Telecom System Security

Presented By: Rami Ailabouni

Based on: Ross Anderson's Book "Security Engineering"

Lecture Contents

- Telecom System: Introduction and Importance
- Early Telecom Systems: Vulnerabilities, Attackers and Attacks
- Telephone Systems: Vulnerabilities, Attackers and Attacks
- Mobile Phones: 1st Generation: Vulnerabilities, Attackers and Attacks
- Mobile Phones: 2nd Generation (GSM): Mechanism, Vulnerabilities
- Mobile Phones 3rd Generation (UMTS): Improvements Over GSM
- Billing Mechanisms Problems
- Mobile Phones Supply Chain VS Security
- Summary

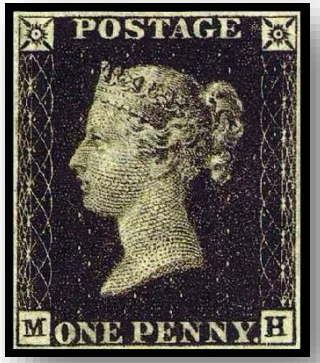
Telecom System

- Tele = Distance, Com = Communication
- System that allows the exchange of information between two entities
- Types of communication systems:
  - Visual signals: smoke signals, signal flags
  - Wired signals: electrical telegraphs (wired version), telephone systems
  - Wireless signals: radio, mobile phones
  - Combination: internet
  - None of the above: postage

- Why is it so important to secure Telecom systems ?

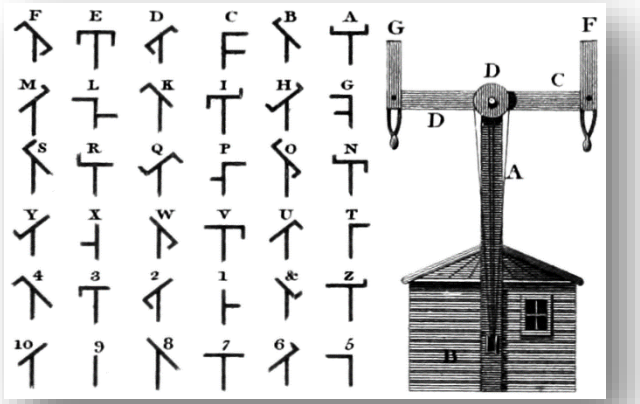
Early Telecom Systems: Postage

- Postage: at first was paid by the recipient
  - Do you see any problems with that ?
- “Solution”: the recipient was allowed to inspect letter and reject it rather than paying for it
  - People started sending short messages to each other on the covers of the letter
  - Recipient read the message and rejected it
- Solution: sender is responsible for paying for the message he sent



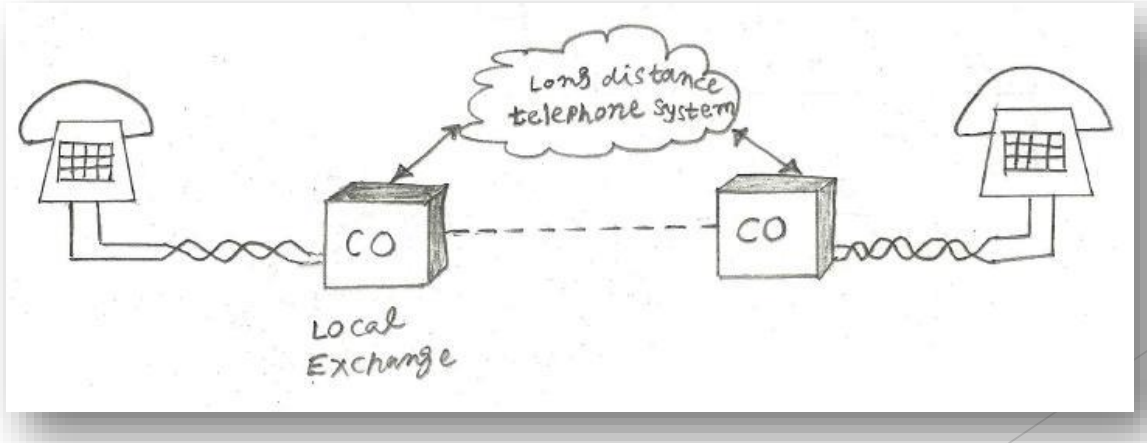
Early Telecom Systems: Telegraphs

- Many types of telegraphs were introduced during the history
- Semaphore telegraph, heliograph, electrical telegraph, etc…
- Used a code to transfer messages: Chappe system, Morse code, etc…
- All of them had their own problems and ways to abuse
- One story is about heliograph and the bets on races



Telephone Systems

- Telephone was invented by 1876, Alexander Graham Bell
- Shortly after that, Hungarian engineer Tivadar Puskás invented the telephone switch, which allowed the formation of telephone exchanges
- Since then many companies offering telephone services were founded
- Basic Telephone system was built of:
  - Back-end Telephones
  - Wires: at first one wire for background signaling and voice, then two separated wires
  - Exchange systems: at first manual then automatic



Telephone Systems

- Since their early days (1877) telephones and the telephone systems were precious target for attacks, each attack was for a different purpose
- Attackers:
  - Phone phreaks: people who love to explore the telephone system, spent hours dialing over the network system to:
    - Find network secrets and problems
    - Dialing without getting charged
  - Police and intelligence agencies to wiretap others
  - Gangs and crooks to evade police wiretapping, to communicate with other gangs' members without getting caught, and to earn money
  - Phone companies attacked other phone companies and their customers
- For each attack some of the defensive measures taken were expensive (billions of $) and/or inadequate

Attacks on Exchange Systems (1)

- Early days: exchange system were manual; an operator sat in the exchange room and connected the two lines together
  - There was no way for that operator to know who is calling
  - Operator started to call back the number given (specially internationals), attackers started to call from callboxes
  - A feature was installed in callboxes to signal that the call is coming from a callbox and not from a private phone
    - It had a BUG!, pressing the “rest” button for quarter a second will disconnect the call from the callbox and call again but now without the signal that the call was from a callbox

Attacks on Exchange Systems (2)

- Exchange systems became automatic
  - Computers running Unix systems
- Kevin Poulsen, a computer hacker/phone phreak from California succeeded to hack to these systems and get a root access 1985-1988, some of his actions were:
  - Calling phones for free
  - Unlawful wiretapping and espionage
  - Obtaining unlisted numbers of celebrities
  - He even won a Porsche from Los Angeles radio station KIIS-FM

Attacks on Exchange Systems (3)

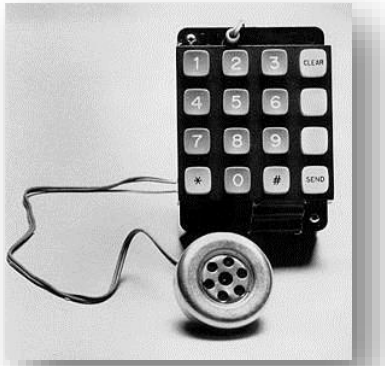
- Intelligence agencies planted backdoors in exchange systems exported to other countries
- These backdoors were used to wiretap the foreign importing countries and even to crash the whole phone system during wartime
- A story about USA invasion of Afghanistan in 2001:
  - Kabul had two exchanges: an old electromechanical one and a new electronic one
    The USAF bombed only the first of these

Physical Attacks on Wiring Systems

- Also called *clip-on*
- Physically attaching a phone to someone else's line to steal their service
- A story about a family from Cramlington, a town in the North East of England in the 1970's
  - Drug dealer used their phone line to:
    - Call his gang members
    - Evade police surveillance
- Solution: challenge response protocol between a wall-socket and the exchange software before a dial tone is given

Non-Physical Attacks on Wiring Systems

- Until the 1980s, phone companies used signaling systems that worked *in-band* by sending tone pulses in the same circuit that carried the speech
- Calling a number and sending a 2600Hz tone disconnected the called party while leaving the caller with a trunk line connected to the exchange, giving him the ability to call a new number for free
- Lucky gifted guys could whistle the 2600Hz tone into the phone speaker and get free calls
- Less gifted guys typically used home-made tone generators, called Blue-Boxes which could generate the 2600Hz tone
- Solution: spending many years and billions of $ to move signaling out of-band, in separate channels



Attacks on User Equipment - PBXs

- Private branch exchange: is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines
- Feature: to allow an external line to call any other external line through it.
- its purpose was allow company's workers to work from home and take the advantage of the low rates a large company can get for long distance calls
- PIN codes were set to default and never changed
- PBXs had at least one backdoor installed to give easy access to law enforcement and intelligence agencies (it's said, as a condition of export licensing)
- Many PBX designs have fixed engineering passwords that allow remote maintenance access
- A story about the Chinese gang in Britain

Social Engineering

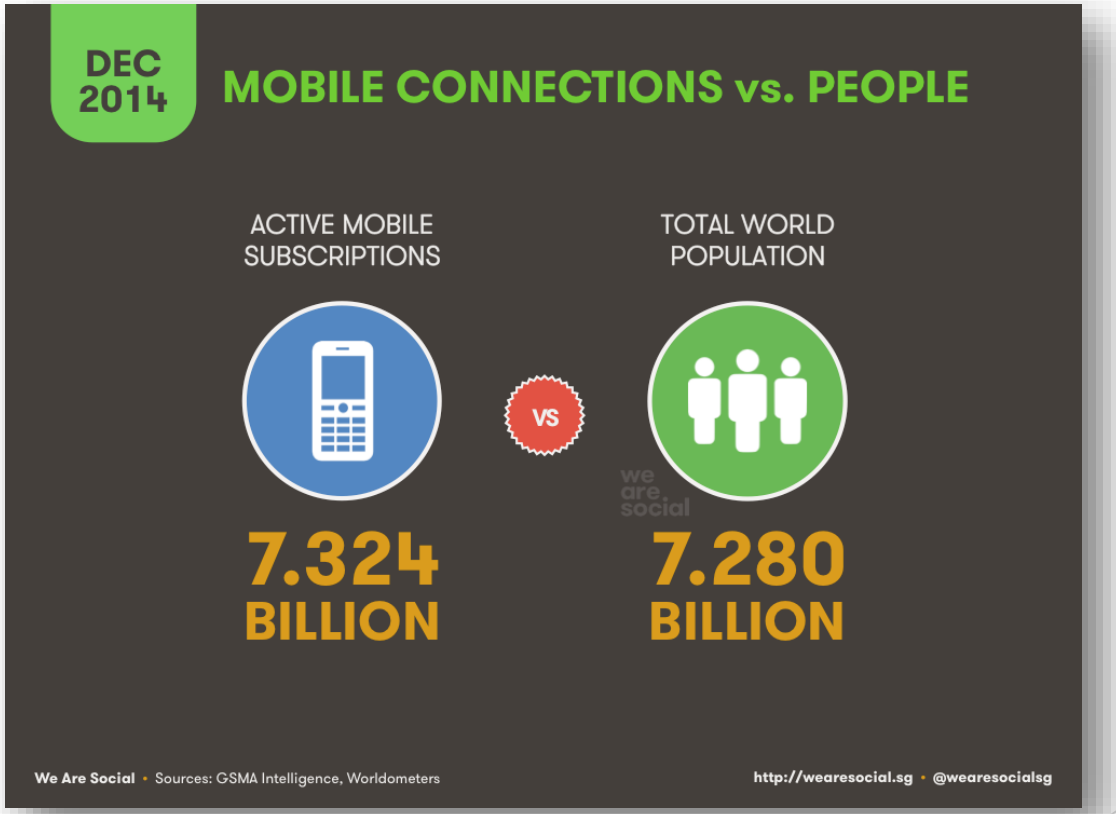
- Social Engineering was always the most wide spread and “most affordable” way to break a system’s security
- ’Companies can spend millions of dollars toward technological protections and that’s wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer’s defenses or reveals the information they were seeking’

  - Kevin Poulsen

- This part of the book has many stories about social engineering, here’s two of them:
  - AT&T “security“
  - Prisoners of a correctional center in Washington state

Mobile Phones

- Since their beginnings as an expensive luxury in the early 1980s,mobile phones have become one of the big technological success stories



First Mobile Generation (1)

- Used analog signals (bad quality calls + so hard to be encrypted)
- Mobile phone sent its own serial numbers (equipment s/n + subscribers s/n) in clear over the air link
- Simple devices were built to capture these number from calls in the neighborhood
- Even more: fake base stations were used to steal the serial numbers from a place with a lot of mobile traffic like a highway/airport
- Cloned phones with these numbers were developed and sold in the black market
- Even more: gangs developed “tumbler” phones which used different identity for each call to evade police tracking

First Mobile Generation (2) - Solutions

- A number of heuristics were developed, For example:
  - Genuine mobiles which roam and call home regularly, but then stop calling home, have usually been stolen
  - Too-rapid movement indicators: calls being made from New York and LA within an hour of each other) and even just a rapid increase in call volume or duration
- Signal characteristics that arise from manufacturing variability in the handset's radio transmitter were used to identify individual devices and tie them to the claimed serial numbers
  - More effective: it was used by Vodafone in the UK to almost eliminate cloning fraud from analogue mobiles
  - More expensive: it involved modifying the base stations

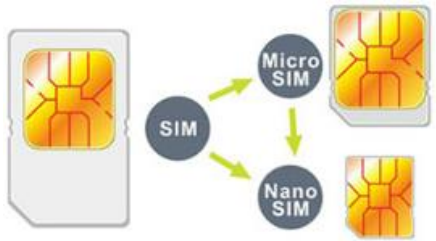
Second Mobile Generation - GSM

- Global System for Mobile communication – founded 1987
  - First service was launched in 1992
- Digital signals – better quality calls
- More secured
- Ability to send text messages
- Set out to secure the system against cloning and other attacks

GSM Network

- Each network has two databases:
  - Home Location Register (HLR): contains data about its own mobiles
  - Visitor Location Register (VLR): contains data about mobiles that roamed in from other networks
- Handsets are commodity items, has no personal data about the subscriber
- They are personalized using a Subscriber Identity Module (SIM)
- SIM contains three numbers:
  - PIN code: to stop stolen mobiles from being used
  - International Mobile Subscriber Identification (IMSI): maps to your mobile phone number (subscription)
  - Subscriber authentication key K_i, a 128-bit number: serves to authenticate that IMSI and is known to your home network

Known to HLR

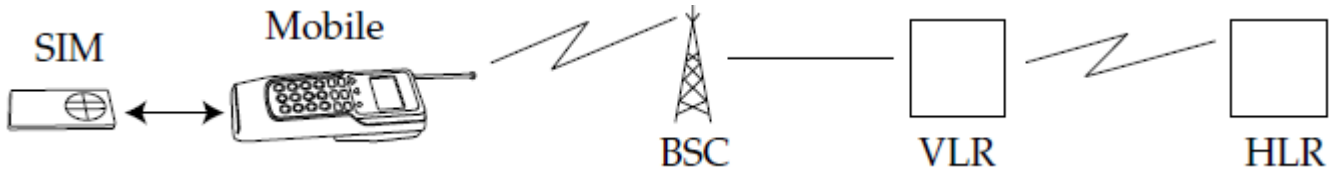


GSM Authentication Protocol

- On power-up, the SIM may request the customer's PIN; if this isn't configured, or once it's entered correctly, this authentication protocol runs:

1) SIM → HLR IMSI
2) HLR → BSC $(RAND, SRES, K_c)$
3) BSC → SIM RAND
4) SIM → BSC SRES
5) BSC → mobile $\{traffic\}_{K_c}$

$E_{ki}(RAND) = SRES \mid K_C$



GSM Authentication Protocol – Vulnerabilities (1)

- Communication between base stations and the HLR pass unencrypted (step 2)
  - Any attacker could send an IMSI of his choice and listen to the communication BSC <-> HLR and know how to en/decrypt traffic
- $E_{ki}(RAND) = SRES | Kc$ of step 2: encryption used a one-way function called Comp128, which turned out to be vulnerable to cryptanalysis.
- Attack: 150,000 chosen challenges to extract the key K_i ~ several hours using software that is now freely available

- **Bottom Line: Having the IMSI of someone's SIM means that you can wiretap his device**

GSM Authentication Protocol – Content Confidentiality Vulnerabilities (2)

- E_{Kc}(traffic) - step 5: traffic was encrypted using the algorithms A5/1 or A5/2 (A5/1 was commonly used in Europe, better than A5/2)
- A5/1 used a 64-bit key and was broken by an attack using a lot of FPGAs that is sold for about $1m
- Optimizations and tradeoffs on the attack by Adi Shamir and Alex Biryukov (1999) led to breaking it using a (< 128MB) precomputed data (movement tables) and:
  - 2 seconds of traffic data and several minutes of processing time on a PC (**The Random Subgraph attack**)
  - 2 minutes of traffic data and one second of processing time on a PC (**The Biased Birthday Attack)**
  - NOTE: Comp128 and A5/1 were kept secret and broken shortly after reverse engineering them. (Importance of Kerckhoffs' Principle)

GSM Authentication Protocol – Location Security Vulnerabilities (3)

- Mechanism: Once a mobile is registered to a network, it is issued with a temporary mobile subscriber identification (TMSI),which acts as its address as it roams through the network
- The Attack: a device called an IMSI-catcher
- Typically operated in a police car tailing a suspect, pretended to be a GSM base station, the suspects mobile tries to register with it (as its signal is stronger)
- The IMSI-catcher claims not to understand the TMSI, so the handset helpfully sends it the clear text IMSI
- The attack depended on the fact that the handset (SIM) never verifies the network

Solution

- Third Mobile Generation – 3gpp (UMTS): used A5/3 which is based on a strong block cipher known as Kasumi

GSM: SUCCESS/FAILURE? (1)

- Depends on whom you ask!
- From cryptography's point of view: FAILURE
  - Comp128 hash function and A5/1,2 encryption algorithms were broken once they became public
- From the point of view of phone companies: SUCCESS
  - Shareholders of GSM operators like Vodafone have made vast amounts of money, The money they've lost after GSM vs the money they've gained is incomparable
- From criminals' points of view: FINE
  - It did not stop them from stealing phone services, only the method of stealing and what to steal changed

GSM Security : SUCCESS/FAILURE? (2)

- From the point of view of customers: Disaster
  - GSM was sold as being completely secured, customers believed that!
  - But it was harder for the victim to prove he's innocent since companies can always claim that it was the victim's SIM card and PIN code which were used to make the thousands of dollars bill calls

- **Bottom line : GSM didn't help the subscriber much but did help the network companies a lot !**

Third Mobile Generation – 3gpp (UMTS)

- 3rd Generation Partnership Project / Universal Mobile Telecommunications System
- 1st appearance 2001 Japan – In Israel since 2005
- Security is much the same as GSM but upgraded to deal with number of known GMS's vulnerabilities, main advantage over GSM is the higher speed rates

G2 VS G3

- Speed: Instead of 9.6kb/s of GSM and tens of kilobits per second of GPRS, 3gpp offers a rate of hundreds of thousands to millions of bits per second
- Cryptography: A5/1, A5,2 and Comp128 in G2 were replaced with a various modes of operations of a block cipher called A5/3 (Kasumi) in G3
- G3 protocol was public and stood public scrutiny
- Cryptography is used to protect the integrity and confidentiality of both message content and signaling data, the protection is from the handset to the main node and not just to the local base station
- Authentication: The authentication is two-way rather than one way, ending the vulnerability of rogue base stations (IMSI catchers)

UMTS Authentication Protocol

- The Home Location Register (HLR) is now known as the *home environment* (HE)
- SIM is now know as the *UMTS SIM* (USIM)

1) $\text{USIM} \rightarrow \text{HE}$ IMSI (this can optionally be encrypted)
2) $\text{HE} \rightarrow \text{VLR}$ $\text{RAND}, \text{RES}, CK, IK, SEQ \oplus AK, MAC$
3) $\text{VLR} \rightarrow \text{USIM}$ $\text{RAND}, SEQ \oplus AK, MAC$
4) $\text{USIM} \rightarrow \text{VLR}$ RES

- Step 2: HE generates: $E_{k_i}(\text{RAND}) = (RES|CK|IK|AK)$
- MAC is computed on RAND and SEQ, USIM verifies it (2-way verification)

Billing Mechanisms Problems

Problems with the billing mechanisms affected customers and phone companies, here are some of these problems:

- Problem 1 (specially with prepaid phones): A call detail record is only generated once the calling phone goas on-hook
- Problem 2: Accounting system was designed in the time phone companies were sleepy government departments or national monopolies, so it has little in the way of audit and non-repudiation.
- Problem 3: Phone companies wanted to be able to charge for high value services. billing programs and mechanisms became (in a short time) more complex and which added many bugs during their development
- Problem 4: If a malware becomes widespread on mobile phones then every customer who has an infected phone will be able to be charged for all sorts of goods and services by getting his phone sending messages of buying new services

Mobile Phones Supply Chain VS Security

Security is made more difficult and complex to follow by the long and complex supply chain:

- Intellectual Property companies like ARM own the chip design
- Foundries like Infineon make the chips
- Handset designers like Samsung manufactures the actual mobile handset
- Symbian, Android provides the operating system with the software compatible with it (which uses location services, credit card, pictures, handsets memory, handsets contacts …)
- Network operator provides the national infrastructure + services

- **Keep in Mind: "A chain is only as strong as its weakest link”**

Summary

- We've talked about the importance of telecom systems in our lives, why it is crucial for attackers to control them and why it is more crucial to defend them
- We've seen that many security problems were there because security wasn't one of the important concepts taken in mind when new systems were developed
- Security was added later to protect companies and then to protect clients (if it did)
- Not thinking about security before/when you develop a system will cause you a lot of pain and money to fix what was attacked
- Device security is not just the responsibility of who develops it but also the operator/people that operate/use it
- There are two kinds of fools. One says, "This is old, therefore it is good." The other says, "This is new, therefore it is better"

Dean William Inge

Questions ?

THANK YOU

Rami Ailabouni