

HITB 首次走进中国

# Telecoms: Generational Evolution of Attack Surfaces

HITB Beijing 2018





# Black Hat Briefings

HONG KONG APRIL 23 & 24  
SINGAPORE APRIL 26 & 27

## Black Hat Asia 2001

there are no audio or video files available for this conference

Track/Speaker/Topic	Presentation	Notes/Tools
<b>Keynote Presentation - Black Hat Asia 2001</b>		
<b>Martin Khoo</b> Post Mortem of a Rootkit Attack		
<b>Bruce Schneier</b> The Three Truths of Computer Security		
<b>Deep Knowledge Track - Black Hat Asia 2001</b>		
<b>Ofir Arkin</b> ICMP Usage In Scanning (The Advanced Methods)		
<b>Halvar Flake</b> Finding Holes iIn Closed-source Software (With IDA)		
<b>Rain Forest Puppy</b> Web Assessment Tools		
<b>Trust Factory</b> Falling Dominos		
<b>Fyodor Yarochkin &amp; ISS R&amp;D</b> Non-common Architectures Buffer Overflows		hpux tools
<b>General Track - Black Hat Asia 2001</b>		
<b>Shaun Clowes</b> Breaking In Through The Front Door		
<b>Emmanuel Gadaix</b> Overall Security Review of the GSM Infrastructure		
<b>JD Glaser &amp; Saumil Udayan Shah</b> Web Hacking		

# Agenda

- Brief history of telecoms
- Generation Zero
- Generation Fixed
- Generation Analog
- Mobile 1G
- Mobile 2G
- Mobile 2.5G
- Mobile 3G
- Mobile 4G
- Mobile 5G

# Telecom History

1876

1844  
Telegram

## 1800 BC Smoke Signals

150 BC

## The Greek Way

What  $\hat{h}^a + \hat{h}$   $\mathbb{G} \circ d$   
is  $\hat{h}^a$ ?

# Telecom Historical Milestones

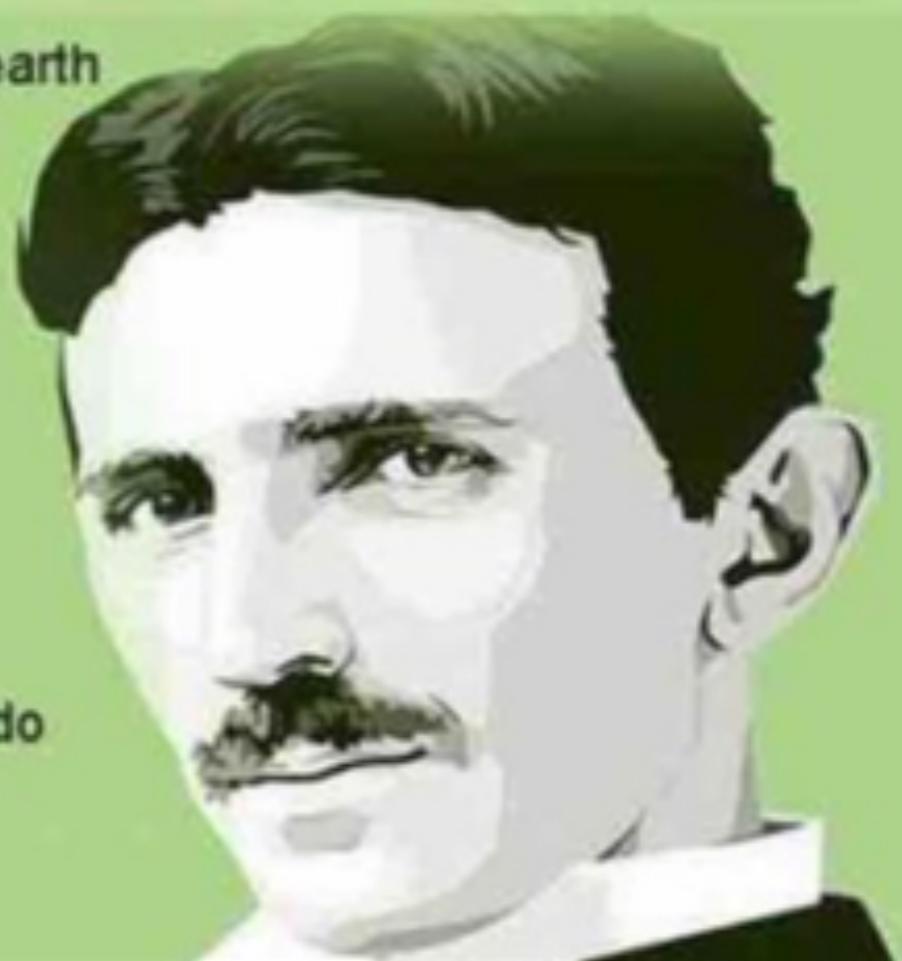
- Semaphore by Chappe brothers 1790
- Telegraph by Morse 1838
- Wireless telegraphy by Tesla 1893
- First radio by Marconi 1896
- Fiber optics invented in the 1920's
- First cell phone used by Swedish police in 1946
- First communications satellites in the 1960's
- First mobile phone 1973 Motorola
- First cellular network 1979 Japan NTT



# Nikola Tesla describing a cell phone back in 1926...

"When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles, and the instruments through which we shall be able to do all of this, will fit in our vest pockets."

Nikola Tesla 1926



# Nikola Tesla (1856-1943)

Can you predict comms tech in year 2100 ?



# Hedy Lamarr (1914-2000)

Actress in the first motion picture to include a nude scene  
and Inventor of Frequency-hopping spread spectrum

# Generation Zero

Basic security problems:

- Lack of authentication
- Difficult to protect against interception
- Messages replay

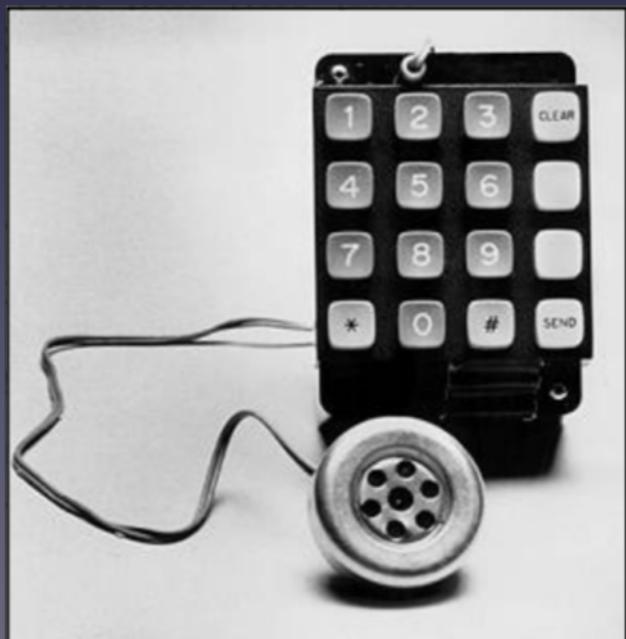


# Generation Fixed



Same basic issues but

- The walled garden paradigm!
- Network perimeter not exposed
- In-band CCITT#5 signalling
- Blue boxing (and red, beige, etc.)
- Fraud issues (subscription, PABX hacking)



# Wardialing Fixed Networks



```
Port Info      : 1200,8,N (/dev/ttyS0) [Random]          CONNECT   : 3
Start/End Scan : 5551000 - 5552000 [1000]           NO CARRIER : 1
Pre/Post Dial  : 919 / [None]                      BUSY      : 4
Log File       : /tmp/iwar.log [N]                  VOICE     : 13
Status         : ATDT9195551873                   TONE/SILENCE: 4
Serial Idle   : 23                                  TIMEOUT   : 5
                                                               Numbers Left: 963

[Terminal Window]
OK
ATM1L3
OK
ATDT9195551378
VOICE
ATDT9195551873
```

GREETINGS PROFESSOR FALKEN  
HELLO  
A STRANGE GAME.  
THE ONLY WINNING MOVE IS  
NOT TO PLAY.  
HOW ABOUT A NICE GAME OF CHESS?

# Generation 1G Analog

Primitive mobile systems suffer from serious flaws.

- First mobile network NMT
- In the US, analog AMPS
- Poor authentication (serial number)
- No OTA encryption
- Phone cloning (fraud)
- Radio frequency eavesdropping



# Analog Phones

- Basic and proprietary firmware
- No data capabilities whatsoever
- Baseband and main CPU not segregated
- No secure enclave
- No integrity mechanisms
- Cannot run custom software
- No roaming



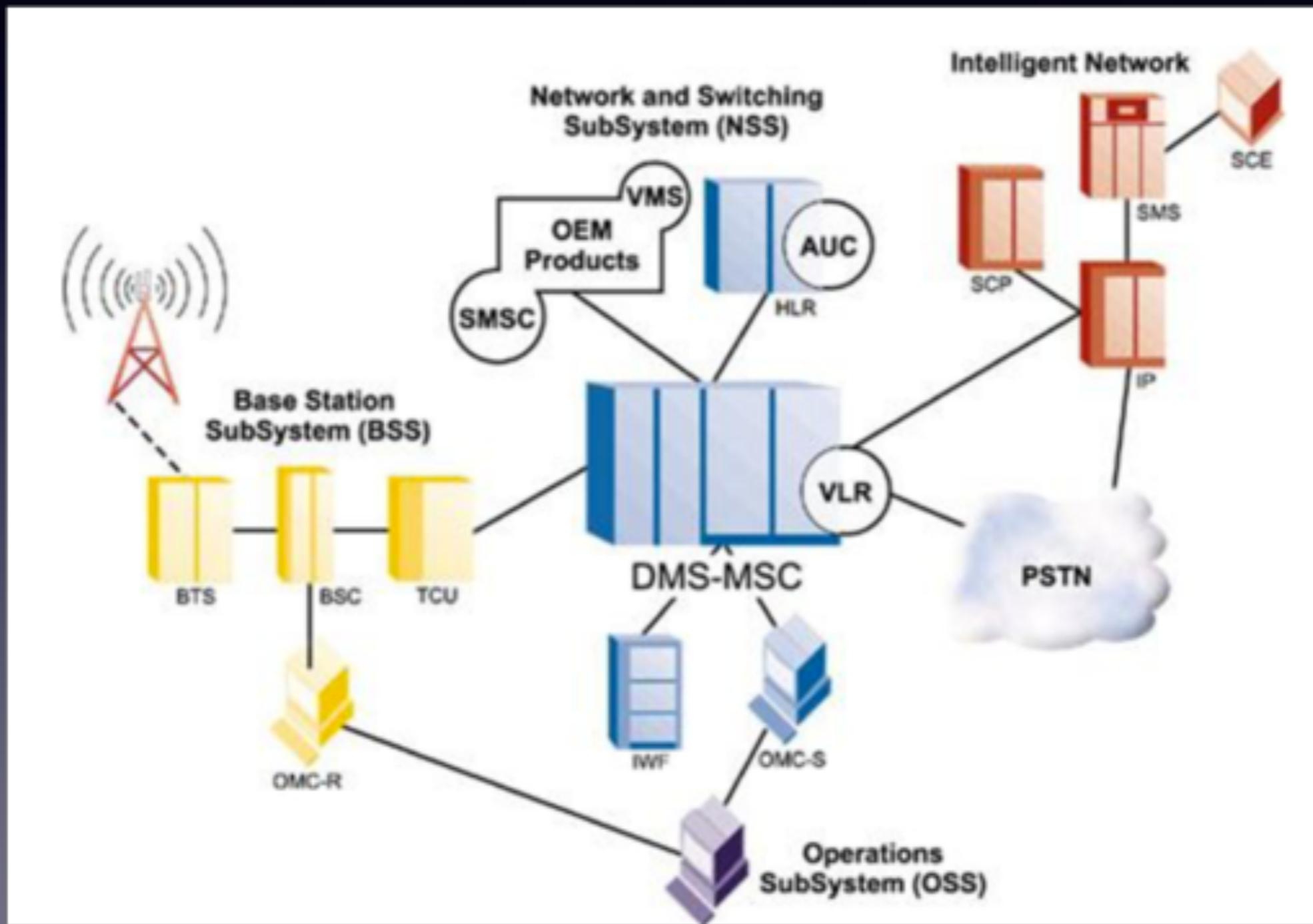
# Mobile 2G

## The GSM revolution

- European consortium “Groupe Spécial Mobile”
- Serious attempt at building a secure network
- OTA encryption with A5/A3 protocols
- Semi-proprietary crypto algorithms (ouch!)
- Authentication through SIM card
- Caller ID functionality
- Out-of-band SS7 signalling
- Explosive growth and worldwide deployment



# Closed GSM network



# GSM Security Golden Years

- From 1989 to 1998, no security issues
- Some academic research into radio protocols
- First cryptanalysis 1998 (COMP128) and 1999 (A5/1 and A5/2)
- First GSM security paper Blackhat Asia 2001
- SIM card security model not broken
- No known compromise of infrastructure
- No signalling abuse, death of phreaking



# GSM Enemies at the Gate

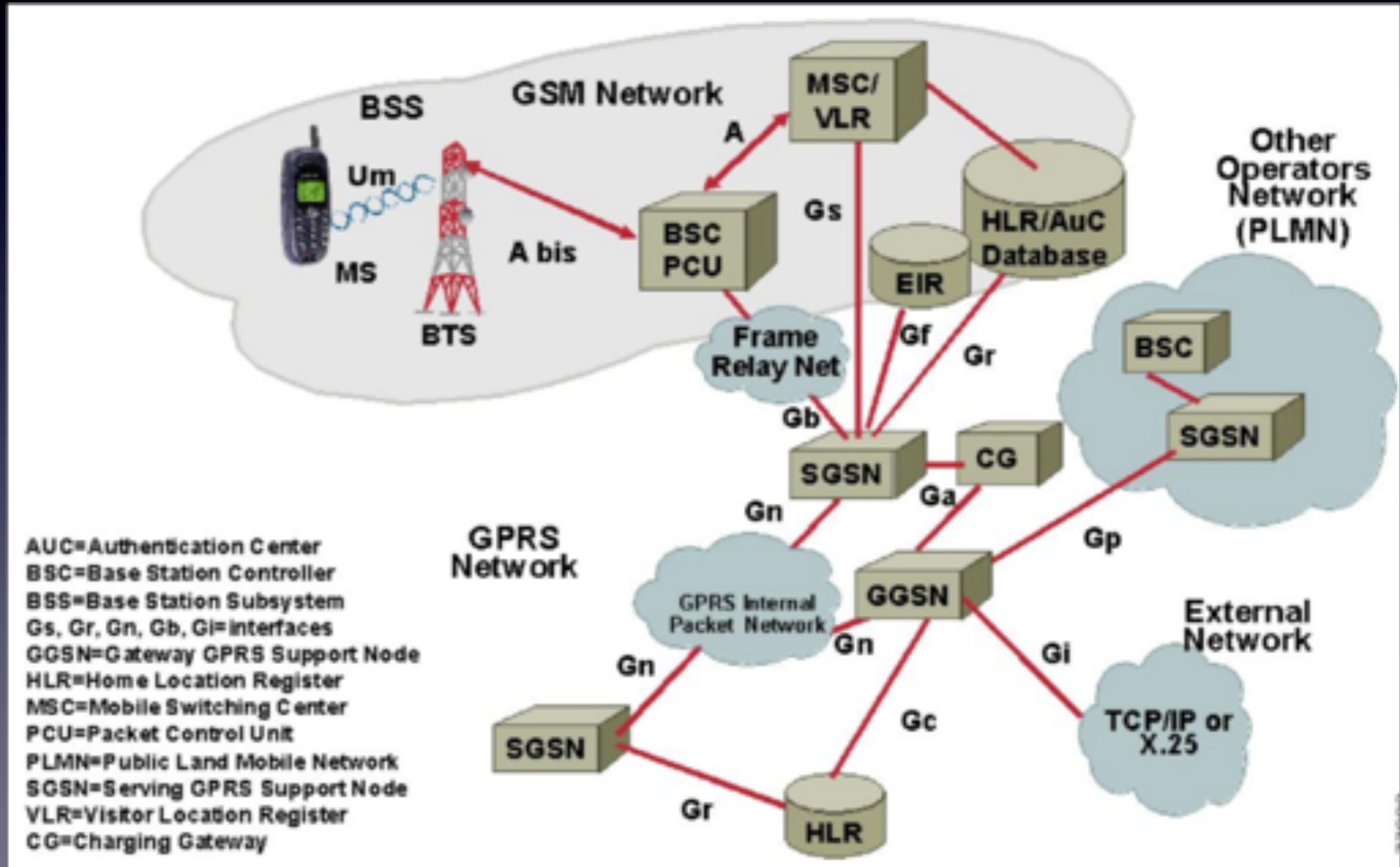


# Cracks in the Wall

- SIM cloning made possible after research by Briceno on the COMP128 algorithm (leaked)
- Cryptography research on A5 algorithms (invented in 1989; some leaks in 1994; reversed by Briceno at Berkeley in 1999; cryptanalysis by Biryukov and Shamir at Weizmann in 1999)
- Hackers groups started researching vulnerabilities in various protocols. Publications by Karsten Nohl and Tobias Engel
- Insider hacking cases starting to mount. Technical fraud by insiders,
- First IMSI catchers for LEA



# Internet at the Gate



# GSM Data – early attempts

A few forgotten technologies:

- Early GSM networks had banks of V.32bis modems
- Dialup-like connections; and Fax too!
- Full interconnection with X.25 networks
- Earliest baud rate 9600 bps
- Complete disconnect between Telcos and Internet

# Early GSM phones

- Proprietary OS (first models from Nokia, Ericsson, Alcatel)
- Data connectivity has low bandwidth, high latency
- Screen real estate not usable for serious data usage
- Web sites and services not compatible with WAP and early data attempt

# Mobile 3G

# 3G landscape

- Data speeds become usable and practical
- Terminals have large screens, better resolution, more resources, can run custom software
- The IP stack becomes used in telcos (not only for GGSN/SGSN but several other Network Elements as well as SIGTRAN signalling)
- Governments increasingly interested in data traffic

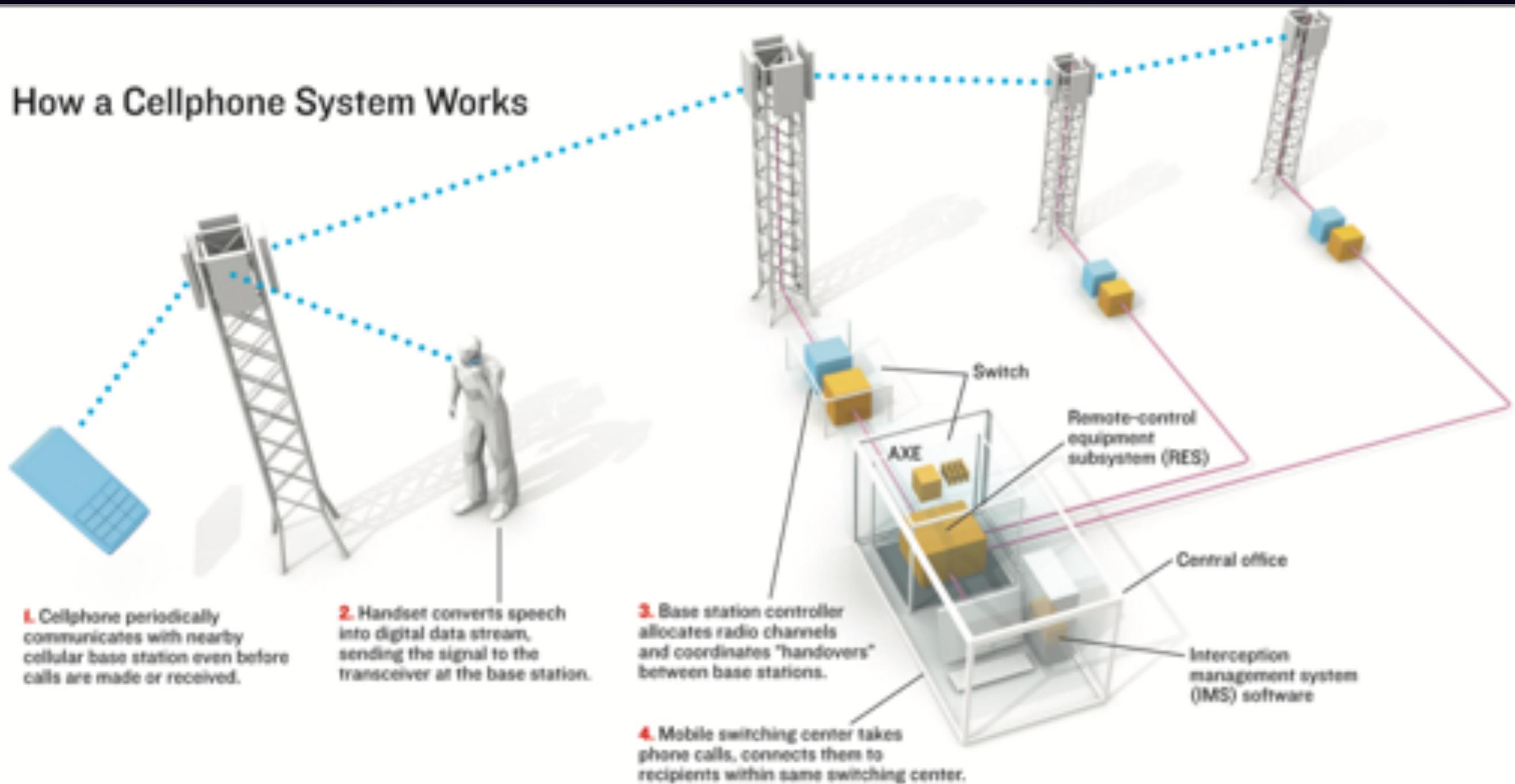
# GSM and Lawful Interception

- LEA and IA always had some form of access to fixed lines and early mobile technologies
- GSM had built-in support from day 1, by defining LIG interfaces and systems
- Real-time, powerful and user-friendly access to all communications, SMS and later on data traffic
- Core Network traffic not encrypted



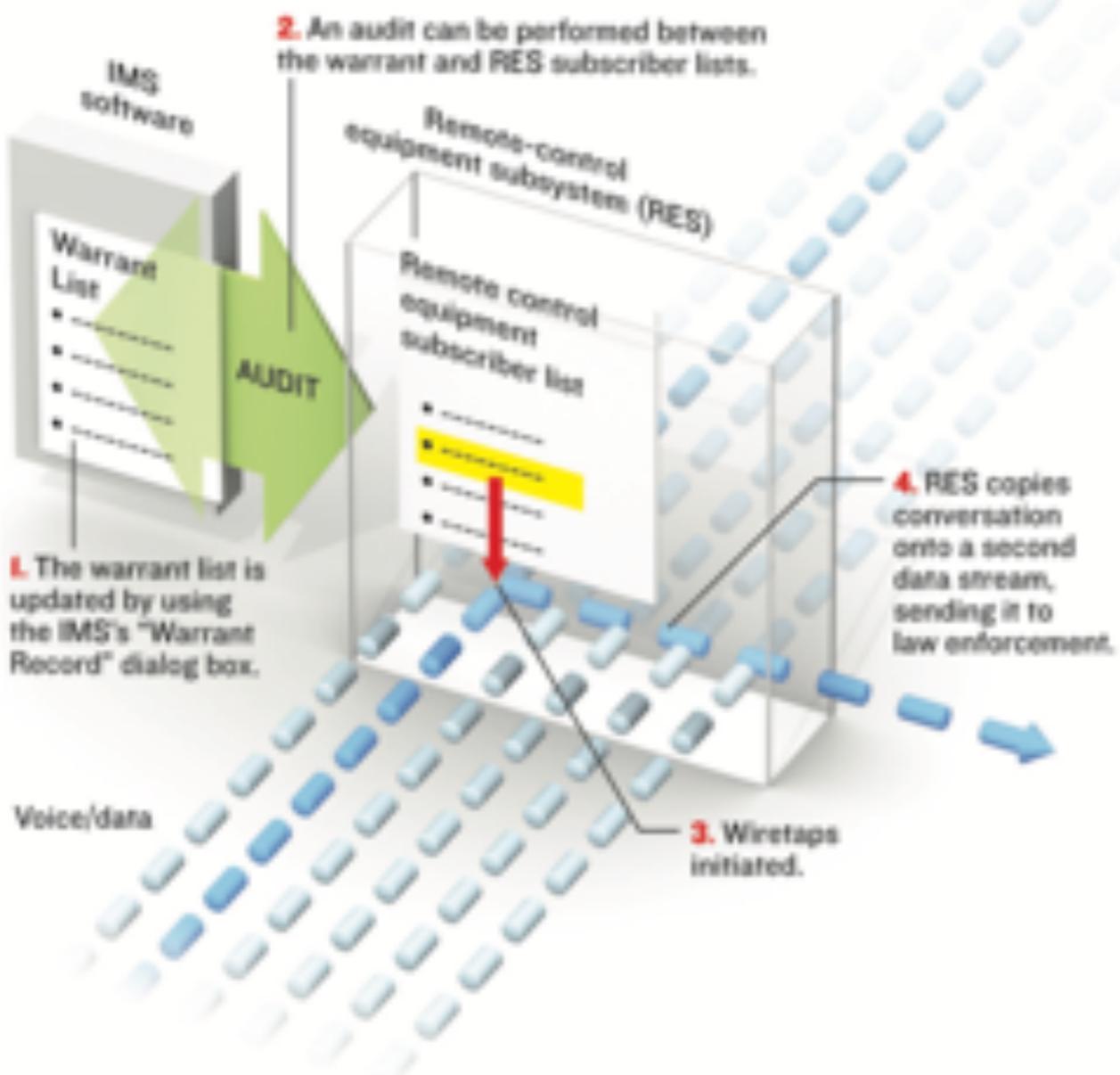
# Nation-State Attacks

## How a Cellphone System Works

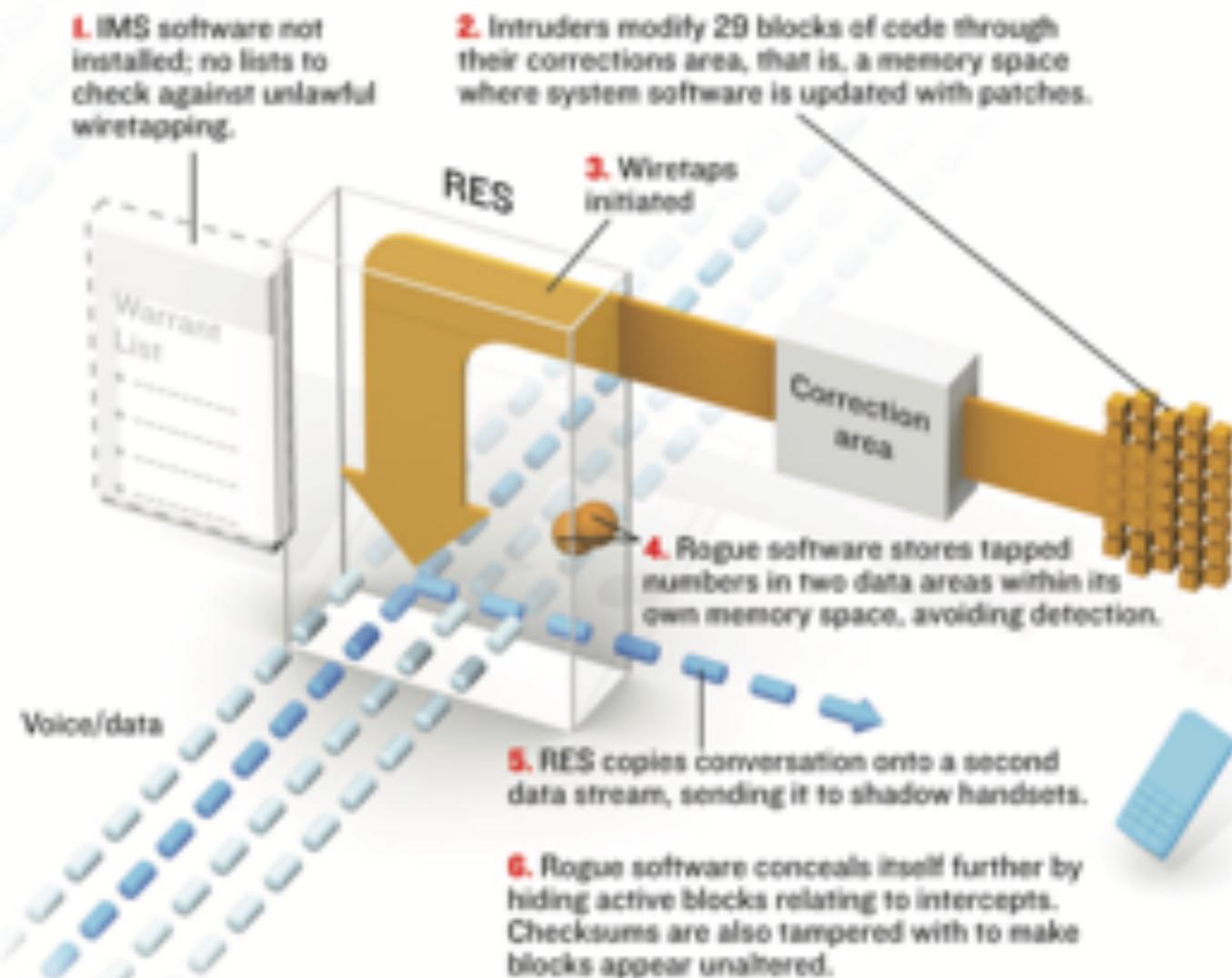


# The Athens Affair

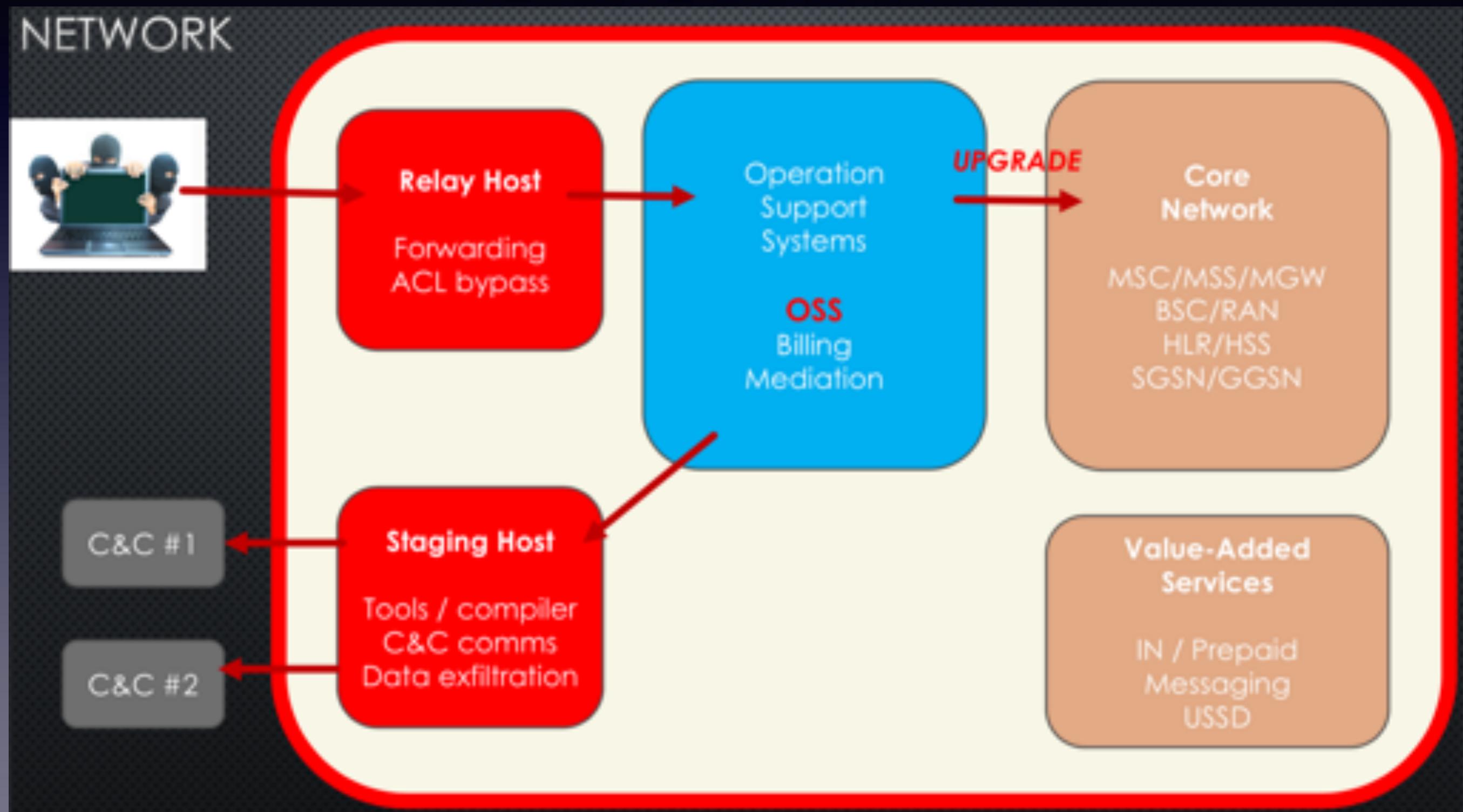
## Typical Ericsson AXE Wiretap System



## How Cellphone System Was Breached

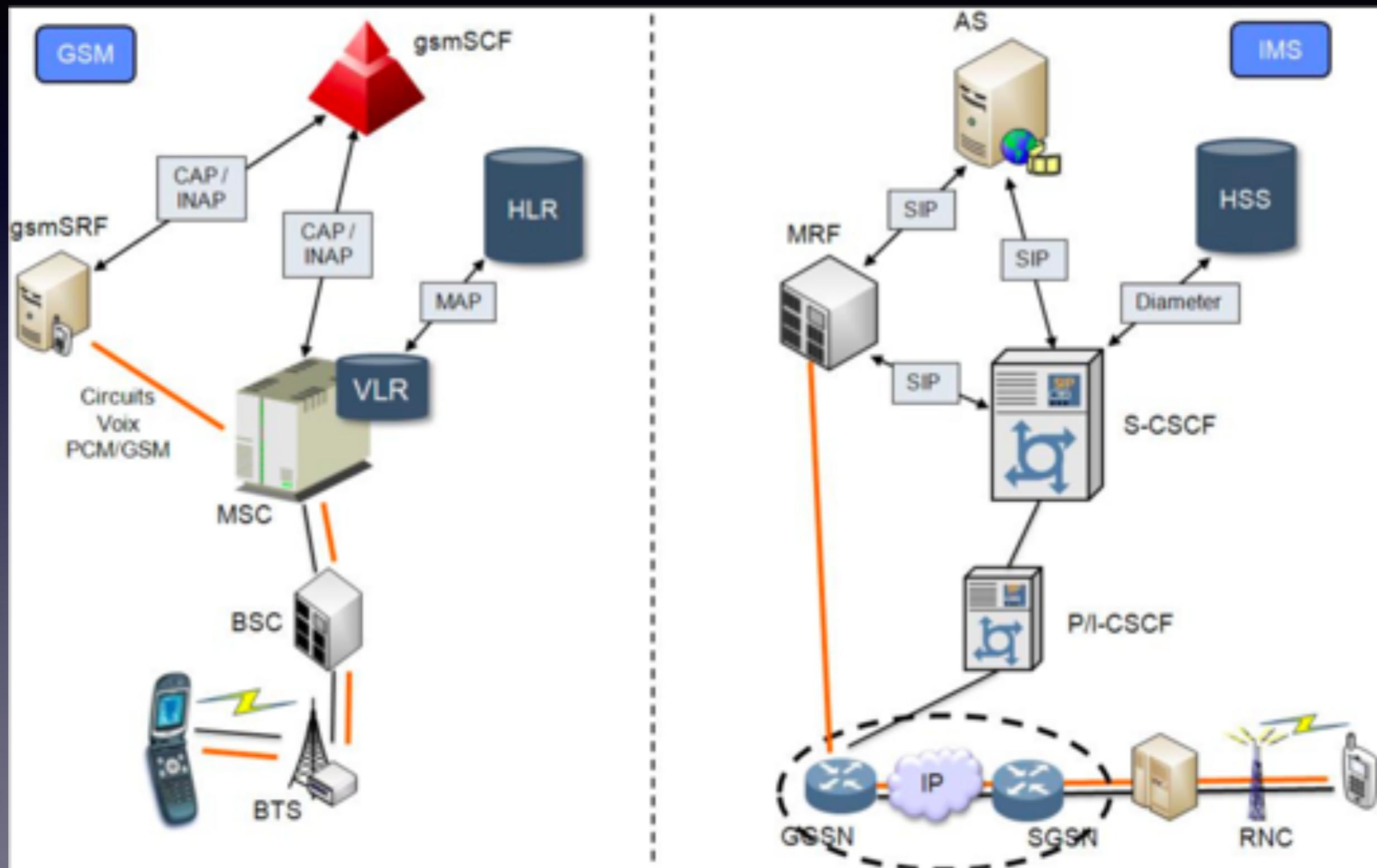


# Compromised Telco



# Mobile 4G

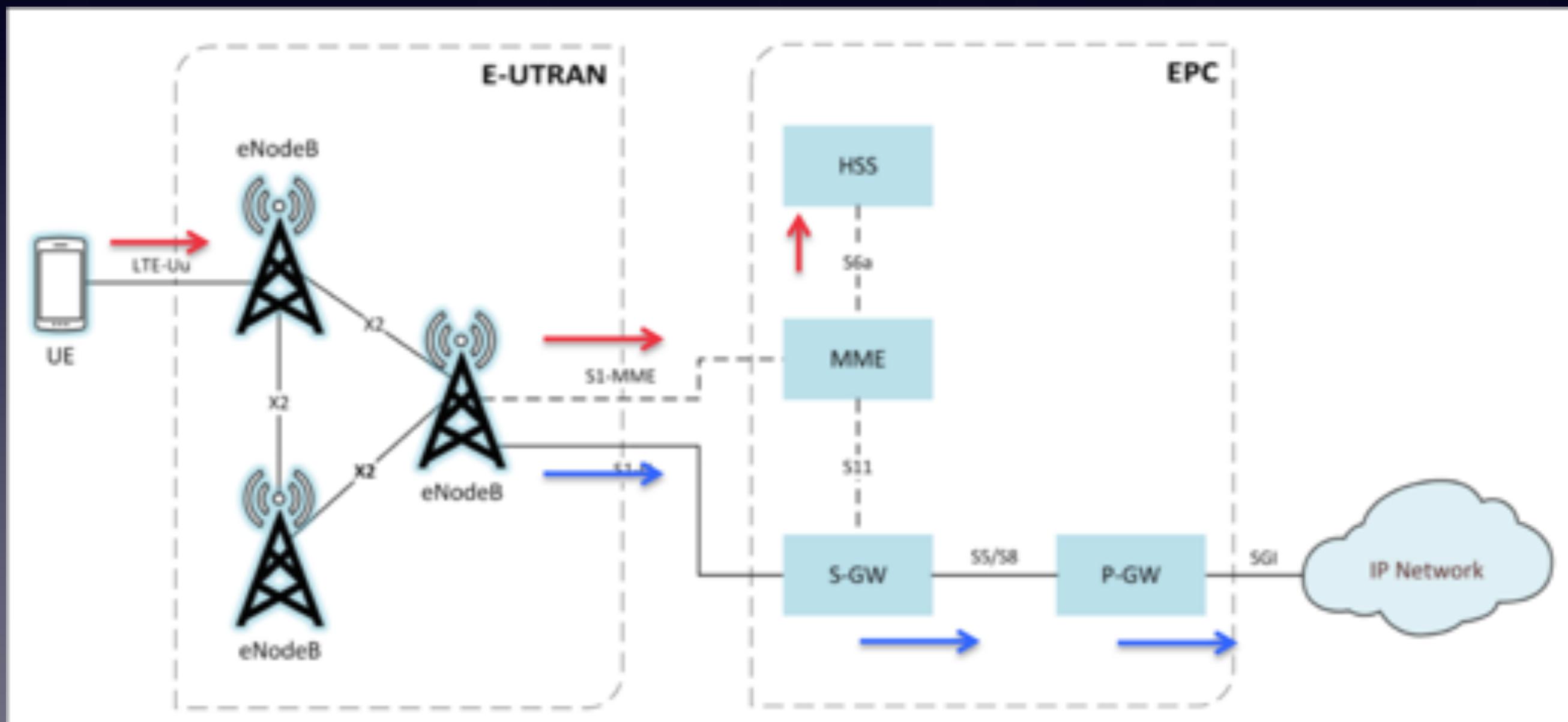
# Evolution of Architecture



# 4G Security

- Use of DIAMETER protocol to replace SS7 signalling.
- Use of Network Elements based on known tech (e.g. Linux, TCP/IP)
- Terminal (UE) and NEs talk SIP and still use the GTP suite of protocols
- Governments now routinely intercept all data communications

# 4G Principles



# 4G Threats

- New attacks based on IP for network elements and terminals
- Portability of SS7 attacks of DIAMETER using Interworking Function
- Hostile encapsulation of protocols within GTP tunnels and SIP packets
- Exposure of internal networks to outside entities
- Increased interconnections between telcos and service providers/vendors

# Security Standards

## ITU-T X.800 Threat Model

### 1 - Destruction (an attack on availability):

- Destruction of information and/or network resources

### 2 - Corruption (an attack on integrity):

- Unauthorized tampering with an asset

### 3 - Removal (an attack on availability):

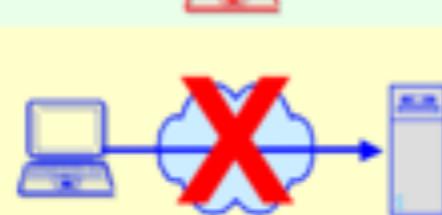
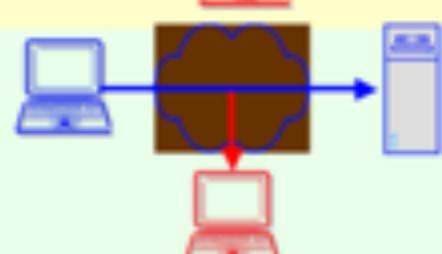
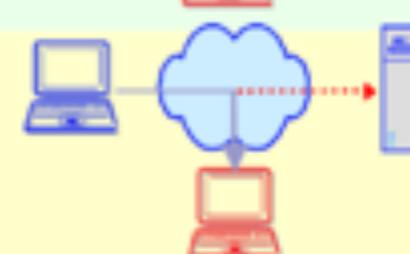
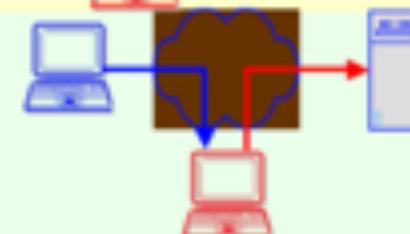
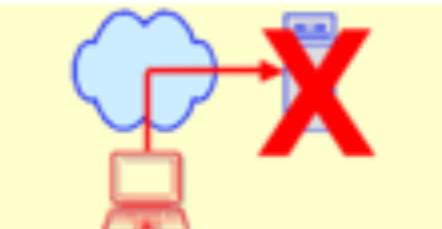
- Theft, removal or loss of information and/or other resources

### 4 - Disclosure (an attack on confidentiality):

- Unauthorized access to an asset

### 5 - Interruption (an attack on availability):

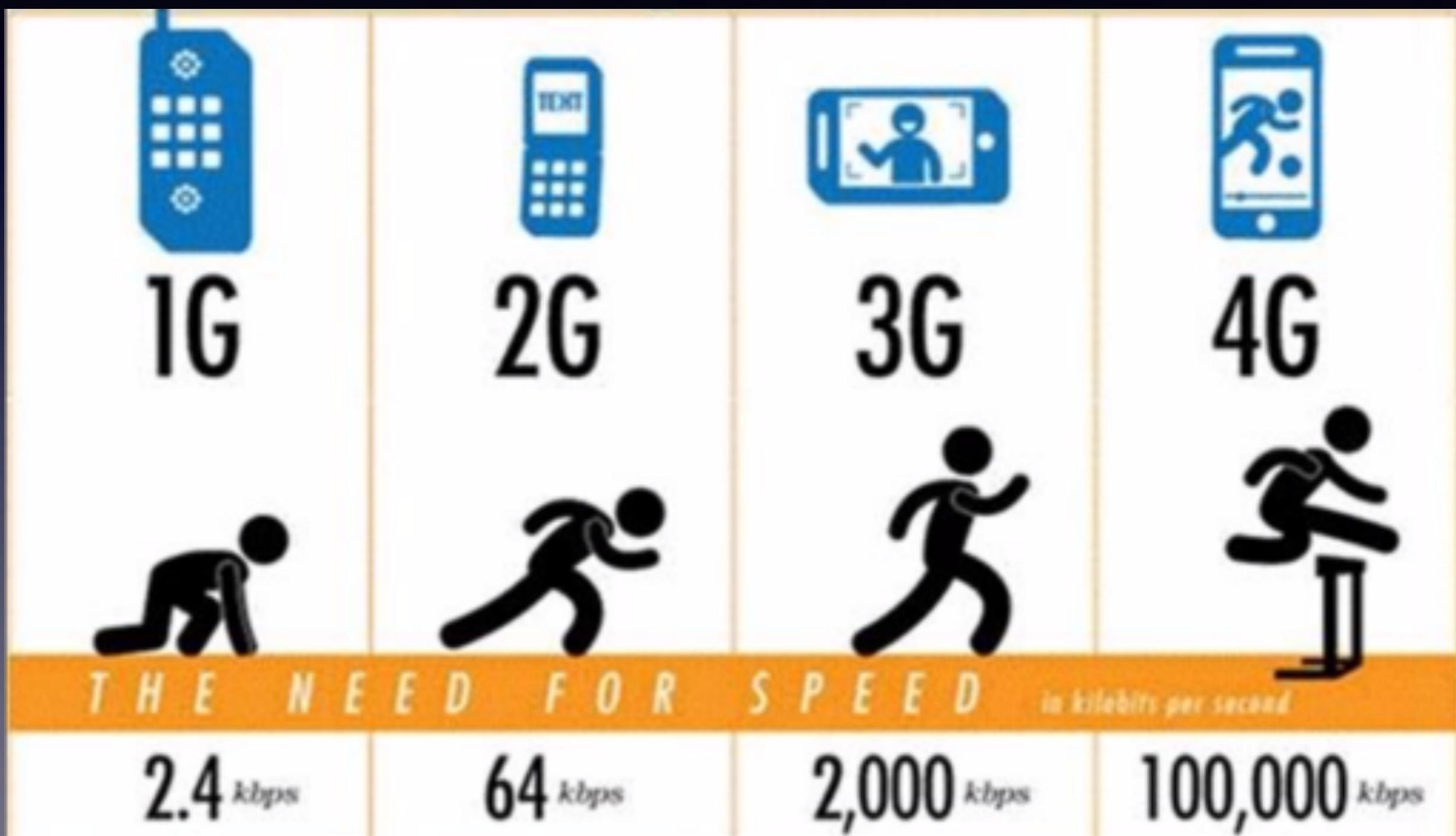
- Interruption of services. Network becomes unavailable or unusable



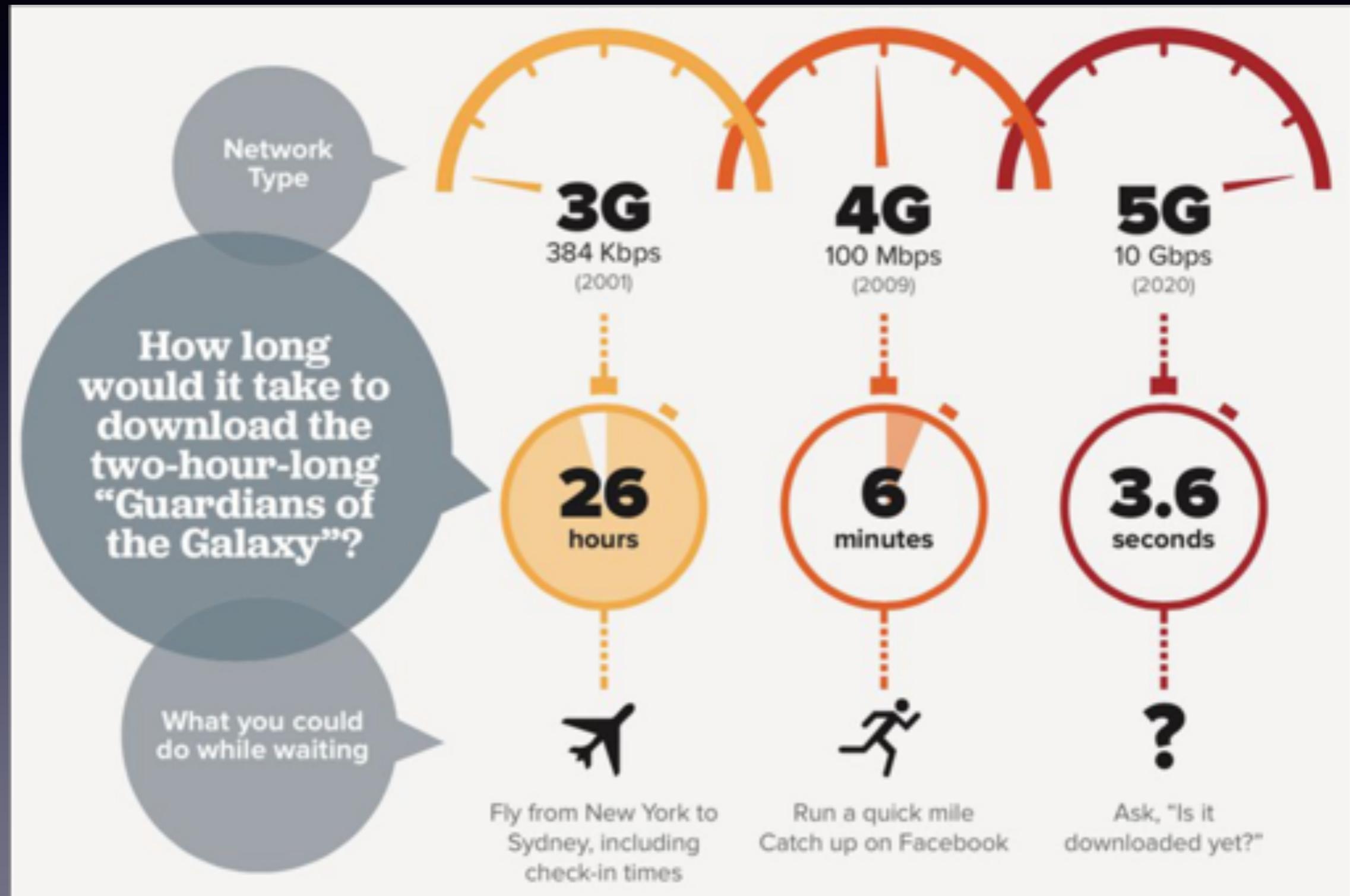
# Managing Security

- To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood.
- To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:
  - Network Security Design
  - Business Continuity Management
  - Network Configuration / Integration
  - Network Security Audits
  - Network Security Implementation
  - Fraud Management

# Where is this going?



# The 5G unknown



# 5G Security

- IOT devices (millions, poorly secured, access)
- Bandwidth and latency unheard of
- Massive terminal computing power
- AI / ML advances
- Full-IP infrastructure
- Complex and ever-growing perimeter
- MANY APPLICATIONS UNFORESEEN



# Conclusions

- Started as a closed garden
- Evolved into a worldwide digital cell network
- Used in every aspect of our lives
- Becoming increasingly hacker-friendly
- Security always an after-thought
- Large attack surface and expanding perimeter

# Thanks!

## Q&A

# Credits

- Philippe Langlois
- Raoul Chiesa
- Ollie Whitehouse
- Dino Covotsos
- Karsten Nohl
- Tobias Engel
- Lin Huang
- John Draper