TELECOM SYSTEM SECURITY

Firas Hiadry

Based on Ross Anderson’s “security engineering” chapter 20
LECTURE CONTENTS

Introduction and Importance
Early Telecom Systems
Attacks on Exchange Systems
Social engineering
Mobile Phones: 1st Generation
Mobile Phones: 2nd Generation (GSM)
Mobile Phones: 3rd Generation (UMTS)
Summary
Communication is a process in which information is transferred from source to destination.

Information can be in any form e.g. Voice, Data, Video, Graphics etc. Voice communication is the simplest mode of communication.

People also use facial expressions and body language to communicate with each other.

Types of communication systems:
- electrical telegraphs.
- radio, mobile phones.
- internet.
- postage.
WHY IS IT SO IMPORTANT TO SECURE TELECOM SYSTEMS?

CAN WE GET A LEVEL THAT WE DON’T NEED TO SECURE MOBILE PHONES MORE?
OUR TOM & JERRY STORY
EARLY TELECOM SYSTEMS: POSTAGE, TELEGRAPHS

Postage:
- Postage was paid by the recipient.
- Unsolicited mail became a huge problem.
- 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, and then rejected it.
- Sender is responsible for paying for the message he sent.

Telegraph:
- People used The early optical telegraphs to place foreknowledge bets on races.
In the 1950’s, the operator in some systems had to listen for the sound of coins dropping on a metal plate to tell that a callbox customer had paid.

Other problems:
- The operator had no way of knowing which phone a call had come from, so she had to ask the caller his number.
- People did it from call boxes.

Solution: call box lines had a feature added to alert the operator if the call is coming from a callbox.

There was a bug: “rest” button.
➢ Another solution:
   • Exchange systems became automatic

➢ 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
physically attaching a phone to someone else’s line to steal their service.

In the 1970’s students used the clip-on method to call home.

a true story!! a family in Cramlington, a town in the North East of England.

Drug dealer used their phone line to:
• Call his gang members.
• Evade police surveillance.
It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

AT&T Security example.
1. Don’t open emails and attachments from suspicious sources.
2. Use multifactor authentication.
3. Be wary of tempting offers.
4. Keep your antivirus/antimalware software updated.

SOCIAL ENGINEERING PREVENTION
Two stories of telephone manipulation involve feature interaction.

- A number of directory-enquiry services will connect you to the number they’ve just given you, as a service to motorists who can’t dial while driving.
- British Telecom launched a feature called ‘Ringback’.
Since their beginnings as an expensive luxury in the early 1980s, mobile phones have become one of the big technological success stories.

According to GSMA real-time intelligence data, there are now over 9.42 Billion mobile connections worldwide, which surpasses the current world population of 7.75 Billion implied by UN digital analyst estimates.

- World Population: 7,756,112,125
- Mobile Connections: 9,426,128,300
- Unique Mobile Subscribers: 5,179,425,550

It’s important to state that not every person in the world has a mobile device. We’re talking mobile connections that come from people with multiple devices, and a fraction with dual SIM’s or other integrated devices like cars.

Sources: WorldMeters U.N. data, GSMA Intelligence
➢ used analog signals with no real authentication.
➢ The handset simply sent its serial numbers in clear over the air link.
➢ villains built devices to capture these numbers from calls in the neighborhood.
➢ Cloned phones with these numbers were developed and sold in the black market.
➢ criminals: enterprising engineers built mobile phones which used a different identity for each call. Known as tumblers, these were particularly hard for the police to track.

➢ Using fake base station to steal a serial numbers.
Several heuristics were developed in order to stop the frauds.

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. It was used by Vodafone in the UK to almost eliminate cloning fraud from analogue mobiles.

Another proposed solution was to adopt a cryptographic authentication protocol, but there are limits on how much can be done without changing the whole network.
SECOND MOBILE GENERATION - GSM

- Good speech quality, mobile phones adopted digital technology.
- Low cost of phones.
- International roaming.
- Separating the Subscriber Identity from the Device Identity.
- Ability to send text messages.
Each network has two databases:
- HLR (home location register): contains the location of its own mobiles.
- VLR (visitor location register): contains data about mobiles that roamed in from other networks

First time using a subscriber identity module (SIM).

The SIM contains three numbers:
- personal identification number (PIN): that you use to unlock the card. In theory, this stops stolen mobiles being used.
- international mobile subscriber identification (IMSI): a unique number that maps on to your mobile phone number.
- subscriber authentication key ($k_i$): a 128-bit number that serves to authenticate that IMSI and is known to your home network.
What is GSM?
GSM AUTHENTICATION PROTOCOL

• Whenever the sim card is activated it sends the IMSI to the closest base station. The base station authenticates the phone by using a challenge response protocol.

SIM → HLR
HLR → BSC
BSC → SIM
SIM → BSC
BSC → mobile

IMSI
(RAND, SRES, Kc).
RAND
SRES
{traffic}Kc
On power-up, the SIM request the customer’s PIN.

The mobile sends the IMSI to the nearest base station.

Nearest base station sends the IMSI to the HLR.

The relationship between these values is that RAND, encrypted under the SIM’s authentication key Ki, gives an output which is SRES concatenated with Kc:

\[ (\text{RAND})_k = (\text{SRES} | \text{Kc}) \]

The standard way to do this encryption is using a one-way function called Comp128, or A3/A8.

HLR generates five triplets. Each triplet consists of:
- RAND, a random challenge
- SRES, a response
- Kc, a ciphering key

HLR sends RAND, SRES, Kc to the nearest base station.
5. Nearest base station sends RAND to the mobile.

6. Mobile sends RAND to SIM.

7. SIM sends SRES to mobile.

8. Mobile sends SRES to the nearest base station.

If SRES that BSC (base station, the cell) has is the same as returned by the device, the connection between the device and the network is open.
GSM AUTHENTICATION PROTOCOL VULNERABILITIES

➢ In most countries the communications between base stations and the HLR pass unencrypted on microwave links.

➢ Triples can be replayed.

➢ The introduction of GSM caused significant shifts in patterns of crime generally.

➢ The GSM system is supposed to provide two further kinds of protection location security and call content confidentiality.
SO WAS MOBILE SECURITY A SUCCESS OR A FAILURE?

➢ Whether mobile-phone security has been a success or a failure depends on whom you ask.

➢ From the point of cryptography’s view: failure.

➢ From the phone companies’ point of view: success.

➢ From the criminals’ point of view: fine.

➢ From the customer’s point of view: failure.
The third generation of digital mobile phones was initially known as the Universal Mobile Telecommunications System (UMTS).

These systems are now available everywhere.

The security is much the same as GSM.

It was upgraded to deal with a number of GSM’s known vulnerabilities.

IMSI-catchers don’t work against third generation mobiles.
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).
FRAUDS BY PHONE COMPANIES

➢ **Cramming**: the company may say ‘Can we call you right back?’ and if you agree then you’re deemed to have accepted the charges, which are likely to be at a high premium rate. The same can happen if you respond to voice prompts as the call progresses.

➢ **Ross Anderson’s example.**

➢ **Slamming**: the unauthorized change of a subscriber’s long distance telephone service provider without their consent.

➢ **fly-by-night phone company.**
BILLING MECHANISMS

➢ The security of the billing mechanisms covers a much wider range of issues. For example:

I. A call detail record (CDR) is only generated once the calling phone goes on-hook.
II. The back-end accounting system was designed in the days when phone companies were sleepy government departments or national monopolies, and there were no premium-rate services through which real money could be extracted from the system.
III. The phone companies also want to be able to charge for relatively high value product and service delivery.
IV. If malware becomes widespread on mobile phones, then the botnet herders who control subverted phones will be able to pay for all sorts of goods and services by getting infected machines to send text messages.
SO HOW CAN PHONE PAYMENT SYSTEMS BE IMPROVED?

ONE PROPOSED WAY OF IMPLEMENTING THIS IS TO INCORPORATE A MICROPAYMENT MECHANISM.

THE INDUSTRY’S PROPOSED SOLUTION IS TO REDESIGN THE CALL DATA RECORD TO CONTAIN A LOT MORE INFORMATION.
Andrew Odlyzko, a scholar of phone-company economics, suggests the eventual way forward will be fixed-price contracts.
SUMMARY

➢ Security was added later to protect companies and then to protect clients.

➢ If security isn’t one of the building blocks, implementing it later will be hard and sometimes useless.

➢ Can we get a level that we don’t need to secure mobile phones more?
Thank you!