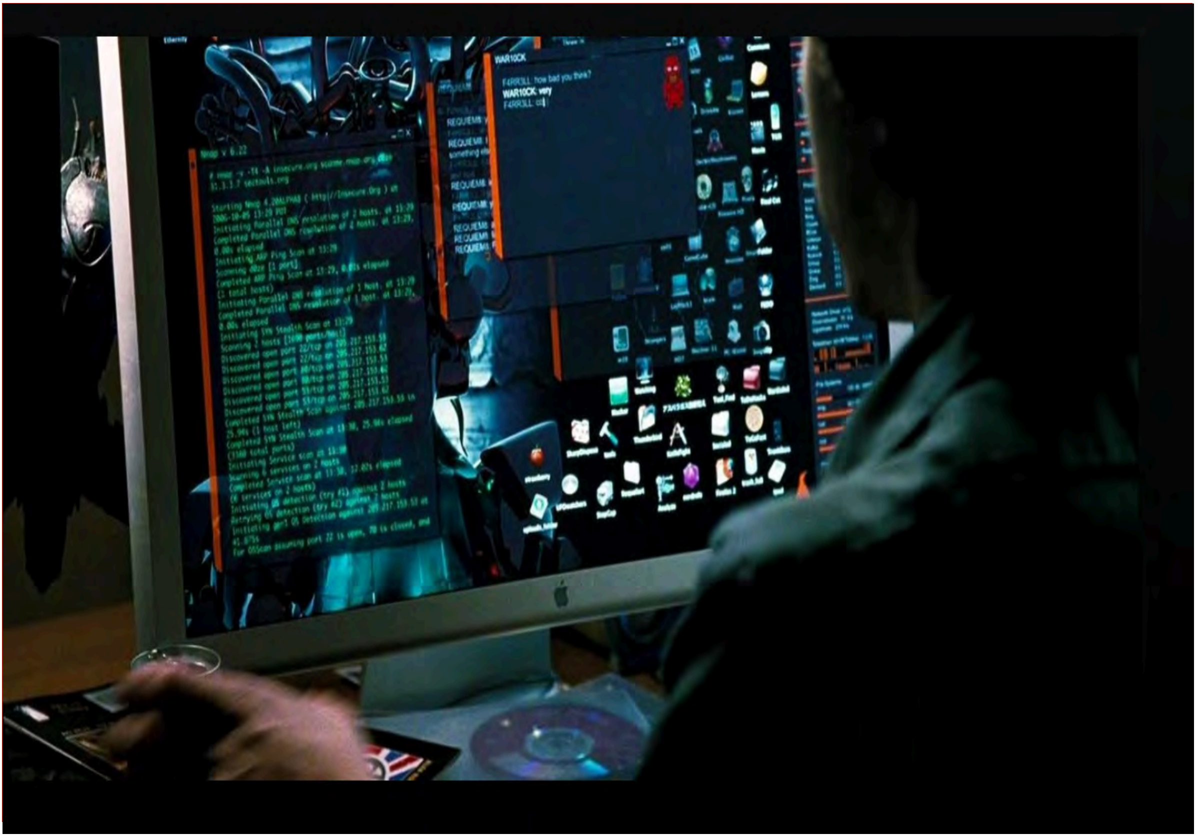
kpn

DEF CON 23 LAS VEGAS



Why Nation-State Malwares Target Telco Networks:

Dissecting Technical Capabilities of Regin and Its Counterparts

Author: Ömer Coşkun

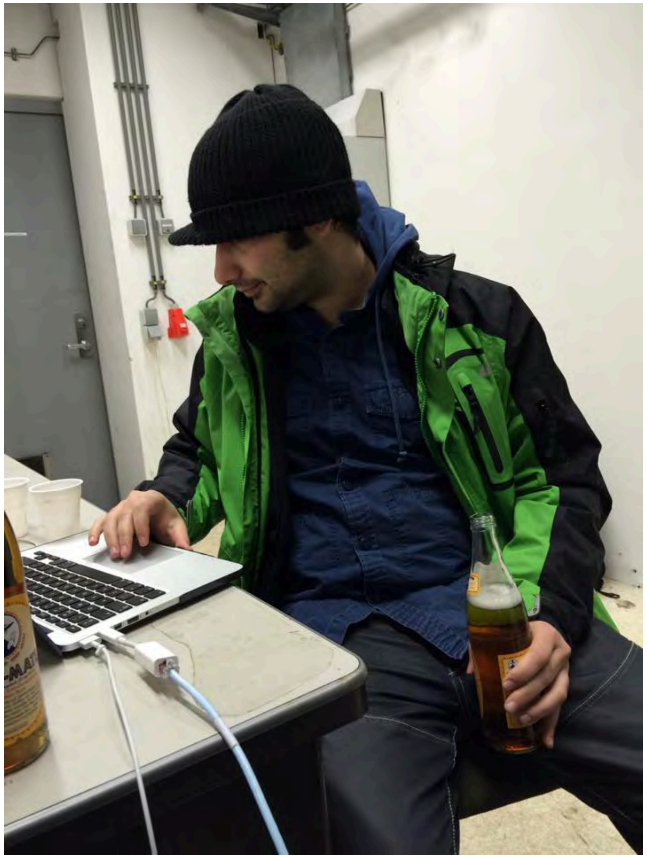
The supreme art of war is to subdue the enemy without fighting*. Sun Tzu*

Outline

1

- Overview
  - Telecom Network Architecture
  - Practical Attack Scenarios
    - SS7 Attack Vectors
    - GRX Attack Vectors
- Rootkit Attacks: Regin and it's counterparts
  - Common Rootkit Techniques and Regin
  - Regin vs. Uruborus and Duqu
  - ***Demo: PoC || GTFO***
- Questions ?

$ whoami



Ömer Coşkun (@0xM3R)

- BEng. Computer Science

  Research Assistant in Quantum Cryptography & Advanced Topics in AI

- Industry Experience

  KPN – CISO , Ethical Hacking

  Verizon – Threat & Vulnerability Management

  IBM ISS – Threat Intelligence

- Interests

  Algorithm Design, Programming, Cryptography, Reverse Engineering, Malware Analysis, OS Internals, Rootkits

kpn

$ REDteam

3

kpn

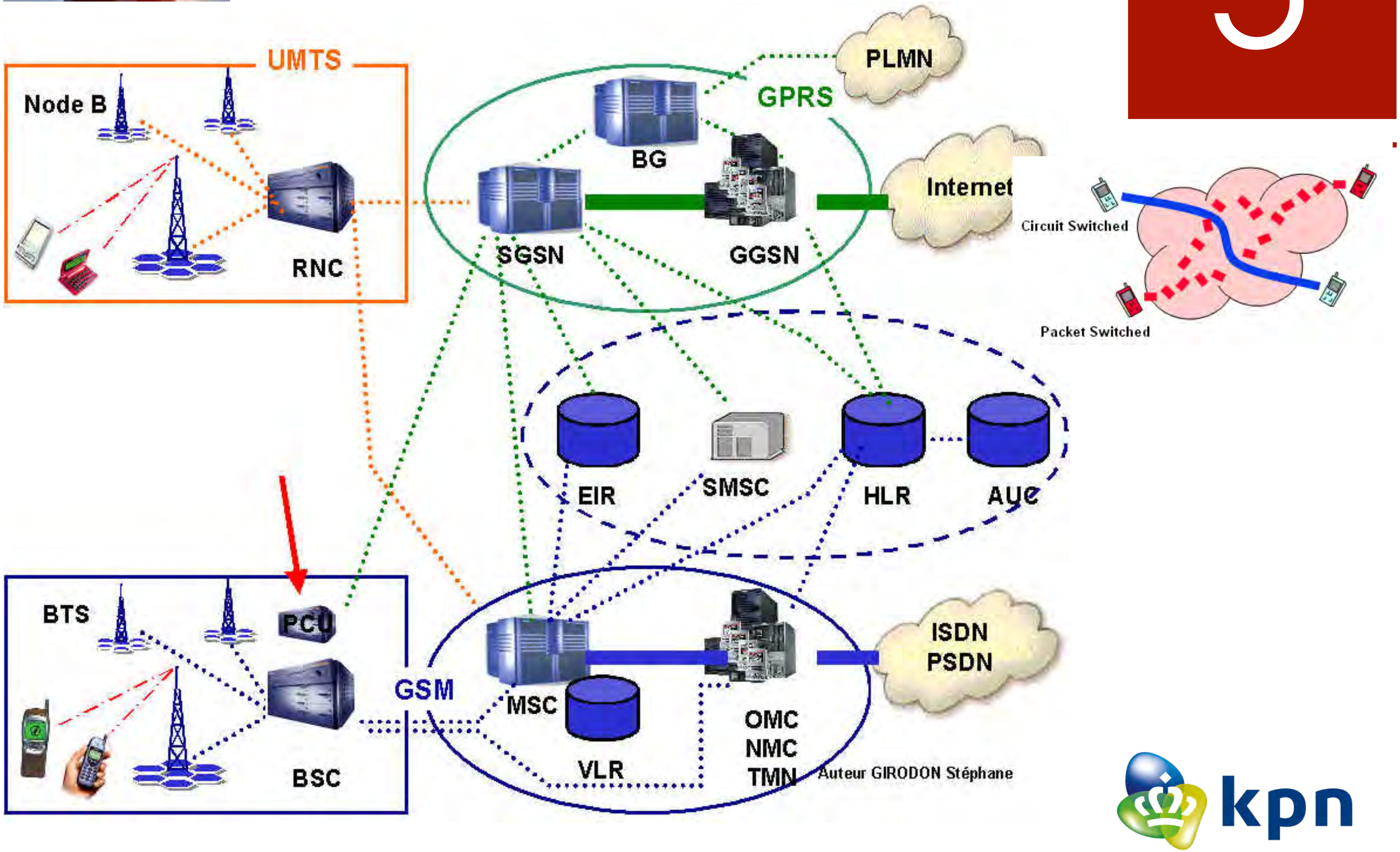
Motivations

4

- Analyze existing vulnerabilities and attack surface of GSM networks
- Governments hack their own citizens
- Surveillance implants shifted focus to telecom networks and network devices
- European Telco companies are really paranoid after Regin attack
- Rootkits are fun : a lot to learn & challenge
- Reproduce the attack scenario and implement it!

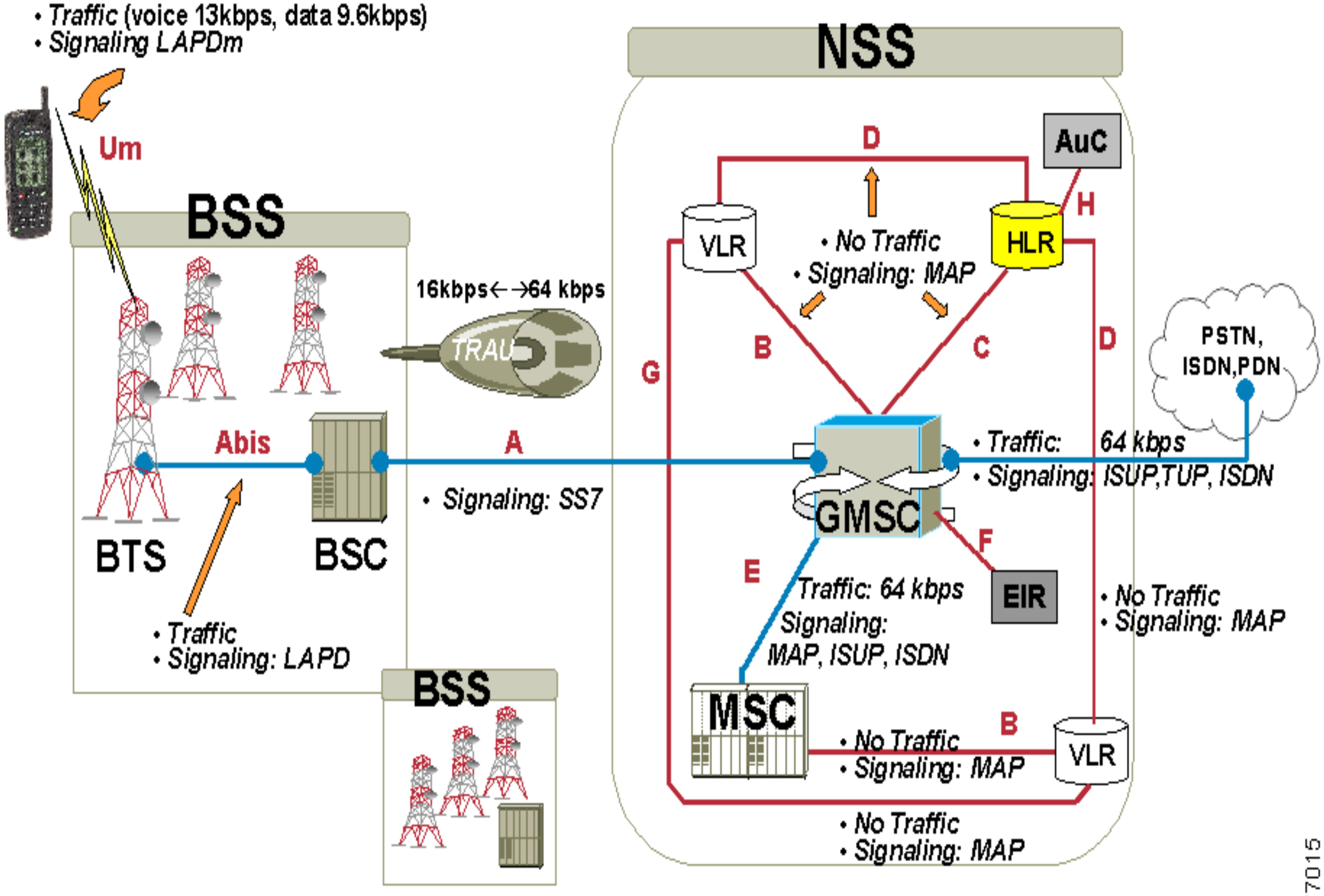
GSM Network Architecture

5



kpn

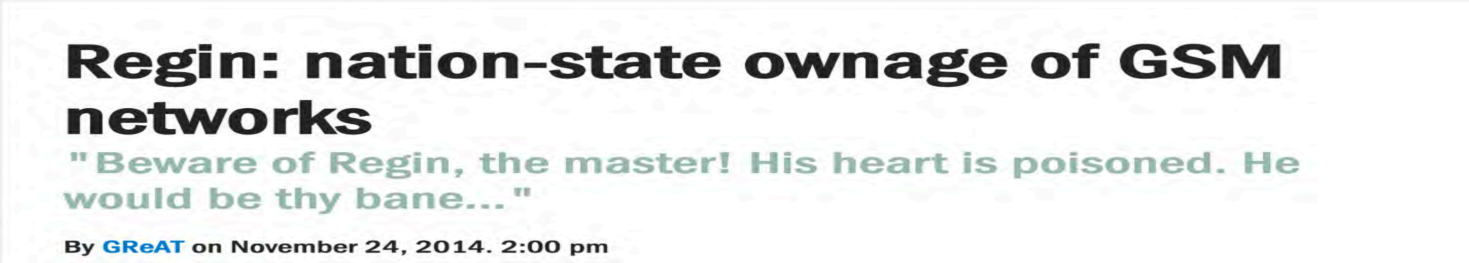
GSM Network Architecture



77015

Regin targets GSM Networks

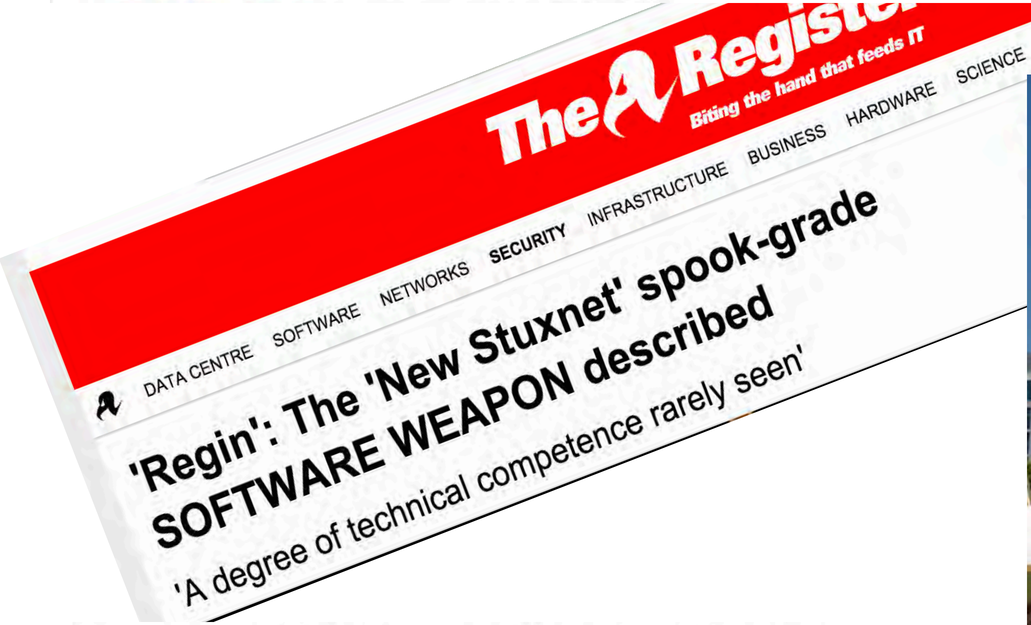
7



Regin: nation-state ownage of GSM networks

"Beware of Regin, the master! His heart is poisoned. He would be thy bane..."

By GReAT on November 24, 2014. 2:00 pm



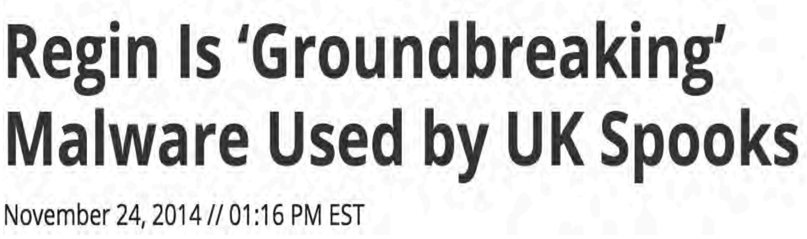
The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE BOOTNOTES

'Regin': The 'New Stuxnet' spook-grade SOFTWARE WEAPON described

'A degree of technical competence rarely seen'

Anti-surveillance rally. Berlin, J



Regin Is 'Groundbreaking' Malware Used by UK Spooks

November 24, 2014 // 01:16 PM EST

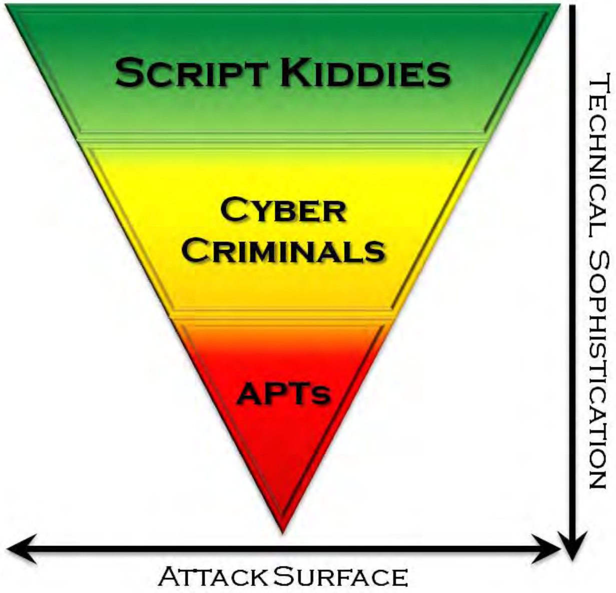
MOTHERBOARD

Written by
JOSEPH COX
CONTRIBUTOR

kpn

Determining Attack Surface

8

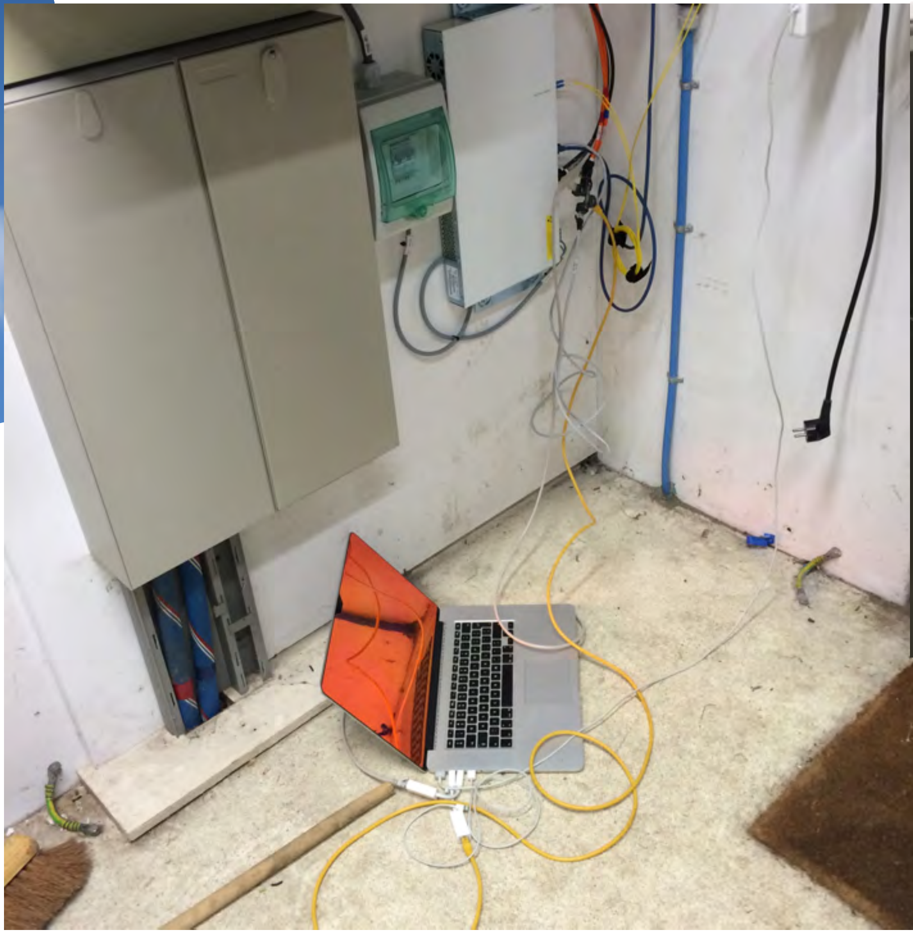


Determining Attack Surface

9

Determining Attack Surface

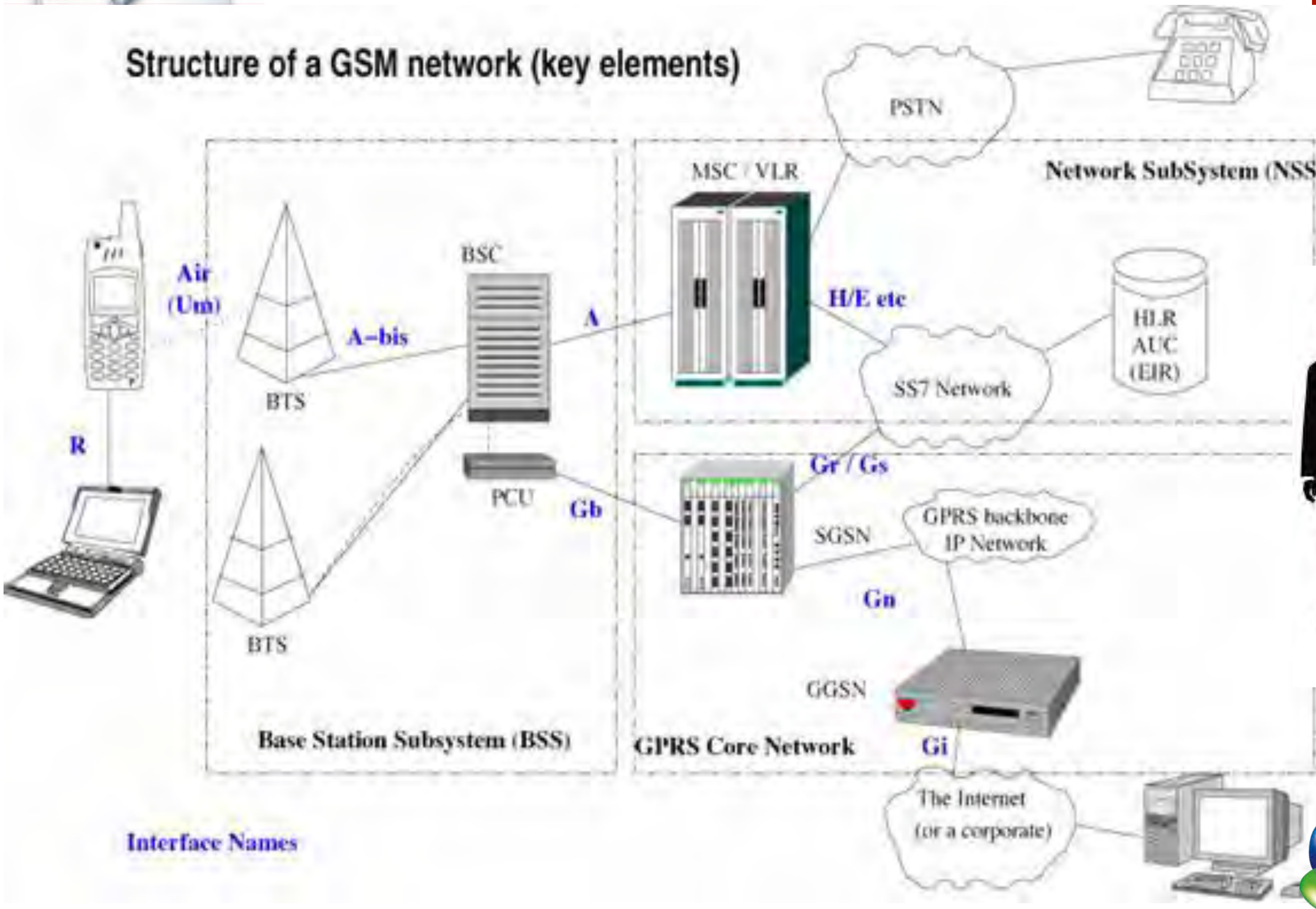
10



Potential Attack Surfaces

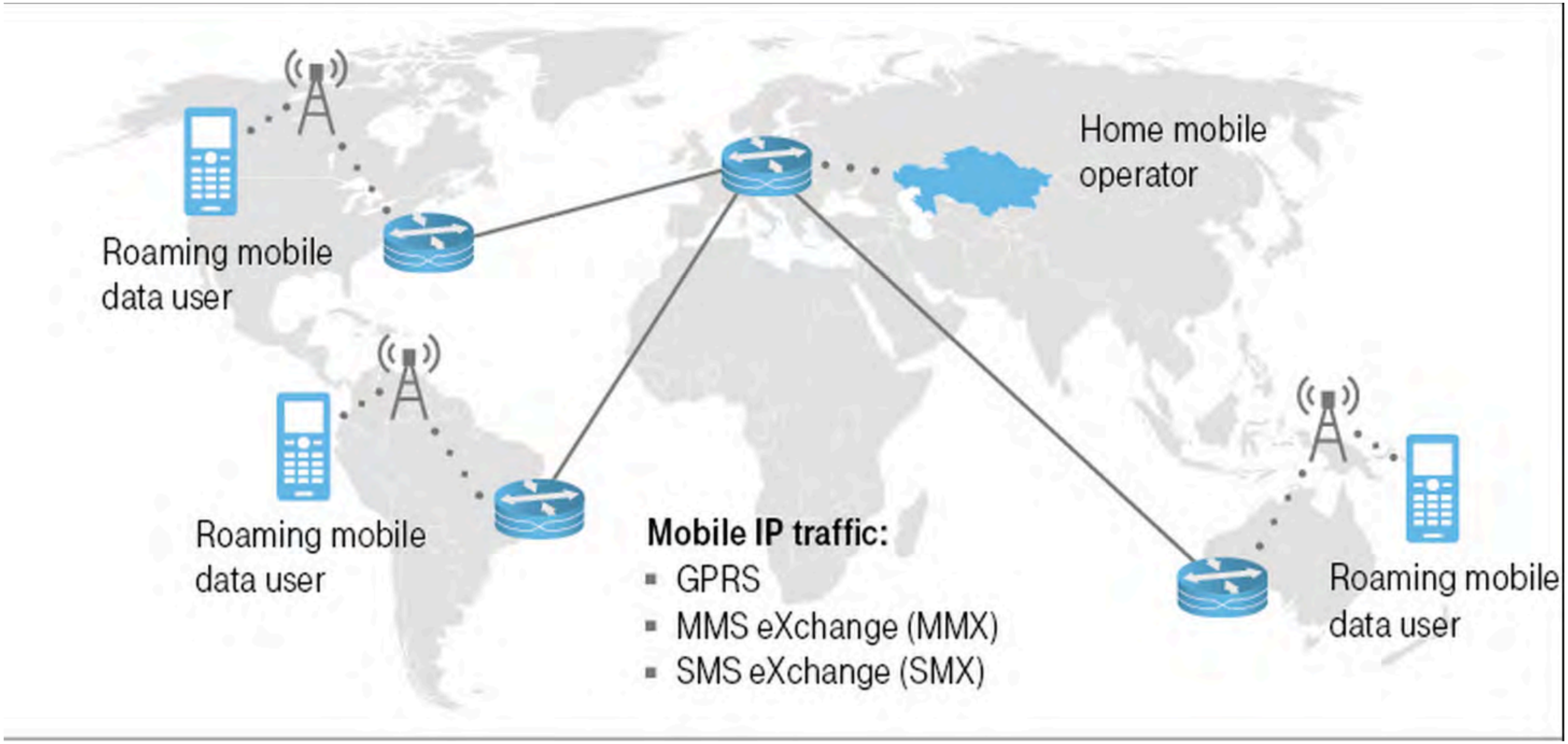
- Absence of physical intrusion detection devices
- Vulnerable services running accessible from BTS
- Absence of tamper resistance and unauthorized access protection
- Improper network segmentation; inner non-routable segments of the Telco company could accessible.
- Core GPRS Network and Network Subsystem (NSS) could be exploitable!

Potential Attack Surfaces



GRX Networks

13



Mobile IP traffic:

- GPRS
- MMS eXchange (MMX)
- SMS eXchange (SMX)

GRX Networks

- GPRS roaming exchange, interconnecting networks.
- Your local GSM provider abroad
- Trust-based, highly interconnected network, made for internet sharing
- A failure or malicious activity would affect multiple connected machines
- Multiple attacks vectors, not limited to a particular segment where you are originating from.

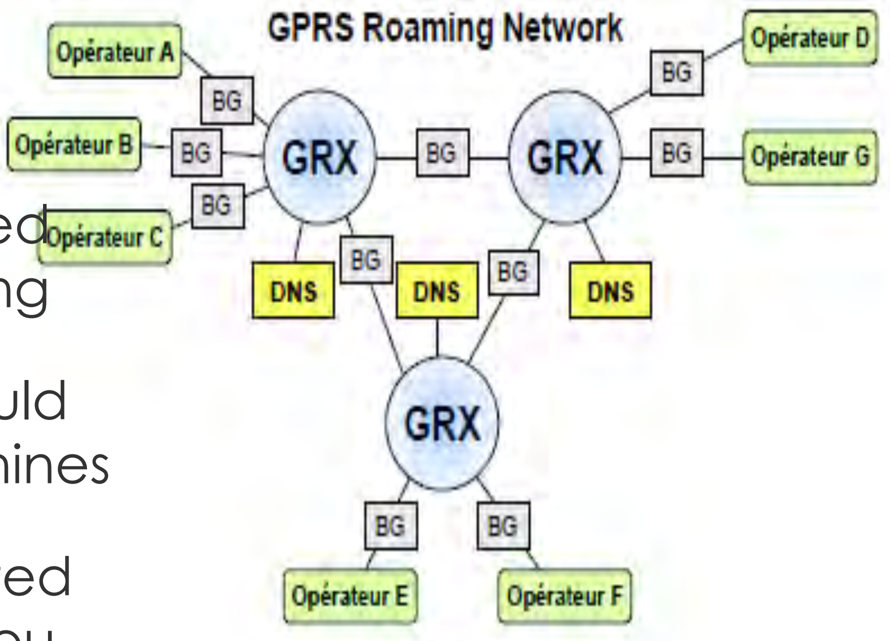
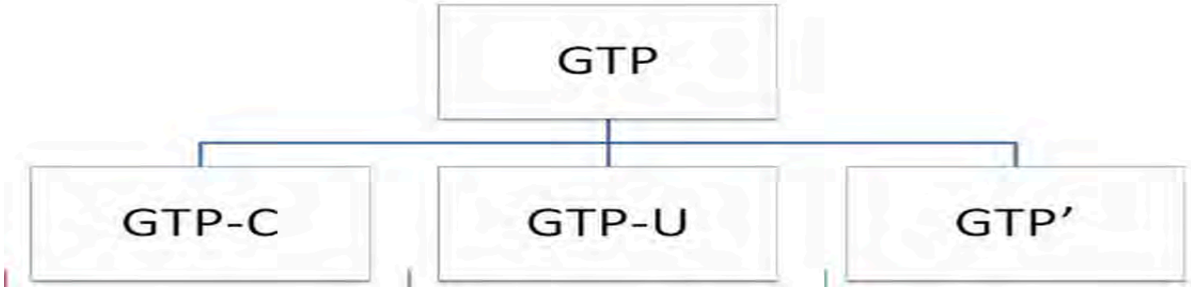
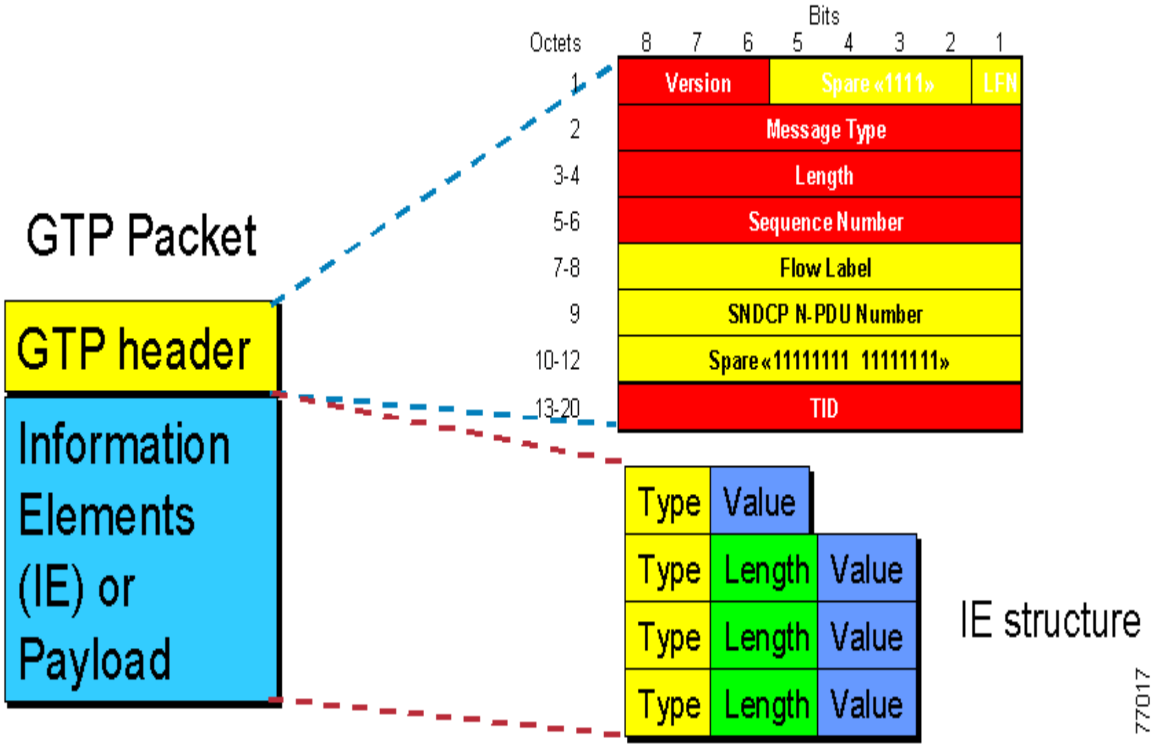


Figure 3 : Réseau GRX

GRX Networks – Attack Vectors

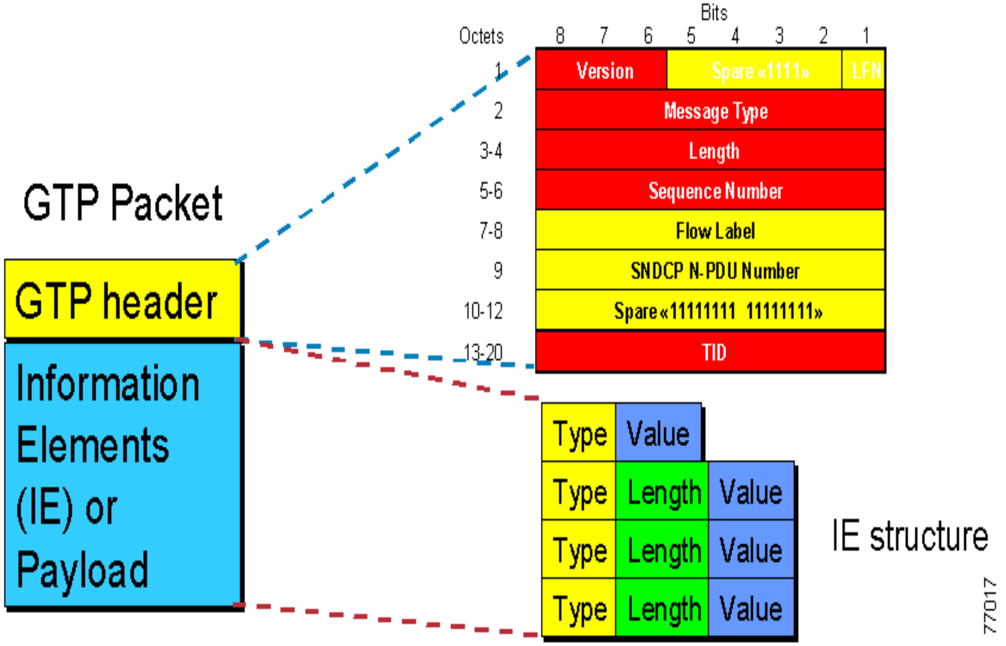




Octets	Bits 8 7 6	5 4 3 2	1
1	Version	Spare «1111»	LFN
2	Message Type		
3-4	Length		
5-6	Sequence Number		
7-8	Flow Label		
9	SNDCP N-PDU Number		
10-12	Spare «11111111 11111111»		
13-20	TID		

GRX Networks – Attack Vectors

- GPRS roaming exchange, interconnecting networks.
- Your local GSM provider abroad
- Trust-based, highly interconnected network, made for internet sharing
- Multiple attacks vectors, not limited to a particular segment where you are originating from.



Octets	Bits 8 7 6	5 4 3 2	1
1	Version	Spare «1111»	LFN
2	Message Type		
3-4	Length		
5-6	Sequence Number		
7-8	Flow Label		
9	SNDCP N-PDU Number		
10-12	Spare «11111111 11111111»		
13-20	TID		

Type	Value	
Type	Length	Value
Type	Length	Value
Type	Length	Value

Demo

Questions ?

Thank you very much for your attention