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.

1876
“Mr. Watson...”
“Come here, I want to see you,” were the first words spoken on a successful telephone call by Alexander Graham Bell.

1844
Telegram
The first telegraph message traveled 40 miles and read “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 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?
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
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
• 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

How a Cellphone System Works

1. Cellphone periodically communicates with nearby cellular base station even before calls are made or received.

2. Handset converts speech into digital data stream, sending the signal to the transceiver at the base station.

3. Base station controller allocates radio channels and coordinates “handovers” between base stations.

4. Mobile switching center takes phone calls, connects them to recipients within same switching center.
The Athens Affair

Typical Ericsson AXE Wiretap System

1. The warrant list is updated by using the IMS’s “Warrant Record” dialog box.
2. An audit can be performed between the warrant and RES subscriber lists.
3. Wiretaps initiated.
4. RES copies conversation onto a second data stream, sending it to law enforcement.

How Cellphone System Was Breached

1. IMS software not installed; no lists to check against unlawful wiretapping.
2. Intruders modify 29 blocks of code through their corrections area, that is, a memory space where system software is updated with patches.
3. Wiretaps initiated.
4. Rogue software stores tapped numbers in two data areas within its own memory space, avoiding detection.
5. RES copies conversation onto a second data stream, sending it to shadow handsets.
6. Rogue software conceals itself further by hiding active blocks relating to intercepts. Checksums are also tampered with to make blocks appear unaltered.
Compromised Telco

- **Relay Host**
  - Forwarding ACL bypass

- **Staging Host**
  - Tools / compiler
  - C&C comms
  - Data exfiltration

- **Operation Support Systems**
  - OSS
  - Billing Mediation

- **Core Network**
  - MSC/MSS/MGW
  - BSC/RAN
  - HLR/HSS
  - SGSN/GGSN

- **Value-Added Services**
  - IN / Prepaid Messaging
  - USSD

**UPGRADE**
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?

1G

2G

3G

4G

THE NEED FOR SPEED

2.4 kbps

64 kbps

2,000 kbps

100,000 kbps

in kilobits per second
The 5G unknown

*Network Type*

- **3G**: 384 Kbps (2001)
  - **26 hours**
  - Fly from New York to Sydney, including check-in times
- **4G**: 100 Mbps (2009)
  - **6 minutes**
  - Run a quick mile
  - Catch up on Facebook
- **5G**: 10 Gbps (2020)
  - **3.6 seconds**
  - ?
  - Ask, “Is it downloaded yet?”

*How long would it take to download the two-hour-long “Guardians of the Galaxy”?*
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