SS7 Attacks

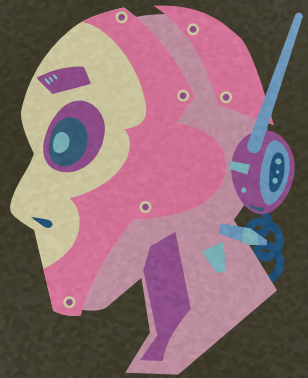
Telecommunication Hacking

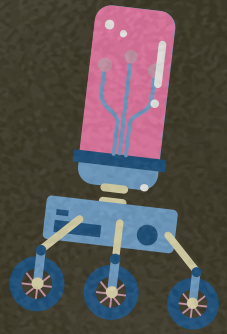
TLP: GREEN

"The slide"

Pierre CEBERIO

21yo, OSINT & Security Analyst @BreacHunt, Co-Founder at Les Pires Hat





Les Pires Hat

https://piresh.at/

Préambule

Plus opaque

Absent de l'infosec français

Pas d'eau chaude

2008

Critique

"Société"

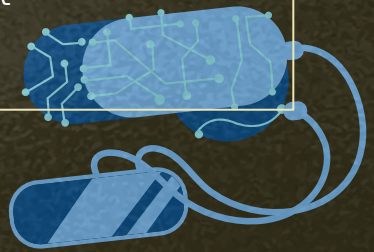
HISTORIQUE

Création en **1975**
Originalement : système fermé accessible aux opérateurs de lignes (paradigme du **jardin clos / "Walled Garden"**)

Arrivée de **SIGTRAN** : extension du SS7 et fin de l'isolation avec l'ouverture du marché

2G et **3G** basés sur SS7 : toujours existant

4G : utilisation de **Diameter**



Explication SS7

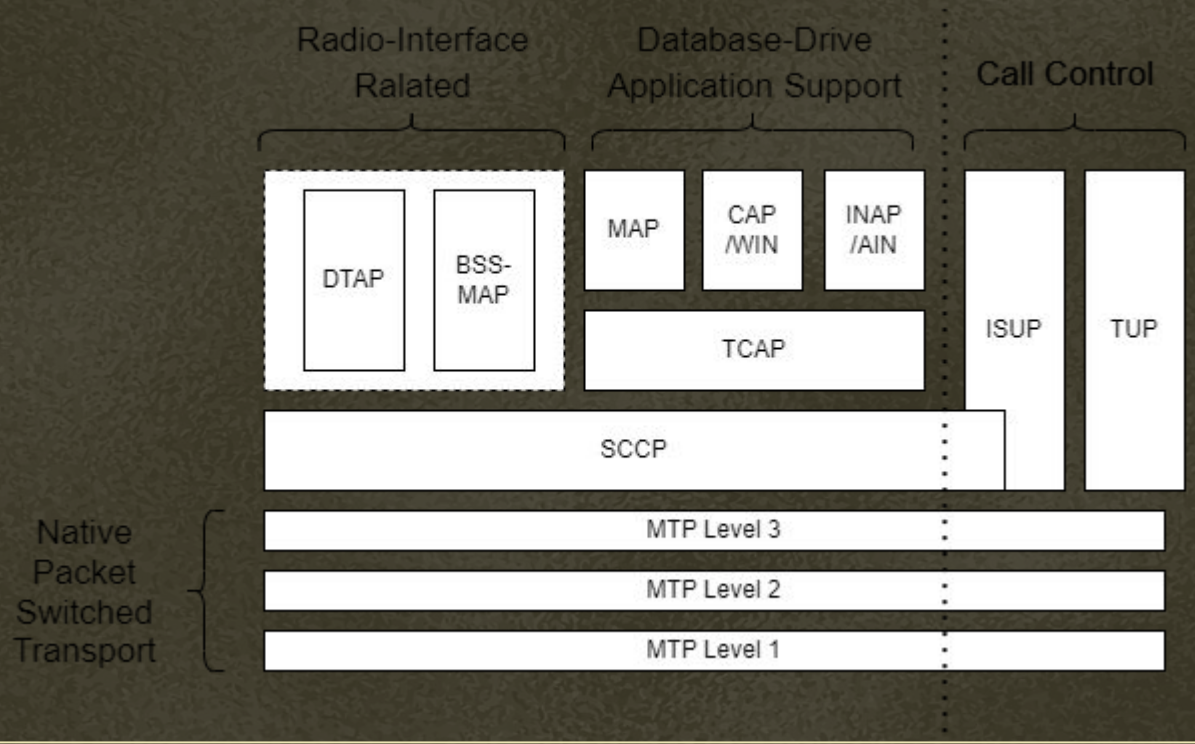
Le **système de signalisation n° 7** est le réseau mondial qui interconnecte tous les opérateurs de télécommunications dans le monde:

- Signal ?
- **Interopérabilité** 2G & 3G
- **Prise en charge** : émission / réception appels et messages texte, suivi facturation, déplacement en itinérance
- Itinérance ?
- Couche SS7 : nécessite une authentification

- Signalling ?
- **Common Channel Signalling**
- Nodes = **Signaling Points** (SP)
- SS7 agit comme "système nerveux"
- Comment marche un appel ?

- & more standard et spécificités ...

SS7 Stack


Radio-Interface Ralated
Database-Drive Application Support
Call Control
DTAP
BSS-MAP
MAP
CAP /WIN
INAP /AIN
TCAP
ISUP
TUP
SCCP
Native Packet Switched Transport
MTP Level 3
MTP Level 2
MTP Level 1

01

MTP

Message Transfer Part

02

ISUP

Integrated Services Digital Network User Part

03

SCCP

Signaling Control Connection Part

04

TCAP

Transaction Capabilities Application Part

05

MAP

Mobile Application Part

06

INAP

Intelligent Network Application Part

Glossaire

Le moment adoré

01

SS7

Signaling System 7

02

HLR

Home Location Register

03

MSC / VLR

Mobile Switching Centre / Visitor Location Register

04

SMSC

SMS Center

05

IMSI / TMSI

International Mobile Subscriber Identity / Temporary

06

MSISDN

Mobile Station International Subscriber Directory Number

01

Operator / Subscriber

Opérateur / Abonné

02

MME

Mobile Management Entity

03

SGW

Serving Gateway

04

SSP

Service Switching Point

05

SCP

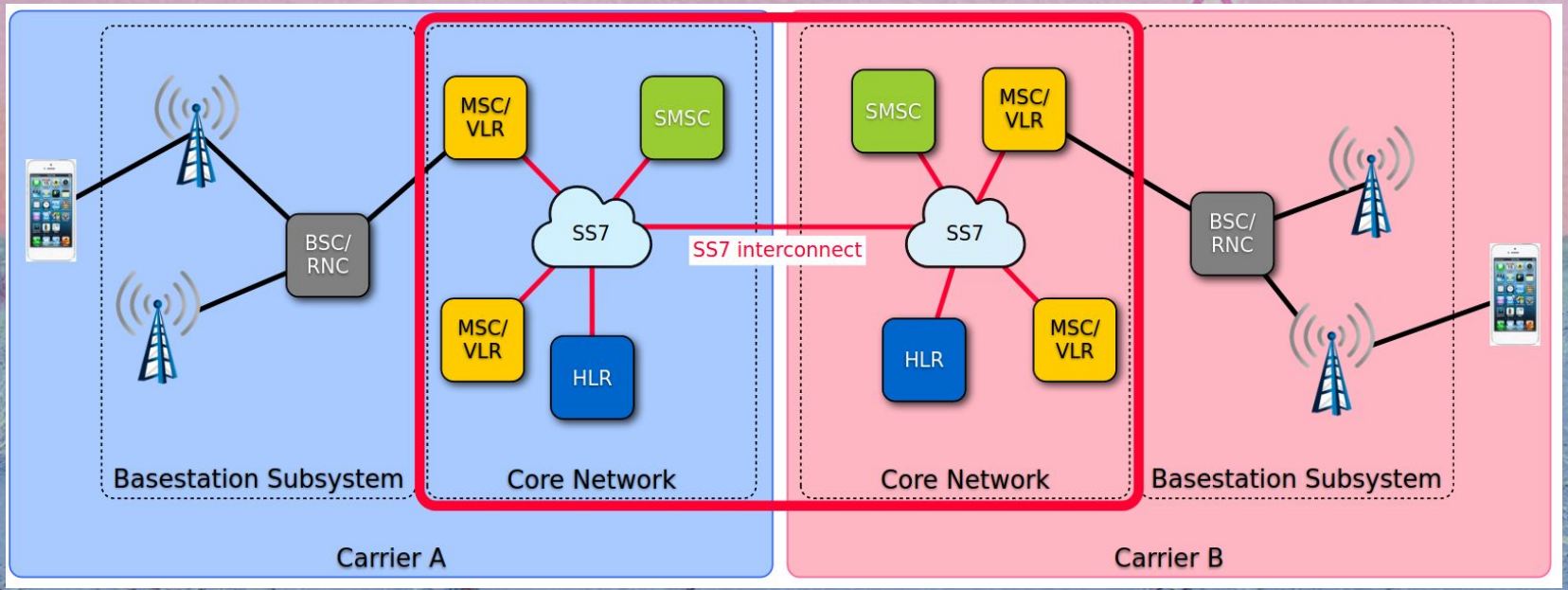
Service Control Point

06

STP

Signal Transfer Point

Architecture Overview



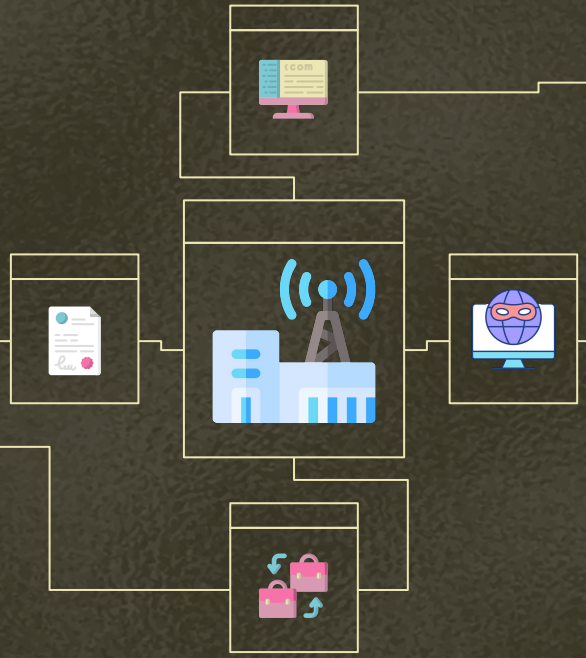
Les points d'entrée

Légal

/ Semi Légal

Hack !

Scan & Hack The Planet



Corruption

Trouver le gars sûr

Deep ?

Scam land

BUDGET

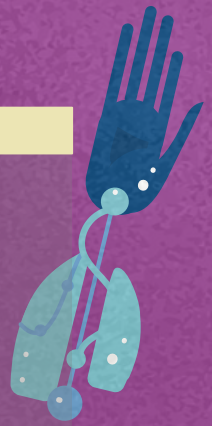
Money, Money, Money

Budget : Rogue BTS GSM maison

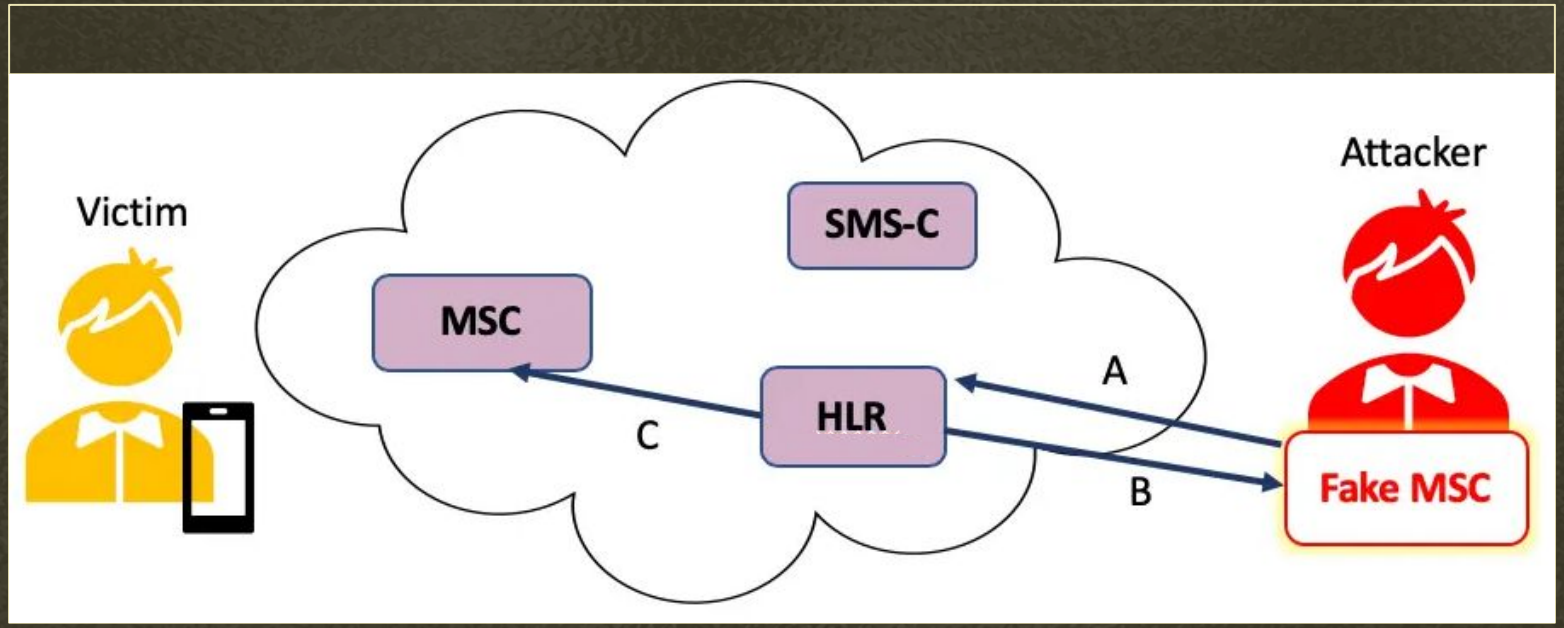
- bladeRF x40 : 420 $
- 2 Quad-band Cellular Duck Antennas SMA : 16 $
- Raspberry Pi 3 : 32 $
- Pack batterie USB : 50 $
- Carte MicroSD (8GB ou +) : 5 $

Prix total : 523 $

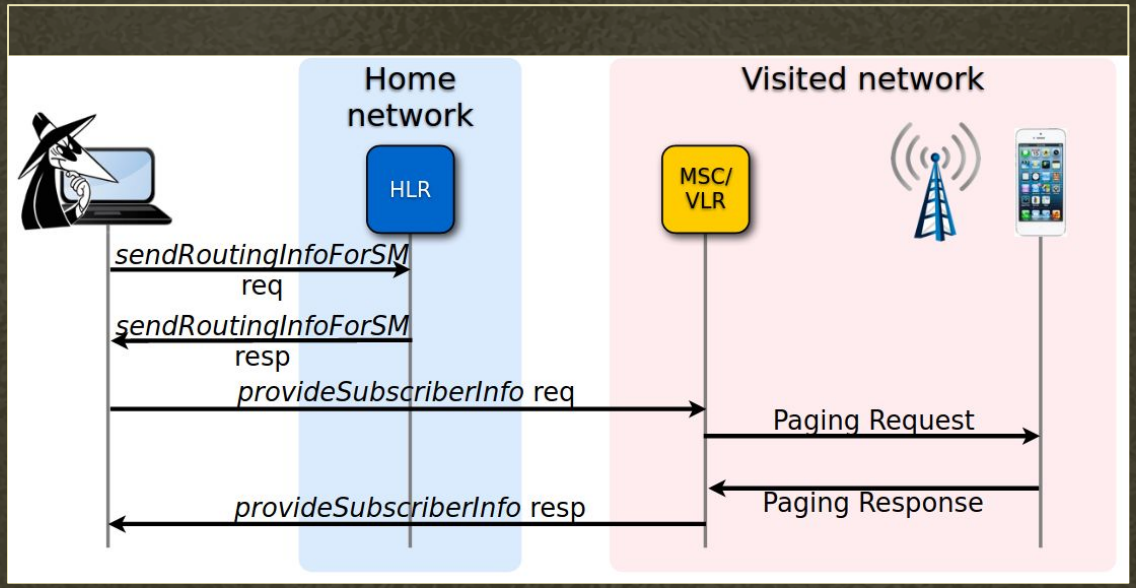
Types d'attaques



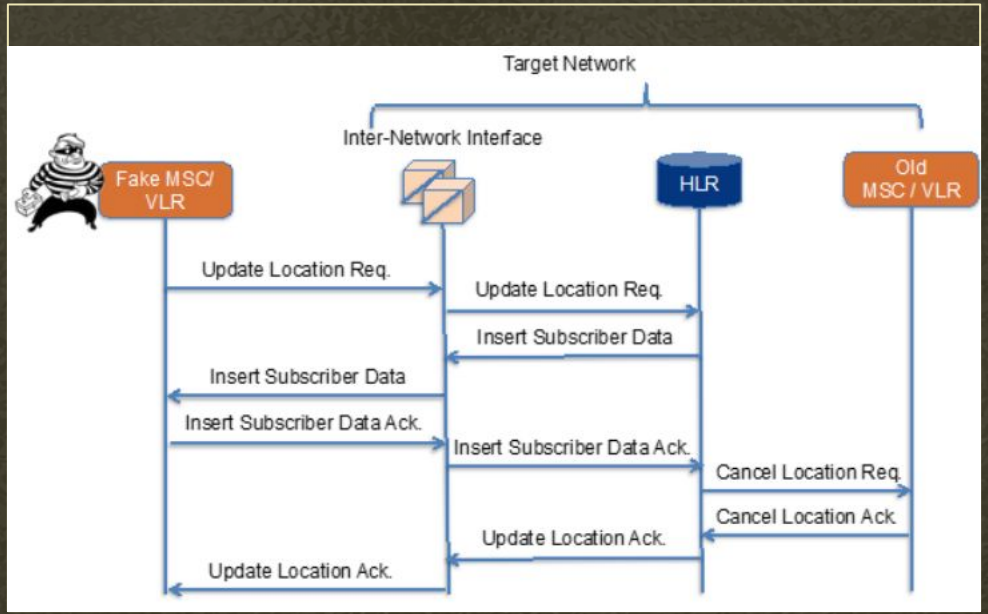
Step 0 : Avoir l'IMSI et le VLR



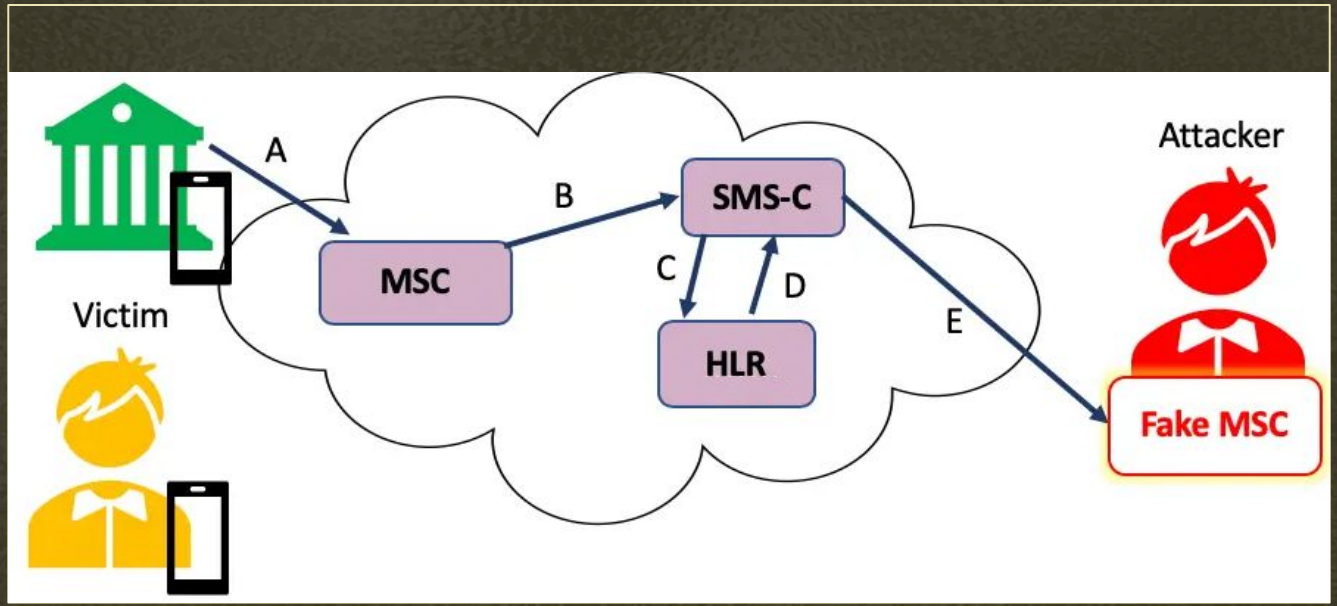
Avoir la localisation



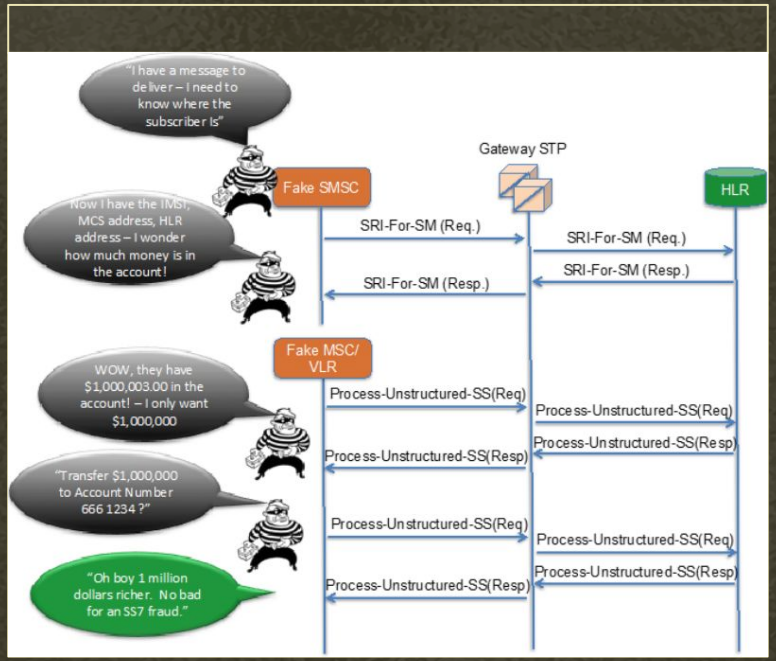
Denial of Service



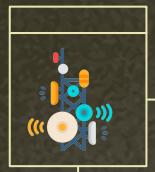
SMS / Call Interception



Manipulation requête USSD

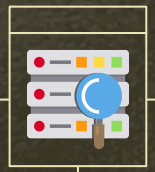


Les outils : pour aller plus loin



SigPloit

Signaling Pentest Framework



GTScan

Nmap scanner for Telco

JSS7

SS7 stack emulated in Java

Osmocomm

Open-source Mobile Communications

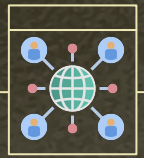
Les défenses et recommandations

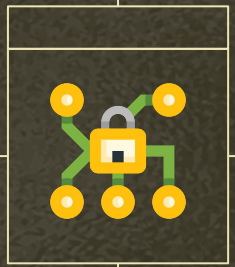
Configurez !

#Balance ton nœud

Stop SMS

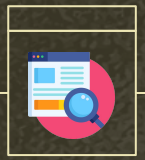
Signal contre Signal





Monitoring

Monsieur est nomade



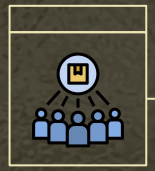
S'outiller

Très coûteux

Conclusion : la fin du monde

Récapitulatif

SS7: La **Foire aux Plaisirs**

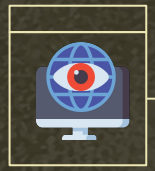


Et l'End-User ?

Dépendant et 2FA

4G & Diameter / 5G ?

VoLTE: Fausse bonne idée ?



Big Brother is watching you

Coup **d'épée** dans l'eau ?

MERCI

@acabthegod

Place au TP

boringthegod@tutanota.com
pierreceberio.com

pierre-ceberio