Mobile Phone Security, Interception and Forensics

Josif I. Androulidakis, PhD

Copyright © 2010 by Iosif I. Androulidakis

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

Copyright © 2010 by Iosif I. Androulidakis

GSM Characteristics

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

Copyright © 2010 by Iosif I. Androulidakis

Disadvantages

- Relatively limited bandwidth for data services (compared to 3G networks)
- Radiation issues
- High technical complexity
- Incompatibilities
- Thefts
- High fidelity
- Increased security (relatively...)

Copyright © 2010 by Iosif I. Androulidakis

GSM

NSS network and switching subsystem
Mobile Services Switching Center (MSC)
Home Location Register (HLR)
Visitor Location Register (VLR)
Base Station Location Register (BS)
Base Transceiver Station (BTS)

Copyright © 2010 by Iosif I. Androulidakis

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

Copyright © 2010 by Iosif I. Androulidakis

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)

Copyright © 2010 by Iosif I. Androulidakis

ARFCN (abs rf channel no)

<table>
<thead>
<tr>
<th>System</th>
<th>Band</th>
<th>Uplink</th>
<th>Downlink</th>
<th>Channel Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM 900</td>
<td>1800</td>
<td>890.0 - 915.0</td>
<td>935.0 - 960.0</td>
<td>1 - 124</td>
</tr>
<tr>
<td>GSM 1800</td>
<td>2100</td>
<td>1710.0 - 1785.0</td>
<td>1805.0 - 1880.0</td>
<td>512 - 810</td>
</tr>
<tr>
<td>GPRS 1800</td>
<td>2100</td>
<td>1710.0 - 1785.0</td>
<td>1805.0 - 1880.0</td>
<td>512 - 810</td>
</tr>
<tr>
<td>GSM-R 900</td>
<td>876.0 - 915.0</td>
<td>921.0 - 960.0</td>
<td>955 - 973, (0, 1-124, 975 - 1023)</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2010 by Iosif I. Androulidakis

Programs

- Global Cell Identifier
  GCI = MCC + MNC + 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)
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**
  - Interception (voice-on-data-or-video)
  - Monitor the user’s environment (sound-video)
  - Location tracking
- **Integrity**
  - Cloning
- **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
  - SMS Buffers
- Draining Battery
- Strange names, invalid characters
  - Specially crafted Voicd
  - Specially crafted SMSIs (i.e. Broken UDHI)
- Obfuscate through Bluetooth
- Jamming

Interception

- **Active**
  - Bluetooth
  - Vibri / Software
  - IMSI Catcher (ME-BTS-BTS)
  - Simple... that!
- **Passive**
  - A interface monitoring
    - (BSC-MSC, A Interface, 3GPP TS 08.0X)
  - B interface monitoring
    - (BTS-BS, A-Bis Interface, 3GPP TS 08.5X)
- Cryptanalysis on A5
  - A.Stephan, A. Shamir and D. Wagner, Real Time Cryptanalysis 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 excessive 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 CDPDU
- Times 128-bit Sub-Subscriber Authentication Key (Ki) that is stored in SIM card to the HLR and produces a 128-bit Encryption Key (Kc) which is used by the HLR
- Produces a 48-bit Gregarious Key (Ki) from the 128-bit random number (Ki) and the 128-bit Ki. Ki can change the same for many cyclics. The Ki data can be determined in a split second
- Uses Ki and the sequence number of the transaction to form and encrypt the speech. Ak is organized into blocks of four
Ki, A3, A8, Kc, A5 etc

Attacks History
- 1991
  - First GSM implementations
- April 1998
  - Sp overhead Developer Association (SSA) and U.C. Berkeley scientists cracked SM COMP128 and extracted Kc in a few hours. Discovered that Kc uses only 54 bits
- August 1998
  - Woes A52 was cracked in a PC in a few seconds
- December 1998
  - Alex Biryukov, Adi Shamir and David Wagner publish a paper where they describe cracking strong Kc1 using 2 minutes of intercepted cryptographical speech they need</p>

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 visit and traditional programming attacks
- Lack of user awareness and technical knowledge

NIST suggests...
- 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.
- E-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

Outline

- GSM Theory
- Threats-Dangers-Fraud
- Net Monitor
- GSM Network Codes
- Mobile Phones Codes
- AT command set
- SMS tricks
- Bluetooth
- Software
- 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 differently
- Call types
  - Voice, fax, data, ALS (Altern. Line Service), SMS

Communication Categories

- All Call types
  - Immediate
  - Set: **21*destination#\[SEND\] Cancel: ##21#\[SEND\] Query: *#21#\[SEND\]
  - No Answer
  - Delay on seconds: max 30 seconds, in 5 second increments
  - Set: **21[destination#\[SEND\] Cancel: ##21#\[SEND\] Query: *#21#\[SEND\]
  - Unsachable
  - Set: **3[destination#\[SEND\] Cancel: ##3#\[SEND\] Query: *#3#\[SEND\]
  - Busy
  - Set: **7[destination#\[SEND\] Cancel: ##7#\[SEND\] Query: *#7#\[SEND\]
  - Cancel All
    - #001#\[SEND\] and/or #004#\[SEND\]
**GSM Codes, Divertions**

- **Voice Calls**

- **Data Calls**
  - No Answer: Delay on seconds: max 30 seconds, in 5 second increments Set: *61*destination*25*nn# [SEND] Cancel: #61*25# [SEND] Query: *#61*25# [SEND]

- **Fax Calls**
  - No Answer: Delay on seconds: max 30 seconds, in 5 second increments Set: *61*destination*13*nn# [SEND] Cancel: #61*13# [SEND] Query: *#61*13# [SEND]

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

**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]
  - 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: Set: **333*barring code# [SEND] Cancel: ##333*barring code# [SEND] Query: #333# [SEND]
  - Change code: **03*XXXXYYYYYYYYY

- **Useful to know the barring code**
  - Vodafone: 1234
  - Cosmote: 1234
  - WIND: 0000
  - Q: 1111

**GSM Codes, Identification**

- **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]

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

- **No provision for SMS forwarding**
  - Release: **31*destination [SEND] Cancel: #31* [SEND]
  - Prevent: #30# [SEND]

**GSM Codes, SMS**

- **Outgoing CLI Restriction**
  - Recipient sees your number: Release: **31*destination [SEND] Cancel: #31* [SEND]
  - Withheld: #30# [SEND]

- **Incoming CLI Presentation**
  - You see the caller's number: Allow: #30# [SEND] Prevent: *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#"

- Unblock SIM pin code
  "05*oldpin*newpin*newpin#"

GSM Codes, Call management

- Call Waiting
  Set: *43* [SEND]
  Cancel: #43* [SEND]
  Query: *#43* [SEND]

- When Call in waiting:
  • To Activate: *77* [SEND]
  • To Deactivate: #77* [SEND]
  • To Check: *#77* [SEND]

- Connected Line Identification Presentation 5 COLP
  - 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 specific call (where this call is X): 2X* [SEND]

GSM Codes, Teleconference

- Connected Line Identification Restriction 5 COLR
  To add the held call to the current conversation: 3* [SEND]
  To make a new call & place others on hold: Number* [SEND]

- IMEI (International Mobile Equipment Identification 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
  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 informative 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 Number: *#06#
- Lock status = **< Shortcut to last dialed numbers: 0#
- Shortcut to sim numbers: On main menu type a number and press #

Secret Menu:

- "0000#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "9999#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "83810#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "85190#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "98110#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "9837#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "8170602112302#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "633771058412125#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "98280#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "83110#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "8170602112302#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "89000#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "83110#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "89999#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "83810#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "85190#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "98110#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "9837#" (K780/6365/6360/6350/6308/6300/6260/6260i/6260s/6260)
- "*01763*278257# Assert Fail Log clear*01763*2783771# ?????*01763*2783772# ?????*01763*2783773# ?????*01763*2783774# ?????*01763*2783775# ?????*01763*3640# (*01763*ENG0#) 555Disable Engineer Mode*01763*3641# (*01763*ENG1#) 555Enable Engineer Mode*01763*4634# (*01763*IMEI#) 555IMEI*01763*476# 555Tests*01763*5640# (*01763*LOG0#) 555Disable LOG*01763*5641# (*01763*LOG1#) 555Enable LOG*01763*6365641# ?????*01763*6370# (*01763*MEP0#) 555Disable MEP menu (unlock menu)*01763*6371# (*01763*MEP1#) 555Enable MEP menu (unlock menu)*01763*63866330# (*01763*NETMODE0#) 555Disable NetMode*01763*737381# (*01763*RESET1#) 555System reset (all default settings)*01763*753371# Sleep Check*01763*79837# (*01763*SWVER#) 555Software version*01763*8371# (*01763*VER0#) 555Firmware Version

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

Language reset <50000> Phone status = Either volume button K750i netmonitor enable 585*0000 + Call or *585*0000# + Send. disable #585#0000 + Send. 

Secret Menu: close flip or activate virtual keyboard then U*DD*D* (P800/P900)
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 I dial 2651007164477875, I will read ΣΗΦΗΣ on screen but 265100716 will be called!

55# shows entry 55 etc.

**Catalog Tricks**

**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+CGML, manufacturer
- AT+CGMM, model
- AT+CGMR, revision
- AT+GML, 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
- AT+GMI, manufacturer
- AT+GMM, model
- AT+GMR, revision

**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
- *21*DN*BS# BS 11=voice
- ATS0=1 autoanswer

**Device Control**

- AT+CKPD, keypad control
- AT*EKSE, key-stroke send
- AT+CMER, event reporting
- AT+CKEY, event key
- AT+CIND, indicator control
- AT*ECAS, callers allowed
- AT*ECAW, write caller allowed
- AT+CVIB, vibrator
- AT+CFL, 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, write-protected stored as SIM
- "FD" – Fixed dialing numbers "MC" – Missed calls "ME" – Phonebook "MT" – "ME" + SIM phonebook "ON" – Own number "RC" – Received calls "TA" – TA phonebook

**Messages**

- AT+CMGS, send message
- AT+CMGW, write sms to mem

**Miscellaneous**

- AT+CCLK, clock
- AT*ESZS, snooze, IR detector
- AT+CFL, ring level
- AT*ESBL, backlight
- AT*ESIL, silence
- AT+CFUN, on/off
- AT+WS46, GSM on/off
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)
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 rendezvous.

---

SMS Contests

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

YOU CAN BE A STAR!!!!

---

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

---

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

---

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 Hacking

Demonstration
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

Symbian & Windows Mobile bugging
- Callmagic 2.0 (vicinity)
- CallTrack
- EmAnywhere
- SmsForwarder
- SpyCall
- TheSpyphone (active call)
- Interceptor (active call)
- Neo Call Mobile-securityware (active call)
- CellPF (active call)
- FlexiSpy PRO-X (active call)
- FlexiSpy (GPRS)
- Proflecoeder (recording)
- Mobile-Spy retina-e (internet)

CellTrack
SmsAnywhere
SmsForwarder
SpyCall
Almost every single cell phone virus spreads through Bluetooth exploiting security holes
Modern cell phones can download and execute programs the same way computers do
TheSpyphone (active call)
Interceptor (active call)
Neo Call Mobile-securityware (active call)
CellPF (active call)
FlexiSpy PRO-X (active call)
FlexiSpy (GPRS)
Proflecoeder (recording)
Mobile-Spy retina-e (internet)

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. ats=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

Symbian & Windows Mobile bugging
Demonstration

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, Ios, GPS)
- Hardware
- Forensics

Mobile Phone Forensics

Use of phones in crimes and illegal activities
Gathering Data
- Call log, Messages, Appointments, Calls, LAI
- SIM
- Power Manager, Flash Memory, Network Provider Info

Methodology

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

Legislation

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!

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 insecure 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

- 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!