# (U)SimMonitor: A Mobile Application for Security Evaluation of Cellular Networks

Christos Xenakis, Christoforos Ntantogian, Orestis Panos

Department of Digital Systems, University of Piraeus
Piraeus, Greece
{xenakis, dadoyan, panos}@unipi.gr

**Abstract**—The lack of precise directives in 3GPP specifications allows mobile operators to configure and deploy security mechanisms at their sole discretion. This may lead to the adoption of bad security practices and insecure configurations. Based on this observation, this paper presents the design and implementation of a novel mobile application named (U)SimMonitor that captures and analyses the security policy that a cellular operator enforces i.e., the invocation and employment of the specified security measures to protect its users. (U)SimMonitor achieve this by executing AT commands to extract network related parameters including encryption keys, identities, and location of users. Using (U)SimMonitor as our basic analysis tool, we have conducted a set of experiments for three mobile operators in Greece in a time period of 9 months. The obtained results allow us to quantify, compare and evaluate their applied security as well as pinpoint a set of generic critical observations. Numerical results and security measurements show that mobile networks have poor security configurations and practices, exposing subscribers to several attacks.

**Keywords**— Cellular networks, Mobile application, Android, AT commands, Security measurements

## 1 Introduction

According to the Group Speciale Mobile Association (or GSM Association) [1], in 2014, there were 3.5 billion cellular unique subscribers in the world. Despite the arrival of fourth generation (4G) technology, the dominant technologies for both voice and data communications were the second generation (2G) and third generation (3G) networks [1]. Over 90% of the world cellular subscribers use the global system for mobile communications (GSM), the general packet radio service (GPRS) and the universal mobile telecommunications system (UMTS) standards. In parallel to the evolution of cellular networks, the mobile phones are also evolving to smartphones with processing capabilities and storage resources that are often equivalent to contemporary personal computers (PCs). The potential of smartphones is leveraged by mobile operating systems (OSs), such as iOS and Android OS that allow end-users to access traditional desktop applications using these portable devices.

Security has played an important role in the design and deployment of cellular networks. The working group 3 of the system and service aspects of the third generation partnership project (3GPP SA-WG3) has provided the security mechanisms as well as, in some cases, their implementation details that are applied in cellular networks [2]. These mechanisms mainly include:

i. The authentication and key agreement (AKA). During AKA, the mobile user is authenticated to the network (i.e., and the opposite if the user is connected to a 3G network) as well as a new encryption (and integrity in case of 3G) key is generated.
ii. The identification of mobile subscribers in the radio access network by means of temporary identities to protect their privacy.
iii. The avoidance of disclosure of subscribers' permanent identities over the radio interface.

iv. The employment of strong encryption (and integrity protection in case of 3G) algorithms over the radio access network.

However, we have pinpointed that these specifications do not explicitly define:

a. The frequency that the connected mobile users will be re-authenticated, as well as the employed encryption or integrity keys will be refreshed.
b. What is the maximum allowed time that a temporary identity should be used.
c. How often the serving network is allowed to request from a mobile station (MS) the subscriber's permanent identity.

The decision on the above depends entirely on the configuration and security policy employed by an operator. It is evident that leaving critical security decisions to mobile operators is a serious flaw that can expose subscribers to several attacks. Moreover, we have identified that the specifications recommend, but do not mandate, the use of strong encryption algorithms, fact that permits operators to decide which encryption algorithms will be used, eventually. Another flaw of 3GPP specifications is that it allows the simultaneous use of 2G and 3G technology, without any restriction and security guidelines, meaning that operators can freely use legacy and broken 2G security mechanisms.

This paper presents the design and implementation of a novel mobile application, named (U)SimMonitor that can capture and analyse the security policy that a cellular operator enforces i.e., the invocation and employment of the specified security measures to protect its users. This is achieved by obtaining, recording and processing real security measurements from the subscribers that are connected to and served by the target cellular network. Such measurements allow for the quantification and comparison of the applied security measures. The key functionality of (U)SimMonitor is to extract security credentials and information of the cellular technology from the SIM and UMTS SIM (USIM) cards including permanent and temporary identities, encryption keys and location of users. This is achieved by executing *AT commands* [16] to the baseband modem of mobile phones. We elaborate on the software architecture of (U)SimMonitor and provide implementation details. Next, we put the discussion into a practical context, by employing the developed (U)SimMonitor to capture and evaluate the security policy and configurations of the three major mobile operators in Greece: Vodafone, Wind and Cosmote. To achieve this, we have collected security data in a simple yet effective manner using typical mobile phones equipped with (U)SimMonitor. More specifically, first we analyze a set of identified critical decisions that the mobile operators should make, describing at the same time how these decisions may affect the security of mobile subscribers. Next, we present a set of experiments and scenarios that have been performed in a time period of 9 months. Finally, we deduce critical observations regarding the security policies and configurations of the three major mobile operators in Greece. Numerical results show that the lack of precise directives in 3GPP specifications leads to poor security configurations, exposing subscribers of mobile networks to several attacks.

Overall the contributions of this paper are threefold:

a) Design and implementation of the (U)SimMonitor
b) Leverage the characteristics of (U)SimMonitor to obtain and analyze security measurements for the three major mobile operators in Greece, with the aim of deriving critical observations regarding their security policies and the related security configurations.
c) Pinpoint and analyze a set of critical security decisions and configurations that a mobile operator should make in order to enforce its security policy, describing at the same time how these may affect the security of mobile subscribers.

The rest of the paper is organized as follows. Section 2 provides the background describing briefly the key components of today's mobile networks as well as discussing the related work. Section 3 presents the design and implementation of (U)SimMonitor. Section 4 first elaborates on the security policy and configurations that mobile operators should employ, and in the sequel, describes the experiments and evaluates the numerical results. Finally, section 5 concludes the article.

# 2 Background

## 2.1 Cellular Technology

Cellular networks are composed of various interworking technologies including 2G and 3G networks [3]. The 2G networks comprise of GSM, GPRS and enhanced data rates for GSM evolution (EDGE) technologies, while 3G of UMTS and high-speed downlink packet access (HSDPA). Figure 1 depicts the core elements of 2G and 3G mobile networks. In particular, MS comprises of the user's equipment (UE) and a service identity module (SIM) or UMTS SIM (USIM) card. The latter is an integrated circuit that stores various parameters of the mobile network (see section 3.2), including the international mobile subscriber identity (IMSI), which is the permanent identity of a subscriber in the cellular technology, as well as encryption and integrity keys. SIM (and USIM) card stores also the temporary mobile subscriber identity (TMSI), which is a temporary identity and its purpose is to enhance the anonymity of an MS. TMSI should be periodically updated by the mobile network and the new TMSI value is assigned to MS in encrypted form, by means of the TMSI reallocation procedure.

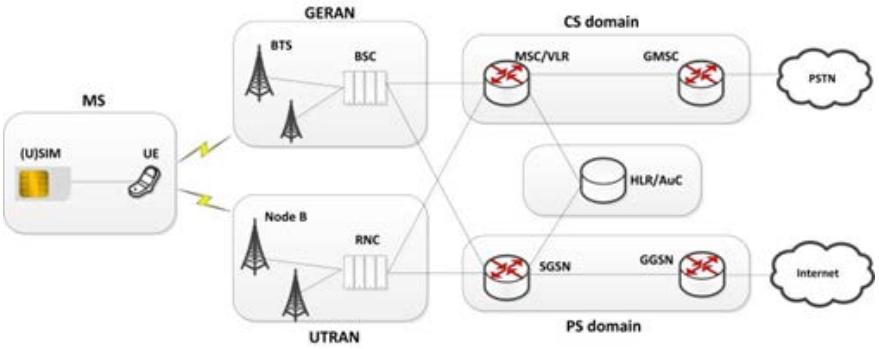


Figure 1: Cellular network architecture

The UE of an MS is often a smartphone that runs a mobile OS. The most prominent mobile OS is Android having a 76.6% market share in the fourth quarter of 2014 [4]. Android applications are implemented with Java programming language and executed in their own virtual machine named Dalvik. The latter relies on the Linux kernel for the underlying OS functionality, such as low-level memory management. Typically, in a smartphone there are two processors: the application processor that is used to run Android OS and the baseband modem processor, where all the radio operations take place. In modern phones, these processors and all other peripheral devices are integrated into one piece of hardware (i.e., System on a Chip).

In GSM, an MS has radio access to the network through a base transceiver station (BTS). A set of BTSs is grouped to a location area (LA) for optimizing signaling, while many BTSs are connected to a base station controller (BSC), which manages radio resources and handoff decisions. BTSs and BSCs constitute the GSM EDGE radio access network (GERAN). BSCs are connected to a mobile switching center (MSC), which carries out call switching and mobility management functions. MSC communicates with the gateway mobile switching center (GMSC), in order to route calls outside the circuit switch (CS) domain of the

mobile network, such as the public switched telephone network (PSTN). The visitor location register (VLR) is a database that contains temporary information that is needed by the network in order to service visiting subscribers. The home location register / authentication centre (HLR/AuC) is the global database that stores permanent information for the mobile subscribers (e.g. IMSI, current location area of an MS, etc.) and produces encryption keys as well as authentication responses for them.

GPRS provides packet switch (PS) services for GSM users by introducing two new core network nodes: serving GPRS support node (SGSN) and gateway GPRS support node (GGSN). SGSN is equivalent to MSC and is responsible for the delivery of data packets from and to MSs within its service area, which consists of many routing areas (RAs), typically subdivisions of LAs. It also forwards packets to GGSN, which interfaces the cellular network to external packet data networks including Internet. Finally, UMTS introduces a new radio access network, called universal terrestrial radio access network (UTRAN). The latter consist of two new network elements: the Node B and the radio network controller (RNC) that are equivalent to BTS and BSC, respectively.

## 2.2 Related Work

The related work in the area of security policies and configurations in cellular networks is rather limited. Recently, the authors of [10] have 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 they 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.

In a work close to ours, the researchers Karsten Nohl and Luca Melette have published a technical report, where they present and analyze the security configurations of GSM mobile networks from several countries around the world [11]. Data was collected using an application developed for Android mobile phones named GSMmap [12]. The same application can operate in a PC with a USB connected Android phone (i.e., the PC version of the application is named xgoldscanner). The rationale behind this application is to automatically make and receive phone calls and SMS, and then log the exchanged messages. Data is uploaded to a server for later analysis. The main limitation of this work is that the application is compatible with a very limited number of mobile devices. In particular, the application operates only on mobile devices that are manufactured with the Intel X-Gold baseband processor [13]. Moreover, the released technical report includes a brief analysis for the security configurations only of GSM mobile networks and there is no evaluation of GPRS, EDGE and 3G networks.

Our work differs in some significant ways from [11]. First, in this work we performed an integrated security measurement of the Greek operators, not only for GSM networks, but also for GPRS, EDGE and UMTS networks for both CS and PS services. Moreover, another significant contribution of this paper is the development of a novel application that allows the extraction of security related data directly from SIM/USIM, eliminating the need of using third party products. The developed application can be installed in rooted iPhone and several Android devices from various vendors, and run transparently in the background.

Regarding the usage of AT commands for security purposes, the authors in [7] utilize AT commands in order to perform SMS fuzzing for iPhone, Android and Windows mobile phones. Their goal was to discover previously unknown software bugs in SMS applications that can be exploited by malicious actors to perform DoS attacks. The authors successfully discovered a set of critical bugs in both iOS and Android SMS

applications.

Moreover, [8] analyses the design and implementation of a passive man-in-the-middle application for iOS and Android phones that listens the communication between the radio interface layer (RIL) (i.e., a software middleware that controls a modem through AT commands) and the modem. In this way, [8] achieved to log all the invoked AT commands by the RIL and the modem during phone calls, SMS sending/receiving, etc. Apart from these works, we have discovered a free online tool named AT command tester [9], which is implemented in Java, and allows the execution of a comprehensive set of AT commands to GSM modules via a web browser.

In our previous work [38] we have elaborated on (U)SimMonitor from a different point of view, by analysing its malware characteristics. In particular, having access to all the security related information and parameters of a mobile subscriber connected to a cellular network, (U)SimMonitor can be employed for malicious (i.e., black hat) usage. To this end, we have explored how (U)SimMonitor can be used as a mobile malware, which is capable of stealing security credentials and sensitive information of the cellular technology through AT commands (e.g., encryption keys, identities, etc.) and compromising the privacy of users and the mobile network security.

Finally, apart from (U)SimMonitor, we have identified some alternatives tools that can be used to perform security measurements in 2G and 3G networks. One of these tools is the Qualcomm extensible diagnostic monitor, named QXDM [28]. The latter can be used to perform diagnostic experiments in mobile networks by real time logging of all over-the-air messages. However, the scope and goals of QXDM and our tool (i.e., (U)SimMonitor) are different. In particular, QXDM is a proprietary PC application that is licensed only to business partners of Qualcomm and not for general use. Moreover, QXDM explicitly requires: 1) a mobile phone with a Qualcomm CPU to perform logging, and, 2) a PC that runs Windows OS and it is connected to the mobile phone through USB to obtain the log data for processing. Thus, it cannot be applied and used in a generic manner. To the best of our knowledge, currently there is no QXDM client that can process the log data directly from the mobile phone. This means that the use of an external PC connected to the phone is mandatory to execute QXDM. In addition, QXDM requires the development of custom parsers to retrieve information and obtain results from the raw QXDM traces.

On the other hand, (U)SimMonitor is a free, open source, mobile application that has a specific goal: To automatically retrieve in the background and present when requested from the user the security parameters of the mobile network. It is executed locally in any rooted mobile phone independently from its CPU that runs either Android or iOS. This means that it does not require the use of an external PC connected to the mobile phone for processing in contrast to QXDM that needs an external PC. This is a key feature of (U)SimMonitor that allowed us to perform experiments and obtain data under daily/typical phone usage of real users (see section 4.2). Moreover, the processing and parsing of data is performed by the mobile application itself and there is no need of developing custom parsers by the users. In addition, the (U)SimMonitor can be extended to include a user-friendly security indicator that will inform mobile users that do not have technical knowledge for the security status of the mobile network in simple and intuitive manner . Finally, as analysed in [38], (U)SimMonitor can be also used as a malware that can compromise the privacy of the users. As a matter of fact, (U)SimMonitor can be combined with other open source monitoring applications such as Androrat [49], to provide advance and diverse monitoring features.

Except for QXDM, another tool which can be used to perform security measurements in mobile networks is the RIL Analyser [50]. The latter is a mobile application for Android devices capable of recording low-

level radio information (such as RRC states) as well as accurate control-plane and user-plane data in mobile networks. However, its main drawback is that it operates only on Android devices that include XGold chipsets.

# 3 (U)SimMonitor

## 3.1 Overview

In this section, we present and analyze the architecture and the key functionality of (U)SimMonitor for the Android OS. Implementation details are presented in [36], while the source code of (U)SimMonitor can be found in [37]. It is important to mention that we have also developed successfully a similar application for the iOS. The main purpose of (U)SimMonitor is to extract security related data from SIM and USIM cards [14]. To achieve this, it communicates with the modem of the mobile phone through a set of AT commands (see section 3.2). This is executed either periodically or based on various events, as analyzed below. (U)SimMonitor stores the fetched data from the modem in a local database on the phone, and periodically or on-demand it uploads the stored data to a server for further processing and analysis. The application runs in the background, while the user can normally operate his/her phone. To this end, the (U)SimMonitor uses the least possible resources of the modem, in order to avoid blocking accidently a voice/data communication. In general, (U)SimMonitor has been designed to collect data transparently, without disrupting the proper operation of the phone.

Moreover, (U)SimMonitor stops and restarts the RIL daemon when it executes an AT command to avoid possible disruptions from the Android. More specifically, the functionality of the RIL daemon is to provide the interface that handles the communication between the Android phone framework services and the radio hardware [15]. During our tests, we observed that initially (U)SimMonitor was not able to communicate directly with the modem through AT commands. After investigation, we discovered that some vendors implement RIL in a way that the modem is able to respond only to one process at a time. For this reason, the (U)SimMonitor could not execute AT commands to the modem, since the latter was always in use by Android. To overcome this limitation, the (U)SimMonitor incorporates a payload that stops the RIL daemon before initiating the execution of AT commands and restarts it immediately after the modem responds to the last AT command. We remark here that during our experiments and usage of the (U)SimMonitor, the normal operation of the phone was not affected by stopping and starting the RIL daemon, since this procedure (i.e., restarting the RIL daemon) is executed in under one second (<1 sec).

## 3.2 AT Commands and Data Collection

AT commands lie at the core of (U)SimMonitor providing various operations to control a modem, as specified in 3GPP TS 27.007 [16]. Based on the provided functionality, AT commands can be categorized as follows:

1) Call control: commands for initiating and controlling calls.

2) Data call control: commands for controlling the data transfer and the quality of service.

3) Network services control: commands for supplementary services, operator selection, locking and registration.

4) SMS control: commands for sending, notifying of received SMS messages, and configuring SMS services.

5) Data retrieval: commands to obtain information for the subscriber and the phone, such the IMSI, the international mobile station equipment identity, radio signal strength, batter status. etc.

(U)SimMonitor makes extensive use of the last category of AT commands (i.e., data retrieval) to extract security related data from the SIM/USIM. A summarizing list of the AT commands, which we used to obtain security related data as well as their proper syntax, is presented in the Appendix. In all our testing mobile devices, we have successfully installed and executed (U)SimMonitor. These devices are: Samsung S-5500, Samsung S-6500, Samsung Galaxy s2, ZTE Blade, HTC Sensation XE with Beats Audio, and Sony Ericsson Xperia LT18i. (U)SimMonitor collects sensitive and security related data [17][2], which are extracted through AT commands. These data are briefly presented below:

**IMSI**: The international mobile subscriber identity is a unique number permanently associated to the holder of the SIM/USIM card. Its size is 8 bytes. The first three bytes of IMSI represent the mobile country code (MCC), while the next two or three bytes represent the mobile network code (MNC). The remaining bytes represent the mobile subscriber identification number (MSIN).

**$K_c$**: A 64 bit ciphering key used to encrypt voice and data communication between the MS and BTS of GSM networks [18].

**$K_{cGPRS}$**: A 64 bit ciphering key used to encrypt communication data between the MS and the SGSN of GPRS networks.

**CK**: A 128 bit ciphering key used to encrypt the communication between the MS and the RNC of UMTS.

**IK**: A 128 bit key to protect the integrity of the signaling data between the MS and the RNC of UMTS network.

**Threshold**: A 24 bit value which represents the lifetime of the CK and IK keys in UMTS networks.

**Ciphering Indicator**: This is a 1 bit flag that allows the MS to detect whether ciphering is switched on (flag set to 1) or off (flag set to 0). The ciphering indicator feature may be disabled by the mobile network operator.

**TMSI**: The temporary mobile subscriber identity is a temporary identity of MS, which is assigned from the mobile network and it is used instead of IMSI for enhancing anonymity. TMSI is valid for CS domain and its size is 4 bytes.

**TMSI Time**: This is a 1 byte value and represents the maximum time interval which the assigned TMSI can be used.

**P-TMSI**: The packet TMSI is the complement of TMSI in the UTRAN/GERAN packet switching (PS) domain.

**P-TMSI Signature value**: This is a signature used by the 3G network for verifying the validity of P-TMSI of MS. Its size is 3 bytes.

**LAI**: The location area identity (LAI) is a 5 bytes unique identifier for each location area in the CS domain. It consists of MCC, MNC and the location area code (LAC).

**RAI**: The routing area identity for PS domains is the analogous to the LAI for CS domains. RAI consists of LAI (which is 5 bytes) and a 1 byte Routing Area Code.

**Provider**: This is the name of the mobile network operator.

**Cell Id**: This is the unique identity of the cell tower, where the MS is connected at the moment of data collection.

**Network type**: This parameter indicates the mobile network technology, where the MS is connected, at the moment of data collection. It may have several values including GSM/GPRS, EDGE, UMTS, HSDPA, LTE, UNKNOWN, etc.

**Roaming**: A 1 bit value that indicates whether MS is outside the coverage area of its home network.

Moreover, (U)SimMonitor may collect some additional metadata as mentioned below:

**Event Type**: This value indicates the event that triggered data collection. The possible event types are: i) outgoing and incoming calls or SMSs, ii) screen on or off, iii) power on or off, iv) periodic (i.e., a time interval where data is collected periodically).

**Latitude, Longitude**: These values are the coordinates of the geographical position of MS at the moment of data collection. The coordinates are determined either by the GPS sensor of the phone or the Wifi signals.

**Timestamp**: The date and time of data collection.

## 3.3 Software Architecture

As shown in Figure 2, the software architecture of (U)SimMonitor consists of five units, each one undertaking a specific task: (i) data collection, (ii) event listener, (iii) metadata collection, (iv) data parsing, and (v) data upload.

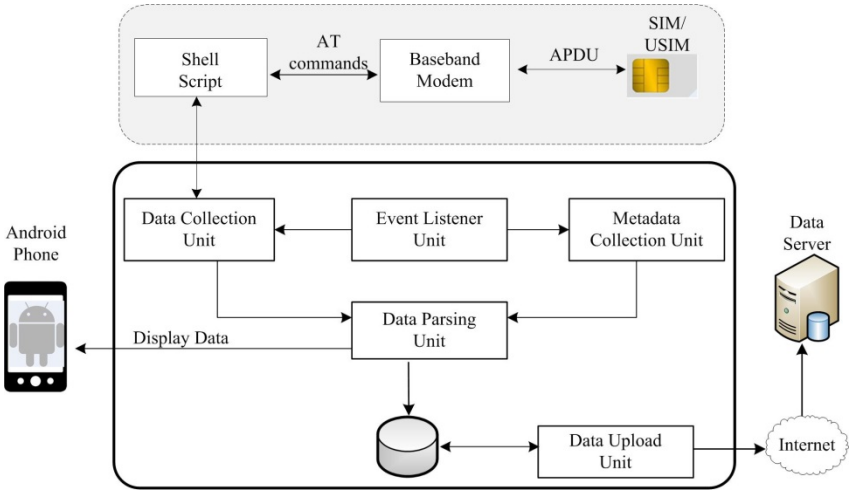


Figure 2: (U)SimMonitor application architecture

More specifically, the event listener unit monitors and captures the occurrence of an event. Possible event types are: i) outgoing and incoming calls or SMSs, ii) screen on or off, iii) power on or off, and iv) periodic (i.e., a time interval where data is collected periodically). When one of these events occurs, the event listener unit triggers the metadata collection and data collection units. The metadata collection unit obtains the coordinates of the smartphone using the GPS sensor or WiFi signals as well as the time that data extraction occurred. On the other hand, the data collection unit obtains data from the SIM/USIM card. To achieve this, first it creates a system process to invoke a shell script (i.e., in Android OS the Linux shell is located in */system/bin/sh*). The latter communicates with the baseband modem by executing sequentially a set of AT

commands (i.e., in our mobile phones the baseband modem is the serial device */dev/smd0*). For each AT command, the modem contacts to USIM/SIM to obtain the related data. The response of each executed AT command is forwarded to the data collection unit through the shell script. After receiving the response of the last executed AT command, the data collection unit terminates the system process in order to save memory resources.

Both the data unit and metadata collection unit transfer the obtained data to the data parsing unit, which filters out unnecessary information and stores the final data in a database. Optionally, the parsing unit can also display the final data in the phone's screen. Figure 3 shows an Android phone and iPhone displaying extracted data using (U)SimMonitor. Finally, as its name implies, the upload unit transfers the database contents to a secure server via secure shell and subsequently deletes the contents of the database to save memory space in the phone.

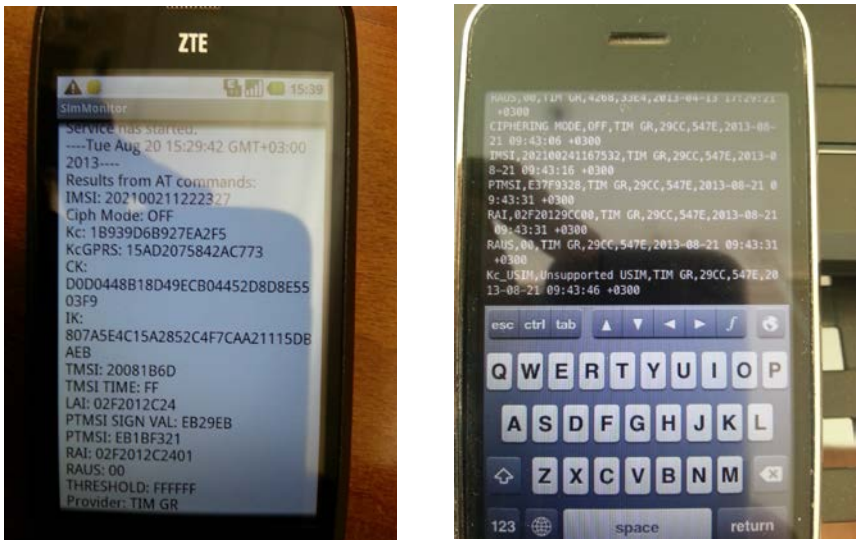


Figure 3: (U)SimMonitor displaying collected data in Android and iOS

# 4 Acquisition and evaluation of the security policies

## 4.1 Motivation

(U)SimMonitor provides helpful and currently unavailable services to both the mobile subscribers and network operators. These services have to do with the acquisition and evaluation of the security policy that a cellular operator applies as well as the configuration of specific security and networking parameters, which have direct impact on the level of security that the deployed cellular network offer to its users. These include:

a) the invocation of certain security procedures specified by the related standards, but their deployment and configuration are left to the operator;
b) the cryptographic algorithms that the operator selects to employ (i.e., from the available set determined by the related standards) to protects its users' communications;
c) the employed technology (i.e., 2G or 3G), since each one is accompanied by a different security architecture [3][19].

A fundamental security procedure that depends on the security policy of the serving cellular network is AKA, where the mobile user is authenticated to the network (i.e., and the opposite if the user is connected to a 3G network) as well as a new encryption (and integrity in case of 3G) key is generated. Due to the lack of precise directives, the operator decides the frequency of performing the AKA procedure. In particular, TS 143.020 [20] clearly mentions that: "*Key setting may be initiated by the network as often as the network operator wishes"*. However, the AKA procedure is time-consuming in case that MSC/VLR or SGSN should contact with HLR/AuC to fetch fresh authentication vectors (i.e., GSM triplets or UMTS quintuplets respectively). This procedure is named as Authentication Data Request (ADR). For this reason, the operator may choose to invoke AKA as rarely as possible, in order to achieve fast connection establishments, as some operators advertize, but with the cost of less security.

When a MS wishes to use the network radio services for a call or data session, it is identified by means of its temporary identity (i.e., TMSI). Before the network releases the assigned radio resources, it may choose to assign a new TMSI to MS using the TMSI reallocation procedure. As stated in TS 143.020 [20], changing TMSI at the end of the communication is optionally and left to the operator. The security implications of this choice are evident. If a temporary identity does not change frequently, it becomes essentially a permanent identity and its exposure threatens the privacy of a subscriber.

The use of the permanent identity of a mobile subscriber (i.e., IMSI) should be avoided, in order to ensure its privacy. However, when MS registers for the first time in a serving network, then MSC/VLR or SGSN should identify MS by means of its IMSI. In such a case, the current MSC/VLR or SGSN could obtain IMSI by requesting it from the previous MSC/VLR or SGSN that served MS. However, according to the TR 23.912 [21], for efficiency reasons the operator can choose to retrieve IMSI directly from MS. In particular, TR 23.912 [21] mentions: "*A reduction in the real-time cost of Inter-VLR Location Updates can be achieved if the subscriber's IMSI is retrieved from the mobile station. However, this option has associated security impacts since the IMSI is communicated over the air interface unciphered."* This means that it is up to the operator's policy when to request for IMSI from a MSC/VLR and when to request it directly from MS, in order to reduce delays, at the cost of less security.

The IMSI of a MS can be also obtained using HLR lookups. More specifically, Internet-accessible web services can perform HLR lookups (for free or with very low cost) using only the mobile number of the MS and disclose the IMSI of MSs, thus compromising their privacy. As a defensive mechanism, mobile operators may optionally hide the IMSI in HLR lookups when it is requested by these web services.

Furthermore, during AKA, MS and the mobile network negotiate on the cryptographic algorithms that will be used to protect voice and data communications. More specifically, first MS sends its ciphering capabilities to MSC/VLR (or SGSN). The latter compares the ciphering capabilities of MS with these that the network supports, and responds to MS by providing the algorithms that will be employed. As a result, even though MS might support the more advanced algorithms, it is the operator that eventually selects the security algorithms that will be used. The available cryptographic algorithms in GSM are A5/1 to A5/3 and in UMTS the Kasumi and SNOW 3G [3]. The security of the earlier versions of A5 (i.e. A5/1 and A5/2) has been broken [23], which means that in case that a mobile operator has not upgraded its network and still uses these insecure algorithms, then its subscribers are exposed to a variety of threats.

Despite the fact that the security of A5/1 is broken, there are two security countermeasures that mobile operators can apply to enhance the security of A5/1 algorithm. The first countermeasure is padding randomization and the second one is the inclusion of the International Mobile Station Equipment Identity

(IMEI) in the cipher mode complete message. More specifically, regarding padding randomization, GSM packets are padded using the predefined value '2b' to reach a specific packet length, and, subsequently they are encrypted. Thus, an attacker that has captured encrypted GSM packets has knowledge of the ciphertext and the portion of the plaintext that correspond to the padding bytes. This observation can be exploited to perform known plaintext attacks in order to retrieve the A5/1 encryption key as quickly as possible. To counteract against known plaintext attacks, GSM specifications [45] recommends but does not mandate mobile networks to use random values for padding packets. The second countermeasure (i.e., inclusion of IMEI in cipher mode command message) also protects cracking A5/1 keys based on known plaintext attacks. More specifically, the first encrypted GSM packet, which is sent from the MS to the BTS, is the ciphering mode complete. Although this packet is encrypted, its plaintext is known to the attacker, because its fields are predictable [18]. To avoid known plaintext attacks based on the ciphering mode complete message, mobile operators can instruct the MS to include the IMEI value (i.e., a unique number used to identify mobile phones) in the ciphering mode complete command, which is unknown to attackers. This feature is optional and depends on the mobile operators whether it will be enabled or not.

Finally, the 3GPP standards (i.e., 3GPP TS 33.102 [2], section 6.8) allow 2G and 3G networks to interoperate at the same time, in order to maximize coverage. Thus, operators may choose to deploy and simultaneously use 2G and 3G networks, without any restriction from the 3GPP specifications, despite the security flaws of 2G networks.

By monitoring and recording security and networking data from the SIM/USIM card of an MS connected to a cellular network, (U)SimMonitor is able to answer to the following questions:

1. What is the network technology that serves MS?
2. How frequently or under what usage and behavior conditions the user is authenticated/re-authenticated?
3. How frequently the employed encryption keys change or what is the maximum time of a key usage?
4. How frequently the assigned temporary identities change or what is the maximum time that a temporary identity is used?
5. How frequently or under what conditions the serving network asks from an MS the subscriber's permanent identity?

Except for the above, another critical question that is also related with the security policy and configurations of a cellular network is what encryption algorithms are employed. However, (U)SimMonitor cannot answer to this question, since there is no such AT command that allows the modem to provide this information. Therefore, for the sake of completeness of the carried evaluation, we have used QXDM [28], to provide results regarding the encryption algorithms employed in both 2G and 3G technologies. It is important to mention that we have also used QXDM to cross-validate the results of (U)SimMonitor.

## 4.2 Methodology of Experiments

We have performed a series of experiments in order to acquire informative data regarding the security policies and configurations of the three major mobile operators in Greece: Vodafone, Wind and Cosmote. In particular, we have focused on the following networking and security related activities: (a) the usage of 2G or 3G network technology; (b) the employed cryptographic algorithms; (c) the frequency of AKA executions and the related change/refresh of keys; (d) the frequency of IMSI requests; and (e) the frequency of TMSI reallocations.

The basic instrument that has been employed to perform the experiments with a simple and efficient manner was (U)SimMonitor. It allowed us to use typical mobile phones as our testbed and obtain data without affecting their normal functionality (see section 3.1). In this way, we successfully performed experiments and gathered data even from daily phone usage. Standalone (U)SimMontor was used to acquire data regarding the usage of 2G or 3G network technology, the frequency of AKA executions and the related change/refresh of keys, and the frequency of TMSI reallocations. (U)SimMomitor combined with simtrace [5][6] was employed to capture data regarding the frequency of IMSI requests; while QXDM was used to obtain data for the employed cryptographic algorithms and whether padding randomization and inclusion of IMEI in the ciphering mode complete message are enabled. The duration of all experiments was 9 months (September 2013 to May 2014).

In total, we performed four sets of experiments that simulate four different usage scenarios:

1. In the first set, we collected data for stationary users. For this reason, we developed a custom android application that automatically initiates calls, SMSs and data requests periodically (i.e., every 1 minute, 10 minutes and 1 hour).
2. In the second set, we obtained data for mobile users. To this end, we performed a wardriving covering a wide geographical area in Athens (see Figure 4) to simulate the behavior of mobile users.
3. In the third set, we captured data by powering off and on the mobile phone periodically (i.e., every 1 hour, 5 hours and 24 hours). We developed a custom application that disables and enables all radio communications of the phone by turning on and off, respectively, the airplane mode (i.e., soft power off).
4. In the fourth set, we acquired data under daily/typical phone usage of real users. The goals of this set of experiments were first to obtain data for maximum and average usage time of cryptographic keys, temporary identities etc., as well as to verify the security policies of the operators that were obtained during the previous experiments

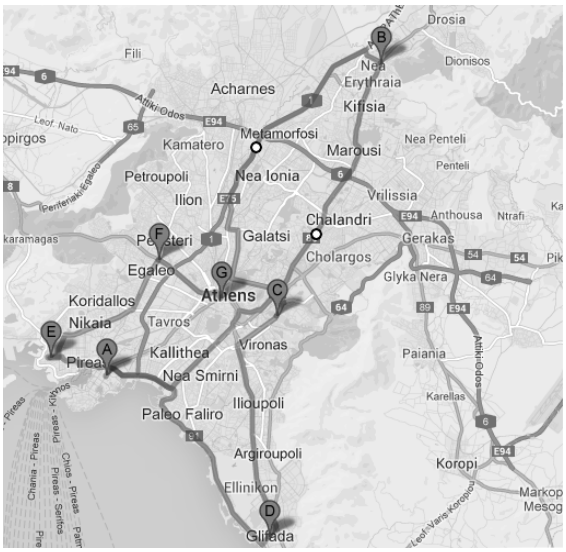


Figure 4: War driving route in Athens

All set of experiments were carried out using four difference network access scenarios: (i) access to the CS domain using 2G network technology; (ii) access to the CS domain using 3G network technology; (iii)

access to the PS domain using 2G network technology; and (iv) access to PS domain using 3G network technology. It is worth mentioning that all experiments were performed for both SIM and USIM cards. After the completion of experiments, we followed a rigorous methodology, in order to analyze large data sets. That is, first, we validated the obtained data to verify its correctness, and then, we used custom Python parsers to sort, filter and aggregate multiple data sources in automated manner. Finally, we derived the numerical results using SQL queries and deduced a set of critical observations.

## 4.3 Evaluation of Numerical Results

### 4.3.1 Network technology, cryptographic algorithms and security countermeasures employed

Table 1 shows the collected measurements regarding the employed technologies by the three cellular operators, during our experiments. The type "unknown" indicates some rare cases that we were not able to identify the network technology. *We may deduce that all three operators utilize both 2G (GSM/GPRS and EDGE) and 3G (UMTS and HSPDA) networks to provide services for their subscribers*. The simultaneous use of 2G and 3G technologies has direct security implications. That is, regardless of the enhanced security of 3G networks, the subscribers are exposed to attacks that exploit the insecurity of 2G networks (i.e., weakest link security).

It is well known that 2G networks lack several important security features, which make them susceptible to wide range of attacks. In particular, the lack of network authentication in 2G allows an attacker to impersonate a network provider and perform a false base station attack, in order to eavesdrop on the victim's conversation. Moreover, 2G uses weak ciphering algorithms [33] combined with small key size (i.e., 64-bit keys), which can be cracked in seconds with modern hardware technologies. Another security feature that 2G lacks is integrity protection of signaling messages, fact that can be exploited by an attacker to perform a man-in-the-middle attack in 3G networks, as described in [27]. As depicted in Table 1, the subscribers that are served by the network of Wind encounter the higher risk regarding the aforementioned threats, since Wind employs 2G technologies nearly 28%. On the other hand, Vodafone and Cosmote utilize 3G technologies above 90% and 2G less than 10%.

The employed ciphering algorithms play the most important role in the establishment of secure communication channels between MSs and the mobile network. We observed (i.e., using QXDM) that all mobile operators use the A5/1 algorithm for the encryption of GSM channels (i.e., voice services over 2G network). A5/1 is an outdated algorithm and several attacks have been published for it [23]. The use of this weak encryption algorithm allows an attacker to easily intercept calls and SMS. *Considering the fact that 10% to 27% of the underlying geographical area is covered by the 2G technology, it is evident that the mobile subscribers that reside at these points and use voice services are vulnerable to the disclosure of their communications.* The deployment of A5/3 in GSM can eliminate a large proportion of these attacks. *However, no mobile operator uses A5/3 in GSM despite the fact that the majority of mobile phones support the particular algorithm.*

On the other hand, in GPRS/EDGE networks (i.e., data services over 2G), it was observed that the mobile operators use the GEA/2 algorithm for channel encryption. GEA/2 is a proprietary stream cipher which employs a 64-bit key. The GEA/2 algorithm has been kept secret (i.e., security by obscurity) and it has not been reversed engineered yet, facts that leave questions regarding its strength. Moreover, as mentioned in [33], the small key size may allow the creation of rainbow tables to recover the employed encryption key. Finally, in 3G, we noticed that the A5/3 algorithm is used by all operators for both voice and data services, providing confidentiality and integrity. A5/3 is based on Kasumi block cipher, which is specified in 3GPP

specifications [34] and employs a 128-bit key size with 64-bit block size. Despite its design weaknesses discovered in [35], there is no practical attack to A5/3, thus its employment is considered to be a good security policy. The percentage of the employment of each algorithm can be easily estimated by considering the coverage of 2G/3G for every operator as well as the underlying type of services.

Table 1: The employed technologies by the Greek mobile operators in Athens

| Operator | GSM/GPRS | GSM/EDGE | UMTS | HSDPA | UNKNOWN |
|---|---|---|---|---|---|
| Vodafone | 8.38% | 1.35% | 78.75% | 11.5% | 0.02% |
| Wind | 0.17% | 27.35% | 14.13% | 53.72% | 4.62% |
| Cosmote | 3.43% | 2.49% | 86.06% | 8.02% | 0% |

Finally, regarding the use of padding randomization and inclusion of IMEI in the cipher mode complete message, we have observed that *none of the mobile operators apply padding randomization*, while only Vodafone instructs MS to include its IMEI value in the cipher mode complete message. These results indicate that 2G subscribers are vulnerable to disclosure of their communications using freely available tools such as Kraken [43] that can be used to retrieve the A5/1 encryption key with probability 90% within seconds [51].

### 4.3.2 Frequency of AKA execution

A mobile network should perform AKA as frequent as possible; otherwise, its subscribers are exposed to several threats for longer time periods and thus, with higher impacts. For example, if an encryption key kc (i.e., employed in GSM) is cracked [23] or compromised by (U)SimMonitor, then an attacker can use this key to: (i) impersonate the legal user; (ii) make calls and send SMSs on behalf of the victim (i.e., overbilling); and (iii) intercept phone calls and SMSs. The time-frame that the attacker can use the cracked/compromised key and carry out the above attacks depends on the frequency of AKA execution. That is, if AKA is performed frequently, then the attacker cannot use the cracked/compromised key for a long time period and, hence the impact of the carried attacks will be lower. On the other hand, the lower the frequency of AKA is, the higher will be the impact of the possible attacks. Another reason to perform AKA frequently is described in [10]. That is, during a TMSI re-allocation procedure, a fresh key is necessary to encrypt the TMSI value, in order to guarantee unlinkability between the old and new TMSI. Otherwise, an attacker can mount a replay attack and identify and track an MS, even if the TMSI value changes frequently.

Table 2 shows the numerical results for AKA execution. For static users we observed that the two operators perform AKA with a specific pattern. In particular, in the CS domain Vodafone perform AKA every 16 calls/SMS, while Wind applies a different AKA execution policy for SIM and USIM cards. That is, Wind performs AKA every 6 calls/SMS for SIM cards and every 1 call/SMS for USIM cards. Cosmote performs AKA, arbitrarily, and we didn't identified any specific pattern. For this reason, we computed an average value that is approximately every 10 calls/SMS. In the PS domain, both Vodafone and Wind follow a different policy for 2G and 3G networks. That is, both operators perform AKA every 1 data request/call/SMS in 2G networks and every 11 data request/calls/SMS in 3G networks. On the other hand, Cosmote performs AKA every 1 data request/call/SMS. *Thus, it can be deduced that the existence of patterns helps a possible attacker in case a key is compromised to organize and perform better an attack, as he/she knows what is the behavior of the network. For static Vodafone subscribers that make/receive 2-*

*3 calls per day, an encryption key might last for days or a week, fact that puts them in high risk. The same happens for static Vodafone and Wind subscribers that present light usage of PS services over 3G. Finally, it is important to mention that the deployment of the new 3G technology in PS domain for Vodafone and Wind comes with a worst security policy, compared to this of 2G.*

In the scenario of mobile users there is a great discrepancy between the mobile operators. In particular, in CS domain Vodafone executes AKA only in 6.5% of the location area change, Cosmote in 57%, while Wind again applies a different security policy for SIM and USIM cards. That is, AKA is performed in 55% for SIM cards and 100% for USIM cards. Except for Wind's USIM cards that perform AKA in all cases of a location area update, Cosmote and Wind's SIM execute AKA in approximately once in every two updates. *This can be consider acceptable for mobile users that cross and change location areas frequently, but for users that move within a small geographical area (i.e., center of the town) this is another bad network configuration, which reduces the rate of performing AKA and changing the employed cryptographic keys*. Even worse is the situation for Vodafone, which performs AKA only once in every twenty location updates, fact that puts its subscribers in high risk. On the other hand, in PS domain, the operators follow different security policies depending on whether an MS access a 2G or 3G network. Specifically, Vodafone presents the best security policy by performing AKA in 91% of the routing area updates, in both 2G and 3G networks; Cosmote follows with 43% in 2G and 92% in 3G; and, finally, Wind depicts the worst with 83% in 2G and only 23% in 3G. *Thus, the introduction of the 3G technology improves the applied security policy in Cosmote; while it makes it worst in the network of Wind*.

In powering-off/on mobile phones scenario we observed that Cosmote has the best configuration, since it always perform an AKA in both CS and PS domain. A worrying fact in the CS domain is that Vodafone performs AKA only in 6.5% of powering on in 2G networks and 55% in 3G. *It seems that the emergence of 3G improves the applied security policy in the Vodafone's network, but the fact that in 3G only one of the two power-off/on is authenticated, is not satisfactory from a security point of view*. Wind again follows a different security policy for SIM and USIM cards in the CS domain. More specifically, we observed that SIM cards perform AKA in 100%, while USIM in 57%. *This means that as the technology evolves and the subscribers replace their old SIM cards with new advanced USIM cards, expecting enhanced 3G services, the actual provided security level becomes lower*. In PS domain, Vodafone and Wind perform AKA 100% when MSs access to 2G networks and 16% and 18% respectively when they access 3G. *This is* a*nother unforeseen result, which proves that as the network technology evolves, the applied security policy may become worst. The results of this set of experiments are alarming, since it is proved that it is feasible for an attacker, first, to steal the temporary identity and the keys of a subscriber (i.e., by simply using (U)SimMonitor) and then, (after the power-off of the user) impersonate the legitimate user performing and receiving calls, SMS, etc. Considering that currently mobile phones are used as authentication entities, by receiving SMS containing one time passwords (e.g., banking applications), the impacts of such attacks can be very severe*.

For typical users, we observed that the best performance in CS domain is presented by Wind, which uses the same cryptographic keys i.e., Kc, CK, IK for maximum 1380 minutes (i.e., 23 hours) and on average 77 minutes, then follows Cosmote with maximum 1680 (i.e., 1 day and 4 hours) and on average 128 (i.e., about 2 hours), and last is Vodafone with maximum 1798 (i.e., 1 day and 6 hours approximately) and on average 145. On the other hand, in the PS domain the best performance belongs to Vodafone with maximum time of key usage 829 minutes (i.e., about 14 hours) and average 37, the second to Cosmote with maximum time of keys usage 940 (i.e., 15,6 hours) and average of 47, and the last to Wind with maximum time 1238

(i.e., 20,6 hours) and average of 90. *Although in PS domain the usage time of the cryptographic keys follows similar patterns with the CS domain, the observed values are lower, mainly, because of two reasons: (i) the smaller dimension of the routing areas, compared to the location areas, meaning that there are more routing area updates than location area updates, and thus, AKA occurs more frequently; and (ii) the security policy applied in the PS domain is better than this of CS. However, it can be deduced that for typical users that move within the city of Athens, changing on average the cryptographic keys between 1 and 2,5 hours is risky; but keeping them for a day or more is unacceptable from the security viewpoint.*

Table 2: AKA execution

| CS domain | | | | |
|---|---|---|---|---|
| Operator | Static users (consequetive requests for AKA) | Mobile users | Power-off/on | Typical users (max-average use time) |
| Vodafone | 16 | 6.5% | 6.5% in 2G \| 55% in 3G | 1798 - 145 (minutes) |
| Wind | 6 SIM \| 1 USIM | 55% SIM \|100% USIM | 100% SIM \| 57% USIM | 1380 - 77 (minutes) |
| Cosmote | 10 (average) | 57% | 100% | 1680 - 128 (minutes) |
| PS domain | | | | |
| Operator | Static users (consequetive requests for AKA) | Mobile users | Power-off/on | Typical users (max-average use time) |
| Vodafone | 1 in 2G \| 11 in 3G | 91% | 100% in 2G \|16% in 3G | 829 - 37 (minutes) |
| Wind | 1 in 2G \| 11 in 3G | 83% in 2G \| 23% in 3G | 100% in 2G \|18% in 3G | 1238 - 90 (minutes) |
| Cosmote | 1 | 43% in 2G \| 92% in 3G | 100% | 940 - 47 (minutes) |

### 4.3.3 Frequency of IMSI requests and TMSI reallocations

As mentioned previously, the specifications lack precise directives regarding when the mobile network should request the IMSI of a user, as well as when a TMSI should be updated (i.e., TMSI reallocation). Ideally, an IMSI should never be transmitted, because a possible attacker can easily read it, as it is conveyed in plaintext. Moreover, TMSI should be re-allocated in every network activity. If a TMSI is not updated frequently, then it tends to become essentially a permanent identity defeating its own purpose. A poor policy for IMSI requests and TMSI reallocations may result in the loss of mobile subscribers' anonymity, and hence, an attacker may achieve to identify and track them. Mobile identities are currently used by market research companies, such as those referred in [24] and [25], 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 shopping habit information without their consent, while usually share the tracking information with third parties to maximize profit [26].

Table 3 shows numerical results for IMSI requests. For static users (i.e., 1st set of experiments), we observed that no IMSI request occurs in CS and PS domain. In the scenario of mobile users (2nd set of experiments), in the CS domain, Cosmote requests the IMSI of an MS over the air interface, rarely, with a rate of 0,6% of the cases that the subscriber changes a location area. Vodafone also presents a low rate of IMSI request, 4%. On the other hand, Wind depicts a high rate of IMSI request that reaches 41% for SIM cards and 55% for USIM cards. *This means that in about half of the cases where the Wind's subscribers change location, they are obliged by the network to disclosure their identities. Thus, if an adversary establishes passive devices that monitor the cellular signaling at the borders of locations areas, he/she may track the movements of almost all the subscribers of Wind*. In the scenario of power-off/on (3rd set of experiments in the CS domain), we noticed alarming results for Vodafone, where in 41% of the cases that MSs access 3G (i.e., it represents about 90% of the network coverage in the area of experiments), the network asks for the subscribers IMSIs. Similar behavior we noticed for the Wind's subscribers that own SIM card. Based on the above, for typical users, (i.e., 4th set of experiments) in the CS domain, the best

performance we noticed in the network of Cosmote where on average a subscriber is asked for its IMSI 4 times in a period of 30 days; Vodafone follows with 1 in a day; while worrying results we obtained for the network of Wind, that is 13 IMSI requests on average, per user, per day.

Table 3: IMSI requests

| CS domain | | | | |
|---|---|---|---|---|
| Operator | Static users | Mobile users | Power-off/on | Typical users |
| Vodafone | 0% | 4% | 4% in 2G \| 41% in 3G | 1 in a day |
| Wind | 0% | 41% SIM \| 55% USIM | 55% SIM \| 0.6% USIM | 13 in a day |
| Cosmote | 0% | 0.6% | 0% | 4 in 30 days |
| PS domain | | | | |
| Operator | Static users | Mobile users | Power-off/on | Typical users |
| Vodafone | 0% | 0% | 0% in 2G \| 10% in 3G | 3 in 30 days |
| Wind | 0% | 0% | 0% in 2G \| 5% in 3G | 2 in 30 days |
| Cosmote | 0% | 0% | 0% in 2G \| 10% in 3G | 3 in 30 days |

On the other hand, in the PS domain all operators present better performance. More specifically, none of them asks for the IMSIs of its subscribers either as the latter stay in the same routing area performing service requests (i.e., static users – 1st set of experiments), or move and change routing areas (i.e., mobile users - 2nd set of experiments), or power-off/on (i.e., 3rd set of experiments) and access 2G network. However, the situation is not the same as the subscribers of the three operators power-off/on their devices and access 3G technology, which represents the majority of the network coverage between 70% and 90%. In this case, Cosmote and Vodafone ask for IMSIs in 10%, while Wind in 5%. *Although the observed values are low, it is alarming that we notice again that the security policy followed in the new network technology (i.e., 3G) is worst than this followed in the old (i.e., 2G).* As a result of the applied security policy in the PS domain for IMSI requests, we observed that on average (i.e., 4th set of experiments) a Vodafone and Cosmote subscriber transmits its identity 3 times in month period, while a Wind subscriber 2 times. Finally, we performed HLR lookups using Internet accessible web services (such as [52]) to examine whether mobile operators hide IMSI in HLR lookups. We observed that Cosmote readily provides the IMSI of its subscribers to third party web services, while Vodafone and Wind correctly hide their IMSI values.

Regarding the frequency of TMSI reallocations for static users (i.e., 1st set of experiments), we observed that none of the operators assigns a new TMSI or P-TMSI as a function of call/SMS/data requests in both (i.e., CS and PS) domains. The operators treat in the same way the MSs that have heavy network usage, and hence utilize their temporary identities, with these that are simply connected/attached to the network without performing any activity. It is important to mention that in all activities with the network, an MS is identified by its temporary identities exposing them to various threats, which attempt to link the TMSI and/or P-TMSI with the subscriber. The recorded data also depict that only Cosmote performs periodic TMSI allocation for static MS every 240 minutes (i.e., 4 hours), which is considered a quite long time-period for subscribers that use their phones. 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 of TMSI reallocation is very weak, because the same TMSI is used for every call/data/SMS request, allowing an adversary to easily identify and track a user.

Table 4: TMSI reallocation

| CS domain | | | | |
|---|---|---|---|---|
| Operator | Static users | Mobile user | Power-off/on | Typical user (max-average use time) |
| Vodafone | No | 100% | 100% in 2G \| 41% in 3G | 1513 - 66 (minutes) |
| Wind | No | 41% SIM \| 55% USIM | 55% in SIM \|100% in USIM | 1780 - 89 (minutes) |
| Cosmote | 240 (minutes) | 100% | 100% | 240 - 39 (minutes) |
| PS domain | | | | |
| Operator | Static user | Mobile user | Power-off/on | Typical user (max-average use time) |
| Vodafone | No | 100% | 100% | 1513 - 66 (minutes) |
| Wind | No | 100% | 100% | 1610 - 77 (minutes) |
| Cosmote | 240 (minutes) | 100% | 100% | 240 - 34 (minutes) |

For mobile users (i.e., 2nd set of experiments), we observed that in the CS domain Vodafone and Cosmote always reallocate the assigned TMSIs (i.e., 100%) when the moving users change location areas; while Wind updates TMSIs only when the network requests for IMSIs, which means 41% for SIM and 55% for USIM cards. On the other hand, in the PS domain the three operators always change P-TMSIs (i.e., 100%) when the corresponding users change routing areas, following a good security practice (i.e., 100%). In the scenario of powering-off/on mobile phones (i.e., 3rd set of experiments), we noticed that in general all operators assign a new TMSI (i.e., 100%). A notable exception is Vodafone in the CS domain, where in the cases that the mobile phone is switched on and connected to a 3G network (i.e., new technology), then a new TMSI is allocated only in 41%. Another exception is the usage of SIM cards in the network of Wind, where TMSI reallocation occurs in 55%.

Finally, studying typical users (i.e., 4th set of experiments), we observed that Cosmote presents the best performance both in the CS and PS domain, since it is the only operator that periodically reallocates TMSIs. Moreover, Cosmote always changes the assigned TMSI to a user that moves and changes location/routing area or power-off/on its phone. As a result of the above, the maximum time of TMSI usage in both CS and PS domain is 240 minutes and the mean time 39 minutes in the CS and 34 minutes in PS domain, respectively. On the other hand, both Vodafone and Wind follow a poor security policy regarding TMSI reallocation in both CS and PS domain. This fact is depicted in the observed values, where the maximum time of TMSI usage for Vodafone is approximately 1513 minutes for both CS and PS domain, while mean time is about 66 minutes. Wind presents even higher values for maximum time of TMSI usage (i.e., 1780 minutes in CS domain and 1610 minutes in PS domain) and mean time (i.e., 89 minutes for CS domain and 77 minutes for PS).

## 4.4 Performance analysis

Based on the above analysis, it is proved that mobile operators follow a rather arbitrary security policy and configuration of the security mechanisms in cellular networks, which expose mobile subscribers to a variety of well-known and feasible threats. However, since the 3GPP specifications do not define strict and explicit security guidelines, a question that arises is: “How should mobile operators configure and deploy security mechanisms to provide the highest level of security for their subscribers?” Considering the conducted experiments and the derived observation, we argue that the following best practises should be adopted by mobile operators:

1. The user and the network should be mutually authenticated and cryptographic (i.e., encryption and integrity) keys should be changed. These functions should be triggered by every phone call, SMS, data session, change of location area, or timer expiration.

2. Similarly, temporary identities should also be changed. Again this should be triggered by every phone call, SMS, data session, change of location area, or timer expiration.
3. The permanent identity of a user should be provided over the radio interface, only, if the network cannot identify him/her by means of his/hers temporary identity.
4. GSM/GPRS security mechanisms should be avoided and used only as fallback mechanism in areas where there is no 3G coverage.

It is evident that these best security practises are difficult to be implemented, always, since they may cause network performance issues. For this reason, mobile networks should configure and deploy security mechanisms in such a way that will minimize security threats as much as possible, without affecting network performance. To put the discussion into a context, in the following we analyze the performance impact of authentication and key updates procedure on the HLR/AuC. To this end, we have estimated the mean number of ADRs based on an analytical model derived in [41]. Recall from section 4.1, that an ADR is performed between the MSC/VLR (or SGSN in 3G networks) and the HLR/AuC during an AKA procedure, when the former wants to obtain fresh authentication vectors from the latter. We argue that the number of ADRs performed in a mobile network is a critical parameter that can significantly affect the performance of the mobile network. More specifically, an ADR is considered an expensive operation, in the sense that it may cause significant delays in the establishment of a voice/data communication channel, especially when the MSC/VLR (or SGSN) and the HLR/AuC are located at different countries [42]. Additionally, a large number of ADRs may disrupt the normal operation of HLR/AuC, which is considered to be one of the most important mobile network elements [5]. In particular, it is a central repository of user location and profile information in the network and undertakes a series of tasks including generation of authentication vectors, delivery of phone call and text messages, data recording for billing, etc. [44].

It is important also to mention that apart from the number of ADRs, there are other performance metrics that can be used to quantitatively characterize the impact of the AKA in HLR/AuC, such as time delays, and throughput in HLR/AuC. However, the computation of these performance metrics for each mobile network is not feasible, because we need access to internal network parameters that operators do not provide publicly, such as mean number of MS in each cell, number of BTS, network dimensioning, etc. To overcome this limitation, some previous works [46][48] have estimated the performance impact of AKA by measuring the related cost and time delay of message exchanges. However, the derived numerical results of these works are theoretical, since they have used normalized values. Finally, in [47] the authors have computed the performance impact of AKA on the level of mobile devices by measuring CPU and memory load but they have not estimated the burden on the network side.

As we mentioned previously, the analytical model that we elaborate in this section is based on [41]. The key assumption of [41] is that for every call that an MS performs, an authentication and key update is performed. However, our experiments showed that this assumption does not hold in general and mobile operators do not employ AKA for each call (see Table 2 - Static users in CS domain). Thus, we extend the model of [41] using an additional parameter denoted as α, which represents the number of the successive calls that are performed without executing AKA. Moreover, let $N$ be the total number of ADRs performed when the MS resides in a specific MSC/VLR (or SGSN) area. For each ADR, the number of authentication vectors obtained from the HLR/AuC is $K$. Assume that the number of outgoing calls form a Poisson process with rate $\lambda$. For a specific time period $\tau$, let $\Theta(n, K, \tau)$ be the probability that there $n$ ADRs to the HLR/AuC. Note that $n$ ADRs are performed if there $(n-1)K + k$ $(1 \leq k \leq K)$ AKAs in the period $\tau$. According to the probability function of the Poisson distribution we have:

$$\Theta(n,K,\tau)=\sum_{k=1}^{K}\left\{\frac{(\lambda\tau/\alpha)^{(n-1)K+k}}{[(n-1)K+k]!}\right\}e^{-(\lambda/\alpha)\tau}$$

Let $t$ be the period that an MS resides in a MSC/VLR (or SGSN) serving area. We assume that the residence time of MS follows exponential distribution with mean $1/\mu$ and density function $f(t)=\mu e^{-\mu t}$. In this case, the probability $P(n,K)$ that there are $n$ ADRs during the MS residence in the MSC/VLR (or SGSN) area can be derived as follows:

$$P(n,K)=\int_{t=0}^{\infty}\Theta(n,K,t)f(t)dt$$

$$P(n,K)=\sum_{k=1}^{K}\int_{t=0}^{\infty}\left\{\frac{(\lambda t/\alpha)^{(n-1)K+k}}{[(n-1)K+k]!}\right\}e^{-\lambda t/\alpha}\mu e^{-\mu t}dt$$

$$P(n,K)=\sum_{k=1}^{K}\left\{\frac{(\lambda/\alpha)^{(n-1)K+k}}{[(n-1)K+k]!}\right\}\int_{t=0}^{\infty}t^{(n-1)K+k}\,e^{-\lambda t/\alpha}\mu e^{-\mu t}dt$$

$$P(n,K)=\left(\frac{\lambda/\alpha}{\lambda/\alpha+\mu}\right)^{(n-1)K}\left[1-\left(\frac{\lambda/\alpha}{\lambda/\alpha+\mu}\right)^{K}\right]$$

Moreover, assume that $E[N]$ is the mean number of ADRs when the MS resides in the MSC/VLR (or SGSN) area. Then,

$$E[N]=\sum_{n=1}^{\infty}nP(n,K)$$

$$E[N]=\frac{1}{1-\left(\frac{\lambda/\alpha}{\lambda/\alpha+\mu}\right)^{K}}$$

$$E[N]=\frac{1}{1-\left(\frac{\lambda}{\lambda+\alpha\mu}\right)^{K}}$$

Figure 5 plots $E[N]$ as a function of $\alpha$ for various values of the call rate $\lambda$. The number $K$ of generated authentication vectors by HLR/AuC is equal to 5, as recommended by the 3GPP specifications [2]. As shown in figure 5, it is evident that the mean number of ADRs is a decreasing function of α. However, it is observed that for high values of α, the mean number of ADRs becomes almost a constant function of α. In particular, for $\alpha>5$ the impact of $\alpha$ becomes almost negligible. From this observation we can deduce that mobile operators do not gain any significant advantage by avoiding the execution of AKA for successive calls greater than 5. For instance, Vodafone that performs AKA every 16 calls may have the same number of ADRs compared to Wind that performs AKA every 6 calls for subscribers with SIM card. Therefore, our findings imply that the adoption of strict security policies (such as executing AKA frequently) does not necessarily increase performance overheads.

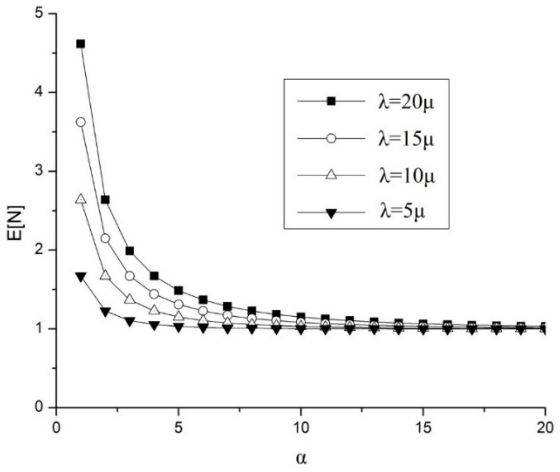


Figure 5: Mean number of ADRs as a function of $\boldsymbol{\alpha}$ (the value of $\boldsymbol{K}$ is 5).

### 4.5 Discussion

From the above analysis we can deduce that mobile operators should evaluate the performance burden caused by each security procedure considering also operator-specific parameters (e.g., number of subscribers) to effectively regulate the tradeoffs between security and performance. We believe that (U)SimMonitor can serve towards this direction. In particular, it can be used to acquire meaningful real security measurements, which depict how specific network configurations affect the security services provided to users. Moreover, (U)SimMonitor enables researchers to evaluate and compare the security services supported by different operators, providing quantitative results. Such an approach will also allow the mobile operators and the standardization groups to study and elaborate on specific security thresholds and reference values, considering the security threats from the one hand, and the network performance from the other.

The existence of security parameters that can be measured (i.e., security metrics), security thresholds and reference values will promote the development of quantitative risk analysis approaches for cellular networks, which will facilitate the better understanding of the notions of network security as well as the related risks. It is important to mention that the existing risk analysis approaches either provide qualitative results [29] or are based on subjective inputs [30][31], resulting in moderate acceptance.

Finally, employing (U)SimMonitor at end-users, they can be aware about the level of security provided by the cellular networks that serve them [32]. This can be performed by monitoring the above cellular security metrics and estimating the distance between the recorded values and best practises. For example, it can notify how often the encryption keys are refreshed and how often the temporary identities are updated. In this way, (U)SimMonitor can serve towards raising awareness for the employed security practises of mobile networks. Such a critical functionality is currently missing from both Android and iPhone devices.

## 5 Conclusions

This paper presented (U)SimMonitor, a novel mobile application which extracts security parameters from the (U)SIM cards allowing the analysis of the security policy that a cellular operator enforces. Using (U)SimMonitor as our basic analysis tool, we conducted a set of experiments for three mobile operators in

Greece in a time period of 9 months. Numerical results revealed that the lack of precise directives in 3GPP specifications result in poor security configurations and weak security policies, exposing subscribers of mobile networks to several threats. Another alarming result that we discovered was that in some cases the 3G network security policies were weaker than the 2G counterparts. Thus, we can derive the rather contradictory observation that the introduction of 3G technology does not necessarily improve the provided security level and sometimes can even deteriorate it. Based on the experimental analysis and findings of this work, we believe that (U)SimMonitor introduces a new security tool that enables both mobile operators and subscribers to evaluate and compare the provided security services in cellular networks. Moreover, it paves the way for the development of new quantitative risk analysis approaches for cellular networks based on real networking and security measurements, facilitating in the better understanding of the notions of mobile network security as well as the related risks.

# 6 Appendix

In this section we present the AT commands (see Table 5) that the (U)SimMonitor uses to extract data. SIM/USIM cards are contact (as opposed to contactless) smart cards, which are specified by ISO standard 7816 [39]. They contain a microprocessor and three types of memory, which are RAM, ROM and EEPROM. The file system is stored in an internal EEPROM and has a hierarchical structure with a root file called Master File (MF). There are also two other types of files: Dedicated Files (DF) and Elementary Files (EF). The main difference between these two types of files is that a DF includes only a header, whereas an EF contains a header and a body. The header contains metadata for the file system, while body contains information related to the mobile network and the subscriber [40].

AT commands can be used to extract information from the SIM and USIM cards. The exact syntax of AT Commands depends on their type. We can recognize two main types of AT commands:

- Basic commands are AT commands that do not start with "+", such as D (Dial), A (Answer), H (Hook control), and O (Return to online data state).
- Extended commands are AT commands that start with "+" and their main functionality is to retrieve data from (U)SIM cards.

(U)SimMonitor uses AT commands from the second category (i.e., extended). In particular, the most useful and frequently invoked AT command of (U)SimMonitor is +CRSM, which extracts various mobile network parameters from (U)SIM cards. A generic format for the +CRSM command invoked by the (U)SimMonitor is the following one:

$$AT+CSRM=x, y, p1, p2, w$$

The value of parameter *x* indicates whether the command will write to or read data from SIM/USIM card. Since the (U)SimMonitor only extracts data, the value of *x* is always equal to “176”, which indicates a READ operation. The value of *y* is an identifier for the EF that we want to extract data. For example, the identifier of the EF that includes the IMSI for SIM and USIM cards is “6F07” (hexadecimal format). The values of *p1, p2* represent the high and low order offset respectively (in terms of number of bytes) from the beginning of the identifier that we want to read or write data. In (U)SimMonitor both values of *p1, p2* were both equal to 0 indicating no offset. Finally, the value of *w* indicates the number of bytes that the specific AT command wants to read or write.

Apart from CSRM, (U)SimMonitor also uses the commands COPS to extract the name of the operator and CREG to extract the LAC and the Cell ID. In the following table, we provide the exact syntax of the AT commands as they are invoked by (U)SimMonitor and their respective functionality.

Table 5: AT commands used in (U)SimMonitor

| Functionality | Storage location in SIM and USIM cards | AT command |
|---|---|---|
| 1. Extraction of IMSI | Stored in 6F07 (decimal 28423) for SIM and USIM | (SIM/USIM) AT+CRSM=176,28423,0,0,3 |
| 2. Extraction of Ciphering Indicator | Stored in 6FAD (decimal 28589) for SIM and USIM | (SIM/USIM) AT+CRSM=176,28589,0,0,3 |
| 3. Extraction of Ciphering Key Kc | Stored in 6F20 (decimal 28448) for SIM and 4F20 (decimal 20256) for USIM | (SIM) AT+CRSM=176,28448,0,0,9<br>(USIM) AT+CRSM=176,20256,0,0,9 |
| 4. Extraction of Ciphering Key KcGPRS | Stored in 6F52 (decimal 28498) for SIM and 4F52 (decimal 20306) for USIM | (SIM) AT+CRSM=176,28498,0,0,9<br>(USIM) AT+CRSM=176,20306,0,0,9 |
| 5. Extraction of Ciphering Key CK and Integrity Key IK | Stored in 6F08 (decimal 28424), applied to USIM only | (USIM) AT+CRSM=176,28424,0,0,33 |
| 6. Extraction of TMSI, TMSI TIME and LAI | Stored in 6F7E (decimal 28542) for SIM and USIM | (SIM/USIM) AT+CRSM=176,28542,0,0,11 |
| 7. Extraction of PTMSI, PTMSI Signature Value, RAI and RAUS | Stored in 6F53 (decimal 28499) for SIM and 6F73 (decimal 28531) for USIM | (SIM) AT+CRSM=176,28499,0,0,14<br>(USIM) AT+CRSM=176,28531,0,0,14 |
| 8. Extraction of THRESHOLD | Stored in 6F5C (decimal 28508), applied to USIM only | (USIM) AT+CRSM=176,28508,0,0,3 |
| 9. Extraction of Provider | - | AT+COPS? |
| 10. Extraction of Lac and Cell ID | - | AT+CREG? |

# 7 Acknowledgment

This research has been partially funded by the European Commission in part of the ReCRED project (Horizon H2020 Framework Programme of the European Union under GA number 653417).

# 8 References

[1] A.T. Kearney, The mobile economy, GSMA, 2014.
[2] 3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 9), 2009.
[3] Christos Xenakis, Lazaros Merakos, “Security in third Generation Mobile Networks,” Computer Communications, Elsevier Science, Vol. 27, No. 7, pp. 638-650, May 2004.
[4] http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[5] 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.
[6] Simtrace, http://bb.osmocom.org/trac/wiki/SIMtrace
[7] Collin Mulliner, Charlie Miller, “Fuzzing the Phone in your Phone”, Black Hat USA 2009.
[8] Fabien Sanglard, “Tracing the broadband: Part 1 and Part 2”, http://fabiensanglard.net/cellphoneModem/
[9] AT module tester, http://m2msupport.net/m2msupport/module-tester/
[10] 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.
[11] http://gsmmap.org/
[12] https://play.google.com/store/apps/details?id=de.srlabs.gsmmap&hl=el
[13] http://www.intel.com/content/www/us/en/wireless-products/mobile-communications/mobile-phone-platforms.html
[14] ETSI TS 102 221 V9.0.0 (2010-02), Smart Cards, UICC-Terminal interface, Physical and logical characteristics (Release 9).
[15] Android Platform Development Kit, Radio Layer Interface, Netmite, http://www.netmite.com/android/mydroid/development/pdk/docs/telephony.html
[16] 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).
[17] 3GPP TS 35.201, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification (Release 9), 2009.
[18] Karsten Nohl, “Attacking phone privacy”, BlackHat USA, Las Vegas, Aug 2010.
[19] Christos Xenakis, “Security Measures and Weaknesses of the GPRS Security Architecture,” International Journal of Network Security, Vol.6, No.2, pp:158–169, Mar. 2008.
[20] ETSI TS 143.020, Digital cellular telecommunications system (Phase 2+); Security related network functions (3GPP TS 43.020 version 10.1.0 Release 10), 2011
[21] 3GPP TR 23.912 3rd Generation Partnership Project; Technical Specification Group Core Network; Technical report on Super-Charger (Release 1999), 2000.
[22] 3GPP TS 35.201, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification, (Release 9), 2009.
[23] K.Nohl and S. Munaut , GSM Sniffing, 27th Chaos Communication Congress, Berlin, Dec. 2010.
[24] http://www.pathintelligence.com
[25] http://www.smart-flows.com
[26] The Register, http://www.theregister.co.uk/2012/01/11/phone_tracking_expert/
[27] U. Meyer, S. Wetzel, “A Man-in-the-Middle Attack on UMTS”, Proceedings of ACM Workshop on Wireless Security (WiSe 2004), Oct. 2004.
[28] QUALCOMM Incorporated, available at: www.qualcomm.com.
[29] Marianthi Theoharidou, Alexios Mylonas, Dimitris Gritzalis, “A Risk Assessment Method for Smartphones”, 27th IFIP TC 11 Information Security and Privacy Conference (SEC 2012), Heraklion, Crete, Greece, June 4-6, 2012
[30] Nikos Vavoulas, Christos Xenakis, “A Quantitative Risk Analysis Method for Deliberate Threats,” In Proc. 5th International Workshop on Critical Information Infrastructures Security, (CRITIS 2010), Athens, Greece, Sept. 2010.
[31] Christos Xenakis, Danae Apostolopoulou, Angeliki Panou, Ioannis Stavrakakis, "A Qualitative Risk Analysis for the GPRS Technology", In Proc. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC-08), Shanghai, China, December 2008.
[32] Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis, “Delegate the smartphone user? Security awareness in smartphone platform”, Computers and Security, Elsevier Science, Volume 34, pp 47–66, May 2013.
[33] K. Nohl, L. Melette, “GPRS Intercept: Wardriving your country”, Chaos Communication Camp (CCCamp 2011), Germany 2011.
[34] 3GPP TS 35.202, Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification”, 2009.
[35] O. Dunkelman, N. Keller, A. Shamir, “A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony”, Cryptology ePrint Archive: Report 2010/013.

[36] Dimitrios Raptodimos, “Design and implementation of an Android application for extraction of security related data from SIM/USIM”, MSc thesis, University of Piraeus, http://digilib.lib.unipi.gr/dspace/bitstream/unipi/5851/1/Raptodimos.pdf
[37] https://github.com/SSL-Unipi/U-SIMonitor
[38] 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), Talinn, Estonia, May 2015.
[39] ISO. Identification Cards - Integrated Circuit Cards with Contacts, http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx
[40] Antonio Savoldi, Paolo Gubian “SIM and USIM filesystem: a forensics perspective” 22nd Annual ACM symposium on Applied computing (SAC '07), Seoul, Korea, March 2007
[41] Y.-B. Lin, Y.-K. Chen, “Reducing authentication signaling traffic in third-generation mobile network”, IEEE Transactions on Wireless Communications, vol.2, no. 3, pp. 493-501, May 2003
[42] Y. Zhang, M. Fujise, “An improvement for authentication protocol in third generation wireless networks”, IEEE Transactions on Wireless Communications, vol.5, no. 9, pp. 2348-2352, Sep. 2006
[43] Kraken, available at https://opensource.srlabs.de/projects/a51-decrypt
[44] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, T. La Porta, “On cellular botnets: measuring the impact of malicious devices on a cellular network core”, 16th ACM conference on Computer and communications security (CCS 2009), Nov. 09-13, 2009, Chicago, Illinois, USA
[45] 3GPP TS 44.006, 3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification (Release 12), 2014
[46] Wei Liang, Wenye Wang," A Quantitative Study of Authentication and QoS in Wireless IP Networks," in Proc. of IEEE INFOCOM'05, Miami, FL, USA, March, 2005.
[47] Z. Faigl, J. Pellikka, L.Bokor, A. Gurtov, “Performance Evaluation of Current and Emerging Authentication Schemes for Future 3GPP Network Architectures”, Computer Networks, Elsevier, Vol. 60. pp:60-74, February 2014.
[48] Chan-Kyu Han, Hyoung-Kee Choi, Jung Woo Baek, Ho Woo Lee, “Evaluation of authentication signaling loads in 3GPP LTE/SAE networks”. IEEE 34th Conference on Local Computer Networks (LCN), Zürich, Switzerland, Oct. 2009
[49] Androrat, available at https://github.com/wszf/androrat
[50] Narseo Vallina-Rodriguez, Andrius Aucinas, Mário Almeida, Yan Grunenberger, Konstantina Papagiannaki, Jon Crowcroft, “RILAnalyzer: a comprehensive 3G monitor on your phone”, Internet Measurement Conference (IMC 2013), Barcelona, Spain, 2013
[51] Decrypting GSM phone calls, available at https://srlabs.de/decrypting_gsm
[52] https://www.hlr-lookups.com/