29. VDE/ITG Fachtagung Mobilkommunikation, May 2025

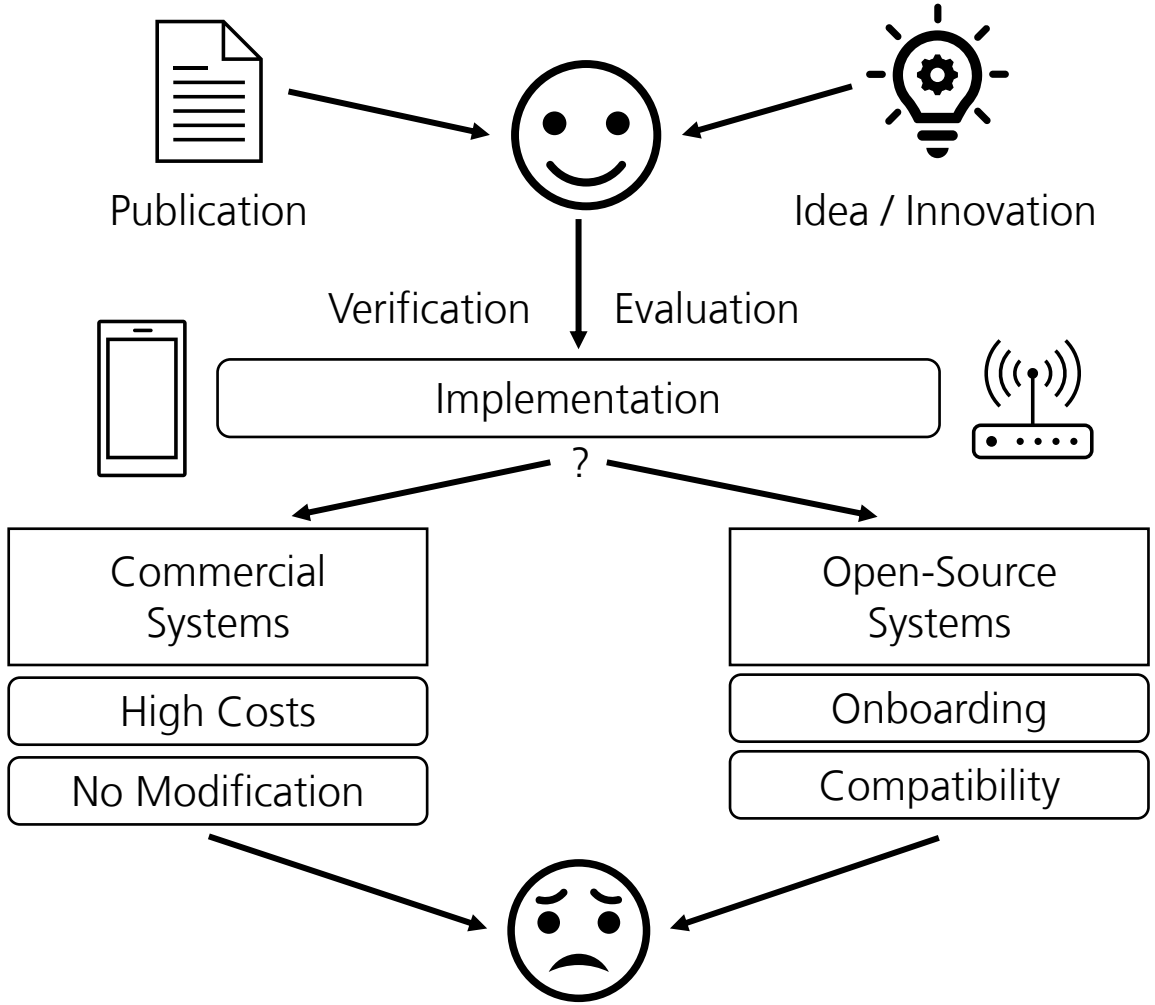
Thorsten Horstmann

open5Gcube: A Modular and Usable Framework for Mobile Network Laboratories

Motivation

The dilemma of (security) researchers in the field of mobile networks

- Research requires **interaction** with real devices / implementations
- **Demonstrability** / verifiability of own research activities
- Commercial solutions (closed source) often do not offer the required interfaces / options for **modifications**
- Open source solutions fragmented and may hard to deploy consistently
  - **Compatibility** with COTS UEs is difficult



open5Gcube
Basic concept

Hardware
- Powerful x86 server
- Software Defined Radio (USRP)
- Optional: External GPSDO for clock synchronization

Containerisation
- All components run in Docker containers
  - Ensures good reproducibility and traceability
- Simple deployment

Networking
- Also controlled via Docker

Management
- Scripts for starting/stopping the containers
- Centralised configuration of the most important parameters
- Distribution of the containers to the hosts?

Idea

Integration of COTS hardware and open-source software for modular, reproducible and unified mobile network testbeds, as well as developments based on it

Simple container orchestration for experimental mobile networks

An unpopular approach?

Kubernetes

+ De-facto **standard** for container orchestration
  - 5G core designed to be cloud-native in the specs
  - **In use** at MNOs
+ Extremely **powerful**

– Steep **learning curve**, many concepts
– Large **overhead**, most of which would not be utilised
– (In our opinion) Completely oversized for lab setups

Docker-Swarm

+ Docker's own container orchestration
+ Very **simple** integration into Docker Compose

– No static IP addresses for the containers
  - Limits reproducibility
  - Some projects need IP addresses in their configuration

Simple container orchestration for experimental mobile networks

An unpopular approach?

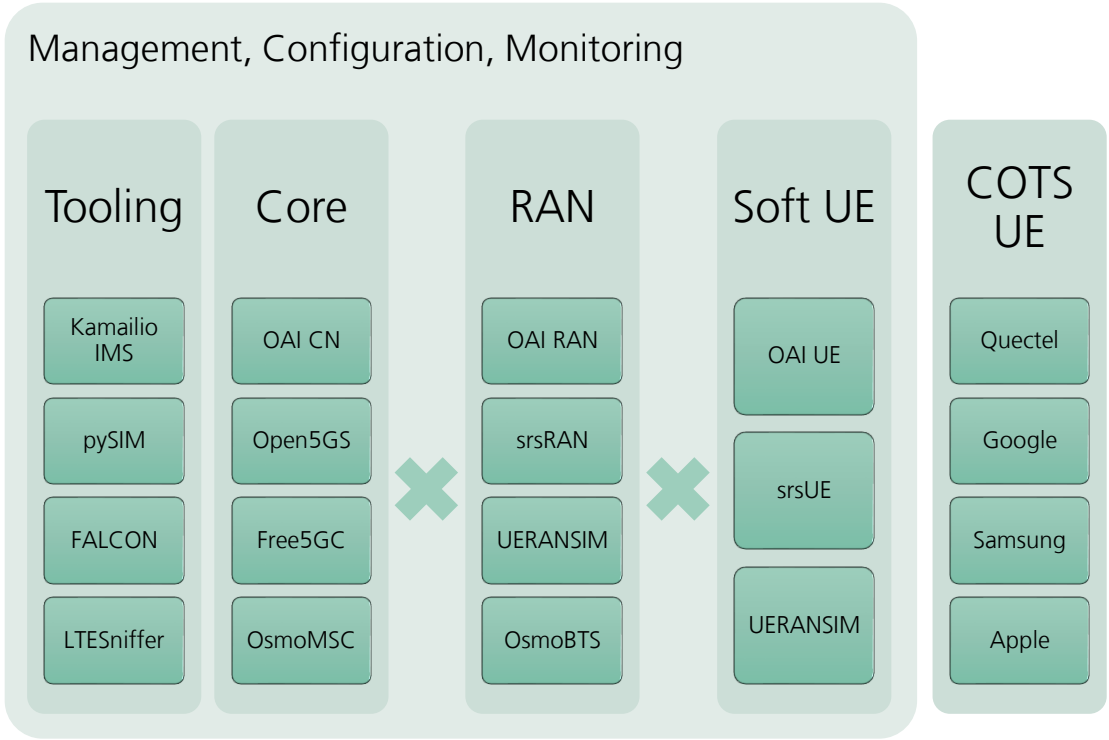
Own orchestration *lite*

- "Controller host" starts all containers
- RAN entrypoint determines that it should be executed on another host
  - Docker-outside-of-Docker (DooD)
  - Use of standard Docker-Compose features
- Magic is limited to a few lines of shell script
- Effective „DIY-solution"

open5Gcube
Implementation

Framework for the flexible combination of different open-source core network, RAN and UE implementations for the realisation of mobile network testbed environments.

- Repository for the most common projects
  - **Tested** versions and configurations
- Containerised for easy installation and good **reproducibility**
- Combination of different services form a **Stack**
  - Docker-Compose
- Each run starts with a **clean state**
  - Databases are populated at Stack startup
- Network segmentation managed via Docker MacVLAN
  - Flexible distribution of containers across multiple servers
  - `rfnet`: RAN to USRP / emulated UE
  - `corenet`: core network services
  - `extnet`: external services and bridge to the outside world



open5Gcube

Usage

WebUI

- *One-click* start/stop of the Stacks
  - Easy configuration of common parameters
- Overview of all running services
- Links to web services of the Stacks
- SIM card reader/writer helpers

Console

- Build of Docker Images

```
$ make docker-build-oai-ran
$ make docker-build-open5gs
```

- Start / Stop of Stacks

```
$ make run-oairan-open5gs-5g
$ make stop-oairan-open5gs-5g
```

Configuration

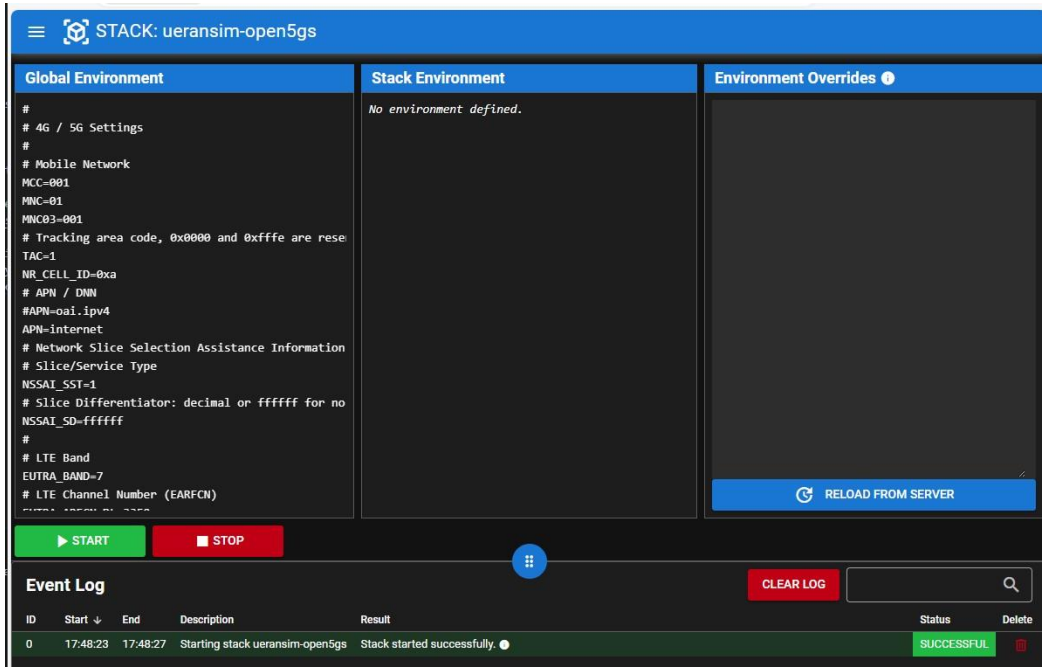
- Simple environment files
- Global < Stack specific < Run

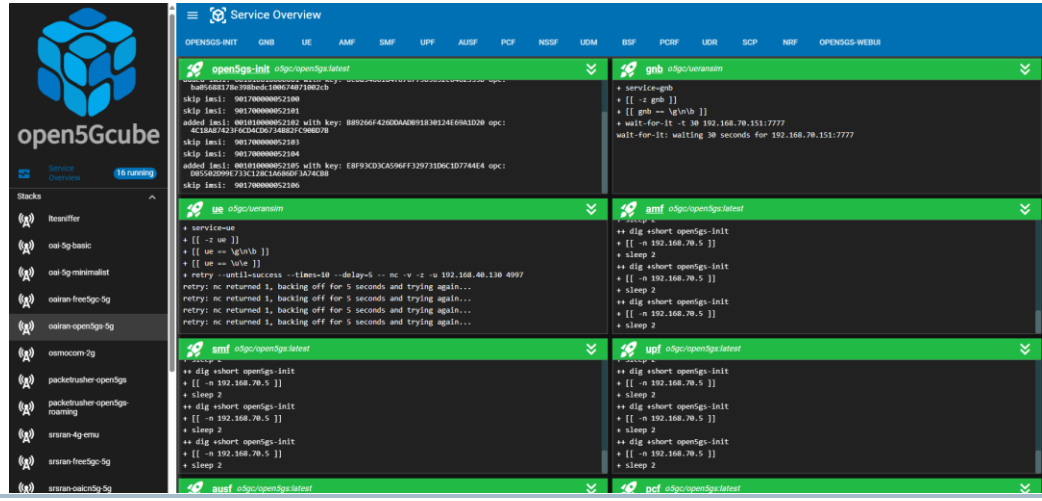
etc/settings.env

```
MCC=001
MNC=01
TAC=1
NR_CELL_ID=0xa
…
```

etc/uedb.env

```
#      IMSI      Key     OPc
UE_1="901700…  F18E…  E83C…"
UE_2="262991…  85DA…  A7EA…"
…
```



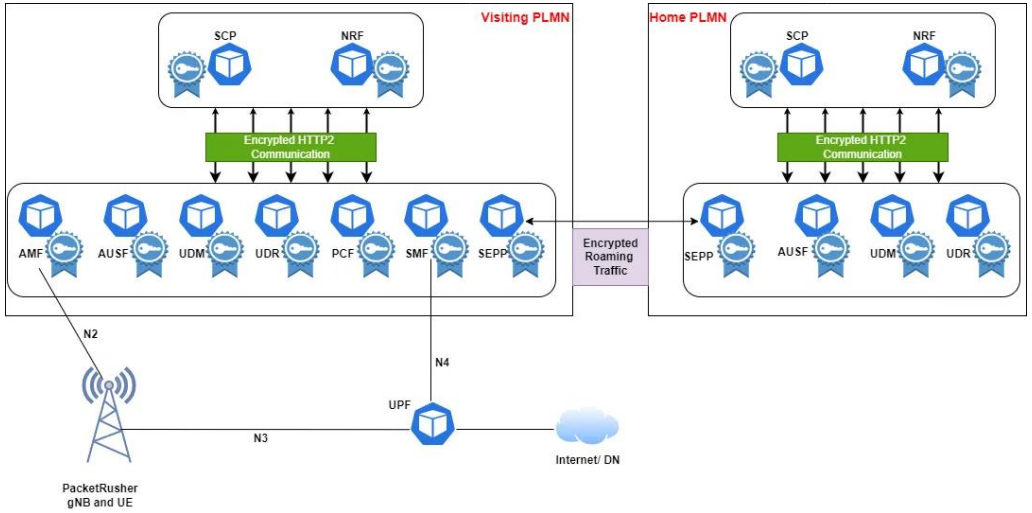


open5Gcube

Selection of some Stacks

(Local Break Out) Roaming with Open5GS

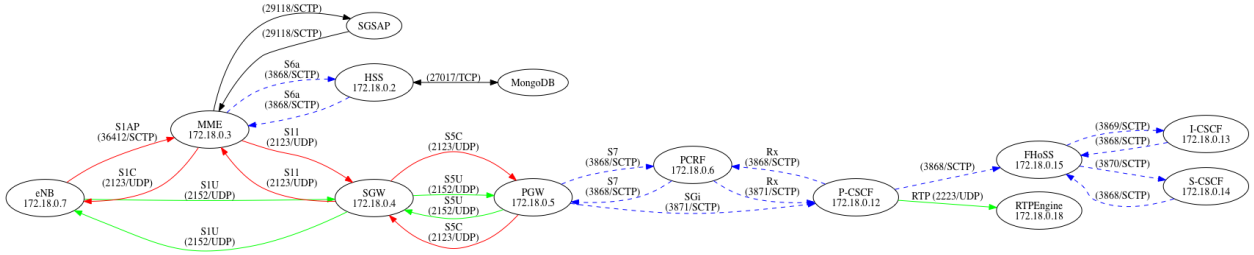
- Complex setup with two core networks
  - Tutorial uses 3 VMs [1]
- PacketRusher as simulated gNB / UE
- Advantage of simple **network segmentation**



futuredon.medium.com/5g-roaming-with-mutual-tls-1468d109129c

VoLTE with Open5GS + Kamailio

- Advantage of high **reproducibility**



open5gs.org/open5gs/docs/tutorial/03-VoLTE-dockerized/

5G SA

- Combination of all common open-source RAN and core network implementations
- SDR with real UEs, Soft-UEs, emulated with UERANSIM
- Advantage of **encapsulating** the configurations in stacks

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

Key Findings

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

Key Findings

- Some UEs work perfectly

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

Key Findings

- Some UEs work perfectly
- Some phones expect an IMS (Voice Service) for 5G SA
  - OpenMobileNetworkToolkit [1] may help

[1] https://github.com/omnt/OpenMobileNetworkToolkit

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

Key Findings

- Some UEs work perfectly
- Some phones expect an IMS (Voice Service) for 5G SA
  - OpenMobileNetworkToolkit [1] may help
- iPhone works with special settings
  - PLMN 999-XX
  - SUCI enabled and configured
  - NAS encryption

[1] https://github.com/omnt/OpenMobileNetworkToolkit

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

Key Findings

- Some UEs work perfectly
- Some phones expect an IMS (Voice Service) for 5G SA
  - OpenMobileNetworkToolkit [1] may help
- iPhone works with special settings
  - PLMN 999-XX
  - SUCI enabled and configured
  - NAS encryption
- VoLTE is complicated
  - OMNT can help here as well

[1] https://github.com/omnt/OpenMobileNetworkToolkit

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

Key Findings

- Some UEs work perfectly
- Some phones expect an IMS (Voice Service) for 5G SA
  - OpenMobileNetworkToolkit [1] may help
- iPhone works with special settings
  - PLMN 999-XX
  - SUCI enabled and configured
  - NAS encryption
- VoLTE is complicated
  - OMNT can help here as well
- 4G Data only and 2G works fine

[1] https://github.com/omnt/OpenMobileNetworkToolkit

open5Gcube

Evaluation with COTS UEs

Stack			S25	One Plus 13	Edge 50P	Rog Phone6	Pixel 9	iPhone 13	Quectel RM500Q
5G	srsRAN	Open5GS	●	●	◗	●	○	●	●
		OAI-Core	●	●	◗	●	○	○	●
		Free5GC	●	●	◗	●	○	●	●
	OAI-RAN	Open5GS	●	●	◗	●	●	●	●
		OAI-Core	●	●	◗	●	●	○	●
		Free5GC	●	●	◗	●	◗	●	●
4G	srsRAN	Open5GS	●	●	●	●	●	●	●
		+ Kamailio	○	●	○	●	○	●	-
2G	Osmocom		●	●	●	●	●	●	●

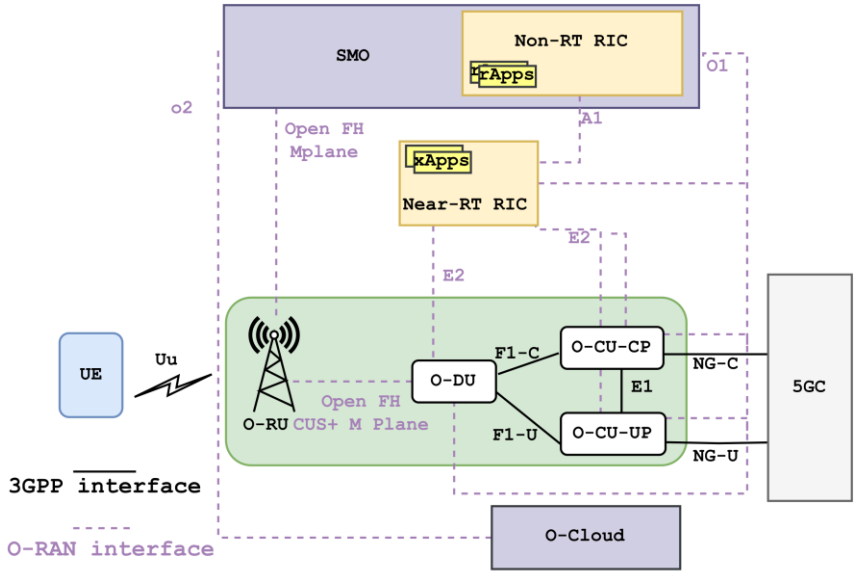
Key Findings

- Some UEs work perfectly
- Some phones expect an IMS (Voice Service) for 5G SA
  - OpenMobileNetworkToolkit [1] may help
- iPhone works with special settings
  - PLMN 999-XX
  - SUCI enabled and configured
  - NAS encryption
- VoLTE is complicated
  - OMNT can help here as well
- 4G Data only and 2G works fine
- Switching between Stacks is easy
  - < 1 Minute to test a new configuration

[1] https://github.com/omnt/OpenMobileNetworkToolkit

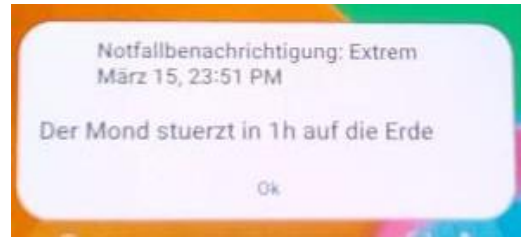
open5Gcube
Outlook

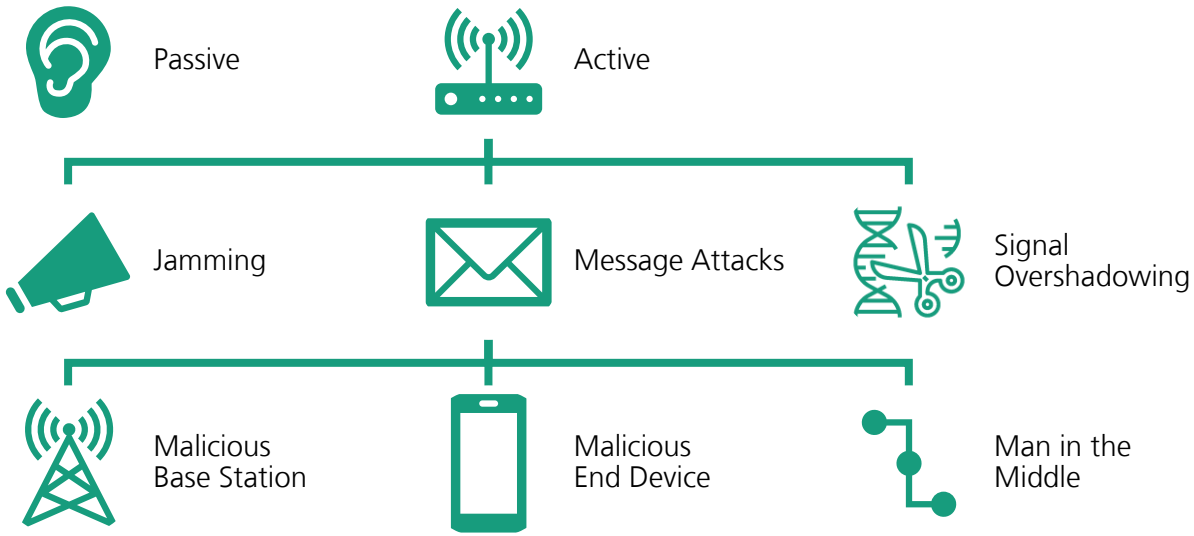
Concept / Architecture
- Continuous integration of current developments (6G)
- OpenRAN fits ‘seamlessly’ into the architecture



Wani, Mohamad Saalim, Mathias Kretschmer, Bernd Schröder, Andreas Grebe, and Michael Rademacher. "**Open RAN: A concise overview**." IEEE Open Journal of the Communications Society (2024).

Security Research
- PoC implementations
- High reusability of code



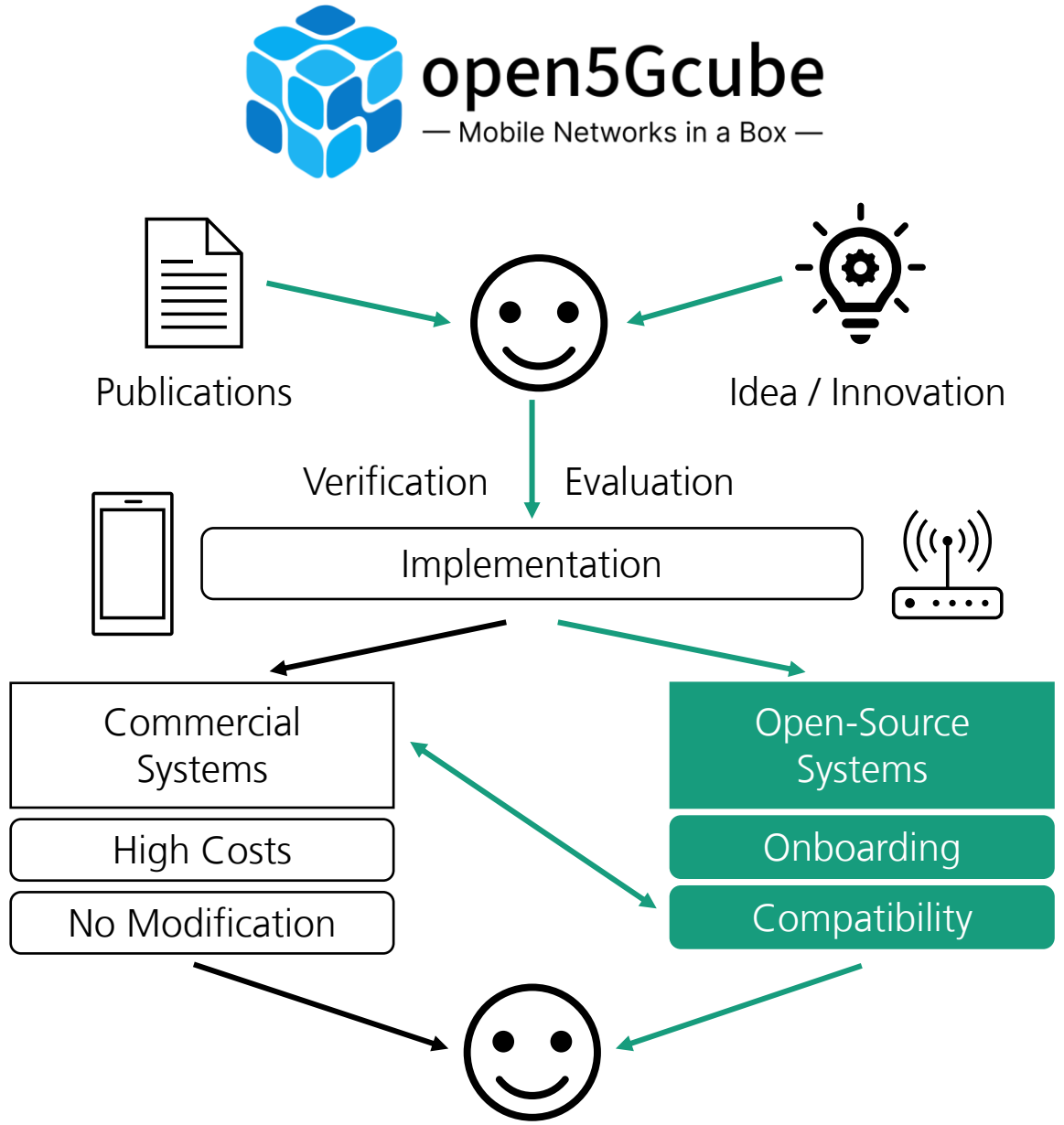


Wani, Mohamad Saalim, Michael Rademacher, Thorsten Horstmann, and Mathias Kretschmer. "**Security vulnerabilities in 5G non-stand-alone networks: A systematic analysis and attack taxonomy**." Journal of Cybersecurity and Privacy 4, no. 1 (2024): 23-40.

open5Gcube
Summary

Modular framework for verification and evaluation of research in the field of mobile communications

- **Integration of various open-source projects**
  - OpenAirInterface, srsRAN
  - Open5GS, free5GC, UERANSIM, PacketRusher, osmocom
  - Kamailio & rtpengine for VoLTE
  - pySIM, LTESniffer, …
- Tested with Android and Apple Smartphones
- Published as open-source:
  https://github.com/open5Gcube/open5Gcube
  - Invitation to try it out
  - We look forward to your feedback



Thank you for your attention!
Questions? Ideas? Suggestions?

Contact

Thorsten Horstmann
Mobile Communication Lab
www.mc-lab.de

Fraunhofer FKIE
Cyber Analysis & Defense
thorsten.horstmann@fkie.fraunhofer.de

Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE
Fraunhoferstr. 20 | 53343 Wachtberg

www.fkie.fraunhofer.de

Hochschule Bonn-Rhein-Sieg
Institute for Safety and Security Research (ISF)
thorsten.horstmann@h-brs.de

Hochschule Bonn-Rhein-Sieg
Grantham-Allee 20 | 53757 Sankt Augustin

www.h-brs.de