



SS7

Attacks

Telecommunication Hacking

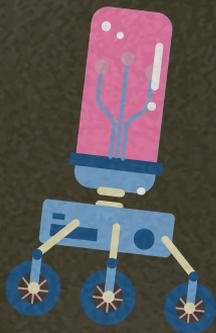
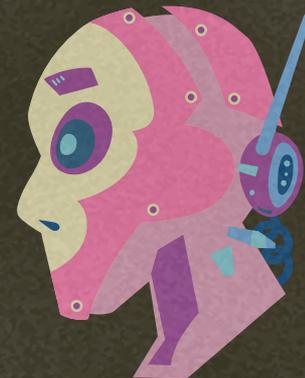


TLP: GREEN

"The slide"

Pierre CEBERIO

21yo, OSINT & Security Analyst
@BreachHunt, 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

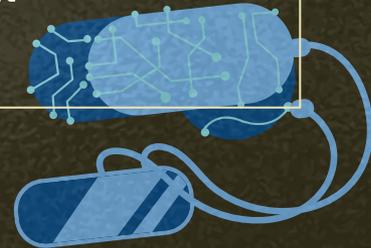
Création en **1975**

Originellement : 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

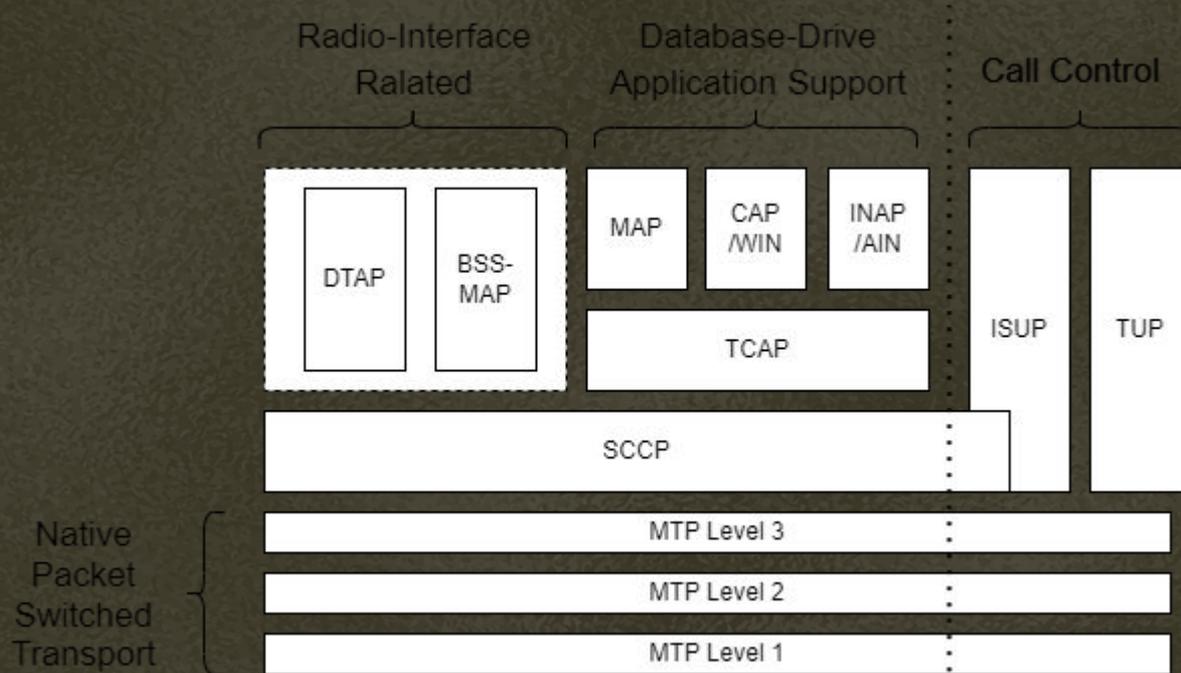
Le **système de signalisation n° 7** est le réseau mondial qui interconnecte tous les opérateurs de télécommunications dans le monde:

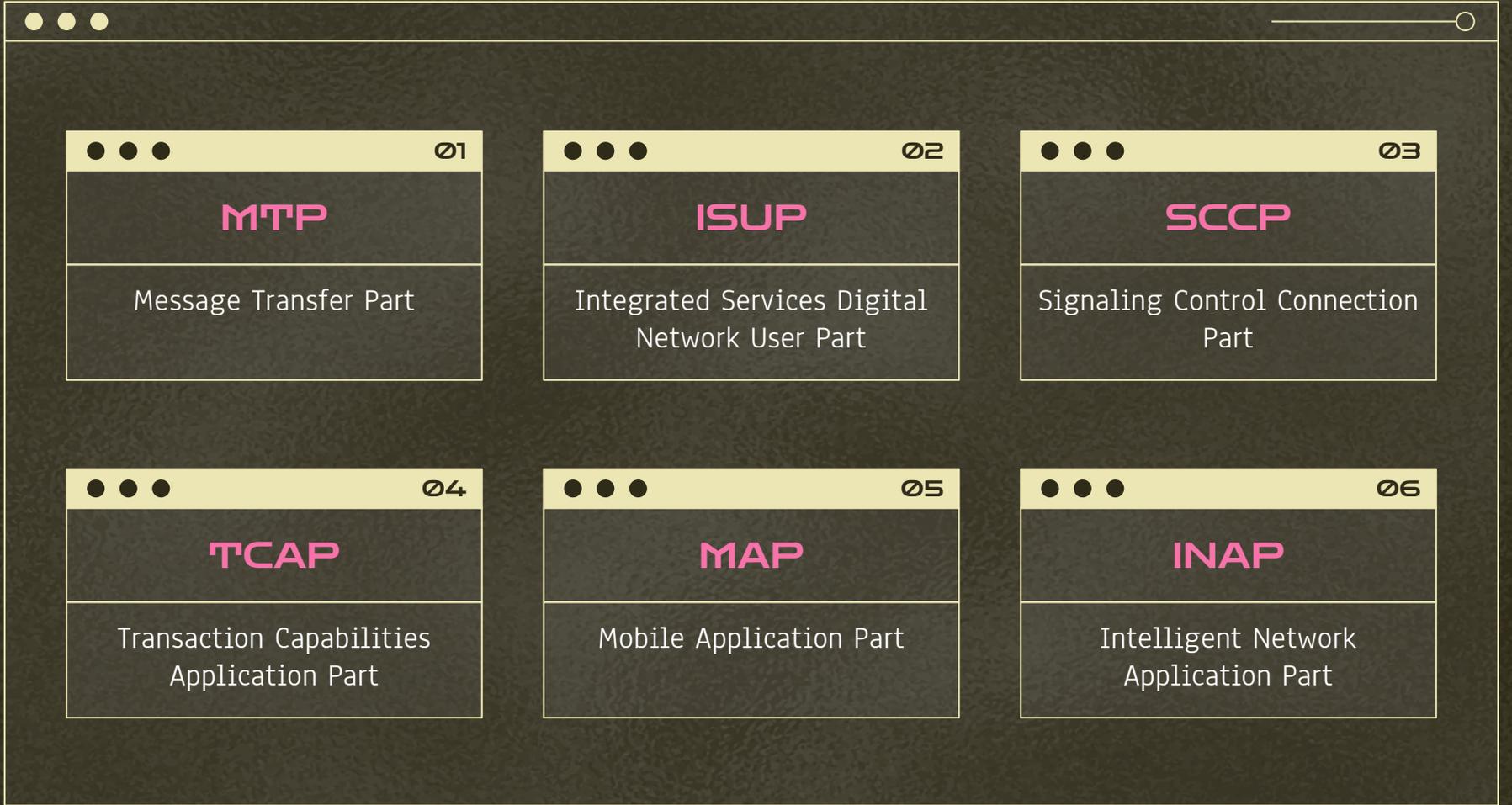
- Signal ?
- **Interopérabilité** 2G & 3G
- **Prise en charge** : émission / réception appels et messages texte, suivi facturation, déplacement en itinérance
- Itinérance ?
- Couche SS7 : nécessite une **authentification**

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

- & more standard et spécificités ...

SS7 Stack





Ø1

MTP

Message Transfer Part

Ø2

ISUP

Integrated Services Digital
Network User Part

Ø3

SCCP

Signaling Control Connection
Part

Ø4

TCAP

Transaction Capabilities
Application Part

Ø5

MAP

Mobile Application Part

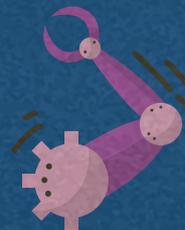
Ø6

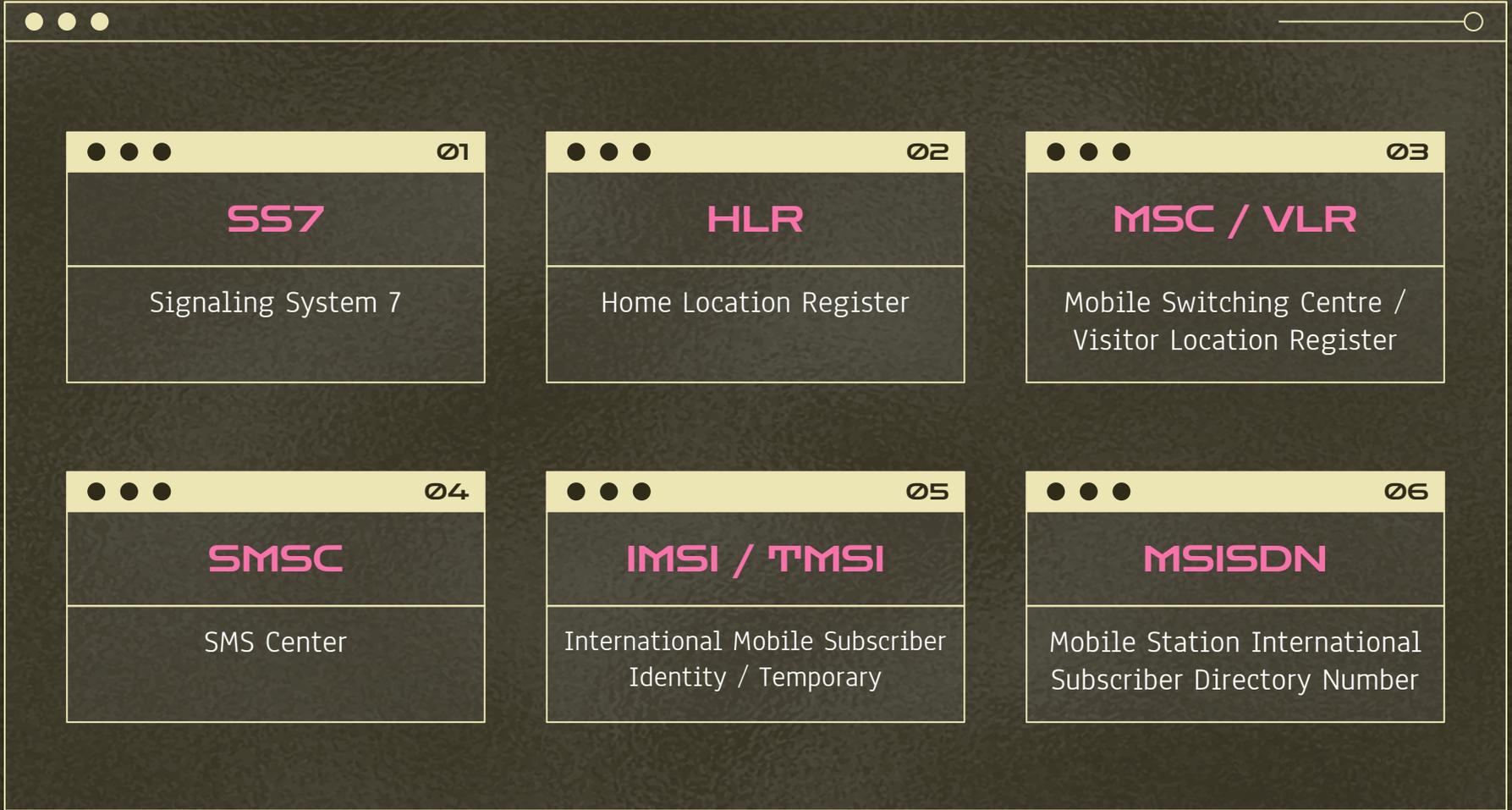
INAP

Intelligent Network
Application Part

Glossaire

Le moment adoré





Ø1

SS7

Signaling System 7

Ø2

HLR

Home Location Register

Ø3

MSC / VLR

Mobile Switching Centre /
Visitor Location Register

Ø4

SMSC

SMS Center

Ø5

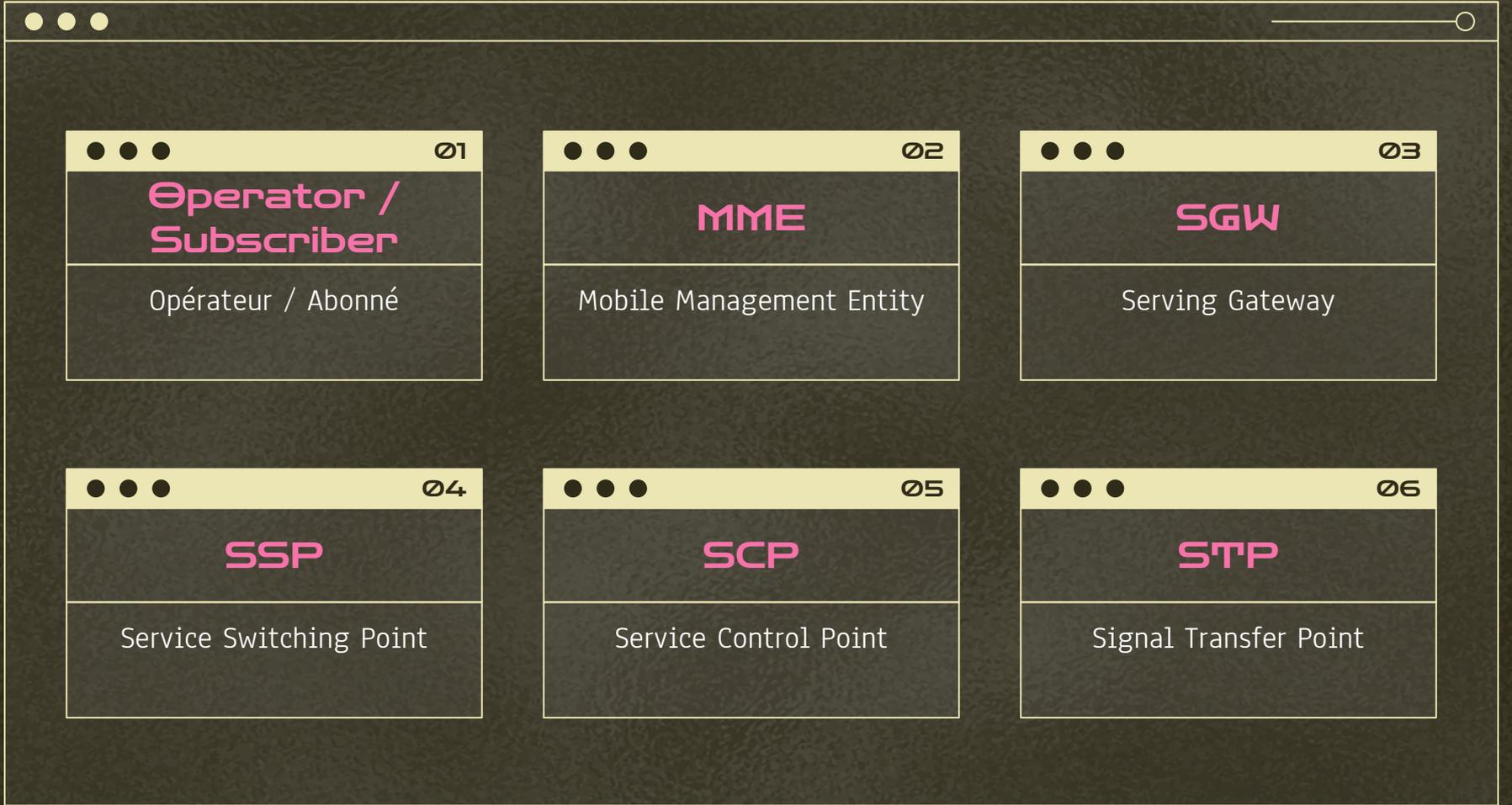
IMSI / TMSI

International Mobile Subscriber
Identity / Temporary

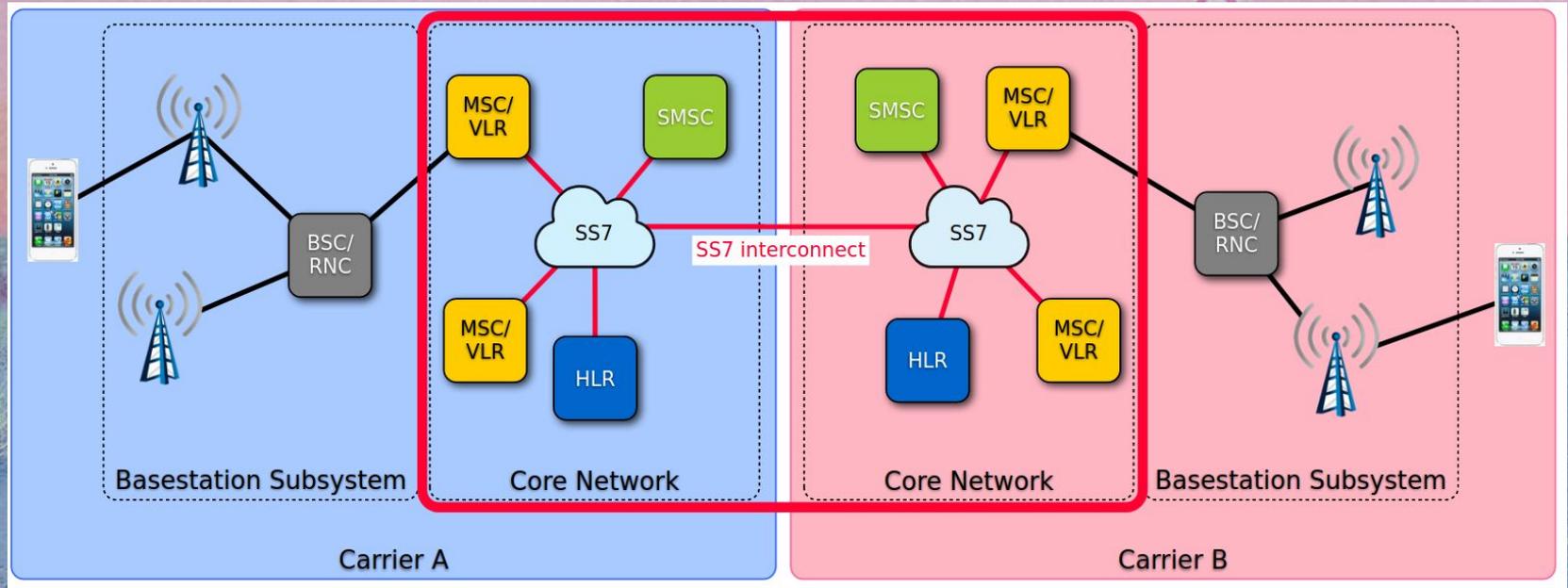
Ø6

MSISDN

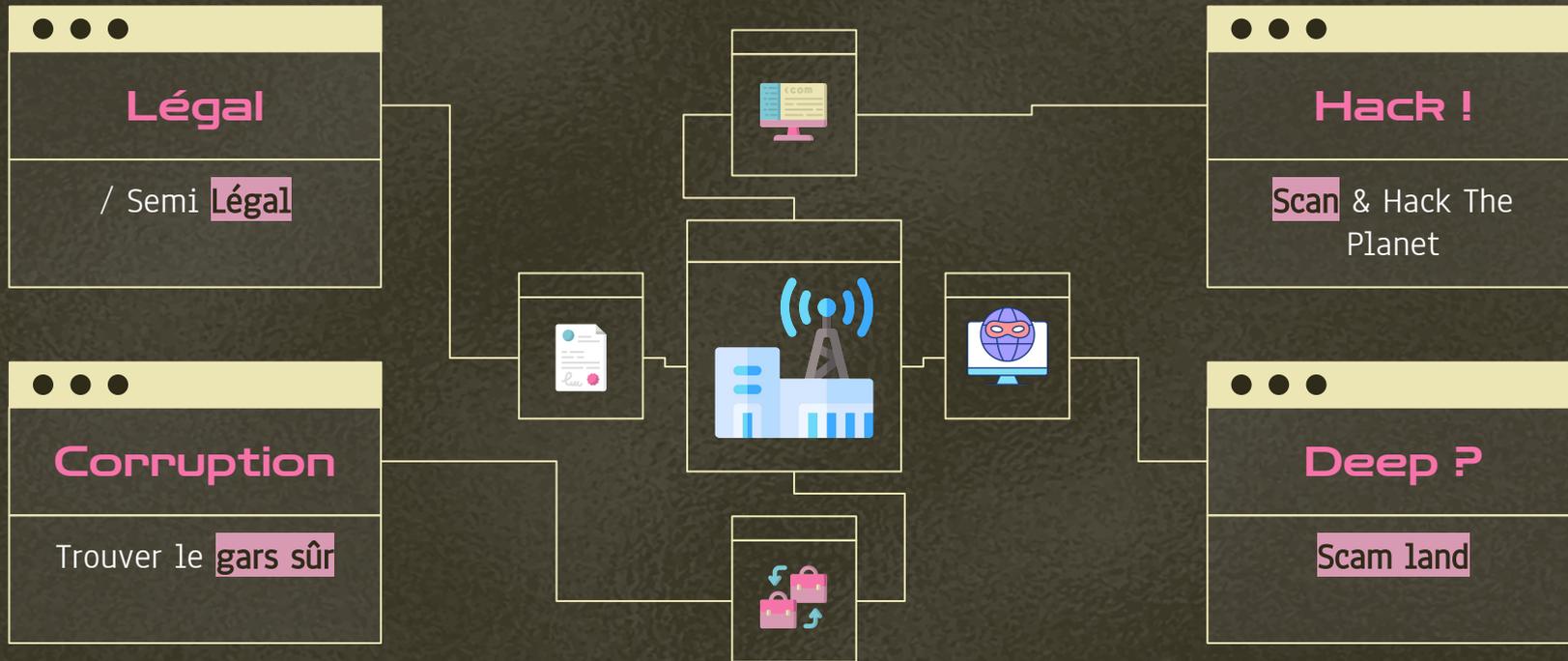
Mobile Station International
Subscriber Directory Number

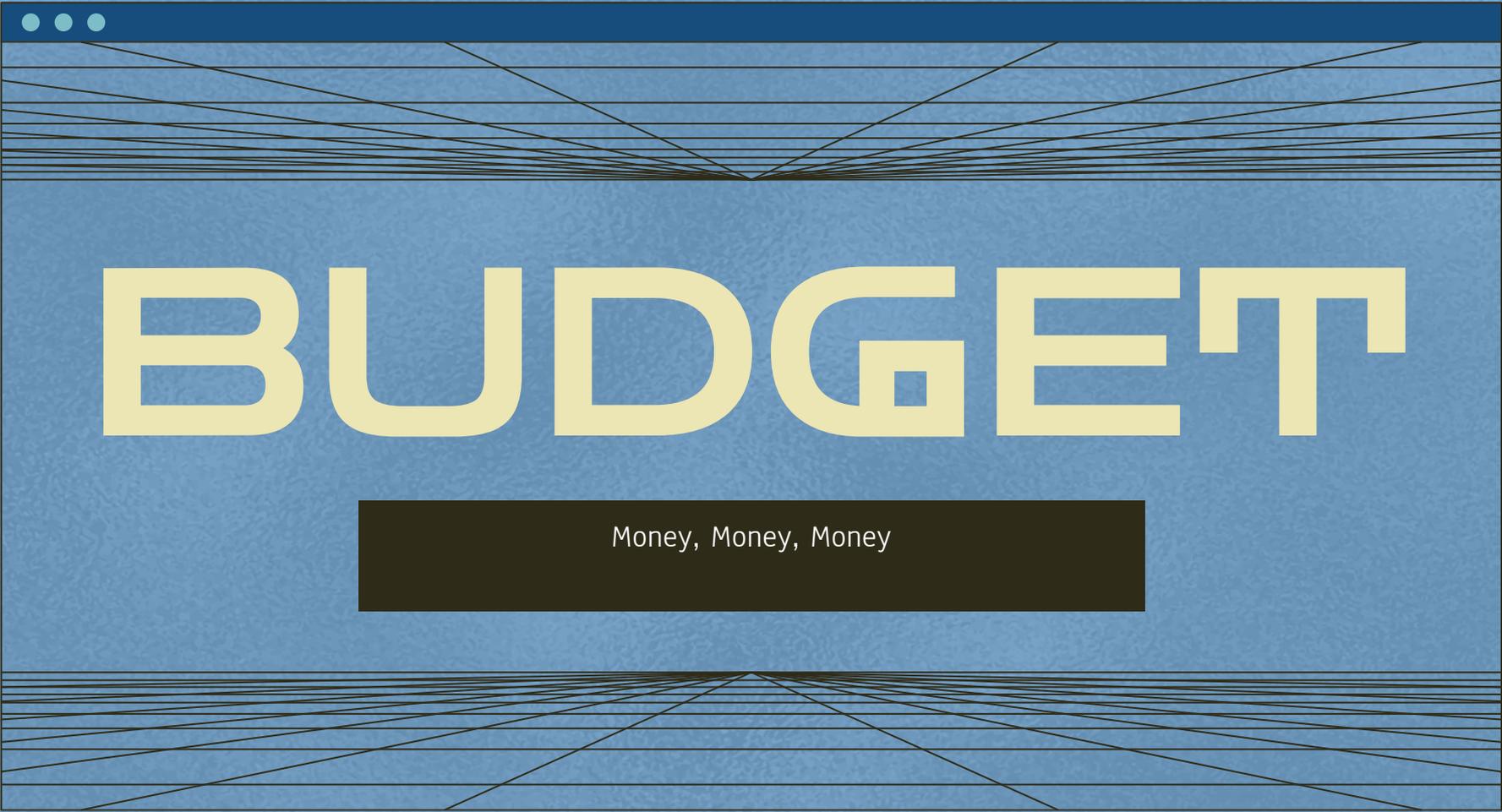


Architecture Overview



Les points d'entrée





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 \$

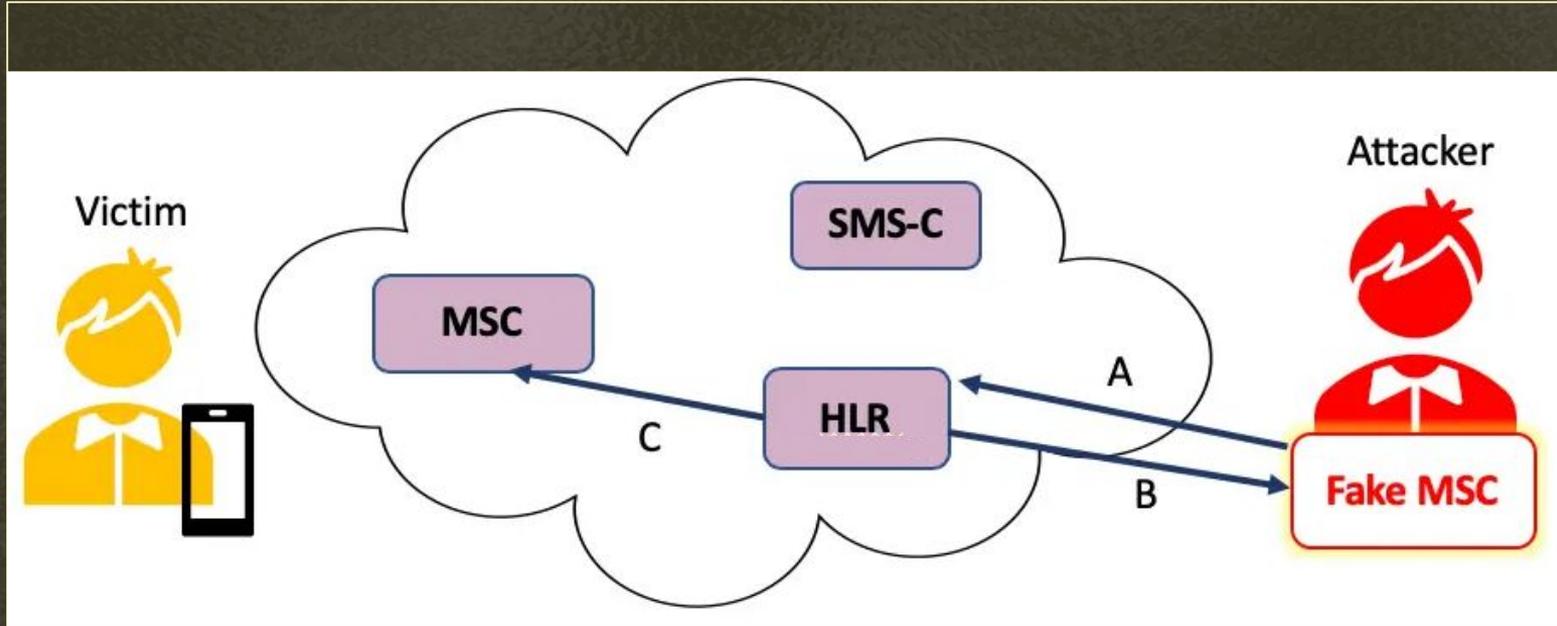
Prix total : 523 \$



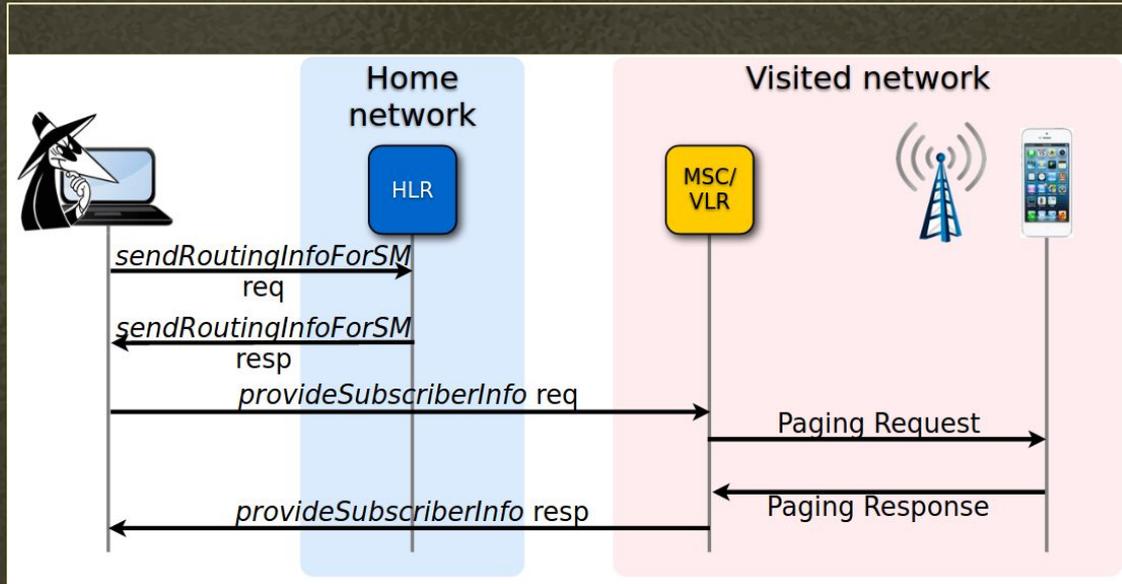
Types d'attaques



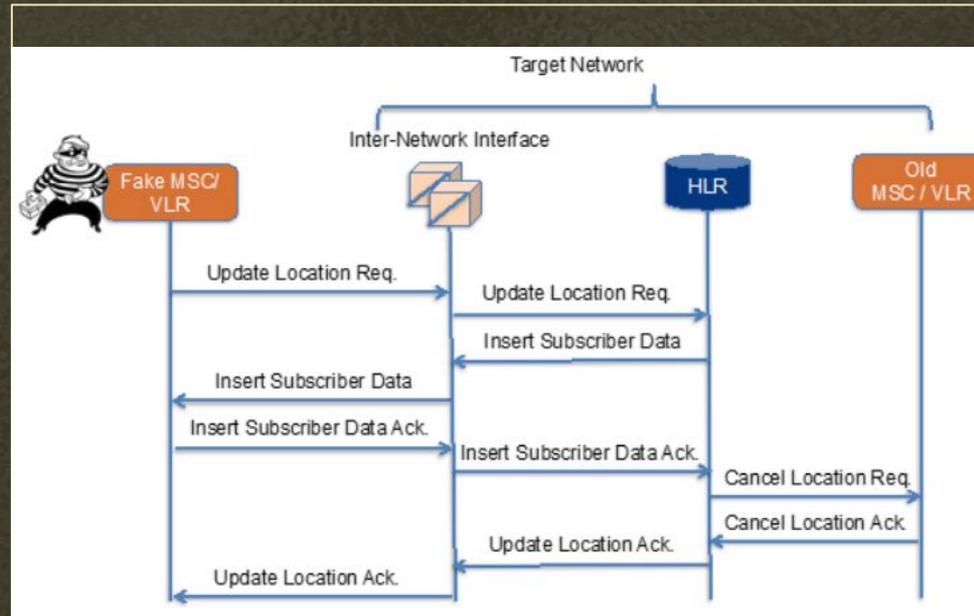
Step 0 : Avoir l'IMSI et le VLR



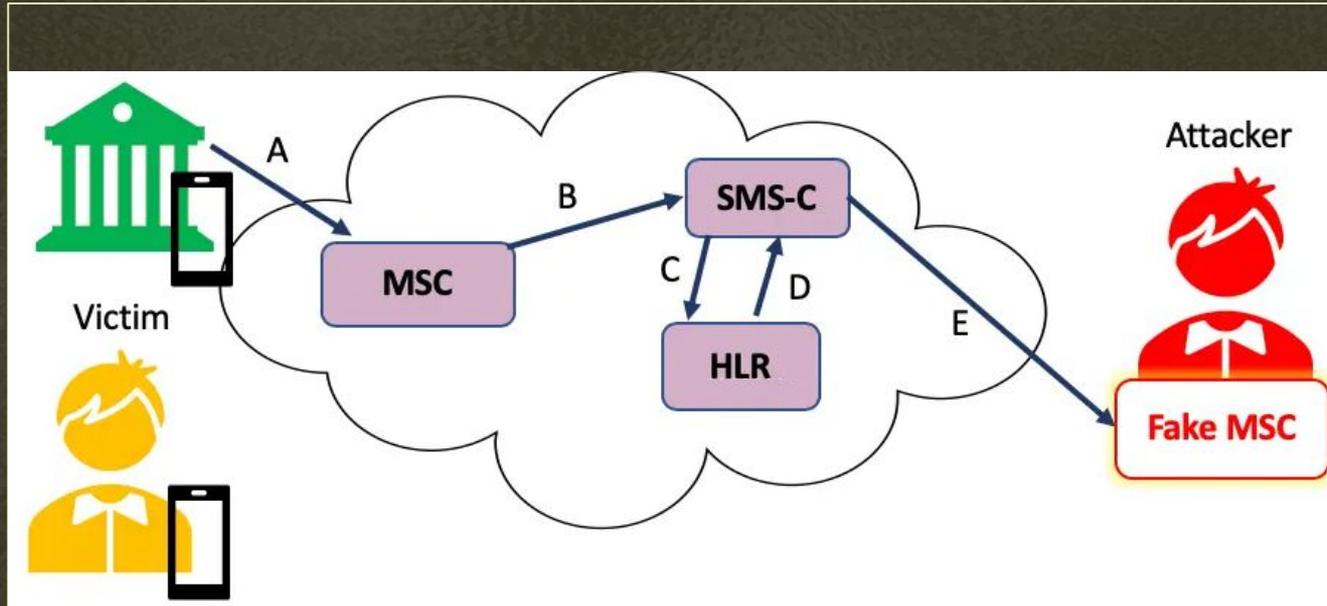
Avoir la localisation



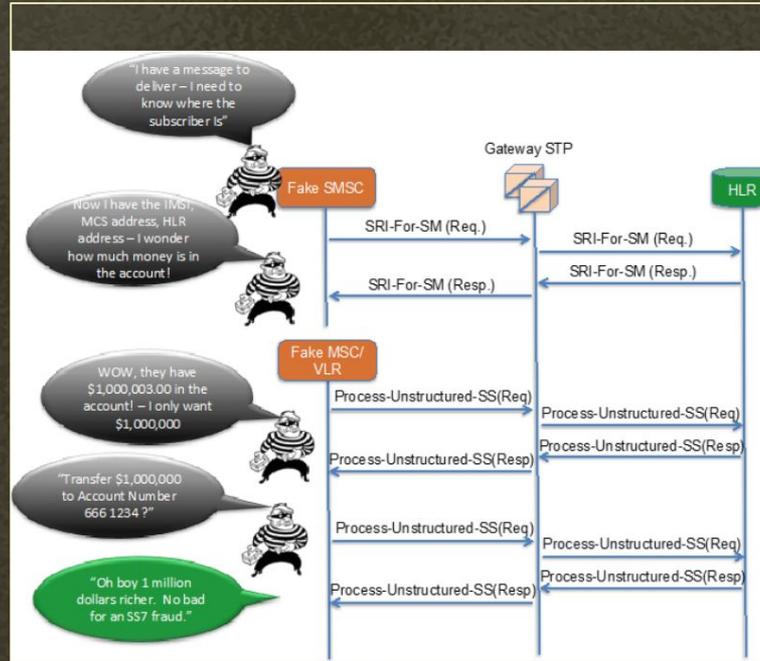
Denial of Service



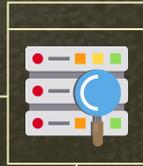
SMS / Call Interception



Manipulation requête USSD



Les outils : pour aller plus loin



SigPloit

Signaling Pentest
Framework

GTSscan

Nmap scanner for
Telco

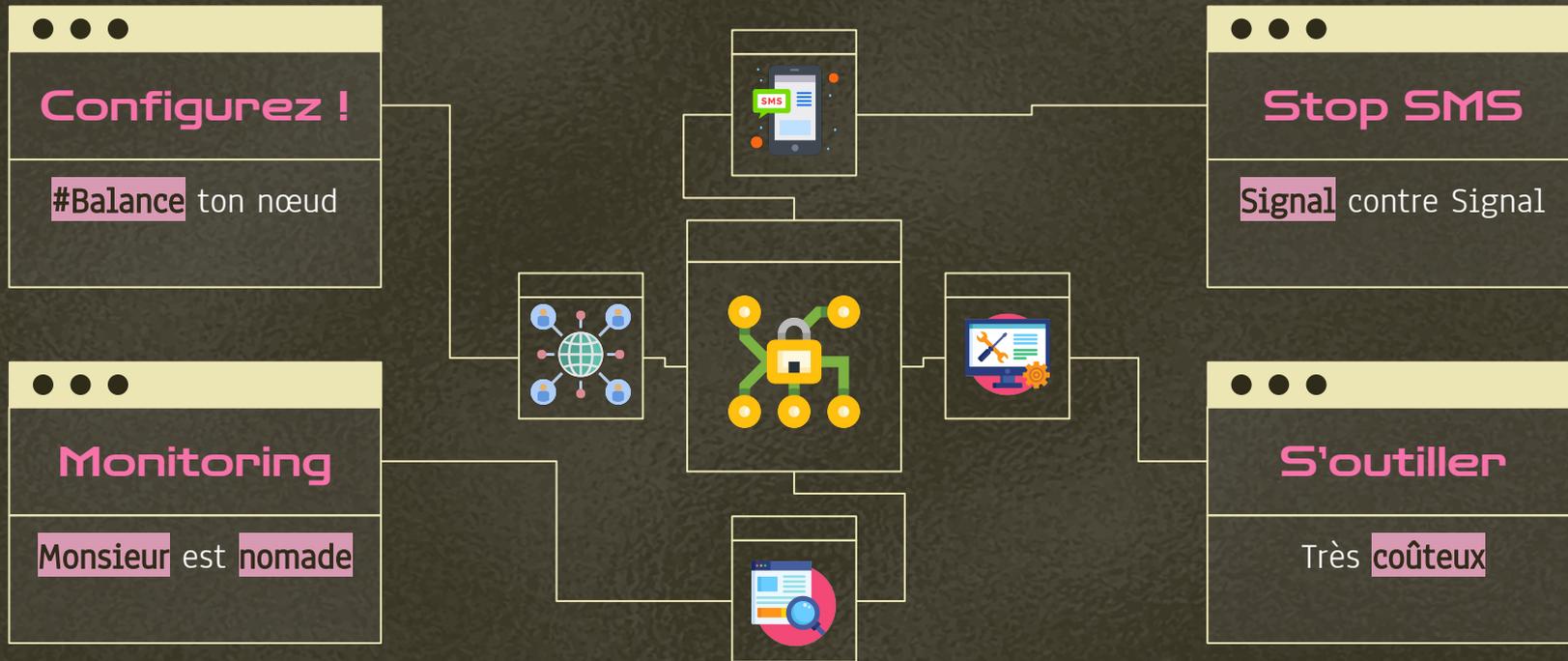
JSS7

SS7 stack emulated in
Java

Osmocomm

Open-source Mobile
Communications

Les défenses et recommandations



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



Place au TP

boringthegod@tutanota.com
pierreceberio.com



 @pireshat

 @lespireshat

 piresh.at



Les Pires Hat

NOS SUPPORTERS

