Information & Security: An International Journal

Iosif Androulidakis, vol.37, 2017, 35-44 https://doi.org/10.11610/isij.3703

GUIDELINES ON A MOBILE SECURITY LAB COURSE

Iosif ANDROULIDAKIS

Abstract: The present article, based on an assortment of previous publications and presentations by the author, shows how to prepare and implement an array of security demonstrations in mobile phones. The proposed demonstrations focus on security issues and shortcomings that affect mobile phones' confidentiality, integrity and availability. The resulting overview can be used as guidance, in the framework of a summer school laboratory course and in order to raise awareness among users.

Keywords: mobile, cybersecurity, security, demonstration, confidentiality, guidelines, lab

Introduction

As with every other modern technology, mobile phones face an array of threats targeting the confidentiality, integrity and availability of their service. Researchers and security professionals reveal in an ever increasing rate new attacks and new security shortcomings. At the same time users are not adequately informed about the security implications of their options and settings in their devices. This work aims at facilitating the creation of practical demonstrations to highlight the importance of the topic. In the following pages, after the general requirements section, three more sections follow with demonstrations affecting confidentiality, integrity and availability. Confidentiality section deals with voice and SMS interception as well as with user location finding. The Integrity part mostly focuses on calls and SMS spoofing and identity masquerading. Finally, the Availability section discusses denial of service attacks.

General Requirements

In order to equip the lab where the demonstrations will be performed, the following can be used, along with mobile phones, depending on the exact scenario to be presented.

- A mobile phone tester: These are professional equipment built to assess the functionality of mobile phones and to help troubleshoot them. Although new models are very expensive, an old, second hand tester, especially if it only tests GSM phones, can be bought for a few hundred euros. They can be used in almost all attack scenarios targeting confidentiality, integrity and availability of both voice and SMS;
- Software defined radio board: These boards, coming in various costs, allow the user to implement a radio frequencies receiver and/or transmitter that can be (re)programmed on the fly with the help of software. In the context of this lab, they can help build a mobile phone base station that will be used to mount almost all possible attacks discussed;
- Software: Various open source implementations of mobile phone network standards can be used along the relevant software defined radio. Moreover, software or scripts can automate the steps a mobile phone testing device performs. Simple software can be used to issue commands in mobile phones (such as AT commands). Finally, mobile phone software (most often malware) can be installed to show how a phone can be bugged;
- Spectrum analyser: A spectrum analyser monitors the radio spectrum and presents the radio activity measuring the strength of signals in various frequency ranges. It can be used in the phone location finding demonstration;
- ISDN telephone or ISDN Private Branch Exchange (PBX): An ISDN connected phone (or a telephony switch-PBX) can offer very fast, software controlled signalling, that can be used in the mobile phone location or the battery deprivation attack;
- Smart Card readers: Smart card readers allow the user to directly read the contents of (U)SIM. That is, they can read the contents of the smart card that all GSM/3G/4G phones use for authentication as well as for the provisioning of the telephony service;
- Cables: Various cables (especially when dealing with older phones where special serial port cables are necessary), along with the standard USB cables in order to connect the phones with the computer;
- Specific older GSM phones: There are some older phones that can be (re)programmed to allow the user direct reception or transmission of signal-

ling. Moreover, older phones readily support AT commands. In more detail, AT commands: AT commands (AT stemming from "Attention") were initially developed to configure and Hayes Smartmodem in 1981 and, following, other modems. Later on, their use was adopted for mobile phones. Quite interestingly, apart from the standardized set of commands, manufacturers are also using their own supersets adding platform specific commands. In any case various AT commands exist for Identification, Call Control, Device Control, Catalogues, Messages, etc.;

- Bulk SMS provider: Such providers offer massive, bulk, transmission of SMSs with very competitive prices. The important point, is, that in most cases they allow the user to freely choose the originator number or name that will be shown in the SMS.

With the help of the aforementioned toolset and services, the instructor can continue implementing the demonstrations that follow in the reset of the sections. We will start with confidentiality attacks, integrity ones will follow and finally we will close with availability-denial of service attacks.

Confidentiality

In General

The primary use of mobile phones is, of course, to communicate with others. It all started with voice communication, then sending SMS and now, users can have the full Internet experience at the palm of their hand. Moreover they can run applications on their phone as if it were a personal computer. Both business and personal communications take place using the mobile phone. Privacy, therefore, is (or at least should be) among the ultimate goods the always-connected citizens of today enjoy. Unfortunately, the confidentiality of communications of users is severely impacted by a multitude of attacks and security shortcomings, to the point that the mobile phone itself constitutes a "bug" (monitoring or intercepting device) that can very effectively eavesdrop not only on phone calls but also on ambient conversations. Moreover, written communication, with SMS, or emails and instant messaging can also be intercepted. Users store in an ever increasing rate personal information in the phone,[1] including multimedia material and photos that can end up in the wrong hands. Finally, the whereabouts of a user can be revealed, helping to locate him or even access his travelling and everyday activities.

Malicious Software

Since smartphones are, essentially computers, they can run software. There already exist dozens of malicious software/intercepting/spy suites, available for all operating

systems that are able to eavesdrop, record, copy and relay information and files and track the location of the user. They either use client-server technology uploading the intercepted information to specific servers using the phone's internet connectivity, or, they relay information using SMSs. However, such software needs to be installed in the victim's phone, either directly by the attacker (e.g. stealing the phone and returning it back), or by the user himself, tricked into installing it (for example with the spy functionality hidden in an application or game). In any case, with costs as low as a few euros per month, or an equally affordable one-off purchase fee, it is easy to buy and demonstrate the use of such software, in a controlled environment.

Man-in-the-Middle Attacks

Exploiting the fact that I pre-3G networks base stations do not authenticate themselves to the mobile phones, man-in the-middle attacks can very-easily be mounted. The tutor, in a controlled environment, can use software defined radio or even GSM testers [2,3] to mimic the behaviour of legitimate infrastructure the same way attackers do. The intermediate step in this attack disables encryption (it actually informs the mobile phone that the base station does not employ encryption), and therefore all communication is sent in plain between the rogue base station and the victim phone. As such, the communication is readily available for eavesdropping and recording. Moreover, in the same demonstration, the tutor can show how attackers can use downgrade attacks. Indeed, attackers using a jammer (as we will discuss in the Availability section), block the 3G band and therefore mobile phones are forced to communicate with GSM infrastructure, falling prey to the man-in-the-middle attack.

Ciphering Indicator

Exactly because of the dangers of unencrypted communication, even since GSM era, standards have mandated the use of special indicators to inform the users as to whether encryption is present or not. It has been shown, however, that most manufacturers and, even worse, the modern operating systems do not offer this kind of visual warning to the user.[4,5] Moreover, in cases where the indicator is present, users are still not aware of its meaning while at the same time the feature is seldom mentioned in the manuals. In this scenario, the tutor can use the set-up of the previous demonstration (either a GSM tester or a software defined radio along with the relative software) to test and demonstrate whether participants' phones actually employ the ciphering indicator.

Revealing Users' Preferences

Short messages can reveal information and user behaviour violating her privacy. In fact, abusing the delivery report of messages a plain user (with no insider's information whatsoever) can find out whether the mobile phone of another user is switched off and the exact moment the user turns it on, and vice versa. This is possi-

ble since the delivery report message will be delivered to the originator as soon as the mobile phone is switched on and will be pending for as long as the mobile phone of the recipient is switched off. Smart techniques [6] make it possible to implement this attack without the unsuspecting user ever knowing he is receiving these messages, since, apparently, sending plain messages (even empty) for this purpose will be immediately spotted. More information on these types of messages will be given in section discussing availability attacks, since the same invisible messages can be used to drain the battery of the victim. In this given demonstration, the tutor uses invisible messages to assess whether a mobile phone is switched on or off. In case there are areas around with no reception (e.g. in a basement), she can also demonstrate that the method can provide a hint that the user might be in this specific no-signal area.

Location

A more elaborate method to locate a given mobile phone with great accuracy, only given as input the phone number and the greater area it is located in (e.g. the city or the neighbourhood) can be found in the works of the author.[7] The principle of operation is based on techniques that stealthily force the mobile phone to transmit radio-waves (as we will describe in the availability section) according to the will of the tracer. Following that it is possible to trace the direction the phone transmits from, based on the reception of radio waves with a directional antenna, using a spectrum analyser, a frequency receiver-scanner, a broadband receiver, or a GSM tester, zooming in in smaller and smaller areas until the exact position of the phone is ultimately found. When sufficiently close, a simple AM radio tuner can also be used. To demonstrate this, the audience can hide a mobile phone in a given area-building, and the tutor can locate it.

Integrity

In General

Integrity shortcomings, in this work, are mostly connected to caller-id and SMSs. There are services in the Internet where the user can place calls choosing whatever caller id he wants. Masquerading occurs not only in voice calls but also in SMS. The identity of the sender can be changed in order to make a malicious message appear legitimate or for spam purposes. We will not discuss integrity problems, connected to economic fraud involving mobile phones.

Caller-ID/SMS Spoofing

There are many services in the internet that allow the user to freely pick a caller-ID and place a call using it.[2] It is a trivial exercise to register in such a service, pay the fee, and demonstrate the effect. If the attacker chooses a phone number that is already present in the contacts catalogue of a device, then when the victim's phone will match

the number to the entry in the catalogue and the screen will show that the call is arriving from that contact. It is equally easy to buy service from a bulk-SMS provider that allows the user to send a message with whatever id she wants (usually there is a limit for a string up to 11 characters or a number up to 16 digits). Again, if the number is found in the contacts catalogue of the device then the SMS will appear as if it were arriving by a trusted person and not by a third malicious user.

Checking SMS and Avoiding SPAM

Technically savvy users can assess whether an SMS is spoofed or not. In order to do so, they need access to the raw message, as it reaches the phone, before being presented in the screen. The basic check to perform is whether the message service centre is in the same country as the originator's phone number implies. For example, an originating number that appears to be Bulgarian with a serving centre's number that appears to be from India is a strong indication that the message might be spam. In this demonstration, based on a system to fight SMS spam as presented in [8] and [9], the tutor can show the interworking of SMS.

Catalogue Integrity

As all users know, phones map the incoming numbers in calls and SMSs (as well as the numbers dialled for outgoing calls) to the respective entries found in their catalogue list. However, they do so by matching only the last digits and not the whole number.[2, 8, 9] This can be abused so that while the phone is calling (or receiving a call or SMS from) a given number, another contact is shown in the display. Let's assume there is a contact named "Iosif" with number "1234567890" in a given phone. The tutor can show that if he dials "34567890" or even "4567890" the screen shows "Iosif". What is more, if he dials "98765432104567890", then the phone calls number "9876543210" but shows "Iosif" (because it only matches the last digits, while the network strips the extra digits to make the call). In short, the user must never trust the displayed name contact presented, and should cross check with the actual number (and not the "translated" contact) dialled/calling.

Other SMS Integrity Issues

Although part of the standards, and with valid reasons to exist, specific SMSs can be abused to affect the integrity of the data in the mobile phone and with potential for malicious use. One such category is SMSs that can control phone's indicators (such as the indication of new voice messages). An attacker can change their status or even permanently switch on an indicator without the user being able to restore it.[6] Another category concerns messages that can later be automatically deleted or replaced by another message.[2] A third characteristic type of SMS can present itself directly on the mobile screen. It is known as flash SMS or more accurately class 0 messages. The re-

cipient does not have to press any keys to read the message as it directly pops-up, in the place of the logo of the network, or below it or in a special window opened for this purpose. All these SMSs can be easily demonstrated using either a bulk-SMS provider that allows binary messages, or using a mobile phone connected to a PC. There also exist phone applications that allow the user to send some of these types of messages (namely the "flash" SMS)

Availability

In General

Given the penetration of mobile phones in modern life, and the increased applications that are now running on phones, it is not a surprise that users have been, more or less, very close connected to their devices. There are even cases of "addiction" phenomena, where users cannot live a normal life without their phone. At the same time, a mobile phone can save lives in emergency situations and where no other communication means is available. These aspects render the availability of the mobile phone service quite important. However, attackers can use many techniques to hinder or completely prevent the use of mobile phones, what is known as Denial of Service attacks. In any case it is quite "normal" for smartphones to require daily charging, while users themselves are not following best practices to minimize energy consumption.[10] Therefore, the techniques presented discussed in this section can even easier lead to denial of service.

Jamming

Denial of service attacks can be escalated using RF (radiofrequency) jamming. The attacker jams the radio spectrum in the band of operation of the mobile phones transmitting high power electromagnetic noise that inhibits normal signalling. Depending on the power of the transmitting jammer, the area of denial of service can extend from one room to a whole city. Jamming affects all mobile phone users around the jammer, so it is not practical for a targeted attack. Moreover, while dozens of such products are available in the internet, their use is illegal in most countries. Depending on the applicable law, the tutor can readily show the effects of jamming in a controlled environment.

Signalling

Instead of jamming, special transmissions in the radio interface of GSM can quickly deplete all available resources. This can be carried out using specific mobile phones, with their firmware modified to act in ways not foreseen by the standards. More sophisticated techniques can target the network backbone leading to extensive areas service black-out. Additionally, a fake base station can instruct a mobile phone to stop working as presented in the works examined in [2].

Old-School Techniques

A very elementary (but more annoying) attack vector is to place consecutive calls to a phone, effectively making it ring nonstop. The user is then forced to switch it off or mute it, leading to a self-induced denial of service result. Additionally, using software (or bulk-SMS providers), the attacker can send hundreds or even thousands of messages to the victim's mobile phone as shown in [6]. In older devices the memory will quickly fill up. In modern phones with ample memory, the user will receive messages but will not be able to immediately distinguish the original message intended for him among the massive amount of messages received. By constantly changing the originator number (possibly using numbers belonging to persons that could be in the catalogue of the victim) the effect is even more amplified.

Battery Deprivation Attacks

The attack scenarios proposed in [11] incorporate repetitive invisible SMSs and/or very short calls interrupted before the actual ringing of the phone. The main concept is that repetitive reception of stealth SMSs and/or very short calls forces the phone to continuously transmit. At the same time the user never realizes that an attack takes place since the messages or calls do not show up. However, the energy consumed completely depletes the battery of the victim leading to a denial of service. In this demonstration the tutor can show how the phone is constantly transmitting and the battery quickly discharges. Moreover, these forced transmission techniques can be used to help locate and fingerprint mobile phones based on their distinctive transmission patterns as mentioned in [7].

Software Bugs

Another means of denial of service using SMSs takes advantage of bugs in the software of mobile phones. Normal looking SMSs (consisting of special or invalid characters or long names) or specially crafted ones, that deviate from the specifications and requirements of the standards in terms of structure and syntax are sent to the phone.[2] Due to bad implementations and errors, instead of being discarded, they lead to crashing, rebooting, freezing or losing network access. In some cases they can even lead to a constant rebooting cycle.

Conclusion

As described in this work, it is easy to demonstrate the security shortcomings of mobile phones, in an interactive user experience, where they can personally test and see the results in a controlled lab environment. This is particularly important, since as recent research has shown, most users acknowledge that are not security aware. There are also users that feel secure and confident, but, in reality they are less secure than they think they are.[12] Along the demonstrations, raising user awareness can also be

enhanced using software. Indeed, in [13] we have proposed a system that pinpoints and informs vulnerable mobile phone helping them protect themselves. Closing, an extension to the lab/course/demonstrations proposed here, in a more advanced level, could deal with mobile phone forensics.

Endnotes

1. Iosif Androulidakis and Gorazd Kandus, "A Survey on Saving Personal Data in the Mobile Phone," *Proceedings of Sixth International Conference on Availability, Reliability and Security, (ARES 2011)*, Sept. 2011, pp. 633-638.
2. Iosif Androulidakis, *Mobile Phone Security and Forensics: A Practical Approach*, 2nd edition (Springer. March 2016)
3. Iosif Androulidakis, "Intercepting Mobile Phone Calls and Short Messages using a GSM Tester," *Proceedings of CN2011, CCIS 160* (Springer Verlag, June 2011), 281-288.
4. Iosif Androulidakis, Dionisios Pylarinos, and Gorazd Kandus, "Ciphering Indicator Approaches and User Awareness," *Maejo International Journal of Science and Technology* 6, no. 03 (Dec. 2012): 514-527.
5. Iosif Androulidakis and Gorazd Kandus, "Mobile phone security – awareness and practices," *The Journal of the Institute of Telecommunications Professionals (ITP*, 7, no. 1 (Jan-Mar 2013): 16-23.
6. Iosif Androulidakis and Chris Basios, "A plain type of mobile attack: Compromise of user's privacy through a simple implementation method," *Proceedings of 3rd International Conference on Communication Systems Software and Middleware 2008, COMSWARE, 6-10 Jan.* 2008, pp.465-470.
7. Iosif Androulidakis, Vasileios Vlachos, and Costas Chaikalis, "An application free method to locate a mobile phone in a given area without user consent or provider help," *Proceedings of the International Conference on Information and Digital Technologies (IDT2015), Jul* 2015, pp. 6-10.
8. Iosif Androulidakis, Vasileios Vlachos, and Alexandros Papanikolaou, "Spam Goes Mobile: Filtering Unsolicited SMS Traffic," *Proceedings of 20th Telecommunications Forum (TELFOR 2012), Nov.* 2012, pp. 1452-1455.
9. Iosif Androulidakis, Vasileios Vlachos, and Alexandros Papanikolaou, "FIMESS: FIltering Mobile External SMS Spam," *Balkan Conference in Informatics 2013 (BCI 2013)*, September 2013, pp. 221-227.
10. Iosif Androulidakis, Vitaly Levashenko, and Elena Zaitseva, "An empirical study on green practices of mobile phone users," *Wireless Networks* 22, (2016): 2203–2220.
11. Iosif Androulidakis, Vasileios Vlachos, and Periklis Chatzimisios, "A methodology for testing battery deprivation denial of service attacks in mobile phones," *Proceedings of the International Conference on Information and Digital Technologies (IDT2015), Zilina, Slovakia, 07-09 Ju,l* 2015, pp. 1-5.
12. Iosif Androulidakis and Gorazd Kandus, "Feeling Secure vs. Being Secure, The Mobile Phone User Case," *Proceedings of 7th International Conference in Global Security, Safe-*

ty and Sustainability (ICGS3), Lecture Notes of the Institute for Computer Sciences 99, Aug 2012, pp 212-219.

13. Iosif Androulidakis and Gorazd Kandus, "PINEPULSE: A system to PINpoint and Educate mobile Phone Users with Low SEcurity," *Proceedings of 7th International Conference in Global Security, Safety and Sustainability (ICGS3), Lecture Notes of the Institute for Computer Sciences* 99, Aug 2012, pp 62-66.

IOSIF ANDROULIDAKIS (BSc in Physics and PhD and MSc in Electronics) has served as Head of the Telephony Department in the Network Operations Centre of the University of Ioannina, Greece. He has an active presence in the ICT security field having authored more than 25 relative papers and having presented more than 50 relative talks and lectures in international conferences and seminars in 15 countries. His research interests focus on security issues in PBXs (private telephony exchanges) where he has more than 15 years of experience, as well as in mobile phones and embedded systems, and holds two patents. He is a member of IEEE (Technical Committee on Security & Privacy) and ACM (Special Interest Group on Security Audit & Control). Finally, he is a certified ISO 9001:2000 quality systems auditor as well as a certified auditor and consultant for ISO 27001:2005 Information Security Management Systems. *E-mail*: sandro@noc.uoi.gr.