Evolution of Security Threats to Telecommunications Infrastructures

HITB Dubai 2018

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

1800 BC
Smoke Signals

In a matter of hours Chinese soldiers, stationed on the Great Wall, could warn their comrades 500 miles away of an impending enemy attack via tower to tower smoke signals.

150 BC
The Greek Way

Polybius, a Greek historian, invented a system of converting Greek alphabetic characters into numeric characters. This enabled messages to be easily sent by coded torch smoke signals.

Aα Bβ Γγ Δδ
Εε Ζζ Ηη Θθ
Ιι Κκ Λλ Μμ
Νν Ξξ Οο Ππ

1876
"Mr. Watson..

..come here, I want to see you," were the first words spoken on a successful telephone call by Alexander Graham Bell.

come here

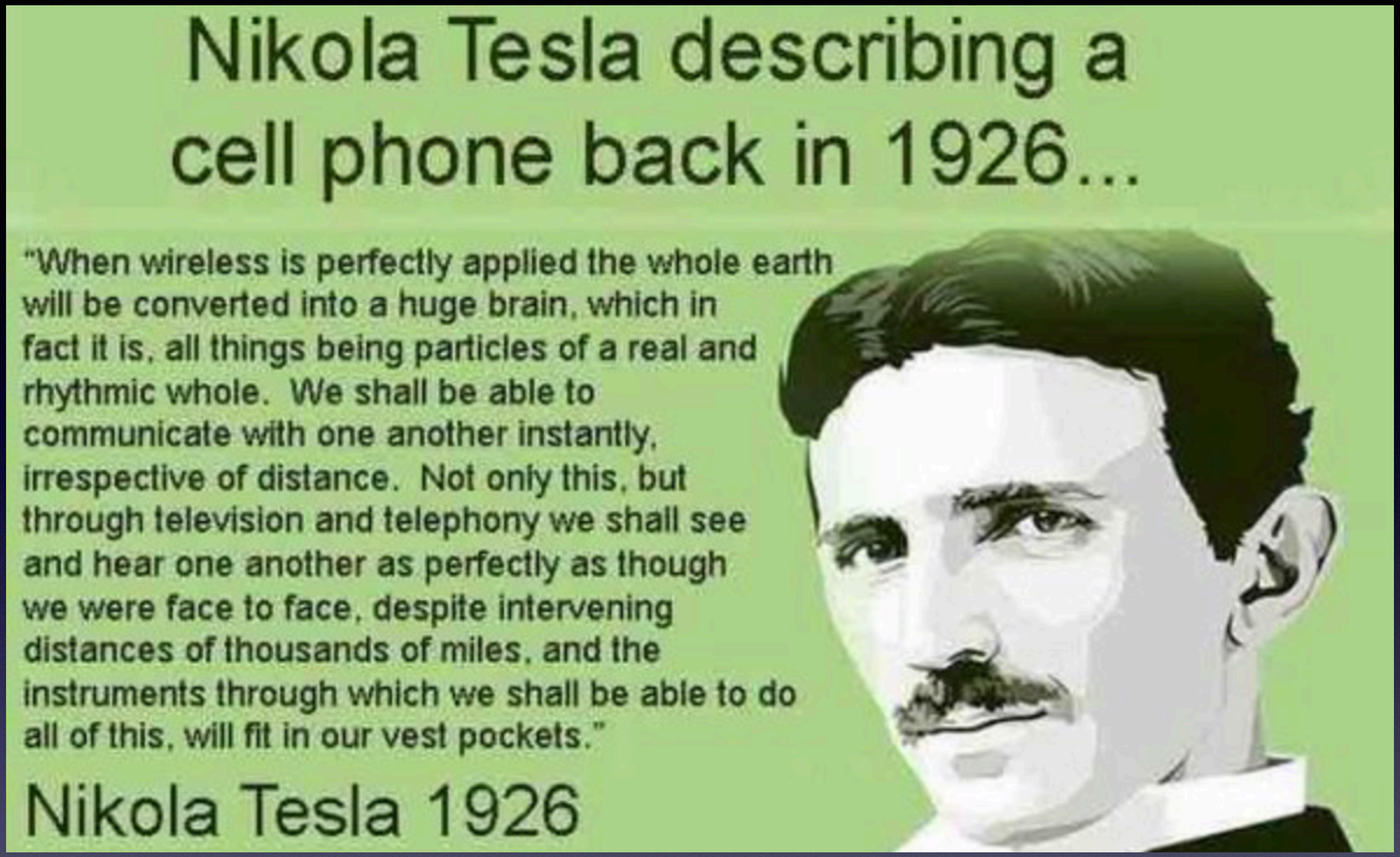
1844
Telegram

The first telegraph message traveled 40 miles and read "What Hath God Wrought?"

what hath God wrought?

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 (1856-1943)

Can you predict comms tech in year 2100 ?

Generation Zero

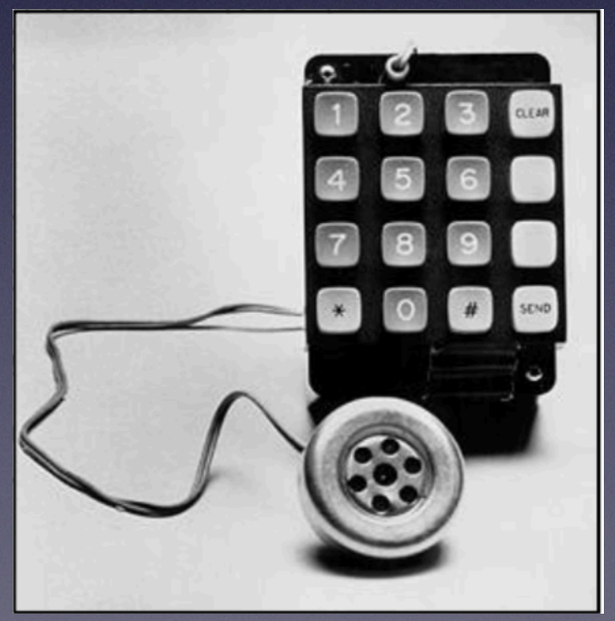
Basic security problems:

- 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

5551535 5551321 5551172
5551894 5551383 5551235 5551187 5551102
5551710 5551623 5551891 5551972 5551810 5551030
5551803 5551767 5551443
5551890 5551061 5551107

[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?
```

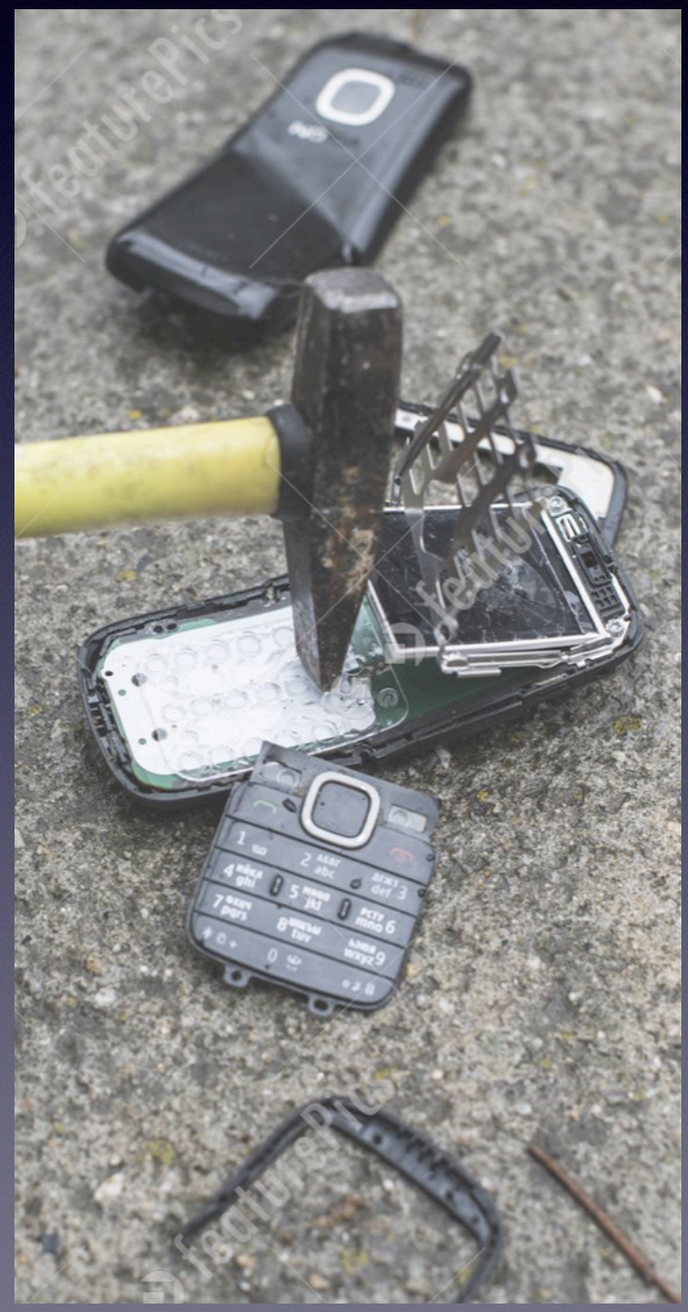
Generation 1G Analog

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

GSM Security Golden Years

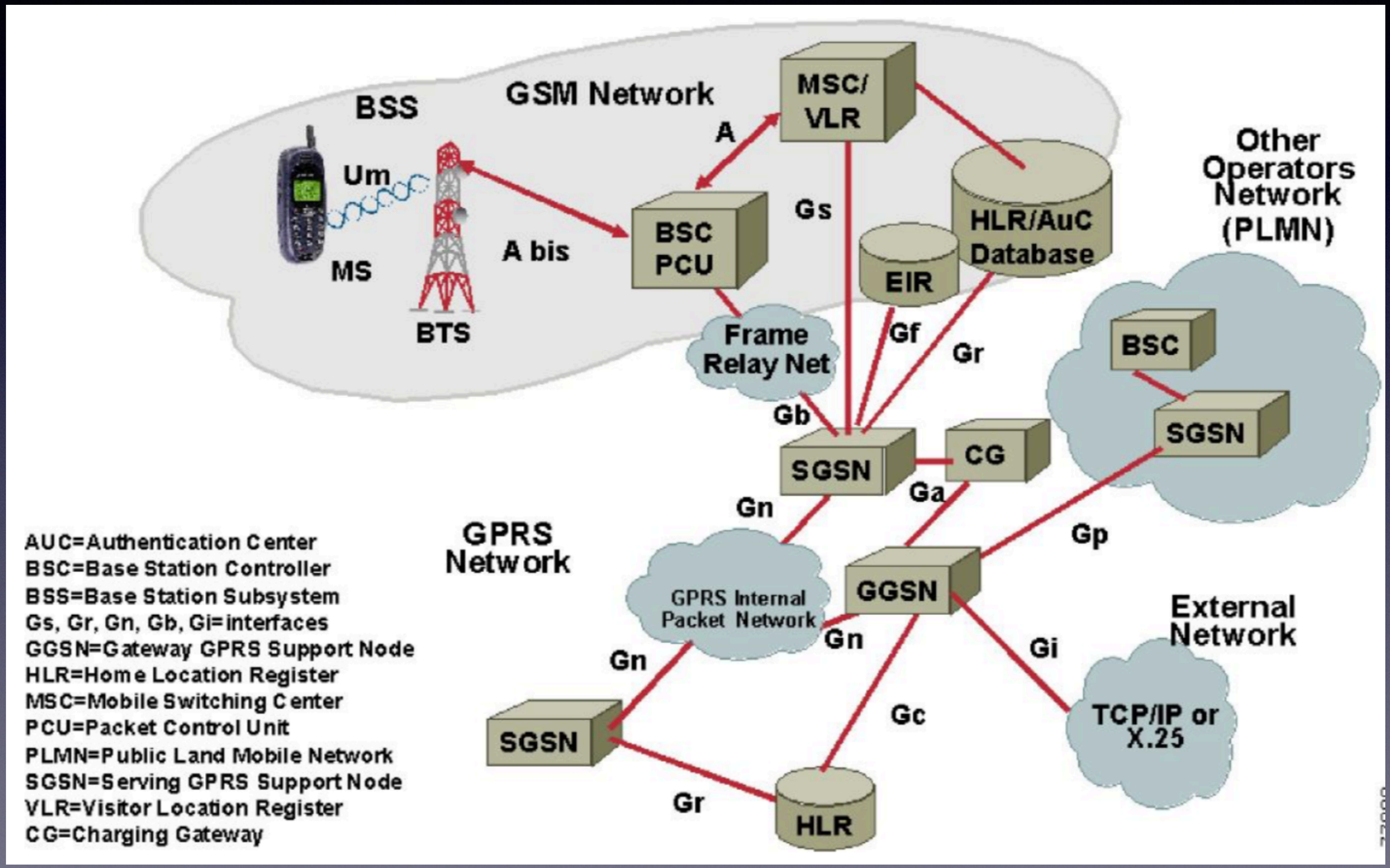
- From 1989 to 1998, no security issues
- Some academic research into radio protocols
- First cryptanalysis 1998 (COMP128) and 1999 (A5/1 and A5/2)
- First GSM security paper Blackhat Asia 2001
- SIM card security model not broken
- No known compromise of infrastructure
- No signalling abuse, death of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

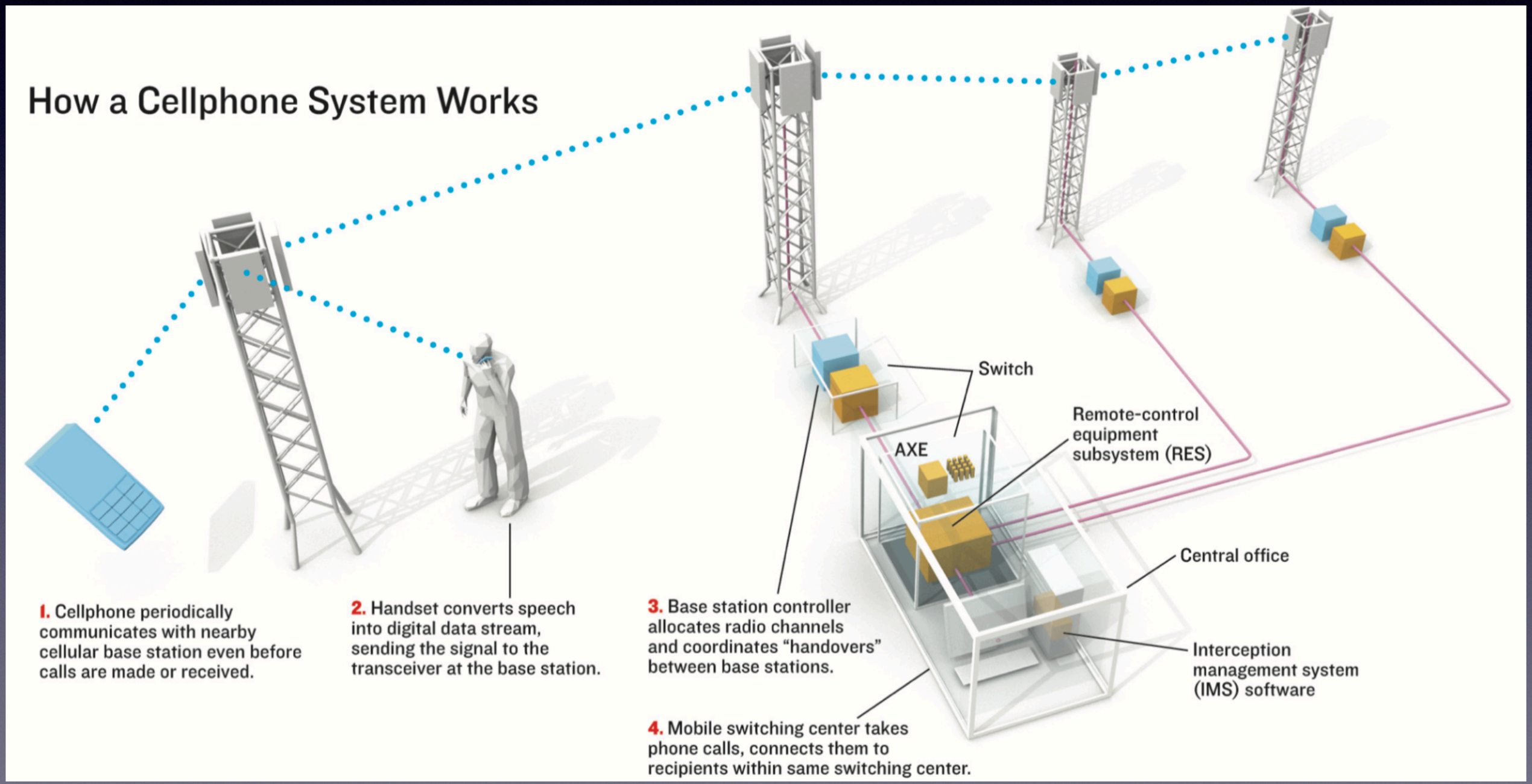
- Proprietary OS (first models from Nokia, Ericsson, Alcatel)
- Data connectivity has low bandwidth, high latency
- Screen real estate not usable for serious data usage
- Web sites and services not compatible with WAP and early data attempt

Mobile 3G

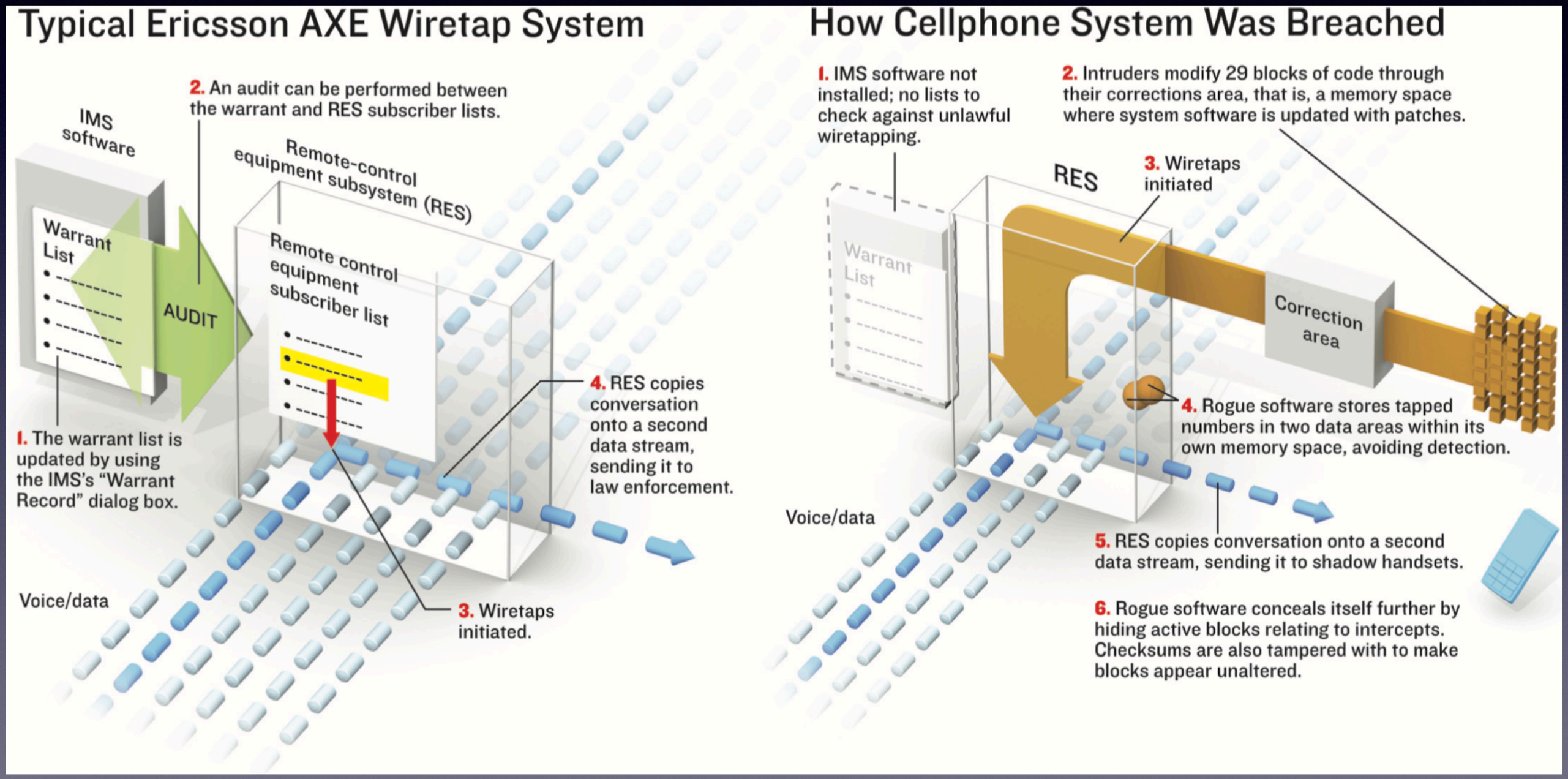
3G landscape

- 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

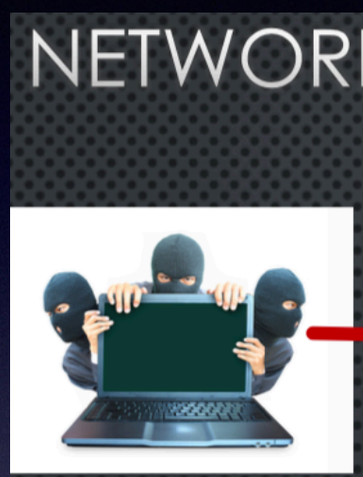
Nation-State Attacks



The Athens Affair

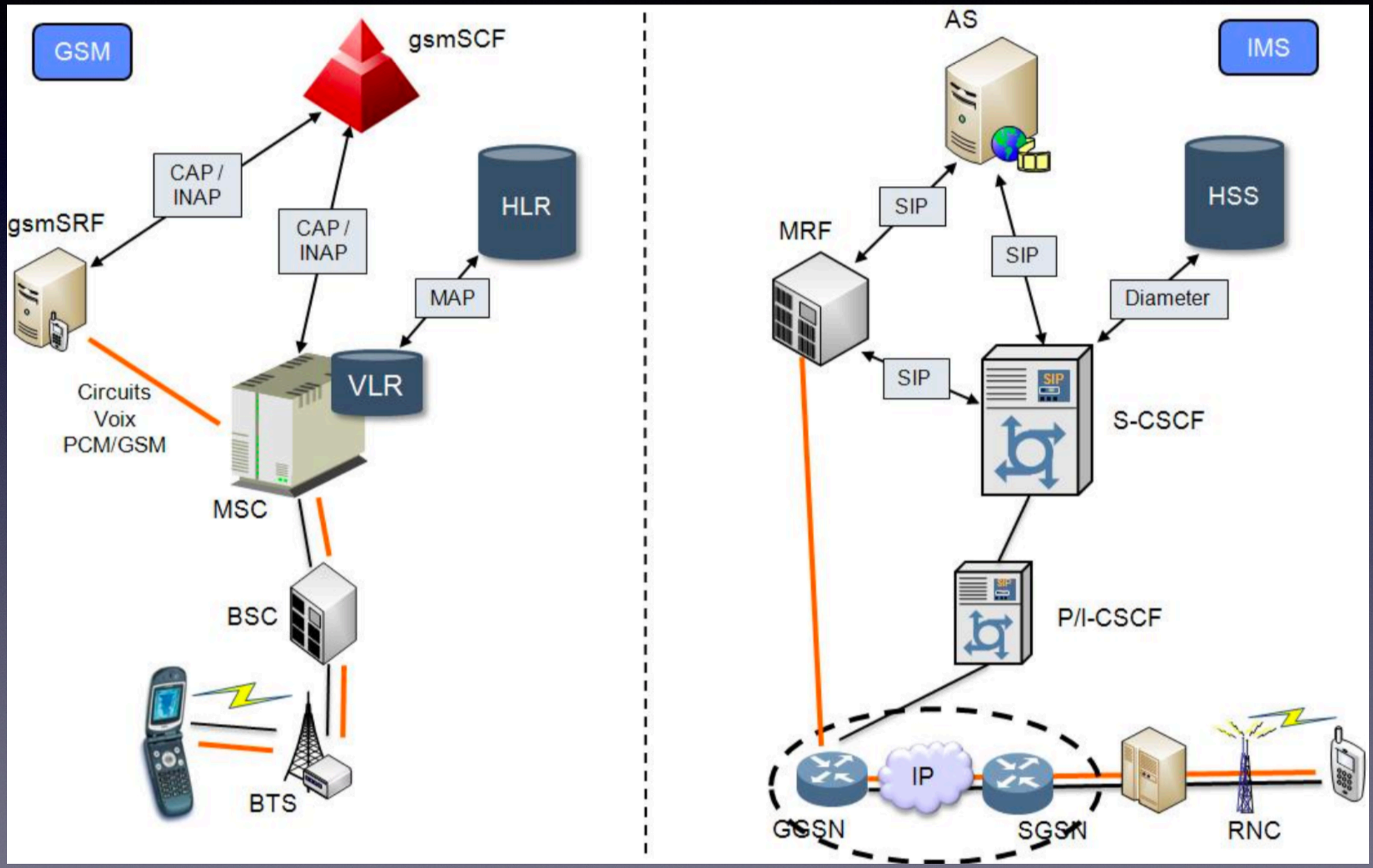


Compromised Telco



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 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):

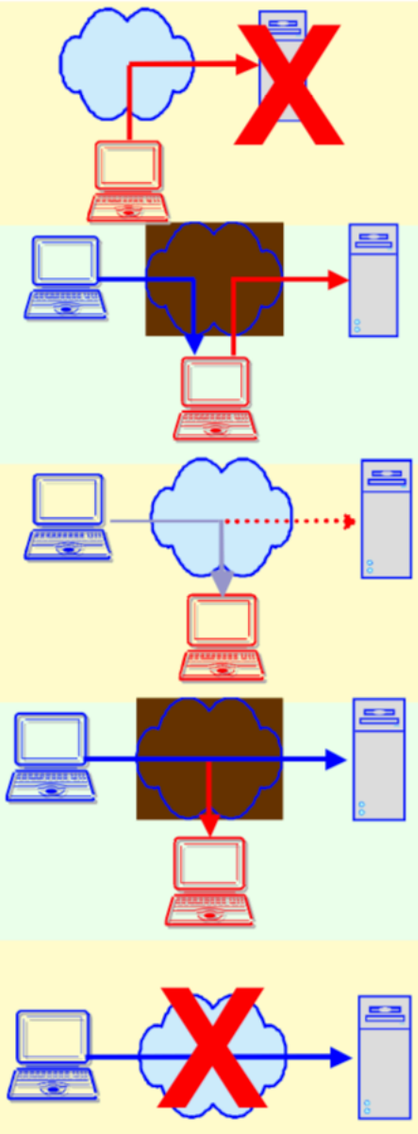
- Theft, removal or loss of information and/or other resources

4 - Disclosure (an attack on confidentiality):

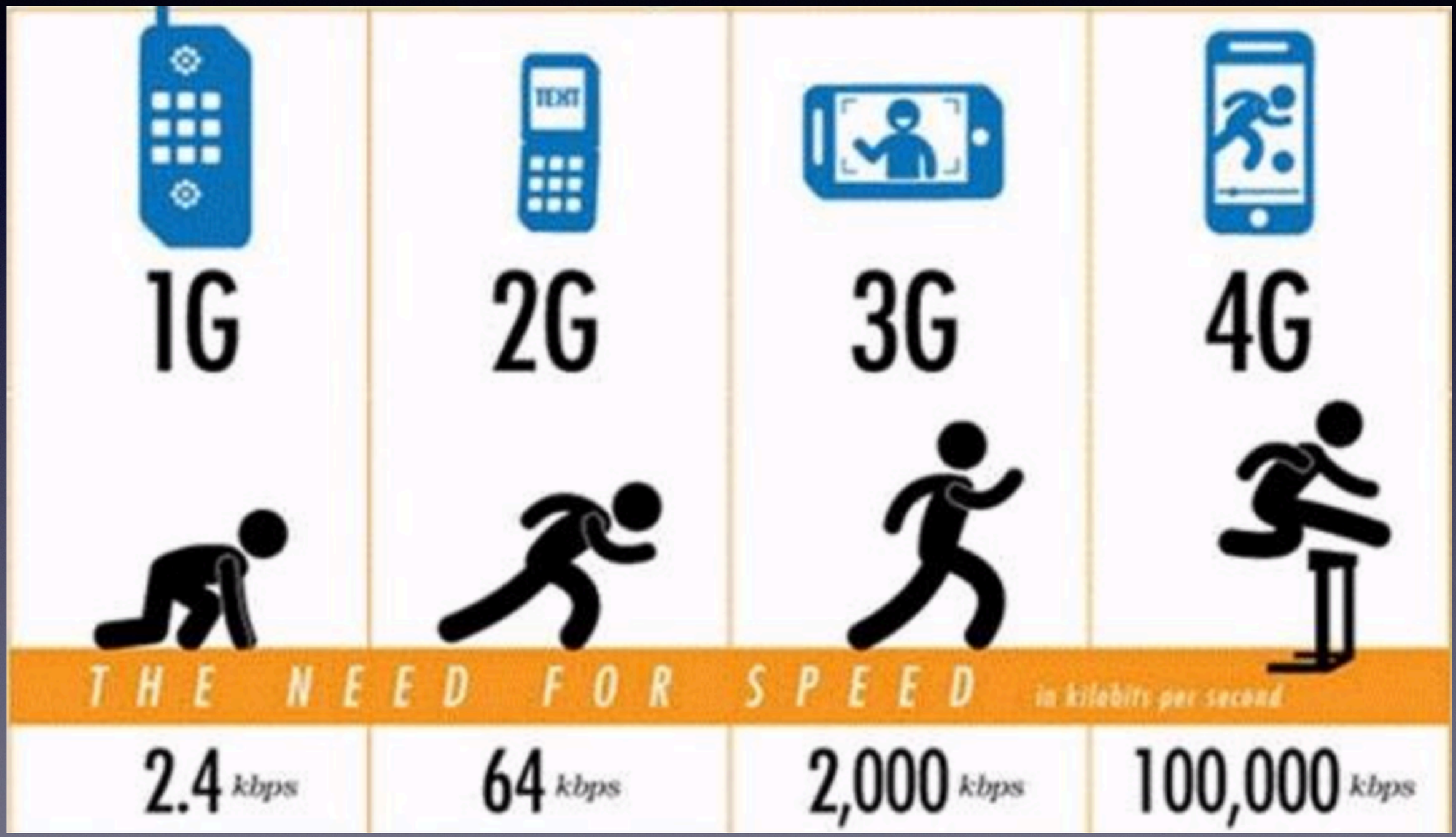
- Unauthorized access to an asset

5 - Interruption (an attack on availability):

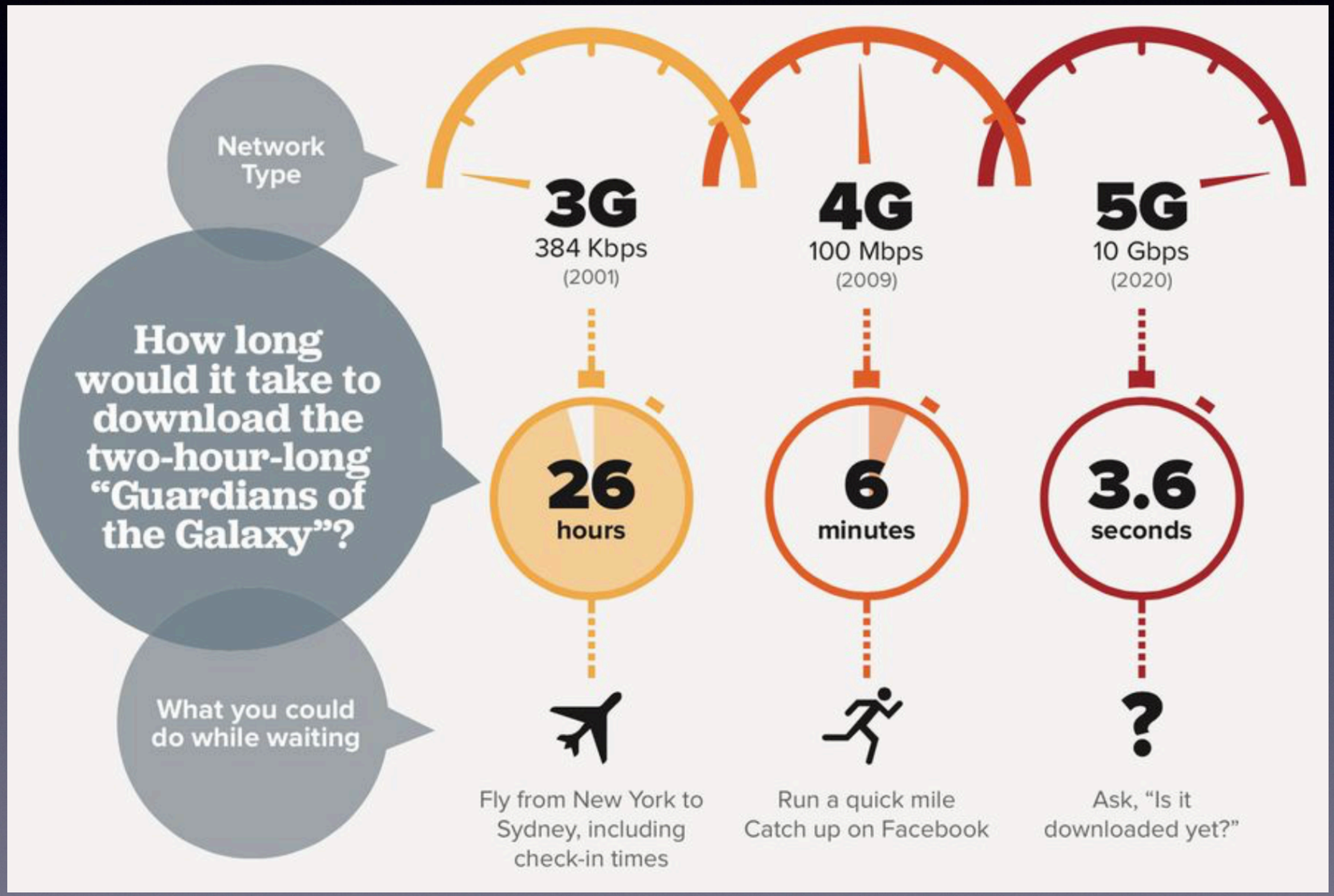
- Interruption of services. Network becomes unavailable or unusable



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
- Loay Hassan Abdelrazek
- Lin Huang
- John Draper