Telecom System Security

“Security Engineering", chapter 20
Ross Anderson

Computer security seminar
Ksenia Vais
27/04/2017
Phone Phreaking

Abuse of communication services:

• Before the invention of the stamp, postage was paid by the recipient (not fair!).

• The early optical telegraphs.
Attacks on Metering

• The one of the easiest phreaks took place in the 1950’s. The operator in some systems had to listen for the sound of coins dropping on metal plate to tell if the callbox user had paid.
• Press the “rest” button for a quarter.
• “magic buttons”.
Attacks on Metering

- *Clip – on*: 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 family from Cramlington started to notice that something was wrong with their phone line.
Attacks on Metering

- Stealing dialing tone from cordless phones.
- Social engineering.
Attacks on Signaling

• *In-band* - sending tone pulses in the same circuit that carried the speech.
• Sending 2600Hz tone would clear down the line of the recipient of the call.
• Joe Engresia - could make free phone calls by whistling a tone he’d heard in the background of a long-distance call.
• *blue boxes* – type of home-made tone generators.
• The phone companies spent years and many billions of dollars upgrading exchanges so that the signaling was moved out *off-band*, in separate channels to which the subscribers had no easy access.
Attacks on Switching and Configuration

• Computers that did the switching were the next target of the attackers. Typically these were Unix machines on a LAN in the exchange.

• Attacking the less protected machines, the hackers could go across the LAN and break into switching equipment.

• Using these techniques, unlisted phone numbers could be found, calls could be forwarded without a subscriber’s knowledge, etc.
Attacks on Switching and Configuration

• Kevin Poulsen - got root access to many of PacBel’s switches and other systems in 1985–1988.

• FBI - attacks on phone company computers can be used by foreign intelligence agencies.

• Countries that import their telephone exchanges rather than building their own, found themselves in a trouble.

• Many attacks on switching involve insiders, who can misconfigure systems to provide free calls from (or through) favored numbers (Social engineering).
Attacks on Switching and Configuration

• Kevin Mitnick – “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”.

• All sorts of people have access to the switching.

• Telcos migrate their networks to IP, and they start to converge with VOIP services that give users access to the IP layer.
Insecure End Systems

- Answering machines.
- Phone company switches that give you dial tone twelve seconds after the other party hangs up.
Insecure End Systems

- Attacks on corporate private branch exchange systems.

- PBX at Scotland Yard was compromised and used by villains to refile calls, costing the Yard a million pounds.

- In another case, Chinese gangsters — hacked the PBX of an English district council.

- Most companies don’t understand the need to guard their ‘dial tone’ and don’t know how to even if they wanted to.

- Moldova Scam.

- Udi Manber – “tricking” the answering machine.
Feature Interaction

• More and more cases of telephone manipulation involve feature interaction.
• Inmates at the Clallam Bay Correctional Center.
• Voice dialing.
• Call forwarding is a source of many scams. For example, a fraudster may tell a victim to confirm her phone number with the bank by dialing a sequence of digits — which forwards her incoming calls to a number controlled by the attacker.
• ‘Ringback’ - If you dial an engaged number, you can then enter a short code and as soon as the called number is free, both your phone and theirs will ring.
• Conference calls.
Mobile Phones

- **1st generation**: Used analog signals.

- The device simply sent its serial numbers in clear over the air link. So villains built devices to capture these numbers from calls in the neighborhood.

- *Tumblers* - mobile phones which used a different identity for each call.

- Fake base station.
Mobile Phones

- Several heuristics were developed in order to stop the frauds.

- RF fingerprinting — are used to identify individual devices and tie them to the claimed serial numbers.
Mobile Phones

- **2nd generation:**
  - Digital technology.
  - GSM - Global System for Mobile Communications.
  - HLR - home location register.
  - VLR - visitor location register.
  - HLR and VLR: These databases enable incoming calls to be forwarded to the correct cell.
  - SIM - subscriber identity module. The SIM can be thought of as containing three numbers: personal identification number, IMSI - international mobile subscriber identification, subscriber key Ki - 128-bit number that serves to authenticate that IMSI and is known to your home network.
Mobile Phones

• Authentication protocol:
  1. 
  2. 
  3.
Mobile Phones

• The HLR generates 5 triplets of: RAND, SRES, $K_c$.
• $\{\text{RAND}\} K_i = (\text{SRES} \mid K_c)$.
• A one-way function called Comp128, or A3/A8, was used to do this encryption.

3.

4.
Mobile Phones

6. If SERS 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.

7.  

8. If SERS 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.
Mobile Phones

There are some problems in the represented protocol:

• In most countries the communications between base stations and the VLR pass unencrypted on microwave links.

• Triples can be replayed.

• Stolen credit cards, using stolen identities, phone mugging.

• Reprogramming IMEI - International Mobile Equipment Identifier.
Mobile Phones

• GSM also provides location security and call content confidentiality.

• Location security - once a mobile is registered to a network, it is issued with TMSI - temporary mobile subscriber identification. TMSI acts like IMSI as it roams through the network.

• IMSI-catcher - pretends to be a GSM base station, claims not to understand the TMSI. The device is of course wants to be helpful and sends the real IMSI.

• Call content confidentiality – supposed to be provided by encrypting the traffic between the device and the base station once the authentication and registration are completed.
Mobile Phones

- **3rd generation:**
  - UMTS - Universal Mobile Telecommunications System.
  - The security is much the same as GSM, but upgraded to deal with a number of GSM’s known vulnerabilities.
  - Higher data rates.
  - IMSI-catchers don’t work against third generation mobiles.
  - HLR became HE - home environment.
  - SIM became USIM - UMTS SIM.
Mobile Phones

- CK - confidentiality key.
- IK - integrity key.
- AK - anonymity key.
- SEQ - sequence number known to the HE and the USIM.
- MAC - computed on RAND and SEQ.
- AV - authentication vector = \{RAND, XRES, CK, IK, SEQ \oplus AK, MAC\}.
- \{RAND\}_k = (RES|CK|IK|AK). (HE).
Mobile Phones

- The new protocol:
  1. USIM → HE
  2. HE → VLR
  3. VLR → USIM

Steps:
1. USIM sends IMSI to HE.
2. HE sends AV to VLR.
3. VLR sends RAND, SEQ ⊕ AK, MAC to USIM.
5. USIM computes the response and the keys, unmask the sequence number, verifies the MAC, and if it’s correct returns the response to the VLR.
Platform Security

• Mobile phones become more widespread and more programmable.

• Usage of DRM (Digital rights Management) mechanism has entered to the mobile phone platforms.

• Security is made more difficult by the long and complex supply chain: chip design -> chip production -> device design and production -> OP -> more software -> national infrastructure provided by network operator -> local operating company sends the bill to the customer.
Platform Security

- Apps provided by third-party software houses.
- Locking - phone is locked to the network.
Frauds by Phone Companies

• Surprisingly one of the growing scams is the phone company frauds.
• Cramming – practice that phone companies use to make the customer to accept the false charges. For example, if you respond to voice prompts as the call progresses you can be charged without knowing that at the moment.
• Ross Anderson’s example.
• Slamming - the unauthorized change of a subscriber’s long distance telephone service provider without their consent.
• AT&T
• Fly-by-night phone companies.
Frauds by Phone Companies

• Phone companies disguising premium rate numbers as international ones.
• Expensive presents ("Pelephone").
Back to mobile phones

- 4th generation:
- Internet connectivity on mobile devices.
- Faster data transfer speed.
- LTE - Long Term Evolution.
- 4G networks must be based on an all Internet protocol (IP) packet switching instead of circuit-switched technology.
- “Burger King “OK Google” “.
Summary

• Questions to conclusion:
  - What security mistakes have you noticed?
  - Why do you think companies (mobile) kept making the same mistakes from generation to generation?