GPRS security

Ksenia Orman

Nowadays wireless mobile communications are very popular among masses. It is easily explainable: people are getting very busy; business traveling becomes a very essential problem which requires a great deal of communication facilities as well as at home, and at the office or outdoors. Mobile phones are very handy for this purpose.

This work is based on two articles mostly:

1. "Authentication and Security in GPRS Environment: An Overview" by Lasse Houvinen
2. "GSM and GPRS Security" by Chengyuan Peng.

More information about these articles and other literature, used in this work, can be found in the References. Some pictures were taken from the master work [1] for better overview.

I will not going to repeat GSM security during this seminar, but a short overview of GPRS security will be given. General Packet Radio Service (GPRS) is a Mobile Data Service available to GSM users of second-generation (2G) mobile phones.
GPRS was developed by European Telecommunication Standards Institute (ETSI). One of the main goals of GPRS design was to support burst data transfer and occasional transmission of large amounts of data economically. GPRS operates with other secured or unsecured networks both. However data transmission security should not be neglected.
Although GPRS is considered to be a GSM service, it has its own core network, with shared radio channel between these two services. GPRS core network is attached to GSM radio channel via open interface. Additionally, GSM may utilize GPRS to achieve better performance and GPRS users may use some of GSM supplementary services from the other side. There is a possibility to build a GPRS network separately from GSM. In such case GPRS network needs its own radio channel.

There are five main areas shown on the next figure, where security of GPRS system is exposed:

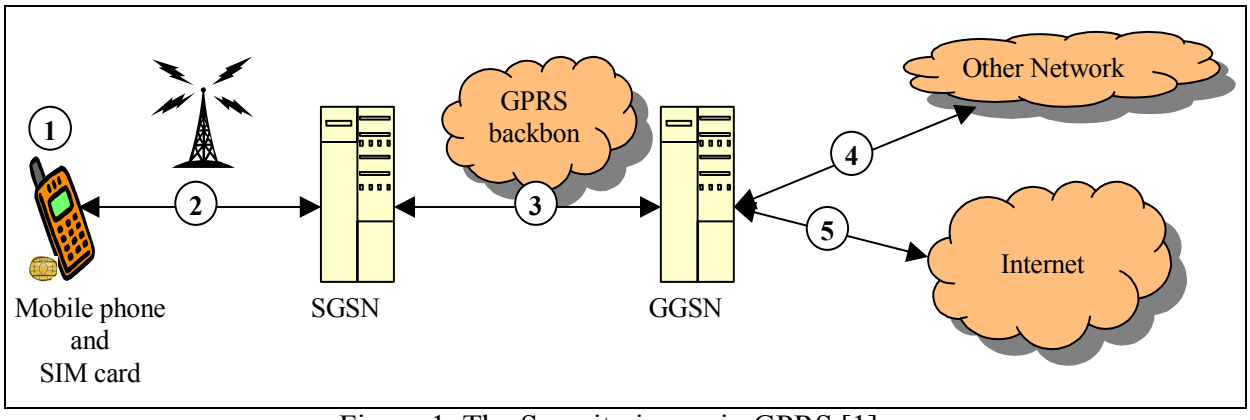

Figure 1. The Security issues in GPRS [1]

1. Mobile phone and SIM card security.
   Authentication of subscriber identity in the network, data confidentiality over the air interface, and file access conditions are supported by security features of the SIM card.

2. Security mechanics between the MS and the SGSN. These includes air interface between MS and BSS.
3. GPRS backbone (traffic between SGSN and GGSN) network security.
4. Security between different operators.
5. Security between GGSN and the external connected networks, like Internet.

Next Figure 2 illustrates structure of GPRS system architecture.

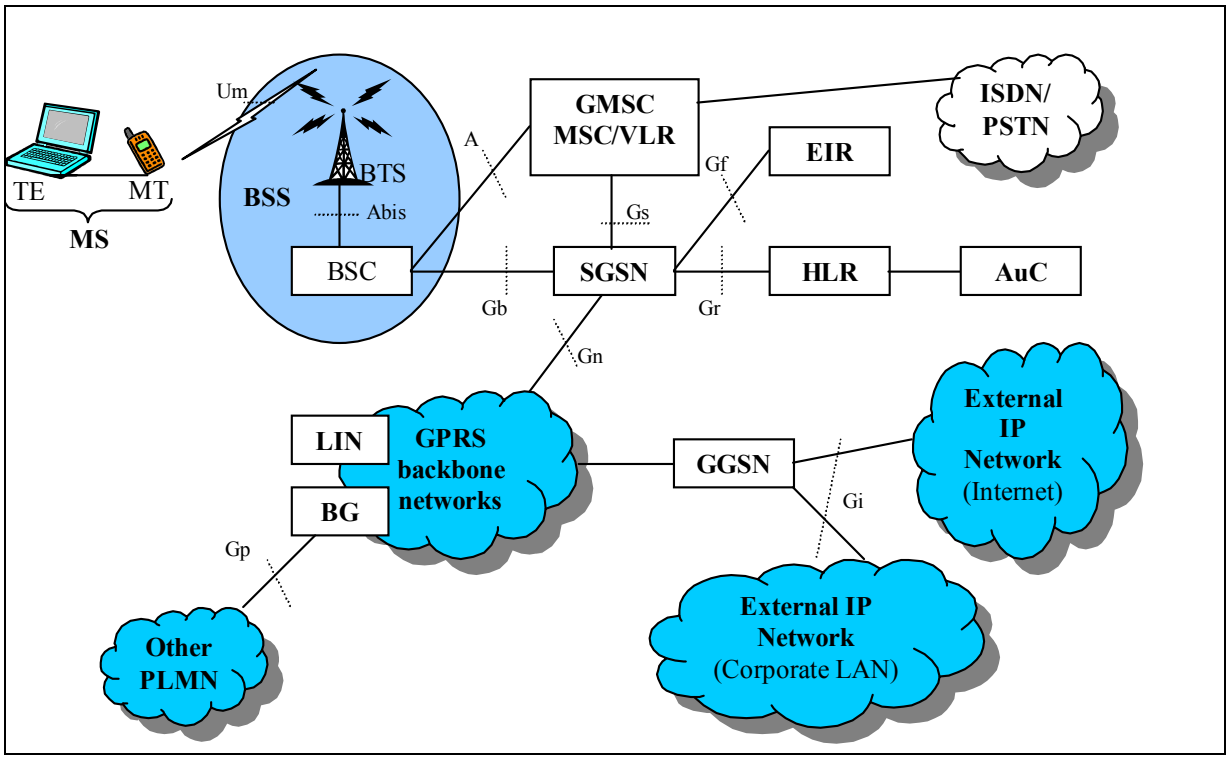

Figure 2. GPRS system architecture [1]

MS – Mobile Station

There are three types of GPRS mobile stations: Class A, Class B and Class C.
Class A can be connected to GPRS and GSM (voice, SMS), using both services at the same time. Class B can be connected to GPRS and GSM using only one of the services at the same time. When GSM service is active, GPRS is suspended; it is activated automatically after GSM service switched off. Most GPRS mobile devices are of Class B. Class C devices are connected either to GPRS service or GSM. Thus the Class C mobiles can be attached either to the GSM or to the GPRS network but not to both at the same time.

BSS – Base Station System

The Base Station System (BSS) consists of Base Station Controller (BSC) and Base Transceiver Station (BTS).

The BTS is the radio equipment that transmits and receives information over the air and lets the BSC to communicate with MSs in the BSC service area. A group of BTSs is controlled by the BSC. The BTS must contain GPRS-specific software.

SGSN – Serving GPRS Support Node

The SGSN is one of the main components of the GPRS network. The main functions of the SGSN are to handle MS registration and authentication into the GPRS network as well as manage MS mobility, relay traffic, collect statistics and charge information.

GGSN – Gateway GPRS Support Node

The GGSN is the interface between GPRS backbone and external data network. Like SGSN, it is a primary and new component in GSM network using GPRS. The functionality of the GGSN is similar to router in data networks. It routes end user data from external data networks to the SGSN and serves as destination between MS and mobile originated data to the external data networks and SGSNs.

BG – Border Gateway

BG is a part of GGSNs. The main function of the BG is to ensure a secure connection between different GPRS networks over the inter-operator backbone. The BG could consist of a firewall, security functions and routing functions. BGs as well as their functionality are selected by the GPRS operators mutual agreement to enable roaming.

HLR – Home Location Register

The main function of the HLR is to store MS profiles. It is the database that holds subscription information for every person who has bought a subscription from the GPRS operator. Information found in the HLR includes, for example, supplementary services, authentication parameters, Access Point Name (APN) such as the subscribers Internet Service Provider (ISP), and whether a static IP address is allocated to the MS. In addition, the HLR includes information about the location of the MS. Subscriber's information is exchanged between HLR and SGSN for GPRS. Note that the authentication triplets are retrieved directly from the HLR to the SGSN.

AuC – Authentication Centre

The AuC includes information for identifying authorized users of the GPRS network and preventing unauthorized use of the network both. AuC is often considered as a physical part of the HLR.

EIR – Equipment Identity Register

In the EIR each mobile device is listed like in GSM: black list for stolen mobiles, grey list for mobiles under observation, and a white list for other mobiles.

LIN – Lawful Interception Node

The LIN is used to collect information about some pre-defined subscriber or subscribers. The information could include, e.g., the data sent and received by the interception target, location information, and subscriber information. The lawful interception is an action based on the law, which is performed by the GPRS network. The GPRS network has to be able to deliver required user data and other network related information to the Law Enforcement Agency (LEA), whenever wanted.

GPRS backbone networks

The GPRS backbone network can be either intra- or inter-operator network. The main function of the intra-operator backbone network is to connect to single operator's GSM. The inter-operator backbone network connects GPRS operators and provides international GPRS roaming. GPRS backbone networks are IP based.

The intra-operator GPRS backbone network is implemented as a set of local area networks (LAN) connected with routers. In most cases, the intra-operator backbone is a private network to ensure the security and good performance. Private IP addresses can be used in the intra-operator backbone because addresses are not visible outside of the network.

The inter-operator GPRS backbone network can be based on either public (e.g., Internet) or private (dedicated) IP network. They are implemented as a wide area network connecting intra-operator backbone networks using routers. It is chosen by the GPRS operators' mutual agreement to enable roaming. All the interconnected GPRS backbone networks comprise one big network and therefore the IP address allocation must be coordinated.

User Authentication and Security inside GPRS Network

The user authentication procedures in GPRS are similar to procedure in GSM. The difference is that the procedures are executed from the SGSN instead of the MSC.
The primary function of the SIM in conjunction with a GPRS network is to authenticate an MS before it gets access to the network. The SIM contains the IMSI, K_i, the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GPRS A5 algorithm is implemented in the Mobile Equipment (ME) together with the International Mobile Equipment Identity (IMEI) that is physically secured in the ME.

The subscriber authentication procedure is illustrated in Figure 3.1, 3.2, 3.3, 3.4, 3.5.

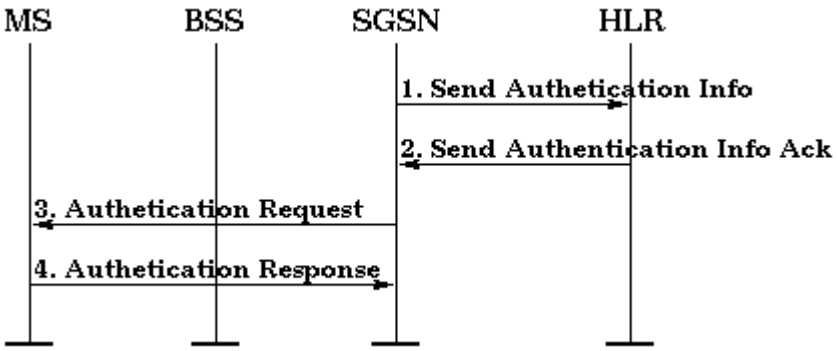

Figure 3.1 GPRS authentication procedure. [2]

If the SGSN does not have previously stored authentication triplets, they are acquired from the HLR by sending message *Send Authentication Info*. The HLR responds with *Send Authentication Info Ack* message and now the SGSN has the authentication triplet. When the SGSN has the authentication triplet it sends message *Authentication Request* including RAND to the MS and the MS computes SRES from RAND and secret Subscriber authentication key K_i. The MS then sends *Authentication Response* including SRES to the SGSN and if the SRES computed by the HLR equals to the SRES computed by the MS, the MS is considered to be authenticated to use the network. During authentication procedure the SGSN informs to the MS whether ciphering is used or not. If ciphering is wanted to use the MS starts ciphering after sending *Authentication Response* message and the SGSN after receiving a valid *Authentication Response*. It is important to note that all security functions inside the GPRS network are based on the secrecy of the secret key K_i. K_i is Individual Subscriber Authentication Key. The length of K_i is 128 bits. It is stored into the SIM (Subscriber Identification Module) card and into the HLR at subscription time and it is not known by the subscriber.

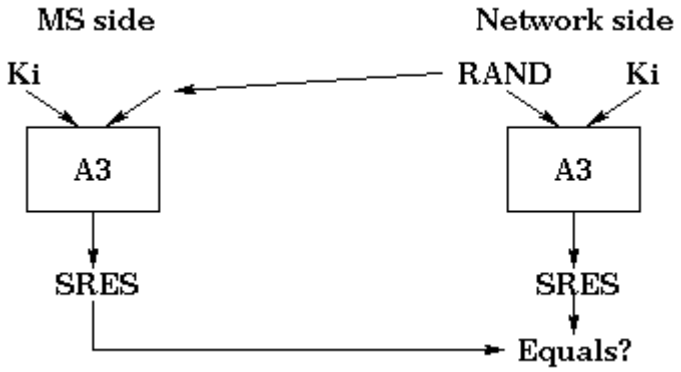

Figure 3.2 Authentication computation [2]

The use of A3 is shown in the Figure 3.2. A3 is the authentication algorithm.
Different operators have the choice to use the ETSI algorithm A3 or they can use an applicable A3 algorithm to their subscribers. The purpose of the algorithm A3 is to allow

authentication of a mobile subscriber's identity. The algorithm A3 must compute an expected response SRES from a random challenge RAND sent by the network. For this calculation, algorithm A3 makes use of the secret authentication key K_i
.

Ciphering

In GPRS data and signalling during data transfer are ciphered. The ciphering method is GPRS Encryption Algorithm (GEA) which is a secret algorithm. The scope of ciphering in GPRS is from the ciphering function at the SGSN to the ciphering function in the MS in contrast to the GSM ciphering which is a single logical channel between the BTS and MS as illustrated in Figure 3.3:

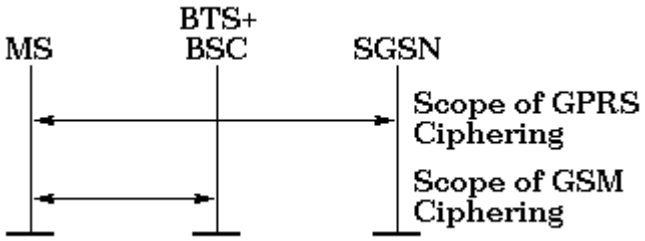

Figure 3.3 Scope of ciphering [2]

Mutual key setting is the procedure that allows the MS and the network to agree on the key K_c to use in the ciphering and deciphering algorithms. The K_c is handled by the SGSN independently from the MSC. If the MS is able to use both GSM and SGSN services then it have two different keys one in the MSC and one in the SGSN. Key setting is triggered by the authentication procedure, but the network may initiate key setting as often as the operator wishes. Key setting procedure is not encrypted and shall be performed as soon as the identity of the mobile subscriber is known by the network. The transmission of the K_c to the MS is indirect and uses the authentication RAND value. K_c is derived from RAND using algorithm A8 and Ki as illustrated in Figure 3.4. The maximum length of K_c is only 64 bits. After computation the key is stored by the MS until it is updated at the next key setting.

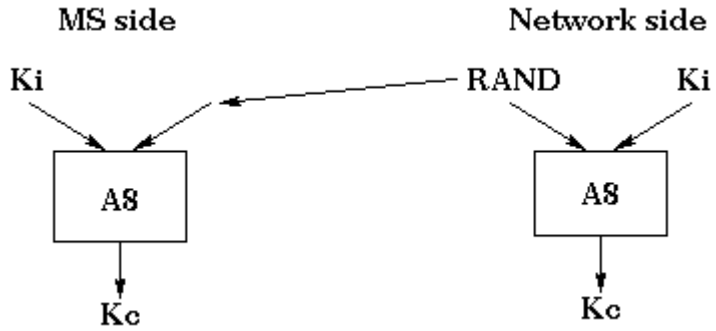

Figure 3.4 K_c computation [2]

K_i Individual Subscriber Authentication Key.
The length of K_i is 128 bits.

A8 The ciphering key generating algorithm.

The A8 algorithm is using the K_i together with the 128 bits authentication RAND to generate the 64 bits Ciphering Key, GPRS- K_c.
The GPRS-A5 algorithm is used for ciphering the data and signalling during data transfer. The range of ciphering in GPRS is from the ciphering function at the SGSN to the ciphering function in the MS. The enciphering stream at one end, and the deciphering stream at the other end, must be synchronized for the enciphering bit stream and the deciphering bit streams to coincide. Synchronisation is guaranteed by driving GPRS-A5 algorithm's explicit variable INPUT per established LLC (Logical Link Control) and DIRECTION, this is illustrated in Figure 3.5. *INPUT* is the sequence number of the LLC packet and its initial value is selected by the network. *DIRECTION* is either from the MS to the network or from the network to the MS allowing *INPUT* to be identical in both directions. The output of the GPRS-A5 is exclusive with the clear text at the sending end and with the ciphered text at the receiving end.

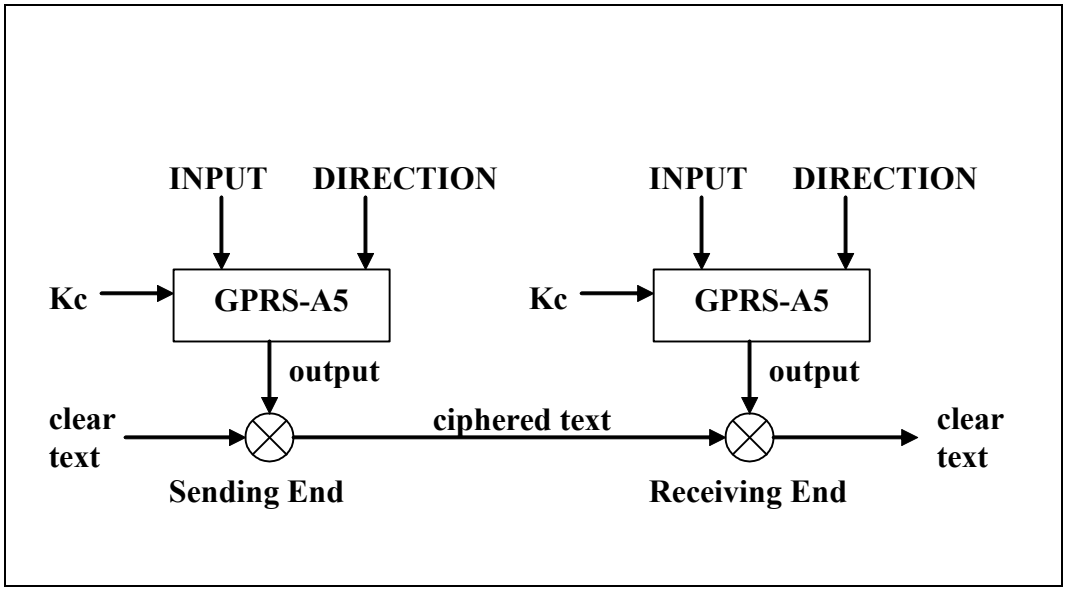

Figure 3.5 Ciphering process [2]

Identity protection

The identity of the user is protected to avoid the possibility for intruder to identify which subscriber is using a given resource on the radio path by listening to the signalling exchange or the traffic. As a condition to accomplice this the IMSI (International Mobile Subscriber Identity) or any other information allowing a listener to derive the IMSI easily, should not normally be transmitted in clear text in any signalling message over the radio path. It is from a security point of view necessary that on the radio path a protected identifying method is used instead of the IMSI. The IMSI should not normally be used as addressing means. But when signalling procedures permit it, signalling information elements that can expose information about the mobile subscriber identity must be ciphered for transmission.

Secure GPRS Interworking with Packet Data Network

GPRS supports interworking with packet data networks (PDN) and more specifically with IP. These interworked IP networks may be either the Internet or intranets. GPRS is able to operate with IPv4 and new IPv6.

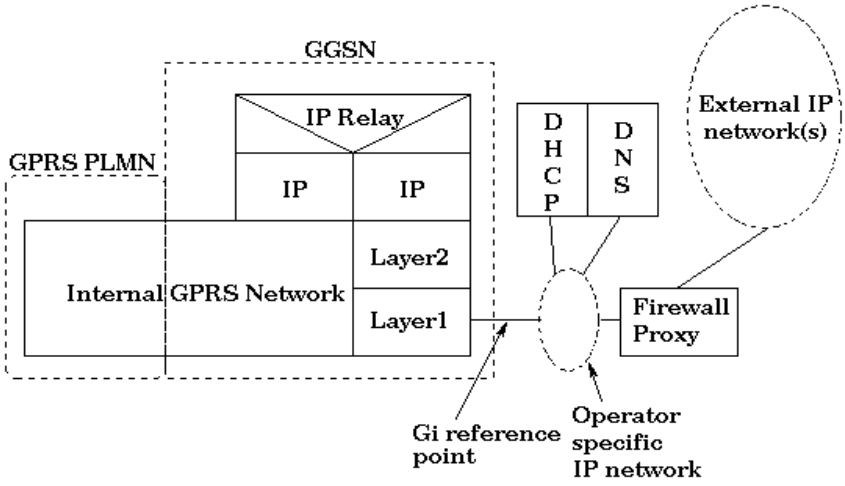

Figure 4. IP network interworking [2]

Figure 4 illustrates the Gi reference point and protocol stack needed for GPRS interworking with IP networks. The Gi reference point is located between the GGSN and the external IP network. From the external point of view, the GGSN is seen as a normal IP router and can been seen in Figure 4. The Layer1 and Layer2 protocols are operator specific and are negotiated between e.g. a GPRS operator and an external IP network operator.

Between the GGSN and the external IP network the following assumptions are valid in generic case:

- A firewall is configured by the GPRS operator. Basically, all applications based on IP are supported but the GPRS operator may restrict their usage. Also, in most cases it is necessary to restrict access from the external IP networks to GPRS network.
- A domain name server is managed by GPRS operator or it can be managed by operator of external IP network operator.
- The GGSN may allocate dynamic PDP addresses by itself or use an external device such as dynamic host configuration protocol (DHCP) server which can be operated, e.g., by external IP network operator.

Transparent access to Internet

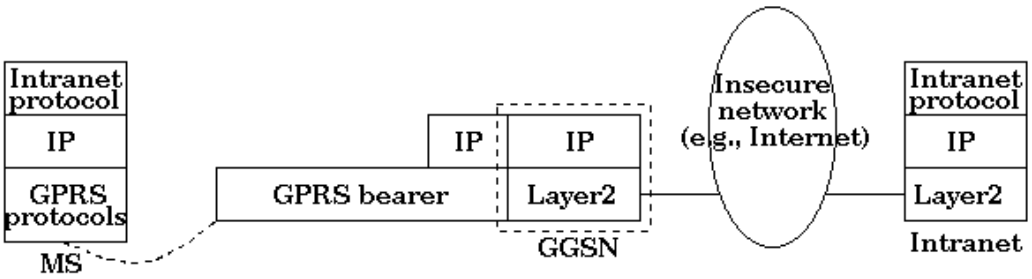

Figure 5. GPRS transparent access [2]

The MS is given an address belonging to the operator's addressing space. The address is either a static address given at subscription time or a dynamic address given at PDP context activation. The received address is used as for packet forwarding between the Internet nodes and GGSN as to map packet within GGSN.
The MS does not need to send any authentication request at PDP context activation or participate in user authentication or authorization processes.
The user authentication and data encryption are completed within the "Intranet protocol" only if one of them is required. This is shown in Figure 5.

Non-transparent Access to Intranet or ISP

The MS receives an IP address which belongs to the address space of the intranet or Internet service provider (ISP). In the same way as the transparent access, the address is either static given at subscription time or dynamic given at PDP context activation. This received address is used for packet forwarding within GGSN, Intranet or ISP. This requires a link between the GGSN and address allocation server belonging to the Intranet or ISP again. Information that is used for the authentication request from GGSN to Intranet or ISP comes from the user in the PDP context activation. The GGSN requests user authentication and configuration from a server.

The connection between GPRS network and ISP can be arranged over any network, even through an insecure one, such as Internet. In case of an insecure connection a dedicated link or a special secured tunnel can be arranged using e.g. IPSec as a security protocol. The security protocol is defined by mutual agreement between the GPRS PLMN operator and the Intranet or ISP administrator.

Threats from the External Networks.

The threats to GPRS differ from the Circuit Switched GSM. The security threats to GSM are quite limited, there are not too many hackers that can or attempt to crack the obscurity SS7 protocol. The GPRS systems are a much more exposed to intruders, because of it IP based backbone. There are a lot of people who have thoroughly knowledge about the TCP/IP in proportion to the SS7.

There are such threats as:

- Integrity of data
- Stolen terminal and SIM card
- Borrowed terminal and SIM card
- Eavesdrop, masquerade or manipulate
- Confidentiality of user data and authentication data
- Cloned SIM card
- Non-type approved terminals and defective equipment

Inside the GPRS network all information, such as subscriber information and routing tables, is in clear text format and not protected. Subscriber's information is confidential information. Also incorrect routing tables may cause huge economical losses for the GPRS operator. Therefore, it is very important to protect GPRS network from crackers making firewall (and GGSN) configuration very important. Another threat concerning configuration of the firewall

is denial of service attacks. If cracker is able to deny service at GGSN (or any other network element) financial losses for the operator will be enormous. Inside GPRS network cracker would be able to send GPRS signaling messages also and thus affecting behavior of the GPRS network and connections.

A cracker could cause huge bills for a GPRS user. In GPRS the billing will be based on the amount of the transferred data. Therefore, it may be possible to cause harm for a GPRS user by sending large spam emails (GPRS user also pays received data) from the external network or to create a virus (located in the user's laptop) which could send dummy packets from the MS without the user even knowing it.

Secure Interworking between GPRS Networks

The interworking between GPRS operators supports roaming. The GPRS subscriber is able to access from other operators GPRS networks (by visiting PLMN) to the home PLMN (HPLMN). There is shown a process of interworking between two GPRS operators on the Figure 6.

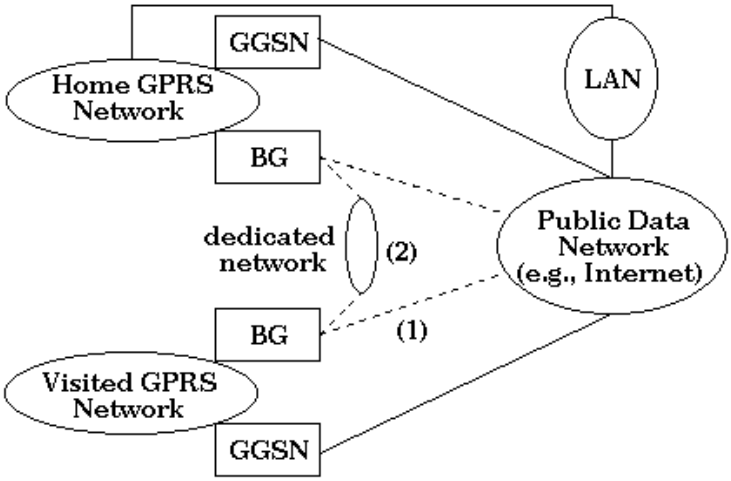

Figure 6. Interworking between GPRS networks [2]

GPRS networks are connected to each other via inter-operator backbone network. The inter-PLMN link can be any packet data network (1) (e.g., the Internet) or dedicated link (2). Dedicated link may be chosen to fulfill requirements of Quality of servise (QoS) and to improve security. All data and signalling between the GPRS operators are transmitted via BGs.

It is shown on the Figure 6, that when the subscriber is roaming in the Visited PLMN (VPLMN) data can be routed to its destination (LAN in this case) in several ways. The actual routing depends on the agreements between the GPRS operators and agreements between the HPLMN operator and the user.

If the subscriber has dynamic IP address then data may be routed via the HPLMN or directly to the LAN via the Internet. The choice depends on the afreements mentioned above. If the

subscriber has static IP address then data is always routed via HPLMN because the IP address points to the GGSN of the HPLMN.

Administrators must pay attention and be very careful when planning LAN protection. Unauthorized users should not have any access to the LAN.

In the case of roaming, the authentication process is done in the AuC of the HPLMN. The key Ki is kept secret all the time.

GPRS operators can enable IPSec and providing specifications for authentication and encryption as a basic set of security functionallity in its BGs. The other security protocols can be selected by the agreement between the GPRS operators.

IPSec

IPSec is an „Intranet protocol" that can be used to offer the GPRS subscriber to communicate over insecure public networks securely. It consists of several open standards and the main purpose of it is to ensure secure private communication over IP networks, e.g. the Internet. IPSec offers encryption and authentication on network layer.

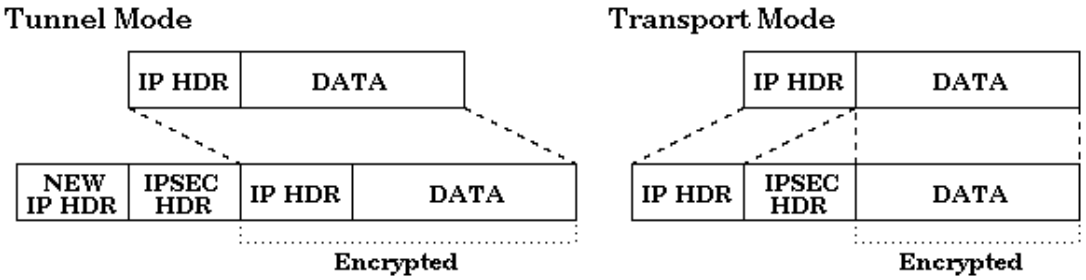

Figure 7. IPSec tunnel and transport modes [2]

Figure 7 shows IPSec operation modes: transport and tunnel.

Transport mode.

In transport mode only the message (payload) of the IP packet is encrypted. It is fully routable since the IP header is sent as a plain text. Transport mode is used for host-to host communications. This mode has the advantage to add only a few bytes to each packet.

Tunnel mode.

In tunnel mode, the entire IP packet is encrypted. It must then be encapsulated into a new IP packet for routing to work. Tunnel mode is used for network-to network communications (secure tunnels between routers) or host-to network and host-to-host communications over the Internet.

IPSec is an mandatory part of Ipv6 and is optional for use with Ipv4. While the standard is designed to be indifferent to IP versions, current deployment and experience concerns Ipv4 implementations.

Since the Internet Protocol does not basically provide any security capabilities, IPSec was introduced to provide security services such as:

- Encrypting traffic (so it cannot be read by non-intended for that parts)
- Integrity confirmation
- Authenticating the peers (ensuring that traffic is from a trusted part)
- Anti-replay (protection against replay of the secure session)

IPSec is implemented by a set of cryptographic protocols for securing packet flows and internet key exchange.

Conclusion

GPRS is „access networks" to other network which offer mobility. It gives possibility that travelling employees can communicate with corporate LAN very easily even being abroad. The system should offer authentication and security functions for possibility to use GPRS service for transmitting confidential or private data. GPRS offers ciphering function over the radio channel as well as authentication to the GPRS network. However, the operator must be very careful with its A3 algorithm, because if the authentication is not trustful a lot of damage could be caused. It does not mean that authentication works against copying of SIM. If it can be copied then unauthorized user can use the identity of the authorized user until the subscription invalidates.

The security of the transmitted data can not be kept cryptographically excellent because the decryption takes place in the SGSN and not in the BTS, and a new A5 ciphering algorithm has been implemented, security is improved. But it is possible to get the identity of the subscribers e.g. using the false BTS. This problem can lead to eavesdropping the other user's traffic. Subscribers should not trust security of the GPRS networks when transferring confidential data more than they do using Internet for the same purpose.

Abbreviations

AuC Authentication Center
BG Border Gateway
DNS Domain Name Server
GEA GPRS Encryption Algorithm
GGSN Gateway GPRS Support Node
GPRS General Packet Radio Service
GSM Global System for Mobile Communications
HLR Home Location Register
IP Internet Protocol
IPSec IP Security protocol
ISP Internet Service Provider
LAN Local Area Network
MS Mobile Station
PDN Packet Data Network

PLMN Public Land Mobile Network
SGSN Serving GPRS Support Node
SIM Subscriber Identification Module
SMS Short Message Service

References

[1] Geir Stian Bjan and Erling Kaasin. Security in GPRS, Master thesis, 2001 http://student.grm.hia.no/master/ikt01/ikt6400/ekaasin/ (last viewed 04.2007)

[2] Lasse Huovinen. Authentication and Security in GPRS Environment: An Overview. Department of Computer Science and Engineering, Helsinki University of Technology. http://users.tkk.fi/~lhuovine/study/netsec98/gprs_access.html (last viewed 04.2007)

[3] Chengyuan Peng. GSM and GPRS Security. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology. 2000