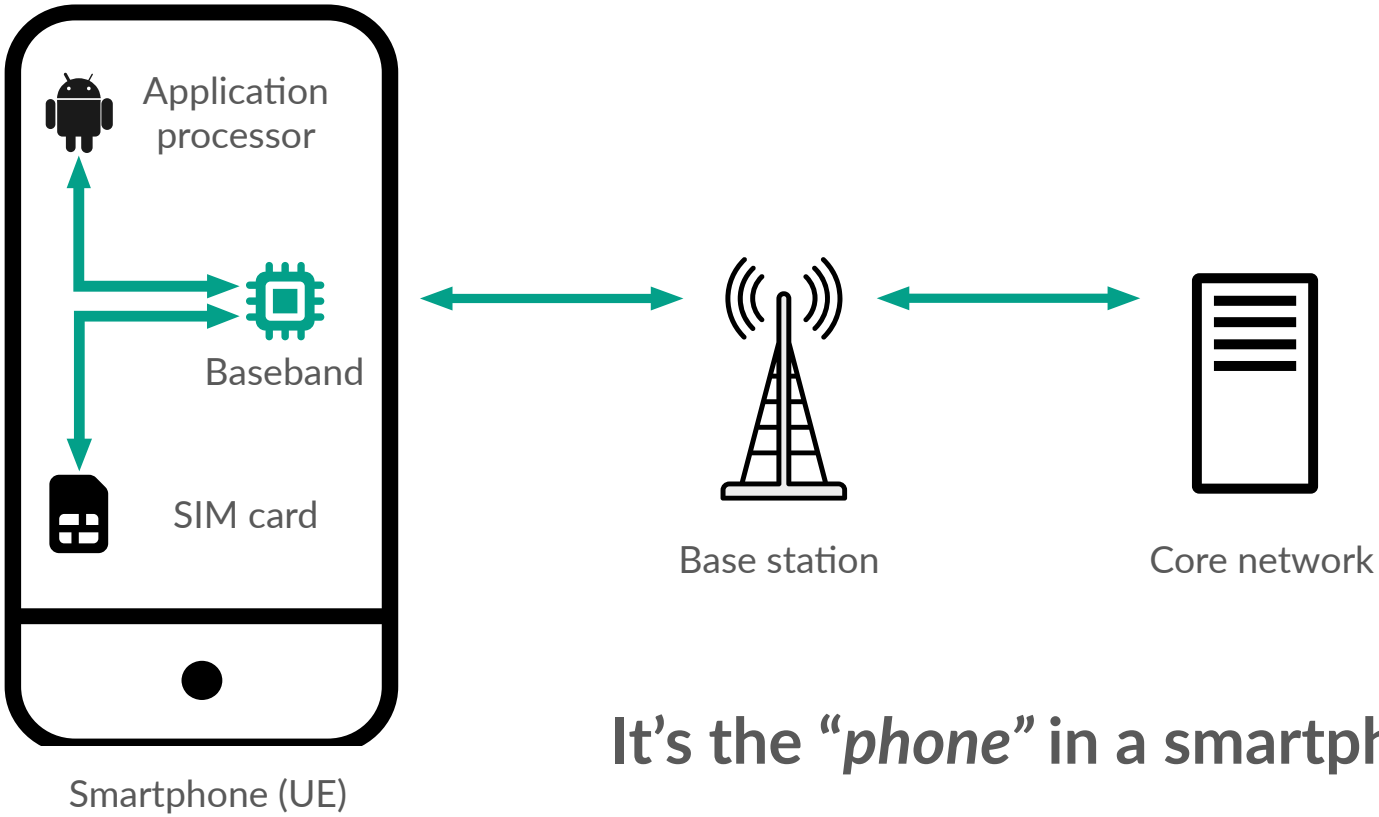
SoK: Insecurity of Cellular Basebands

Henri CARNOT (Avantix / EURECOM)
Aurélien FRANCILLON (EURECOM)

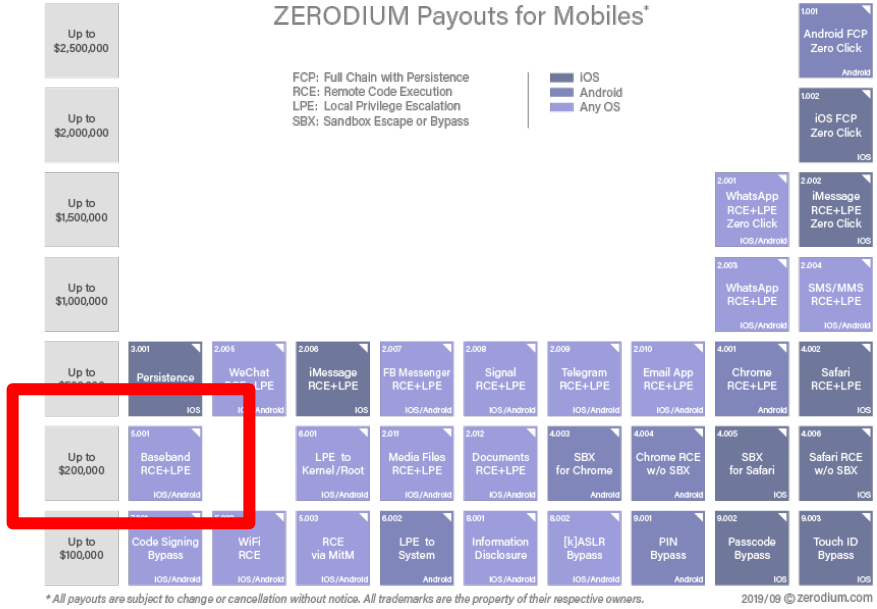
Tuesday, August 11, 2026

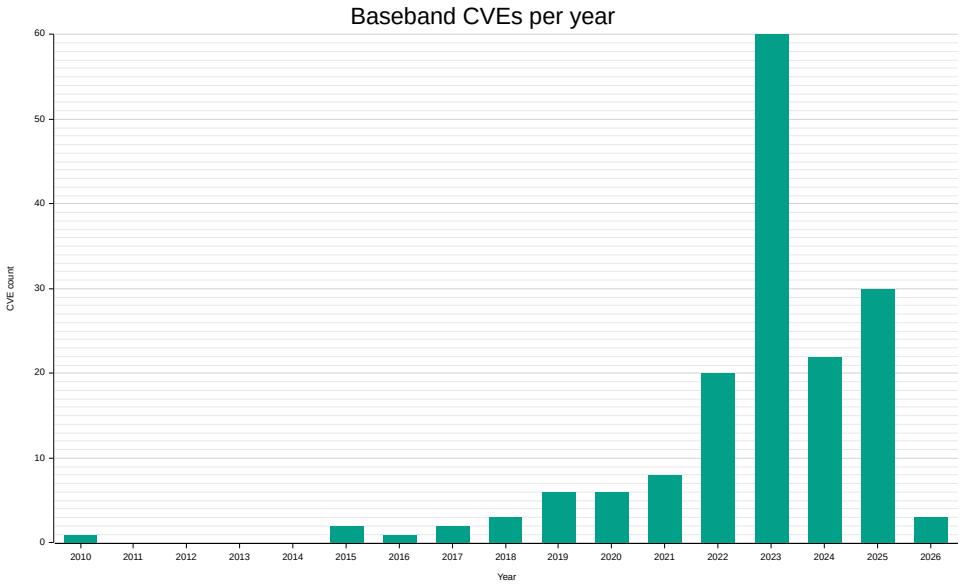
What is a baseband?



It's the "*phone*" in a smartphone.

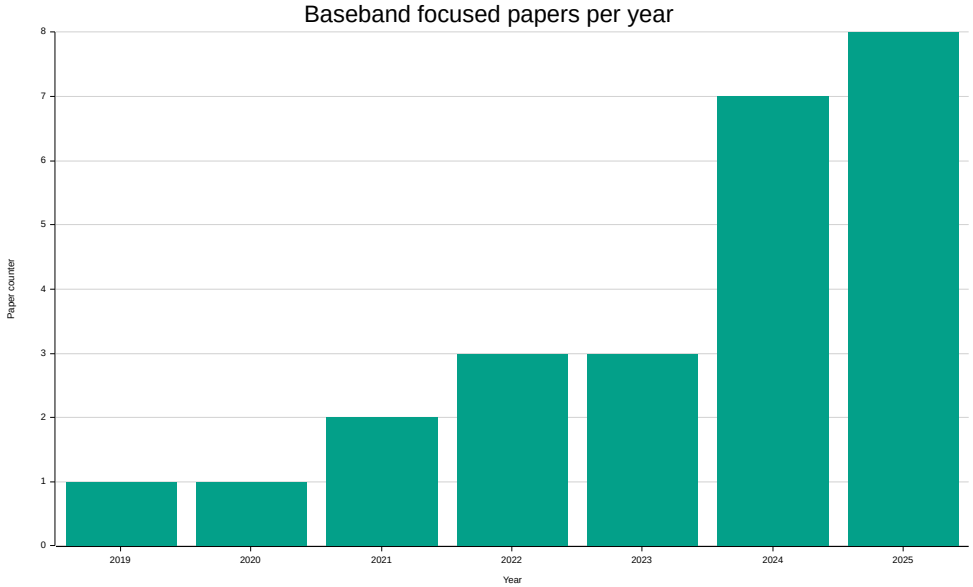
Increasing security research





State of the art review

- 26 papers from 2019 to 2025
- Targeted on baseband's firmware security analysis
- Academic and non-academic work



5GHOUL: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing

Matheus E. Garbelini, Zewen Shang, Shijie Luo, Sudipta Chattopadhyay, Sumei Sun, Ernest Kurniawan

FIRMWIRE: Transparent Dynamic Analysis for Cellular Baseband Firmware

Grant Hernandez*¶, Marius Muench†¶, Dominik Maier‡, Alyssa Milburn†,
Shinjo Park‡, Tobias Scharnowski§, Tyler Tucker*, Patrick Traynor*, Kevin R. B. Butler*
*University of Florida, {grant.hernandez, tylertucker1, traynor, butler}@ufl.edu
†Vrije Universiteit Amsterdam, {m.muench, a.a.milburn}@vu.nl
‡TU Berlin, {dmaier, pshinjo}@sect.tu-berlin.de
§Ruhr-Universität Bochum, tobias.scharnowski@rub.de

DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices

CheolJun Park*, Sangwook Bae*, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim
Korea Advanced Institute of Science and Technology (KAIST)
{fermioncj, hoops, beomseoko, jiholee, ekleez, insuyun, yongdaek}@kaist.ac.kr

Difficult to analyze



Large binaries



No symbols



Undocumented firmware



Use of custom architectures and/or ISAs



Interfacing with the baseband requires special permissions



Debug interface disabled

Interesting to analyze

CVE-2026-23792

Incorrect handling of unauthenticated downlink RRC Setup messages can cause the baseband to crash

Jul 05, 2026

CVE ID	CVE-2026-23792
Description	Incorrect handling of unauthenticated downlink RRC Setup messages can cause the baseband to crash
Affected Product	Exynos 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 2500, W1000, Modem 5300, Modem 5400, Modem 5410
Affected Component	NR RRC
Severity	Medium
Reported Date	2025-10-22
Acknowledgment	Denis Kraemer, University of Applied Sciences Upper Austria, Campus Hagenberg

One vulnerability…

…many basebands

A device at risk



Written in memory unsafe languages (C/C++)



Independent form the application processor

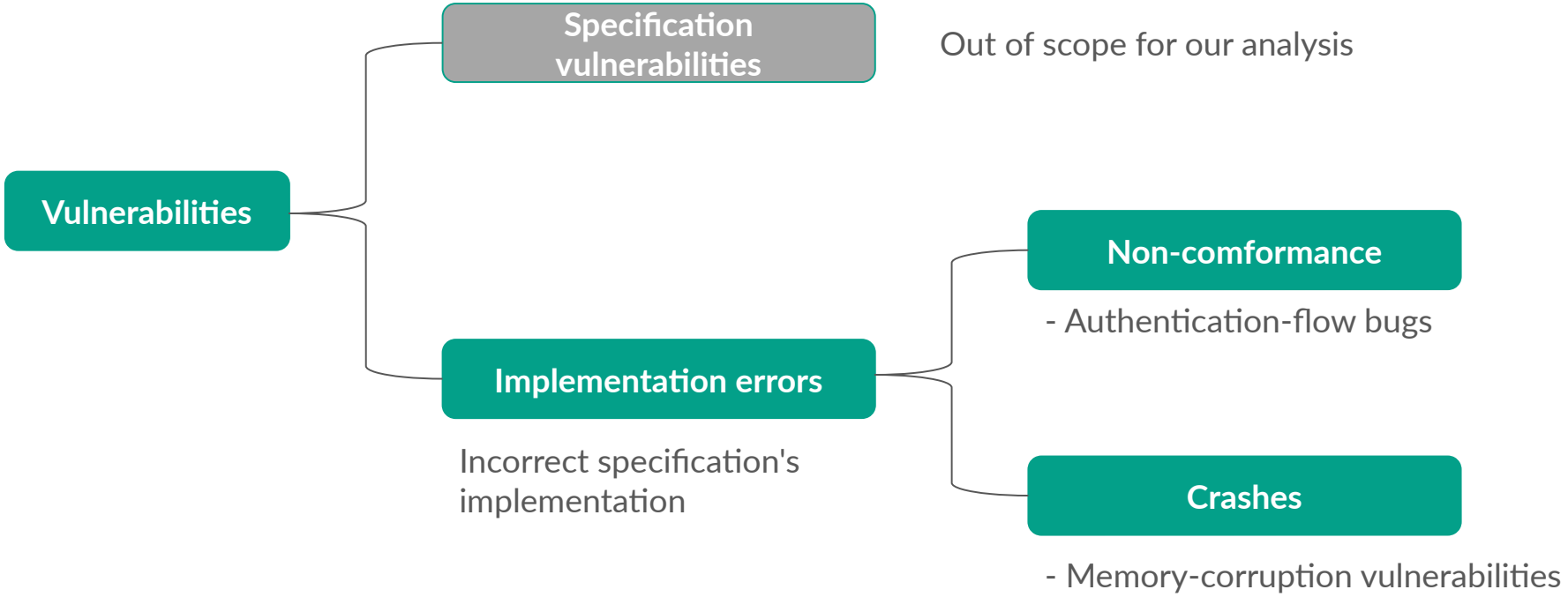


Accessible remotely



Limited hardening (ASLR…)

Context of the analysis



Cellular standards

2G 1991	**GSM**	No mutual authentication. Slowly phased out
3G 2001	**UMTS**	Add mutual authentication between the User Equipment (UE) and the core network
4G 2008	**LTE**	All IP architecture
5G 2019	**NR**	Add anti rollback protection. Device identity protection



Multiple generation of cellular protocols needs to be supported by the baseband

Research questions

RQ1 What is the baseband attack surface?

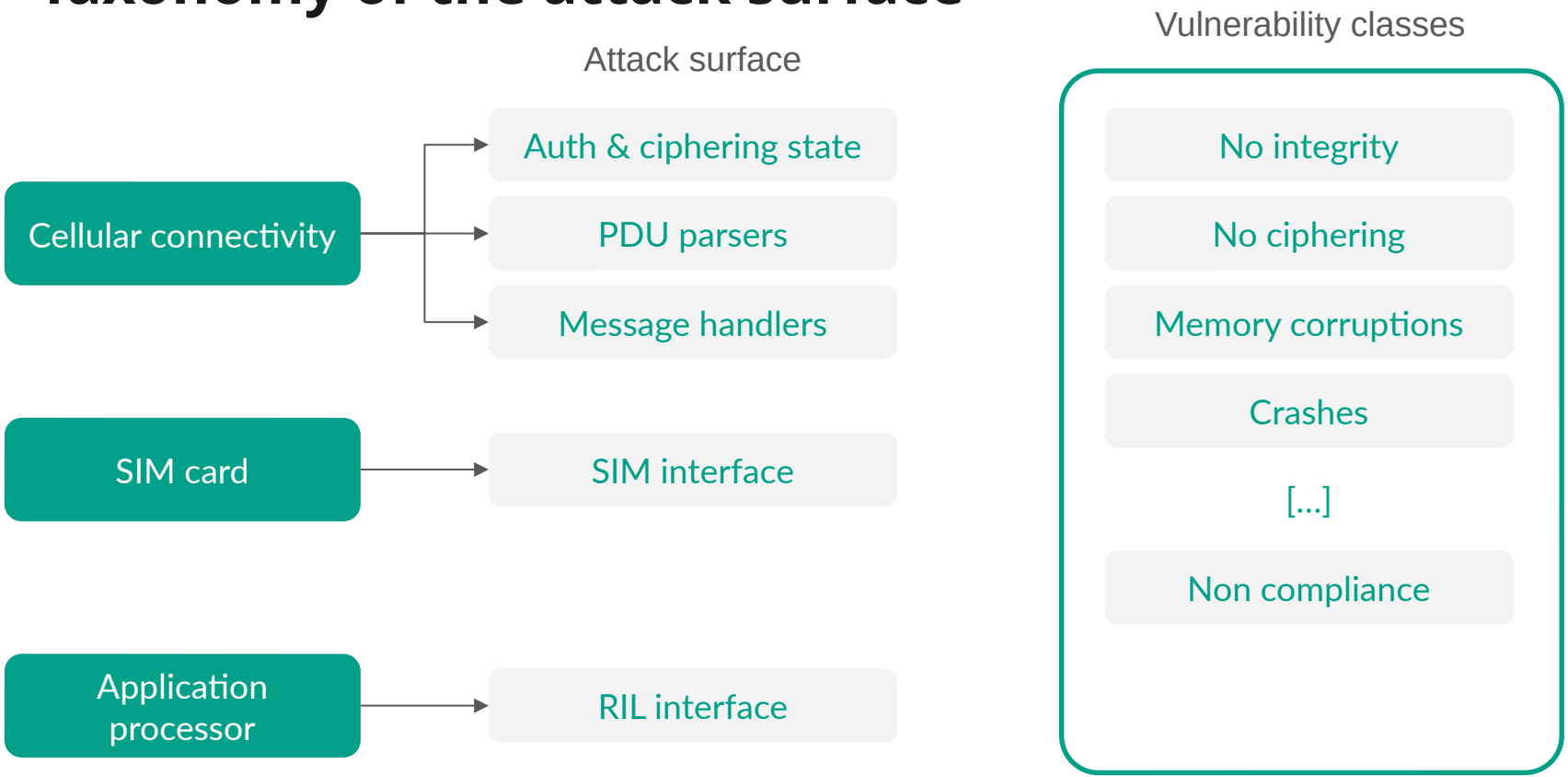
RQ2 What threat model and vulnerabilities classes are known?

RQ3 How can security-relevant test cases be systematically generated?

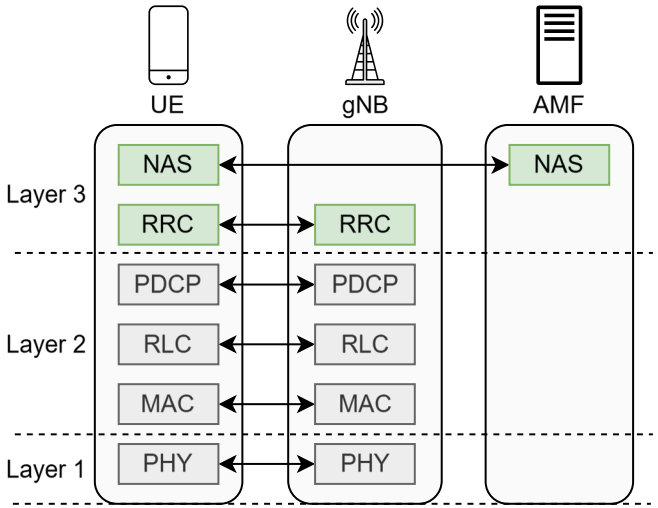
RQ4 How can stateful protocol testing be handled?

RQ5 How can crashes or anomalous behavior be detected on a black-box device?

Taxonomy of the attack surface



Cellular protocol layers



Layer 3

Handle control plane information

- Identity & security context management

Focus of most works

Layer 2

Vast pre-authentication attack surface

Explored in recent works **[LLFuzz, 5Ghoul]**

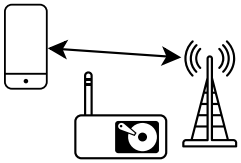
[LLFuzz] Luo et al., "*Sni5gect: A practical approach to inject aNRchy into 5g NR*", USENIX Security 2025.

[5ghoul] E. Garbelini et al., "5ghoul: Unleashing chaos on 5g edge devices via stateful multi-layer fuzzing", IEEE Transactions on Dependable and Secure Computing, June 2025.

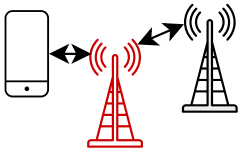


Attacker capabilities

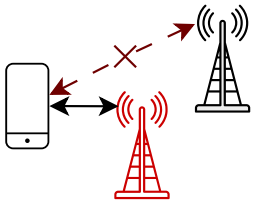
Attacker capabilities



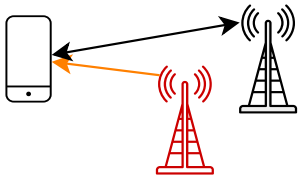
Sniffing



Man-in-the-middle



Fake base station



Signal injection **[SNI5GECT]**

Attacker information



No information

Access to the network keys



Pre-authentication attack surface

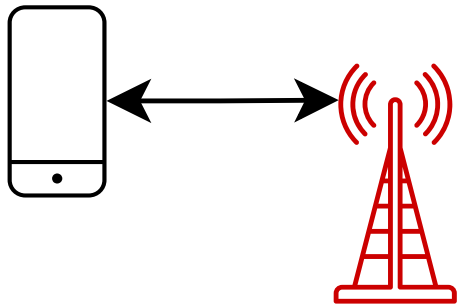


Post-authentication attack surface

[SNI5GECT] Luo et al., "*Sni5gect: A practical approach to inject aNRchy into 5g NR*", USENIX Security 2025.

Attacker capabilities

Rogue base station [OTABase]



Attacker information

- ✗ No information
- 🔑 Access to the network keys

- ✓ Pre-authentication attack surface
- ✓ Post-authentication attack surface

[OTABase] Park et al., "*OTABase: Enhancing Over-the-Air Testing to Detect Memory Crashes in Cellular Basebands*", IEEE ACSAC 2025.



Taxonomy of the analysis techniques

Taxonomy of analysis techniques

Axis 1
Test Case Generation

Axis 2
Test Case Evaluation

Axis 3
Test Oracles

Axis 4
Reaching deep states

Axis 1: Test Case Generation

From the specification

Specification provides compliance testing

Negative testing **[DoLTEst]**

State machine inference

Divergence between multiple devices?

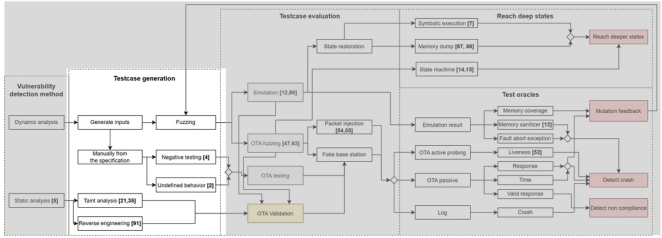
Fuzzing

Challenge: guiding the fuzzing

Static analysis

Reverse engineering
Taint analysis

Challenge:
- requires long reverse engineering
- Complex to generalize to different vendors



[DoLTEst] Park et al., "*DoLTEst: In-depth downlink negative testing framework for LTE devices.*", USENIX Security 2022.

Axis 2: Test Case Evaluation

Over-the-Air (OTA)

Ground-truth: real hardware response, no emulation gap

Slow: each test takes time.

Limitation: resetting the device state is difficult

Physical constraints:
- lower-layer have strict time constrains
- Requires being capable to emits the wireless signal (e.g. fake base station)

Emulation

Partial | Full-system

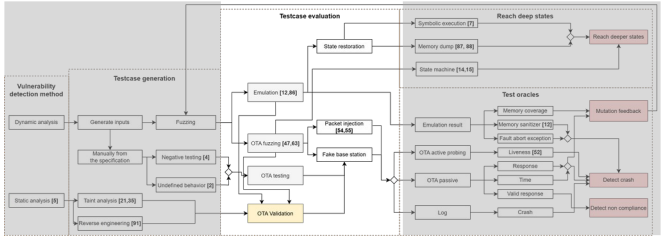
Low fidelity: low level peripheral interaction difficult to emulate

Fast: can be parallelized, snapshot possible

Stable: the testing can be made deterministic

Limitation: Full-system emulation requires to be able to emulate devices' peripherals

OTA validation required for emulation and static analysis to confirm the bug on ground truth



Axis 3: Test Oracles

[OTA] Passive probing

Wireless: wait for response to test input (e.g. ACK)

Serial: monitor ADB logcat for magic keywords

[OTA] Active probing

Send probe message after a few test cases to monitor device's health **[OTABase]**

Emulation

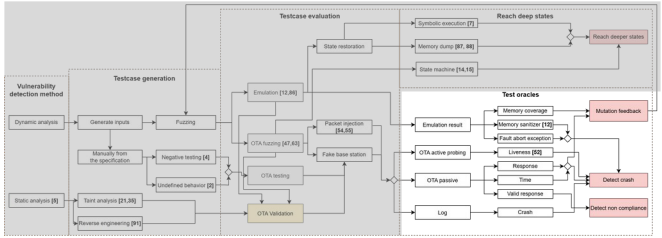
Memory sanitizer **[BaseSafe]**

Hooks in the interrupt table

Hooks in the baseband's error handler

Limitation: some vulnerabilities are silent

No standard crash-reporting interfaces exist: requires per-vendor heuristics such as ADB's logcat magic words filtering



Axis 4: Reaching deep states

[OTA, Emulation] Fuzzing

Time feedback: measure input's response time.

Coverage feedback: requires emulation

[Emulation] State restoration / modelling

Via a crash dump **[FirmState, BaseBridge]**

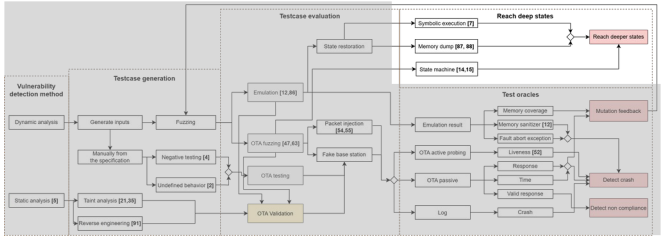
Via symbolic analysis **[Loris]**

[OTA] Avoid early rejection

Fuzzing trade-off: generation invalid messages may lead to discover bugs but increases the chance for the message to be early rejected

[**FirmState**] Jeong et al., "*FirmState: Bringing cellular protocol states to shannon baseband emulation*", ACM 2025.

[**BaseBridge**] Klischies et al., "*Bridging the gap between over-the air and emulation testing for cellular baseband firmware*", IEEE 2025.



Unsupported messages in open-source base station may expose rarely tested code paths and trigger vulnerabilities

[**Loris**] Ranjbar et al., "*Stateful analysis and fuzzing of commercial baseband firmware*", IEEE 2025.

Conclusion

- Basebands are critical devices and difficult to analyze
- Over-the-Air analysis is accurate but slow
- Emulation allows higher fuzzing speed and better instrumentation but requires heavy reverse engineering efforts

Future challenges

- Analysis of understudied architectures
  - Huawei, Unisoc
  - Apple: new baseband
  - Qualcomm: early non academic work shows that it‘s possible

- Some vendors are now encrypting their firmware

Thanks!

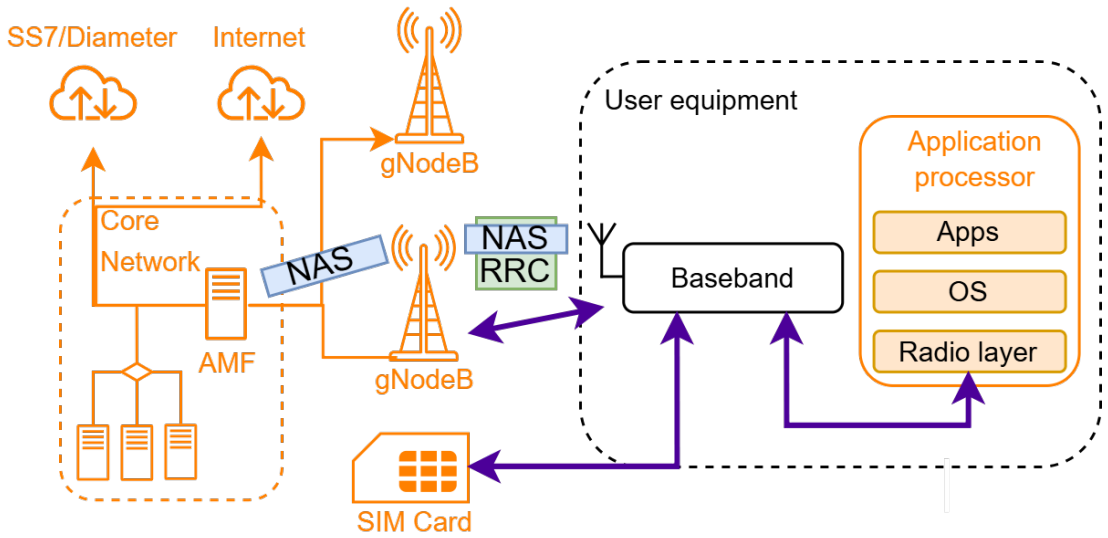
EURECOM
Sophia Antipolis

AVANTIX

Contact

henri.carnot@eurecom.fr

@henri2h.bsky.social



Paper

Henri Carnot, Aurélien Francillon
SoK: Insecurity of Cellular Basebands