

| HACKATHON26

Huu-Nghia Nguyen

Montimage



5Greplay - a 5G network traffic fuzzer



Co-funded by
the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.

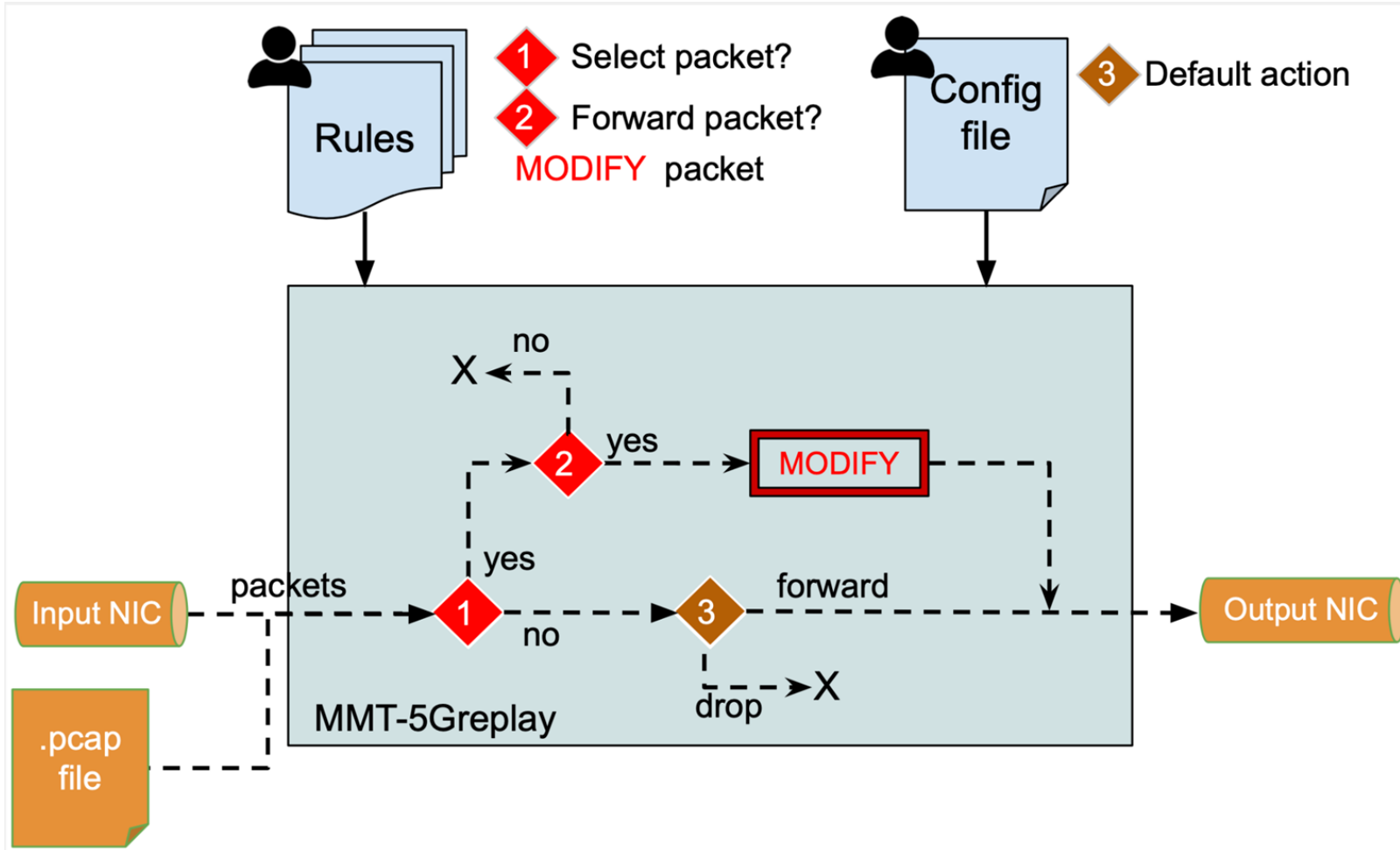


- 01 Context & Motivation
- 02 5Greplay Architecture
- 03 Tool Overview
- 04 What Can You Explore?



- 5G new technologies require to be tested from a functional and non-functional
- New cybersecurity threats
- Previously adopted security and privacy mechanisms become ineffective
- **Goal:** The creation of new sets of security test cases and tools specifically targeting 5G security concerns

5Greplay: An **open-source** solution to perform **fuzz testing** of 5G networks, allowing to forward network packets from one NIC to another with or without **modifications**.



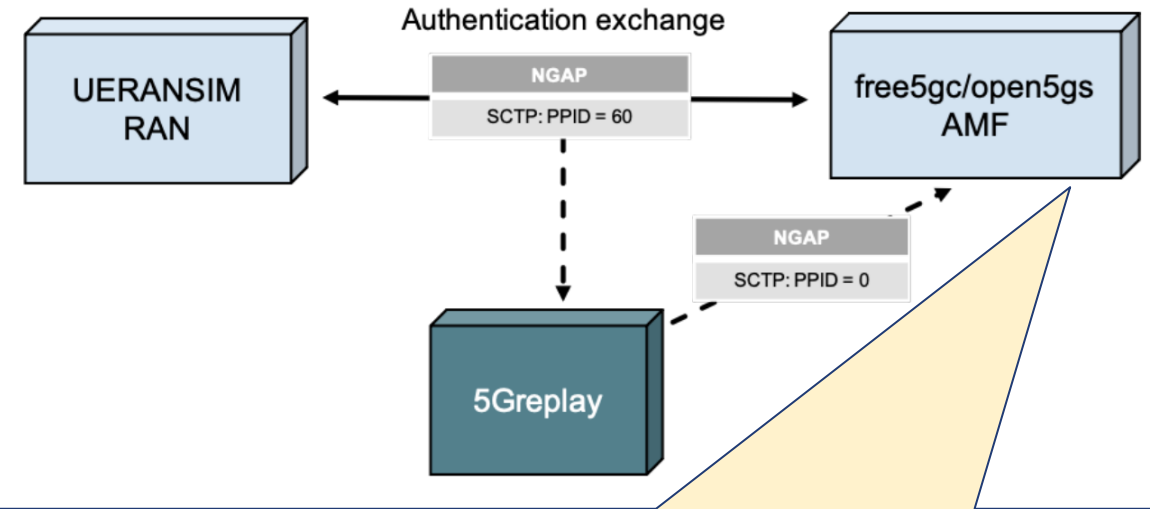
Mutation operators:

- ✓ delete packets
- ✓ duplicate packets
- ✓ modify attributes



montimage

- **CLI-based tool** with multiple commands covering different scenarios
- **Deployment:** Run locally or in Docker containers
- **Integration:** Exposed through commands, APIs, or MCP interfaces.
- **Project:**
 - <https://github.com/montimage/5greplay>
 - <https://5greplay.org/docs.html>



```
05/19 13:05:47.869: [mem] FATAL: No OGS_CLUSTER_8192_SIZE (../lib/core/ogs-pkbuf.c:327)
05/19 13:05:47.869: [mem] ERROR: ogs_pkbuf_alloc() failed [size=8192] (../lib/core/ogs-pkbuf.c:198)
05/19 13:05:47.869: [core] FATAL: ogs_asn_encode: Assertion 'pkbuf' failed. (../lib/asn1c/util/message.c:31)
05/19 13:05:47.870: [core] FATAL: backtrace() returned 13 addresses (../lib/core/ogs-abort.c:37)
/usr/lib/x86_64-linux-gnu/libogsasn1c-util.so.2(ogs_asn_encode+0x124) [0x7f72e68e6004]
/usr/lib/x86_64-linux-gnu/libogsngap.so.2(ogs_ngap_encode+0x33) [0x7f72e71b6b23]
/usr/bin/open5gs-amfd(+0x24df2) [0x55dfb927fdf2]
/usr/bin/open5gs-amfd(+0x12423) [0x55dfb926d423]
/usr/bin/open5gs-amfd(+0x2af99) [0x55dfb9285f99]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x16) [0x7f72e75d5c76]
/usr/bin/open5gs-amfd(+0x1ab72) [0x55dfb9275b72]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(ogs_fsm_dispatch+0x16) [0x7f72e75d5c76]
/usr/bin/open5gs-amfd(+0x5ec6) [0x55dfb9260ec6]
/usr/lib/x86_64-linux-gnu/libogscore.so.2(+0xd718) [0x7f72e75cd718]
/lib/x86_64-linux-gnu/libpthread.so.0(+0x76db) [0x7f72e59c86db]
/lib/x86_64-linux-gnu/libc.so.6(clone+0x3f) [0x7f72e56f1a3f]
Open5GS daemon v2.2.7

2021-05-19T06:33:44-07:00 [ERR0][N3IWF][NGAP] [SCTP] DialSCTP(): connection timed out
2021-05-19T06:33:44-07:00 [ERR0][N3IWF][NGAP] Failed to connect to AMF.
2021-05-19T06:33:44-07:00 [ERR0][N3IWF][Init] Start NGAP service failed: NGAP service run failed
```

- Replay real or pre-captured 5G traffic
- Create rules to modify, duplicate, delete, or drop packets
- Test different 5G protocols and network scenarios
- Test 5G core components such as Open5GS or free5GC
- Observe how the 5G core reacts to unexpected or malformed messages
- **Step-by-Step Tutorials** (including screencast):
 - <https://5greplay.org/docs/tutorial/replay-open5gs/>
 - <https://5greplay.org/docs/tutorial/replay-oaicn/>
 - <https://5greplay.org/docs/tutorial/smc-message/>



Cyber Suite | HACKATHON26

Thank you for your attention!



Montimage



Huu-Nghia Nguyen



huunghia.nguyen@montimage.eu



<https://montimage.eu/>



Co-funded by
the European Union

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Digital Europe Programme. Neither the European Union nor Digital Europe Programme can be held responsible for them.