Security in the telecom business

From the equipment manufacturer’s point of view

Ulf Larson,
System Manager for Security at Ericsson Packet Core
IT-security consultant at Ajilon Consultants AB
OWASP Gothenburg co-founder and co-leader

About the speaker

- Ulf Larson
- Educated (Ph.D.) at Chalmers University, Computer Security -> Intrusion detection
- Employed at Ajilon Consultants
- Consultant (System Manager with security focus) at Ericsson, Packet Core, SGSN-MME

45 minutes on telecom security

ulf.larson@ajilonconsultants.se

45 minutes on telecom security

- Setting the stage - Telecom and the core infrastructure

45 minutes on telecom security

› Setting the stage - Telecom and the core infrastructure

› Why is security important in telecom?

45 minutes on telecom security

- Setting the stage - Telecom and the core infrastructure
- Why is security important in telecom?
- The Athens Affair - a historical breach and its implications

45 minutes on telecom security

- Setting the stage - Telecom and the core infrastructure
- Why is security important in telecom?
- The Athens Affair - a historical breach and its implications
- Current telecom security trends

45 minutes on telecom security

- Setting the stage - Telecom and the core infrastructure
- Why is security important in telecom?
- The Athens Affair - a historical breach and its implications
- Current telecom security trends
- Working as a system manager with security focus at Ericsson

Setting the stage – Telecom and the core infrastructure

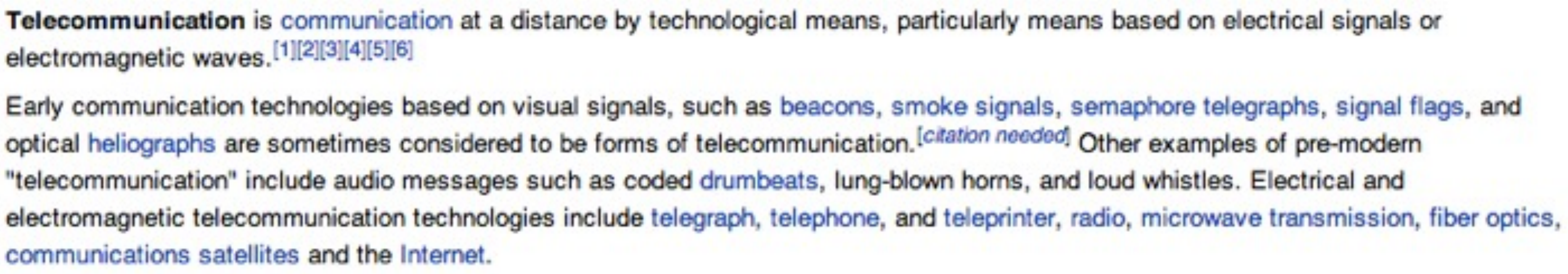
Ajilon

ulf.larson@ajilonconsultants.se

www.ajilonconsultants.se

What is telecom?

What is telecom?



Telecommunication is communication at a distance by technological means, particularly means based on electrical signals or electromagnetic waves.[1][2][3][4][5][6]

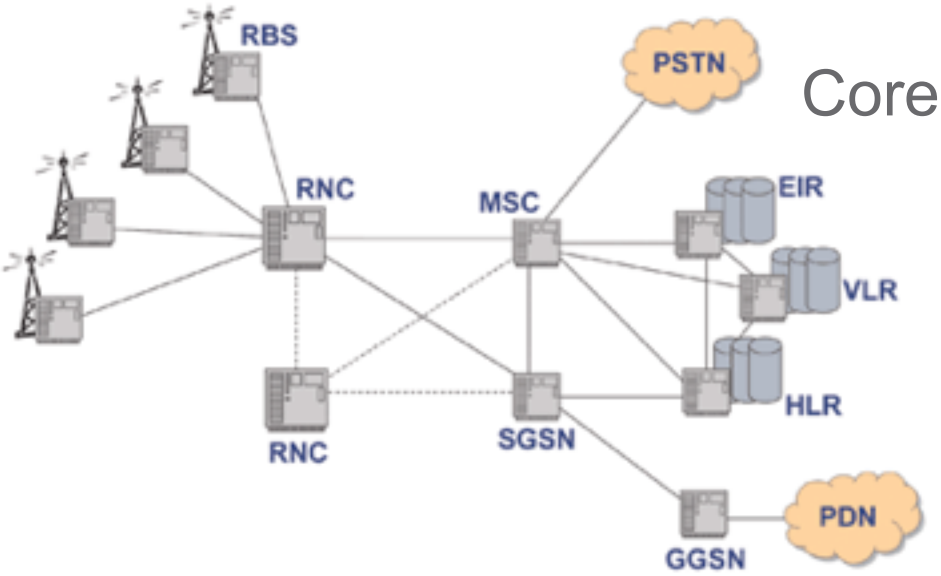
Early communication technologies based on visual signals, such as beacons, smoke signals, semaphore telegraphs, signal flags, and optical heliographs are sometimes considered to be forms of telecommunication.[*citation needed*] Other examples of pre-modern "telecommunication" include audio messages such as coded drumbeats, lung-blown horns, and loud whistles. Electrical and electromagnetic telecommunication technologies include telegraph, telephone, and teleprinter, radio, microwave transmission, fiber optics, communications satellites and the Internet.

Typical telecom components

Telecommunication (in the modern era) is the science and practice of transmitting information by electromagnetic means

User Equipment

Radio stations and controllers



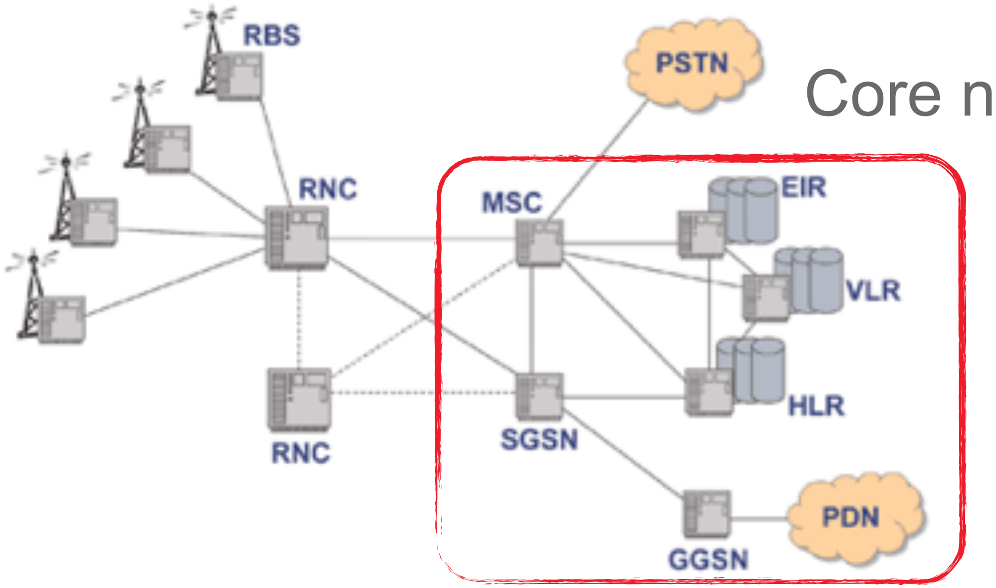
Core network

Typical telecom components

Telecommunication (in the modern era) is the science and practice of transmitting information by electromagnetic means

User Equipment

Radio stations and controllers



Core network

Ajilon

The Packet Core

Infrastructure architecture for IP packet services in GSM (2G), WCDMA (3G) and LTE (4G) networks

Two core network architectures:

- GPRS core network for GSM and WCDMA
- EPC core network for LTE

Core network handles

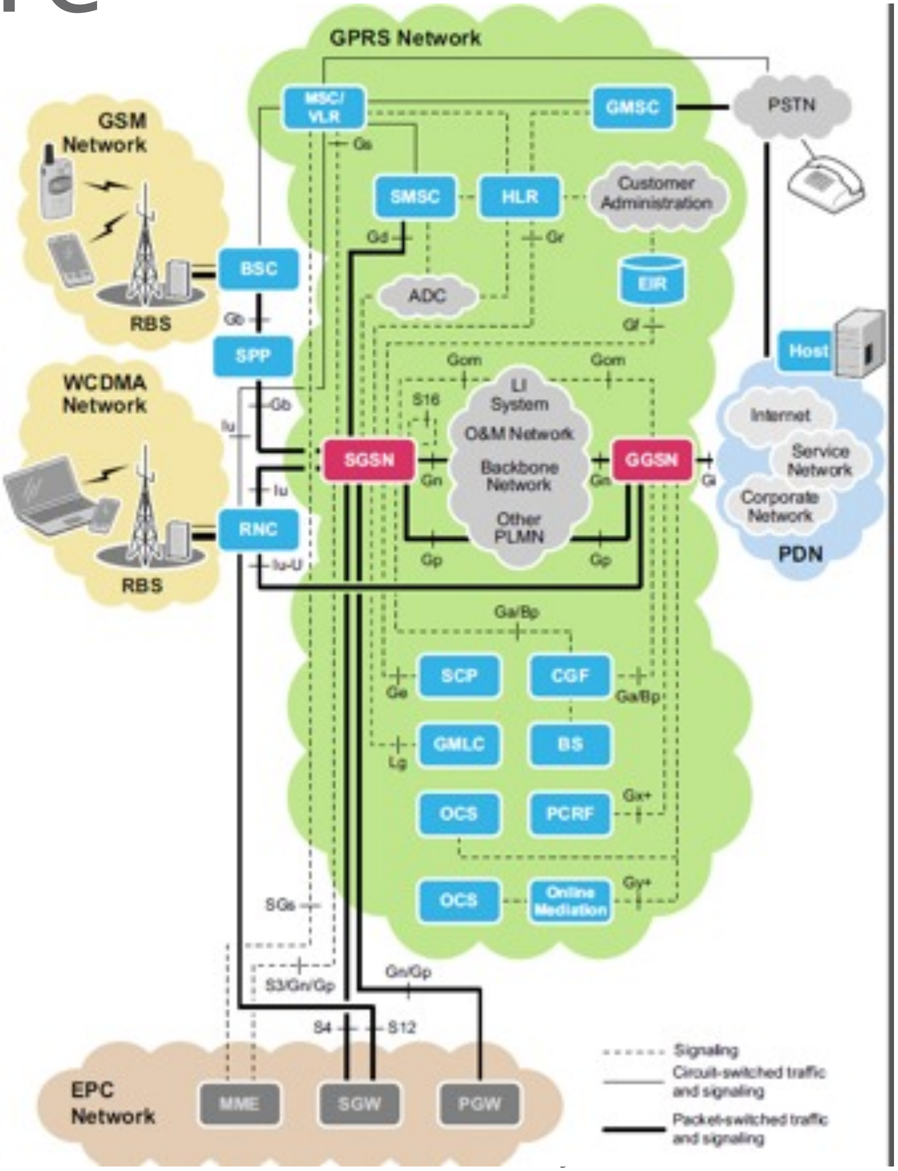
- Mobility management and transport
- Billing and lawful interception

Architecture is specified as open standard by 3GPP

GPRS packet core

- General Packet Radio Service
- Allows transmission of data over GSM and WCDMA networks

- Network interfaces (Gb, Gi)
- Core elements (SGSN, GGSN, HLR ...)



Why is security important in telecom?

Why is security important in the telecom area?

- Who are the stakeholders?
  - Subscribers
  - Operators
  - Equipment manufacturers

The subscriber

- Buys user equipment, i.e., mobile phones and laptops, mobile broadband ...
- Uses the operator’s network (or other operator’s network) to make calls and transmit data

The operator

- Manages the network
- Buys equipment from the equipment manufacturers
- Charges subscribers for used bandwidth according to an agreement (one of seemingly unlimited number of offers)
- Requires functionality and features that fit their business strategy and way forward

The equipment manufacturer

- Sells equipment to the operators
- Follows (or leads) development within 3GPP to be in the forefront of technology evolution
- Implements features based on customer requests

ERICSSON

Potential threats – Actors

- External penetrators
  - All types of malicious users
- Insiders misusing their privileges
  - Employees at Operator
  - Employees at Equipment manufacturer
- Fraudsters
- Researchers trying to figure out how telecom works

- Employees making mistakes ...

Potential threats – what can happen?

- Leakage of private subscriber data
- Unlawful intercept - unauthorized use of data collection features
- Intrusions and malware planting, rootkits
- Network outage and denial of service
- Misuse of legitimate privileges
- Physical disruption
- Subscription fraud
- Subverted or modified cell phones sending strange or unexpected input data or signaling messages

Possible effects

- Unwanted media attention -> reputation loss -> financial loss
- Broken contracts, lawsuits ->financial loss
- Government imposed fines -> financial loss
- Costly investigations -> financial loss

But why is this a problem for the manufacturer?

- Isn’t it the operator’s responsibility to make sure that these events don’t occur?

But why is this a problem for the manufacturer?

- Isn’t it the operator’s responsibility to make sure that these events don’t occur?

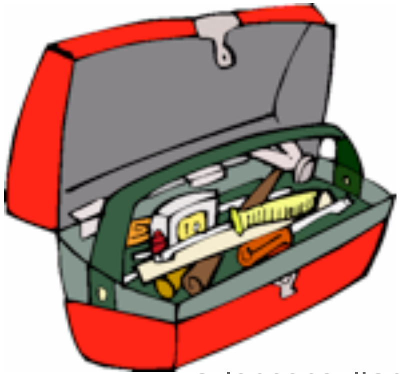
I’m all ears!

But why is this a problem for the manufacturer?

- Isn’t it the operator’s responsibility to make sure that these events don’t occur?

I’m all ears!

To be able to act responsible, the operators must first have the means to do so



Ajilon

ulf.larson@ajilonconsultants.se

www.ajilonconsultants.se

As equipment manufacturer...

As equipment manufacturer...

- E/// can:
  - Use customer documentation to recommend that the customer configures their network and equipment according to security best practices

As equipment manufacturer...

- E/// can:
  - Use customer documentation to recommend that the customer configures their network and equipment according to security best practices

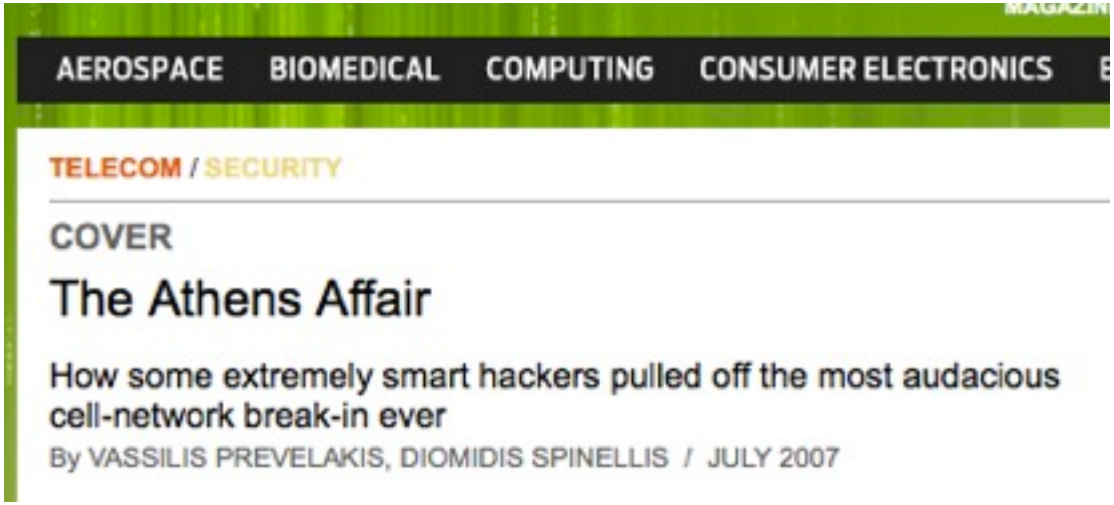
- and:
  - Perform risk assessment to show that we are aware of security risks and has taken an active decision to handle these appropriately
  - Perform vulnerability assessment activities to find previously unknown vulnerabilities and mitigate these

As equipment manufacturer...

- E/// can:
  - Use customer documentation to recommend that the customer configures their network and equipment according to security best practices
- and:
  - Perform risk assessment to show that we are aware of security risks and has taken an active decision to handle these appropriately
  - Perform vulnerability assessment activities to find previously unknown vulnerabilities and mitigate these
- and:
  - Ourselves follow best practices to provide the customers with the prerequisites for securing their components, i.e., access control, authorization, logging …
  - provide user instructions on how to perform additional network equipment hardening

The Athens Affair

The Athens Affair



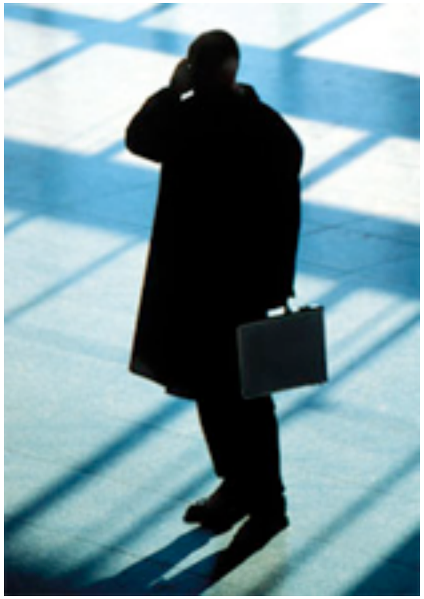
TELECOM / SECURITY

COVER

The Athens Affair

How some extremely smart hackers pulled off the most audacious cell-network break-in ever

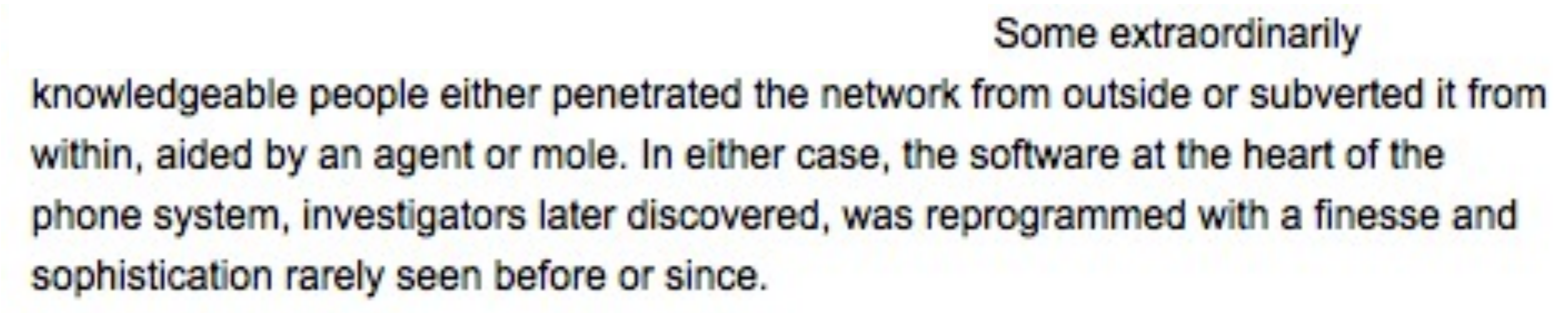
By VASSILIS PREVELAKIS, DIOMIDIS SPINELLIS / JULY 2007



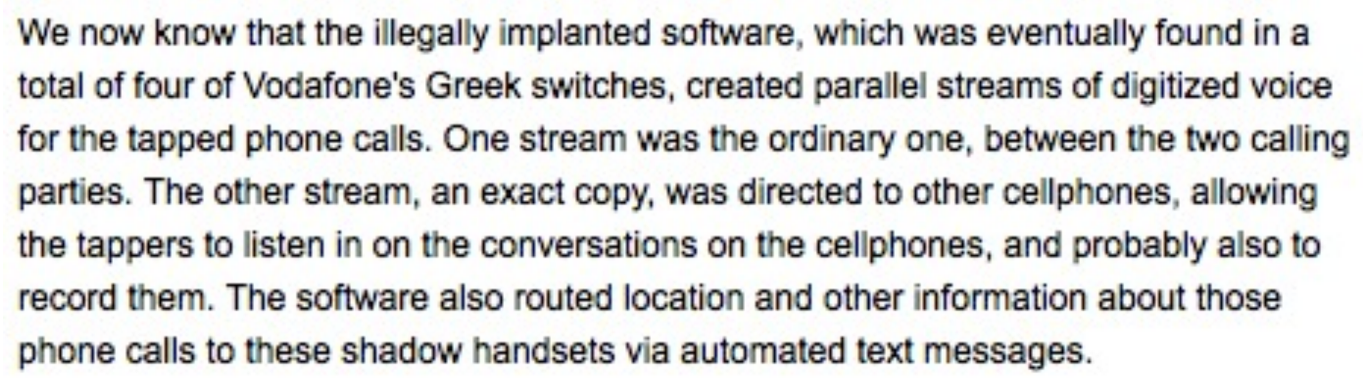
How a hundred CEOs, MPs and a PM’s mobile phones were wiretapped between August 2004 and March 2005

http://spectrum.ieee.org/telecom/security/the-athens-affair/0

The Athens Affair

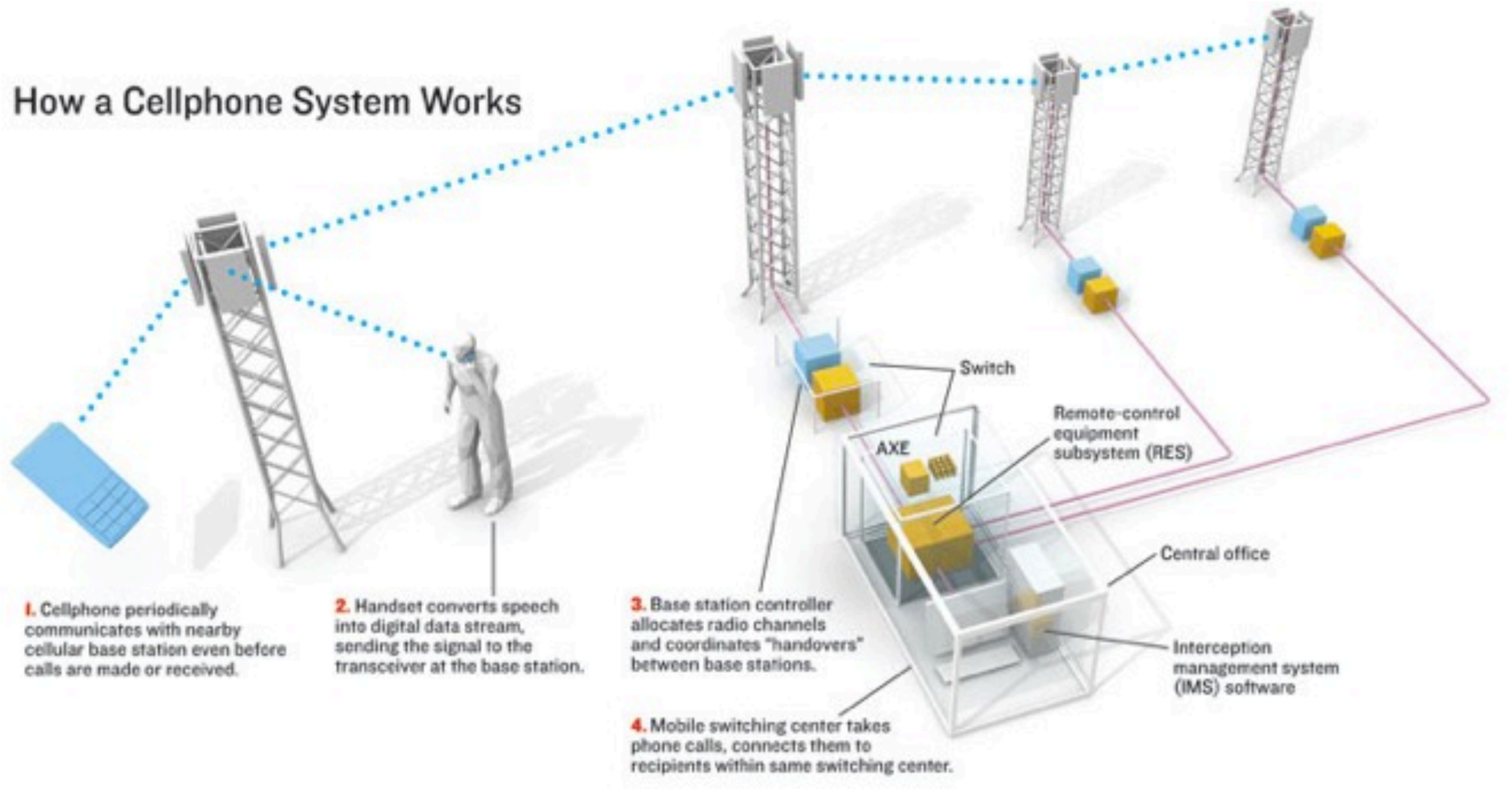


Some extraordinarily knowledgeable people either penetrated the network from outside or subverted it from within, aided by an agent or mole. In either case, the software at the heart of the phone system, investigators later discovered, was reprogrammed with a finesse and sophistication rarely seen before or since.



We now know that the illegally implanted software, which was eventually found in a total of four of Vodafone's Greek switches, created parallel streams of digitized voice for the tapped phone calls. One stream was the ordinary one, between the two calling parties. The other stream, an exact copy, was directed to other cellphones, allowing the tappers to listen in on the conversations on the cellphones, and probably also to record them. The software also routed location and other information about those phone calls to these shadow handsets via automated text messages.

The Athens Affair


How a Cellphone System Works
Switch
AXE
Remote-control equipment subsystem (RES)
Central office
Interception management system (IMS) software

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.

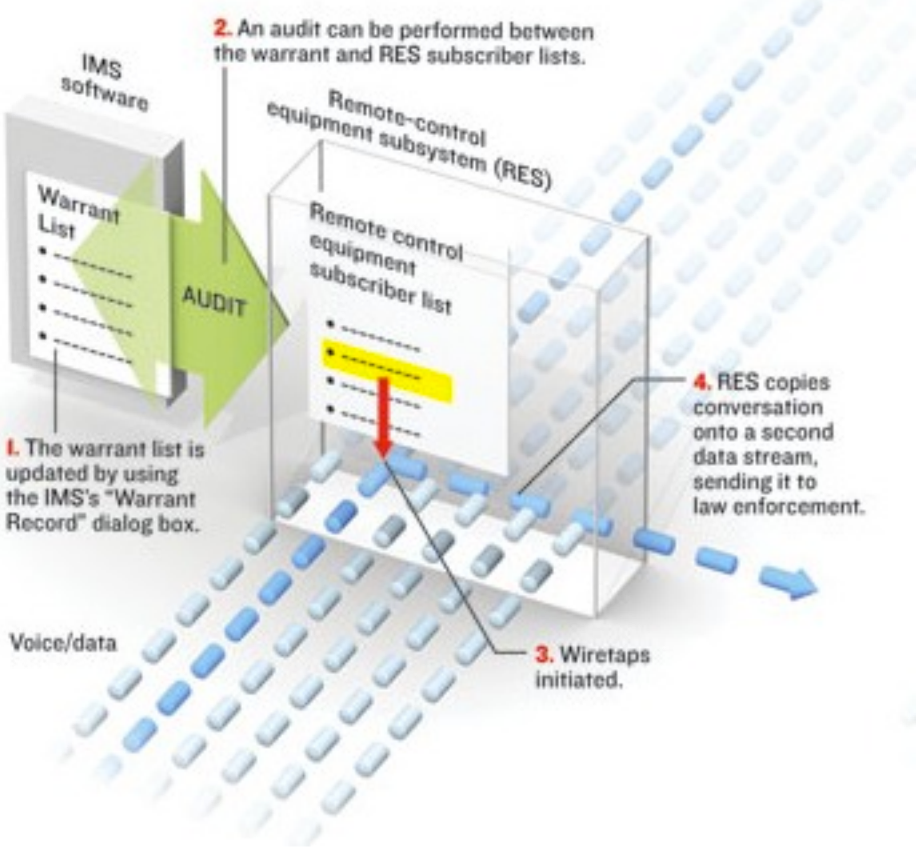
4. Mobile switching center takes phone calls, connects them to recipients within same switching center.

RES - Remote controlled equipment subsystem

IMS - Interception management system

The Athens Affair

Typical Ericsson AXE Wiretap System



IMS software
Warrant List
AUDIT
Remote-control equipment subsystem (RES)
Remote control equipment subscriber list
Voice/data

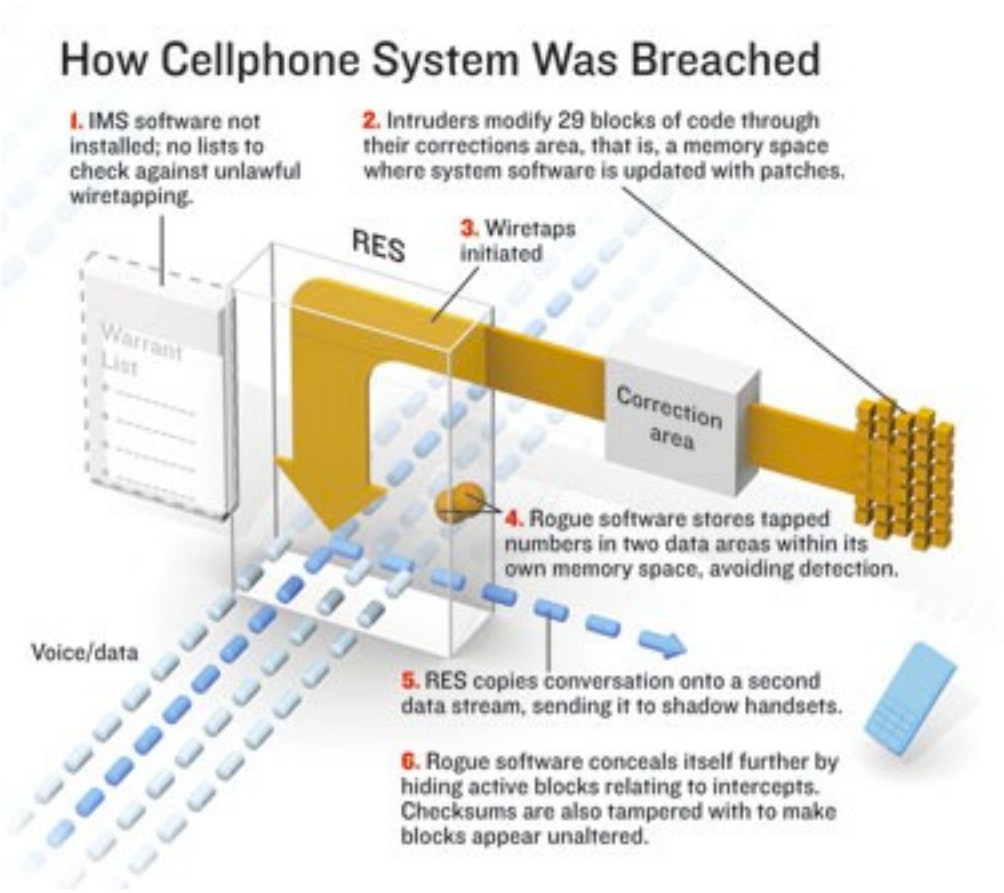
1. The warrant list is updated by using the IMS's "Warrant Record" dialog box.

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.

The Athens Affair



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.

The Athens Affair: Q&A

The Athens Affair: Q&A

- Why were the attackers not detected...

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator’s management center?

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator’s management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator's management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead
  - In process lists?

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator's management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead
  - In process lists?
    - Attackers modified the process list showing active blocks to hide the running interception blocks (as a root kit would modify the ps command on a Linux device)

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator’s management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead
  - In process lists?
    - Attackers modified the process list showing active blocks to hide the running interception blocks (as a root kit would modify the ps command on a Linux device)
  - By upgrade and verification engineers?

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator's management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead
  - In process lists?
    - Attackers modified the process list showing active blocks to hide the running interception blocks (as a root kit would modify the ps command on a Linux device)
  - By upgrade and verification engineers?
    - Attackers modified checksums on code blocks to avoid being detected when operators verified the old blocks before inserting new code into the corrections area, changing the block (also as a root kit would be able to)

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator’s management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead
  - In process lists?
    - Attackers modified the process list showing active blocks to hide the running interception blocks (as a root kit would modify the ps command on a Linux device)
  - By upgrade and verification engineers?
    - Attackers modified checksums on code blocks to avoid being detected when operators verified the old blocks before inserting new code into the corrections area, changing the block (also as a root kit would be able to)
  - In logs?

The Athens Affair: Q&A

- Why were the attackers not detected...
  - In operator’s management center?
    - No IMS system in place, this would have shown the tapped phones, now, nothing was shown instead
  - In process lists?
    - Attackers modified the process list showing active blocks to hide the running interception blocks (as a root kit would modify the ps command on a Linux device)
  - By upgrade and verification engineers?
    - Attackers modified checksums on code blocks to avoid being detected when operators verified the old blocks before inserting new code into the corrections area, changing the block (also as a root kit would be able to)
  - In logs?
    - The command parser was rewritten to not log certain commands if a special sequence of characters was input (six spaces)

The Athens Affair

- Outcome
  - Vodafone Greece were fined 76 million USD
  - The head of the network operations was found hanging from his ceiling (possibly unrelated, no information disclosed)
  - Follow up questions to keep in mind
    - What was the driving factors between the successful wiretap?
    - By at least which four means could this have been discovered (but was not, and why)?

Current telecom security trends

Current telecom security trends

- Threats against infrastructure
- Mobile Network Security
- Customer focus on security

Threats Against Infrastructure

- Motivation
  - Tools and knowledge for attacks against exposed interfaces of mobile network infrastructure are widely available
    - Currently mainly targeting GSM air interface
  - "Hacker"/security researcher interest is high
    - A new frontier to explore
  - Operators and governments are getting concerned
    - Performing their own tests
    - Likely coming requirements related to cybersecurity/assurance

Mobile Network Security

Mobile network security has become a hot topic in the hacker community

- Hacking phones
  - Jailbreaking iPhones & rooting Android phones (privilege escalation)
  - Looking for remotely exploitable vulnerabilities
    - Binary SMS
    - Baseband stack
- Search for vulnerabilities in the infrastructure
  - Academic work
    - Design principles and DoS [Ricciato et al., 10]
  - Hacking talks & demos
    - RACHell, IMSI Flood, IMSI Detach, … [Blackhat]
  - In Real Life
    - HSS/HLR attack – privacy issue (shady operator business)
    - SMS Spam origination
    - Fraud using interconnect [P1 Security]
- Market reports on infrastructure security
  - Heavy Reading report Nov -10

Customer focus on security

- An increasing focus on security from customers
  - More security oriented queries
  - More feature requests

  - Customers assume, rather than query, that certain documents are available
  - Fines, e.g., India DoD

  - Likely will security be a competitive advantage in the future

Working as a system manager with security focus at Ericsson

Ajilon

ulf.larson@ajilonconsultants.se

www.ajilonconsultants.se

Working as a system manager with security focus at Ericsson

- Plan security work for future releases together with product management and design

- Run feature investigations, i.e., translate requirements from product management or customers to feature implementation overview for designers

- Perform security activities before release deadlines (twice a year)
  - Risk assessment
  - Vulnerability assessment
  - Update Node Hardening User Instruction

Working as a system manager with security focus at Ericsson

- Q&A expert in security related matters
  - "From which release do you support YYY"
  - "Is the initialization vector for GEA3 random or always zero?"
- Supervise thesis workers

Working as a system manager with security focus at Ericsson

- And last but not least ... Can you guess it?

Working as a system manager with security focus at Ericsson