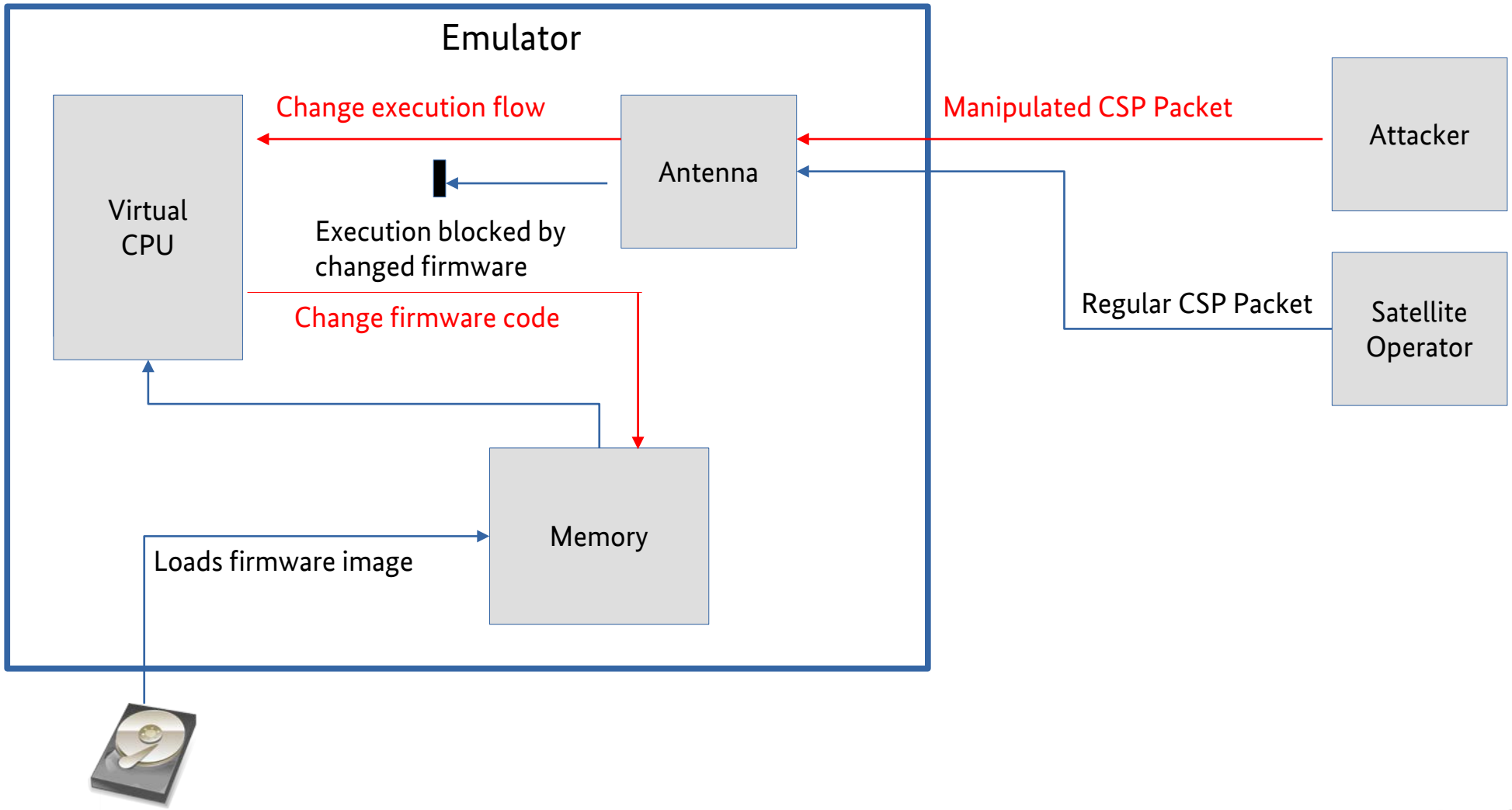
Fuzzing


Seed
Emulator
Virtual CPU
2. Firmware input handling
Memory
1. Write test case to memory
Observes CPU state
AFL Fuzzing Tool
3. Coverage information
Fuzzing integration
4. Crash information / End of execution
Loads firmware image
Reports

Ergebnisse

- Fuzzing kann effektiv auf Sateliten Firmware angewendet werden
- Mindestens 2 Schwachstellen im OPS-SAT
- Mindestens bei einer: Remote Code Execution

Exploit


Emulator
Virtual CPU
Change execution flow
Antenna
Manipulated CSP Packet
Attacker
Execution blocked by changed firmware
Change firmware code
Regular CSP Packet
Satellite Operator
Memory
Loads firmware image

Live-Demo

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

Florian Göhler
Referat SZ13 – BSI-Standards und IT-Grundschutz

florian.goehler@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de