Attacking GSM Networks as a Script Kiddie Using Commodity Hardware and Software

Christoforos Ntantogian[1], Grigoris Valtas[2], Nikos Kapetanakis[2], Faidon Lalagiannis[2],
Georgios Karopoulos[3], Christos Xenakis[1]

[1,2] Department of Digital Systems, University of Piraeus
[1]{dadoyan, xenakis}@unipi.gr
[2]{gregbaltas, nickkap, flalagiannhs}@ssl-unipi.gr
[3] Department of Informatics and Telecommunications, University of Athens
[3]gkarop@di.uoa.gr

Abstract. With the emergence of widely available hardware and software tools for GSM hacking, the security of cellular networks is threatened even by script kiddies. In this paper we present four different attacks in GSM networks, using commodity hardware as well as open source and freely available software tools. All attacks are performed using a common DVB-T TV tuner, which is used as a sniffer for the GSM radio interface, as well as an Arduino combined with a GSM shield that is used as a software programmable mobile phone. The attacks target both mobile users and the network, ranging from sniffing the signaling traffic to tracking and performing denial of service to the subscribers. Despite the script kiddie style of the attacks, their consequences are critical and threaten the normal operation of the cellular networks.

Keywords: Mobile networks, GSM hacking, Script kiddie, Software defined radio, Arduino.

1 Introduction

Today, Long Term Evolution (LTE) is being deployed in all regions, and subscriptions for this technology are predicted to reach 2.6 billion by 2019 [1]. Despite the proliferation and rapid migration to 4G networks, mainly in developed markets, GSM remains the dominant cellular technology in many countries. In fact GSM-only subscriptions represent the largest share of mobile subscriptions today [5]. As most new LTE devices are backwards compatible to GSM, the latter will not be replaced, but rather complement 3G and 4G connectivity, operating as a fallback mechanism.

The security of GSM networks has been extensively analyzed in the literature. Many works have pinpointed the fact that the GSM security is based on some arbitrary trust assumptions that malicious actors can violate and attack both mobile users and the network [2]. However, a common limitation of the previous works lies to the fact that the discovered vulnerabilities and attacks were presented and analyzed in a theoretical manner, thus their feasibility is questionable. This can be attributed to the closed nature of the GSM industry players including the phone manufacturers, baseband vendors and infrastructure equipment suppliers, which do not release specifications of their products. Additionally, the hardware and software to perform practical experiments to GSM networks were very expensive or they were available only to mobile operators to assess their network. This situation was beneficiary for the mobile operators, since they were not pressured to enhance their provided level of security despite the discovered vulnerabilities.

In the last years, radio communications systems based on Software Defined Radio (SDR) as well as open-source micro controller boards have been emerged, allowing anyone to perform experiments in GSM networks in a cost-effective and flexible manner. These low-cost and widely available hardware/software systems can become a powerful tool at the hands of malicious actors, introducing an asymmetric threat to mobile operators, since anyone, including script kiddies, can use them to disrupt the normal operation of a mobile network. Driven by this observation, this paper presents four different attacks in GSM networks using commodity hardware as well as open source and freely available software tools. The main equipment of our test bed is a common DVB-T TV tuner [15], which is used as a sniffer to the GSM radio interface, as well as an Arduino [6] combined with a GSM shield that is used as a software programmable mobile phone. The above testbed allowed us to perform a variety of attacks targeting the Mobile Station (MS) and the mobile operator. The performed attacks are:

1. Retrieve sensitive data (identities and keys) from the SIM card with the aim of identifying potential issues regarding the security configuration of the mobile operators in Greece.
2. Sniff, capture and analyze paging requests and derive useful observations regarding traffic load, security policies and the number of roaming subscribers for the Greek mobile operators.
3. Perform a stealthy Denial of Service (DoS) attack to a targeted MS. The result of this attack is that the victim MS cannot receive legitimate phone calls, without noticing any suspicious activity.
4. Track MS with a granularity of a cell coverage area.

The simplicity yet effectiveness of our attacks depicts that no security mechanisms are implemented to prevent, block or even monitor malicious activities in cellular mobile networks. We believe that security mechanisms, including firewalls and intrusion detection systems, should be specifically designed and incorporated in mobile networks to increase the provided level of security.

The rest of the paper is organized as follows. Section 2 provides the background presenting the GSM network architecture, the GSM channels as well as the paging procedure, while section 3 includes the related work. Section 4 elaborates on the performed attacks and evaluates their results and impact. Finally, section 5 contains the conclusions.

2 Background

2.1 Architecture

The technology of GSM is based on Time Division Multiple Access (TDMA) transmission methods, while its radio interface operates in the 900MHz and 1.8GHz bands in Europe and in 850MHz and 1.9GHz in the US. An outline of the GSM architecture is depicted in figure 1(a), focusing only on the network elements relevant to this paper [3]. The Mobile Station (MS) comprises the mobile phone and the subscriber identity module (SIM) card and interacts with the Base Transceiver Station (BTS) over the radio interface. Note that in this paper we will use the words MS and subscriber interchangeably. BTS is responsible for the radio coverage of a given geographical area, while the Base Station Controller (BSC) maintains radio connections towards MSs and terrestrial connections towards the fixed part of the network (core network). Both BTS and BSC constitute the Base Station Subsystem (BSS) that controls the GSM radio path. The GSM service area is divided into Location Areas (LAs), where each LA includes one or more radio cells. Every LA and radio cell has a unique identifier named Location Area Code (LAC) and Cell-ID, respectively.

The GSM Core Network mainly includes the Home Location Register / Authentication Centre (HLR/AuC), the Visitor Location Register (VLR) and the Mobile Service Switching Centre (MSC). HLR/AuC is a database used for the management of permanent data of mobile users and also maintains security information related to subscribers' identity. VLR is a database of the service area visited by an MS and contains all the related information required for the MS service handling. MSC is a network element responsible for circuit-switched services and provides connectivity to the Public Switched Telephone Network (PSTN).

2.2 GSM physical and logical channels

GSM uses a variety of channels to carry information over the air interface [4], which are broadly divided in two categories: i) physical and ii) logical. A physical channel is determined by one or more carrier frequencies, including the hopping sequence and the time slot, while a logical channel is characterized by the information carried within the physical channel. Logical channels are used to carry both data and signaling load and, therefore, can be separated into: i) traffic and ii) signaling channels. Traffic channels transmit voice and data packets, while signaling channels carry control information allowing the system to operate correctly. The most important GSM signaling channels that are related to this work are:

- **Broadcast Control Channel (BCCH):** A broadcast downlink channel that repeats system information messages that contain the identity, configuration and available features of the BTS (e.g., Cell-ID, Location Area Identifier that includes the LAC, list of neighboring cells, etc.).
- **Paging Channel (PCH):** A downlink channel used by the BTS to locate and identify an MS.

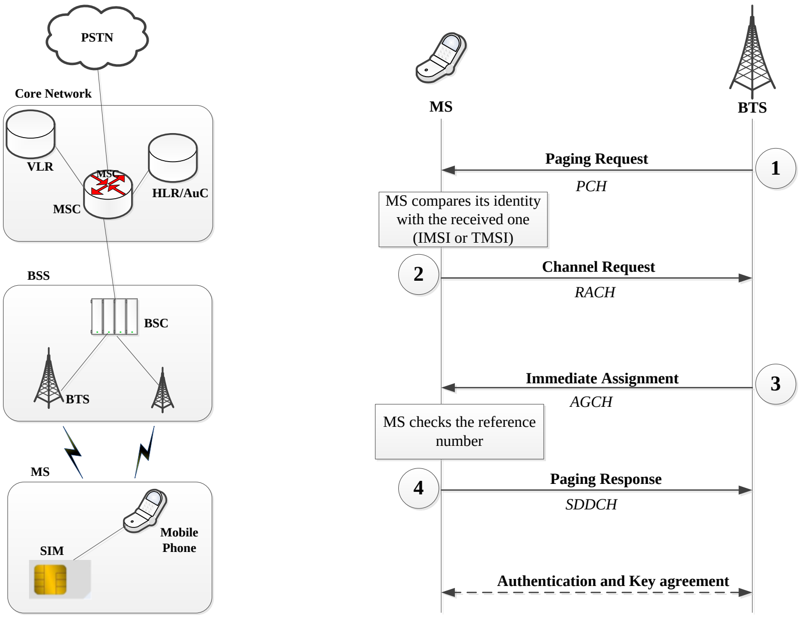
- **Random Access Channel (RACH):** A shared uplink channel used by MSs to request dedicated channels from the BTS.
- **Access Grant Control Channel (AGCH):** A downlink channel used by the BTS to assign dedicated control channel to MSs in response to the related channel requests received on the RACH.
- **Standalone Dedicated Control Channel (SDCCH):** An uplink and downlink channel employed for call setup, SMS delivery and signaling exchange between BTS and MS.

2.3 Paging

The delivery of GSM services (voice call, SMS, etc.) to a mobile phone, requires from the MSC to discover the exact location of the respective MS, by performing the procedure of paging. First, the core network interrogates the HLR of the target MS to identify which MSC/VLR serves it. Next, the underlying MSC obtains from the employed VLR the LA of the destination MS, and, then it forwards a paging message to all the BSCs of the considered LA. This message includes a list of Cell-IDs and base stations identifiers that constitute the specific LA, where the MS resides [4], as well as the identity of the MS either in the form of International Mobile Subscriber Identity (IMSI) or Temporary Mobile Subscriber Identity (TMSI). TMSI, as its name implies, is a temporary identity (i.e., pseudonym) that provides anonymity.

At this point, the BSC sends a paging command message to all BTSs of the considered LA, which in turn they forward a paging request message to the downlink PCH (see step 1-figure 1(b)). Each MS that receives this request compares its own identity with the one that was included in the message. If these match for a specific MS, then the latter sends a channel request that includes a random reference number using the uplink RACH (step 2 of figure 1(b)). Upon receiving this message, the corresponding BTS allocates radio resources and a dedicated channel, acknowledges the request, and sends the details of the allocated channel to the MS using an immediate assignment message on the AGCH downlink (step 3-figure 1(b)). This message also contains the random reference that was included in the respective channel request message of the previous step. Upon receiving this assignment, the MS compares the contained random reference (i.e., with the one sent in the channel request) and if the comparison is true, the MS tunes to the dedicated signaling channel that is assigned by the respective assignment message. At this point, the MS establishes a signaling link over SDCCH and sends a paging response message (step 4-figure 1(b)). After this, an authentication and key agreement procedure takes place, but the details of this procedure are omitted, since it is irrelevant to this work.

The GSM specifications [4] specify three types of paging requests (i.e., type 1, 2, and 3) which are related to the number of subscribers that can be addressed with a single procedure. More specifically, type 1 can page one or two subscribers, type 2 two or three subscribers, and type 3 four subscribers at once. Finally, it is important to notice that all of the above messages are transmitted in clear text, which means that an adversary can trivially sniff and eavesdrop on them for malicious purposes, as we analyze below.



(a) (b)

Fig. 1. Paging procedure

3 Related Work

In this section, we present the related work focusing on papers that elaborate on discovered attacks in GSM networks from a practical viewpoint. [12] showed that GSM networks leak enough information that an adversary can exploit to track a mobile user. In particular, the authors proposed several methods to check whether a user is present within a small area, or absent from a large area, simply by listening to the broadcast GSM channels. The necessary information was available simply by dialing the number of the target subscriber and aborting the call, before the cell phone rings to avoid detection. To demonstrate the practicality of this, the authors performed location tracking experiments to specific mobile operators. They were able to track down a cellular device within a 10-block area in Minneapolis, using a T-Mobile G1 smartphone and a modified OsmocomBB firmware [7], which is a free open-source GSM baseband software implementation. However, it is important to mention that osmocomBB supports old phones (that don't have an application CPU, but only a modem) and also requires a computer.

Recently, a novel DoS attack was presented in [11]. This attack exploits a race condition where an adversary can attempt to answer to a paging request faster than the intended subscriber. If he/she succeeds to do this, then the BTS ignores the paging response of the intended victim subscriber, which receives a channel release message from the network. In this way, an effective DoS is achieved to the victim subscriber, since he/she cannot answer an incoming call. To demonstrate the feasibility of this attack, the authors modified the osmocomBB firmware [7].

In [13], the authors, quantitatively, characterize a distributed DoS attack to an HLR/AuC, coordinated by a botnet of infected mobile devices. This work provides numerical estimations for various parameters to successfully perform the attack, such as the required number of infected mobile phones, the rate of flooding messages, the service requests and network operations that incur the greatest burden to the HLR/AuC, etc. It identifies that the insert/delete call forwarding requests, which allow a user to redirect incoming phone calls to other devices, are the most suitable, from an attacker perspective, to flood the HLR/AuC. It reveals that the registration procedure is not so effective to flood the HLR/AuC, due to the caching mechanism of authentication vectors in the serving MSC. That is, during an MS registration, the serving MSC may provide to the MS an authentication vector already stored from a previous authentication data request, meaning that the MSC does not have to perform a request to the home HLR/AuC. Finally, the authors have estimated the throughput reduction of an HLR/AuC under DoS attack, using insert call forwarding requests.

The work in [14] presented some design and implementation weaknesses in the TMSI reallocation procedure that allow the identification and/or tracking of mobile subscribers. Using experimental and formal analysis, the authors concluded that the TMSI reallocation procedure is vulnerable to a linkability attack, when the same keys are used to encrypt it. Moreover, they have proposed countermeasures to address the identified security issues.

Finally, in our previous work [8], we have performed practical experiments in which we identified and proved some zero-day vulnerabilities of the 3G network that can be exploited by malicious actors to mount various attacks. Specifically, based on the observations of the conducted experiments, we have revealed an Advanced Persistent Threat (APT) in 3G networks that aims to flood an HLR/AuC of a mobile operator. In this attack, a group of adversaries first collect IMSIs that belong to the same HLR/AuC. Next, residing in roaming networks, they perform successive registrations using the collected IMSIs that trigger the execution of authentication requests to the specific HLR/AuC. The continuous execution of authentication requests, in a very short period of time, incurs the depletion of the computational resources of the HLR/AuC, eventually leading to system saturation. To this end, a mobile application was implemented that performs continuous network registrations using AT commands. The application utilizes the dial command to initiate phone calls using a different IMSI for each call request. This was achieved by employing a device named simtrace [10], which acts as an active man-in-the-middle between the modem and SIM/USIM card changing the IMSI identity, when it is requested by the modem.

4 Practical Attacks in GSM networks

4.1 Testbed

Our performed attacks were based on a testbed that is exclusively composed of commodity and off-the-shelf hardware and software tools, which are affordable and widely available. The total cost of the equipment was around 100 Euro and the most important components of the testbed are:

- **RTL-SDR / DVB-T TV Tuner 15(€10):** This is a cheap wideband SDR scanner based on a DVB-T TV-Tuner USB dongle. RTL-SDR is broadband (60MHz to 1700MHz) and it is capable of sniffing GSM signals as well as Receiving/Decoding GPS signals. RTL-SDR requires the GNU Radio, which is a software development toolkit that provides signal processing blocks to implement software radios and signal processing systems. It is important to notice that RTL-SDR is able to capture only the GSM downlink traffic (BTS to MS), but not the uplink traffic (MS to BTS).
- **Arduino (€20) and GSM Shield 6(€70):** Arduino is an open-source electronics prototyping platform, based on a programmable microcontroller. The functionality of an Arduino board can be easily extended using interchangeable add-on modules, known as shields. One such shield is the GSM shield, which allows an Arduino board to connect to the internet, make/receive voice calls and send/receive SMS messages, using the GSM modem.
- **Open-source software tools:** Our testbed includes various open source and free software tools including: i) Airprobe for protocol parsing and decoding; ii) Wireshark for packet analysis, and, iii) Kalibrate which scans for GSM BTSs in a given frequency band. It is important to mention that all the above tools are available in the Linux operating system.

4.2 Retrieving security parameters of mobile networks

In this attack, we retrieve sensitive data (identities and keys) from the SIM card with the aim of identifying potential issues regarding the security configuration of the mobile operators. To achieve this, we use the Arduino combined with the GSM shield to simulate a MS. Overall, we have conducted three experiments in total. In the first one, we estimated how often the Kc key is renewed. In the second, we measure how frequently the TMSI identity of a static user (i.e., a MS located in the same LA) is reallocated. And, finally, in the third experiment, we performed a war-driving, in order to estimate how frequently the TMSI of a mobile user (i.e., a MS that changes its LA) is reallocated. All experiments took place at the city of Athens and the three Greek mobile operators: Vodafone, Wind and Cosmote. To carry out the experiments, we have developed custom scripts for Arduino in C++ programming language, which automate the following procedures: i) initiate and terminate voice calls repeatedly, ii) restart periodically the phone, and, iii) retrieve important parameters from the SIM card including Kc, TMSI, IMSI, LAC and Cell-ID. The custom scripts that we have developed perform the above three procedures by means of AT commands [9], which provide various operations to control a GSM modem. The specific AT commands used in our custom scripts are analyzed in [21].

Table 1. Rate of Kc keys renewals for each mobile operator

Operator	Kc renewal rate
Vodafone	16 voice calls
Wind	6 voice calls
Cosmote	10 voice calls (on average)

In the first experiment (see table 1), we observed that Vodafone updates the Kc key every 16 voice calls, while Wind every 6 voice calls. Cosmote performs Kc updates, arbitrarily, and we didn't identified any specific pattern. For this reason, we computed an average value that is approximately every 10 voice calls. It is evident that a mobile network should update the Kc key as frequent as possible; otherwise, its subscribers are exposed to several threats including interception of phone calls and impersonation for longer time periods and thus, with higher impacts [16]. Unfortunately, the obtained numerical results show that mobile operators in Greece do not refresh the encryption key for every voice call. In the second experiment (i.e., TMSI reallocations for static users), we observed that both Vodafone and Wind do not change the TMSIs of their static users (see table 2). On the other hand, Cosmote reallocated the TMSI with a new incremented value (without any specific pattern). It is alarming that both Vodafone and Wind do not perform periodic TMSI reallocation for static users. This means that as long as the mobile subscribers stay in the same location/routing area (i.e., office building, home, etc.) and use their phones, they will have the same temporary identities. This configuration is very weak, because the same TMSI is used for every call/SMS request, allowing an adversary to easily identify and track a user.

Table 2. TMSI values assigned to static users

Cosmote TMSI	Vodafone TMSI	Wind TMSI
23B9C7A8	701590D9	A8B32A7A
23BA25D0	701590D9	A8B32A7A
23BA82D0	701590D9	A8B32A7A
23BAE940	701590D9	A8B32A7A
23BB46B0	701590D9	A8B32A7A
23BBADE8	701590D9	A8B32A7A
23BC0A98	701590D9	A8B32A7A
23BC7448	701590D9	A8B32A7A
23BCD8B0	701590D9	A8B32A7A
23BD4298	701590D9	A8B32A7A
23BDB418	701590D9	A8B32A7A
23BE15D8	701590D9	A8B32A7A
23BE74B0	701590D9	A8B32A7A
23BED9C8	701590D9	A8B32A7A

Finally, in the third experiment (i.e., TMSI reallocations for mobile users), we observed as shown in table 3 that each time a user changes its LA, then Vodafone and Cosmote reallocate the TMSIs with a new value. On the other hand, Wind does not update the TMSI, exposing its subscribers. Thus, if an adversary establishes passive devices that sniff the cellular signaling (e.g., like the RTL-SDR / TV-tuner) at the borders of LA, he/she may easily track the movements of almost all the subscribers of Wind.

Table 3. TMSI values assigned to mobile users that change LA

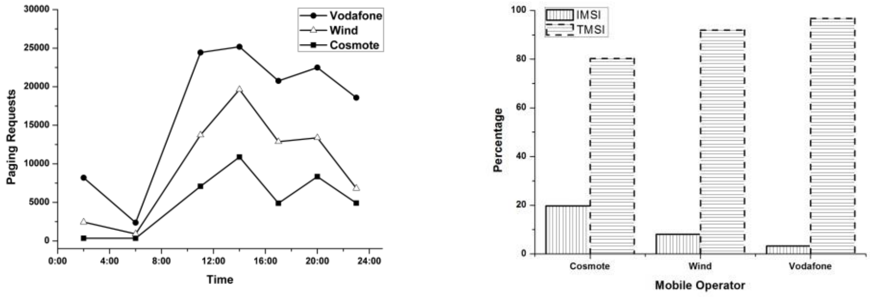
Vodafone		**Cosmote**		**Wind**	
LAC	**TMSI**	**LAC**	**TMSI**	**LAC**	**TMSI**
004A	4921B2CF	0025	12A83908	3908	58B315A2
0016	18242A12	0020	14A9E4B8	29CC	58B315A2
0025	4823F122	0021	15AF0E08	2744	58B315A2

4.3 Capturing paging requests

In this attack we use the RTL-SDR /TV tuner and the Kalibrate tool to sniff, capture and analyze paging requests in a specific LA. In particular, for each one of the Greek mobile operators, we captured paging requests messages from the downlink traffic (i.e., from BTS to MS) and we analyzed them using Wireshark. The latter can correctly decode GSM control packets, allowing us to extract TMSI and IMSI identities from the paging requests.

Figure 2(a) plots the number of paging requests that include either an IMSI or a TMSI during one day in a specific LA. Paging activity varies throughout the time of the day (which is the same for all operators), reflecting human activity. We can point out that during midday the traffic greatly increases reaching its highest point in 14:00 for all mobile operators. Moreover, in figure 2(b) we show the percentage of paging requests that include IMSIs or TMSIs versus the total number of paging requests in a specific LA. Ideally, an IMSI should never be transmitted, because a possible attacker can easily read it, as it is conveyed in plaintext. We notice that Cosmote uses IMSIs in a whopping 19% of paging requests, while Wind and Vodafone in 8.04% in 3.02% respectively. On the other hand, Cosmote uses TMSIs 81% of paging requests, while Wind and Vodafone in 91.96% in 96.98% respectively. It is clear that Cosmote follows a poor policy regarding the privacy of MS, since on average one IMSI is exposed in every five paging requests. Due to the loss of mobile subscribers' anonymity, an attacker may achieve to identify and track them. Mobile identities are currently used by market research companies, such as those referred in [17] and [18], in order to track the movements of visitors within a specific place (e.g., shopping malls, exhibition centers, etc.). These companies identify and track subscribers to collect information on the shopping habits without their consent, while usually they share the tracking information with third parties to maximize profit [19].

An advantageous characteristic of GSM is its international roaming capability, allowing users to seamlessly access the same services when traveling abroad. To this end, we have analyzed the obtained IMSIs to find roaming subscribers as well their foreign mobile operators. Based on this analysis, we can get informed about the different roaming agreements that the Greek Mobile operators have. This information was obtained using the mobile country code (MCC), which is the first three digits of the IMSI followed by the mobile network code (MNC), which is 2 digits or 3 digits. As shown in table 4, most roaming subscribers of Cosmote are from Germany with the Telecom/T-Mobile mobile operator. For Vodafone, most roaming subscribers are from Turkey with the Vodafone-Telsim mobile operator. Finally, Wind has roaming subscribers mainly from Philippines with Smart mobile operator (see table 5). It is interesting to mention that there are foreign operators that have roaming agreements with two different Greek mobile operators at the same time. For example, we have discovered IMSIs of the Vodafone-Telsim operator from both Vodafone and Cosmote.



(a) (b)

Fig. 2. Paging requests vs. time in a specific LA

Table 4. Cosmote and Vodafone roaming subscribers

Cosmote			**Vodafone**		
Sub-scribers	**Country**	**Operator**	**Sub-scribers**	**Country**	**Operator**
174	Germany	Telecom/T-Mobile	17	Turkey	Vodafone-Telsim
22	Turkey	AVEA/Aria	5	Turkey	AVEA/Aria
20	Finland	TeliaSonera	5	UK	O2 Ltd.
14	Turkey	Vodafone-Telsim	4	Denmark	Telia
10	Austria	T-Mobile/Telering	3	South Africa	Vodacom
9	Czech Republic	T-Mobile/ RadioMobile	3	UK	Vodafone
7	Egypt	Vodafone	2	USA	T-Mobile

Table 5. Wind roaming subscribers

Wind		
Subscribers	**Country**	**Operator**
9	Philippines	Smart
2	Brazil	Vivo S.A./Telemig
2	Russia	VimpelCom
2	Netherlands	Vodafone Libertel
1	Venezuela	Movistar/TelCel
1	USA	AT&T Wireless Inc.
1	Albania	Vodafone

4.4 A stealthy denial of service attack to MS

In this attack, we use the Arduino microcontroller combined with the GSM shield to perform a DoS to a targeted MS where the latter can no longer receive any legitimate phone call. The attack vector is simple yet effective. That is, we continuously call the mobile phone of the targeted MS. As a result, the mobile phone of the targeted MS is always occupied (due to the multiple calls) and legitimate calls to the mobile phone cannot be performed. The key characteristic of this attack is that it is performed in a stealthy manner in the sense that the victim MS cannot identify that he/she is under attack, because the phone does not actually ring.

To better understand how we perform the attack and achieve to keep occupied a phone without ringing, consider the time sequence of figure 3, which shows three events that occur successively: 1) phone dialing, 2) paging request and 3) phone ringing. More specifically, at time t0 suppose that we dial the phone number that we want to perform a call (see figure 3). At time t1, assume that the related paging request is transmitted from the BTS to the phone. Notice that from time t1 and afterwards, the phone is occupied meaning that all other paging requests initiated from other calls to the phone are rejected. Moreover, as shown in figure 3, the phone ringing occurs at time t2. We have experimentally estimated the time differences between the three events shown in figure 3. That is, we have estimated that the elapsed time between the dialing of the phone number and the paging request is on average 3 seconds (t1-t0=3 sec.), while the elapsed time between the paging request and the actual phone ringing is on average 2.5 seconds (t2-t1=2.5 sec.). Thus, the total time from the moment that a phone number is dialed until the phone actually rings is on average 5.5 seconds (t2-t0=5.5 sec.).

We have exploited the above observations to perform a stealthy DoS attack. That is, we have developed a custom script for Arduino based on AT commands, which repeatedly calls a mobile phone, and after L seconds terminates the call. Evidently, the value of L should be less than 5.5 seconds (i.e., $L < 5.5$), in order to avoid phone ringing (see figure 3). In this way, we can achieve to occupy a targeted phone by continuously dialing and terminating calls, without however actually ringing the phone.

As a result, the victim (i.e., the owner of the phone) cannot become aware of the attack, since no call activity occurs in his/her phone. It is important to mention that the attacker's repetitive calls are not shown in the targeted phone as missed calls.

The focal point of this attack is that an adversary equipped with commodity hardware, like Arduino, can perform a DoS to a MS, simply, by performing continuous phone calls. The simplicity of this attack depicts the alarming fact that no security mechanisms are implemented to block or mitigate this kind of DoS attacks in cellular networks.

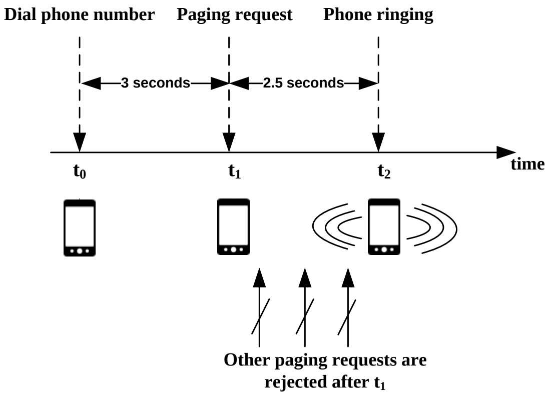


Fig. 3. Time sequence of a call setup

4.5 Users Location Area Leakage

Lastly, we demonstrate an attack for user tracking with a granularity of a radio cell coverage area using the Arduino and the GSM shield as well as the RTL-SDR/TV tuner. The only prerequisite for this attack is that the adversary knows the mobile phone number of the targeted MS that wants to geographically track. It is important to mention that the adversary is capable to sniff only the downlink channel of GSM, due to the limitations of the RTL-SDR/TV tuner (see section 4.1). The attack consists of two sequential phases. In the first phase, the adversary locates the LA (i.e., a wide area network segment served by a group of BTSs), where the MS resides. Then, in the second phase the adversary tries to locate the respective MS in the geographic area of a radio cell. More specifically, the attack is performed as follows.

Phase A: Discover the current LA of the MS

Assume that the adversary wants to discover whether the targeted MS resides in a specific LA that we name it as LA_X. This phase includes 3 steps.

1. The adversary resides in the coverage area of a randomly chosen BTS of the LA_X. Using Arduino and the GSM shield, the adversary performs *k* consecutive phone calls to the targeted MS (we elaborate below on the exact value of *k*). To avoid raising suspicions, the adversary may use the same technique as in the previous attack (i.e., stealthy DoS attack to MS) exploiting the delay between the paging and

phone ringing. That is, the MS receives paging requests, but the calls are terminated before the phone rings.

2. At the same time, the adversary captures the downlink traffic of the BTS that resides using the RTL-SDL / TV tuner.
3. After steps 1 and 2 of phase A, the adversary analyzes the captured packets of the downlink traffic using Wireshark. If the adversary discovers *k* paging requests that include the same IMSI or TMSI, he/she may infer that both (i.e., the targeted MS and the adversary) are located in the same LA (i.e., $\mathrm{LA_X}$). This can be justified as follows. First recall from section 2.3, that paging requests are broadcast messages conveyed in plaintext and used as an identifier the IMSI or TMSI of the MS. Recall also that during an incoming call to a MS, the mobile network instructs all BTSs of the LA that MS resides in, to broadcast paging requests. Therefore, if the targeted MS is indeed in the same LA with the adversary (i.e., $\mathrm{LA_X}$), then all the BTSs of $\mathrm{LA_X}$ (including the BTS that the adversary captured the downlink traffic) will broadcast *k* paging requests with the IMSI or TMSI of the targeted MS. This means that if the adversary discovers *k* paging requests, which were performed during the *k* calls in step 1, he/she can deduce that a MS resides in $\mathrm{LA_X}$.

Phase B: Discover the current radio cell that MS is located

The adversary now knows that MS resides in $\mathrm{LA_X}$. Based on this information, in this phase the adversary now wants to identify in which specific cell of $\mathrm{LA_X}$ the targeted MS resides.

1. The adversary resides in the coverage area of a randomly chosen BTS of the $\mathrm{LA_X}$. The adversary repeats steps 1 and 2 in a randomly selected radio cell of the identified LA. Similarly to step 1 of phase A, the adversary performs *z* consecutive calls to the targeted MS.
2. Similar to step 2 of phase A, the adversary captures the downlink traffic using the RTL-SDL / TV tuner.
3. The adversary now investigates the captured packets. If the adversary discovers *z* immediate assignments messages to the targeted MS (we elaborate below on the exact value of *z*), then he/she can infer that both (i.e., the adversary and the targeted MS) are located within the same radio cell. This can be justified as follows: Recall that immediate assignment messages are transmitted from BTS to MS, only when the latter is included in the coverage area of the former, and includes the description of the dedicated channel to be used for authentication and cipher negotiation. Therefore, the discovery of *z* immediate assignment messages to the MS indicates that the MS and the adversary are located in the same cell.
4. If the adversary does not find *z* immediate assignments, then he/she can repeat step 1 and 2 using another BTS of the $\mathrm{LA_X}$.

To prove the feasibility of this attack and estimate the numerical values of the parameters *k* and *z*, we have performed experiments in a mobile operator. The experiments were conducted in low traffic load hours (i.e., nightly hours) in order not to overload the channel and disrupt the normal operation of the network. In order to distinguish our paging requests with legitimate ones, we have experimentally found that the minimum number of consecutive calls for phase A should be 80 (i.e., *k*=80). Regarding phase B, we have experimentally found that the minimum number of consecutive calls should be 100 (i.e., *z*=100).

5 Conclusions

This paper elaborated on four different attacks in GSM networks using commodity hardware and open source tools. The described attacks can be performed by script kiddies and include:

1. Retrieve sensitive data (identities and keys) from the SIM card with the aim of identifying potential issues regarding the security configuration of the mobile operators in Greece.
2. Sniff, capture and analyze paging requests and derive useful observations regarding traffic load, security policies and the number of roaming subscribers for the Greek mobile operators.
3. Perform a stealthy Denial of Service (DoS) attack to a targeted MS. The result of this attack is that the victim MS cannot receive legitimate phone calls, without noticing any suspicious activity.
4. Track MS with a granularity of a cell coverage area.

We have experimentally proved the feasibility of each one of these attacks using a common DVB-T TV tuner as well as an Arduino microcontroller combined with its GSM shield. The simplicity yet effectiveness of our attacks depicts that no security mechanisms are implemented to prevent, block or even monitor malicious activities in cellular mobile networks. We believe that security mechanisms, such as firewalls and intrusion detection systems described in [20], should be specifically designed and incorporated in cellular mobile networks to increase the provided level of security.

Acknowledgements. This research has been funded by the European Commission as part of the SMART-NRG project (FP7-PEOPLE-2013-IAPP Grant number 612294).

6 References

1. Ericsson mobility report June 2014, http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf
2. Christos Xenakis, "Malicious actions against the GPRS technology," Computer Virology, Springer, Vol. 2, No. 2, Nov. 2006, pp. 121-133
3. 3GPP TS 03.6 (V7.9.0), ”GPRS Service Description, Stage 2”, Sept. 2002.
4. 3GPP TS 04.01 V8.0.0 – Mobile Station - Base Station System (MS - BSS) interface; General aspects and principles. http://www.3gpp.org/ftp/Specs/html-info/0401.htm, March 2000.
5. The mobile economy, GSMA, 2014
6. Arduino, The Open Source Electronics Platform, http://arduino.cc

7. The osmocombb project – open source gsm baseband software implementation. http://bb.osmocom.org/
8. Christos Xenakis, Christoforos Ntantogian, “An advanced persistent threat in 3G networks: Attacking the home network from roaming networks,” Computers & Security, Elsevier Science, Vol. 40, Issue 1, pp:84-94, February 2014.
9. 3GPP TS 27.007 V11.5.0 (2012-12), 3rd Generation Partnership Project, Technical Specification Group Core Network and Terminals, AT command set for User Equipment (UE) (Release 11).
10. Simtrace, http://bb.osmocom.org/trac/wiki/SIMtrace
11. Nico Golde, Kévin Redon, Jean-Pierre Seifert, “Let me answer that for you: exploiting broadcast information in cellular networks”, 22nd USENIX conference on Security, Washington DC, USA, Aug. 2013.
12. Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim, “Location Leaks on the GSM Air Interface”, Network & Distributed System Security Symposium (NDSS) 2012, San Diego, California, USA.
13. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick Drew McDaniel, Thomas F. La Porta, “On cellular botnets: measuring the impact of malicious devices on a cellular network core”, ACM Conference on Computer and Communications Security, 223-234, 2009.
14. Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, Mark Ryan, “Privacy through Pseudonymity in Mobile Telephony Systems”, 21st Network and Distributed System Security Symposium (NDSS) 2014, California, USA.
15. http://www.rtl-sdr.com/
16. Karsten Nohl, “Attacking phone privacy”, BlackHat USA, Las Vegas, Aug 2010
17. http://www.pathintelligence.com
18. http://www.smart-flows.com
19. http://www.theregister.co.uk/2012/01/11/phone_tracking_expert/
20. Patrick P. C. Lee, Tian Bu, Thomas Y. C. Woo, “On the Detection of Signaling DoS Attacks on 3G/WiMax Wireless Networks”, Elsevier Science, Computer Networks Volume 53 Issue 15, October 2009
21. Christos Xenakis, Christoforos Ntantogian, “Attacking the Baseband Modem of Mobile Phones to Breach the Users’ Privacy and Network Security”, 7th International Conference on Cyber Conflict (CyCon 2015), Tallinn, Estonia, May 2015.