Malicious Actions Against the GPRS Technology

Christos Xenakis
xenakis@di.uoa.gr

Computer Network Laboratory, Department of Informatics and Telecommunications
University of Athens, 15784 Athens, Greece.
tel: + 30 210 7275418, fax: + 30 210 7275601.

Abstract

This paper presents the malicious actions (attacks), which threaten the GPRS network, the GPRS mobile users, and the data that either reside at the network or are transferred through it. These attacks may be performed by malicious third parties, mobile users, network operators or network operator personnel, which exploit the security weaknesses of the GPRS security architecture. Moreover, the attackers take advantage of the lack of adequate security measures that should protect certain parts of the GPRS architecture. The possible attacks against GPRS targets the equipment of mobile users, the radio access network, the GPRS backbone network, and the interfaces that connect the latter to other GPRS networks or the public Internet. The results of these attacks might be the compromise of end-users security, the users over billing, the disclosure or alteration of critical information, the services unavailability, the network breakdown, etc. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept mobile Internet. In order to defeat certain attacks and enhance the level of security provided by GPRS, specific security measures are proposed.

Keywords: GRPS, security architecture, security weaknesses, security attacks, security measures

1 Introduction

The General Packet Radio Services (GPRS) [1] is a service that provides packet radio access for Global System for Mobile Communications (GSM) users. It enables the provision of a variety of packet-oriented multimedia applications and services to mobile users, realizing the concept mobile Internet. For the successful implementation of these applications and services over GPRS, security is considered as a vital factor. In order to meet security objectives, GPRS

uses a specific security architecture, which aims at protecting the network against unauthorized access and the privacy of users. This architecture is based on the security measures applied to GSM, since the GPRS system is built on the GSM infrastructure. However, GPRS is more exposed to intruders compared to GSM because it uses the IP technology, which presents known vulnerabilities. Similarly to IP networks, intruders to the GPRS system may attempt to breach the confidentiality, integrity, availability or otherwise attempt to abuse the system in order to compromise services, defraud users or any part of it.

Upon their nature, the attacks against the GPRS system can be categorized into passive and active attacks. A passive attack happens when an attacker un-intrusively taps on a communication channel between two nodes without disturbing the communication. The primary purpose of this attack is to discover some valuable information about the data or control messages sent over the communication channel. On the other hand, an active attack typically involves an attacker's direct intervention with the data and/or control information sent. An active attacker can listen, modify, and inject data into the communication channel. Active attacks can be further classified into two groups, external and internal attacks. External attacks are caused by nodes/persons that do not belong to GPRS, while internal attacks are usually caused by compromised nodes/persons that belong to it. Hence, internal attacks are more difficult to be detected and the protection against them requires more sophisticated solutions.

This paper presents the malicious actions (attacks), which threaten the GPRS network, the GPRS mobile users, and the data that either reside at the network or are transferred through it. These attacks may be performed by malicious third parties, mobile users, network operators or network operator personnel, which exploit the security weaknesses of the GPRS security architecture. Moreover, the attackers take advantage of the lack of adequate security measures that should protect certain parts of the GPRS architecture. The possible attacks against GPRS targets the equipment of mobile users, the radio access network, the GPRS backbone network, and the interfaces that connect the latter to other GPRS networks or the public Internet. The results of these attacks might be the compromise of end-users security, the users over billing, the disclosure or alteration of critical information, the services unavailability, the network breakdown, etc. The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept mobile Internet. In order to defeat certain attacks and enhance the level of security provided by GPRS, specific security measures are proposed.

The rest of this article is organized as follows. Section 2 briefly describes the GPRS network architecture, and section 3 presents the security architecture applied to it. Section 4 analyzes the attacks that threaten the GPRS mobile users, the GPRS network and the data that either reside at the network or are transferred through it. Section 5 proposes some security measures that defeat certain attacks and enhance the level of security provided by GPRS.

Finally, section 6 contains the conclusions.

2 GPRS network

The network architecture of GPRS [1] is presented in Figure 1. A GPRS user owns a Mobile Station (MS) that provides access to the wireless network. From the network side, the Base Station Subsystem (BSS) is a network part that is responsible for the control of the radio path. BSS consists of two types of nodes: the Base Station Controller (BSC) and the Base Transceiver Station (BTS). BTS is responsible for the radio coverage of a given geographical area, while BSC maintains radio connections towards MSs and terrestrial connections towards the fixed part of the network (core network).

The GPRS Core Network (CN) uses the network elements of GSM such as the Home Location Register (HLR), the Visitor Location Register (VLR), the Authentication Centre (AuC) and the Equipment Identity Register (EIR). HLR is a database used for the management of permanent data of mobile users. VLR is a database of the service area visited by an MS and contains all the related information required for the MS service handling. AuC maintains security information related to subscribers' identity, while EIR maintains information related to mobile equipments identity. Finally, the Mobile Service Switching Centre (MSC) is a network element responsible for circuit-switched services (e.g., voice call) [1].

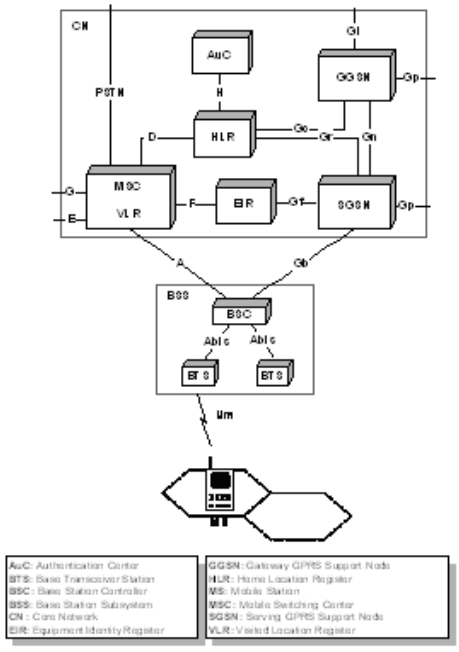

Figure 1: GPRS network architecture

As presented previously, GPRS reuses the majority of the GSM network infrastructure.

However, in order to build a packet-oriented mobile network some new network elements (nodes) are required, which handle packet-based traffic. The new class of nodes, called GPRS support nodes (GSN), is responsible for the delivery and routing of data packets between a MS and an external packet data network (PDN). More specifically, a Serving GSN (SGSN) is responsible for the delivery of data packets from, and to, a MS within its service area. Its tasks include packet routing and transfer, mobility management, logical link management, and authentication and charging functions. A Gateway GSN (GGSN) acts as an interface between the GPRS backbone and an external PDN. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format (e.g., IP), and forwards them to the corresponding PDN. Similar is the functionality of GGSN in the opposite direction. The communication between GSNs (i.e., SGSN and GGSN) is based on IP tunnels through the use of the GPRS Tunneling Protocol (GTP) [4].

3 GSM security architecture

In order to meet security objectives, GPRS employs a set of security mechanisms that constitute the GPRS security architecture. Most of these mechanisms have been originally designed for GSM, but they have been modified to adapt to the packet-oriented traffic nature and the GPRS network components. The GPRS security architecture, mainly, aims at two goals: a) to protect the network against unauthorized access, and b) to protect the privacy of users. It includes the following components [5]:

- Subscriber Identity Module (SIM)
- Subscriber identity confidentiality.
- Subscriber identity authentication.
- User data and signaling confidentiality between the MS and the SGSN.
- GPRS backbone security.

3.1 Subscriber Identity Module-SIM

The subscription of a mobile user to a network is personalized through the use of a smart card named Subscriber Identity Module (SIM) [6]. Each SIM-card is unique and related to a user. It has a microcomputer with a processor, ROM, persistent EPROM memory, volatile RAM, and an I/O interface. Its software consists of an operating system, file system, and application programs (e.g., SIM Application Toolkit). The SIM-card is responsible for the authentication of the user by prompting for a code (Personal Identity Number - PIN), the identification of

the user to a network through keys, and the protection of user data through cryptography. To achieve these functions it contains a set of security objects including:

- A (4-digit) PIN code, which is used to lock the card preventing misuse.
- A unique permanent identity of the mobile user, named International Mobile Subscriber Identity (IMSI) [7].
- A secret key, Ki, (128 bit) that is used for authentication.
- An authentication algorithm (A3) and an algorithm that generates encryption keys (A8) [4].

Since the SIM-card of a GSM/GPRS subscriber contains security critical information, it should be manufactured, provisioned, distributed, and managed in trusted environments.

3.2 Subscriber identity confidentiality

Subscriber identity confidentiality deals with the privacy of the IMSI and the location of a mobile user. It includes mechanisms for the protection of the permanent identity (IMSI) when it is transferred in signaling messages, as well as measures that preclude the possibility to derive it indirectly from listening to specific information, such as addresses, at the radio path.

Subscriber identity confidentiality is mainly achieved by using a Temporary Mobile subscriber Identity (TMSI) [5] [7], which identifies the mobile user in both the wireless and wired network segments. The TMSI has a local significance, and, thus, it must be accompanied by the routing area identity (RAI) in order to avoid confusions. The MS and the serving VLR and SGSN only know the relation between the active TMSI and the IMSI. The allocation of a new TMSI corresponds implicitly for the MS to the de-allocation of the previous one. When a new TMSI is allocated to the MS, it is transmitted to it in a ciphered mode. The MS stores the current TMSI and the associated RAI in a non-volatile memory, so that these data are not lost when the MS is switched off.

Further to the TMSI, a Temporary Logical Link Identity (TLLI) [6] identifies also a GPRS user on the radio interface of a routing area. Since the TLLI has a local significance, when it is exchanged between the MS and the SGSN, it should be accompanied by the RAI. The TLLI is either derived from the TMSI allocated by the SGSN or built by the MS randomly, and, thus, provides identity confidentiality. The relationship between the TLLI and the IMSI is only known in the MS and in the SGSN.

3.3 Subscriber identity authentication

A mobile user that attempts to access the network must first prove his identity to it. User authentication [1] protects against fraudulent use and ensures correct billing. GPRS uses the

authentication procedure already defined in GSM with the same algorithms for authentication and generation of encryption key, and the same secret key, Ki, (see Figure 2). However, from the network side, the whole procedure is executed by the SGSN (instead of the base station) and employs a different random number (GPRS-RAND), and, thus, it produces a different signed response (GPRS-SRES) and encryption key (GPRS-Kc) than the GSM voice counterpart.

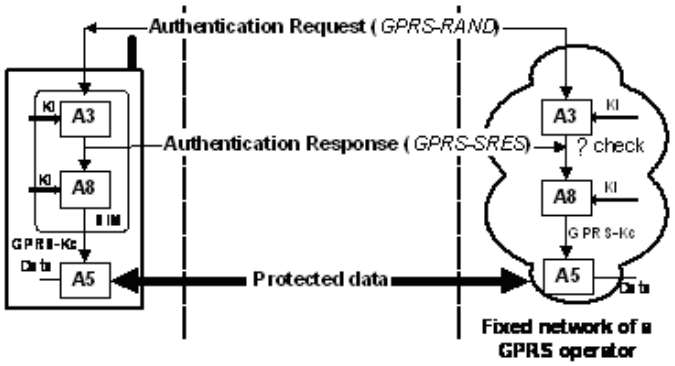

Figure 2: GPRS authentication

To achieve authentication of a mobile user, the SGSN must possess security related information for the specific user. This information is obtained by requesting the HLR/AuC of the home network that the mobile user is subscribed. It includes a set of authentication vectors, each of which includes a random challenge (GPRS-RAND), and the related signed response (GPRS-SRES) and encryption key (GPRS-Kc) for the specific subscriber. The authentication vectors are produced by the home HLR/AuC using the secret key Ki of the mobile subscriber.

During authentication the SGSN of the serving network sends the random challenge (GPRS-RAND) of a chosen authentication vector to the MS. The latter encrypts the GPRS-RAND by using the A3 hash algorithm, which is implemented in the SIM-card, and the secret key, Ki. The first 32 bits of the A3 output are used as a signed response (GPRS-SRES) to the challenge (GPRS-RAND) and are sent back to the network. The SGSN checks if the MS has the correct key, Ki, and, then, the mobile subscriber is recognized as an authorized user. Otherwise, the Serving Network (SN) rejects the subscriber's access to the system. The remaining 64 bits of the A3 output together with the secret key, Ki, are used as input to the A8 algorithm that produces the GPRS encryption key (GPRS-Kc).

A3 and A8 algorithms are not included in the specifications of GSM/GPRS, but the latter describe only their external interfaces. For the implementation of these algorithms, many network operators use an example algorithm, called COMP128, which is included in the GSM memorandum of understanding. COMP128 is a keyed hash function [13]. It takes a 16 byte (128 bits) key, K, and 16 byte (128 bits) of data, R, to output a 12 byte (96 bits) hash. The

algorithm first loads K and R in a 32-byte vector X[]. K is stored in X[0..15] and R is stored in X[16..31]. Then, eight iterative loops are applied on X[]. Each iteration starts with a compression that follows the butterfly-structure (see Figure 3). The compression consists of five levels of table lookups using T0[512], T1[256], T2[128], T3[64] and T4[32] respectively. In all iterations except for the last, a permutation follows the compression. Each Ti contains only (8-i)-bit values. Thus, compression results in 32 4-bit values, which are then assembled into 16 bytes before the permutation is applied. These 16 bytes are stored into X[16..31] and K is loaded into X[0..15] before a new iteration begins. The resulting 128 bits after the eight iterations are further compressed to 12 bytes, which form the output of the algorithm.

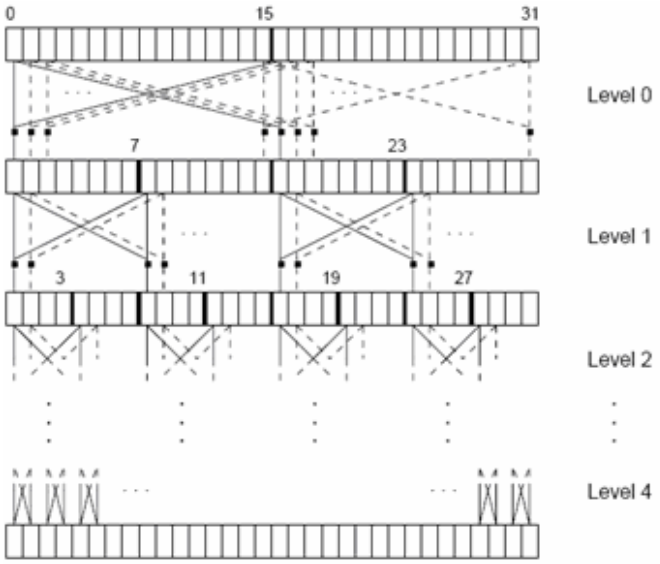

Figure 3: The butterfly structure of compression in COMP128

For each level, the compression works on pairs of equal sized sections of X[]. In level 0, (j = 0), X[] is split into two sections X[0..15] and X[16..31]. The value of each right element, X[i+16], (i = 0..15) is combined with that of the left element, X[i], to compute y=(X[i] + 2*X[i+16]) mod 512. Similarly, the value of the left element, X[i] is combined with the corresponding right element to compute z=(2*X[i]+X[i+16]) mod 512. X[i] and X[i+16] are then replaced by T0[y] and T0[z] before the next level starts. This crosswise substitution, as shown in Figure 3, is referred as the butterfly-structure. On every new level, a section gets divided into a pair of sections in which the same scheme is applied [13].

3.4 Data and signaling protection

User data and signaling protection over the GPRS radio access network is based on the GPRS ciphering algorithm (GPRS-A5) [8], which is also referred to as GPRS Encryption Algorithm (GEA) and is similar to the GSM A5. Currently, there are three versions of this algorithm:

GEA1, GEA2 and GEA3 (that is actually A5/3), which are not publicly known, and, thus, it is difficult to perform attacks on them. The MS device (not the SIM-card) performs GEA using the encryption key (GPRS-Kc), since it is a strong algorithm that requires relatively high processing capabilities. From the network side, the SGSN performs the ciphering/deciphering functionality protecting signaling and user data over the Um, Abis, and Gb interfaces (see Figure 1).

During authentication the MS indicates which version(s) of the GEA supports, and the network (SGSN) decides on a mutually acceptable version that will be used. If there is not a commonly accepted algorithm, the network (SGSN) may decide to release the connection. Both the MS and the SGSN must cooperate in order to initiate the ciphering over the radio access network. More specifically, the SGSN indicates whether ciphering should be used or not (which is also a possible option) in the Authentication Request message, and the MS starts ciphering after sending the Authentication Response message (see Figure 2).

GEA is a symmetric stream cipher algorithm (see Figure 4) that uses three input parameters (GPRS-Kc, INPUT and DIRECTION) and produces an OUTPUT string, which varies between 5 and 1600 bytes. GPRS-Kc (64 bits) is the encryption key generated by the GPRS authentication procedure and is never transmitted over the radio interface. The input (INPUT) parameter (32 bits) is used as an additional input so that each frame is ciphered with a different output string. This parameter is calculated from the Logical Link Control (LLC) frame number, a frame counter, and a value supplied by the SGSN called IOV (input offset value). IOV is set up during the negotiation of LLC and layer 3 parameters. Finally, the direction bit (DIRECTION) specifies whether the output string is used for upstream or downstream communication.

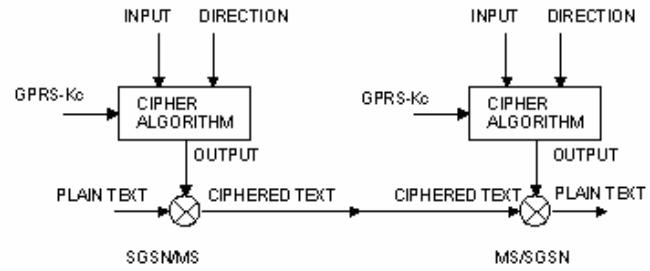

Figure 4: GPRS ciphering

After the initiation of ciphering, the sender (MS or SGSN) processes (bit-wise XOR) the OUTPUT string with the payload (PLAIN TEXT) to produce the CIPHERED TEXT, which is sent over the radio interface. In the receiving entity (SGSN or MS), the OUTPUT string is bit-wise XORed with the CIPHERED TEXT, and the original PLAIN TEXT is obtained. When the MS changes SGSN, the encryption parameters (e.g., GPRS-Kc, INPUT) are trans-

ferred from the old SGSN to the new SGSN, through the (inter) routing area update procedure in order to guarantee service continuity.

3.5 GPRS backbone security

The GPRS backbone network includes the fixed network elements and their physical connections that convey user data and signaling information. Signaling exchange in GPRS is mainly based on the Signaling System 7 (SS7) technology [9], which does not support any security measure for the GPRS deployment. Similarly, the GTP protocol that is employed for communication between GSNs does not support security. Thus, user data and signaling information in the GPRS backbone network are conveyed in clear-text exposing them to various security threats. In addition, inter-network communications (between different operators) are based on the public Internet, which enables IP spoofing to any malicious third party who gets access to it. In the sequel, the security measures applied to the GPRS backbone network are presented.

The responsibility for security protection of the GPRS backbone as well as inter-network communications belongs to mobile operators. An operator utilizes private IP addressing and Network Address Translation (NAT) [11] to restrict unauthorized access to the GPRS backbone. He may also apply firewalls at the borders of the GPRS backbone network in order to protect it from unauthorized penetrations. Firewalls protect the network by enforcing security policies (e.g., user traffic addressed to a network element is discard). Using security policies the GPRS operator may ensure that only traffic initiated from the MS and not from the Internet should pass through a firewall. This is done for two reasons: (a) to restrict traffic in order to protect the MS and the network elements from external attacks; and (b) to protect the MS from receiving un-requested traffic. Un-requested traffic may be unwanted for mobile subscribers since they pay for the traffic received as well. The GPRS operator may also want to disallow some bandwidth demanding protocols preventing a group of subscribers to consume so much bandwidth that other subscribers are noticeably affected. In addition, application level firewalls prevent direct access through the use of proxies for services, which analyze application commands, perform authentication and keep logs.

Since firewalls do not provide privacy and confidentiality, the Virtual Private Network (VPN) technology [11] has to complement them to protect data in transit. A VPN is used for the authentication and the authorization of user access to corporate resources, the establishment of secure tunnels between the communicating parties, and the encapsulation and protection of the data transmitted by the network. In current GPRS implementations, preconfigured, static VPNs can be employed to protect data transfer between GPRS network elements (e.g., an SGSN and a GGSN that belong to the same backbone), between different GPRS backbone networks that belong to different mobile operators, or between a GPRS

backbone and a remote corporate private network. The border gateway, which resides at the border of the GPRS backbone, is a network element that provides firewall capabilities and also maintains static, pre-configured VPNs to specific peers.

4 Attacks on GPRS Security

Although GPRS supports a set of security measures that attempts protects it, these measures present some essential security weaknesses and they do not adequately protect certain parts of the GPRS architecture. These facts may lead to the realization of attacks that threaten the GPRS mobile users, the GPRS network and the data that either reside at the network or are transferred through it. Based on the architecture of GPRS and the employed security measures, there are five critical areas where the GPRS security is exposed and security attacks may be carried out [12] (see Figure 5):

- The mobile station and the SIM-card (I).
- The interface between the MS and the SGSN (II).
- The GPRS backbone network (III).
- The packet network that connects different operators (IV).
- The public Internet (V).

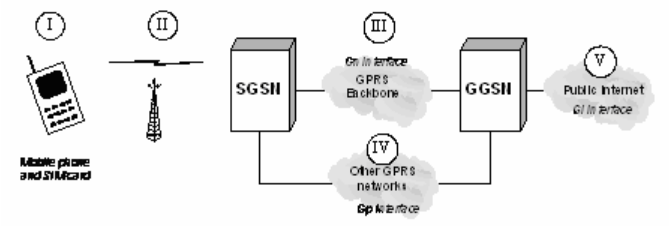

Figure 5: Points of attacks in the GPRS architecture [12]

In the following, the above-mentioned vulnerable areas of the GPRS network architecture are analyzed, and the potential attacks that may be carried out in each area are elaborated.

4.1 Mobile Station and SIM

MSs mostly operate in public places such as market-places, stations, etc., where the concentration of people is high and physical access controls are omitted. These facts increase the risks associated with the MS usage and enable adversaries to perform various attacks. However, not only the MS but also the SIM module can be targeted by adversaries. Since the SIM module

is implemented on a smart card, any vulnerability of smart cards, immediately, affects on the security of the information stored in the SIM (e.g., IMSI and Ki). In the following, the most prominent security attacks that may be performed against a GPRS MS and the included SIM card are presented and analyzed.

4.1.1 Attacks on the mobile terminal

GPRS terminals may deal with some of the same security threats that normal computers, which are connected to the public Internet, encounter. They are threatened by rogue code such as viruses, Trojan horses, worms, etc., since they are always on and are possibly equipped with well-known software like Internet browsers and email applications. Intruders to MSs may modify, insert, or delete application or data stored in them. In addition, the use of smart applications and software, which allow computer code to be downloaded to and executed on mobile terminals, might cause several security attacks. The results of these attacks on a GPRS MS may be the monitoring of the MS usage, the downloading of unwanted files, the realization of unwanted session calls, etc., which annoy the end-user and possibly hinder the execution of requested services [17].

4.1.2 Attacks on the SIM-card

The security model of GPRS is primary based on the secret key, Ki, which is stored in the SIM-card of the MS. If an attacker is able to retrieve this key, he can intercept data conveyed between the MS and the SGSN, or he can produce a clone of the original SIM card, and, thus, engage in transactions, which are billed to the original subscriber.

As mentioned previously (see sect. 3.3), for the implementation of A3 and A8 the COMP128 algorithm may be used. Although never officially published, COPM128 description was found and crypto-analyzed allowing an attacker to find the shared key (Ki) of the MS and the network. The attack is achieved by sending a set of chosen challenges (aprox. 115000) to the SIM-card and analyzing the responses. This attack exploits the lack of diffusion, since there is a narrow pipe inside COMP128. Specifically, after the second round (compression and substitution) of the first iterative loop the bytes X[i], X[i+8], X[i+16], X[i+24] depend only on the input bytes i, i+8, i+16, i+24. Two of these bytes are key bytes, namely X[i]=Ki[i] and X[i+8]=Ki[i+8] (for every i from 0 to 7). Therefore, performing a chosen challenge attack, it is possible to find a collision on the four bytes after the second round. Once a collision occurs on the second round, it propagates right through the hash function until the end of the last round. Comparing the MACs that are sent back by the SIM-card, this collision can be recognized. Then, performing a 2R-attack (term of differential crypto-analysis) the two bytes of the secret key involved in the collision are recovered. This attack can be iterated

for each pair of key bytes (i.e., for i from 0 to 7), and, thus, the whole secret key Ki can be recovered. Recently, this attack has been optimized by pre-computing all collisions and finding the challenges that collide more. By doing this, the attacker manage to reduce significantly the number of required challenges (i.e., from 115000 to 20000) and the relative time [13] [14] [15] [16].

Another type of attacks against the SIM-cards of GSM/GPRS is side-channel attacks [18]. These attacks allow an adversary to obtain sensitive information from side-channels (such as timing of operations, power consumption, electromagnetic emanations, etc.,) of cryptographic implementations, mainly, in constrained devices such as the SIM-cards. In view of these exposures, some vendors of cryptographic systems employ a variety of software and hardware countermeasures to "harden" their implementations against side-channel attacks [18]. However, many of these measures are inadequate in cases that an algorithm implementation employs large table lookups. The COMP128 algorithm, which is used for the implementation of A3 and A8 in the SIM-cards of GSM/GPRS, requires the lookup of large tables. This lookup on simple devices, such as the SIM-cards, can only be achieved in a complicated way resulting in the leakage of sensitive information into the side channels (i.e., the COMP128 algorithm requires lookup of five tables with size 512, 256, 128, 64 and 32 bytes each).

An improved class of side-channel attacks, which can be used to attack implementations that may otherwise resist some side-channel attacks, is called partitioning attacks [18]. The partitioning attack on COMP128 exploits weaknesses and vulnerabilities in the implementation of table lookups, which introduce non-linearity, in a very effective way. Specifically, the entire 128-bit key (Ki) can be recovered from a SIM card using less than 1000 invocations with random inputs, or 255 chosen inputs, or only 8 adaptively chosen inputs. Thus, an adversary who possesses a SIM card for a minute can easily extract the key. In contrast, the previously best technique to attack GSM/GPRS SIM-cards was to employ a cryptanalytic attack on the COMP128 algorithm using a set of 20.000 to 115.000 chosen inputs.

A peculiar attack on smart cards, which is called optical fault induction, has been revealed by Skorobogatov and Anderson [20]. They exposed to light the microprocessor circuit, embedded in a smart card, by scraping most of the protective coating from its surface. By focusing the light (flash) on individual transistors within the chip, and by sequentially changing the values of the transistors used to store data, they were able to reverse engineer the memory address map, which allows them to extract the secret data from the smart card. The authors also asserted that they have developed a technology to block these attacks.

4.2 Access network

The interface between the MS and the SGSN is amongst the most exposed elements of the GPRS architecture. As mentioned previously, the GPRS system protects this part of the network by employing a set of security mechanisms that ensure authentication of mobile users, confidentiality of users identity, and ciphering of users data and signalling information exchanged through it. However, exploiting some weaknesses that these mechanisms present, an adversary may perform the following attacks, which may result in the system breakdown or the compromise of end-user security.

4.2.1 Denial of Service attack

A common attack on the wireless interface of mobile/wireless networks is the denial of service. This attack aims at preventing transmission of user data, and signaling and control information over the air interface, disrupting communication and network operation. It can be achieved by malicious third parties who: (i) jam user data and signaling traffic using special devices called jammers; (ii) induce specific protocol failures (i.e., violate protocol integrity by changing protocol status, flags, etc.); or (iii) masquerade as network elements and then prevent data traffic (user, signaling or control) from being transmitted.

4.2.2 Man-in-the-Middle attack

GPRS is vulnerable to a man-in-the-middle attack, which allows an attacker to impersonate a false base station to a victim MS and, at the same time, impersonate the victim to a real network. It is assumed that the attacker has a devise capable of emulating a base station, which is integrated with a MS with a valid GPRS network subscription (see Figure 6). This attack is feasible because the MS is authenticated to the network, but the network is not authenticated to the MS. In order to mount this attack, the attacker forces the MS to connect to a false base station by broadcasting the network code of the subscriber's home network in best signal quality. Then, the false base station impersonates the MS to the GPRS network. In the subsequent authentication process, the attacker can either simply forward the authentication traffic between the MS and the real network, or he can be authenticated to the network using his own subscription discarding the MS authentication data.

Since the encryption between the MS and the network (SGSN) is not mandatory and the related signaling data are exchanged unencrypted without origin authentication, the attacker can request to turn off the encryption between the MS and the false base station. Additionally, if the attacker chooses not to be authenticated to the network, he can disable the encryption between the false base station (him) and the network by sending false information about his encryption capabilities (his device) to the network. Thus, the attacker mediates in the

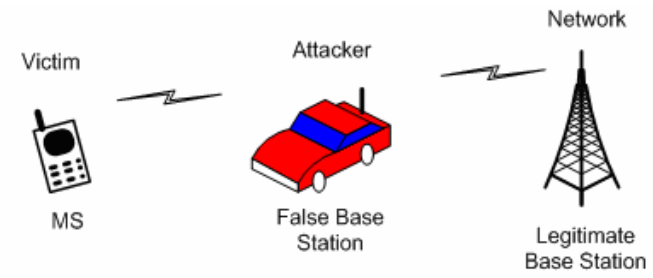

Figure 6: Man-in-the-middle attack

communication between the MS and the network allowing him to eavesdrop on, insert, and modify traffic. In case that the attacker has been authenticated to the network using his own subscription, he pays the transaction. Otherwise, the transaction is paid by the victim MS.

Besides the deactivation of the encryption process over the air interface, the man-in-the-middle attack may result in the retrieval of the encryption key used. In this form of the attack, the attacker listens to the GPRS-RAND sent by the network to the MS under attack for authentication purposes. Then, the attacker impersonates a voice network that initiates a radio session with the MS, and starts the authentication procedure using the GPRS-RAND value that he intercepted (as a GSM-voice RAND). After authentication completion, the attacker asks from the MS to start encrypting with A5/2, which is a weak version of the A5 algorithm that is widely used. By receiving a few milliseconds of encrypted voice traffic (4 frames), the attacker is able to recover the corresponding encryption key, Kc, (by performing the cipher-text-only attack [13] within less than a second, and ends the voice-session. Since the retrieved Kc equals to the GPRS-Kc, the attacker is able to decrypt the GPRS traffic exchanged between the MS under attack and the legitimate network. Alternatively, the attacker can record this traffic, and performs the impersonation attack in order to retrieve the GPRS-Kc with which the recorded data can be decrypted, at any later time. In case that A5/2 is not supported by the MS, but A5/1 is supported (a stronger version of A5), then, the aforementioned attack against A5/1 and GPRS can be performed using the (more complex) cryptanalysis of A5/1, instead of A5/2 [20]. Since many network operators initiate a new authentication process, rarely, and use the key created in the last authentication, the attacker can use the retrieved key to intercept more than one session between the MS and the GPRS network.

4.3 Attacks on the GPRS core network

The GPRS backbone network, which connects the fixed nodes of the GPRS architecture, is also threatened by malicious actions. These actions refer to both IP and SS7 technologies that are employed to convey user data and signalling information in the GPRS backbone. In the following, the security attacks against the GPRS backbone classified by the transmission

technology used (IP and SS7) are presented and analyzed.

4.3.1 Attacks on the IP technology (Gn Interface)

The IP technology is used to connect the SGSN and the GGSN of the same network operator (Gn interface). This connection may be built on the top of an already existing IP network, which is not dedicated to the GPRS traffic. Therefore, traffic that originates from outside of the GPRS network shares the GPRS backbone links with the GPRS traffic. The latter is conveyed in clear-text in the GPRS backbone since the GTP protocol, which is employed for both signaling and user data, does not support any security measure. The above situation might cause performance problems to the GPRS backbone (i.e., network overload) and expose the GPRS traffic to security threats (e.g., denial of service attacks, IP spoofing, compromise of confidentiality and privacy etc.) that the public Internet encounters. Therefore, the Gn Interface is vulnerable to attacks that can potentially lead to network downtime, loss of service, revenue loss and disgruntle customers. In the following, the most prominent security attacks that may be carried out against this part of the GPRS backbone network are presented.

Since the IP network that is used as a basis for the GPRS backbone is not dedicated to it, a malicious third party may masquerade as a legitimate part of the GPRS network by spoofing the address of a GPRS network component (e.g., GGSN or SGSN). Once the malicious party establishes himself as a legitimate network element, he is able to perform various actions that are detrimental to the mobile subscribers and the network operator. By executing commands that normally a legitimate network component does, the attack remains undetected until its results are noticeable. One of these attacks is related to the GTP protocol, and more specifically to the exploitation of the GTP commands like PDP context create, PDP context delete, PDP context update, etc. [4]. The attacker, who has access to the GPRS backbone network, is able to get information regarding the GTP tunneling by simply monitoring the GTP traffic, which is unencrypted. Without encryption, data carried by the GTP protocol can either be read or manipulated. Possessing the appropriate information, the attacker may create and forward to the GGSN of the network PDP context create, delete and update commands. These commands overload the GGSN under attack and change the servicing contexts of the mobile users that are currently served by the network, resulting in denial of service.

In addition to malicious third parties that get access to the GPRS backbone network, the mobile users (legitimate or not) may represent a threat to it. Since the MSs are behind the firewall, which is located between the GGSN and the public Internet, they may get access to the network elements of the GPRS backbone (i.e., SGSN, GGSN, DNS servers, O&M workstations, etc.). Having access to these elements, a malicious MS may perform various attacks such as denial of service, IP spoofing, compromise of confidentiality and privacy, etc. In addition, once

the malicious MS gets access to the GPRS network, it may send massive amounts of data to unsuspecting users. Since the GPRS is a usage-based service, the mobile users under attack are over billed for content that they did not request for. Such an attack would be even more harmful than spam is for email, as it becomes much more than an annoyance.

Finally, a malicious MS in cooperation with a malicious server, which is located outside of the GPRS network, may also perform an over billing attack to a legitimate mobile subscriber. The malicious MS may hijack the IP address of the legitimate MS, and invokes a download from the malicious server. Once the downloading begins, the malicious MS exits the session. The legitimate MS (MS under attack) receives and gets charged for traffic that never requests for. The malicious parties could also execute this attack by sending broadcasts of unsolicited data to legitimate mobile subscribers. The result is still the same: the subscribers are billed for data that they did not solicited and might not have wanted.

4.3.2 Attacks on the SS7 tehcnology

If an attacker gets access to the GPRS backbone, he may also gain access to the signaling part of the network, and consequently to the network components that are connected through it, such as the AuC, the HLR, the VLR, etc. Having access to the signaling part of the network, the attacker is able to listen to critical information for the mobile subscribers and the network operation such as the permanent identities of mobile users (IMSI), temporary identities (TMSI, TLLI), location information, authentication triplets (RAND, SRES, Kc), charging and billing data, etc. This is feasible because the signaling network (SS7), used in GSM/GPRS, does not support security measures. Except for listening to the critical information exchanged, the attacker may either perform denial of service attacks to the GPRS signaling components or try to retrieve the sensitive information that they hold. For example, the AuC contains authentication information of the subscribed home users. A similar attack to that performed to retrieve the Ki from a SIM-card can also be carried out to retrieve the Ki from the AuC. The AuC has to answer to a request made by a GPRS network component and returns valid triples to be used in the authentication procedure of the involved MS. Thus, exploiting the absence of authentication and integrity protection mechanisms in SS7, a malicious party may masquerade as a network element and retrieve critical information that should be kept confidential.

4.4 Attacks on the interface between network operators (Gp Interface)

The Gp Interface (see Figure 5), which provides connectivity between GPRS networks that belong to different operators, is also vulnerable to malicious actions. This interface supports users roaming and conveys: (a) GTP traffic between a local network and the home network of a roaming user; (b) roaming information between a GPRS network and a GPRS Routing

Exchange (GRX) operator, which provides roaming services to cooperating networks; and (c) Domain Name Server (DNS) information. The security threats to the Gp interface mainly concern with the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred. A vital security issue of the Gp interface is the lack of security measures in the GTP protocol. In the following, the most important security attacks that target the Gp interface are presented and analyzed.

Trust and reliability between the cooperating GPRS network operators influence the level of security that each operator supports. A malicious operator has the ability to generate a sufficient amount of traffic (either IP or GTP) directed at the border gateway, the SGSN or the GGSN of an operator under attack. In this way, the GPRS nodes are flooded with useless and unwanted traffic that consumes the majority of processing and communication resources. This may result in preventing subscribers from being able to roam, to be attached to the GPRS network, to forward data to external networks (i.e., Internet), etc. In addition, the attacker (the malicious operator) might perform attacks that target the GTP protocol, such as deleting or updating PDP contexts. These actions remove or modify the GTP tunnels between the SGSN and the GGSN (of an operator under attack) that are used for user data transfer, and, thus, denying users service.

Since the GTP protocol provides no authentication for SGSNs and GGSNs, a malicious operator or an attacker with access to the Gp Interface may create a bogus SGSN. Using information regarding users subscription, which can be captured from the GTP traffic (GTP messages are conveyed unencrypted), the bogus SGSN may create GTP tunnels between itself and a legitimate GGSN. After the establishment of such tunnels, the network, where the legitimate GGSN belongs to, provides unauthorized Internet access to the attacker and, possibly, access to cooperating networks. In addition, the bogus SGSN may send Update PDP context request messages to a legitimate SGSN, which is handling the GTP sessions of a mobile subscriber. In this way, the bogus SGSN takes the responsibility for handling the GTP sessions of the user. Thus, the attacker may intercept the user data exchanged by the sessions, compromising end-user security.

4.5 Attacks on the interface to the public Internet (Gi Interface)

The network of a GPRS operator is not only threatened by attacks that originate from inside of it and the networks of cooperating operators, but also from outside of them. The Gi interface (see Figure 5) connects the GPRS network to the public Internet and service providers that provide services to mobile subscribers. Since the applications of mobile subscribers can be whatever is carried by the Internet technology, the Gi interface may carry any type of traffic.

This fact exposes the GPRS network elements and the mobile subscribers to a variety of threats that the public Internet encounters, such as viruses, Trojan horses, worms, and other malicious network traffic [19]. A Trojan horse is a malicious piece of software hidden in a program that performs normal tasks. When started, this program behaves as expected by the user and, then, stealthily executes the Trojan horse payload. On the other hand, worms are self-propagating pieces of malicious software. They propagate from one computer/device to another via a network link. The first worms for mobile terminals and smart phones have been showed-up targeting Symbian terminals and propagating itself via Bluetooth links [17]. The ultimate goal of a Trojan horse or a worm usually is a denial of service attack.

Denial of service attacks represent the largest threat to the Gi interface. Attackers may be able to flood the links that connect the GPRS network to external packet data networks with useless traffic, thereby, prohibiting legitimate traffic to pass. The flood traffic might target to the MSs or the network elements causing availability problems to the followed network paths and the involved components.

Apart from harm to the network availability, the GPRS data are conveyed unprotected over the public Internet enabling anyone to read and/or manipulate them, and, thus, compromising user data confidentiality and integrity. In addition, an adversary may exploit the unprotected user related information causing huge bills to the GPRS users. This is feasible because the GPRS billing system is based on the amount of traffic transmitted and received. The over billing attack can be achieved by sending large emails from a malicious external network to the MSs, or by creating viruses that are transferred to the MSs. A virus may have the property to send dummy packets from the infected MS to a malicious server, without any notice to the user.

5 Security measures

The analyzed attacks against the GPRS network increase the risks associated with the usage of such networks influencing their deployment, which realizes the mobile Internet. In order to defeat some of these risks, a set of security improvements to the existing GPRS security architecture may be incorporated. Additionally, some complementary security measures, which have been originally designed for fixed network and aim at enhancing the level of security that GPRS supports may be applied. In the following, the specific security improvements and the application of the complementary security measures are briefly presented and analyzed.

5.1 SIM-card

The majority of the attacks that are related to a MS and the SIM-card of a mobile user has to do with the vulnerabilities of COMP128. To address these, the old version of COMP128 (currently

named as COMP128-1) is replaced by two newer versions COMP128-2 and COMP128-3, which defeat the known weaknesses. There is an even newer version COMP128-4, which is based on the 3GPP algorithm MILENAGE that uses Advanced Encryption Standard (AES). In addition, it is mentioned to the GPRS operators that the COMP128 algorithm is only an example algorithm, and that every operator should use its own algorithm in order to support an acceptable level of security.

The partitioning attacks, which also target COMP128 implementations on SIM-cards, can be defeated too. IBM Research has developed a technique to protect table lookup operations from side channel attacks [18]. In this technique, a table lookup operation consults a table in computer memory to retrieve a value stored in a particular location. Thus, it replaces a single table lookup operation, which leaks information on the retrieved value in the side channel, with a sequence of table lookups at completely random locations, which leaks no information.

5.2 User data

User data conveyed over the GPRS backbone and the public Internet most likely remain unprotected (except for the cases that the operator supports pre-established VPNs over the public Internet), and, thus, are exposed to various threats. The level of protection that GPRS provides to the data exchanged can be improved by employing two security technologies: (a) the application of end-user security, and (b) the establishment of mobile IPsec-based VPN, dynamically. End-user security is applied by using application layer solutions such as the Secure Sockets Layer protocol (SSL) [24]. SSL is the default Internet security protocol that provides point-to-point security by establishing a secure channel on top of TCP. It supports server authentication using certificates, data confidentiality and message integrity. On the other hand, IPsec protects traffic on a per connection basis, and, thus, is independent from the applications that run above it. An IPsec-based VPN is used for the authentication and the authorization of user access to corporate resources, the establishment of secure tunnels between the communicating parties and the encapsulation and protection of the data transmitted by the network. On demand VPNs that are tailored to specific security needs are especially useful for GPRS users, which require any-to-any connectivity in an ad hoc fashion. Regarding to the deployment of mobile VPNs over the GPRS infrastructure, three alternative security schemes have been proposed: (a) the end-to-end [25], (b) the network-wide [27], and (c) the border-based [26]. These schemes mainly differ in the position where the security functionality is placed within the GPRS network architecture (MS, SGSN, and GGSN), and whether data in transit are ever in clear-text or available to be tapped by outsiders.

5.3 Signaling plane of the GPRS backbone

The lack of security measures in the signaling plane of the GPRS backbone gives the opportunity to an adversary to retrieve critical information such as the permanent identities of mobile users (IMSI), temporary identities (TMSI, TLLI), location information, authentication triplets (RAND, SRES, Kc), charging and billing data, etc. The possession of this information enables an attacker to identify a mobile user, to track his location, to decipher the user data transferred over the radio interface, to over bill him, etc. To address this inability of GPRS, we propose the incorporation of the Network Domain Security (NDS) features [21] into the GPRS security architecture. NDS features, which have been designed for the latter version of UMTS, ensure that signaling exchanges in the backbone network, as well as in the whole wireline network are protected. For signaling transmission in GPRS the SS7 and IP protocol architectures are employed, which incorporate the Mobile Application Part (MAP) [9] and the GTP protocol [4], respectively. In NDS both architectures are designed to be protected by standard procedures based on existing cryptographic techniques. Specifically, the IP-based signaling communications will be protected at the network level by means of the well-known IPsec suite [23]. On the other hand, the realization of protection for the SS7-based communications will be accomplished at the application layer by employing specific security protocols [22]. However, until now only the MAP protocol from the SS7 architecture is design to be protected by a new security protocol named MAPsec [24]. To address the increasing security needs, this effort has to be continued to cover the entire set of the SS7 protocol stack.

5.4 Gp and Gi Interfaces

The Gp and the Gi interfaces of GPRS are subject to malicious actions that target the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred. In the Gp interface, some of the previously mentioned security concerns can be addressed by implementing pre-configured VPNs (IPsec tunnels) between roaming partners. Only GTP and DNS traffic that originate from authorized parties should be allowed over these tunnels, and, thus, should be entered to the network. In addition to IPsec tunnels, the establishment of firewalls at the Gp interface protects the system against intruders, malicious traffic, denial of service attacks, etc. Firewalls provide packet filtering and stateful inspection to the information exchanged (both incoming and outgoing) through the Gp interface. These functions allow traffic that originates from or destined to authorized network operators, which have signed roaming agreement. Moreover, they discard GTP packets that are malformed, have illegal headers, or are not of the state. Thereby, firewalls protect the GPRS network from processing illegal or malformed traffic, being a target of some kind of denial of service attacks, or being used as a source to attack other

roaming partners.

Likewise the Gp Interface, the Gi interface and the data transferred through it can be protected by employing pre-configured VPNs and establishing firewalls at the border of the GPRS backbone. Firewalls at this point should incorporate a GPRS-based security policy that allows only a MS to initiate a connection to a public networks and implements stateful packet filtering so that a MS never receives traffic that is initiated from a public network. If required, trusted application servers have to be implemented, which are permitted by the policy to push public network services to MSs.

6 Conclusions

This paper has presented the security attacks, which threaten the GPRS mobile users, the GPRS network, and the data that either reside at the network or are transferred through it. The possible attacks against GPRS targets the equipment of mobile users, the radio access network, the GPRS backbone network, and the interfaces that connect the latter to other GPRS networks or the public Internet. More specifically, the MS may deal with some of the same security threats that a normal computer, which is connected to a network (e.g., the Internet), encounters. The results of these attacks may be the monitoring of the MS usage, the downloading of unwanted files, the realization of unwanted session calls, etc. However, not only the MS but also the SIM-card can be targeted, maliciously, resulting in the disclosure of the secret key, Ki. Possessing this key an adversary can intercept data conveyed between the MS and the SGSN, or he can produce a clone of the original SIM card, and, thus, engage in transactions, which are billed to the original subscriber.

The interface between the MS and the SGSN is amongst the most exposed elements of the GPRS architecture. Exploiting some weaknesses that the GPRS security architecture presents, an adversary may perform denial of service and man-in-the-middle attacks, which may result in the system breakdown and the compromise of end-users security. The same results derive from attacks that target the GPRS backbone network. These attacks target both IP and SS7 technologies that are employed to convey user data and signaling information in the GPRS backbone network. However, the network of a GPRS operator is not only threatened by attacks that originate from inside of it, but also from outside. The results of external attacks mainly concern with the availability of resources and services, the authentication and authorization of users and actions, and the integrity and confidentiality of the data transferred.

The analyzed attacks and their consequences increase the risks associated with the usage of GPRS, and, thus, influence its deployment that realizes the concept mobile Internet. In order to defeat certain attacks and enhance the level of security provided by GPRS, specific security measures have been proposed.

References

[1] 3GPP TS 03.6 (V7.9.0), "GPRS Service Description, Stage 2", Sept. 2002.

[2] P. Pagliusi, "A Contemporary Foreword on GSM Security", Proc. Infrastructure Security International Conference (InfraSec 2002), LNCS 2437, Springer-Verlag, 2002, pp. 129-144.

[3] C. Mitchell, "The security of the GSM air Interface protocol", Technical Report, Royal Holloway University of London, Aug. 2001, `http://www.ma.rhul.ac.uk/techreports/`

[4] 3GPP TS 09.60 (V7.10.0), "GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface", Dec. 2002.

[5] GSM 03.20, "Security Related Network Functions", Nov. 1999.

[6] ETSI TS 100 922 (v7.1.1), "Subscriber Identity Modules (SIM) Functional characteristics", July 1999.

[7] 3GPP TS 03.03 (v7.8.0), "Numbering, addressing and identification", Sept. 2003.

[8] 3GPP TS 01.61 (v7.0.0), "GPRS ciphering algorithm requirements", Sept. 2001.

[9] 3GPP TS 09.02 (v7.15.0) "Mobile Application Part (MAP) specification", March 2004.

[10] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, Aug. 1999.

[11] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, Feb. 2000.

[12] G. S. Bjaen, E. Kaasin "Security in GPRS", Master Thesis, Agder University College, Norway, May 2001, `http://student.grm.hia.no/master/ikt01/ikt6400/ekaasin/Master%20Thesis%20Web.htm`

[13] E. Barkan, E. Biham, N. Neller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", in Proc. Advances in Cryptology (CRYPTO 2003), LNCS 2729, Springer-Verlag, Aug. 2003, pp. 600 - 616.

[14] D. Hulton, "Smart Card Security: From GSM to Parking Meters", `http://dachb0den.com`

[15] M. Briceno, I. Goldberg, D. Wagner, "GSM Cloning",`http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html`

[16] H. Handschuh, P. Paillier, "Reducing the Collision Probability of Alleged Comp128," Proc. of the International Conference on Smart Card Research and Applications, LNCS 1820, Springer-Verlag, 2000, pp. 366-371.

[17] F-Secure Virus Description:http://www.f-secure.com/v-descs/

[18] J. Rao, P. Rohatgi, H. Scherzer, S. Tinguely, "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards," in Proc. IEEE Symposium on Security and Privacy, Oakland, California, USA, May 2002.

[19] A. Nikishin, "Malicious software - past, present and future", Information Security Technical Report, Vol.9, No.2, April 2004, pp. 6-18.

[20] S. Skorobogatov, R. Anderson, "Optical Fault Induction Attacks," Proc. of CHES '02, LNCS 2523, Springer, 2002, pp. 2-12. http://www.cl.cam.ac.uk/~sps32/ches02-optofault.pdf

[21] P. Ekdahl, T. Johansson, "Another attack on A5/1", IEEE Transactions on Information Theory Vol. 49, No. 1, pp. 284-289, 2003.

[22] C. Xenakis and L. Merakos, "Security in third Generation Mobile Networks", Computer Communications, Vol. 27, No. 7, May 2004, pp. 638-650.

[23] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Nov. 1998.

[24] 3GPP TS 33.200 (v4.3.0) "3G Security; Network Domain Security; MAP application layer security", March 2002.

[25] V. Gupta and S. Gupta, "Securing the Wireless Internet," IEEE Communications Magazine, Vol. 39, No. 12, Dec. 2001, pp. 68-74.

[26] C. Xenakis, E. Gazis, L. Merakos, "Secure VPN Deployment in GPRS Mobile Network", Proc. European Wireless 2002, Florence Italy, Feb. 2002, pp. 293-300.

[27] C. Xenakis, L. Merakos, "Dynamic Network-based Secure VPN Deployment in GPRS", Proc. PIMRC 2002, Lisboa, Portugal, Sept. 2002, pp. 1260-1266.

[28] C. Xenakis, L. Merakos, "On Demand Network-wide VPN Deployment in GPRS", IEEE Network, Vol. 16, No. 6, Nov/Dec. 2002, pp. 28-37.