Towards Securing Next-Generation Networks Attacking 5G Core-RAN Testbed

G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, S. Ouzounidis, M. Zevgara, I. Moscholios, S. Goudos, P. Sarigiannidis

Authors

George Amponis, Panagiotis Radoglou-Grammatikis, S. Ouzounidis, M. Zevgara
Research and Development Department
K3Y Ltd., Bulgaria
{gamponis, pradoglou, souzounidis, mevgara}@k3y.bg

Thomas Lagkas
Department of Computer Science, International Hellenic University, Greece
{tlagkas}@cs.ihu.gr

Ioannis Moscholios
Department Informatics & Telecommunications
University of Peloponnese, Greece
idm@uop.gr

Sotirios Goudos
Department of Physics,
Aristotle University of Thessaloniki, Greece
idm@uop.gr

Panagiotis Sarigiannidis
Department of Electrical and Computer Engineering
University of Western Macedonia, Greece
psarigiannidis@uowm.gr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952672 (SANCUS)

Outline

- Motivation
- Background
- Design & Implementation
- Conclusion

Motivation

Motivation[1/2] – Introduction

- As 5G and next-generation telecommunications become more prevalent, it is important to address security issues arising in such environments and network typologies.
- Currently, there exist virtually no 5G security datasets, and no integrated frameworks for training Intrusion Detection and Prevention Systems (IDPSs), or network security administrators.
- In this paper, we investigate the potential for the development of an integrated cybersecurity testbed incorporating both the 5G Core and a Radio Access Network (RAN).
- The key contribution of our work is the proposal of a fully containerized testbed, incorporating the 5G core, a RAN, a set of potentially vulnerable hosts, and the appropriate entry points.
- We establish and automate a fully secured sandbox capable of emulating complex cybersecurity.

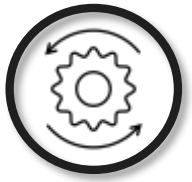
Motivation[2/2] – Aim of this work

The developed testbed is envisaged to pave the path towards facilitating the generation of realistic datasets containing malicious traffic captured over 5G tunnels for enhancing the security of next generation telecommunications.

We consider realistic application-layer attacks against various services.

- We explore the potential of a completely containerized testbed for the purpose of complete automation and sandboxing.

- We validate the capability of the established network to offer connectivity between virtualized subscribers and legitimate hosts in the DN.

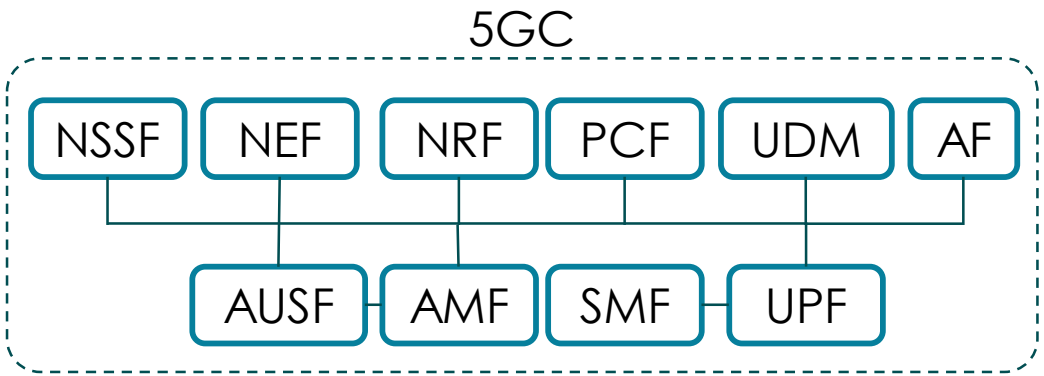


- We investigate a set of attacks focusing on realism and quantifiability of results.

Background

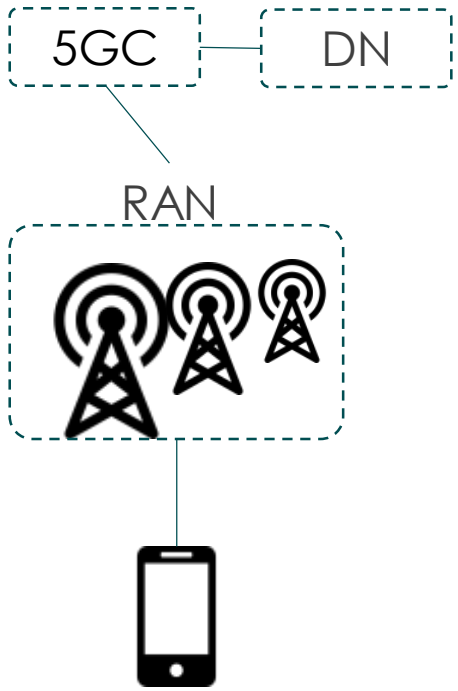
Background[1/3] – 5GCore

- What is the 5G Core?
  - It is **a network composed of standardized Network Functions (NFs)**.
  - It is **the heart of a 5G mobile network,** as it establishes reliable, secure connectivity to the Data Network (DN) for user equipment (UE) and provides access to its services.
- The standardized 5G core is composed of 10 NFs:
  1. Access and Mobility Management Function (AMF)
  2. Session Management Function (SMF)
  3. User Plane Function (UPF)
  4. Network Slice Selection Function (NSSF)
  5. Network Exposure Function (NEF)
  6. Network Repository Function (NRF)
  7. Policy Control Function (PCF)
  8. Unified Data Management (UDM)
  9. Application Function (AF)
  10. Authentication Server Function (AUSF)



Background[2/3] – 5G RAN

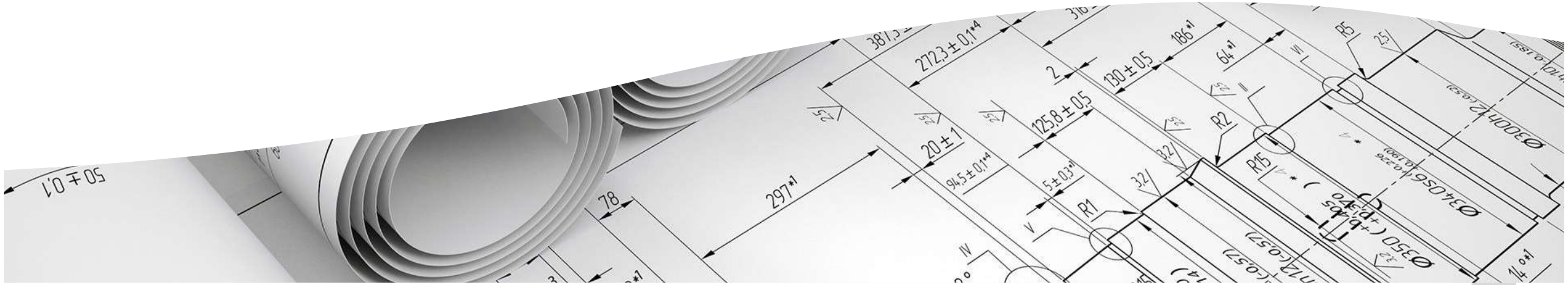
- What is the 5G RAN?
  - It is the main physical-layer component of a mobile telecommunication system and implements radio access for the subscribers.
  - It is a set of cellular antennae (gNodeB), and User Equipment (UE) devices.
- Conceptually, it resides between the UE and the 5GC.
- It is possible for a single UE to be simultaneously connected to multiple radio access networks (dual mode UEs). Such devices seamlessly transfer an ongoing call between different radio access networks without the user noticing any disruption in service.
- It implements the GPRS Tunneling Protocol (GTP) and thus establishes a direct "tunnel" between the subscriber and the DN.



Background[3/3] – Emulation Frameworks

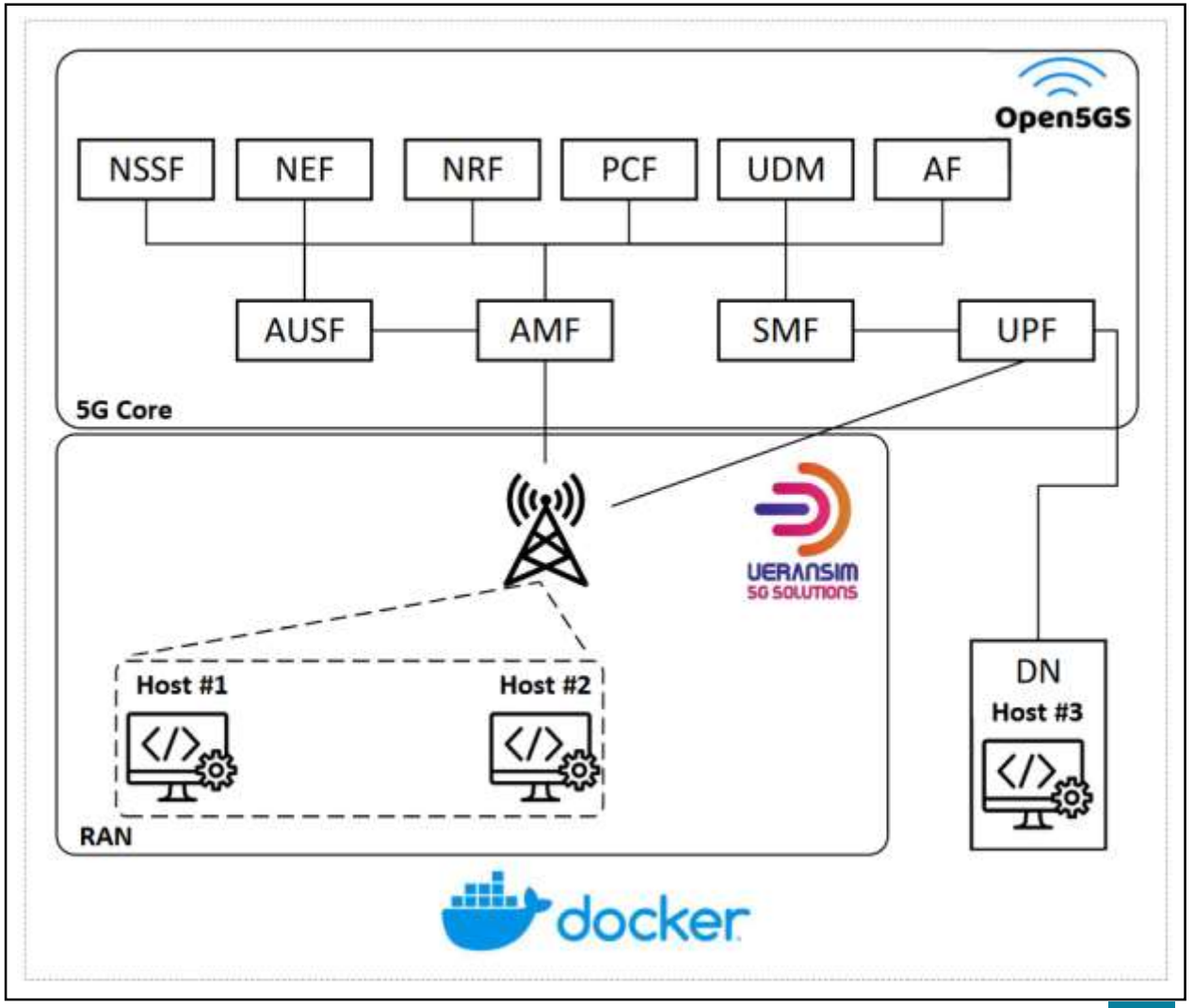
- 5GC: **Open5GS**
  - An open-source implementation for 5G Core, i.e. the core network of LTE/NR network (Release-16).
  - Docker images of individual NFs available.
  - Can be used to build a complete private network using a gNB/eNB and UE emulator, If available.
  - Provides a web-based user interface for registering new subscribers.
- 5G RAN: **UERANSIM**
  - An open source 5G UE and gNodeB simulator.
  - It can be used for testing 5GC Networks in a realistic manner.
- **Docker-compose:**
  - Definition of multi-container applications
  - Supports deployment using a single yaml file.

Design & Implementation



Implementation[1/4] – Testbed Design

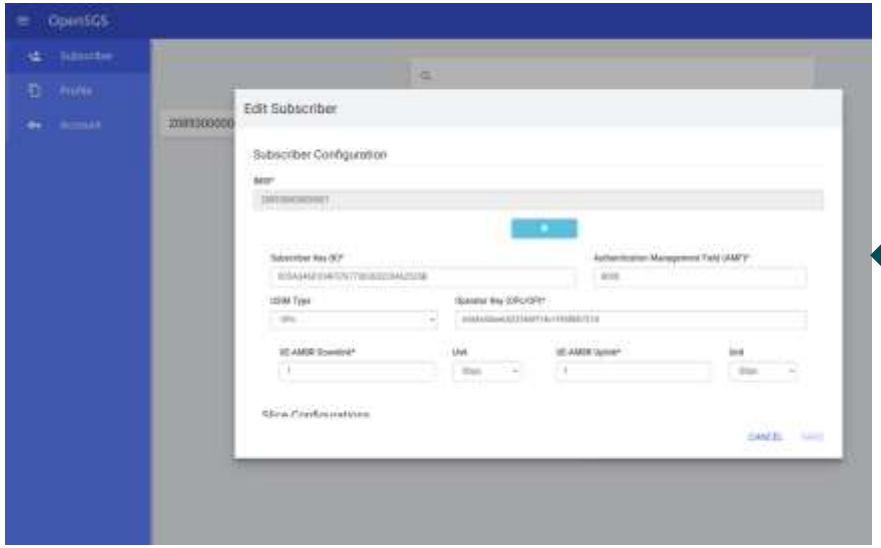
- Overall design is composed of:
  - Open5GS
  - Ueransim
  - Three hosts
- Containers are linked within a docker network.
- All hosts can communicate with each other.
- All hosts in the RAN can ping and receive responses from the DN.
- Subscribers have unique identifiers and are registered by the operator.



Implementation[2/4] – Session Establishment

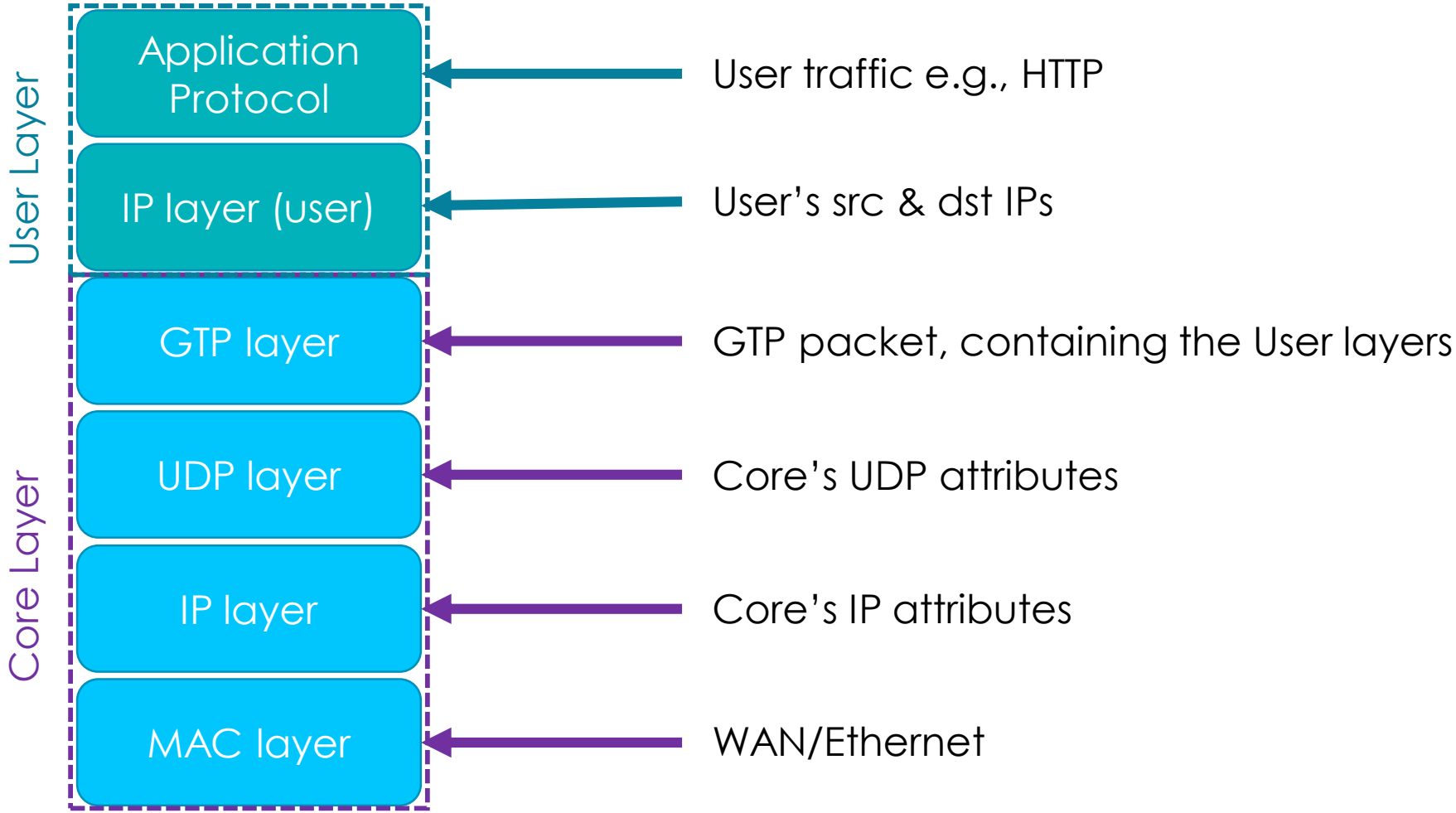
- The attributes needed to register a new user are:
  1. The International Mobile Subscriber Identity (IMSI)
  2. The unique Key
  3. The Operator Code (OPC)
- Subscriber logs indicating successful session establishment:

```
root@ueransim-ue:/UERANSIM/build# ./nr-ue -c ./oai-ue.yaml
[nas] [info] UE switches to state [MM-DEREGISTERED/PLMN-SEARCH]
[rls] [debug] Coverage change detected. [1] cell entered
[nas] [info] Serving cell determined [UERANSIM-gnb-208-93-1]
[nas] [info] UE switches to state [MM-DEREGISTERED/NORMAL-SERVICE]
[nas] [debug] Sending Initial Registration
[nas] [info] UE switches to state [MM-REGISTER-INITIATED/NA]
[rrc] [debug] Sending RRC Setup Request
[rrc] [info] RRC connection established
[nas] [info] UE switches to state [CM-CONNECTED]
[nas] [debug] Security Mode Command received
[nas] [debug] Selected integrity[2] ciphering[0]
[nas] [debug] Registration accept received
[nas] [info] UE switches to state [MM-REGISTERED/NORMAL-SERVICE]
[nas] [info] Initial Registration is successful
[nas] [info] Initial PDU sessions are establishing
[nas] [debug] Sending PDU Session Establishment Request
[nas] [debug] PDU Session Establishment Accept received
[nas] [info] PDU Session establishment is successful PSI
[app] [info] Connection setup for PDU session is successful
```



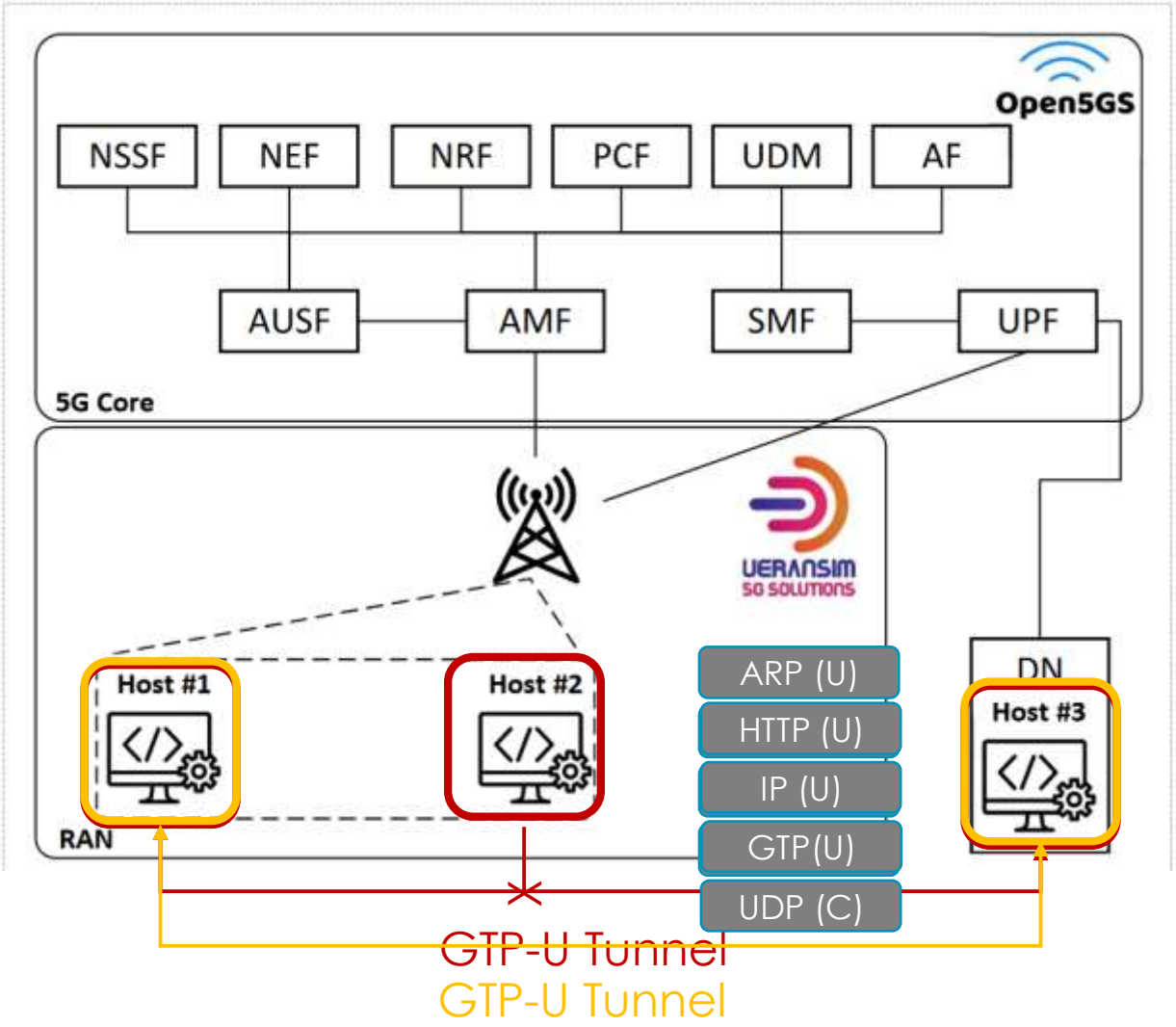
Registering new subscribers in the Open5GS Web UI using the IMSI, key and OPC.

Implementation[3/4] – The GTP protocol stack



Implementation[4/4] – Considered Attack Scenarios

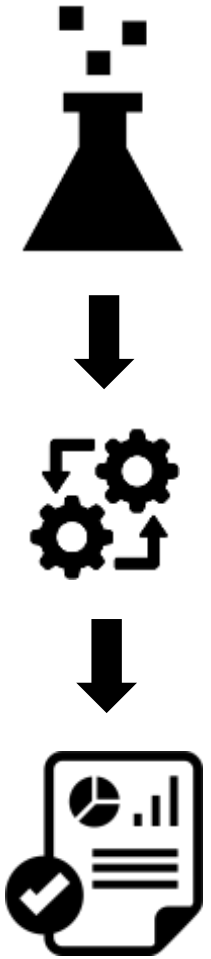
- Man-in-the-Middle Scenario:
  - Involves a legitimate host, a server, and a malicious entity.
  - The malicious entity attempts to eavesdrop the traffic exchanged between Host #1 and Host #3.
  - Attacker performs an arp cache poisoning and captures exchanged traffic.
- Brute-force Scenario:
  - Involves a single UE (malicious entity), and a set of DN-located services synthesizing the ONAP Software Defined Networking Controller (SDNC).
  - Attacker uses hydra to transmit a massive number of https-get requests to gain access to the Direct Graph Builder and highjack the SDN infrastructure.



Conclusion & Future Work

Conclusions & Future Work

- We developed a completely containerized, lightweight and automatically deployable 5GC testbed with RAN capabilities.
- We considered diverse cyberattack scenarios to model the behavior of 5G protocols under such conditions.
- Future work will focus specifically on 5C security and will target specialized attributes of protocols, associated malicious intent in NG cellular networks.
- We are soon going to release a dataset, complimentary to this work, using the same testbed as a basis.
- The presented testbed and the overall virtualized infrastructure has the potential to be used in both industrial and academic environments, for the purposes of:
  - Testing new NF developments
  - Training specialists and cybersecurity personel
  - Teaching the function of the 5GC and the RAN



Thank you for your attention!

Reach out at: gamponis@k3y.bg