Telecom system security

Nitay Duek

Based on Ross Anderson’s “security engineering” chapter 20
Lecture content

- Phone phreaking.
- Mobile phones.

Phone Phreaking

-Phreaking is a slang term similar to hacking, meaning “interacting with a system in an unexpected way”.

http://www.digitaltrends.com/apple/phone-phreaking-archive-available-online/#/ HKXjd
Phone Phreaking - Signaling

-Until the 80s phone companies used the same physical line for both speech and background signaling.
Phone Phreaking - Signaling cont’

-The User makes a regular call.
-Produce a specific tone (2600 Hz typically).
   The tone clears the line on the other side, and the user is left with a clear, payed line.
-Later, the same kind of attacks was used to discover and abuse wiretapping signals that the police and agencies used.

-Phone companies slowly built new lines.
Phone Phreaking - Exchanges

- New UNIX based exchanges developed. Thus exposing the system to attacks on the exchange itself.
- A popular target was unlisted celebrity numbers.
-Countries were afraid to purchase exchange and phone systems from foreign countries.
Phone Phreaking - End Systems

- Many products had big security vulnerabilities in them.
- PBXs make a great example.
- A PBX, Private Branch Exchange. Is a local telephone exchange. Meant to deal with internal calls and be able to make and receive external calls too.
-PBXs came with a special PIN number that enabled low cost calls to long distance numbers. These became known with time and widely used.
- New PBXs had a built in remote maintenance option.
- A good feature on one hand. A huge security vulnerability on the other.
A big scale attack of this kind was made in Britain. Over 1 million pounds worth of calls were made to China from some local district council PBX.
Phone Phreaking - End Systems cont’

-The reason behind these kind of attacks is not the free calls, but the anonymity and lack of wiretapping.
Phone Phreaking - End Systems cont'

- Conclusions:
  - Think about security!
  - Expect the unexpected.
Mobile Phones

-Started at the 80s
-Today the number of mobile phones subscriptions is 6 billion!
Mobile Phones - Cloning

- First generation mobile phones, as with any new technology did not have security features.
- To call, a handset would send its serial number in plain text.
- The base station would then bill the call to that serial number.
Mobile Phones - Cloning cont’

- An attacker with the right equipment could listen to these serial numbers and bill calls to them.
Mobile Phones - Cloning cont’

-A proposed solution was to use cryptography. The problem was that it required hardware changes which are pricy.
-Cloning ended only in the next generation of phones.
Mobile Phones - GSM

-The GSM project security standards was to be “as good as a wire line”
-The security policy was to keep all the crypto secret.
-This decision was the source of many security vulnerabilities later on.
Mobile Phones - GSM cont’

- So how GSM works.
- Each handset must contain a SIM card (Subscriber Identity Module). The SIM cards are unique, and contain 3 important numbers.
Mobile Phones - GSM cont’

- PIN, a number used by the user to open the SIM card.
- IMSI, the phones ID.
- K, a cryptographic key.
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.
Mobile phones - GSM

- The values are related as follows:
  Encrypt\_K(RAND) = RES | Kc.
- Kc will be the session’s encryption key.
Encrypt_K(RAND) = RES|Kc

Encrypt_K(traffic) = RES

Generate: RAND, RES, Kc

IMSI

RAND

RES

User

base station
Mobile phones - GSM cont’

-The original encryption function used in GSM initialization is called comp128.
-Quickly after the design leaked many attacks were found on comp128.
Mobile phones - Attacks on GSM

-Another problem was that the base station traffic with the company’s databases was not encrypted or authenticated.
Mobile phones - Attacks on GSM cont’

-The call encryption algorithm was A5.
-A5 was also designed in secret, and again, once the design leaked, many attacks were found.
-Later, a new and more secure version was introduced and called A5/3.
- A5, or A5/1 had an even weaker variant, A5/2.
- First world countries used A5/1, all other countries (Israel included) used A5/2.
- A5/2 is still being used today.
Mobile phones - 3G

-It is the latest phone network protocol.
-3G’s security goals was to achieve what GSM tried to. and support 2 way authentication.
-The whole protocol was public and stood public scrutiny.
Mobile phones - 3G cont’

3G protocol: Uses the same values as GSM.
- 3G uses some additional values.
- **Ki**: The integrity key, used for authentication
- **Ka**: The anonymity key, used to encrypt SEQ.
- **SEQ**: A sequence number that changes every connection, used to authenticate the network.
Encrypt_K(RAND) = RES|Kc|Ki|Ka
Mobile phones - 3G cont’

-3G achievements: It is not a revolution in terms of security, but it achieved what GSM meant to achieve.
To who?

In the users perspective, it’s hard to bill to you calls that you did not do.

Authorities and criminals with enough effort can still get to your calls.

A small improvement.
Mobile phones - success or failure

- In the telephone company’s perspective cloning is not an issue any more which is a great success.
- Users can’t get free calls or anything like that.
- Pretty good for the phone companies.
Mobile phones - success or failure

- From an attacker's point of view it requires more effort to attack the users or the company’s, and no free phones by cloning.
- Attackers are in a worse situation, but not that worse.
Mobile phones - success or failure

-Big intelligence agencies are also fine, they have the capabilities to get the data anyway.