Mobile Phone Security, Interception and Forensics

Iosif I. Androulidakis, PhD

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software (Java, Virii, GPS)
- Hardware
- Forensics

GSM Characteristics

- Digital system
- Voice and Data
- International access
- High capacity
- High fidelity
- Increased security (relatively…)

Disadvantages

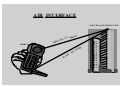
- Relatively limited bandwidth for data services (compared to 3G networks)
- Radiation issues
- Thefts
- High technical complexity
- Incompatibilities
- Social problems

GSM

NSS network and switching subsystem
Mobile Services Switching Center (MSC)
Home Location Register (HLR)
Visitor Location Register (VLR)

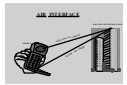
Base Station Controller (BSC)
Base Transceiver Station (BTS)

GSM frequency channels



- Uplink frequency band (MS->BS) : 890 - 915 MHz
- Downlink frequency band (BS->MS): 935 - 960 MHz
- 124 channels of 200 kHz each in each band
- 8 TDMA slots – users in each channel

ARFCN (abs rf channel no)



System	Band	Uplink	Downlink	Channel Number
GSM 400	450	450.4 - 457.6	460.4 - 467.6	259 - 293
GSM 400	480	478.8 - 486.0	488.8 - 496.0	306 - 340
GSM 850	850	824.0 - 849.0	869.0 - 894.0	128 - 251
GSM 900 (P-GSM)	900	890.0 - 915.0	935.0 - 960.0	1 - 124
GSM 900 (E-GSM)	900	880.0 - 915.0	925.0 - 960.0	975 - 1023, (0, 1-124)
GSM-R (R-GSM)	900	876.0 - 915.0	921.0 - 960.0	955 - 973, (0, 1-124, 975 - 1023)
DCS 1800	1800	1710.0 - 1785.0	1805.0 - 1880.0	512 - 885
PCS 1900	1900	1850.0 - 1910.0	1930.0 - 1990.0	512 - 810

Cell Size

- Cell Size determines how many cells are needed to cover a certain area using frequency reuse. It also determines the available capacity
- Capacity depends on bandwidth and other operational parameters
- Range from 100 meters in the city to even 35 Kilometers in rural areas
- SIM remembers last LAI (Location Area Identifier)

Programs

Global Cell Identifier
GCI = MCC + MNC + LAC + CID
GCI = LAI + CID

- CellTrack
  - **Cellid, LAC, Net Name (Cell Broadcast Service) Signal, Description (database), Cell History**
- MiniGPS
  - **Events accordingly to Cellid**
  - **Log in/out alarm, switch profile, power off, change image, SMS, Bluetooth**
- Google Maps Mobile (My Location)

Outline

- GSM Theory
- **Threats-Dangers-Fraud**
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software (Java, Virii, GPS)
- Hardware
- Forensics

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**

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**

DoS Attacks

- Denial of Service in fixed/mobile phones
- Consecutive dialing (i.e. using ATD)
- Denial of Service in the network or the device with sms flooding
  - Device Buffers
  - SMSC Buffers
- Draining Battery
- Strange names, invalid characters
  - Specially crafted Vcards
  - Specially crafted SMSs (i.e. Broken UDH)
  - Obexftp through luetooth
- Jamming

Interception

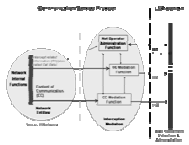
- Active
  - Bluetooth
  - Virii / Software
  - IMSI Catcher (ME-BTS-BTS)
  - Simple …theft!
- Passive
  - A interface monitoring
    (BSC-MSC, A Interface, 3GPP TS 08.0X)
  - A-bis interface monitoring
    (BTS-BSC, A-bis Interface, 3GPP TS 08.5X)
  - Cryptanalysis on A5
    A. Biryukov, A. Shamir and 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

Other issues

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



Ki, A3, A8, Kc, A5 etc

A3: Authentication with COMP128

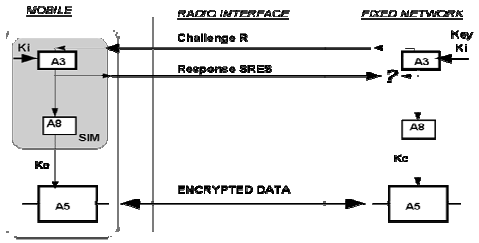
Takes the 128 bit Subscriber Authentication Key (Ki) that is stored into SIM and to the HLR and produces a 32 bit Signed Response (SRES) answering to a random 128 bit number (RAND) which is send by the HLR

A8: Produces a 64 bit Session Key (Kc) from the 128 bit random number (RAND) and the 128 bit Ki. Kc can stay the same for many days. The last 10 bits are 0 so effectively it is a 54 bit key.

A5 uses Kc and the sequence number of the transmitted frame and cryptographs the speech. A5 is implemented into the phone.

A5 Encryption: A5/0: No encryption, A5/1: Original, Europe, A5/2: Weaker, A5/3: Strong Encryption

Ki, A3, A8, Kc, A5 etc



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
- 2009
  - Karsten Nohl, Passive A5 hacking, Lookup tables using NVIDIA Video Cards

Internal Fraud

- **Connection activated without being registered to the billing system. Produces Call Detail Records but it does not get to billing platform**
- **Normal connection gets barred (i.e. due to debts). Barring is canceled through poking to the HLR. The billing system still thinks the connection is barred.**
- **Modification of Postpaid profile to a Prepaid profile. Traffic is routed to the Prepaid platform where does not exist any data for that subscriber.**

Other Problems

- **Bad implementations from manufacturers due to extensive costs and stringent time to market deadlines**
- **Specific lack of security in some Bluetooth implementations**
- **Modern cellphones-PDA-smartphones use generic Operational Systems which can be valuable to virii and traditional programming attacks**
- **Lack of user awareness and technical knowledge**

NIST suggests…

NIST National Institute of Standards and Technology

- Running a safe wireless network is a tough job
- The National Institute of Standards and Technology (NIST) recommends agencies not to undertake wireless deployment for essential operations, until they have examined and can acceptably manage and mitigate the risks of their information, system operations and continuity of essential operations.

What about…

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

In the future…

•Pressing competition among providers leads to implementing products and services without evaluating all the dangers and without ensuring their full security.

•M-Commerce growth will pose new risks since experience using them is still limited

Outline

- GSM Theory
- Threats-Dangers-Fraud
- **Net Monitor**
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software
- Hardware
- Forensics

NetMonitor

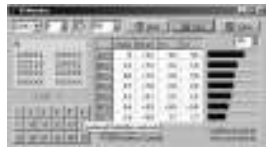
- Secret service menu
- Dozens of interesting things regarding network, cells, peripherals, SIM, cryptography etc.

NetMonitor: Enable

- **Modifying EEPROM**
- **Cable and/or program**
- **Special keyboard code**
- **Special code into specific memory position of the SIM phone catalog**
- **AT commands (AT^S^MI)**

NetMonitor

- Mini monitor
- Serving Cell
- Neighbor Cell
- Gprs monitor
- Accessories
- Irda Monitor
- Audio Monitor



NetMonitor

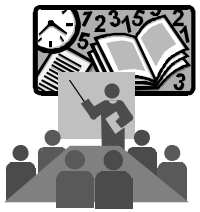
- Charge Monitor
- Serial monitor
- CSD monitor
- L1RR monitor
- Bluetooth Monitor
- ACCU monitor
- ENIP Monitor
- (S) Exit
- Heap Monitor

NetMonitor

- Date/Time
- History
- History GPRS
- SAT Commands
- Java
- Exit Info Config
- Heap Ovl Config
- Configuration

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- **GSM Network Codes**
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software
- Hardware
- Forensics



GSM network codes

- **GSM standard describes the use of codes to take advantage of network services such as divertion, barring, PIN changing etc.**
- **Most cell phones implement them through menus but there are always limitations**
- **Providers do not always stick strictly to the standard and implement services differentely**
- **Call types**
  - **Voice, fax, data, ALS (Altern. Line Service), SMS**

Communication Categories

- 10 - All
- 11 - Divert Voice
- 12 - All Data
- 13 - Divert Fax
- 16 - Divert SMS
- 19 - All except SMS
- 25 - Divert Data
- 50 - All PLMN specific teleservices
- 51 - PLMN specific teleservice 1
- 52 - PLMN specific teleservice 2
- 53 - PLMN specific teleservice 3
- 54 - PLMN specific teleservice 4
- 55 - PLMN specific teleservice 5
- 56 - PLMN specific teleservice 6
- 57 - PLMN specific teleservice 7
- 58 - PLMN specific teleservice 8
- 59 - PLMN specific teleservice 9
- 60 - PLMN specific teleservice 10
- 61 - PLMN specific teleservice 11
- 62 - PLMN specific teleservice 12
- 63 - PLMN specific teleservice 13
- 64 - PLMN specific teleservice 14
- 65 - PLMN specific teleservice 15
- 70 - All PLMN specific bearer services
- 71 - PLMN specific bearer service 1
- 72 - PLMN specific bearer service 2
- 73 - PLMN specific bearer service 3
- 74 - PLMN specific bearer service 4
- 75 - PLMN specific bearer service 5
- 76 - PLMN specific bearer service 6
- 77 - PLMN specific bearer service 7
- 78 - PLMN specific bearer service 8
- 79 - PLMN specific bearer service 9
- 80 - PLMN specific bearer service 10
- 81 - PLMN specific bearer service 11
- 82 - PLMN specific bearer service 12
- 83 - PLMN specific bearer service 13
- 84 - PLMN specific bearer service 14
- 85 - PLMN specific bearer service 15

GSM Codes, Divertions

- **All Call types**
- **Immediate**
  Set: **21*destination#[SEND]
  Cancel: ##21#[SEND]
  Query: *#21#[SEND]
- **No Answer**
  Delay nn seconds: max 30 seconds, in 5 second increments
  Set: **61*destination*nn#[SEND]
  Cancel: ##61#[SEND]
  Query: *#61#[SEND]
- **Unreachable**
  Set: **62*destination#[SEND]
  Cancel: #62#[SEND]
  Query: *#62#[SEND]
- **Busy**
  Set: **67*destination#[SEND]
  Cancel: ##67#[SEND]
  Query: *#67#[SEND]
- **Cancel All**
  ##002#[SEND] and/or ##004#[SEND]

GSM Codes, Divertions

- Voice Calls
- Immediate
  Set: **21*destination*11#[SEND]
  Cancel: ##21*11#[SEND]
  Query: *#21*11#[SEND]
- No Answer
  Delay nn seconds: max 30 seconds, in 5 second increments
  Set: **61*destination*11*nn#[SEND]
  Cancel: ##61*11#[SEND]
  Query: *#61*11#[SEND]
- Unreachable
  Set: **62*destination*11#[SEND]
  Cancel: ##62*11#[SEND]
  Query: *#62*11#[SEND]
- Busy
  Set: **67*destination*11#[SEND]
  Cancel: ##67*11#[SEND]
  Query: *#67*11#[SEND]

GSM Codes, Divertions

- Data Calls
- Immediate
  Set: **21*destination*25#[SEND]
  Cancel: ##21*25 [SEND]
  Query: *#21*25#[SEND]
- No Answer
  Delay nn seconds: max 30 seconds, in 5 second increments
  Set: **61*destination*25*nn#[SEND]
  Cancel: ##61*25#[SEND]
  Query: *#61*25#[SEND]
- Unreachable
  Set: **62*destination*25#[SEND]
  Cancel: ##62*25#[SEND]
  Query: *#62*25#[SEND]
- Busy
  Set: **67*destination*25#[SEND]
  Cancel: ##67*25#[SEND]
  Query: *#67*25#[SEND]

GSM Codes, Divertions

- Fax Calls
- Immediate
  Set: **21*destination*13#[SEND]
  Cancel: ##21*13#[SEND]
  Query: *#21*13#[SEND]
- No Answer
  Delay nn seconds: max 30 seconds, in 5 second increments
  Set: **61*destination*13*nn#[SEND]
  Cancel: #61*13#[SEND]
  Query: *#61*13#[SEND]
- Unreachable
  Set: **62*destination*13#[SEND]
  Cancel: #62*13#[SEND]
  Query: *#62*13#[SEND]
- Busy
  Set: **67*destination*13#[SEND]
  Cancel: ##67*13#[SEND]
  Query: *#67*13#[SEND]

GSM Codes, Divertions

- 2nd Line Diversion
- Immediate
  Set: **21*destination*89#[SEND]
  Cancel: #21*89#[SEND]
  Query: *#21*89#[SEND]
- No Answer
  Delay nn seconds: max 30 seconds, in 5 second increments
  Set: **61*destination*89*nn#[SEND]
  Cancel: ##61*89#[SEND]
  Query: *#61*89#[SEND]
- Unreachable
  Set: **62*destination*89#[SEND]
  Cancel: ##62*89#[SEND]
  Query: *#62*89#[SEND]
- Busy
  Set: **67*destination*89#[SEND]
  Cancel: ##67*89#[SEND]
  Query: *#67*89#[SEND]

GSM Codes, Barring

- Useful to know the barring code

- Vodafone: 1234
- Cosmote: 1234
- WIND: 0000
- Q: 1111

- Change code: **03*XXXX*YYYY*YYYY#
- XXXX old code
- YYYY new code

GSM Codes, Barring

- Call Barring
- No diversion should be active
- All Calls
  Set: **330*barring code#[SEND]
  Cancel: ##330*barring code#[SEND]
  Query: *#330#[SEND]
- Outgoung
  Set: **333*barring code#[SEND]
  Cancel: ##333*barring code#[SEND]
  Query: *#333#[SEND]
- Incoming
  Set: **35*barring code#[SEND]
  Cancel: ##35*barring code#[SEND]
  Query: *#35#[SEND]

GSM Codes, Barring

- International Outgoing
  Set: **331*barring code#[SEND]
  Cancel: ##331*barring code#[SEND]
  Query: *#331#[SEND]
- International Outgoing (allow home country)
  Set: **332*barring code#[SEND]
  Cancel: ##332*barring code#[SEND]
  Query: *#332#[SEND]
- Incoming calls when out of home country
  Set: *351*barring code#[SEND]
  Cancel: #351*barring code#[SEND]
  Query: *#351#[SEND]
- Cancel All Call Barring
  #330*barring code#[SEND]

GSM Codes, SMS

- No provision for SMS forwarding (are you sure?)

- Barring incoming SMS
  Set: *35*barring code*16#[SEND]
  Cancel: #35*barring code*16#[SEND]

GSM Codes, Identification

- Outgoing CLI Restriction (recipient sees your number)
  Release: *31# destination [SEND]
  Withhold: #31# destination [SEND]
  Query default: *#31#[SEND]

- Incoming CLI Presentation (you see the caller's number)
  Allow: *30#[SEND]
  Prevent: #30#[SEND]
  Query default: *#30#[SEND]

GSM Codes, Identification

- **Connected Line Identification Presentation - COLP**
  To Activate: * 76 # [SEND]
  To Deactivate: # 76 # [SEND]
  To Check: * # 76 # [SEND]
- **Connected Line Identification Restriction - COLR**
  To Activate: * 77 # [SEND]
  To Deactivate: # 77 # [SEND]
  To Check: * # 77 # [SEND]

GSM Codes, PIN Change

- **Change Call Barring pin code**
  ****03*oldpin*newpin*newpin#**
- **Change SIM pin code**
  ****04*oldpin*newpin*newpin#**
- **Change SIM pin2 code**
  ****042*oldpin*newpin*newpin#**
- **Unblock SIM pin code**
  ****05*PUK*newpin*newpin#**
- **Unblock SIM pin code**
  ****06*PUK2*newpin*newpin#**

GSM Codes, Call management

- **Call Waiting**
  Set: *43#[SEND]
  Cancel: #43#[SEND]
  Query: *#43#[SEND]
- **When Call in waiting:**
  Reject: 0 [SEND]
  Drop current call and answer: 1 [SEND]
  Drop specific call (where this call is X) press: 1X [SEND]
  Hold current call and answer: 2 [SEND]
  Hold others and answer specific call (where this call is X): 2X [SEND]
- **To add the held call to the current conversation: 3 [SEND]**
- **To make a new call & place others on hold: Number [SEND]**
- **To end all call's together (except a waiting call): [END]**

GSM Codes, Teleconference

Using the previous codes:

1. **Call A**
2. **Call B (A goes into park – call waiting)**
3. **Press 3 [SEND] and … presto … Teleconference**
4. **Can drop out which one I want with 1 or 2 [SEND]**

Works for 2 incoming calls too

The other 2 parties (excluding the party that started the teleconference) are getting an informatory beep in regular time intervals (i.e. every 15 seconds)

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- **Mobile Phones Codes**
- AT command set
- SMS tricks
- Bluetooth hacking
- Software
- Hardware
- Forensics

IMEI

- **IMEI** (**I**nternational **M**obile **E**quipment **I**dentification code) (GSM/DCS/PCS)
- Unique 14-digit number in each cell phone in the world
- Can be seen with ***#06#**
- TAC (Type allocation code): 8 digits
  - (2 digits Reporting Body and 6 digits ME type identifier)
- SN: 6 digits
- Check digit (Luhn formula)

TAC	Serial No	Check Digit
NNXXXX YY	ZZZZZZ	A

Shortcuts…

NOKIA
Connecting People

- ***#0000#**
- ***#9999#**
- ***#3110#**
- ***#3810#**
- ***#5190#**
- ***#6190#**
- ***#8110#**
- ***#837#**
- ***#1706021123 02#**
- ***#682371158412125#**
- ***#2820#**
- ***#WAR0ANTY#**
- ***#WARRANTY#**
- ***#WAR0ANTY# (+9268)**
- ***HRC0# - #HRC0#.**
- ***EFR0# - #EFR0#**

Shortcuts…

Sony Ericsson

Secret Menu: >*<<*<* (K700/T630/T610/T68/T310/T200/T100/R600)

Secret Menu: close flip or activate virtual keyboard then U*DD*D* (P800/P900) (applications screen -> Edit -> System Information) (P800/P900)

phone model -software info -IMEI -configuration info -sim lock status -REAL time clock -total call time - text labels - test services and hardware (main display, camera, LED/illumination, Flash LED, keyboard, earphone, speaker, microphone, radio and vibrator tests)

IMEI Number: *#06#

Lock status = <<**

Shortcut to last dialed numbers: 0#

Shortcut to sim numbers: On main menu type a number and press #

Language reset <- 0000 ->

Phone status = Either volume button

K750i netmonitor enable 585*0000 + Call or *585*0000# + Send. disable #585#0000 + Call or #585#0000# + Send.

Shortcuts…

SHARP

***01763*278257# Assert Fail Log clear**
***01763*2783771# ?????**
***01763*2783772# ?????**
***01763*2783773# ?????**
***01763*2783774# ?????**
***01763*2783775# ?????**
***01763*3640# (*01763*ENG0#) — Disable Engineer Mode**
***01763*3641# (*01763*ENG1#) — Enable Engineer Mode**
***01763*4634# (*01763*IMEI#) — IMEI**
***01763*476# — Tests**
***01763*5640# (*01763*LOG0#) — Disable LOG**
***01763*5641# (*01763*LOG1#) — Enable LOG**
***01763*6365641# ?????**
***01763*6370# (*01763*MEP0#) — Disable MEP menu (unlock menu)**
***01763*6371# (*01763*MEP1#) — Enable MEP menu (unlock menu)**
***01763*638633 0# (*01763*NETMODE0#) — Disable NetMode**
***01763*638633 1# (*01763*NETMODE1#) — Enable NetMode**
***01763*737381# (*01763*RESET1#) — System reset (all default settings)**
***01763*7 53371# Sleep Check**
***01763*7 9837# (*01763*SWVER#) — Software version**
***01763*8371# (*01763*VER0#) — Firmware Version**
***01763*8781# (*01763*TST1#) — Test #1**
***01763*8782# (*01763*TST2#) — Test #2**
***01763*8783# (*01763*TST3#) — Test #3**
***01763*8784# (*01763*TST4#) — Test #4**
***01763*8785# (*01763*TST5#) — Test #5**
***01763*8786# Test #6**
***01763*8787# Test #7**
***01763*87870# Test #70**
***01763*87871# Test #71**
***01763*87872# (*01763*TST72#) — Test #72**
***01763*87873# Test #73**
***01763*87874# Test #74**
***01763*8788# (*01763*TST8#) — Test #8**
***01763*87891# ?????**
***01763*87892# ?????**

Catalog Tricks

- **The catalog application in most cell phones matches only the 6-8 last digits of a number in order to show the relative entry name.**
- **If +30694577875=ΣΗΦΗΣ, then 4577875 shows also ΣΗΦΗΣ but of course can't be called**
- **If I dial 2651007164477875, I will read ΣΗΦΗΣ on screen but 265100716 will be called!**
- **55# shows entry 55 etc.**

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- **AT command set**
- SMS tricks
- Bluetooth hacking
- Software
- Hardware
- Forensics

AT commands

- AT command (Attention) is a very useful way to setup and control telecommunications equipment (i.e. Modems)
- Hayes
- 3GPP (3d Generation Partnership Program)

3GPP TS 27.007

Identification

- AT* list all commands
- AT+CLAC list all available commands
- AT+CGMI, manufacturer
- AT+CGMM, model
- AT+CGMR, revision
- AT+GMI, manufacturer
- AT+GMM, model
- AT+GMR, revision
- AT+CGSN, IMEI (*#06#)
- AT+CIMI, IMSI
- ATI
- AT+CNUM, number
- AT+ESIR, interface release
- AT*EMLR, menu list

Call control

- AT+CHUP, hung up
- AT+CREG, net registration
- AT+COPN operator names
- ATD, dial
- AT+CLIP, caller id
- AT*EDIF, divert
- AT*EIPS, identity presentation
- AT+CPAS, state of mobile
- AT+CBC battery
- AT+CSQ signal quality
- AT+CACM (call meter)
- AT^SBNR (call meter)
- AT+CRMP playback melody
- AT+VTS send DTMF
- AT+CCFC call forward
- *21*DN*BS# BS 11=voice
- ATS0=1 autoanswer

Device Control

- AT+CKPD, keypad control
- AT*EKSE, keystroke send
- AT+CMER, event reporting
- AT+CKEV, event key
- AT+CIND, indicator control
- AT*ECAS, callers allowed
- AT*ECAW, write caller allowed
- AT+CVIB, vibrator
- AT*ERIL, ring level
- AT*ESBL, backlight
- AT*ESIL, silence
- AT+CFUN, on/off
- AT+WS46, GSM on/off

Catalogs

- AT+CPBS (Select the phonebook type)
  - "DC" – Dialed calls
  - "EN" - Emergency numbers, writeprotected stored on SIM
  - "FD" - Fixdialing numbers
  - "MC" - Missed calls
  - "ME" - Phonebook
  - "MT" - "ME" + SIM phonebook
  - "ON" - Own number
  - "RC" - Received calls
  - "TA" - TA phonebook
- AT+CPBR (Read phonebook)
- AT+CPBR=? (Reads out the number of supported entries from the phonebook)
- AT+CPBR=2 (Reads the entry number 2 of the phonebook)
- AT+CPBF (Search by name in phonebook)
- AT+CPBF="Max" (Searches for an entry with name "Max" and displays it)
- AT+CPBR=11 (phonebook)
  +CPBR: 11,"2220",129,"infoArea"

Messages

- AT+CPMS="SM", select list
- AT+CMGL=1, list messages
- AT+CMGR, read messag
- AT+CMGR=2 (read sms)
  +CMGR: "REC READ","+349995533","","05/03/30,17:39:55+08"
- AT+CMGS, send message
- AT+CMGW, write sms to mem

Miscellaneous

- AT+CCLK, clock
- AT*ESZS, snooze, IR detector

Remote Control

- **GSM+AT+Microprocessor = telemetry applications to remotely control other devices (or even …people)**
- **Java programs to do the same**

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- **SMS tricks**
- Bluetooth hacking
- Software
- Hardware
- Forensics

SMS theory

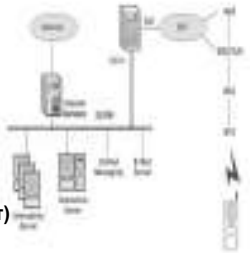
Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP)

3GPP TS 03.40 version 7.5.0 ,1998

ETSI TS 100 901 V7.5.0 (2001-12)

SMS Architecture

- **Store and Forward**
- **Cleartext with many different formats among manufacturers (SMPP, EMI/UCP, TAP κλπ)**



SMS Attacks

- **Denial of Service in the network or the phone with consecutive messages (from another phone or the net)**
  - **Phone Buffers**
  - **SMSC Buffers**
- **Long names, invalid characters**
  - **Especially crafted Vcards**
  - **Especially crafted SMSs (i.e. Broken UDH)**
  - **Obexftp through Bluetooth**
- **History: Nokia 5100 all dot SMS crash**
- **SMS spoofing**

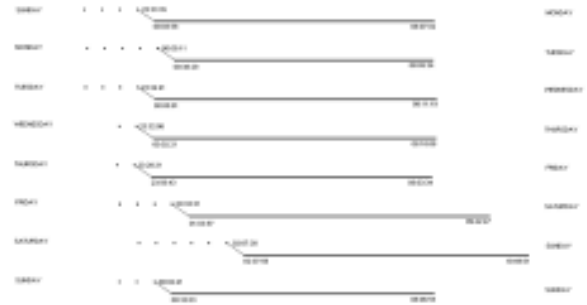
SMS flash

- Flash message appears immediately on the screen usually close to the Network Name
- User does not have to "open" the message to read it. It is already "opened"
- Can deceit the user to trust that it comes from the provider. Can be used for various Social Engineering attacks

SMS ping

- **Every simple user (not the mighty provider!) can stealthily discover whether another user has her cell phone switched on or off!**
- **He can reveal her behavior using patterning techniques (i.e. time of awakening or sleeping)**

SMS ping



SMS ping

Refresh SMS

The GSM standard includes a special category of "magic" short messages which can refresh themselves (they are replaced by new messages in the same memory position) changing this way their content

Very useful for stock exchange listings, weather forecasts, or if you are late in a rendez-vous

SMS Contests

Automated multiple voting for our favorite player to sway contests, televoting and other results

YOU CAN BE A STAR!!!!

SMS-scandal overshadows Eurovision victory for Rivas

SMS Spoofing

Bulk SMS through marketing companies

Bulksms, Prosms, Websms, Sendsms

You can arbitrarily chose originator name or number

11 latin characters or 16-digit number

Interconnection fee

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- **Bluetooth hacking**
- Software
- Hardware
- Forensics

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**

Bluetooth security

- Disable Bluetooth when not needed (security and battery)
- If needed, at least set it to invisible
- Do not accept any unsolicited connections
- Use a lengthy PIN in every pairing
- Do not pair devices in unsecure areas
- Check periodically the trusted devices list
- Update firmware
- Enable encryption during pairing with PC
- If under BlueJack attack, move away
- Perform precautionary BT sniffing to locate forgotten BT devices or hostile ones

Bluetooth Hacking

Demonstration

Outline

- Θεωρία GSM
- Απειλές-Απάτες-Κίνδυνοι
- Net Monitor
- GSM Network Codes
- Mobile Phone Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- **Software**
- Hardware
- Forensics

Software

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

VIRII

- Almost every single cell phone virus spreads through Bluetooth exploiting security holes

Fortinet.com reports 383 SymbOS virii mutations

Symbian & Windows Mobile bugging

- Callmagic 2.0 (vicinity)
- CellTrack
- SmsAnywhere
- SmsForwarder
- SpyCall
- TheSpyphone (active call)
- Interceptor (active call)
- Neo Call Mobile-secuware (active call)
- CellPI (active call)
- FlexiSpy PRO-X (active call)
- FlexiSpy (GPRS)
- ProRecorder (recording)
- Mobile-Spy retina-x (internet)

Symbian & Windows Mobile bugging

Demonstration

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software
- **Hardware**
- Forensics

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

Telemetry

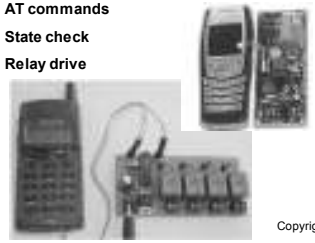
Cheap and easy

Using microcontrollers

AT commands

State check

Relay drive



GSM + GPS = …

- GPS BLUETOOTH modules
- LOMMY
- TRIMTRACK
- SANJOSE
- MobiTrack

Jammers

- Various models with different range
- From a couple of meters to a whole city
- Jamming the GSM frequency bands
- Relatively easy to construct and implement

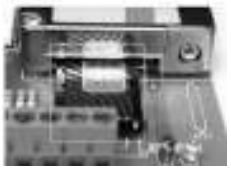
Demonstration

GSM - PSTN bridge (spying PSTN lines)

James Bond phone

Jammer

GSM-GPS



Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software (Java, Ioι, GPS)
- Hardware
- **Forensics**

Mobile Phone Forensics

Use of phones in crimes and illegal activities

Gathering Data

- **Catalog, Messages, Appointments, Calls, LAI**
  - **SIM**
  - **Phone Memory / Flash Memory**
  - **Network Provider Info**

Methodology

- **Theory**
- **PC SDK**
- **AT commands, OBEX**
- **FBUS Nokia, JTAG**
- **Professional devices**

Legal stuff

Conclusions

Methodology

- Understand security and data integrity requirements
- Understand device design
  - Explore both electronic and mechanical parts
  - Explore interfaces
  - Use public sources (I.e. Internet fora, patents)
  - Study schematics
- Choose steps
  - Define storage area and extraction capabilities
  - Spot available control interfaces
  - Calculate time and cost
- Extract Data

Forensics

Demonstration

Review

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth hacking
- Software (Java, Virii, GPS)
- Hardware
- Forensics

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 (security and battery)
- If needed, at least set it to invisible
- Do not accept any unsolicited connections
- Use a lengthy PIN in every pairing
- Do not pair devices in unsecure areas
- Check periodically the trusted devices list
- Update firmware
- Enable encryption during pairing with PC
- If under BlueJack attack, move away
- Perform precautionary BT sniffing to locate forgotten BT devices or hostile ones

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**
  - **Privacy invasion issues**
- **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 FOR YOUR ATTENTION!!!

Iosif I. Androulidakis, PhD