Intercepting mobile phone calls and short messages

Iosif I. Androulidakis

Senior PBX Administrator
Network Operations Center
University of Ioannina, GR
sandro @ noc.uoi.gr

Outline

- Introduction
- Theory
- Practice
  - Software
  - Hardware
- Protection
- Conclusions
- Demonstration

The CIA triplet in mobile phones

- **Confidentiality**
  - Interceptions (voice-sms-data-multimedia)
  - Monitor the user's environment (sound-video)
  - Location tracking
- **Integrity**
  - Cloning
  - Charging
- **Availability**
  - Denial of Service

Wireless Dangers

- Wireless inherits the traditional wired networks dangers and threats plus being vulnerable to new wireless-specific ones
- Radio waves travel freely and cannot easily be confined
  - Intruders can intercept and manipulate our data without even coming close
  - Using directional antennae the interception distance can exceed 1 Km!
- DoS Attacks
- Position Logging and Tracking
- Counterfeit devices, "Evil Twins" mimic legal ones
- Small devices can be easily stolen

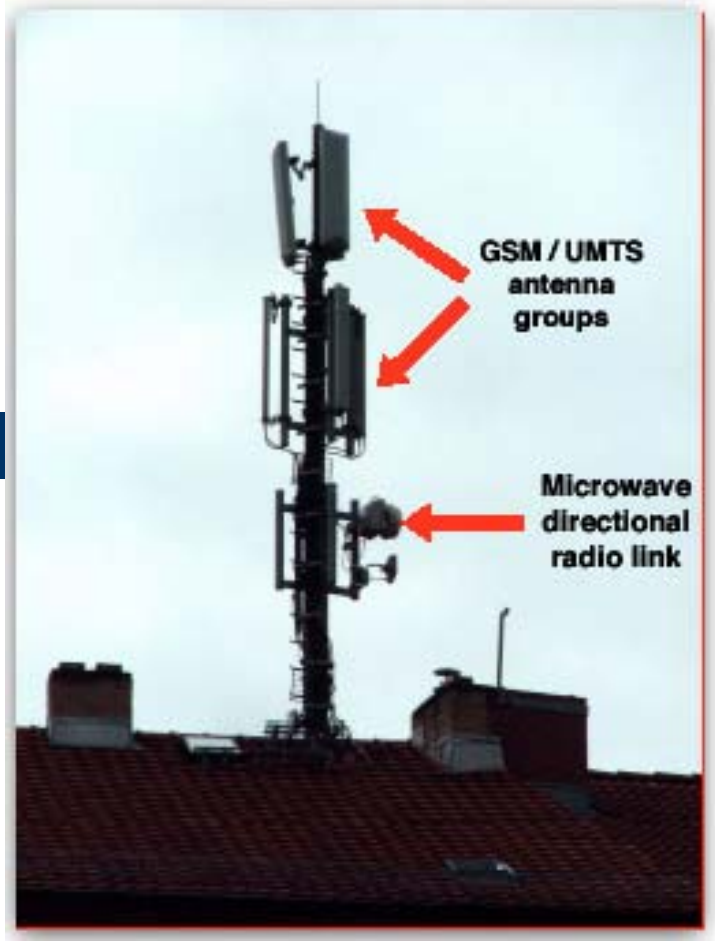
GSM Security Issues

- Communication and Signaling in the fixed backbone network are unprotected, usually without encryption. Crypto stops early
- There is no defense against “active attacks” where a counterfeit-enemy equipment appears as a new element of the network (i.e. IMSI catcher)
- There is no indication for the cryptography level used (or not used) to the user of the device
- Data and Signaling transmitted «en blanc» between wireless microwave links

Interception

- Active
  - Bluetooth
  - Virii / software
  - IMSI Catcher (ME-BTS-BTS)
  - Simple …theft!

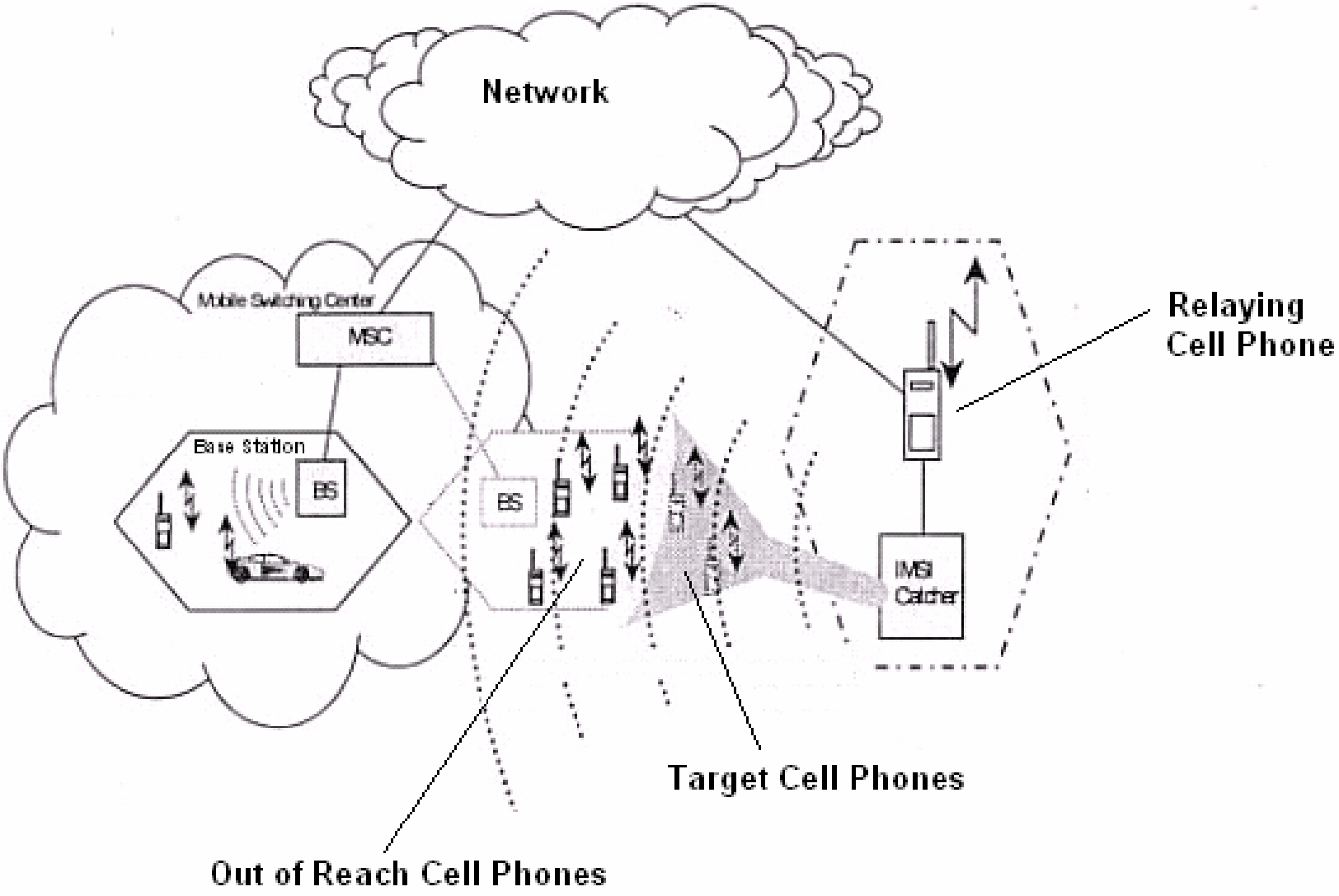
- Passive
  - A interface monitoring
    (BSC-MSC, A Interface, 3GPP TS 08.0X)
  - A-bis interface monitoring
    (BTS-BSC, A-bis Interface, 3GPP TS 08.5X)
  - Cryptanalysis on A5
    A. Biryukov, A. Shamir and D. Wagner, Real-Time Cryptanalisis of A5/1 on a PC



Fake Base Stations

- IMSI Catcher
- Man in the middle
- Ceases cryptography (forces A5/0 algorithm)
- Voice & SMS interception
- Provides cloning data: IMSI, Ki
- Provides IMEI

Fake Base Station



Attacks History

- 1991
  - First GSM implementations
- April 1998
  - Smartcard Developer Association (SDA) and U.C. Berkeley scientists cracked SIM COMP128 and extracted K_i in a few hours. Discovered that Kc uses only 54 bits
- August 1999
  - Weak A5/2 was cracked in a PC in la few seconds
- December 1999
  - Alex Biryukov, Adi Shamir and David Wagner publish a paper where they describe cracking strong A5/1. Using 2 minutes of intercepted cryptographed speech they need just 1 second to break it.
- May 2002
  - IBM R&D team discovers side-channel attacks to steal COMP128 keys.
- 2003
  - Barkan et al. Active attack, GSM phones can be convinced to use the much weaker A5/2 cipher briefly.

Attacks History

- 2006
  - Barkan, Biham, Keller attacks against A5/X Ciphers. ciphertext-only attack on A5/2 that requires a few dozen milliseconds of encrypted off-the-air cellular conversation and finds the correct key in less than a second on a personal computer.
  - (more complex) ciphertext-only attack on A5/1. (active) attacks on the protocols of networks that use A5/1, A5/3, or even GPRS. These attacks exploit flaws in the GSM protocols, and they work whenever the mobile phone supports a weak cipher such as A5/2.
  - attacks are on the protocols and are thus applicable whenever the cellular phone supports a weak cipher, for example, they are also applicable for attacking A5/3 networks using the cryptanalysis of A5/1.
  - do not require any knowledge of the content of the conversation.
- 2007
  - Universities of Bochum and Kiel started a research project to create a massively parallel FPGA based crypto accelerator COPACOBANA. Enables brute force attacks against GSM eliminating the need of large precomputated lookup tables.
- 2008
  - “The Hackers Choice” group launched a project to develop a practical attack on A5/1. The attack requires the construction of a large look-up table of ~ 3 Terabytes.

Bluetooth

- Bluetooth is a secure standard per se
- Problems lie into applications and sloppy implementations from manufacturers
- Social engineering: Caution and common sense is always needed
- Passive crypto attacks need special gear
- Main way of mobile phone virii spreading
- Can be used to locate a user

Software

- Modern cell phones can download and execute programs the same way computers do
- JAVA (J2ME), Symbian, PALM OS, Windows Mobile
- Millions of applications, games, utilities
- Fortinet.com reports 383 SymbOS virus variants
- Symbian & Windows Mobile intercepting software

James Bond Cellphone

Forgotten-Left behind cellphone, appears completely dead. It is working secretly. When called switches the microphone on and can monitor the place (worldwide coverage bug!)

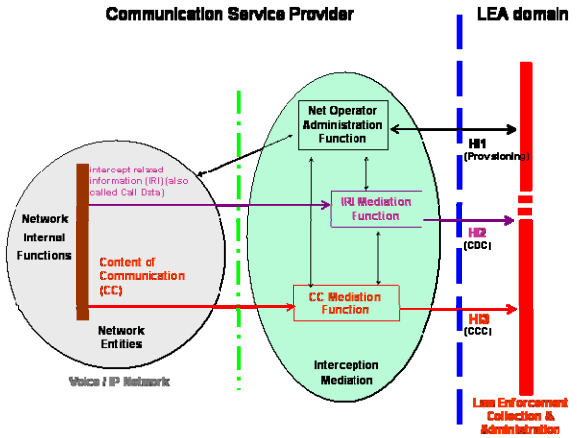
Hardware modification and/or Software (i.e. ats0=1, silence etc.)

More elaborate models work as every other innocent phone but when they get a call from a special predefined number start their silent spying. They can also intercept voice calls, sms, call history etc and send it to another preprogrammed number

Also known as Ghost phones

Other issues

- Bad implementations from manufacturers due to extensive costs and stringent time to market deadlines
- Social Engineering attacks to users
- Internal fraud
- Lawful interception abuse



Ways of protection

- Use cryptophones
- Keep your PIN secret
- Do not save sensitive data
- Keep firmware updated
- Use an antivirus
- Pay attention to the indicators
- Do not lend your phone or leave it unattended
- Do not accept unknown files through BT, WAP, email, MMS, IR etc
- Do not install unknown applications
- Check your bills

Bluetooth security

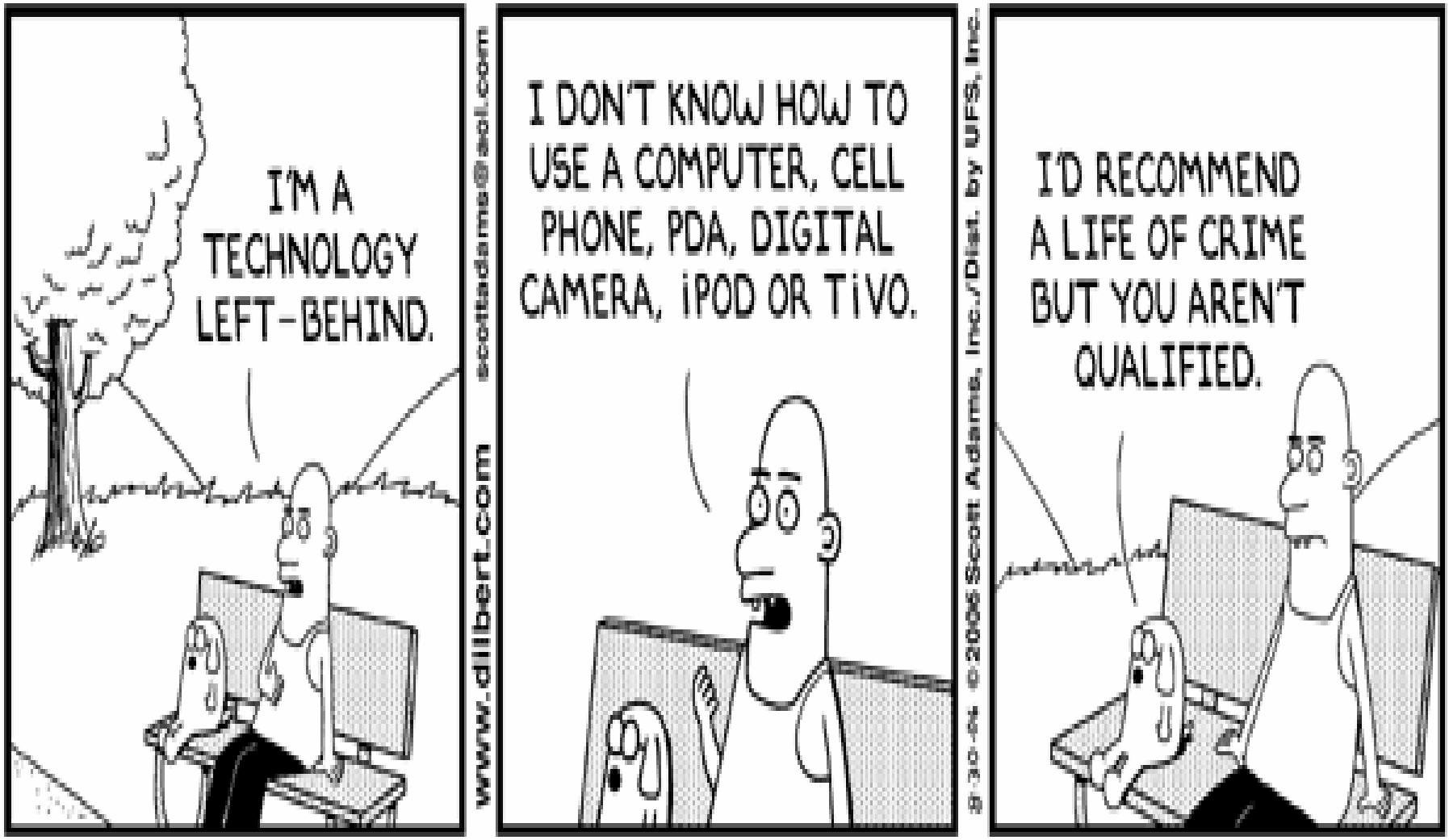
- Disable Bluetooth when not needed or at least set to invisible
- Do not accept any connections
- Use a lengthy PIN in every pairing
- Do not pair devices in unsecure areas
- Check periodically the trusted devices list
- Enable encryption

What about…

- Location tracking
- Data interception
- DoS attacks
- SMS tricks
- Forensics usage

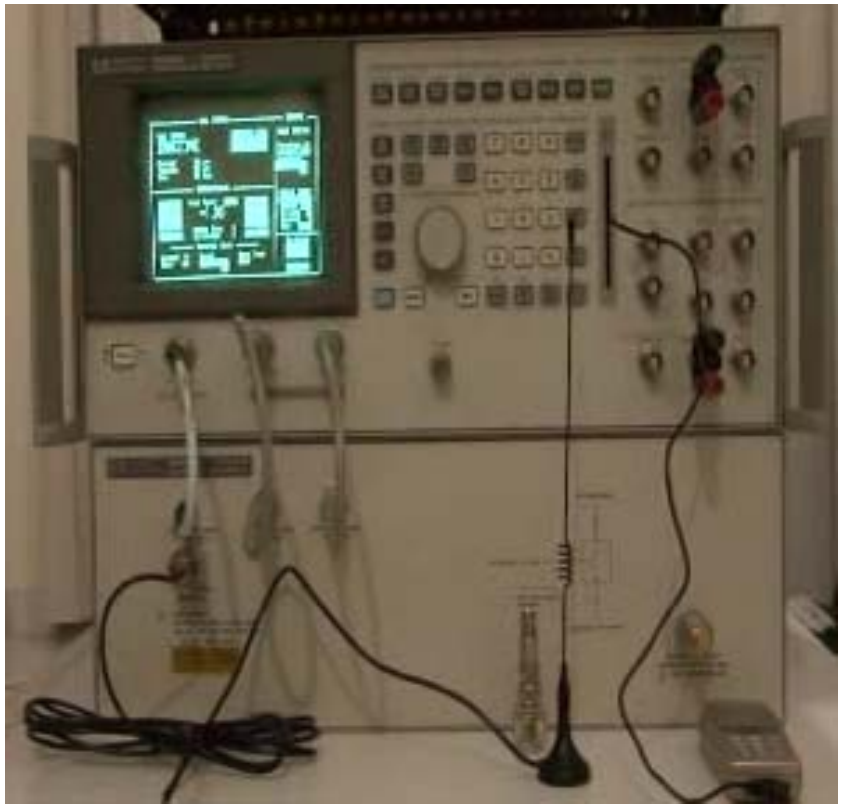
Conclusions

- GSM used to be a relatively secure standard - NOT ANY MORE
- Threats, Frauds and Dangers as in every modern technology
  - "Closed" algorithms design (security through obscurity)
  - Unsecure core network
  - Bad implementations
  - Lack of mutual authentication
  - Internal fraud
- For a (truly?) secure communication use a cryptophone
- Future systems expected to be more secure
  - Public Design, Mutual authentication, Lengthier keys, Security in the core network
- Until then, use common sense and the necessary precautions!



Demonstration

- Intercept
- VOICE
- SMS
- IMSI, IMEI



THANK YOU!!!

Iosif I. Androulidakis

Senior PBX Administrator
Network Operations Center
University of Ioannina, GR
sandro @ noc.uoi.gr