Security Measures and Weaknesses of the GPRS Security Architecture

Christos Xenakis
Security Group, Communication Networks Laboratory, Department of Informatics & Telecommunications
University of Athens, 15784 Athens, Greece (Email: xenakis@di.uoa.gr)

(Received Jan. 19, 2006; revised and accepted May 7, 2006 & Nov. 8, 2006)

Abstract

This paper presents an evaluation of the security architecture employed in the General Packet Radio Services (GPRS). More specifically, the security measures applied to protect the mobile users, the radio access network, the fixed part of the network, and the related data of GPRS are presented and analyzed in details. This analysis reveals the security weaknesses of the applied measures that may lead to the realization of security attacks by adversaries. These attacks threaten network operations and data transfer through it compromising end-users and network security. To address some of the identified security weaknesses, a set of security enhancements that aims at improving the GPRS security architecture and providing advanced security services to user data traffic is proposed. The proposed enhancements can be easily integrated in the existing GPRS technology, minimizing the required changes.

Keywords: GPRS, mobile internet, mobile VPN, security

1 Introduction

The General Packet Radio Services (GPRS) [3] is a service that provides packet radio access for Global System for Mobile Communications (GSM) users. The GPRS network architecture, which constitutes a migration step toward third-generation (3G) communication systems, consists of an overlay network onto the GSM network. In the wireless part, the GPRS technology reserves radio resources only when there is data to be sent, thus, ensuring the optimized utilization of radio resources. The fixed part of the network employs the IP technology and is connected to the public Internet. Taking advantage of these features, GPRS 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 the new emerging applications and services over GPRS, security is considered as a vital factor. This is because of the fact that wireless access is inherently less secure, and the radio transmission is by nature more susceptible to eavesdropping and fraud in use than wireline transmission. In addition, users mobility and the universal access to the network imply higher security risks compared to those encountered in fixed networks. 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 mainly based on the security measures applied in GSM, since the GPRS system is built on the GSM infrastructure.

Based on the above consideration, the majority of the existing literature on security in second-generation (2G) mobile systems refers to GSM [15, 16], which is considered that also covers GPRS. However, GPRS differs from GSM in certain operational and service points, which require a different security analysis. This is because GPRS is based on IP, which is an open and wide deployed technology that presents many vulnerable points. 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. Thus, the GPRS system is more exposed to intruders compared to GSM.

This paper presents an evaluation of the security architecture employed in GPRS. More specifically, the security measures applied to protect the mobile users, the radio access network, the fixed part of the network, and the related data of GPRS are presented and analyzed in details. This analysis reveals the security weaknesses of the applied measures that may lead to the realization of security attacks by adversaries. These attacks threaten network operation and data transfer through it, compromising end-users and network security. To address some of the identified security weaknesses, a set of security enhancements that aims at improving the GPRS security architecture and providing advanced security services to user data traffic is proposed. The proposed enhancements can be easily integrated in the existing GPRS technology, minimizing the required changes.

The rest of this article is organized as follows. Section 2 describes briefly the GPRS network architecture. Section 3 presents the security architecture applied to GPRS,

and section 4 analyzes its security weaknesses. Section 5 proposes some enhancements that improve the level of security provided by GPRS. Finally, section 6 contains the conclusions.

2 GPRS Network

The network architecture of GPRS [3] 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) [3].

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 Tunnelling Protocol (GTP) [5].

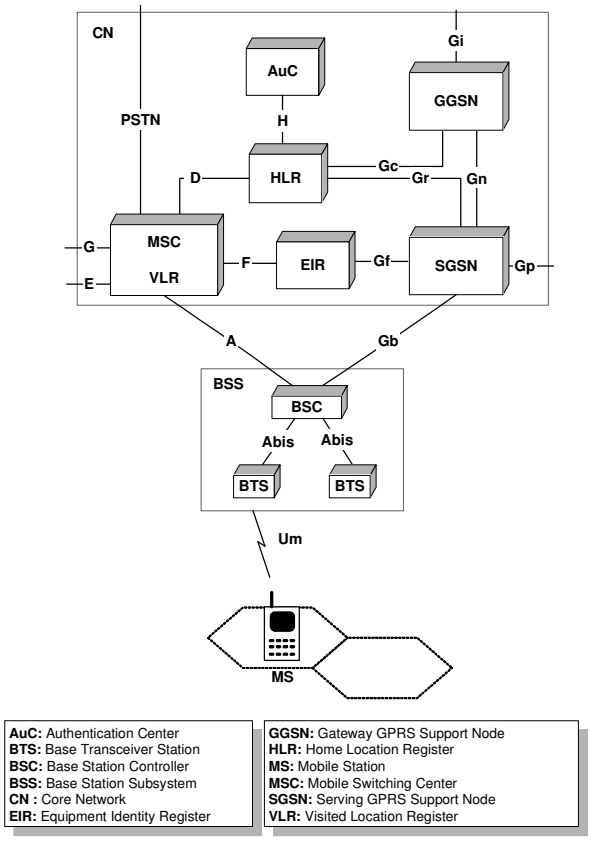

Figure 1: GPRS network architecture

3 GPRS Security Architecture

In order to meet security objectives, GPRS employs a set of security mechanisms that constitutes 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 [11]:

- 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) [8]. 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) [2];
- A secret key, Ki, (128 bit) that is used for authentication;
- An authentication algorithm (A3) and an algorithm that generates encryption keys (A8) [11].

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

The 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.

The subscriber identity confidentiality is mainly achieved by using a Temporary Mobile subscriber Identity (TMSI) [2, 11], 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) [2] 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 [3] 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.

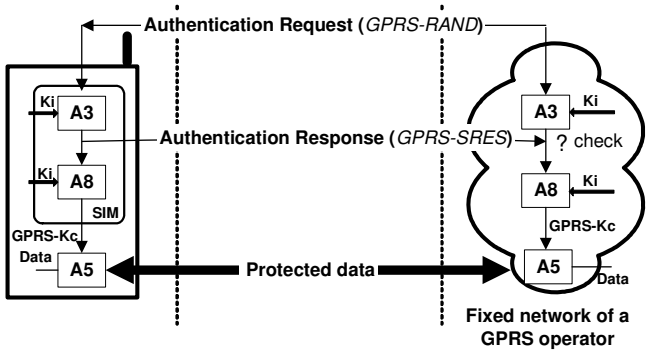

Figure 2: GPRS authentication

To achieve authentication of a mobile user, the serving 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).

3.4 Data and Signalling Protection

User data and signaling protection over the GPRS radio access network is based on the GPRS ciphering algorithm (GPRS-A5) [1], which is also referred to as GPRS En-

cryption 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 serving SGSN performs the ciphering/deciphering functionality protecting signaling and user data over the Um, Abis, and Gb interfaces.

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 3) 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 the IOV (input offset value). The 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.

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

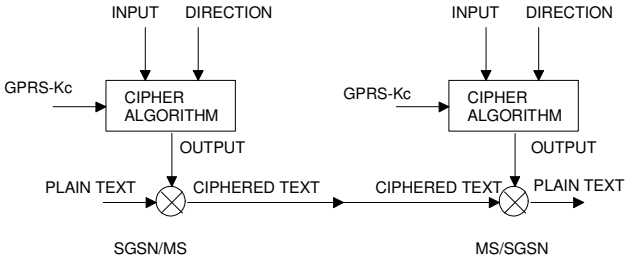

Figure 3: GPRS ciphering

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 [4], 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. They utilize private IP addressing and Network Address Translation (NAT) [17] to restrict unauthorized access to the GPRS backbone. They 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 the 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 [9] 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, pre-configured, 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 GPRS Security Weaknesses

Although GPRS have been designed with security in mind, it presents some essential security weaknesses, which may lead to the realization of security attacks that threaten network operation and data transfer through it. In the following, the most prominent security weaknesses of the GPRS security architecture are briefly presented and analyzed.

4.1 Subscriber Identity Confidentiality

A serious weakness of the GPRS security architecture is related to the compromise of the confidentiality of subscriber identity. Specifically, whenever the serving network (VLR or SGSN) cannot associate the TMSI with the IMSI, because of TMSI corruption or database failure, the SGSN should request the MS to identify itself by means of IMSI on the radio path. Furthermore, when the user roams and the new serving network cannot contact the previous (the old serving network) or cannot retrieve the user identity, then, the new serving network should also request the MS to identify itself by means of IMSI on the radio path. This fact may lead an active attacker to pretend to be a new serving network, to which the user has to reveal his permanent identity. In addition, in both cases the IMSI that represents the permanent user identity is conveyed in clear-text over the radio interface violating user identity confidentiality.

4.2 Subscriber Authentication

The authentication mechanism used in GPRS also exhibits some weak points regarding security. More specifically, the authentication procedure is one-way, and, thus, it does not assure that a mobile user is connected to an authentic serving network. This fact enables active attacks using a false base station identity. An adversary, who has the required equipment, may masquerade as a legitimate network element mediating in the communication between the MS and the authentic base station. This is also facilitated by the absence of a data integrity mechanism on the radio access network of GPRS, which defeats certain network impersonation attacks. The results of this mediation may be the alternation or the interception of signaling information and communication data exchanged.

Another weakness of the GPRS authentication procedure is related to the implementation of the A3 and A8 algorithms, which are often realized in practise using COMP128. COMP128 is a keyed hash function, which uses two 16-byte (128 bits) inputs and produces a hash output of 12 bytes (96 bits). While the actual specification of COMP128 was never made public, the algorithm has been reverse engineered and cryptanalyzed [7]. Thus, knowing the secret key, Ki, it is feasible for a third party to clone a GSM/GPRS SIM-card, since its specifications are widely available [8].

The last weakness of the GPRS authentication procedure is related to the network ability of re-using authentication triplets. Each authentication triplet should be used only in one authentication procedure in order to avoid man-in-the-middle and replay attacks. However, this depends on the mobile network operator (home and serving) and cannot be checked by mobile users. When the VLR of a serving network has used an authentication triplet to authenticate an MS, it shall delete the triplet or mark it as used. Thus, each time the that VLR needs to use an authentication triplet, it shall use an unmarked one, in preference to a marked. If there is no unmarked triplet, then, the VLR shall request fresh triplets from the home HLR. If fresh triplets cannot be obtained, because of a system failure, the VLR may re-use a marked triplet. Thus, if a single triplet is compromised, a false BS can impersonate a genuine GPRS network to the MS. Moreover, as the false BS has the encryption key, Kc, it will not be necessary for the false BS to suppress encryption on the air interface. As long as the genuine SGSN is using the compromised authentication triplet, an attacker could also impersonate the MS and obtain session calls that are paid by the legitimate subscriber.

4.3 Data and Signalling Protection

An important weakness of the GPRS security architecture is related to the fact that the encryption of signalling and user data over the highly exposed radio interface is not mandatory. Some GPRS operators, in certain countries, are never switch on encryption in their networks, since the legal framework in these countries do not permit that. Hence, in these cases signalling and data traffic are conveyed in clear-text over the radio path. This situation is becoming even more risky from the fact that the involved end-users (humans) are not informed whether their sessions are encrypted or not.

As encryption over the radio interface is optional, the network indicates to the MS whether and which type(s) of encryption it supports in the Authentication request message, during the GPRS authentication procedure. If encryption is activated, the MS start ciphering after sending the Authentication response message, and the SGSN starts ciphering/deciphering when it receives a valid Authentication response message from the MS. However, since these two messages are not confidentially and integrity protected (data integrity is not provided in the GPRS radio interface except for traditional non-cryptographic link layer checksums), an adversary may

mediate in the exchange of authentication messages. The results of this mediation might be either the modification of the network and the MS capabilities regarding encryption, or the suppression of encryption over the radio interface.

4.4 GPRS Backbone

Based on the analysis of the GPRS security architecture (see sect. 3) it can be perceived that the GPRS security does not aim at the GPRS backbone and the wire-line connections, but merely at the radio access network and the wireless path. Thus, user data and signaling information, conveyed over the GPRS backbone, may experience security threats, which degrade the level of security supported by GPRS. In the following, the security weaknesses of the GPRS security architecture that are related to the GPRS backbone network for both signaling and data plane are presented and analyzed.

4.4.1 Signaling Plane

As mentioned previously, the SS7 technology, used for signaling exchange in GPRS, does not support security protection. Until recently, this was not perceived to be a problem, since SS7 networks belonged to a small number of large institutions (telecom operator). However, the rapid deployment of mobile systems and the liberalization of the telecommunication market have dramatically increased the number of operators (for both fixed and mobile networks) that are interconnected through the SS7 technology. This fact provokes a significant threat to the GPRS network security, since it increases the probability of an adversary to get access to the network or a legitimate operator to act maliciously.

The lack of security measures in the SS7 technology, used in GPRS, results also in the unprotected exchange of signaling messages between a VLR and a VLR/HLR, or a VLR and other fixed network nodes. Although these messages may include critical information for the mobile subscribers and the networks operation like ciphering keys, authentication data (e.g., authentication triplets), user subscription data (e.g., IMSI), user billing data, network billing data, etc., they are conveyed in a clear-text within the serving network, as well as between the home network and the serving network. For example, the VLR of a serving network may use the IMSI to request authentication data for a single user from its home network, and the latter forwards them to the requesting VLR without any security measure. Thus, the exchanges of signalling messages, which are based on SS7, may disclose sensitive data of mobile subscribers and networks, since they are conveyed over insecure network connections without security precautions.

4.4.2 Data Plane

Similarly to the signaling plane, the data plane of the GPRS backbone presents significant security weaknesses, since the introduction of IP technology in the GPRS core shifts towards open and easily accessible network architectures. In addition, the data encryption mechanism employed in GPRS does not extend far enough towards the core network, resulting also in a clear-text transmission of user data in it. Thus, a malicious, which gets access to the network, may either obtain access to sensitive data traffic or provide unauthorized/incorrect information to mobile users and network components. As presented previously, the security protection of users data in the fixed segment of the GPRS network mainly relies on two independent and complementary technologies, which are not undertaken by GPRS, but from the network operators. These technologies include firewalls that enforce security policies to a GPRS core network that belongs to an operator, and pre-configured VPNs that protect specific network connections.

However, firewalls were originally conceived to address security issues for fixed networks, and, thus, are not seamlessly applicable in mobile networks. They attempt to protect the clear-text transmitted data in the GPRS backbone from external attacks, but they are inadequate against attacks that originate from malicious mobile subscribers, as well as from network operator personnel or any other third party that gets access to the GPRS core network. Another vital issue regarding the deployment of firewalls in GPRS has to do with the consequences of mobility. The mobility of a user may imply roaming between networks and operators, which possibly results in the changing of the user address. This fact in conjunction with the static configuration of firewalls may potentially lead to discontinuity of service connectivity for the mobile user. Moreover, in some cases the security value of firewalls is considered limited as they allow direct connection to ports without distinguishing services.

Similarly to firewalls, the VPN technology fails to provide the necessary flexibility required by typical mobile users. Currently, VPNs for GPRS subscribers are established in a static manner between the border gateway of a GPRS network and a remote security gateway of a corporate private network. This fact allows the realization of VPNs only between a security gateway of a large organization and a mobile operator, when a considerable amount of traffic requires protection. Thus, this scheme can provide VPN services neither to individual mobile users that may require on demand VPN establishment, nor to enterprise users that may roam internationally. In addition, static VPNs have to be reconfigured every time the VPN topology or VPN parameters change.

5 Security Improvements in GPRS

The weak points of the GPRS security architecture may lead to compromises of end-users and network security of the GPRS system. These compromises may influence the system deployment and the users trend to utilize GPRS

for the provision of advanced multimedia services, which realizes the concept of mobile Internet. In the following sections, security enhancements that aim at improving the GPRS security architecture and providing advanced security services to user data traffic are presented.

5.1 Identity Confidentiality

To limit the exposure of the permanent identities (IMSI) of mobile users over the vulnerable radio interface, the additional usage of two complementary temporary identities for each mobile subscriber that is attached to the network has been proposed [22]. One of these temporary identities will reside at the serving network ($TMSI_{ALT}$), and the second one at the home network of the mobile user ($TMSI_{HE}$). When the VLR of the serving network fail to page a mobile user using the current TMSI, it can try to page him using the alternative temporary identity ($TMSI_{ALT}$), which also resides in the VLR. In case of a VLR database failure or a corruption of the temporary identities (i.e., TMSI and $TMSI_{ALT}$) that resides in the VLR, the VLR requests the temporary identity (i.e., $TMSI_{HE}$) from the home network, by which it can page the mobile user. This identity resides in the user's home network in order to avoid a possible corruption after a database (VLR) failure. In case that none of the TMSI is valid or all of them are corrupted, the user is not attached to the network.

Both the additional temporary identities (i.e., $TMSI_{ALT}$ and $TMSI_{HE}$) derive from the current TMSI. The latter consists of 4 octets and its generation procedure is chosen by the mobile operator. However, some general guidelines are applied in all implementations in order to avoid double allocation of TMSIs, after a restart of the allocating node (i.e., VLR or SGSN). For this reason, some part of the TMSI may be related to the time when it was allocated or contain a bit field, which is changed when the allocating node has recovered from the restart. After the generation of a TMSI, the allocating node applies two individual hash functions (i.e., $HASH_{ALT}$ and $HASH_{HE}$), which produce the corresponding $TMSI_{ALT}$ and $TMSI_{HE}$, respectively. Then, the allocating node forwards the three temporary identities to the involved mobile user and the $TMSI_{HE}$ to its home network. In cases that the home and the serving network are the same, the $TMSI_{HE}$ can be stored in HLR, which is not affected by the reasons that corrupt the other two temporary identities. Finally, each time that the current TMSI is renewed, the two additional temporary identities change in order to eliminate the possibility of an adversary to link them to the permanent user's identity.

5.2 Signalling Protection

To address the lack of security measures in the signaling plane of the GPRS backbone, we propose the incorporation of the Network Domain Security (NDS) features [22] 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) [4] and the GTP protocol [5], 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 [14]. 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 [6]. To address the increasing security needs, this effort has to be continued to cover the entire set of the SS7 protocol stack.

5.3 User Data Security

Another weakness of the current GPRS security architecture that can be overcome is related to the lack of effective protection of user data in the fixed part of the GPRS network. To address this problem, two alternative security solutions, which are based on existing security technologies, can be used: (a) the application layer security, and (b) the establishment of mobile VPNs, dynamically, that satisfy users' needs.

5.3.1 Application Layer Security Solutions

Application layer security solutions integrate security into applications at the level of end-users. The most prominent protocol that provides security at this layer for the Internet technology is the Secure Sockets Layer protocol (SSL) [12]. SSL supports server authentication using certificates, data confidentiality, and message integrity. Since SSL is relatively "heavy" for implementations on mobile devices, which are characterized by limited processing capabilities, a lightweight version of SSL named "KiloByte" SSL (KSSL) have been proposed [12]. This SSL implementation (KSSL) provides an advantage by enabling mobile devices (GRPS MS) to communicate directly and securely with a considerable number of Internet web servers that support SSL.

Application layer security is also applied in the Wireless Application Protocol (WAP) suite [18]. The WAP architecture is designed for the delivery and presentation of Internet services on wireless terminals, taking into account the limited bandwidth of mobile networks and the limited processing capabilities of mobile devices. It separates the network in two domains (i.e., the wireless and the Internet domain) and introduces a WAP gateway that translates the protocols used in each domain. The WAP architecture has been standardized in two releases (Version 1.2.1 and Version 2.0).

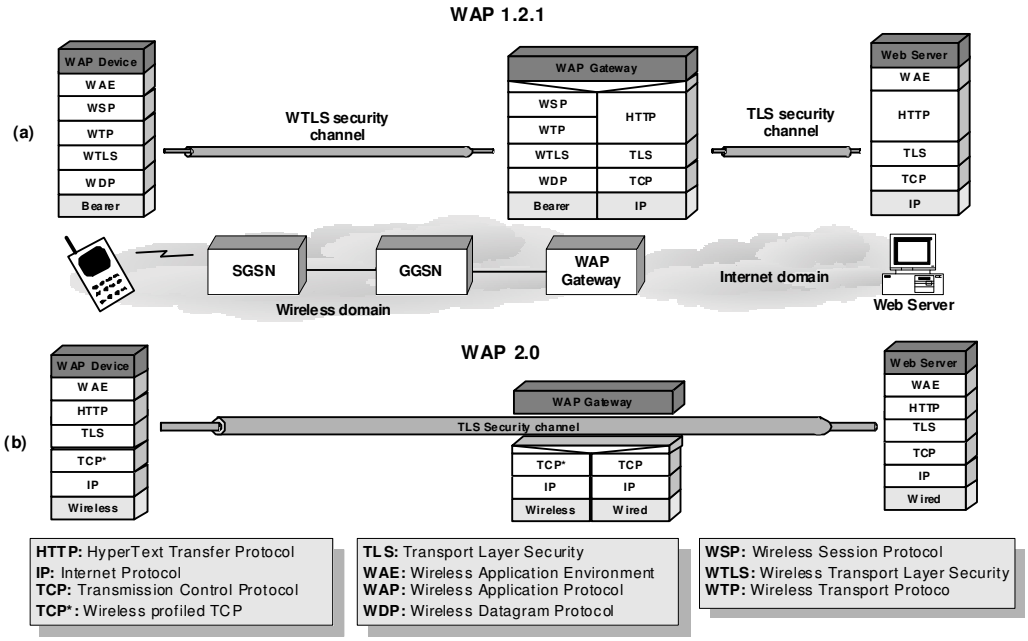

Figure 4: The architecture of WAP (a) WAP 1.2.1, (b) WAP 2.0

The WAP deployment over the GPRS network architecture is presented in Figure 4. In WAP 1.2.1 (see Figure 4 (a)), security is applied by using the Wireless Transport Layer Security (WTLS) protocol [18] over the wireless domain and the Transport Layer Security (TLS) protocol over the Internet domain. WTLS, which is based on TLS, provides peers authentication, data integrity, data privacy, and protection against denial-of-service in an optimized way for use over narrow-band communication channels. However, WAP 1.2.1 does not support end-to-end security, since the conveyed data are protected by two separate security channels (i.e., WTLS security channel and TLS security channel).

On the other hand, WAP 2.0 (see Figure 4 (b)) introduces the Internet protocol stack into the WAP environment. It allows a range of different gateways, which enable conversion between the two protocol stacks anywhere from the top to the bottom of the stack. A TCP-level gateway allows for two versions of TCP, one for the wired and another for the wireless network domain. On the top of the TCP layer, TLS can establish a secure channel all the way from the MS to the remote server. Thus, the availability of a wireless profile for TLS enables end-to-end security allowing interoperability for secure transactions.

5.3.2 Mobile VPN

An alternative approach to the above solutions that employ security at the application layer pertains to these that employ security at the network layer. The most prominent technique for providing security at the network layer is IPsec [14]. As a network layer security mechanism, IPsec protects traffic on a per connection basis, and, thus, is independent from the applications that run above it. In addition, IPsec is used for implementation of VPNs [10]. 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 the deployment of VPNs over the GPRS infrastructure, three alternative security schemes have been proposed: (a) the end-to-end [21], (b) the network-wide [20], and (c) the border-based [19]. 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.

End-to-end security scheme:
The end-to-end security scheme integrates the VPN functionality into the communicating peers, which negotiate and apply security. More specifically, a MS and a remote security gateway (SG) of a corporate private network establish a pair of IPsec Security Associations (SAs) between them, which are extended over the entire multi-nature communication path, as shown in Figure 5. Thus, sensitive data are secured as they leave the originator site (MS or SG), and remain protected while they are conveyed over the radio interface, the GPRS backbone net-

work, and the public Internet, eliminating the possibilities of being intercepted, or to be altered by anyone.

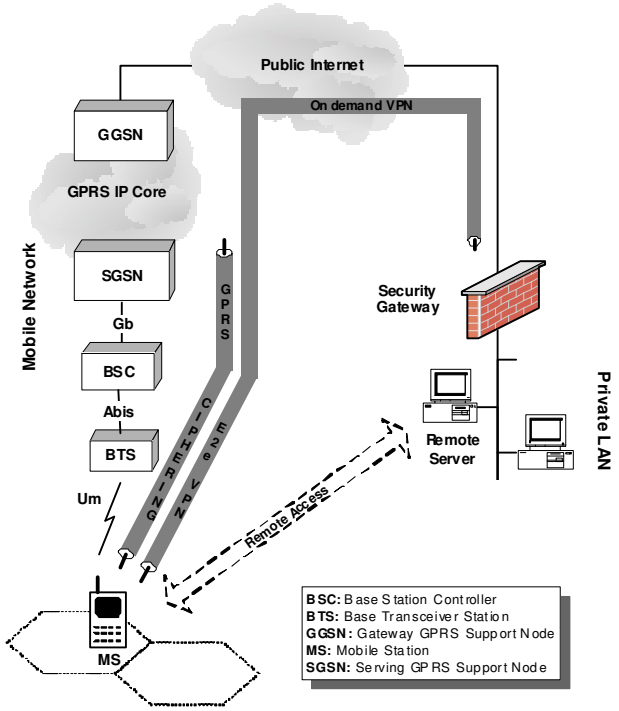

Figure 5: The end-to-end security scheme

For the end-to-end VPN establishment the IKE [13] protocol is employed. However, its standard version must be enhanced to resolve the problems arising from the NAT presence, and configured to operate in a mobile environment. IKE provides secure key determination via Diffie-Hellman (DH) exchanges with authentication of participants, protection against reply, hijacking, flooding attacks, and negotiation of encryption and/or authentication transforms. Authentication is performed by end-hosts using digital certificates, issued by a trusted certificate authority. The SA negotiation is not transparent to the mobile subscriber and his device. However, the mobile network operator does not even realize the existence of an end-to-end VPN, and, thus, neither service level agreement nor trusted relations between the security endpoints and the network operator are required. In this scheme, the trusted relations are limited between the security endpoints and the certificate authority, which issues digital certificates and facilitates authentication process.

The deployed end-to-end VPN has no interrelation with the underlying network operation and the provided network connectivity. It operates above the network layer, and, thus, the security parameters, which are contained within the IPsec SA, are not affected by the MS movement. For this reason the MS may freely move within the GPRS coverage area maintaining network connectivity and VPN service provision. The GPRS mobility management procedures keep track of the user location, and, therefore, the incoming packets are routed to the MS.

In the end-to-end security scheme, the necessary enhancements for security service provision have minimal impact on the existing network infrastructure. Specifically, the GPRS network nodes, and the intermediate IP routers require no further enhancements or modifications to support the particular VPN scheme. The changes are limited to the security endpoints (MS and SG), which incorporate the IPsec functionality, including the IKE protocol to negotiate, establish, and apply security associations. However, the mobile devices (i.e., MS) are characterized by limited power and processing capabilities. This may increase significantly the processing latency and result in service inadequacy. In addition, GPRS employs an optimized ciphering for packet data transmission over the radio interface. Thus, the end-to-end security scheme duplicates encryption (packet encapsulation) over the scarce radio interface, which increases the overall communication cost, and decreases the access network capacity.

Finally, the end-to-end security scheme is not compatible with the legal interception option, or any other application that requires access to the traversing data within the mobile network. The enforcement of network security policy, traditionally performed by border firewalls, is devolved to end hosts, which establish VPN overlays. Despite this, the border firewalls remain to perform packet filtering and counteract against denial of service attacks [23].

Network-wide and border-based security schemes: Contrary to the end-to-end security scheme, the network-wide [20] and the border-based [19] schemes integrate the VPN functionality into the GPRS network infrastructure following a network-assisted security model. In both schemes a MS initiates a VPN that is negotiated and established by the network infrastructure, thus, minimizing the impact to end-users and their devices. The network operators provide the security aggregation facilities, which are shared amongst the network subscribers, as a complementary service granting added value. They have solid network management expertise and more resources to effectively create, deploy and manage VPN services originating from mobile subscribers.

For the deployment of both security schemes (i.e., network-wide and border-based) the MS must be enhanced with a security client (SecC) and the GPRS core network should incorporate a security server (SecS). The SecC is employed by the user to request for VPN services and express his preferences. It is a lightweight module that does not entail considerable processing and memory capabilities, and, thus, it can be easily integrated in any type of mobile device causing minor performance overhead. On the other side, the SecS establishes, controls and manages VPNs between itself and remote SGs at corporate LANs on behalf of the mobile users. The SecS comprises an IPsec implementation modified to adapt to the client-initiated VPN scheme and the security service provision in a mobile GPRS environment. It can be read-

ily integrated in the existing network infrastructure, and, thus, both schemes can be employed as add-on features of GPRS.

When a mobile user wants to establish a secure remote connection towards a SG, it uses the SecC to request for an IPsec SA from the corporate SecS. VPN initialization and key agreement procedures are based on an IKE-proxy scheme [20], which enables the MS to initiate a VPN establishment, while outsourcing key negotiation to the network infrastructure. The SecS (on behalf of the MS) and the remote SG authenticate each other using digital signature. After the VPN establishment, data exchanged between the MS and the SG are encrypted/decrypted in the SecS, which resides in the GPRS core network, relying on the mobile network operator security policy. Thus, the mobile subscriber and the administrator of the private network have to trust the mobile network operator. Moreover, all the involved parties (mobile users, mobile operator, and corporate LAN) have to trust the authority, which issues the digital certificates.

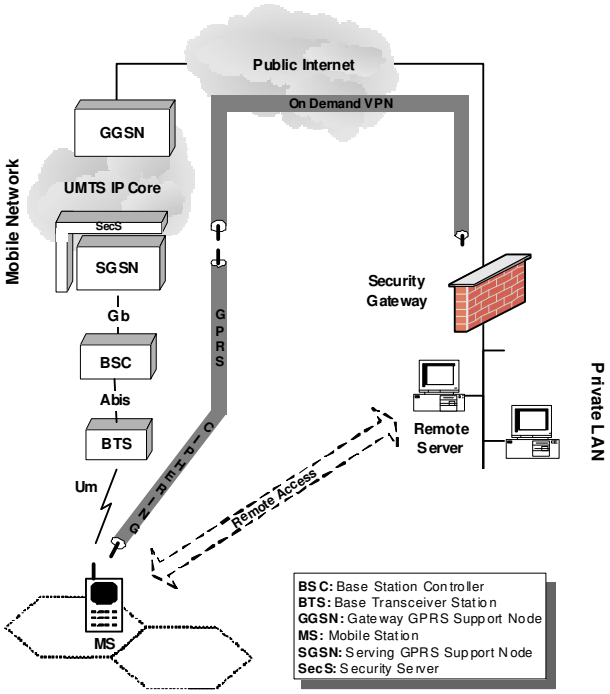

Figure 6: The network-wide security scheme

The network-wide scheme (see Figure 6) integrates the SecS into the SGSN of the GPRS network infrastructure. This scheme provides maximal security services to the communicating peers by employing the existing GPRS ciphering over the radio interface and extending a VPN over the GPRS backbone and the public Internet. Thus, sensitive user data remains encrypted for the entire network route between the originator and the recipient. In order to achieve VPN continuity as a mobile user moves and roams, the standard GPRS mobility management procedures needs to be enhanced. The enhancements include the transfer of the related context (named as security context), which contains the details of the deployed security associations that pertain to the moving user, to the new visited access point. This transfer enables the reconstruction of the security associations of the moving user to the new visited access point, when the user connects to it, providing continuous VPN services from the end-user perspective. The network-wide scheme is compatible with legal interception; however, UDP encapsulation is applied for NAT traversal. Finally, the network security policy is enforced by the SGSN, which incorporates the SecS.

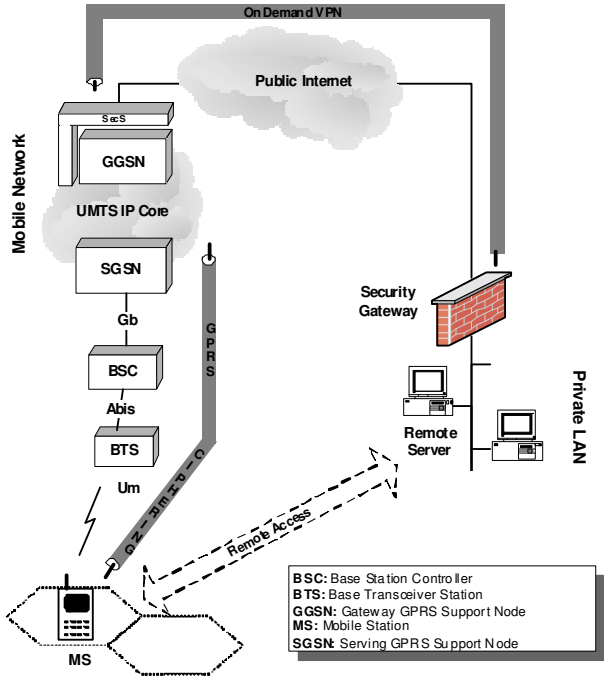

Figure 7: The border-based security scheme

By placing the SecS in the GGSN, the border-based VPN deployment scheme is realized (see Figure 7). This scheme protects data conveyance over the public Internet, which is a vulnerable network segment. The user mobility is transparent to the VPN operation, as long as the user remains under the same network operator coverage and is served by the same GGSN. However, whenever the mobile user roams to another GGSN, the existing security association cannot be used and a new VPN should be established. The border-based scheme is compatible with the legal interception option and NAT presence. Moreover, since the SecS resides at the GGSN, it also provides firewall services to the GPRS network applying network security policy.

6 Conclusions

This paper has presented an evaluation of the security architecture employed in GPRS. This architecture comprises a set of measures that protect the mobile users,

the radio access network, the fixed part of the network and the related data of GPRS. Most of these measures 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 operational differences between the application of these measures in GSM and GPRS have been outlined and commented. In addition, the security measures that can be applied by GPRS operators to protect the GPRS backbone network and inter-network communications, which are based on IP, have been explored.

Although GPRS have been designed with security in mind, it presents some essential security weaknesses, which may lead to the realization of security attacks that threaten network operations and data transfer through it. These weaknesses are related to: (a) the compromise of the confidentiality of subscriber's identity, since it may be conveyed unprotected over the radio interface; (b) the inability of the authentication mechanism to perform network authentication; (c) the possibility of using COMP128 algorithm (which has been cryptanalyzed) for A3 and A8 implementations; (d) the ability of reusing authentication triplets; (e) the possibility of suppressing encryption over the radio access network or modifying encryption parameters; and (f) the lack of effective security measures that are able to protect signaling an user data transferred over the GPRS backbone network.

The weak points of the GPRS security architecture may lead to compromises of end-users and network security of the GPRS system. These compromises may influence the system deployment and the users' trend to utilize GPRS for the provision of advanced multimedia services, which realizes the concept of mobile Internet. To address some of the above-mentioned weaknesses, a set of security enhancements has been proposed. These enhancements aim at improving the GPRS security architecture and providing advanced security services to user data traffic. They include: (a) the use of two additional temporary identities for each mobile user that is attached to the network; (b) the incorporation of NDS features into the GPRS security architecture; (c) the use of application layer security; and (d) the establishment of mobile VPNs, dynamically, that satisfy users' needs. The proposed enhancements can be easily integrated in the existing GPRS infrastructure, minimizing the required changes.

References

[1] 3GPP TS 01.61 (v7.0.0), *GPRS Ciphering Algorithm Requirements*, Sep. 2001.

[2] 3GPP TS 03.03 (v7.8.0), *Numbering, Addressing and Identification*, Sep. 2003.

[3] 3GPP TS 03.6 (V7.9.0), *GPRS Service Description, Stage 2*, Sep. 2002.

[4] 3GPP TS 09.02 (v7.15.0), *Mobile Application Part (MAP) specification*, Mar. 2004.

[5] 3GPP TS 09.60 (V7.10.0), *GPRS Tunnelling Protocol (GTP) Across the Gn and Gp Interface*, Dec. 2002.

[6] 3GPP TS 33.200 (v4.3.0), *3G Security; Network Domain Security; MAP Application Layer Security*, Mar. 2002.

[7] E. Barkan, E. Biham, and N. Neller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," in *Proceedings Advances in Cryptology (CRYPTO 2003)*, LNCS 2729, pp. 600-616, Aug. 2003.

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

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

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

[11] GSM 03.20, *Security Related Network Functions*, Nov. 1999.

[12] V. Gupta and S. Gupta, "Securing the wireless internet," *IEEE Communications Magazine*, vol. 39, no. 12, pp. 68-74, Dec. 2001.

[13] D. Harkins and D. Carrel, *The Internet Key Exchange (IKE)*, RFC 2409, Nov. 1998.

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

[15] 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/)

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

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

[18] Wireless Application Forum (WAP), WAP specifications. (http://www.wapforum.org/what/ technical.htm)

[19] C. Xenakis and L. Merakos, "Dynamic network-based secure VPN deployment in GPRS," in *Proceedings of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'02)*, pp. 1260-1266, Lisboa, Portugal, Sep. 2002.

[20] C. Xenakis and L. Merakos, "On demand network-wide VPN deployment in GPRS," *IEEE Network*, vol. 16, no. 6, pp. 28-37, Nov/Dec. 2002.

[21] C. Xenakis, E. Gazis, and L. Merakos, "Secure VPN deployment in GPRS mobile network," in *Proceedings of International Conference on European Wireless*, pp. 293-300, Florence Italy, Feb. 2002.

[22] C. Xenakis and L. Merakos, "Security in third generation mobile networks," *Computer Communications*, vol. 27, no. 7, pp. 638-650, May 2004.

[23] C. Xenakis and L. Merakos, "Alternative schemes for dynamic secure VPN deployment over UMTS," *Wireless Personal Communications*, vol. 36, no. 2, pp. 163-194, Springer, Jan. 2006.

Christos Xenakis received his B. Sc degree in computer science in 1993 and his M.Sc degree in telecommunication and computer networks in 1996, both from the Department of Informatics and Telecommunications, University of Athens, Greece. In 2004 he received his Ph. D. from the University of Athens (Department of Informatics and Telecommunications). From 1998 - 2001 he was with a Greek telecoms system development firm, where he was involved in the design and development of advanced telecommunications subsystems for ISDN, ATM, GSM, and GPRS. Since 1996 he has been a member of the Communication Networks Laboratory of the University of Athens and, currently, he is the head of the Security Group. He has participated in numerous projects realized in the context of EU Programs (ACTS, ESPRIT, IST). His research interests are in the field of system and network security. He is the author of over 25 papers in the above area.