Law Enforcement, Forensics and Mobile Communications

Vanessa Gratzer[1]
1. Université Paris II Panthéon-Assas
Hall Goullencourt, casier 55
12 place du Panthéon, F-75231 Paris CEDEX 05
vanessa.gratzer@gmail.com

David Naccache[1+2]
2. École Normale Supérieure
Équipe de Cryptographie
45 rue d'Ulm, F-75230 Paris CEDEX 05
david.naccache@ens.fr

David Znaty[3]
3. Cabinet Znaty Expert Witness
8 rue Dupleix, F-75015, Paris, France
dznaty@alum.mit.edu

Abstract

By the end of 2004, the GSM *Association reported that over 600 networks in more than 200 countries were serving more than 1.2 billion users [1]. This extraordinary development of inexpensive and flexible mobile communications is also a source of new security challenges.*

This paper briefly lists the forensic challenges raised by handsets and overviews the handset analysis techniques used (or usable) by law enforcement officers in the course of criminal investigations.

1. Introduction

According to the GSM Association [1], by the end of 2004, 1.2 billion individuals were using GSM phones. This pervasive availability of mobile communications is the source of new security challenges.

This paper overviews the handset-related methods usable by law enforcement agencies for gathering evidence during criminal investigations.

The "telegraphic" style of this extended abstract stems from the obligation to comply with the page limit enforced in these proceedings. A longer, more detailed version, is expected to appear as a full paper soon.

2. Handset Types

Handsets feature various degrees of complexity and a high variance in functionalities. The simplest phones (that we term *Basic*) are designed to fulfill the minimal functionality one can expect from a handset: send a receive calls. *Intermediate* phones usually feature a color screen, a digital camera and a WAP browser. *Smart* phones and PDAs would usually be capable of performing advanced operations such as email exchange or agenda synchronization.

According to Gartner Dataquest, in 2004 the 1.2 billion handsets in use broke-down into 72% intermediate phones, 22% basic phones and 5% smart phones.

3. Wording the Warrant

Handset analysis warrants should request at least the following information elements:

- **User data:** phone directory, incoming/outgoing/lost calls, SMS, WAP bookmarks, MMS, images, movies, agenda, mail and documents.
- **Operator data:** IMSI (International Mobile Subscriber Identity), last Kc, network priority and restrictions, geographic data (last base station) SMS and WAP parameters.
- **Handset data:** IMEI (International Mobile Subscriber Identity) and an indication of active internal parameters.

Namely, the assignment should allow the expert to extract from the SIM, the handset and the network the following data elements:

Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)
0-7695-2520-2/06 $20.00 © 2006 IEEE
IEEE COMPUTER SOCIETY

- SIM **data elements**: Phase (phase ID), SST (SIM service table), ICCID (smart card serial number), LP (language preference), SPN (telecom operator's name), MSISDN (the subscriber's phone number), AND (short dial number), FDN (fixed dialing numbers), LND (last dialed numbers, usually limited to ten), EXT1, EXT2 (dialing extensions), GID1, GID2 (groups), SMS (text messages), SMSP (text message parameters), SMSS Text message Status, CBMI (preferred network messages), PUCT (charges per unit), ACM charge counter, ACMmax (charge limit), HPLMNSP (HPLMN search period), PLMNsel (PLMN selector), FPLMN (forbidden PLMNs), CCP (capability configuration parameter), ACC (access control class), IMSI (SIM's identity number) LOCI (location information), BCCH (broadcast control channels), Kc (voice encryption session-key), PUK (PIN unlocking code, extractable only invasively from the SIM).
- **Handset data elements**: IMEI (handset identity number, usually appearing inside the phone or by dialing *#06#), short dial numbers, SMS, language, time, date, ring tone and volume settings, stored audio and video recordings, stored images, stored documents, logged incoming, missed or dialled numbers, stored executable programmes and applets (added by the user), stored calendar events, GPRS, WAP and Internet settings.
- **Network subscriber database elements**: Customer names and address, billing name and address, user name and address, billing account details, MSISDN (the subscriber's phone number), IMSI (SIM's identity number), the SIM's serial number, PUK, PIN, services allowed.
- **Network Call Data Record (CDR) database elements**: originating and terminating MSISDNs and IMEIs, duration, type of service, initial serving base station.

Finally, the assignment should instruct the expert to intersect these elements between seizures in order to shed light on connections between individuals, dates and events.

4. Seizure Protection

To avoid annulment risks, seizures should be properly conditioned by police officers. We recommend the following guidelines:

- SIM PIN**s:** Forensic experts frequently receive blocked SIM cards due to three consecutive false PIN presentations. No matter how important the case is, police personnel should avoid experimenting random PINs (the probability of a random PIN being correct is around 0.3%). Instead, during primary interrogation, police officers should systematically ask suspects to:
  - Disclose their PIN codes (never let a suspect remanipulate his mobile phone).
  - Write-down the operator's name (to avoid confusion between SIMs in case the suspect has several handsets, a very frequent case as shown below).

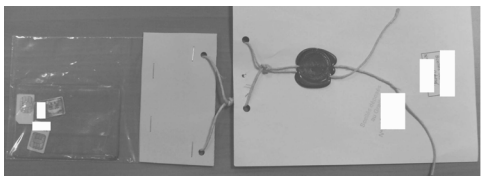

Figure 1. SIM**s in French Evidence Bag**

  - Declare if, to the suspect's best knowledge: 1. He still has the papers received when the subscription was opened[1]. 2. The subscription has expired or is inactive. 3. The SIM or handset is dysfunctional (this declaration is important to avoid later evidence destruction claims).
- **Handset:** By opposition to practitioners who recommend to turn the handset off and place it in an exhibit bag, we recommend the following:
  - If the suspect's handset implements secret modes[2] or secret-code containers[3] ask the suspect to disclose their codes.
  - If the telephone is an uncommon or foreign model, ask the suspect if he still has the handset's power supply (this can shorten analysis cycle-time, especially when dealing with asian phone brands such as DBTEL for instance).
  - Declare if the handset contains, to the suspect's best knowledge, emails, photographs or documents and if the phone is capable of synchronizing with a PC agenda. If so, identify this PC.
  - If the handset is switched-on record or photograph what is on the display. Place the handset in a rigid metal box with a power-supply cable passing through a tiny hole in the box. The box

[1] in these papers the investigator should be able to find the SIM's PUK code

[2] *e.g.* Sharp's V603SH

[3] *e.g.* Sony Ericsson's S700i

IEEE COMPUTER SOCIETY

is assumed to fulfill two functions: 1. Act as a Faraday cage and 2. Prevent people from manipulating the phone's keyboard through the exhibit bag. Place the box in the exhibit bag and keep the device powered-on until handover to the forensic expert. If this is impossible use at least Paraben's Wireless StrongHold Bag.

Cover the handset's infra-red and data ports with thin copper conductive foil tape[4] for extra security.

- If the handset is switched-off, extract the battery and seal it in a separate exhibit bag, place this first bag in a second one and add the handset into it. The goal of this packaging method is twofold: 1. Prevent people from switching on the phone through the bag and 2. Avoid battery misplacement, confusion or loss.
- If procedures allow, write the handset's IMEI on the exhibit bag.

Figure 2. Handset in French Evidence Bag

5. Interception, Correlation, Bugging

Interception is the tapping of a telecommunication that takes place between individuals. We refer the reader to `http://www.gliif.org` for a very rich repository on lawful interception technologies, standards and regulations.

Beyond classic interception, law enforcement agencies frequently **correlate** network information. For instance, serial rapists are frequently identified by correlating two reappearances of a given SIM in the vicinity of two consecutive crime scenes (a detail most rapists won't think of). Blackmailers sending threats from cybercafés are usually discovered by tracing back their emails to a specific cybercafé and comparing the list of SIM-cards present in the vicinity of the cybercafé with a potential list of suspects (*e.g.* list of competing brands employees). Similarly, credit card thieves are frequently identified by correlating the simultaneous appearance of a given SIM and a credit-card purchase done at a specific time and place. The owners of anonymous payphone cards (bought without presenting an ID at any grocery shop) are identified by correlating the usage of a given phone card in two public phone booths with the repeated appearance of a specific SIM in the vicinity of theses booths.

Tracking the repeated physical proximity of two non-communicating SIMs also helps re-construct the ring of relations of a given individual.

It should be noted that more and more law offenders become well aware of theses risks. For instance, on February 23, 2005 The Times reported the story of a couple, David and Jennifer, who was going through a bitter divorce. Jennifer complained that David had sent her death threats and showed the messages to the police. In reality, she plotted against her husband by driving six miles to her husband's new home, put his old SIM card in her second phone and then made the threatening calls to her own phone. Fortunately, a deep enquiry found that the calls had been made on Jennifer's handset[5].

Bugging consists in transforming the handset into a listening device regardless the user's intention to communicate. Bugging may be achieved by replacing the handset's battery (while the suspect is under temporary arrest) by a battery containing an independent listening device or by turning on remotely the handset so as to listen to surrounding conversations (ghost phones). In a specific Asian phone model the camera can even be activated remotely provided that the downloading of applets into the SIM and handset are authorized (this feature is usually disabled though).

6. Handsets as Bomb Parts

CNN[6] reports that on various occasions terrorists have been using the built-in alarms in mobile phones to set off explosives:

- The bombers who targeted commuter trains in Madrid on March eleven 2004 used the built-in alarm clock in mobile phones to set off explosives.
- In Jerusalem, it is believed a call to a cell phone in a rucksack set off a bomb at Hebrew University in 2002, killing seven.

[4] only the top surface of this tape is conductive and it has a silicone based non-conductive adhesive

[5] remember that, as listed in section 3, the Network Call Data Record preserves the originating IMEI.

[6] `www.cnn.com/2004/TECH/04/04/mobile.terror`

IEEE COMPUTER SOCIETY

- One of the Bali bombs outside the Sari nightclub in October 2002 had a cell phone attached, as did a car bomb which killed twelve people at the Jakarta Marriott hotel last August.

The ease with which a handset can be turned into a bomb trigger and the ability to trigger an explosion from a safe distance call are real concerns.

7. The Forensic Expert's Toolbox

The authors are often asked what tools should a handset forensic expert buy or download to get started:

7.1 SIM Analysis Tools

We recommend Gemplus' GemXplore CASE for editing information present in 2G or 3G SIM cards. The tool's capacities stretch beyond the mere inspection of data and care should be taken not to inadvertently modify the seizure (the tool does not always ask for confirmation). GemXplore allows to save data elements as PC files and interacts with the user via a graphical interface offering a drag and drop feature between the SIM and the PC. Despite its somewhat high price we highly recommend this tool to handset forensic experts. Gemplus also markets a second (less expensive), software tool called MySIMeditor which is much easier to use but doesn't allow to visualize all the data elements that GemXplore CASE is capable of accessing. Note that none of these tools will be of any help if the forensic expert does not possess the SIM's PIN or PUK codes.

Figures 3 and 4 show screen shots of this tools (actual forensic elements redacted).

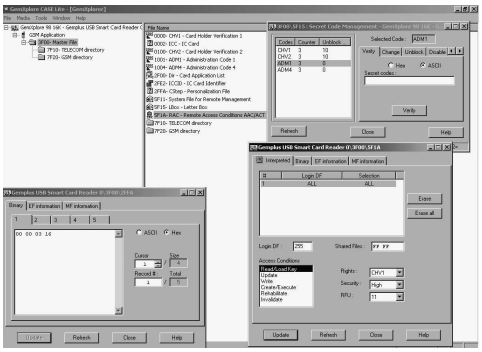

Figure 3. GemXplore CASE

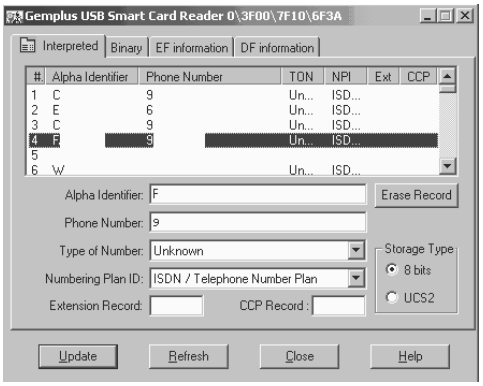

Figure 4. Directory Reading with GemXplore

There are a number of more or less user friendly solutions (*e.g.* by TULP2G and Radio Tactic) that the authors did not benchmark in a forensic context.

A last word about general public tools: Unexperienced forensic experts using general public tools to inspect information present in SIM cards. This should avoided given that such tools usually do not allow to visualize erased SMS messages that frequently contain very significant evidentiary information[7]. Also, before using *any* smart card kit for forensic purposes, the expert should qualify the tool's behavior on a sample and ascertain that none of the ISO-7816 commands sent to the SIM by the tool can possibly affect the information present in the SIM.

7.2 Handset Connection Kits

Gartner Dataquest reports that worldwide handset sales over 2001-2004 break-down as follows: Nokia 37%, Samsung 10%, Siemens 10%, Motorola 10% and a multitude of brands with less than 5% of market-share. In other words, the capacity to analyze four brands provides the forensic expert with the ability to cover nearly 70% of the market's devices. We consider that any serious handset forensic laboratory should maintain privileged relations with these brands' R&D teams and benchmark most new handsets manufactured by these brands.

From a regional perspective in EMEA (Europe, Middle East and Africa) Nokia's market share is around 50%[8] and Siemens' 15% while in Asia, Nokia's share is slightly higher than 20% while Samsung and Motorola represent *circa* 10% each.

Besides the brands' original connection kits we recommend two multi-brand products: The XRY handset analysis

[7] this is possible by proper re-interpretation of byte 2-176 indicating the message's status

[8] this probably explains the emergence of Nokia-specific forensic tools such as Oxygen Phone Manager II for Nokia phones (Forensic version)

IEEE COMPUTER SOCIETY

box by Micro Systemation and Float MobileAgent (freely available). We did not experiment Paraben Forensic's Cell Seizure v3.0 but note its existence for interested readers.

Figure 5. Micro Systemation's XRY

Notes:

- Informal handset flashers (usually undocumented) greatly facilitate access to the handset's memory [2]. As there is no guarantee that the flasher will preserve the evidence present in the device's memory intact, the authors usually disassemble the flasher's code and track its behavior with a logical analyzer to understand its effect on the handset. If this is impossible, an agreement with the investigating judge (see section 7.4) should be reached.

- When analyzing flash cards found in mobile phones care should be taken to equip the examining PC with a write-blocker.

- A number handset models detect SIM replacement and automatically erase all data linked to the previous SIM upon detection of a new one. Forensic analysts should be aware of this and always ascertain experimentally (on an identical handset model) that this cannot cause loss of evidence.

7.3 The Faraday Tent

All handset manipulations should be done in an electromagnetically protected area. A very cost-effective solution for doing so is Paraben's Wireless StrongHold Tent, the tent is easy to setup and take down and guarantees an average shielding effectiveness of 85db from 30 Mhz to 10 Ghz.

7.4 Invasive Analysis

Invasive investigations allow to bypass PINs (which is particularly useful when the seizure is a foreign SIM, the suspect isn't talkative[9] and international cooperation procedure are expected to take too much time or have un uncertain outcome).

There are essentially two methods to bypass PINs: fault attacks and hostile applets. Both require an extreme degree of specialization and specific assumptions about the target. We refer the reader to [3] for an introduction to fault attacks.

Any analysis method which is likely to modify or destroy the seizure should be agreed upon with the judiciary authorities before accepting the case. The authors recommend the following process:

- Buy a sufficiently large number of devices in all points similar to the seizure.

- Use some of these devices to develop an experimental protocol. As the protocol is stable, apply it to the remaining devices and count the occurrences of the six possible outcomes : {information extracted, information not extracted}$\times${device unaltered, device altered, device destroyed}.

- Document the protocol precisely and communicate it to the investigating judge along with the experimental statistics.

7.5 Conclusion

This extended abstract briefly overviews a panel of techniques allowing to extract forensic information from handsets and SIM cards. The authors will demonstrate a few of these tools during the Third IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2006).

References

[1] GSMA Annual Report, www.gsmworld.com, 2004.

[2] S. Y. Willassen, Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Vol. 2, Issue 1, 2003.

[3] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, C. Whelan, The Sorcerers Apprentice Guide to Fault Attacks, Cryptology ePrint Archive, Report 2004/100, 2004, http://eprint.iacr.org.

[9] suspects will rarely refuse to disclose their PINs but would frequently "forget" them...

IEEE COMPUTER SOCIETY