Manipulating Mobile Devices with a private GSM Base Station - a Case Study

Christoph Kemetmüller, Mark Seeger, Harald Baier, and Christoph Busch

Center for Advanced Security Research Darmstadt (CASED)
Mornewegstraße 32
64293 Darmstadt, Germany
{christoph.kemetmueller,mark.seeger,harald.baier,christoph.busch}@cased.de

Abstract. The ascending number of mobile devices is accompanied by an ever increasing effort of malware developers to find new means of infecting them. GSM, as a basic technology for mobile communication used by most mobile phones, lacks certain security aspects. In order to access a provider network the mobile equipment authenticates itself against the network, whereas the latter does not have to prove its authenticity. Based on this design flaw we demonstrate an approach to remotely reconfigure a mobile device in order to manipulate its system settings. This can give an attacker the opportunity to hijack data connections or even infect the mobile device with malware. Examination of the applicability of our theoretical approach in a field experiment proofed the lack of security in GSM. Reconfiguration of mobile devices during the field experiment was only successful for a few devices because of the technical limitations and user cautiousness.

Keywords: GSM; Client Provisioning; Mobile Security

1 Introduction

The current number of Global System for Mobile Communications (GSM) and High Speed Packet Access (HSPA) subscriptions is 3.976 billion [1,2], which represents almost 90 percent of global mobile subscribers. The remaining 10 percent are comprised of code division multiple access (CDMA) and other technologies. According to [2] the number of subscriptions is still going to rise until 2014 due to emerging markets and the low price equipment. At the same time most mobile personal devices nowadays offer a large set of functionality way beyond speech communication and short text messages and for that reason mobile devices can rather been seen to be nodes in a mobile internet where each node potentially grants access to valuable assets. As with nodes in the wired internet this provides motivation for attackers to perform malicious actions against the subscribers, ranging from Denial-of-Service (DoS) attacks to identity theft. Recent developments in the area of Software Defined Radio (SDR) enable everybody to setup their own mobile network. The expenses to buy a SDR and develop

the software are minimal compared to conventional network equipment. A working example for the required software is openBTS[1], which was made publicly available by its developers. The idea behind openBTS is to provide researchers and less developed countries with an affordable GSM system. Prior to this development research has concentrated on the encryption scheme utilized in the GSM communication protocol [3,4]. Current work includes practical attacks on the encryption scheme [5] and vulnerability discovery on the mobile station (MS) of the customer [6]. Nohl and Paget [7] present the discoveries they experienced during tests with openBTS and MSs and, moreover, give an overview of attacks on the encryption scheme. The research of over-the-air (OTA) reconfiguration in [8] is closely related to GSM security and this paper in particular.

One specific security flaw in GSM is the lack of mutual authentication. The MS has to authenticate against the network before getting access to the network. On the other hand, authentication of the network is not covered by the respective authentication algorithm A3 [9]. Identification of the MS in order to access the right subscriber information for billing and authentication in the provider's Home Location Register (HLR) happens via the secret International Mobile Subscriber Identity (IMSI) that the handset has to send to the base transceiver station (BTS) before the actual authentication process is started. An IMSI catcher can exploit this flaw and thus could for instance enable law enforcement to intercept calls. This hardware device is expensive and not publicly available. Yet, with a SDR, openBTS and knowledge of the network identification code everybody is capable of intercepting GSM communication. Furthermore, an adversary can by these means gain access to secret subscriber information, for instance, the IMSI.

A provider offers a multitude of services for its customers. Keeping these service configurations for each MS up to date is not feasible via direct access through customer service. Also taking into consideration the handset's numerous configuration settings (e.g. Synchronization, Wireless) amplifies the urge for remote OTA management of MSs. This issue is addressed by the Open Mobile Alliance (OMA) Device Management working group and the OTA Client Provisioning standards in particular.[2] Client provisioning allows anybody to send configuration updates to a MS. Before a provisioning message is accepted by the handset its authenticity is validated by checking a Hash-based Message Authentication Code (HMAC) value. A network operator can use the secret subscriber information as the shared secret for the HMAC function. As mentioned in the preceding paragraph, an adversary can also gain access to this secret information. Consequently, he is capable of constructing authentic configuration messages in order to abuse the client provisioning functionality, for example, to redirect internet connections or install malicious software on the MS.

In this paper we present a novel approach to attack handsets with the aim of controlling the MS's configuration. We show that the GSM standard endorses an adversary in alluring MSs into connecting to a private BTS in theory and provide

[1] see `http://openbts.sourceforge.net` (accessed 02/01/2010)

[2] see `http://www.openmobilealliance.org/Technical/DM.aspx` (accessed 02/01/2010)

evidence for its practical applicability as experienced during our experiments. Consequently, we implemented a basic proof of concept, based upon a SDR and openBTS to prove the theoretical aspects of the attack. To assess the practical effectiveness of the approach we conducted a field experiment in combination with a questionnaire to estimate the probability of a successful attack. From the perspective of an attacker our approach provides new ways of attacking mobile devices, which can be synthesized into follow-up attacks.

The remainder of the paper is organized as follows. An overview of related work in the area of GSM and mobile security is presented in Section 2. Section 3 introduces the technical background for our approach. The technical description of the implementation is presented in Section 4. We provide validation of our approach via a field experiment in Section 5. Finally, we give a conclusion and describe future work in Section 6.

2 Related Work

The well-known flaws in the GSM standard have been addressed in [10] and taken into consideration for subsequent standards. The approach of forging OTA Client Provisioning messages has already been investigated in [8]. Yet, our technique differs in that it also involves a private BTS, which gives an adversary a bigger scope to attack mobile devices. Compared to the conventional OTA attack, this new approach introduces novel use cases.

Other research, which is related to our work of gaining a certain level of control over a MS, concentrates on mobile malware. Wang et al. [11] modeled the potential spreading patterns for malware on mobile devices. Their research on propagation of mobile malware concentrated on Bluetooth technology, as introduced in the first emerging worms for mobile devices, for instance, Cabir [12], Commwarrior [13]. Propagation was limited in terms of physical proximity to other vulnerable mobile devices. Wang et al. also created a spreading model for malware propagating via multimedia messaging. Their conclusion is that for a major mobile malware outbreak the market would have to be more uniform. Our approach is based on a well-supported standard and is only limited by terms of base station transmission range. The basis in [14] is mobile messaging and a vulnerability in a VoIP service. Their results point out the limits of self-propagating malware in terms of network capabilities as well as possible counter-measures on the network level to oppose a malware outbreak.

As our approach omits the network provider, monitoring the mobile device is a good option to counter the novel technique. One indicator for an infection is an increased number of processes. Kim et al. [15] took up this concept and presented an approach to detect anomalies in power consumption levels of a mobile device. Their starting position is malicious software that tries to utilize WiFi with its increased energy requirements. Another indicator for a potential infection is taken into consideration in [16]. By monitoring the usage of text messaging and Bluetooth activity of a mobile device via an agent process, ibid. called SmartSiren, malware would immediately be detected when trying to contact or

infect other systems. Their assumptions are based on known malware, e.g., Cabir [12], Commwarrior [13] and FlexiSpy [17]. The developer of openBSC[3], Harald Welte, started investigating protocol conformance and MS stability based on fuzzing the radio interface [6].

The main goal of this paper is to point out yet another security issue with GSM. Others are going towards the same direction with their research. Hulton [5], for example, is concentrating on the network security of GSM and recently presented his work on passively intercepting GSM traffic with a SDR. The aim of Hulton's work is to point out the weak encryption scheme utilized in GSM. Nohl et al. [7] perform similar efforts to attack the GSM encryption. By distributedly calculating a rainbow table they provided the means to decrypt recordings of GSM communication.

3 Technical Aspects

Certain aspects and flaws of the mobile network technology are essential for our approach. Both concepts, the GSM protocol and the OTA Client Provisioning, and in particular their particular issues concerning security are presented in the subsequent section.

3.1 GSM Fundamentals

A GSM network is built upon numerous subsystems and utilizes various protocols for the different network sections, e.g., the air interface or the wired network. Those have been designed more than 15 years ago and nowadays miss certain security features nowadays deemed essential for wireless networks.

The significant security problem in GSM protocol is the lack of mutual authentication between the BTS and the MS. As standardized in [9] the authentication algorithm A3 only covers mobile device authentication towards the base station but not the base station authentication towards the MS. When the specifications were created this problem has not addressed, as a man-in-the-middle attack was unfeasible because of the lack of the required technical equipment. Lawful interception on the other hand was made possible with this design flaw.

Fundamental to being able to exploit this flaw is getting the MS to connect to a private cell. The handset keeps an internal list of available cells and chooses the most suitable one in terms of connection quality according to the two standardized criteria [18]. One criterion is used for cell selection whereas the other criterion is used for cell reselection, which is one being more relevant for our approach. It selects the cell with the best radio connection, taking into consideration the signal strength as well as the duration the cell has been visible on the handset. One crucial factor for the method of selection is the signal strength emitted by the BTS for a single cell.

Yet, before having a MS connect to a private base station another prerequisite must be met. The handset has an internally stored list of preferred networks

[3] see `http://openbsc.gnumonks.org` (accessed 02/02/2010)

when connecting to a new cell. This means that it will connect to the best, in terms of signal strength, available cell under the control of any of the preferred networks. Identification of the network provider is merely based on an operator identifier that is broadcasted on the Broadcast Control Channel (BCCH) of every cell. This identifier is constructed from the Mobile Network Code (MNC) and the Mobile Country Code (MCC). Every country is identified by a three digit MCC whereas the MNC identifies the operator; the MCC for Germany is, for instance, "262". The allocation of the MNC numbers is administered by a country-specific official institution, for example, the *Bundesnetzagentur* in Germany. For instance T-Mobile Germany was assigned the MNC "01" and is consequently identified by "262-01". These identifiers are publicly available on the internet, or they can either be exposed by the MS or intercepted from the air interface. Impersonating a particular network operator requires little effort compared to setting up a working GSM base transceiver station.

In retrospect, broadcasting a regular operator identification code makes one's own openBTS based fraudulent cell appear to be a legitimate base station for GSM handsets, as there is no mechanism for the MS to verify the genuineness of the MCC-MNC combination.

3.2 Client Provisioning Mechanism

OMA Client Provisioning is the process by which a Wireless Application Protocol (WAP) client is configured with a minimum of user interaction. OMA Client Provisioning V1.1 [19] is a backwards compatible extension of the client provisioning functionality included in WAP 2.0. Client provisioning enables a network operator to send new settings over the air. After receiving the settings, depending on the handset's reconfiguration mechanism, either the customer manually confirms the installation of the new device settings or the handset is reconfigured transparently. Subsequently, the subscriber is able to use the new configuration.

The options and structure for OMA Client Provisioning messages are defined in [20]. Numerous mobile device characteristics are used to configure the different device settings, for example, proxies, network access points (NAPs), vendor specific parameters, options related to applications and client identity parameters. Additional characteristics may also be added.

A directory listing mobile equipment (ME) with their respective supported version of the OMA Client Provisioning specifications is not available. Yet, the OMA is comprised of companies working in the GSM sector, for example, Nokia, Ericsson, Microsoft, Orange SA, and was formed in 2002. Devices introduced into the market after this date presumably support the OMA Client Provisioning specifications.

In terms of security the provisioning mechanism incorporates shared-secret authentication of messages. This is achieved by mutual computation of a HMAC value. The HMAC value is calculated by feeding the encoded provisioning content as well as the secret to the hash algorithm, which is the Secure Hash Algorithm 1 (SHA-1) in the case of OMA Client Provisioning. OMA Provisioning Bootstrap supports four different security mechanisms [21]. All four are based on a

shared secret between the MS and the sender of the provisioning message. One of them is called "USERPIN", which requires the recipient to enter a message specific Personal Identification Number (PIN) (not to be confused with the Subscriber Identity Module (SIM) PIN) in order to validate the settings. The user must know the PIN that was utilized to sign the OTA message to reproduce the HMAC value. Secret subscriber information, which is the IMSI, represents the shared secret for the HMAC calculation of the "NETWPIN" security option. Checking the authenticity of the message happens transparently without any user interaction. "USERNETWPIN" represents a combination of the earlier described options. The secret key for the HMAC calculation is compromised of the subscriber's IMSI and PIN. To validate the settings the subscriber has to enter the PIN so the HMAC value can be reproduced and verified. "USERMACPIN" security relies on an out-of-band delivery of the authentication information (HMAC and PIN) which makes it the least preferred method for OMA Client Provisioning. The particular security type utilized in a provisioning message is specified in the provisioning message header, along with the respective HMAC value.

4 Reconfiguring a Handset

First of all, we are going to describe our approach on how to attack MSs. To review and put our attack to test we implemented a proof of concept. Assembling the test system required coping with technical issues with the SDR hardware.

4.1 Attack scenario clarification

For our approach we combined the shortcomings described in Section 3. Provisioning messages sent by a network operator are usually secured with the "NETWPIN" mechanism, as the required user interaction for these reconfiguration messages is minimal. The network operator has knowledge of the secret IMSI number that is utilized with these security settings. By setting up a private BTS, taking into consideration the limitations concerning cell selection, an attacker is able to gain knowledge of this subscriber identification. At this point, after retrieving the IMSI during the MS's authentication, the adversary is capable of creating authentic provisioning messages. Figure 1 depicts the three essential steps during an attack.

The different characteristics available for configuration are covered in [20]. With these options it is possible to rewrite the homepage of the handset's browser or reconfigure the data network connection in order to route all internet traffic through a private proxy. Depending on the latent shortcomings in the MS's security, an attacker might even install additional software on the device.

To send these configuration updates to the handset in a private GSM cell, an adversary only needs to encode the content according to the GSM specifications and incorporate them in a text message. As the header of this message matches a default text message it can be delivered using the traditional way.

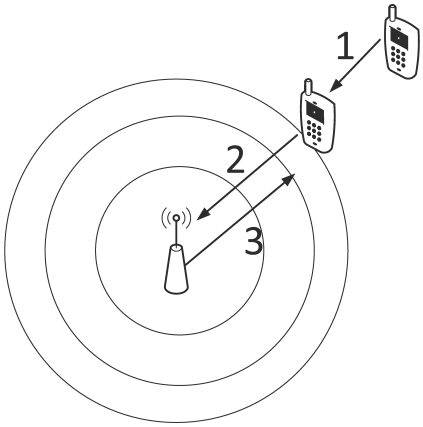

Fig. 1. First of all (1), the handset arrives in transmission range of the private BTS. Afterwards (2), it selects the private cell accordingly to the cell reselection criterion and connects to the same. The third and final step is to send the provisioning message to the handset in order reconfigure it.

Different scenarios relying on the OMA Client Provisioning functionality are viable, depending on the ME capabilities. Some particular attacks are described in [8].

The general driving force behind this attack is gaining control over a MS on a long-term basis. Particularly industrial espionage is one potential scenario. Employees might be equipped with one particular type of MS. An attacker would forge a convenient reconfiguration message and place his private BTS close to the company facilities. With the handsets under the attacker's control retrieving confidential company information is straightforward. Botnets will also focus on mobile devices for different reasons, e.g., mobility, lack of security, number of potential victims. By reconfiguring mobile devices with our approach a network operator cannot take actions to prevent this kind of attack.

4.2 Practical Realization

The principal component for the realization of the test implementation is a freely programmable and adaptable hardware device. Tampering with the different layers of the GSM protocol is one of the requirements that have to be met when performing research in this area. Acquiring professional equipment for running a GSM network would not allow unhindered research. The Universal Software Radio Peripheral (USRP) from Ettus Research LLC met the requirements.[4] It is just the plain motherboard for signal processing, so we also had to commission the appropriate transceiver boards plus antennas. As this motherboard is general purpose hardware many different types of daugtherboards are available. Each of

[4] see `http://www.ettus.com/order` (accessed 02/02/2010)

these is equipped for a particular frequency range and transmission requirements. The full equipment for the tests consists of a rev4 USRP, two RFX1800 transceiver-daugtherboards, each combined with a VERT900 antenna.

A SDR, the USRP in particular, provides a hardware interface by which it can be accessed via the software that performs all the signal processing. GNU radio[5] is a software component specifically developed for the USRP and takes care of the signal processing and interfacing to the SDR. With this software package a developer is not confronted with all the different aspects of signal processing while being in control of the actual data.

The final component for running our own GSM network is the logics behind the signal processing. This important aspect is handled by openBTS, a project that provides the essential GSM functionality and requires GNU Radio to interface the USRP. Another similar project is openBSC, which utilizes legacy hardware. Yet, the community behind openBTS is more active and it is based on the GNU radio project which offers adaptability for future research in combination with the USRP.

Running a radio network in our test lab environment in Germany requires an official permit by the *Bundesnetzagentur*. To comply with these regulations we applied for a test license for our system and received an allowance for that particular location and for the Absolute Radio Frequency Channel Number (ARFCN) 866. This allotted channel corresponds to an uplink frequency of 1781 megahertz (MHz) and a downlink frequency of 1876 MHz.

The software had to be configured to the allotted ARFCN 866 as openBTS is by default tuned to the 900MHz frequency band and required minor changes to be able to transmit with 1800MHz.

4.3 Challenges during Realization

One major issue in implementing a working GSM network based on openBTS was an infirmity with the internal clock of the USRP. The GSM standard demands an accuracy of 0.05 parts per million (ppm) for this particular part, whereas the clock on the USRP drifts with about 20 ppm. The consequence was that our test handsets (HTC Snap) were not able to correctly identify the BCCH, not to mention successfully establishing a connection to the BTS.

The solution to this problem was to find an external clock with a proper accuracy, disable the onboard clock and feed the external signal to the USRP. An assembly kit "FA-SY 1"[6] by the German magazin for amateur radio and radio technology "funkamateur" could provide the required 64MHz while maintaining an acceptable drift. Audits of the output frequency as to adjust the onboard heating module allowed for a accuracy of about 8 ppm before the clock was fit into the casing of the USRP. This variance between the tests of the USRP showed enough stability for our test handsets to successfully connect and allowed us to place a test call between the phones.

[5] see `http://gnuradio.org/redmine/wiki/gnuradio` (accessed 02/01/2010)

[6] see `http://www.box73.de/catalog/product_info.php?products_id=1869&osCsid=f7t0mheibgj27p8h5oeknkdj54` (accessed 02/01/2010)

4.4 Lab Testing

Sending a provisioning message is not a feature of openBTS and had to be added to its functionality. The implemented functions take the XML configuration (see Listing 1.1) and calculate the HMAC value over that data using the "NETWPIN" security mechanism. As soon as a MS connects to the openBTS base station the previously mentioned functions assemble the message as well as the corresponding HMAC value and send it to the target device.

```
<wap-provisioningdoc version="1.1">
<characteristic type="APPLICATION">
        <parm name="APPID" value="w2" />
        <characteristic type="RESOURCE">
                <parm name="URI" value="http://www.cased.de" />
                <parm name="NAME" value="CASED" />
                <parm name="STARTPAGE" />
        </characteristic>
</characteristic>
</wap-provisioningdoc>
```

Listing 1.1. An OMA Client Provisioning Message for setting the browser homepage that we used during the experiments.

For testing the reconfiguration mechanism of our proof of concept we could utilize two HTC Snap handsets with Windows Mobile 6.1 Standard installed. The installation of the settings on the particular test devices happened transparently. Solely after the reconfiguration an information message would acquaint the user with the following message: "Your device settings were changed successfully".

5 Field Experiment

To evaluate the practicality of our proof of concept we conducted a field experiment in conjunction with a survey to assess mobile security awareness of subscribers. Prior to the experiment we estimated the probability of a successful attack depending on the technical knowledge and security awareness of the subscriber. Also the attack might be subject to certain constraints and limitations that can only be experienced during real world conditions.

5.1 Scenario Clarification

For the field experiment with the USRP a suitable location had to be found. Retaining the transmission power of the SDR and taking into consideration the cell reselection criterion narrows down the potential locations to test our approach. Good locations either provide poor reception or are subject to continuous changes of the available cells. Setting up a private BTS at such a location facilitates the attack as handsets will more likely connect to it because of better signal strength and period of visibility of the cell (cell reselection criterion).

A EuroCity train constitutes a good playground as it traverses multiple cells during a journey and it also provides power to run the hardware. Yet, many currently deployed carriages are equipped with GSM repeaters that act as a radio interface link between the outside provider BTSs and the inside of the carriages in order improve the service quality therein. Because of that, we had to reason out disruptive aspects for the test prior to commencing the actual field experiment. Running the base station was technically possible and the test phones connected to our GSM cell.

For the field experiment auditability and verification of the results were essential aspects. To comply with these requirements the homepage of the phones' browsers were reconfigured via a OTA Client Provisioning message (see Listing 1.1). Assessment of the successful reconfiguration happened as part of a questionnaire, which provided additional data to estimate the success rate of our approach.

5.2 Experiment Results

During the tests different network identifications were configured in the BTS. Prior to commencing the actual experiment the functionality of the systems was validated with the test devices and a test network identification (MCC=001, MNC=01). This identification should not be found in the real world as it is solely used for test equipment. For the actual experiment we planned to utilize German telecom provider identifiers to imitate legitimate base stations.

Surprisingly, during testing the openBTS functionality numerous mobile devices connected to our GSM cell within minutes. The IMSI latter gave indication about their particular home network provider, as the network provider identifier is part of this number. The connected MSs came from different network providers and favored the test network to their home provider. Running the BTS with the three major German network provider identifications (T-Mobile, Vodafone, e-plus) for the same time period resulted in disproportionally less handsets establishing a connection to the base station. For that reason part of the field experiment was carried out with only relying on the test network identification.

In conformity with the lab tests, the OTA configuration updates were sent to the MSs on establishing a connection to our BTS. Auditing the performance of the reconfiguration was carried out as part of the questionnaire. This data should be combined with the subscribers' answers provided in the survey in order to calculate the likelihood of a successful attack as a function of subscriber security awareness.

We expected the overall rate of success to be moderate. Furthermore, we estimated that with increasing familiarity with IT security the chance of a successful attack would decline. The assessment during the survey showed that all mobile devices encountered during the experiment required the user to manually decide whether to install our update to the mobile device or to discard the provisioning message. One part of the involved persons stated to have deleted the message

because of superfluity. The other part of the victims clicked the message away in a fright.

The results of the field experiment are that an attack is highly dependent on the OTA configuration mechanism on the MS. As soon as the user is confronted with a reconfiguration message by the handset the attack is quite likely to fail. Yet, as nobody was aware of the OMA Client Provisioning mechanism combining our approach with social engineering might increase the feasibility of a successful attack.

By conducting the survey we also received some vital information about the general importance of mobile phones to the subscribers. We asked the persons involved in the field experiment to take part in the survey and 29 people contributed to the following results. For 76% of the interviewees the mobile phone is very important (see Figure 2), while 62% of them preferably use the handset for private purposes. Accordingly, a derogation of MS functionality would pose a problem to the particular group and yet, only 17% of the interviewees are familiar with IT security. Moreover, only 31% are familiar with their phone's functionality. This means that a majority of the subscribers is dependent on their MS while lacking knowledge about potential risks and means to oppose those threats. 10% of the interviewees use their handsets preferably for business. These 10% also assess their mobile devices of being more important to them than to the average. This can be deduced from the presence of fundamental business data on those respective MSs, which would designate them as a primary target for attackers and espionage. About 59% have heard of malware on mobile devices and only one participant yet discovered malware on his handset. The PIN security feature for locking the device during moments of abstraction is activated by 41%, taking into consideration that older handsets do not offer such a security feature. 21% of the interviewees have already installed additional software on their MS. Installing additional software can be seen as one easy way of infecting a mobile device and yet is countered by mobile operating systems with, for instance, signed executables.

5.3 Capabilities and Limitations during the Test

The timespan between activation of the base station and the first handset to connect was less than a minute. This period would vary depending on different factors, e.g., the signal strength of operator cells.

The coverage of our private cell was limited to the one carriage where the BTS was running in. During the field experiment devices within this radius would connect to our GSM cell.

The OTA messages were handled differently by the various handsets. Generally, Sony Ercisson and Nokia phones require the user to permit the installation of the messages. During the survey it became clear, that confronted with such a message a subscriber would certainly reject the reconfiguration message.

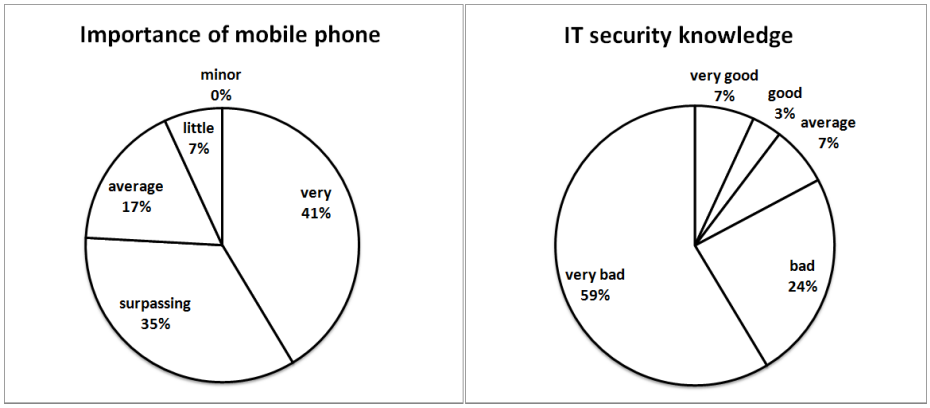

Fig. 2. For 76% of the interviewees their mobile phone is important, while 83% of them have no or little knowledge about IT security.

6 Conclusions

The number of GSM subscriptions is still going to rise until 2014 [2] until successive technologies are going to supersede GSM. During this time SDR equipment as well as the respective software will become publicly available. Because of this and as long as security is not improved, attacks on the network are going to become more presumable.

The approach we presented in this paper provides another way of attacking a MS in a GSM network. Limitations of our practice are imposed by the transmission range and signal strength. In fact, the field experiment showed the lack of security awareness amongst mobile phone users, whereas the question of the applicability of reconfiguring MSs could be negated. As the field experiment pointed out the attack was not successful as rated by the number of reconfigured devices. This also leads to the conclusion that related work, Mune et al. [8] in particular, who can only utilize the "USERPIN" security option for the HMAC calculation, cannot be practically applied. Future work will concentrate on recent technologies in order to develop means to prevent DoS attacks on MSs and provide protection for the subscriber.

Acknowledgements

The authors would like to thank Michael Müller for his kind help with regard to solving the clocking problem. Michael Massoth also provided guidance and input for the research of this paper, as well as Reinhard Riedmüller.

References

1. Global mobile Suppliers Association: Fast Facts. Online `http://www.gsacom.com/news/gsa_fastfacts.php4` (sighted 01/06/2010) (2009)

2. Frost & Sullivan: Global GSM Market Analysis. Online http://www.frostchina.com/download/Global%20GSM%20Market%20Analysis.pdf (sighted 01/06/2010) (2009)
3. Biryukov, A., Shamir, A., Wagner, D.: Real Time Cryptanalysis of A5/1 on a PC. In: In FSE: Fast Software Encryption, Springer-Verlag (2000) 1–18
4. Barkan, E., Biham, E.: Conditional Estimators: An Effective Attack on A5/1. In: Selected Areas in Cryptography. (2005) 1–19
5. Hulton, D., Steve: Intercepting GSM traffic. In: Black Hat DC 2008. (2008)
6. Welte, H.: Using OpenBSC for fuzzing of GSM handsets. In: 26C3. (2009)
7. Nohl, K., Paget, C.: GSM SRSLY. In: 26C3. (2009)
8. Mune, C., Gassira, R., Piccirillo, R.: Hijacking Mobile Data Connections. In: BlackHat Europe. (2009)
9. 3GPP: Security-related network functions. TS 43.020, 3rd Generation Partnership Project (3GPP) (2001)
10. 3GPP: Security Objectives and Principles. TS 33.120, 3rd Generation Partnership Project (3GPP) (1999)
11. Wang, P., González, M.C., Hidalgo, C., Barabási, A.L.: Understanding the Spreading Patterns of Mobile Phone Viruses. research **324**(5930) (May 2009) 1071–1076
12. F-Secure: Virus description: Cabir. Online http://www.f-secure.com/v-descs/cabir.shtml (sighted 12/22/2009) (s.d.)
13. F-Secure: Virus description: Commwarrior. Online http://www.f-secure.com/v-descs/commwarrior.shtml (sighted 12/22/2009) (s.d.)
14. Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G.M., Mehes, A.: Can you infect me now?: malware propagation in mobile phone networks. In: WORM '07: Proceedings of the 2007 ACM workshop on Recurring malcode, New York, NY, USA, ACM (2007) 61–68
15. Kim, H., Smith, J., Shin, K.G.: Detecting energy-greedy anomalies and mobile malware variants. In: MobiSys '08: Proceeding of the 6th international conference on Mobile systems, applications, and services, New York, NY, USA, ACM (2008) 239–252
16. Cheng, J., Wong, S.H., Yang, H., Lu, S.: SmartSiren: virus detection and alert for smartphones. In: MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services, New York, NY, USA, ACM (2007) 258–271
17. F-Secure: Virus description: Flexispy. Online http://www.f-secure.com/v-descs/flexispy_a.shtml (sighted 12/22/2009) (s.d.)
18. 3GPP: Radio Subsystem Link Control. TS 05.08, 3rd Generation Partnership Project (3GPP) (1990)
19. OMA: Provisioning Architecture Overview. Technical report, Open Mobile Alliance (oma) (2009)
20. OMA: Provisioning Content. Technical report, Open Mobile Alliance (oma) (2009)
21. OMA: Provisioning Bootstrap. Technical report, Open Mobile Alliance (oma) (2009)