Secure VPN Deployment in GPRS Mobile Networks

Christos Xenakis, Evangelos Gazis and Lazaros Merakos

Communication Networks Laboratory
Department of Informatics & Telecommunications, University of Athens 15784 Athens, Greece.

Ph.: + 30 10 7275341, Fax: + 30 10 7275601, e-mail: {xenakis,gazis,merakos}@di.uoa.gr

ABSTRACT
The growth of the Internet and the success of mobile networks suggest that the next trend will be an increasing demand for mobile access to Internet applications. It is therefore increasingly important that mobile radio networks support these applications in an efficient manner. Moreover, in such a hybrid environment, where clients are connecting to ever growing networks in an ad-hoc fashion, the security requirements of such practices become even more important. An end-to-end Virtual Private Network (VPN) deployment scenario over the GPRS mobile network is presented and analyzed. The VPN deployment is based on the IPsec protocol suite. A specific protocol configuration of the IPsec is proposed, in order to make it operational on a mobile network environment. The potential incompatibility problems that may arise from the integration of different technologies are elaborated. Finally, a qualitative evaluation of the proposed VPN scheme and the outline of an alternative approach for future work are presented.

1. INTRODUCTION

In the recent years, IP-based user applications are becoming increasingly popular and the Internet technology has emerged as the major driving force behind new developments in the area of telecommunication networks. Meanwhile, mobile networks face a similar trend of growing importance to users. The rapid deployment of wireless devices is changing the way people communicate and conduct business. The combination of both developments, the growth of the Internet and the success of mobile networks, suggests that the next trend will be an increasing demand for mobile access to Internet applications. It is therefore increasingly important that mobile radio networks support these applications in an efficient manner. Moreover, in such a hybrid environment where clients are connecting to ever growing networks in an ad-hoc fashion, the security requirements of such practices become even more important.

The most widely deployed public mobile data network, which enables the integration of IP world with mobile networks and constitutes a migration step toward third-generation (3G) networks, is the GPRS. GPRS allows network operators to implement an IP-based core architecture for data applications, which will continue to be used and expanded for 3G services, such as integrated voice and data applications. However, the introduction of IP as a network layer in the GPRS backbone network signifies not only a shift towards packet switching, but also a shift towards completely open and easily accessible protocols. Nonetheless, security issues and the vulnerabilities in this emerging hybrid network environment are still open.

IP is a connectionless and stateless protocol that was designed to connect trusted users on an insecure network. It is relative easy to forge the IP address, modify the contents of the IP packet, replay old packets, and inspect the contents of the packets in transit [30]. Therefore, there is no guarantee that the IP datagrams received are from the claimed sender; that they contain the originally sent data; or that the original content was not inspected by a third party while in transit.

In order to solve the IP security weaknesses, the IETF has developed the IPsec protocol suite to protect both integrity and confidentiality of IP packets by establishing VPN. One of the difficulties of deploying IPsec and setting up VPNs, is the configuration of IPsec protocol and the handling of VPN alternatives, since there are no official guidelines, especially, for mobile networks.

In this paper, an end-to-end VPN deployment scenario over the GPRS mobile network is presented and analyzed. More specifically, a protocol configuration for the IPsec suite is proposed, and the potential incompatibility problems that may arise from the integration of different technologies are elaborated. Finally, an evaluation of the particular VPN scheme is presented.

This paper is organized as follows. Section 2 introduces the GPRS network architecture. Section 3 briefly describes the IPsec protocol suite and the VPN technology. In section 4, the end-to-end VPN deployment over the GPRS network is elaborated, focusing on the IPsec protocol suite configuration and operation, as well as on the potential incompatibilities that may arise. Section 5 presents an evaluation of the proposed VPN scheme, and section 6 contains the conclusions.

2. GPRS

The GPRS is a new service that provides packet radio access for GSM users. The main benefit of GPRS is that it reserves radio resources only when there is data to send, thus enabling the efficient provision of a variety of new and unique services [3, 10] to the subscribers.

From a high level, GPRS can be thought of as an overlay network onto a second-generation GSM [1] network enabling packet data transport at rates from 9.6 to 171 kbps. GPRS attempts to reuse the existing GSM network elements as much as possible, but in order to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols that handle packet traffic are required [2, 3]. The new class of network nodes, called GPRS support nodes

(GSN), is responsible for the delivery and routing of data packets between the mobile stations (MS) and the external packet data networks (PDN). The communication between the GSN nodes is based on IP tunnels [17] through the use of the GPRS Tunneling Protocol (GTP) [11]. In Fig.1, the enhanced GPRS network architecture is illustrated.

A Serving GSN (SGSN) is responsible for the delivery of data packets from and to the MS within its service area. Its tasks include packet routing and transfer, mobility management, logical link management, authentication, and charging functions.

A Gateway GSN (GGSN) acts as an interface between the GPRS backbone network and the 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. In the other direction, the PDP addresses of incoming data packets are converted to the GSM address of the destination user.

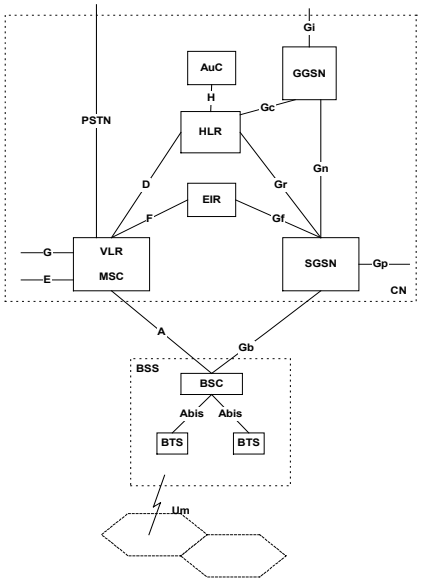

Figure 1: GPRS system architecture

To exchange data packets with external PDNs after a successful GPRS "attach" procedure, the MS must apply for an IP address (PDP address). For each session, a so-called PDP context is created, which describes the characteristics of the session. Its attributes contain the PDP type (e.g., IPv4), the PDP address assigned to the MS (e. g., 195.134.66.3), the requested QoS, and the address of a GGSN that serves as the access point to the PDN. This context is stored in the MS, the SGSN, and the GGSN. With an active PDP context, the MS is "visible" to the external PDN and is capable of sending and receiving data packets [6]. The mapping between the two addresses, PDP and IMSI [7] (International Mobile Subscriber Identifier), enables the GGSN to transfer data packets between PDN and MS.

Since the GPRS may be connected to a public network [6], it is subjected to security threats. As the Internet has come to play a critical role in mobile network evolution and networking, protection from undesirable Internet inhabitants is a necessity.

3. VPN

3.1 General

One of the key elements of safe networking is the proper design and configuration of VPNs [12]. VPNs allow for private data to be encrypted and transmitted securely over public networks. A VPN is a network that extends, dedicated connections between remote branches, or remote access to mobile users, over a shared infrastructure. Implementing a VPN on a public network makes security issues such as confidentiality, integrity, and authentication, paramount. Currently, a number of different security solutions for IP networks exist.

Application-layer security builds security features into individual applications. Security at this level is by far the easiest to deploy, as long as all users are running a homogeneous application on a standard platform. While these methods are effective for solving specific security problems, such solutions are by their nature limited to their specific niches [9].

In contrast to the application-layer security protocols, the IPsec [13, 18] standard aims at securing the network itself. Therefore, the IPsec protocol suite guarantees security for any application that uses the network, and makes the cost effective realization of the secure VPN possible.

3.2 IPsec

IPsec is a developing standard for security at the network or packet processing layer. It provides encryption and integrity protection of packets on both IPv4 and IPv6, as well as authentication of the communicating entities.

IPsec grants two choices of security service: Authentication Header (AH) [19], and Encapsulating Security Payload (ESP) [20]. The AH provides support for connectionless integrity, data origin authentication, and protection against replays, but does not provide secrecy. On the other hand, ESP supports confidentiality, connectionless integrity, anti-replay protection, and optional data origin authentication. A key concept that appears in both security services, and represents a one-way relationship between a sender and a receiver is the Security Association (SA) [13].

Both AH and ESP support two modes of use: transport and tunnel mode [13]. The transport mode mainly provides end-to-end protection, where the IP packet payload is encrypted. The tunnel mode encapsulates the entire IP packet (including the IP header) within a new IP packet [17] to ensure that no part of the original packet is visible or may be changed as it is forwarded through a network.

3.3 IKE

Secure key exchange is an integral part of the IPsec standards [13]. In order to establish a SA between two hosts, they must first agree to apply compatible policy and cryptographic algorithms. They must also share a secure mechanism for determining keying material over an insecure channel. The default IPsec method for secure key negotiation is the Internet Key Exchange (IKE) [14] protocol. IKE allows several types of authentication methods and standard cryptographic groups to be used. It provides secure key determination via Diffie-Hellman (DH) [25] exchanges. Unlike the rest of IPsec, which

resides at or just below the network layer, IKE is an application-layer protocol.

Recently, some scepticism has been raised concerning the complexity of the IKE and the related protocols [21]. Discussions in the IETF IPsec working group also indicate that IKE has confused a number of experienced implementers. Key negotiations and determinations for IKE are covered in four RFC's: IKE [14], ISAKMP [22], OAKLEY [23] and the ISAKMP Domain of Interpretation [24].

IKE consists of two phases. Phase 1 creates an ISAKMP SA (or IKE SA) using a DH exchange. The purpose of IKE phase 1 is to establish a bi-directional secure channel, so that phase 2 negotiations (IPsec SA) can occur privately. The establishment of an ISAKMP SA must always be the first step of an IPsec transaction. Multiple IPsec SAs can be established from a single ISAKMP SA, which may be considered as a "control channel" on which IKE is the control protocol.

3.4 Authentication

The key management mechanism that is used to distribute keys is coupled to the authentication mechanisms, which are specified separately. There are four types of authentication available with IKE: preshared key, digital signature, and public key encryption with four and two encryptions respectively [14]. From those methods, the preshared key is the simplest form of authentication. In order for authentication to occur, the initiator and the responder must agree upon a key, typically using some out-of-band technique [21]. For example, the network administrator could give the remote user a password. When attempting a key negotiation, the remote user is challenged for the password.

3.5 VPN deployment

Concerning the VPN deployment, there are two general schemes regardless of the security protocol employment and the mode of operation. The first is based on customer premises equipment (CPE) where the VPN capabilities are being integrated into a variety of CPE devices. This scheme does not have an impact on the network design, topology, or any routing decisions. The communicating end-points must have the appropriate software to negotiate a SA and apply security.

The second scheme pertains to network based-VPNs, where the operation of the VPN is outsourced to the network operator or a service provider. There is significant interest in such solutions both by customers seeking to reduce support costs and by network operators seeking new revenue sources. However, the network based VPN service scheme, requires the introduction of security modules within the network infrastructure and places an additional burden on it. Additionally, the biggest consideration with VPN services is that one's company security infrastructure is not directly under his control.

In the following sections, an end-to-end VPN security scheme over the GPRS mobile network is analysed.

4. VPN DEPLOYMENT SCENARIO IN GPRS

4.1 General

The continuously increasing demand for wireless access to the Internet, particularly the mobile access to corporate Intranets through the GPRS infrastructure, requires the provision of authentication, confidentiality, and integrity services. The most prominent security mechanisms, such as VPNs and IPsec, were originally conceived to address network security issues for fixed networks. Nevertheless, the increased user/device mobility and the new emerging integration trend between mobile and fixed networks have introduced a whole new realm of security scenarios that were not previously foreseen.

Even though there is some criticism on IPsec, it is commonly admitted that it is the best IP security protocol available today [26]. It facilitates the transparent encryption and integrity protection of packets on both IPv4 and IPv6 networks, and authentication of the communicating entities. It is especially useful for implementing VPNs, and for remote user access to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Additionally, IPsec is employed below the transport layer (TCP, UDP), so is transparent to the end users and their applications. Finally, another strength of IPsec is its flexibility, which simplifies deployment across any existing IP network [27].

On the other hand, the main drawback of IPsec is its complexity. It contains too many options, and too much flexibility, that there are often several ways of doing the same or similar things [26]. Additionally, a number of individuals have argued against IKE's complexity. They claim that the difficulty of analyzing the security of a system increases with complexity. The core of most complaints is that IKE tries to be a "Swiss Army knife" with options for a large number of general scenarios, instead of focusing on addressing a limited number of needs in a simpler fashion [21].

Unfortunately, the rollout of VPN services using the IPsec protocol suite is not problem-free [30], especially, over the GPRS mobile network. Except for IPsec and IKE protocol configuration, a major identified problem is the incompatibility of Network Address Translation (NAT) [34, 35] and IPSec. NAT maps an isolated address realm with private unregistered addresses to an external realm with globally unique registered addresses. The widely used NAT has prohibited full use of IPsec VPNs, as IPsec views the packet processing of NAT as a violation of communication integrity [29]. Additionally, potential incompatibilities may be caused by the GPRS specific protocol employment.

In the following sections, a detailed analysis of an end-to-end VPN scenario over the GPRS mobile network using the IPsec protocol suite is presented, taking into account the rules and requirements imposed by the mobile environment.

4.2. Network architecture

Consider a mobile network subscriber carrying on an MS and attempting to establish an end-to-end secure remote connection to a corporate Intranet and access a remote server, as shown in Fig.2. In order to access the GPRS, the MS first makes its presence known to the network by performing a GPRS "attach", which establishes a logical link between the MS and the SGSN. Then, for sending and receiving data, the MS activates the PDP address, which introduces the MS to the corre-

sponding GGSN, and interworking with external data networks can commence.

Through the "attach" and the "PDP context activation" procedures, the MS acquires an IP address, a GTP tunnel between the employed SGSN – GGSN is established, and the physical route among the GGSN, SGSN and the MS is configured. Then, in order to access the remote server at the private LAN the mobile user initiates a session between itself and the LAN's Security Gateway (SG). The SG is a gatekeeper device positioned between Internet and the private network. It functions as a proxy device providing security services to nodes on the private network it protects.

It is assumed that the GPRS backbone network, as well as the Internet backbone, are based on IPv4. Additionally, both the GGSN and the SG use NAT.

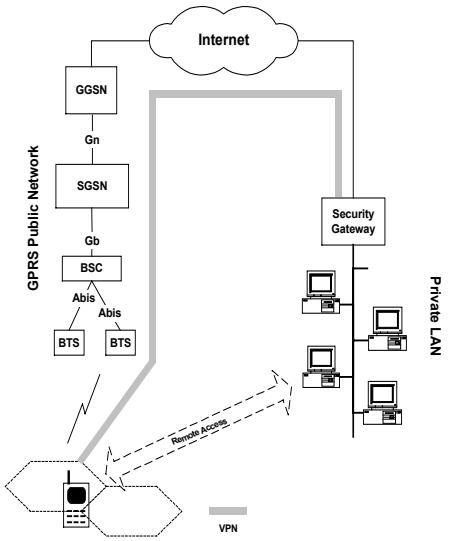

Figure 2: Network architecture

4.3 IKE deployment

For the VPN establishment between the MS and the SG, first the IPsec session using the IKE protocol is negotiated. During phase 1, an ISAKMP SA negotiation in aggressive mode (AM) takes place (see fig. 3). The AM of the IKE key negotiation is an option defined to speed up the IKE transaction at the cost of slightly less security. Moreover, the authentication method used in AM doesn't involve the IP address of the initiator. Thus, the IKE protocol is operational in a mobile network environment where dynamic (not static) IP addresses may be used.

In message (1) a cookie (C_{MS}) (64-bit random number which facilitates prevention of flooding attacks), the ISAKMP SA data (ISA_{MS}), the Diffie-Helman [25] half key, a nonce (N_{MS}) (a large random number between 64 - 2048 bits that adds randomness), and the identification data (ID_{MS}) are forwarded to the SG. Then, the SG replies with message (2), which contains the cookie pair as well as its ISAKMP SA response, the DH half-key, a nonce, its identity, and the $HASH_{SG,}$ which contains SG's authentication information. Finally, in message (3) the MS transmits its authentication information ($HASH_{MS}$) to the SG together with the cookie pair (see fig. 3).

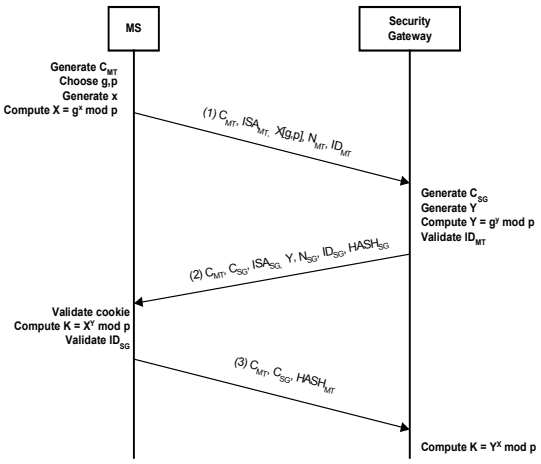

Figure 3: ISAKMP SA negotiation in aggressive mode

The authentication of endpoints (MS & SG) is based on a preshared key method, as it is the simplest form of authentication, compared to digital signature and public key encryption authentication methods, and fits better in the mobile scenario. The authentication computation is based on the identification (ID) packet payload, which is static, rather than on the IP address, which may vary.

Having established an ISAKMP SA between the MS and the SG, the communicating parties have agreed on [9, 14]:

- the encryption algorithm to protect data.
- the hash algorithm to reduce data for signing.
- the authentication method for signing data.
- the Diffie-Hellman exchange.
- an optional pseudo-random function (PRF) used to hash certain values during the key exchange for verification purposes.

Following the successful completion of phase 1, an IKE phase 2 negotiation (quick mode) is performed to establish an IPsec SA between the MS and the SG. All packets pertaining to phase 2 are encrypted using the pre-established ISAKMP SA. In Fig. 4, the quick mode transactions between the MS and the SG are shown.

In message (1), the MS transmits the cookies (C_{MS} , C_{SG}), its IPsec SA request (SA_{MS}), its nonce (N_{MS}), the DH half key and the identities of the MS and SG (ID_{MS} , ID_{SG}, respectively). Additionally, the MS authenticates the message with HASH(1), which is computed as follows:

HASH(1)=$hashfunc(SKEYID_a , M_{ID} |SA_{MS} |N_{MS} |X |ID_{MS} |ID_{SG})$

$SKEYID_a$ is a key derived from SKEYID and is used as authentication key. SKEYID is derived differently for each authentication method. Using the preshared key authentication method the SKEYID is computed as follows:

SKEYID=$hashfunc(PSKEY, N_{MS} |N_{SG})$ where PSKEY is the preshared key.

$SKEYID_a$=$hashfunc(SKEYID, SKEYID_d |k |C_{MS} |C_{SG} |1)$.

Similarly, $SKEYID_d$=$hashfunc(SKEYID, k |C_{MS} |C_{SG} |0)$, where k is the key resulting from the DH exchange. $SKEYID_d$ is used to derive more keying material. Finally, M_{ID} is the value of the message identifier, which is a generic part of ISAKMP header, and is included in all IKE packets.

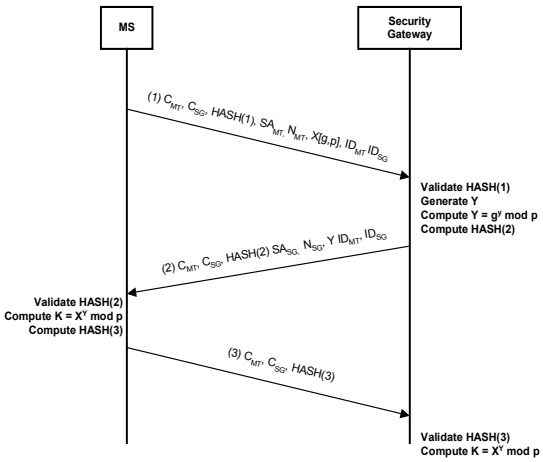

Figure 4: IPsec SA negotiation (Quick Mode)

In message (2), the SG transmits the cookies, its IPsec SA response, its nonce, the DH half key, and the (MS & SG) identities. The security gateway also authenticates the message with HASH(2) which is computed as follows:

HASH(2)=*hashfunc(*$SKEYID_a$ *,* M_{ID} $|SA_{SG}$ $|N_{SG}$ $|Y|ID_{MS}$ $|ID_{SG}$ *)*

In message (3), the MS authenticates the transaction with HASH(3) which is computed as follows:

HASH(3)=*hashfunc(*$SKEYID_a$ *, 0* $|M_{ID}$ $|N_{MS}$ $|N_{SG}$*).*

After this dialog between the MS and SG, an IPsec SA, which groups all the necessary parameters for secure communication, has been established. This SA specifies the following [9, 13, 16]:

- the Security Parameter Index.
- the IP destination address.
- the security protocol identifier (ESP).
- the IPsec protocol mode (Transport mode).
- the encryption algorithm used in ESP and the keys to be used.
- how authentication is performed.
- how often those keys are to be changed.
- the lifetime of the SA itself.
- the SA source address.

As a SA is used only in one direction, for bi-directional communications between the MS and the SG, two SAs are required. Each SA implements a single mode and protocol.

4.4 IPsec operation

Having established a pair of IPsec SA between the MS and the SG, a bi-directional private channel that allows for the secure data exchange between these two nodes has been set up. The GPRS MS, which is located in a public land mobile network (PLMN), may now send and receive IP packets to and from a remote server connected to the private LAN through the Internet.

ESP protocol employment is considered more advantageous in this setup/architecture, given that ESP can provide integrity protection as well [26]. Furthermore, the IPsec protocol is configured in transport mode because one of the VPN termination points is the MS, which is rather difficult to operate in tunnel mode. If the MS is configured in tunnel mode then, an unnecessary IP encapsulation in the MS and an unwanted extra overhead over the radio interface (IF) will be carried out.

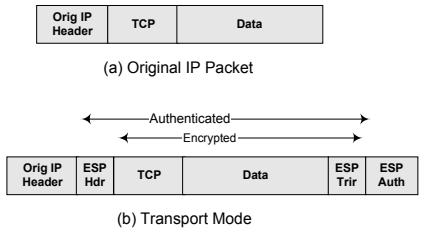

Figure 5: ESP protection in transport mode

The original IP packets are encrypted and authenticated as shown in fig.5. Transport mode permits encryption and authentication of the upper layer protocols (e.g. TCP segment), excluding the original IP header. A protected datagram is created by surrounding the original IP datagram data with header and trailer fields, and then, inserting the encapsulated data into the payload field of an IP datagram. The cipher algorithms, which may be used by the present security framework, are symmetric block algorithms such as DES, CAST, and Blowfish.

The SGSN that the MS is registered with, encapsulates through GTP the already encrypted IP packets coming from the MS, examines the PDP context, and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates (GTP) the packets, and applies NAT on them. The NAT implication at the GGSN node in the VPN operation is analyzed in detail in the following section. Then, the packets are forwarded to the public IP network and the latter delivers them to the SG at the private LAN.

Upon receiving protected IP packets, the SG terminates the IPsec tunnel, decrypts the packets and forwards them to the inner LAN destination. Because NAT is employed, the SG changes the destination address in the IP header. The NAT employment within the SG has no impact on the IPsec operation, since IPsec is located at the public address space, and thus, the combination of IPsec with NAT is feasible without any incompatibility problems [28].

Whenever the remote server at the private LAN sends IP packets to the MS, the SG receives these packets, changes their source IP address (NAT), and then, maps them to the appropriate SA. The encrypted packets are forwarded through the IP network and are routed to the GGSN (the home-GGSN of the MS). The MS's IP address, which has been assigned by the home-GGSN, has the same network prefix as the IP address of the GGSN. The encapsulates (GTP) the incoming IP packets and tunnels them through either the intra-PLMN or inter-PLMN GPRS backbone (in case of roaming) to the appropriate SGSN. The SGSN decapsulates the packets and delivers them to the MS.

In Fig. 6, the employed protocol stack for the end-to-end VPN scenario over the GPRS mobile network is depicted.

4.5 GTP implication

Communication between the GSNs is based on IP tunnels [17]. This means that standard IP packets, as soon as they reach a GSN node, are encapsulated in new IP packets and routed accordingly. GTP [11] is an integral part of the GPRS technology and operates transparently for the VPN services. A potential problem that may arise from the GTP employment in the specific end-to-

end VPN scenario concerns performance issues. More specifically, the duplicate encapsulation of the original IP packet (IPsec and GTP) for the secure transmission over the GPRS network, induces a waste of valuable resources, and may cause network efficiency problems and performance degradation.

4.6 NAT implication

Generally, the use of NAT is quite troublesome in conjunction with IPsec, since the later either hides private addresses through encryption and thus let them escape translation, or it experiences integrity violations as a consequence of the NAT manipulating protected IP addresses [21].

In this particular VPN scenario, there are two points (GGSN and SG) where NAT may be applied. The SG at the private LAN combines both IPsec and NAT functionality in the same box. By far this is the easiest way to avoid problems, i.e. by placing the IPsec endpoint in the public address space (NAT before IPsec) [29], and thus, the coexistence of IPsec with NAT doesn't raise any incompatibility problem.

On the other hand, the NAT at the GGSN takes place between the VPN termination points (MS and SG), contrary to the aforementioned rule, and therefore, a number of the potential incompatibilities may arise [28, 29, 30]:

- incompatibility between IPsec authentication and NAT.
- incompatibility between TCP checksum and NAT
- incompatibility between IKE address identifiers and NAT

ESP employs a message digest algorithm for packet authentication, but unlike AH, the created hash does not include the outer packet header fields (see Fig. 5). This enables the GGSN node to modify the original IP header without experiencing IPsec integrity failure.

When TCP is involved in data transmission – as happens in this scenario – then, an incompatibility problem between TCP and NAT occurs. Because NAT modifies the TCP packet, it must also recalculate the checksum used to verify integrity. If NAT updates the TCP checksum, the ESP authentication will fail. If NAT does not update the checksum, then TCP verification will fail. Therefore, the TCP checksum should be turned off. In other words, ESP can pass through NAT in transport mode with TCP checksums disabled or ignored by the receiver [29]. It is worth noting that, since IPsec traffic is integrity protected and authenticated using strong cryptography, modifications to the packet can be detected prior to checking TCP checksums. Thus, checksum verification only provides assurance against errors made in internal processing [29].

Another solution to the TCP incompatibility problem would be the use of UDP encapsulation. In this approach, the IPsec packets are encapsulated in UDP prior to being sent. The receiver discards the outer IP header and the UDP encapsulation disregarding any changes that may have been made by NAT [33].

Further to the aforementioned solutions, IETF is now defining a NAT alternative called Realm-Specific IP (RSIP) [31, 32] that may prove friendlier to IPsec. With RSIP, the IP payload flows from source to destination without modifications that may cripple IPsec. To do this, the host wraps the original packet inside a privately addressed outer packet. This encapsulation can be accomplished using any standard tunneling protocol. Upon receipt, the RSIP gateway strips off the outer packet and forwards the original packet across the public network towards the destination linking a private network to Internet.

Finally, concerning the incompatibility between IKE address identifiers and NAT, the proposed VPN scenario employs the IKE in AM, because it uses identification data instead of IP addresses for end-node authentication. The same authentication method should also be used during the quick mode of IKE negotiation, in order to eliminate the incompatibility problems between IKE address and NAT.

4.7 Mobility implication

The mobile subscriber may freely move within the GPRS coverage area maintaining both, network connectivity, and VPN service provision. The main task of location management is to keep track of the user's current location, so that incoming packets can be routed to his MS.

When the MS moves to a routing area (RA) that is assigned to the same SGSN, the later has already stored the necessary user profile and assigns a new packet temporary mobile subscriber identity (P-TMSI) to the user. Since the routing context does not change, the VPN between the MS and the SG remains the same.

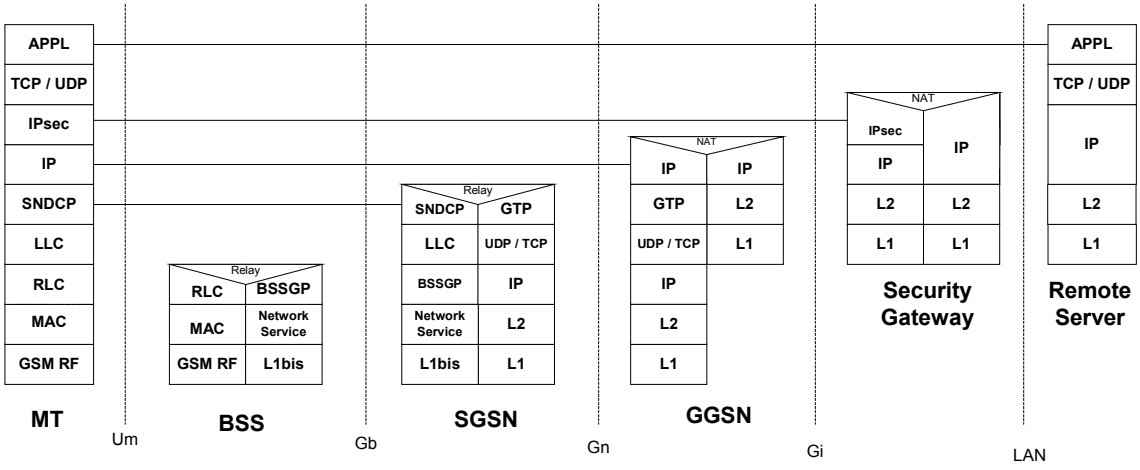

Figure 6: End-to-End VPN protocol stack

In case that the new RA is administered by a different SGSN than the old, the new SGSN realizes that the MS has changed to its RA and requests the old one to send the PDP contexts of the user. Afterwards, the new SGSN informs the involved GGSN, HLR and optionally the MSC/VLR about the user's new routing context. However, the VPN operates just over layer 3 and none of the security parameters, which are contained within the IPsec SA, has been changed.

Therefore, the VPN operates transparently regardless of the MS's movement and the GMM procedures.

5. VPN SCENARIO EVALUATION

5.1 MS characteristics

Before evaluating the proposed VPN scheme over the GPRS mobile network, it is worth mentioning the MS's key characteristics. As outlined in [15], the following are the main constraints on lightweight mobile devices:

- Low CPU processing power.
- Limited battery power.
- Limited memory capacity.
- Communications bandwidth latency
- Small screen size
- Limited input capabilities
- Operating System's (OS) restrictions

5.2 Advantages

From the customers' point of view, end-to-end VPN connections provide the best security. Traffic is encrypted at the VPN client and decrypted at the corporate SG, thus, the traffic remains encrypted for the entire connection. Authentication is also in the hands of the mobile subscribers.

The required security enhancements have a minimal impact on the existing network infrastructure. More specifically, the GPRS core network nodes and the intermediate IP routers require no further enhancements or modifications to support the specific VPN scenario. The necessary changes are limited to the security endpoints (MS and SG). Consequently, this setup does not place an additional signalling burden on the mobile network.

In the scenario presented here, the mobile subscriber can access the Internet from any capable GGSN, and thus, can choose the cheapest access. Also, user traffic flows encrypted all the way from the MS to the corporate SG, which means that it is charged as normal data traffic.

Additionally, any flow constraint is imposed to the encrypted traffic. All traffic that has security services applied to it goes through the two peering security endpoints, regardless of the intermediate routes that may follow. This allows for the encrypted traffic to be treated according to the network policy routing mechanisms for congestion confinement, without affecting the encryption process.

Finally, as a consequence of the VPN transparency to mobile network operation, mechanisms such as the GTP and the GMM do not cause any incompatibility problem.

5.3 Drawbacks

The main drawback of the proposed end-to-end VPN scheme, derive from the fact that each MS must have the appropriate software (IPsec) in order to apply the required security policy.

The use of IPsec imposes computational costs on the hosts that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, and the computation of integrity check values, encryption and decryption, and is added in a per-packet fashion [13]. Considering the aforementioned constraints imposed by the nature of the mobile devices (low CPU processing power, limited battery power and limited memory capabilities), it can be perceived that IPsec integration in MS is quite troublesome. The computational overhead of applying IPsec at the MS will be manifested by increased latency, and possibly, by reduced throughput.

Another essential issue is that the user must be aware of when encryption is required. End-station software may require the user to make decisions and configure the appropriate security policy. Generally, in this scenario the SA configuration may not be transparent for the mobile subscriber.

The use of IPsec also imposes bandwidth utilization costs on data transmission due to the increase in the packet size from the addition of the ESP headers [13]. It is anticipated that the increased bandwidth demand will not noticeably affect the Internet infrastructure, however it will have significant influence over the radio IF. Furthermore, GPRS employs specific authentication and ciphering procedures, which are optimised for packet data transmission over radio IF, between the MS and the SGSN [4, 5, 8]. Therefore, the proposed end-to-end VPN scheme duplicates encryption (packet encapsulation) over the expensive radio IF, which increases the communication cost and decreases the overall access network efficiency.

Finally, the end-to-end scenario tends to cause problems when NAT is used, which is the case in most mobile remote access VPNs. Traditional IPsec solutions will not allow NAT for many reasons.

5.4 Summary – Future work

One can conclude that, when security is the main concern, the end-to-end VPN is an attractive solution. In table 1, the evaluation of the proposed scenario is presented in a tabular form.

End-to-End VPN scenario	
Advantages	*Drawbacks*
Best security for end users, authentication in their hands	VPN operational constrains because of MS limitations.
Minimize mobile network enhancements	User awareness of when and what encryption is required
No further signalling burden on mobile network	Transmission overhead on radio interface
Encrypted traffic is charged and treated as a normal traffic	Duplicated encryption between MS and SGSN
VPN transparency regarding GTP and GMM procedures	NAT incompatibilities

Table1: End-to-End VPN scheme's features

An alternative solution to the end-to-end VPN would be a network-based VPN. Under this approach, the VPN functionality is outsourced to the GSN nodes and therefore, the main drawbacks, which pertain to the end-to-end scheme, can be confined. However, the network-based VPN places the IPsec functionality within the GPRS core network, and thus, introduces a further burden on it. Additionally, the biggest consideration is that the VPN operation is not directly under the end user control

6. CONCLUSIONS

In this paper, an end-to-end VPN scenario deployment over the GPRS mobile network has been presented and analyzed. The VPN deployment is based on the IPsec protocol suite. Specific protocol configuration of the complex IPsec framework is proposed, in order to make it operational in a mobile network environment. The potential incompatibility problems that may arise from the integration of different technologies have been elaborated. Finally, a qualitative evaluation of the proposed VPN scheme has been presented, and an alternative network-based VPN scheme has been outlined for future work.

REFERENCES

[1] M. Mouly and M.B. Pautet, The GSM System for Mobile Communications, 1992.

[2] GSM 03.02, Network architecture, 1998

[3] GSM 03.60, GPRS, Service Description, 1998.

[4] GSM 03.20, Security Related Network Functions, 1998.

[5] GSM 02.09, Security Aspects, 1998.

[6] GSM 09.61, GPRS, General requirements on interworking between the PLMN supporting GPRS and PDN, 1998

[7] GSM 03.03, Numbering Addressing and Identification, 1998.

[8] GSM 04.64, GPRS; Mobile Station-Serving GPRS Support Node (MS_SGSN) Logical Link Control (LLC) Layer Specification, 1998.

[9] "Understanding IPsec protocol suite" ALCATEL Technical paper, Oct 2000.

[10] GSM 02.60, GPRS; Service Description, 1998.

[11] GSM 09.60 GPRS, GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface, 1998.

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

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

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

[15] Samantha Donovan, et. all "VPN and lightweight clients" Elsevier Science, Information Security Technical Report Vol 6, No 1, March 2000

[16] Stallings W., "IP Security" Cisco, The Internet Protocol Journal, vol 3, No 1, March 2000.

[17] C. Perkins, "IP Encapsulation within IP" RFC 2003, May 1996

[18] R. Thayer, N. Doraswamy and R. Glenn, "IP Security Document Roadmap" RFC 2411, Nov 1998

[19] S. Kent and R. Atkinson, "IP Authentication Header" RFC 2402, Nov 1998

[20] S. Kent and R. Atkinson, "IP Encapsulation Security Payload (ESP)" RFC 2404, Nov 1998

[21] Michael Borella, "Methods and Protocols for Secure Key Negotiation Using IKE", IEEE Network, July/August 2000.

[22] D. Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, Nov 1998.

[23] H. Orman, "The OAKLEY Key Determination Protocol," RFC 2412, Nov 1998

[24] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407, Nov 1998.

[25] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Info. Theor*y, vol. 22, Nov 1976

[26] N. Ferguson and B. Schneier, "A cryptographic evaluation of IPsec", Jan 2000, available from http://www.counterpane.com/ipsec.html

[27] Georgina Schafer, "Placement of Intelligence Within Networks to Provide Corporate VPN Services", Elsevier, Information Security Technical Report, vol 6, No 1, March 2000.

[28] Phifer, L., "IP Security and NAT: Oil and Water?" ISP-Planet, June 15, 2000 available from http://www.isp-planet.com/technology/nat_ipsec.html

[29] Bernard Adoba, IPSec-NAT, Compatibility Requirements draft-ietf-ipsec-nat-reqts-00.txt, Internet Draft (work in progress), June 2001.

[30] Nicolas Gabriel "VPN and Firewall Traversal" Nov 2000.

[31] Phifer, L., "Realm-Specific IP for VPNs and Beyond" ISP-Planet, June 23, 2000 available from http://www.isp-planet.com/technology/rsip.html

[32] Borella M., Grabelsky D., Lo J., Taniguchi K., Realm-Specific IP:Protocol Specification" Internet Draft (work in progress) draft-ietf-nat-rsip-protocol-07.txt, July 2000.

[33] Huttenen, A, Sie J, Micr V, Di L, Ipsec "ESP Encapsulation in UDP for NAT Traversal" Internet Draft (work in progress) draft-huttenen-ipsec-esp-in-udp-01.txt, March 2001.

[34] Egevang, K. and Francis, P., "The IP Network Address Translator (NAT)," RFC 1631, May 1994.

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