RUHR UNIVERSITÄT BOCHUM RUB

CISPA

Scaling Software Security Analysis to Satellites

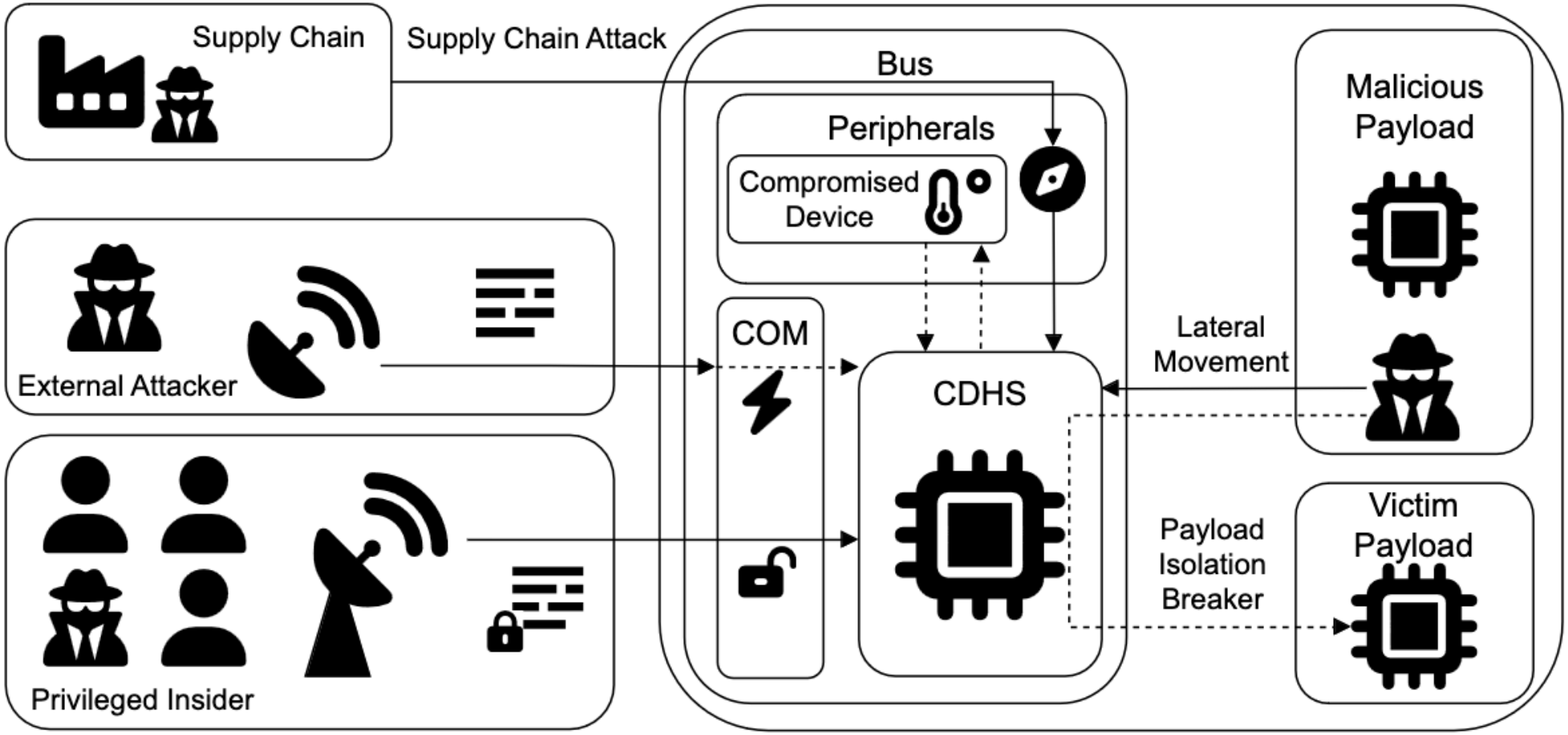
Automated Fuzz Testing and Its Unique Challenges

Johannes Willbold*, Moritz Schloegel^, Florian Göhler*,
Tobias Scharnowski^, Nils Bars^, Simon Wörner^, Nico Schiller^, Thorsten Holz^

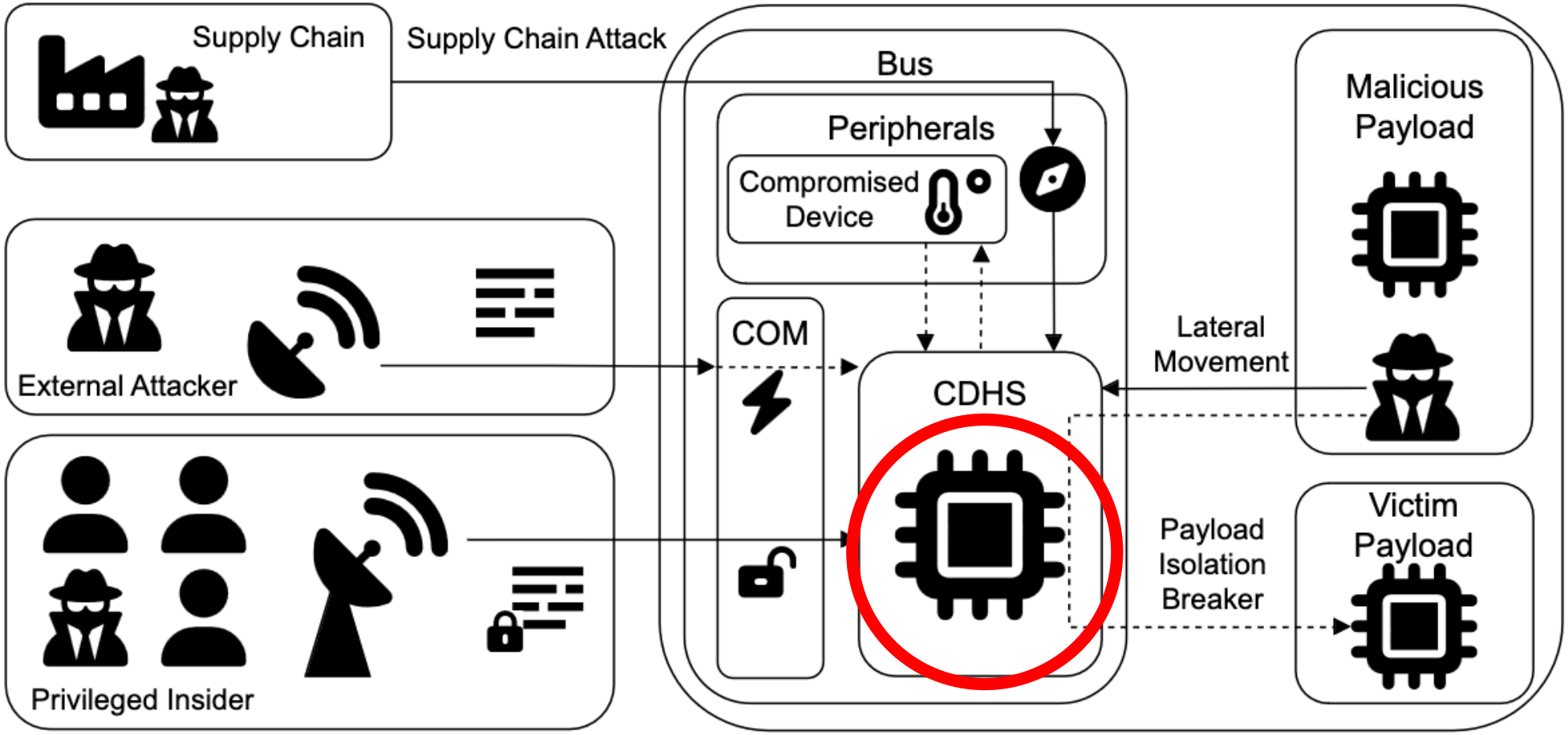
*Ruhr University Bochum, Chair for Systems Security
^CISPA Helmholtz Center for Information Security

v1.0

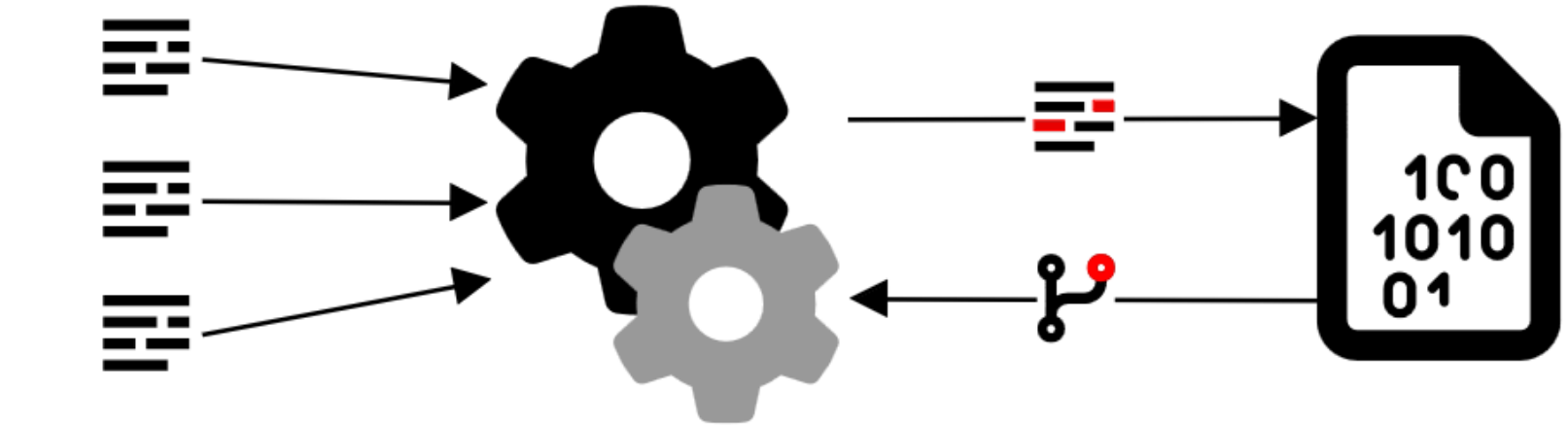
Scenario


Supply Chain
Supply Chain Attack
Bus
Peripherals
Compromised Device
Malicious Payload
External Attacker
COM
Lateral Movement
CDHS
Payload Isolation Breaker
Victim Payload
Privileged Insider

Scenario


Supply Chain
Supply Chain Attack
Bus
Peripherals
Compromised Device
Malicious Payload
External Attacker
COM
Lateral Movement
CDHS
Payload Isolation Breaker
Victim Payload
Privileged Insider

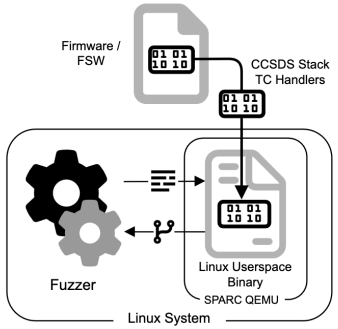
Fuzzing

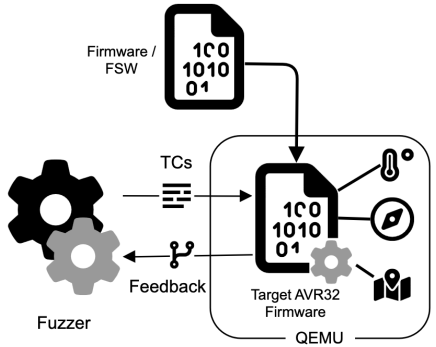


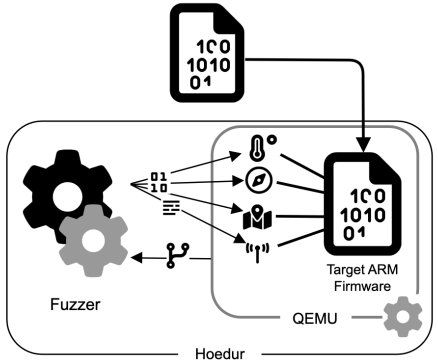
Challenges

1. Complex Satellite Boot Process
2. Only Crashing Inputs
3. Computing Hardware with Limited-Performance
4. Highly Specialized and Individual Setups
5. Performance of Existing Digital Twins

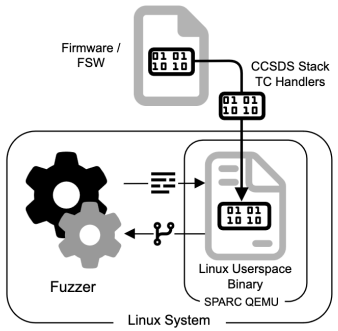
Approaches

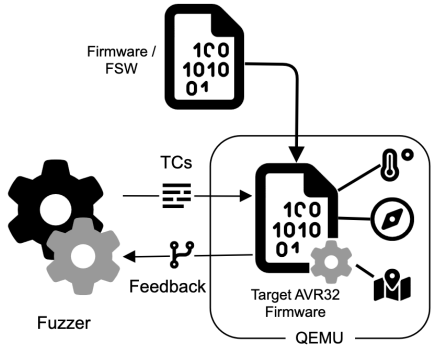

Firmware /
FSW
CCSDS Stack
TC Handlers
Fuzzer
Linux Userspace
Binary
SPARC QEMU
Linux System

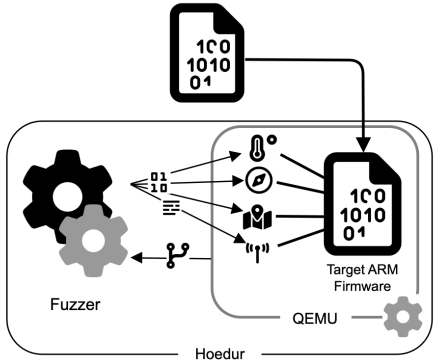

Firmware /
FSW
TCs
Feedback
Fuzzer
Target AVR32
Firmware
QEMU


Fuzzer
Target ARM
Firmware
QEMU
Hoedur

Approaches

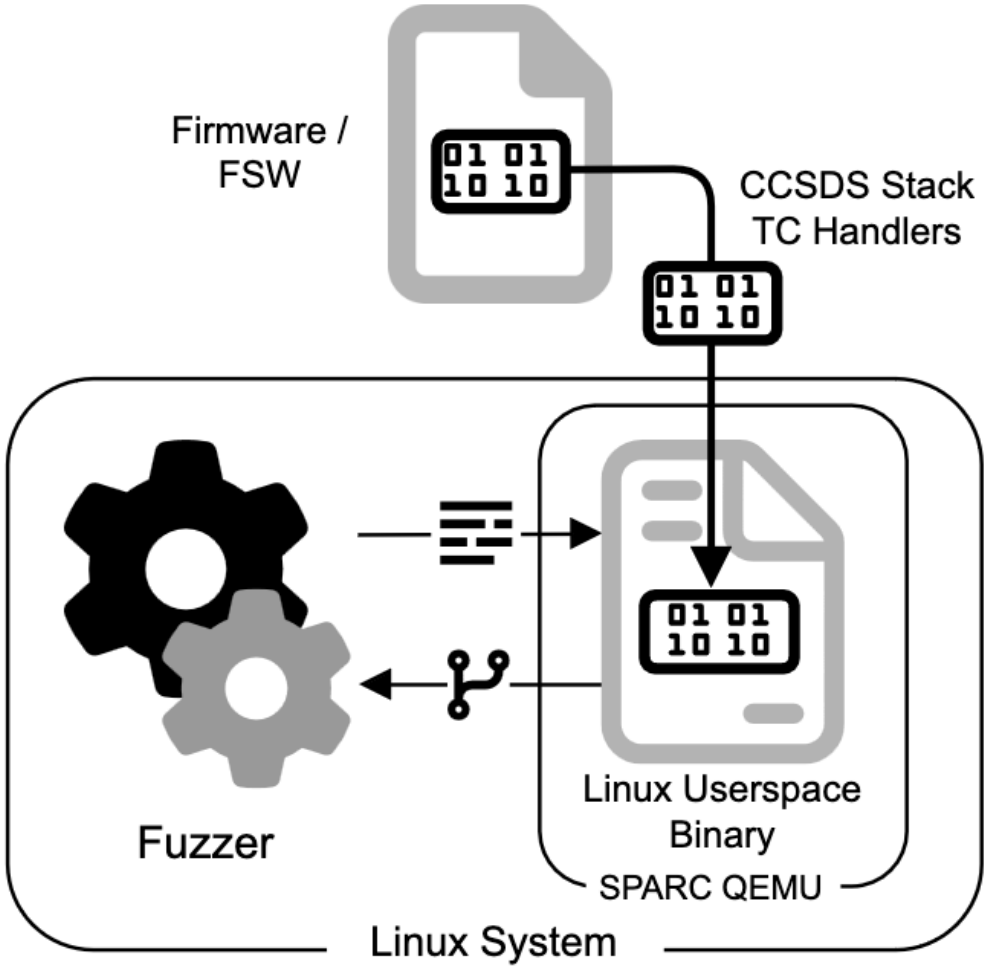






=> No Hardware

Subsystem Extraction

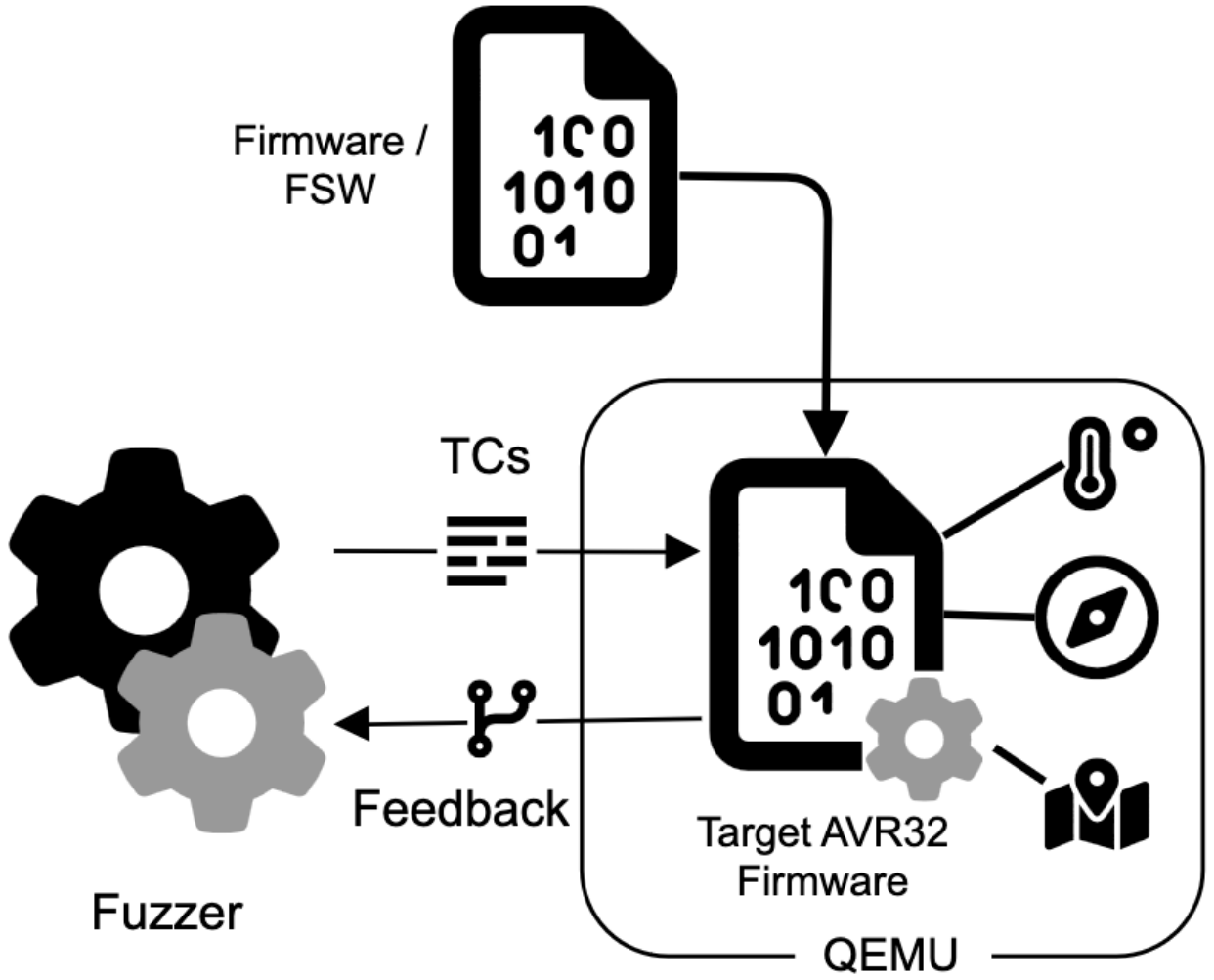


Subsystem Extraction

Issues:

- Many global objects
  - Require manual initialitation and code extraction
- Linux incompatible low-level code
- Extensive manual changes required
- No interactions between components

Persistent Mode Fuzzing

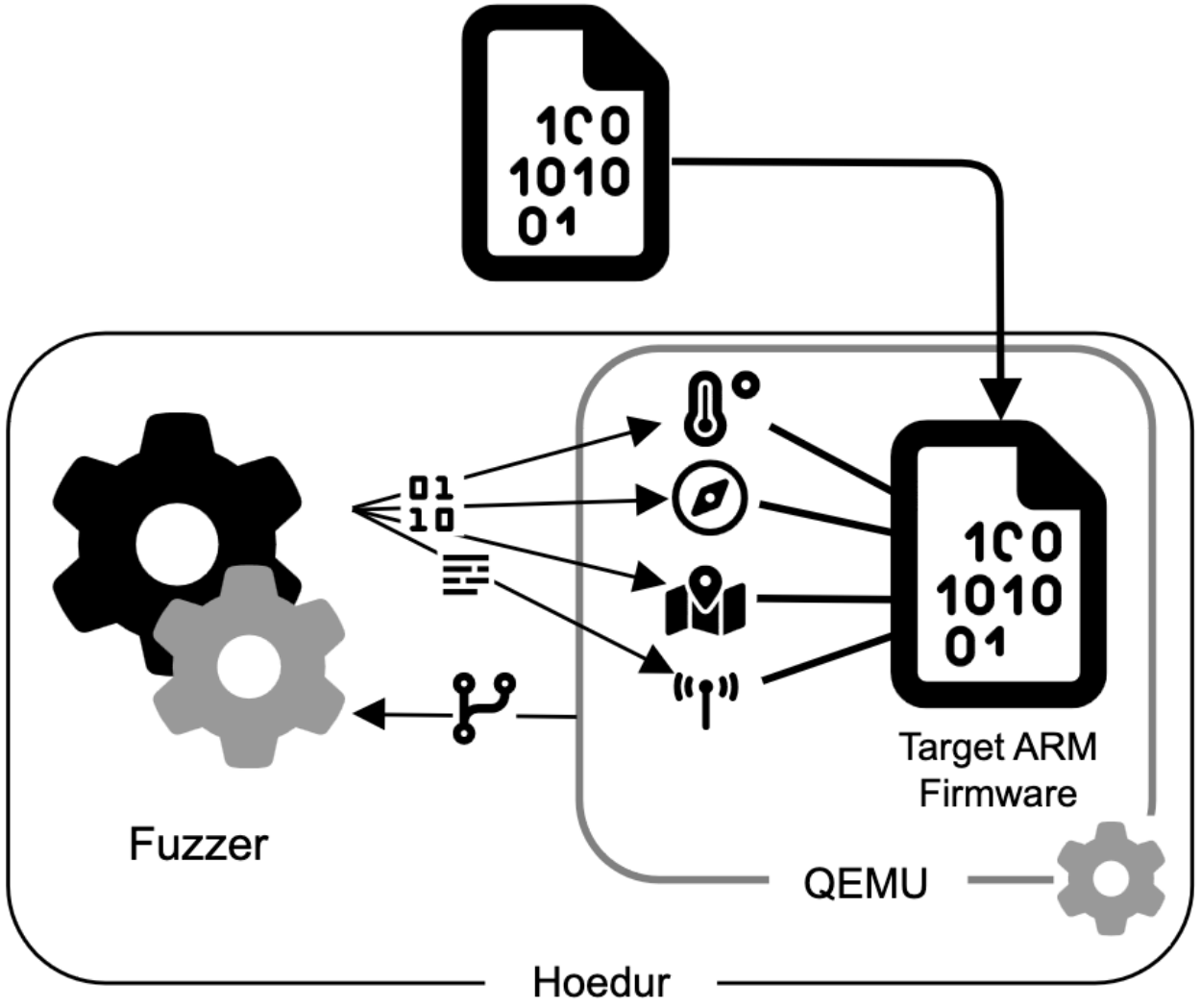


Persistent Mode Fuzzing

Observations

- Skipped bootprocess due to persistent mode
- Potentially non-reproducible bugs due to persistent mode
- Missing peripherals
  - Peripherals with statis responses

Firmware Rehosting



Firmware Rehosting

Observations

- Peripheral modelling replaces specific peripheral simulation
- Snapshoting replaces persistent mode
  - But does not have accumulated state
- Read-only regions allow to detect "Dangerous TCs"

Results

Usual Metric: Code Coverage

Results

~~Usual Metric: Code Coverage~~

Results

~~Usual Metric: Code Coverage~~

Here: TC Coverage

Results

~~Usual Metric: Code Coverage~~

Here: TC Coverage

Metric	Subsys. Extraction	Persistent Mode Fuzzing	Firmware Rehosting
TC Handlers Reached	-	59/59 (100%)	128/128 (100%)
Code Coverage in TC Handlers	-	1300/1704 (76%)	763/981 (78%)

Results

~~Usual Metric: Code Coverage~~

Here: TC Coverage

Metric	Subsys. Extraction	Persistent Mode Fuzzing	Firmware Rehosting
TC Handlers Reached	-	59/59 (100%)	128/128 (100%)
Code Coverage in TC Handlers	-	1300/1704 (76%)	763/981 (78%)

Roadblocks

- Hashes & CRC-Sums
- Large Value Comparisons
- Grammer Formats
- ...

Q&A

- Fuzzing introudction
- Five satellite fuzzing challenges
- Three fuzzing setups with no hardware
- Evaluation

/jwillbold

Johannes Willbold - johannes.willbold@rub.de