Public Networks (Telco) Risk & Threats.

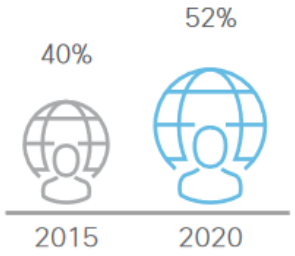
ADVANTIO

CISCO

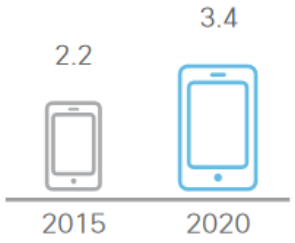
VNI Complete Forecast Highlights

Global

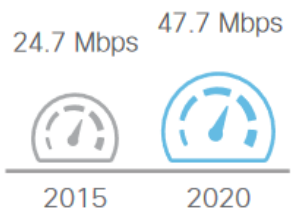
Internet Users: % of Population



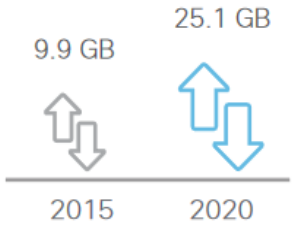
Devices and Connections per Capita



Average Speeds



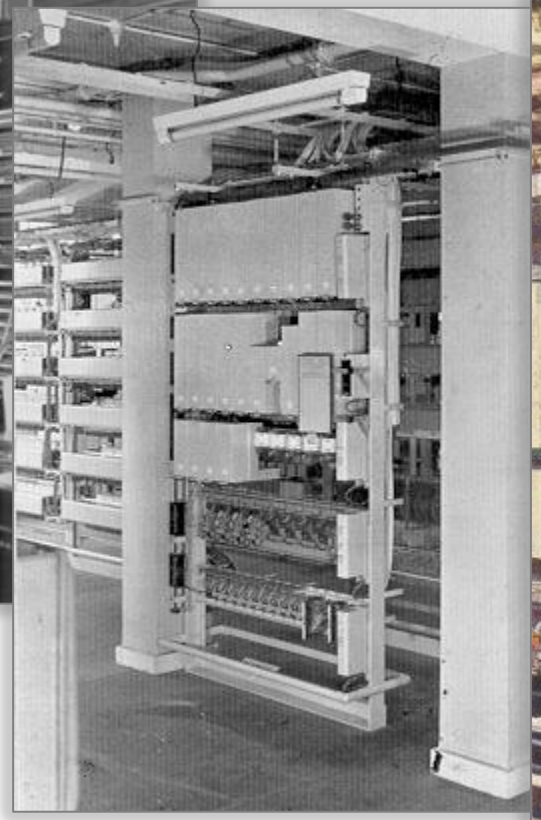
Average Traffic per Capita per Month

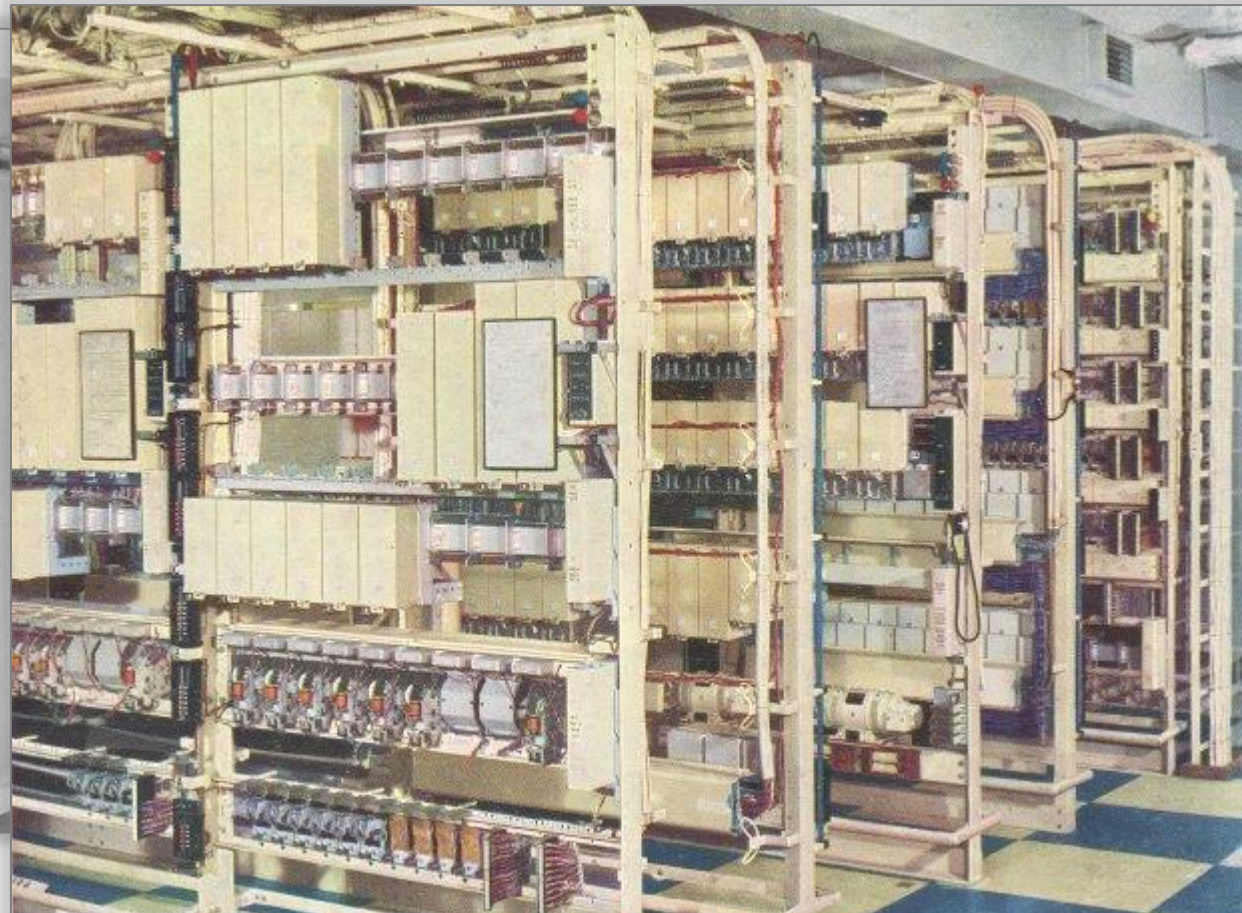


Most of security compliances, Standards and regulations dedicate an entire requirement for the data transmission over public Networks :

- ISO 27001 - A.14.1.2
- PCI DSS – Requirement 4.
- PA DSS – Requirement 10 & 11.
- Payment Brands security Programs (Visa MasterCard, JCB, AMEX..)
- NIST 800-53 …

Yesterday: Closed Ecosystems





Security Myths

- Telco technology is based on proprietary systems that are completely isolated.
- Hacker cannot access radio equipment since it's not based on IP.
- External resources (web, mail, etc.) are not a part of Telco business.
- Telecom equipments vendors are delivering secure and hardened devices.

Telecom today is not just a mobile network !

- Huge distributed networks.
- Unification of various services (mobile communication, broadband access, Wi-Fi, hosting, VoIP, etc.).
- Great number of applications and systems on the perimeter (Applications and VAS Platforms).
- Lots of perimeters!
- Many networks belong to third parties.
- A phone network node was once a “black box”, but now nodes are built on popular hardware and software platforms (Linux, Solaris, and xWorks).

The reality in details

- Exotics inside and outside? Most of telecom equipment is no longer based on proprietary systems and uses well known operation systems and application software.
- PSTN, 2G, 3G and 4G are now interconnected and are converging toward IP.
- The more G's, the more IP. The More IP, the more threats!
- Huge non-segmented networks.
- Security is still focusing on IT networks and not focusing on Radio part as it worth.

The reality in details

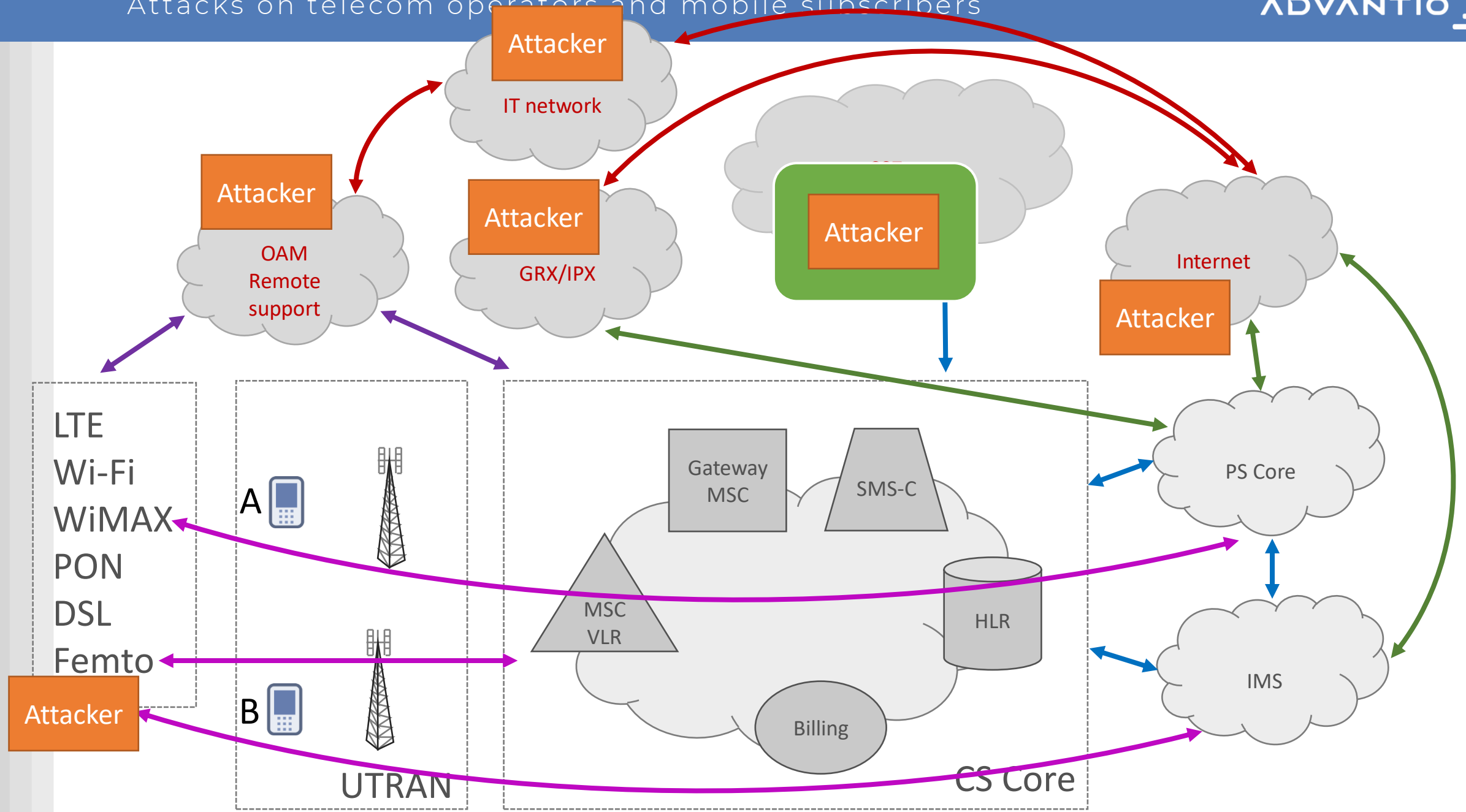
•A wide range of access layer devices and the greater access to new functions exposes the network to new threats for potential attacks coming from outside and from the inside as well.

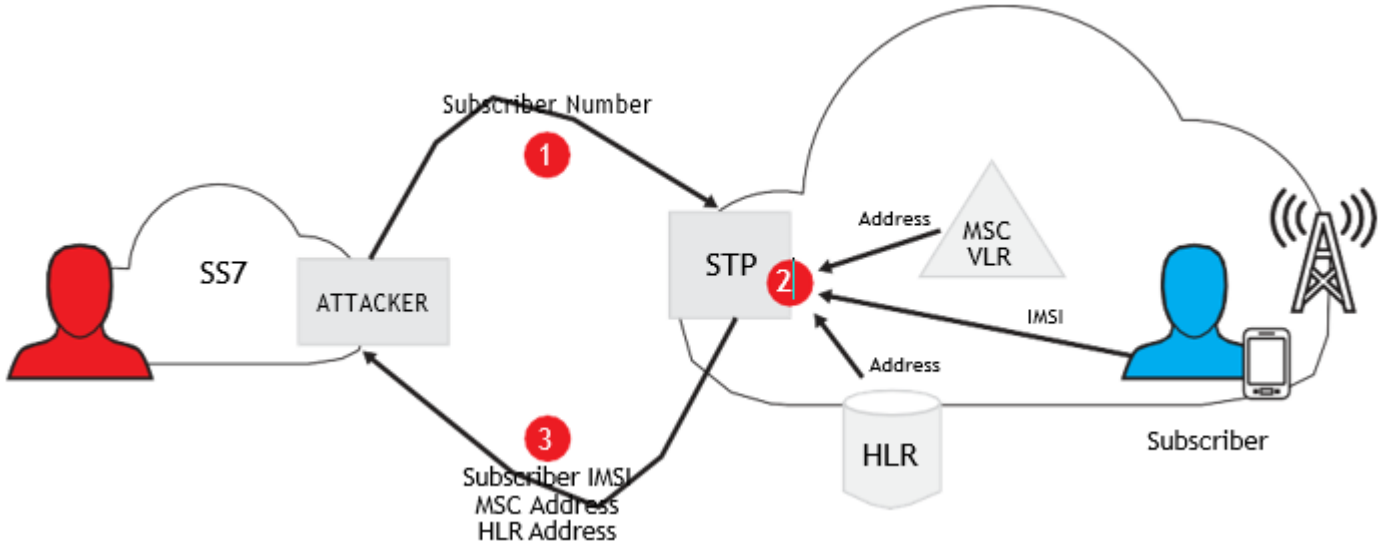
•Many networks belong to third parties. Peer relationship between operators. New perimeters – New Threats!

•Forensics nightmare.

Attack vectors.

- SS7
- BRAN: intrusion, interception, jamming, denial of service, Fraude
- SIM cards,
- VAS
- Grx, GTP
- Hosting,
- Etc.

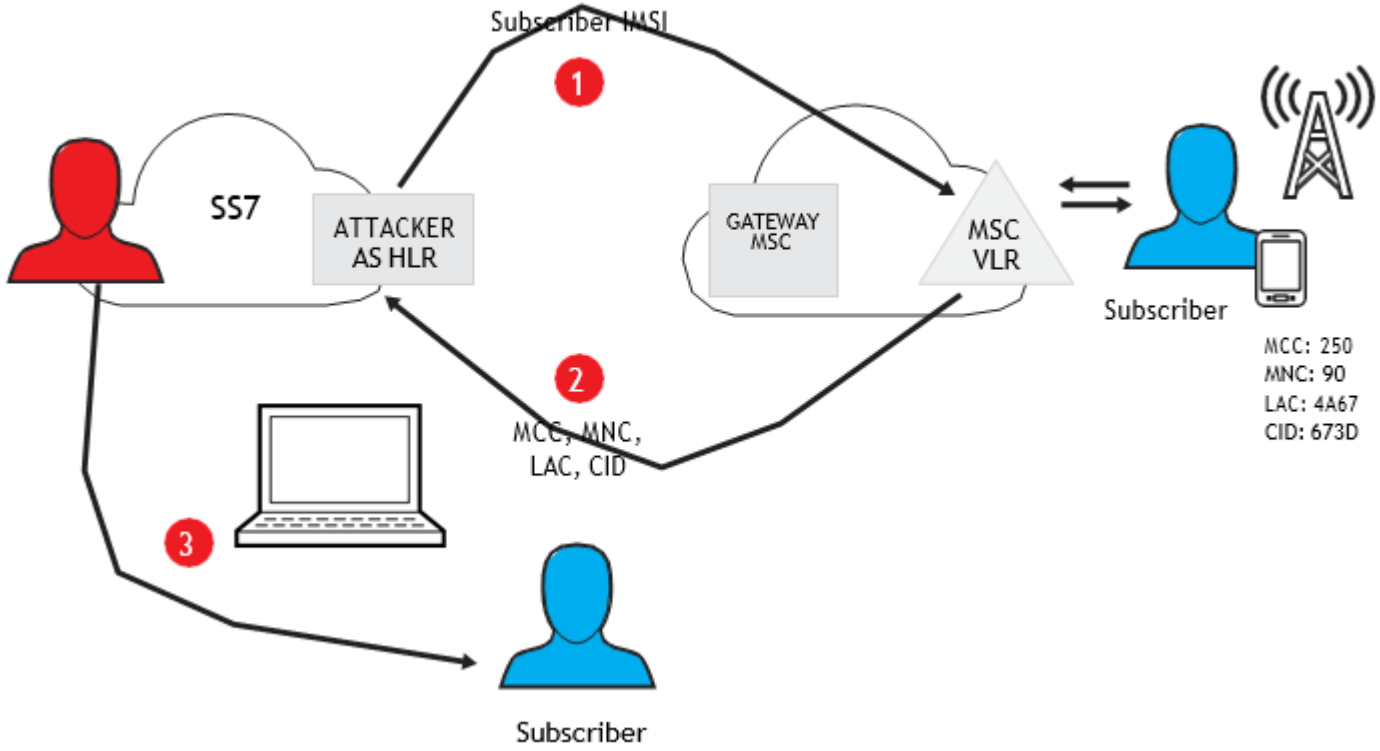

Attacker
IT network
Attacker
OAM
Remote
support
Attacker
GRX/IPX
Attacker
Internet
Attacker
LTE
Wi-Fi
WiMAX
PON
DSL
Femto
A
B
Attacker
UTRAN
Gateway
MSC
SMS-C
MSC
VLR
HLR
Billing
CS Core
PS Core
IMS



IMSI disclosure

- **Result:** In case of successful exploitation, an attacker obtains the following data:

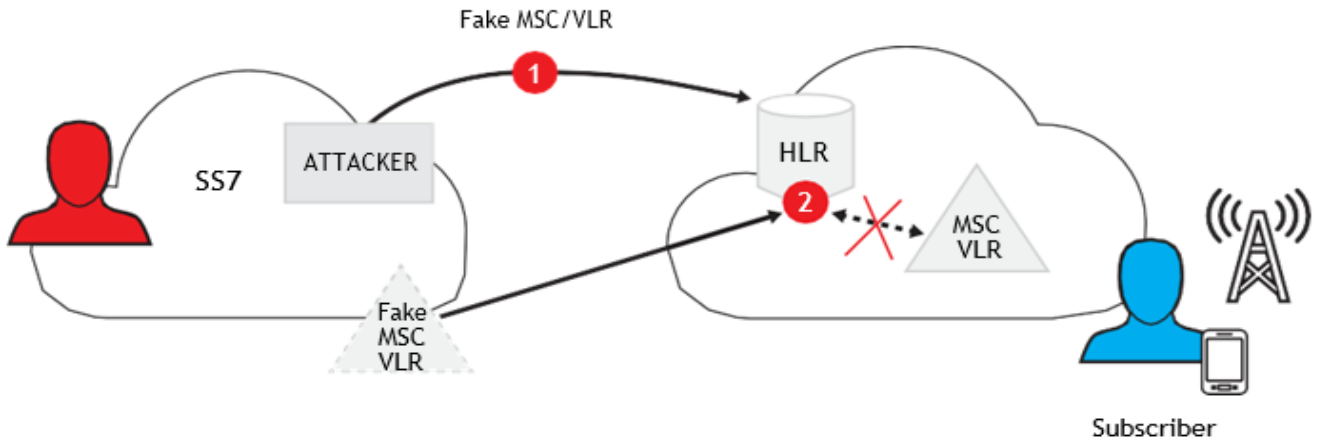
- Subscriber's IMSI , Servicing MSC/VLR address, Home Location Register (HLR) address where the subscriber's account data is located



Determining a subscriber's location

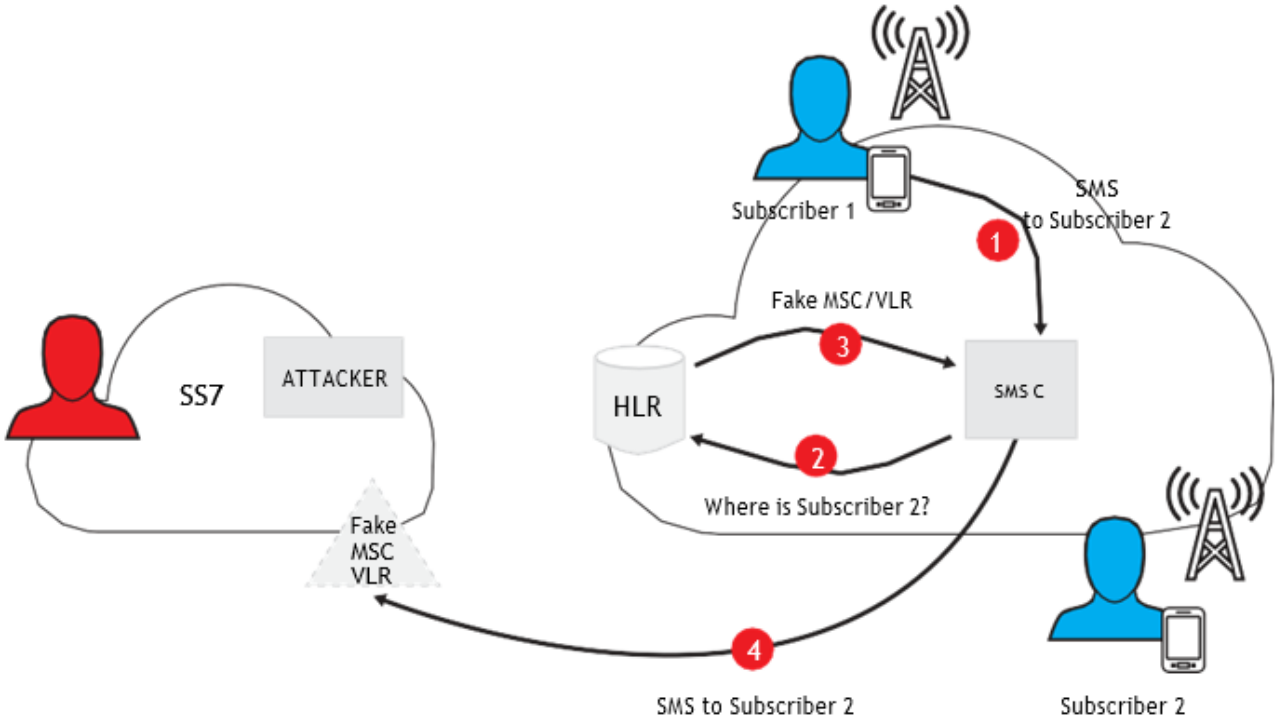
- **Result:** The intruder obtains the CGI, which consists of:

Mobile Country Code (MCC), MNCMobile Network Code (MNC), Location Area Code (LAC) and Cell Identity (CID).



Block a subscriber from receiving incoming calls and text messages

- Result:Although the phone indicates connectivity to the network, the subscriber cannot receive calls or text messages. Subscriber services remain blocked until he/she travels to another MSC/VLR area, reboots the phone or makes an outgoing call.

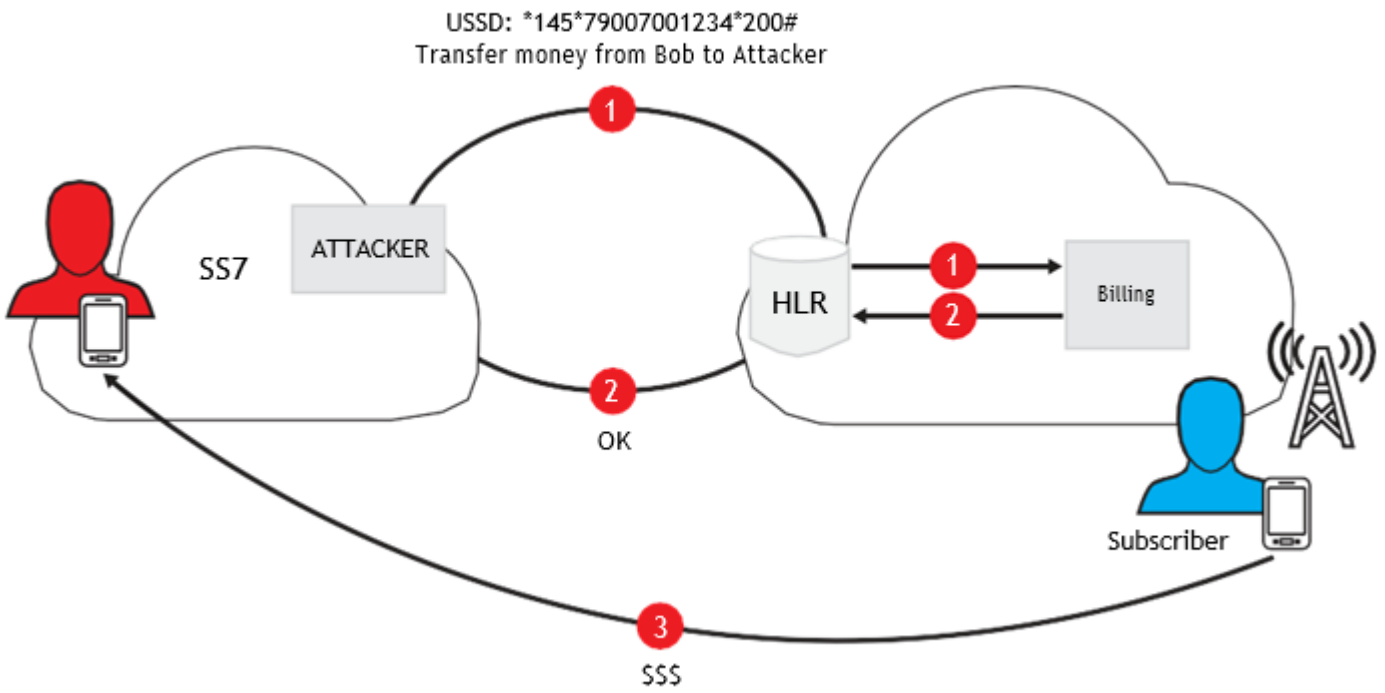


Intercept a subscriber's incoming SMS messages.

Result:

-Steal one-time mobile banking passwords delivered as SMS messages

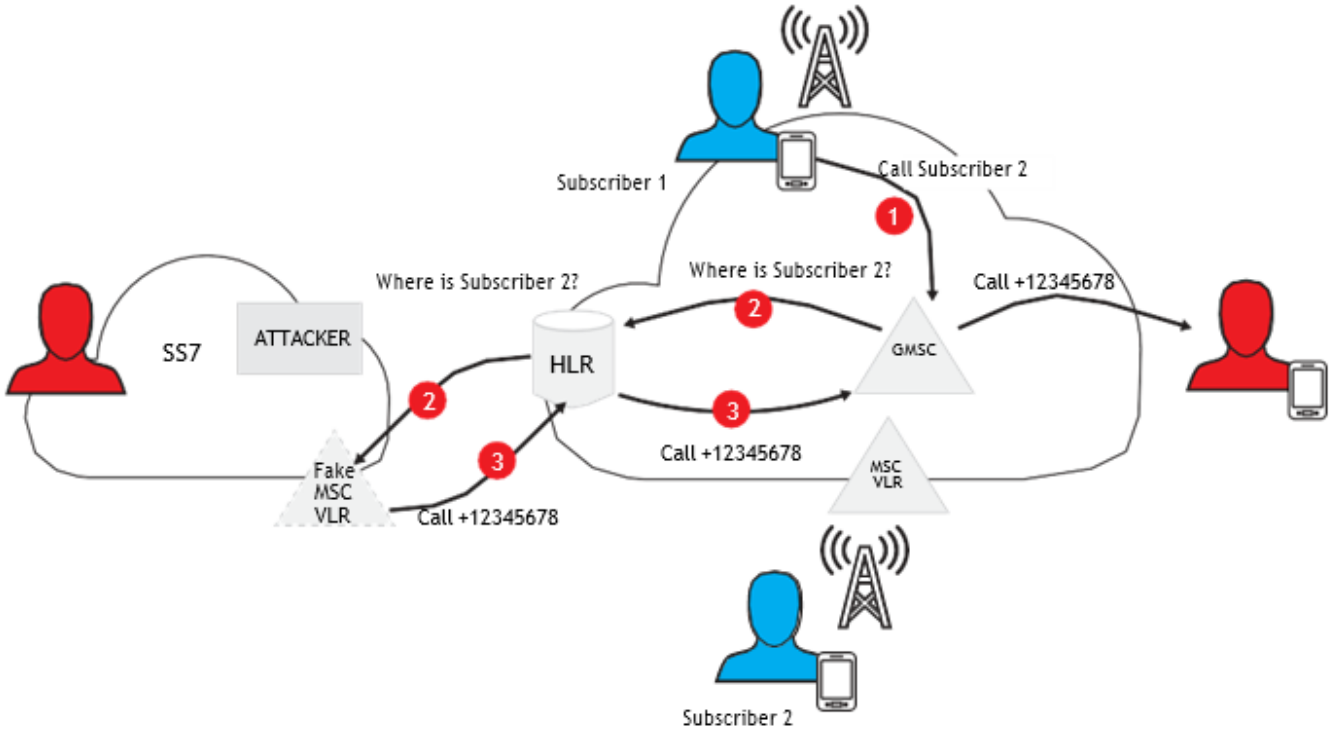
-Intercept or recover passwords used for various internet services (email, social networks, etc.)



USSD request manipulation

Result:

The most dangerous scenario related to this attack would be sending a request to transfer funds between a subscriber's accounts. Such an action might go unnoticed for quite some time, even if the service provider sends an SMS notification about the transaction. Further, to block any such notification, an attack could combine this attack with the previous attack.



Change voice call routing and redirect incoming Calls

Result:

An attacker is able to redirect calls. In this particular case he/she redirects an incoming call to an arbitrary number.

Stealing money, determining subscriber location, tapping calls and disrupting communication services are all threats made possible by exploiting SS7 vulnerabilities.

With connections made possible by the Internet, mobile communication has become a preferred attack point for hackers looking to penetrate critical infrastructures and the enterprise.

Stealing money, determining subscriber location, tapping calls and disrupting communication services are all threats made possible by exploiting SS7 vulnerabilities.

With connections made possible by the Internet, mobile communication has become a preferred attack point for hackers looking to penetrate critical infrastructures and the enterprise.

Mitigation by Telecom Operator

- Analyze provider hosts in the SS7 network.
- Control message filtering.
- Monitor SS7 traffic
- Examine the potential for attacks and fraud
- Find equipment configuration errors and vulnerabilities in protocols.
- Penetration Testing.
- Vulnerability detection and analysis.
- Application testing, configuration.

QUESTIONS?

ADVANTIO

THANK YOU

Hassen Trabelsi

Senior Information Security Consultant – PCI & PA DSS QSA, IS27001 LI, CEH.

Hassen.trabelsi@ADVANTIO.COM

+216 27 09 11 52