# Security Testing and Monitoring of Cloud Native 5G Networks

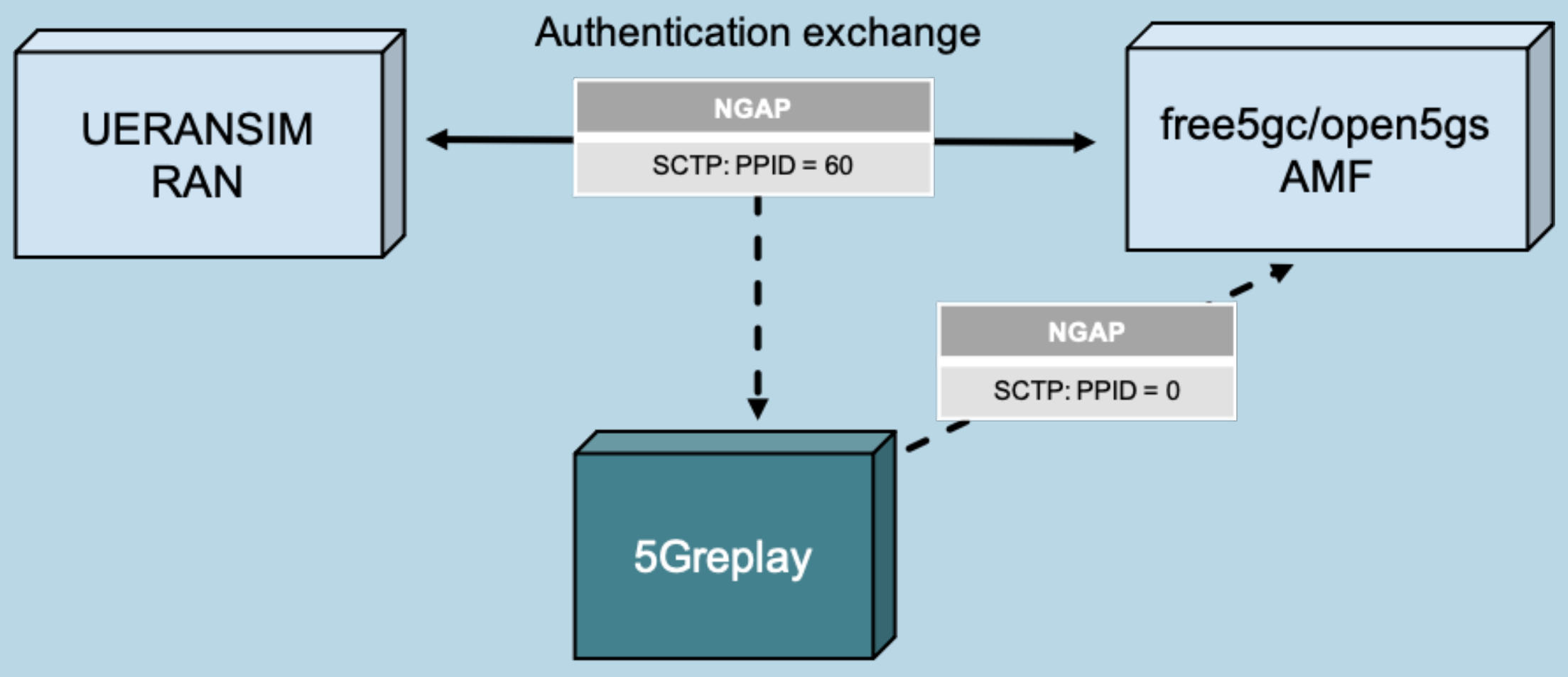
Zujany Salazar, Wissam Mallouli,
Ana R. Cavalli, Fatiha Zaidi

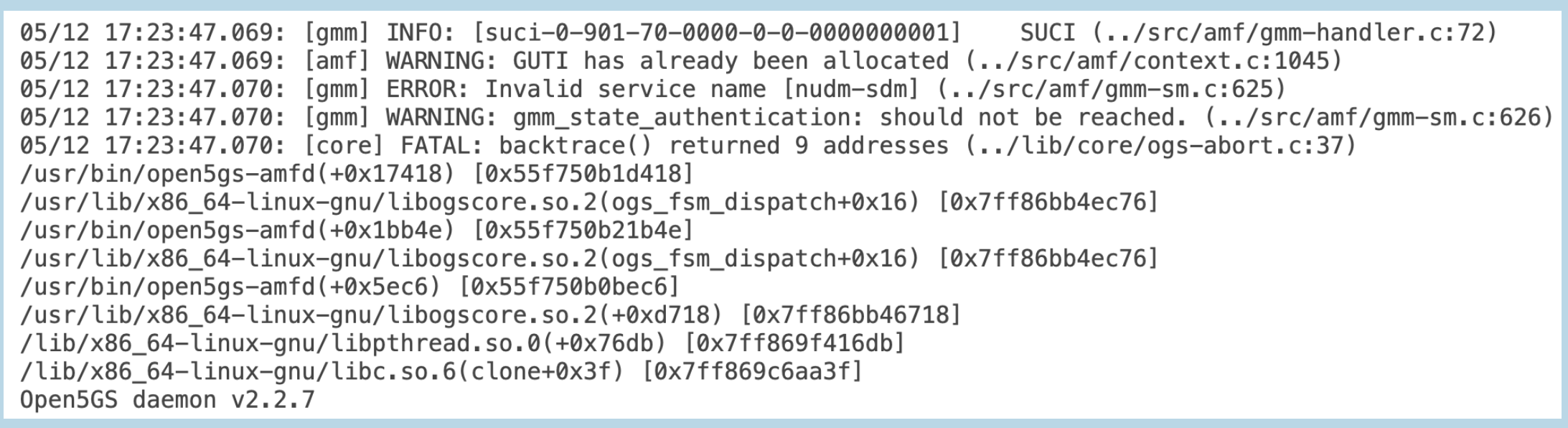
## 5G Security Challenges

- New set cybersecurity issues (threats, vulnerabilities, attacks...)
- Previous protection mechanisms not applicable to the new architecture
- Lack of publicly available labeled data sets containing realistic user behavior and up-to-date attack scenarios
- Lack of open-source solutions that enable to manually create or edit existing 5G network protocol packets and injecting them in a network, allowing to easily test the proposed detection schemes

## Scenario 1: Malformed packets

Create and send malformed packets to a 5G core network, in order to evaluate 5Greplay robustness against unexpected entries at run-time.

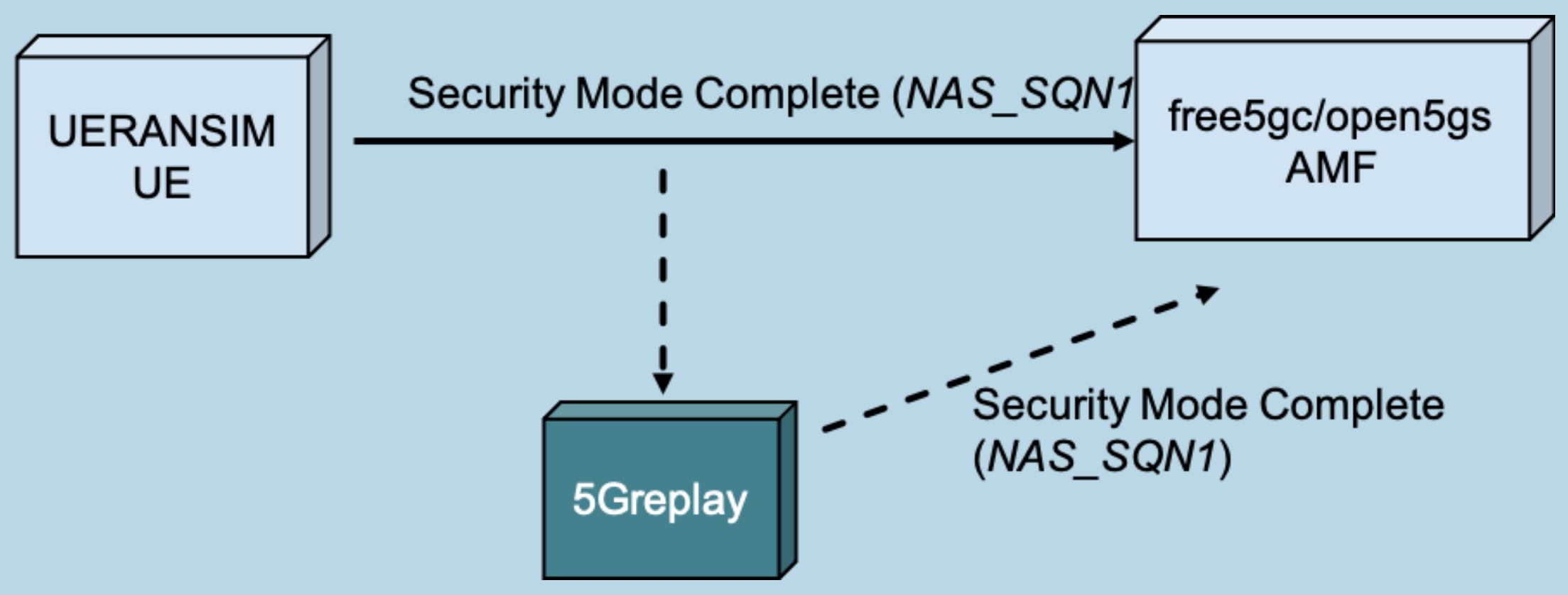


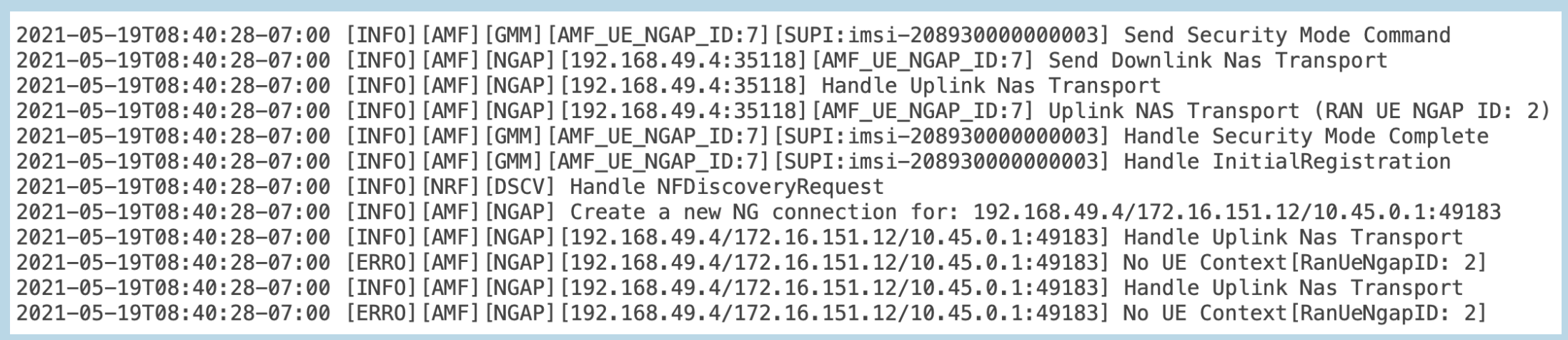


```
05/12 17:23:47.069: [gmm] INFO: [suci-0-901-70-0000-0-0-0000000001]    SUCI (../src/amf/gmm-handler.c:72)
05/12 17:23:47.069: [amf] WARNING: GUTI has already been allocated (../src/amf/context.c:1045)
05/12 17:23:47.070: [gmm] ERROR: Invalid service name [nudm-sdm] (../src/amf/gmm-sm.c:625)
05/12 17:23:47.070: [gmm] WARNING: gmm_state_authentication: should not be reached. (../src/amf/gmm-sm.c:626)
05/12 17:23:47.070: [core] FATAL: backtrace() returned 9 addresses (../lib/core/ogs-abort.c:37)
/usr/bin/open5gs-amfd(+0x17418) [0x55f750b1d418]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x16) [0x7ff86bb4ec76]
/usr/bin/open5gs-amfd(+0x1bb4e) [0x55f750b21b4e]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x16) [0x7ff86bb4ec76]
/usr/bin/open5gs-amfd(+0x5ec6) [0x55f750b0bec6]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(+0xd718) [0x7ff86bb46718]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x76db) [0x7ff869f416db]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x3f) [0x7ff869c6aa3f]
Open5GS daemon v2.2.7
```

## Scenario 2: Replay attack

Perform security tests by modifying and injecting network traffic into a specif target.





```
2021-05-19T08:40:28-07:00 [INFO][AMF][GMM][AMF_UE_NGAP_ID:7][SUPI:imsi-208930000000003] Send Security Mode Command
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4:35118][AMF_UE_NGAP_ID:7] Send Downlink Nas Transport
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4:35118] Handle Uplink Nas Transport
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4:35118][AMF_UE_NGAP_ID:7] Uplink NAS Transport (RAN UE NGAP ID: 2)
2021-05-19T08:40:28-07:00 [INFO][AMF][GMM][AMF_UE_NGAP_ID:7][SUPI:imsi-208930000000003] Handle Security Mode Complete
2021-05-19T08:40:28-07:00 [INFO][AMF][GMM][AMF_UE_NGAP_ID:7][SUPI:imsi-208930000000003] Handle InitialRegistration
2021-05-19T08:40:28-07:00 [INFO][NRF][DSCV] Handle NFDiscoveryRequest
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP] Create a new NG connection for: 192.168.49.4/172.16.151.12/10.45.0.1:49183
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] Handle Uplink Nas Transport
2021-05-19T08:40:28-07:00 [ERRO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] No UE Context[RanUeNgapID: 2]
2021-05-19T08:40:28-07:00 [INFO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] Handle Uplink Nas Transport
2021-05-19T08:40:28-07:00 [ERRO][AMF][NGAP][192.168.49.4/172.16.151.12/10.45.0.1:49183] No UE Context[RanUeNgapID: 2]
```

## Scenario 3: Stress tests

Validate the scalability of 5Greplay.For this, we configured the tool to replay the traffic as much as possible.

| | #packet copies | Avg. packets/s | Avg. kbit/s |
|---|---|---|---|
| open5Gs | 1780 | 509.5 | 834 |
| free5GC | 3000 | 594.9 | 974 |

## Acknowledgements

H2020 projects SANCUS N° 952672, INSPIRE-5Gplus N° 871808, and the French ANR project MOSAICO.

## Security testing and monitoring

The main objective of this thesis is to contribute to the Security testing and monitoring of 5G networks, in order to adapt it to challenges that the new technologies introduce.
For that we will divide the thesis in 3 main stages:

Testing
Monitoring
Reaction

- Security testing
- Attack injection

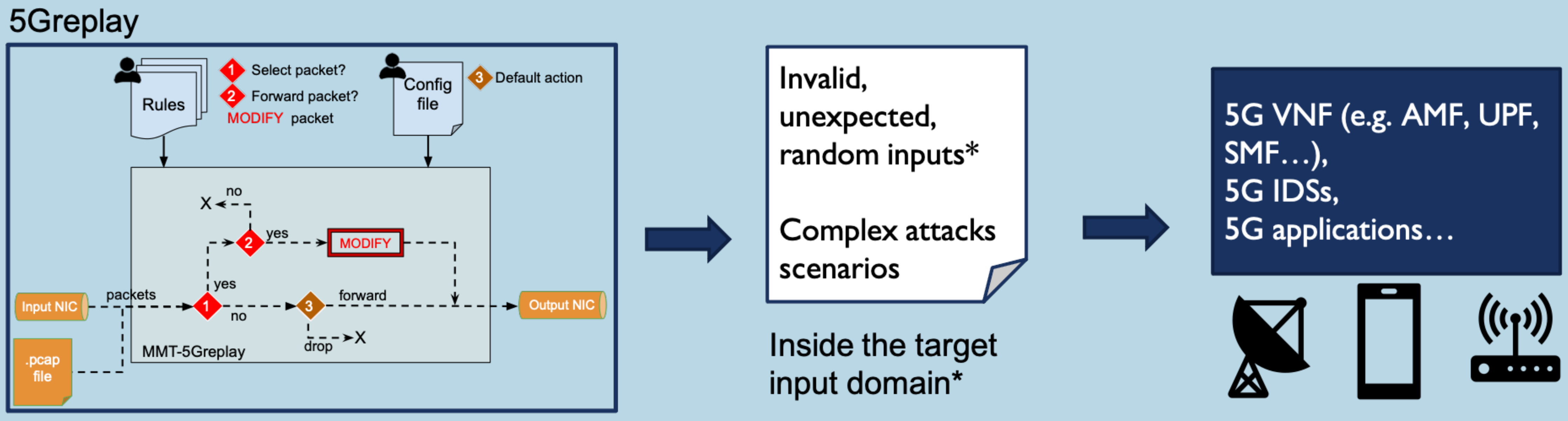
- Identified vulnerabilities and threats

- Countermeasures

## 5Greplay: a 5G Network Traffic Fuzzer

**5Greplay** is an open-source solution entirely developed by the authors that allows forwarding network packets from one network interface card to another with or without modification.

- One-way bridge between the input NIC (Network Interface Controller) and the output one
- Take as input pre-captured packets in PCAP-format file or live traffic
- Behavior is controlled by **user defined rules** and completed by a **configuration file**



```
<property value="THEN"  delay_units="ms" delay_min="0" delay_max="1" property_id="100" type_property=
     "FORWARD" description="Forwarding NAS security mode COMPLETE that answers to NAS security mode
     COMMAND" if_satisfied="#update(sctp_data.data_ppid, 0)">
    <event event_id="1" description="NAS Security mode COMMAND"
         boolean_expression="(nas_5g.message_type == 93)"/>
    <event event_id="2" description="NAS Security mode COMPLETE"
         boolean_expression="(nas_5g.security_type == 4)"/>
</property>
```

## Fuzzing Operators

5Greplay aims performing fuzz testing, a type of mutation testing that injects invalid, unexpected, or random inputs to evaluate the response of a test target, in this case the 5G virtual network functions, the Intrusion Detection Systems, the 5G applications, etc.

**DEL_PKT(P)** Delete a packet.

**CH_ATTR(P)** Change a specific attribute on the header of a network protocol message.

**ORD(P1,P2)** Exchange the order of two consecutive packets.

**DUP_PKT(P)** Duplicate packet.

## References

[1] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov: *Overview of 5G Security Challenges and Solutions*, IEEE Communications Standards Magazine 2, 1(2018)

[2] Hajar Moudoud,Lyes Khoukhi,and Soumaya Cherkaoui *Prediction and Detection of FDIA and DDoS Attacks in 5G Enabled IoT*, IEEENetwork 35, 2 (2021)

[3] Gulyas, Laszlo et al.: *Betweenness Centrality Dynamics in Networks of Changing Density.* Presented at the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010)

[4] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler: *A Formal Analysis of 5G Authentication.*. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security(2018)