Security in GPRS

Master Thesis
in
Information and Communication
Technology

by
Geir Stian Bjåen and Erling Kaasin

Grimstad, May 2001

Security in GPRS

Abstract

GPRS offers the user an “always on” connection to Internet and Intranet. Some of the services may require high level of security. This can be financial transaction over the Internet, or exchange of confidential documents from a company’s Intranet to an employee. It is important to have strong focus on the security, so companies and persons that demand high level of security can take advantage of the services GPRS offered. What normally happens is that the services wins against the security. This is in most cases adequate security for what a normal subscriber requires.

This thesis covers which security functions that exists in GPRS, the threats it meets, how to avoid attacks, and the consequences for the attacked part. The thesis is also meant for the Ericsson AS’ employees as a supplement to their knowledge about GPRS security issues.

The GPRS has inherited most of the security threats that exists in the GSM system. In addition the GPRS encounter new and bigger challenges. This since GPRS employs IP technology and it is connected to the Internet. Threats to the GPRS are not only from the insecure public network, Internet. Attacks on the data at the air interface, or operators handling of data that are transmitted or stored in their network, can also be a threat.

Mobile terminals and GPRS equipment are the two main areas that need to be protected from the GPRS point of view. This also includes protection of subscriber information and other information that is stored in the GPRS network. Firewalls and Border Gateways are used to protect the mobile terminals and the GPRS equipment from external network and other operators network. The placements of firewalls are complicated because of the different connections it has to handle, and what routing procedure the GPRS operator uses. This thesis treats the subject of placement of firewalls.

During the work with the thesis we got the possibility to participate and execute tests on the GPRS system in order to evaluate its security. These tests were done at Ericsson AS’s test lab in Grimstad, and we choose to focus the test on how the new GPRS node in the operators network can be attacked. This thesis includes a description and the results from the test.

The results from the test gives an indication on how difficult it is to get access to the GPRS node, and what possibilities an intruder has if he gets access.

Preface

This postgraduate thesis is a part of the Master of Engineering degree in Information and Communication Technology at the Agder University College in Grimstad. This assignment is a closure on the education that lead to the Norwegian degree Sivilingeniør, which is equivalent to a Master of Science degree.

The assignment is given by Ericsson AS and gives a theoretical evaluation on the security in GPRS. It also contain a more thoroughly test on the CGSN component in GPRS. It has been a comprehensive and challenging task to complete this thesis, and it has required a lot of information collections and understanding.

This work is based on a co-operation with Fryvil Cecilie Heggelund Lia at Ericsson AS. We would like to thank Mrs Heggelund Lia for her time and for giving us excellent advises during the work.

Jan Peter Wiborg and Terje Morten Solvang at Ericsson AS were very supportive and gave us outstanding information related to our test against the security in GPRS.

We would also thank Ericsson AS and Stein Bergsmark at Ericsson AS that has made this thesis possible.

Grimstad
Spring 2001

Geir Stian Bjåen

Erling Kaasin

Contents

1 Introduction

1.1 Background

We are moving towards a society with great demands for the future. We would like to have the same facilities when we are travelling as we have at the office and at home. To meet our demands, the GPRS service has evolved from GSM to make high-speed data transmission possible.

The GPRS system offers high data rate packet switched connections and improves the utilisation of the network and radio resources. Compared to the circuit switched radio transmission, where single users occupy a complete traffic channel for the entire call period, GPRS allow multiple users to share one physical channel.

GPRS is designed to support from intermittent data transfers to occasional transmission of large volumes of data. It offers several quality of service profiles, and fast allocation of resources for packet transmission, normally 0,5 to 1 second. Charging is typically based on the amount of data transferred [14].

One of the facilities that GPRS offers is connection to the Internet. Since the GPRS is using IP technology to communicate over the Internet, the GPRS systems meets challenges to keep a satisfying security for the subscribers and the operators network elements. Even at the first glance it seems to be sufficient to protect the GPRS system from attacks initiated from the Internet, but the GPRS system is much more complex and attacks to other parts of the system is also a realistic threat.

It is important to take care of the security and protect the subscribers and the different network elements against intruders that want to harm or take advantage of the damage.

This thesis is basically a theoretical study about how the security is covered, what threats the GPRS system meets, what are the consequences of attacks and what can be done to take care of the security. We have also done a test in Eriksson AS's lab environment. The test is focused on the possibilities for an intruder to get illegal access to GPRS nodes.

1.2 The Thesis definition

Project title:

Security in GPRS

Purpose of the Project:

The purpose of this project is to identify insecurity in the GPRS system. How can the weaknesses in the GPRS system be attacked and what are the consequences due to these intrusions? Also estimate the possibilities to avoid security attacks.

Definition of the Project:

This task will be closely tied up towards the development of GPRS (General Packet Radio Service) application ongoing at Ericsson AS in Grimstad.

The subject is mainly a theoretical evaluation and the following issues will be outlined:

- Literature studies of security in GPRS; what security mechanisms exists today and are the security functions sufficiently covered
- What risks threatens the security in the GPRS network, how is this attacks accomplished and what are the consequences of this intrusion
- What are the weaknesses with this kind of IP-networks
- Is it possible to improve the security and how much does it cost to accomplish these improvements?

1.3 Limitation of the Thesis

Early in the project period we agreed, together with our supervisor Fryvil Cecilie Heggelund Lia, to drop the cost estimation on how to improve the security. This was done because the cost estimation itself is a large issue and it is also outside our course of study.

1.4 A overview of the security in GPRS

1.4.1 Introduction

The GPRS is a new service that is offered to the mobile phone users. Netcom and Telenor, who are the two largest operators in Norway introduced GPRS on January 31 and February 1, 2001. So far it is just a small number of mobile phone on the marked that supports GPRS and it is also difficult to get hold of a mobile phone. The operators offer a limited numbers of services to the GPRS costumers. One of the services that GPRS is supporting today is the MobilMail. MobileMail is possible to use with the entire mobile phone that use WAP, but with the GPRS functionality “always on” the email service MobileMail is more attractive [27].

It is important that the security is taken care of. This is because the users; both private persons and companies, can feel safe and use the services that the operators offer. Services that demand a high level of security could be financial transactions, transfer of medical information or exchange of personal e-mail messages.

In the next two subchapters we have explained which part in the GPRS system we are focusing on and the test we did in the Ericsson AS’s lab environment.

1.4.2 Security issues in GPRS

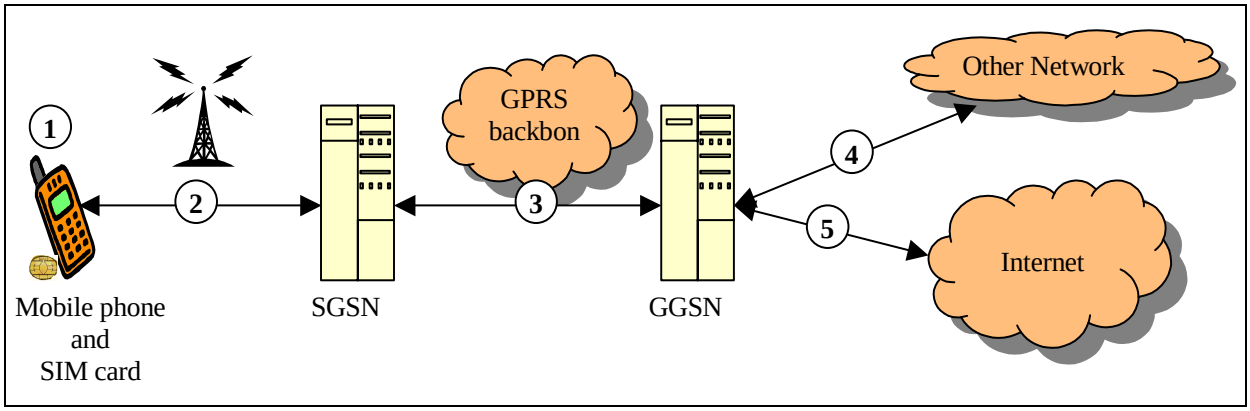

Figure 1.1 The security issues in GPRS

From the figure there are five main areas where security in the GPRS system is exposed. These five areas are:

1. Security aspect related to the mobile phone and the SIM card.
2. Security mechanics between the MS and the SGSN. These include also the air interface from the MS to the BSS.
3. The PLMNs backbone network security that mainly referred to the traffic between the SGSN and the GGSN. But also handling the flow of subscriber information, like triplets between the HLR and SGSN.
4. Security between different operators.
5. Security between GGSN and the external connected networks, like Internet.

1.4.3 Testing the security of the CGSN

This Thesis also includes a description of a test done at the Ericsson security lab in Grimstad. It will describe how to reveal weaknesses that can lead to a security breach in the GPRS system. Included is also a part with a general overview of how an intruder usually will prepare a system attack by taking advantage of the weak points.

1.5 Method and report outline

In the beginning of our thesis we participated in a two day GPRS course. This course was held by Ericsson. The “Introduction” chapter about GPRS is basically based on the information and documentation from that course.

In this report there are many references to different European Telecommunication Standards Institute - ETSI documents. These documents often include a large amount of information. The information that was essential to the security issues in GPRS was located in many different documents. This document is focused on gathering the different security aspects in GPRS and give a more uniform description. The two main chapters; “Security functions in GPRS” and “Security threats to the GPRS” are where we have used the ETSI documents most.

From the Internal Ericsson document, “Ericsson GPRS Security Solutions” we got some good ideas to the “Protecting the different GPRS parts” chapter.

When using the Ericsson test lab, we used Ericsson’s descriptions of how to execute system tests. We used some of this documentation when describing the test, but we also used information from the Nessus homepage about the Nessus tool.

Especially in the beginning of the project period we searched for information related to our thesis on newsgroups, Internet and Ericsson’s Intranet. The information was limited, but we discovered some information we could use to get an overview of hackers interest and knowledge on GPRS. There were also assignments, done by students at Helsinki University, which covered some of our theoretical part of the thesis.

We have chosen to build our thesis on the five issues described in chapter 1.4.2. The test part is also explained with concern on these issues. The chapter “How to protect the different GPRS parts” is not according to this structure. In this chapter we have mainly chosen to focus on how IP networks and IP traffic in the GPRS system can be protected by firewalls, Virtual Private Networks and the IP security protocol IPSec.

2 GPRS overview

2.1 An introduction to the GPRS

The GPRS is a GSM phase 2+ service and is also an essential first step towards third generation mobile network (UMTS). The standardisation of GPRS started in 1993 by the ETSI (European Telecommunication Standards Institute)[8].

2.2 The GPRS System

The Figure 2.1 illustrates the GPRS architecture. This chapter describes the elements in the GPRS system. It has focused on the components that are added to the GSM system, but it also includes components that are already known in the GSM system.

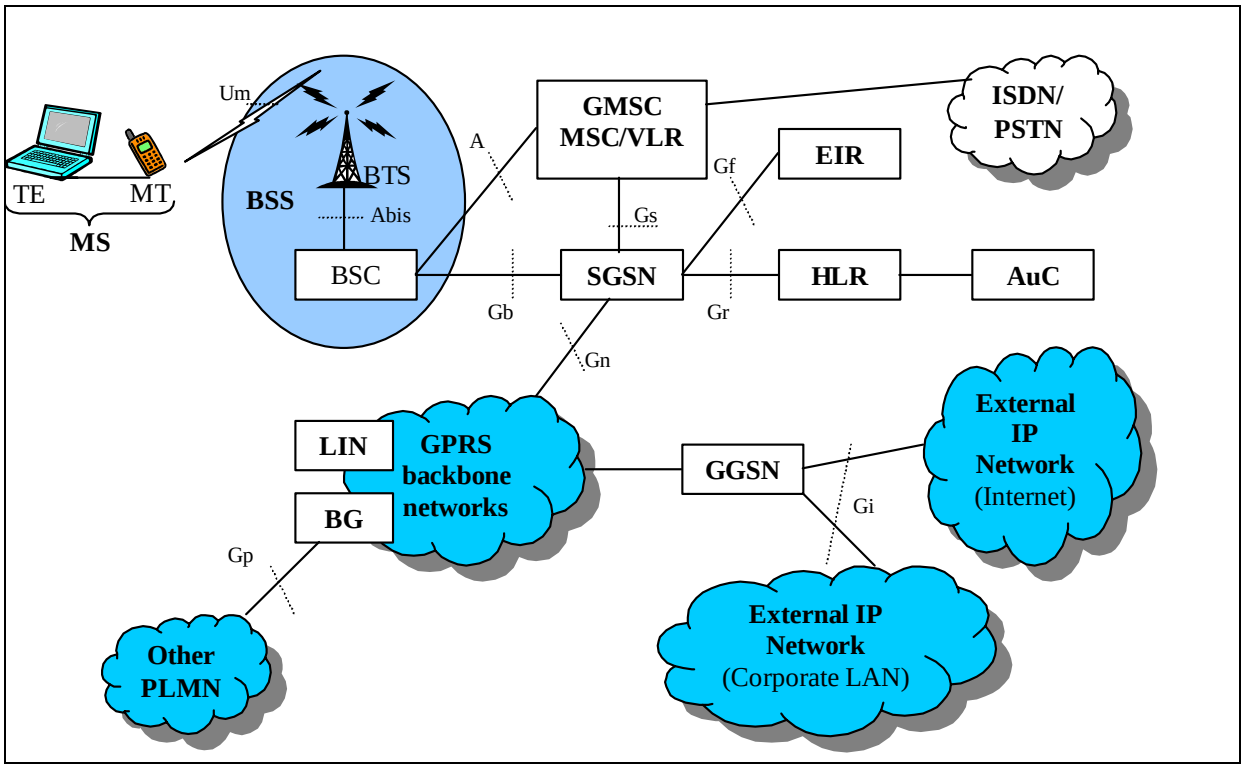

Figure 2.1 GPRS logical architecture

MS - Mobile Station

Depending on the Mobile Station (MS) and the network capabilities, GPRS MSs can operate in three different modes:

- Class A mode of operation allows an MS to have a Circuit Switched (CS) connection at the same time as it is involved in a packet transfer.

- Class B mode of operation allows an MS to be attached to both CS and Packet Switched (PS), but it cannot use both services at the same time. However, MS that is involved in a packet transfer can receive a page for CS traffic. The MS can then suspend the packet transfer for the duration of the CS connection and afterwards resume the packet transfer.

- Class C mode of operation allows a MS only to be attached to one service at the time. A MS that only supports GPRS and not CS traffic will always work in class C mode of operation.

The combination of a Terminal Equipment (TE) and Mobile Terminal (MT) is a MS, but TE and MT components could actually be in the same piece of equipment. From the TE point of view e.g. a laptop computer, you could compare the MT to a modem, connecting the laptop computer to the GPRS system.

The MT is associated with a subscriber in the GPRS system. The MT establishes a link to a SGSN. Channel reselection is provided at the radio link between the MT and the SGSN. The IP connection is static from the TE point of view; that is, the TE does not know it is mobile and retains its assigned IP address until the MT detaches.

BSS – Base Station System

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

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

HLR – Home Location Register

The Home Location Register (HLR) 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. For GPRS, subscribers information is exchanged between HLR and SGSN. Note that the authentication triplets are retrieved directly from the HLR to the SGSN.

VLR – Visitor Location Register

The Visitor Location Register (VLR) database contains information about all MSs that are currently located in the SGSN routing area.

The VLR contains temporary subscriber information needed by the SGSN to provide services for visiting subscribers.

SGSN – Serving GPRS Support Node

The Serving GPRS Support Node (SGSN) is a primary component in the GSM network using GPRS and is a new component in GSM. The SGSN forwards incoming and outgoing IP packets addressed to/from a mobile station that is attached within the SGSN service area, and it also provides packet routing and transfer to and from the SGSN service area. It serves all GPRS subscribers that

are physically located within the geographical SGSN service area. A GPRS subscriber may be served by any SGSN in the network all depending on location.

The SGSN also provides:

- Ciphering and authentication.
- Session management
- Mobility management
- Logical link management towards the MS

GGSN - Gateway GPRS Support Node

Like the SGSN, the Gateway GPRS Support Node (GGSN) is a primary component in the GSM network using GPRS and is a new component. The GGSN provides

- The interface towards the external IP packet networks. The GGSN therefore contains access functionality that interfaces external ISP functions like routers and RADIUS servers (Remote Access Dial-In User Service), which are used for security purposes. From the external IP network's point of view, the GGSN acts as a router for the IP addresses of all subscribers served by the GPRS network. The GGSN thus exchanges routing information with the external network.
- GPRS session management; communication setup towards external network.
- Functionality for associating the subscribers to the right SGSN.
- Output of billing data. The GGSN collects billing information for each MS, related to the external data network usage. Both the GGSN and the SGSN collect charging information on usage of the GPRS network resources.

CGSN – Co-located GPRS Support Node

Co-located GPRS Support Node (CGSN) means that the SGSN and GGSN functionalities are combined in the same physical node (network element), but they may also reside in different physical nodes. SGSN and GGSN contain GPRS backbone network protocol (IP) routing functionality, and they may be interconnected with IP routers.

BG – Border Gateway

SGSN and GGSN can be located in different PLMNs. The two PLMNs will then be connected via Border Gateways (BG) for security and interoperability reasons. The Border Gateways are part of the GGSNs. 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.

EIR – Equipment Identity Register

The Equipment Identity Register (EIR) is a database containing mobile equipment identity information, which helps to block calls from stolen, unauthorized, or defective MSs.

AuC – Authentication Center

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

AuC is a GSM-specified entity that provides triplets to the authentication and ciphering process used within GSM. The authentication for GPRS and for GSM subscribers is the same. The change in security for GPRS is related only to the new ciphering algorithm. This change does not require an update for AuC.

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 the GSNs of a single operator. The inter-operator backbone network connects GPRS operators and provides international GPRS roaming. GPRS backbone networks are IP based.

3 Security functions in GPRS

3.1 Background

This chapter is about how it is recommended to take care of the security. It is basically based on different ETSI documents. Before the details of the five issues, we have explained some keywords related to security.

3.2 Overview

Confidentiality, Integrity and Authentication (CIA) are three different services that computer and network security should cover. All the three services have to be protected, an attack against one or some of them are possible. It is important to have strict control for who should have Access control and dispense with Denial-of-Service for the authorized users.

Confidentiality – The property of information that has not been disclosed to unauthorized parties[4]. Confidentiality has traditionally been seen as the most formidable threat in the communications system. To provide confidentiality encryption is used.

Integrity – The property of information that has not been changed by unauthorized parties [4]. Integrity is normally associated with error correction and retransmission techniques to ensure that data are not corrupted. Cryptographical checksum is a technique to ensure that data is not wilfully modified.

Authentication – The provision of assurance of the claimed identity of an entity[4]. Authentication is reference to the user identity verification. Challenge-Response is a common authentication mechanism that active challenge the user to claim that he is the right person, so the user has to give the right response.

Access control – The prevention of unauthorized use of a resource, including the prevention of a resource in an unauthorized manner [4]. Access control is to give access to services for authorized user and denying unauthorized user the same services.

Denial-of-Service – While access control is about denying the unauthorized user access to the services, Denial-of-Service can be seen as a security service to ensure that unauthorized users are denied access to the services [8].

3.3 Terminal and the SIM card

The SIM-card contains the identity of the subscriber. When it is inserted into a Mobile Equipment (ME), they together form a Mobile Station (MS)[18].

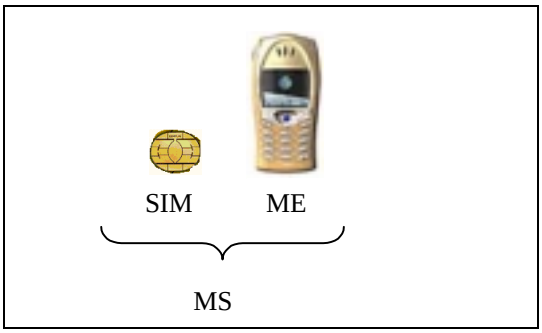

Figure 3.1 Mobile Station

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, Ki, the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN)[7]. The GPRS A5 algorithm is implemented in the ME together with the International Mobile Equipment Identity (IMEI) that is physically secured in the ME. The authentication procedure is described more thoroughly in chapter 3.3

SIM

IMSI International Mobile Subscriber Identity
Every subscriber in the GPRS system has a unique IMSI. IMSI consist of three digits Mobile Country Code (MCC), two digits Mobile Networks Code (MNC) and 10 digits Mobile Subscriber Identity Number (MSIN) as shown in Figure 3.2

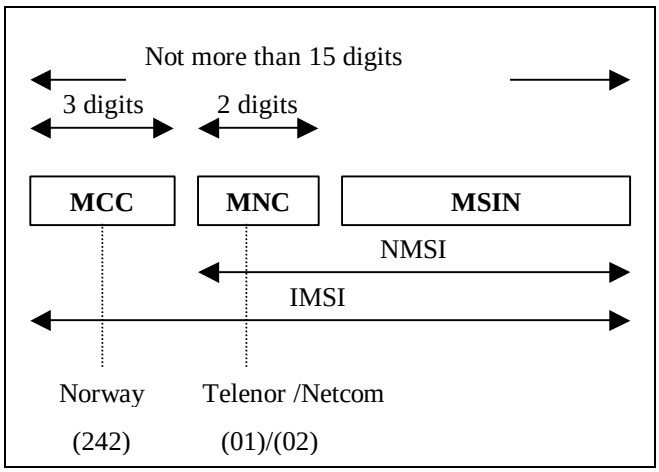

Figure 3.2 International Mobile Subscriber Identity

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

A8 The ciphering key generating algorithm.
The A8 algorithm is using the Ki together with the 128 bits authentication RAND to generate the 64 bits Ciphering Key, GPRS-Kc. This is illustrated in Figure 3.3.

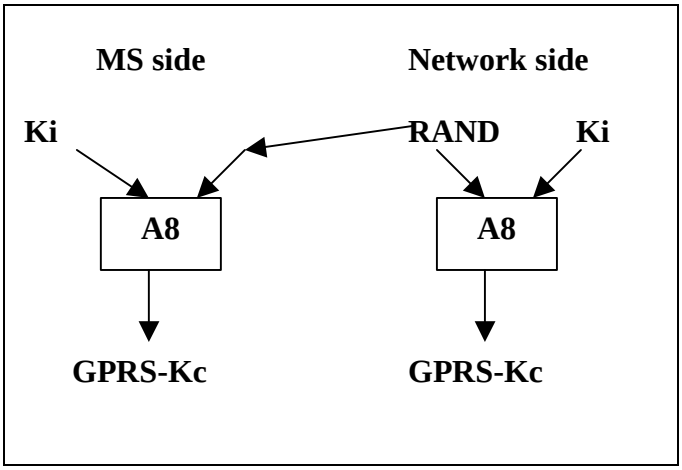

Figure 3.3 Using A8

A3 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 [1]. 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 Ki. The use of A3 is shown in the Figure 3.4.

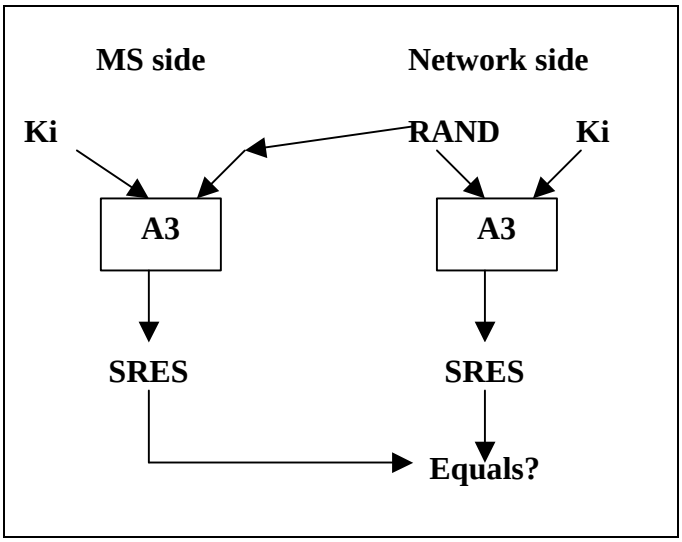

Figure 3.4 The use of A3 algorithm

PIN Personal Identification Number
PIN is an access condition to control user access to the SIM. If the subscriber types the PIN code incorrectly e.g. three times, the SIM will be blocked [12].

ME

GPRS–A5
As mention earlier the GPRS-A5 algorithm is installed in the ME, to be totally correct the algorithm can actually reside in the ME, Terminal Adaptation (TA) or the Terminal Equipment (TE) from a MS point of view [19].

The GPRS-A5 algorithm is used for ciphering the data and signaling during a 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 Algorithm GPRS-A5 by an explicit variable INPUT per established LLC (Logical Link Control) and DIRECTION [1], this is illustrated in Figure 3.5.

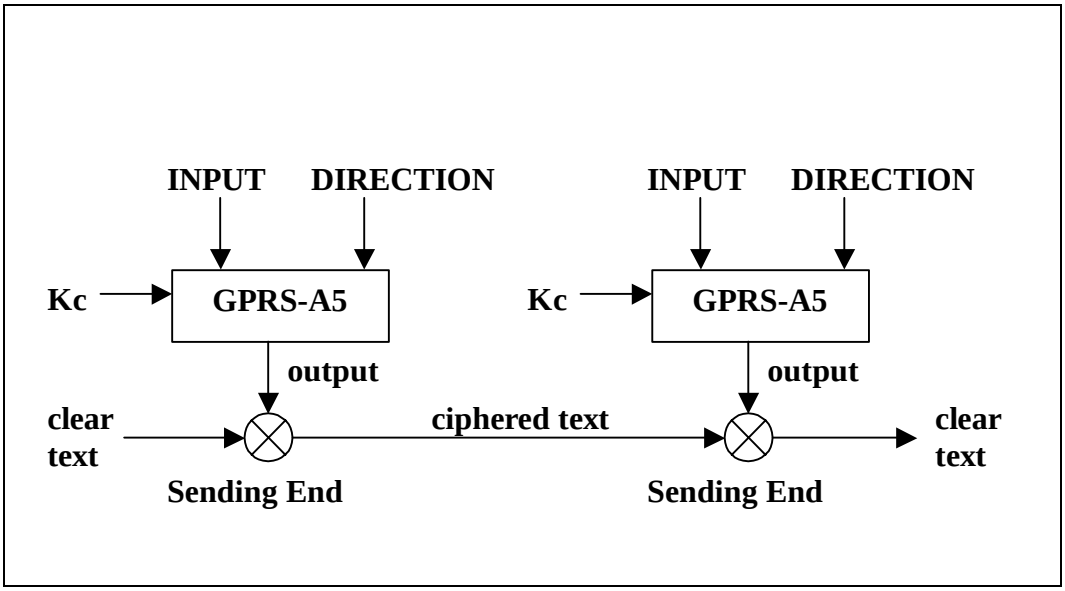

Figure 3.5 GPRS-A5 ciphering process

The equipment security relies on the integrity of the International Mobile Equipment Identity (IMEI)[3]. The IMEI is a 14 digit decimal number composed of three distinct elements [20]:

- a 6 digit Type Approval Code (TAC)
- a 2 digit Final Assembly Code (FAC) and
- a 6 digit Serial Number (SNR).

A check digit complements the IMEI. The check digit is not part of the digits transmitted at IMEI check occasions. The Check Digit shall avoid manual transmission errors, e.g. when customers register stolen MSs at the operators customer care desk.

The unique IMEI shall be securely stored in the terminals during the manufacturing process. The main objective is to be able to take measures against the use of stolen equipment or against equipment that no longer can be tolerated by the system for technical reasons.

The Equipment Identity Register (EIR) contain a database where the IMEI are stored. Three registers are defined for an administrative use of the IMEI, these are known as *white lists*, *grey lists* and *black lists*.

> The *white list* is composed of all number series of equipment identities that are permitted for use.
>
> Equipment on the *grey list* are not barred, but are tracked by the network for evaluation or other purposes.
>
> The black list contains all equipment identities that belong to equipment that needs to be barred.

3.4 Mechanism between the MS and the SGSN

Background

The GPRS network offers various security related services on the radio path. This is to give the user a secure and reliable service. The functions offered can be divided in three groups [1][7]:

- Confidentiality of the user identity
- Confidentiality of user data
- Confidentiality of signalling information elements and connectionless user data

Figure 3.6 gives an overview of the security functions and procedures between the GPRS network and the MS in the case of an attach request.

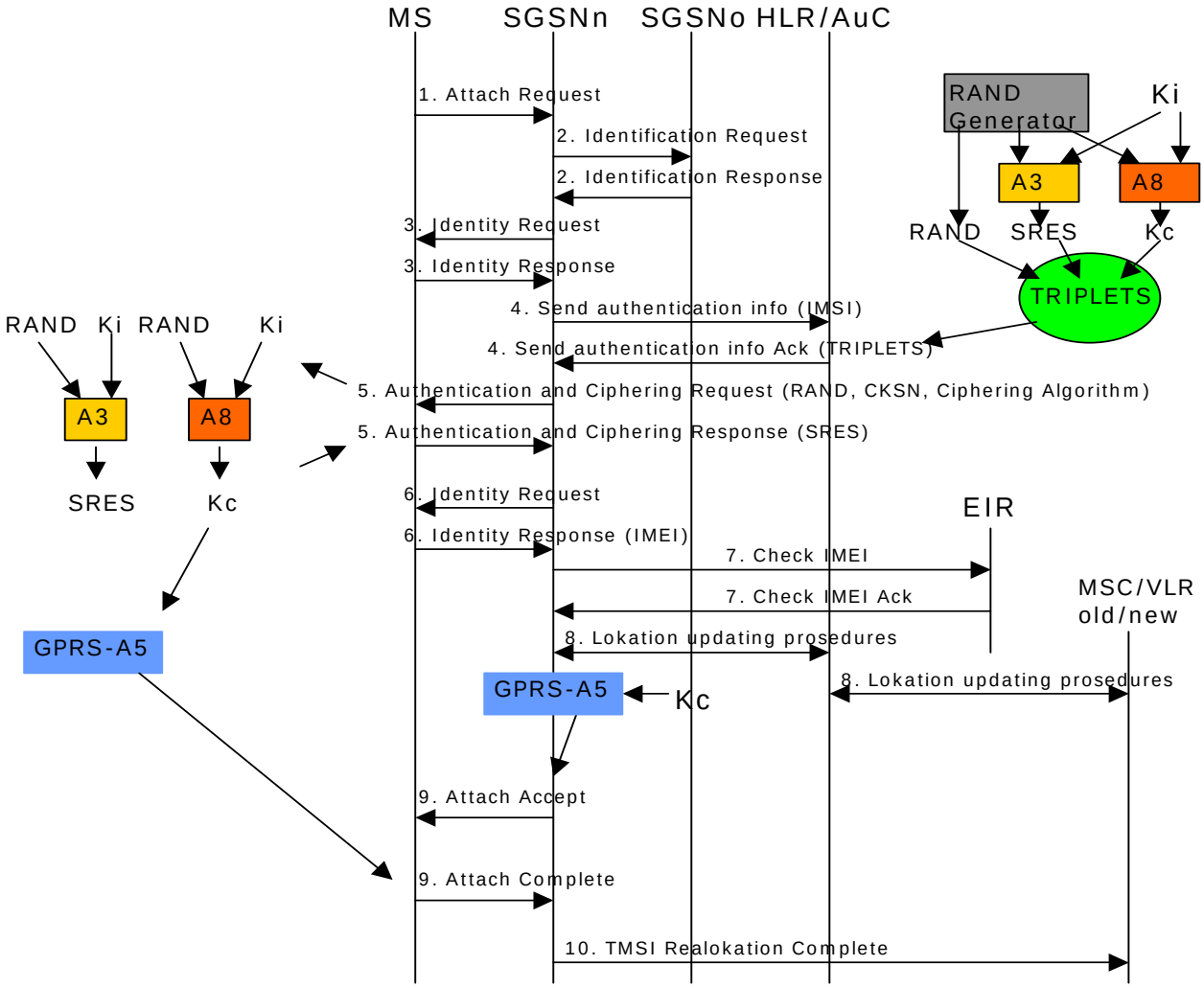

Figure 3.6 Attach procedure

To get a better understanding of the figure, each step is here explained in more detail:

1. Attach Request
   The Attach Request includes: (IMSI or P-TMSI and old RAI, Classmark, CKSN, Attach Type, DRX Parameters, old P-TMSI Signature)

2. Identification Request and Identification Response
   The new SGSN (SGSNn) sends an Identification Request to the old SGSN (SGSNo) if the SGSN has changed since detach, the Identification Request includes (P-TMSI, old RAI, old P-TMSI Signature). The SGSNo responds with Identification Response (IMSI, Authentication Triplets) if the MS is known otherwise it will respond with an error cause. This is only done if the MS identify itself with P-TMSI.

3. Identity Request and Identity Response
   The SGSN sends an Identity Request (Identity Type = IMSI) to the MS if it is unknown in both the SGSNn and SGSNo. The MS will then responds with Identity Response (IMSI).

4. Send authentication info (IMSI) and Send authentication info Ack (TRIPLETS)
   If the SGSN does not have any stored authentication triplets, a Send Authentication Info (IMSI) is sent to the HLR. The HLR responds with a Send Authentication Info Ack (Authentication Triplets).

5. Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) and Authentication and Ciphering Response (SRES)
   When the SGSN receive the TRIPLETS it send a Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) to the MS which responds with Authentication and Ciphering Response (SRES). After sending this message the MS starts ciphering. The SGSN start ciphering after it receives the message from the MS.

6. Identity Request and Identity Response (IMEI)
   If the SGSN decides to do an equipment check it sends Identity Request (Identity Type) to the MS. The MS then responds with Identity Response (Mobile Identity).

7. Check IMEI and Check IMEI Ack
   If the SGSN decided to do a equipment check it can check this against the EIR by sending Check IMEI (IMEI) to it. The EIR responds with Check IMEI Ack (IMEI).

8. Location updating procedures
   If the SGSN number has changed since detach or it attach for first time, it is necessary for the SGSN to initiate some Location updating procedures. This procedure includes informing HLR, which then will inform the SGSNo to cancel the MS and sends subscription data to the SGSNn. If Attach Type in step 1 indicated GPRS Attach while already IMSI attached, or combined GPRS and IMSI attach, then the VLR should also be updated if the Gs interface is installed.

9. Attach Accept and Attach Complete
   The SGSN then selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS. If the SGSN allocates a new P-TMSI the P-TMSI is included. The MS

acknowledges the received information by returning an AttachComplete message to the SGSN, if P-TMSI or VLR TMSI was changed.

10. If VLR TMSI was changed, the SGSN confirms the VLR TMSI re-allocation by sending a TMSI Reallocation Complete message to the VLR.

If the SGSN is not able to attach the MS or if the Attach Request cannot be accepted, the SGSN will return an Attach Reject (IMSI, Cause) message to the MS.

This is a combined GPRS and IMSI Attach procedure and it is not always necessary to perform all the steps. E.g. if the MS is known in the SGSNo or SGSNn, step 3 will not be necessary.

Confidentiality of the user identity

The identity of the user is protected to avoid the possibility for an intruder to identify which subscriber is using a given resource on the radio path by listening to the signalling exchange or the user 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 [1].

To identify a mobile subscriber on the radio path a Temporary Logical Link Identity (TLLI) is used. The TLLI is a local number and has only a meaning in a given Routing Area (RA), it is accompanied by the Routing Area Identity (RAI).

The relation between the TLLIs and IMSIs are stored in a database at the SGSN. So when a TLLI is received with a RAI that does not correspond to the current SGSN, the IMSI is requested from the SGSN in charge of the RA indicated in the RAI. If the address of that SGSN is unknown the IMSI is requested from the MS.

When a new TLLI is allocated to a MS, it is transmitted from the SGSN to the MS in a ciphered mode produced with the GPRS-A5 algorithm. This is not completely the truth since the fixed part of the network can acquire the identification of the MS in clear. However this is a breach in the provision of the service, and should only be used when necessary to cope with malfunctioning, e.g. arising from software failure.

Confidentiality of user data

The SGSN can request security related information for a MS from the HLR/AuC corresponding to the IMSI, which will include an array of pairs of corresponding RAND and SRES. This is done in the HLR/AuC by using RAND and the key Ki in the A3 algorithm. The pairs are stored in the SGSN as part of the security information. The HLR/AuC responds the SGSN by sending the vectors RAND/SRES in the Authentication Vector Response which also includes the key Kc.

These sets of information (RAND/SRES and Kc) are stored in the SGSN. And they should be marked as *used* when they have been used, but it is the operators that decide how many times a set can be used before it is marked. If there is no more unused sets left, the SGSN may use a used set. In order to get rid of sets that is

used the SGSN is to delete all the records marked as *used*, when it successfully request security related information from the HLR. The sets may also be re-sent by the HLR depending on the rules for re-use of sets set by the operator.

Confidentiality of user information and signalling between MS and SGSN

The needs for a protected mode of transmission are fulfilled by a ciphering function in the LLC layer. It is the GPRS-A5 algorithm that ciphers the LLC layer information. A mutual key setting is produced to allow the MS and the network to agree on the key Kc to be used in the ciphering and the deciphering algorithms GPRS-A5. The Kc is transmitted to the MS in the RAND value and it is derived from the RAND by using the A8 and the Subscriber Authentication key Ki.

The MS and the SGSN must co-ordinate when the ciphering and the deciphering processes should start. The SGSN indicates if the ciphering should be used or not in the Authentication and Ciphering Request message, and the MS starts the ciphering after sending the Authentication and Ciphering Response message. In order for the enciphering bit stream at one end and the deciphering bit stream at the other end to coincide, the streams must be synchronised. This is done by using an explicit variable INPUT, the DIRECTION and the Kc in the algorithm GPRS-A5, illustrated in Figure 3.5. The synchronisation of ciphering at LLC frames level is done by a bit in the LLC header indicating if the frame is ciphered or not.

When a inter SGSN routing area update occurs, the necessary information (e.g Kc, INPUT) is transmitted within the system infrastructure to enable the communication to proceed from the old SGSN to the new one. The key Kc may remain unchanged at Inter SGSN routing area update.

The MS should indicate which version of the GPRS-A5 algorithm it supports when it wants to establish a connection to the network. The negotiation of the GPRS-A5 algorithm happens during the authentication procedure. The network can decide to release the connection if there is no common GPRS-A5 algorithm, or if the MS indicates an illegal combination of supported algorithms. Otherwise the network selects one of the mutual acceptable versions of the GPRS-A5 algorithms to be used.

3.5 GPRS Backbone

The operator is responsible for the security of its own Intra-PLMN backbone, which includes all network elements and physical connections. The operator shall prevent unauthorised access to its Intra-PLMN backbone. A secure Intra-PLMN backbone guarantees that no intruder can eavesdrop or modify user information and signalling in the Intra-PLMN backbone[1].

The GPRS architecture utilises GPRS tunnelling and private IP addressing within the backbone to restrict unauthorized access to it. User traffic addressed to a network element shall be discarded. Firewall functionality may provide these means at the access points of the Intra-PLMN backbone.

The Inter-PLMN links shall be negotiated between operators as part of the roaming agreement. They shall ensure that the Inter-PLMN links are secure providing integrity and confidentiality. For example, secure links can be achieved by point to point links, private Inter-PLMN backbones or encrypted tunnels over the public Internet [1].

Operators shall be able to determine the origin of packets coming from the inter-PLMN backbone. One example is to use a Frame Relay PVC between two operators.

The GPRS Tunnelling Protocol (GTP) is the protocol between GPRS Support Nodes (GSNs) which allow multi-protocol packets to be tunnelled through it in the GPRS backbone network. All kind of protocols can be present in the GTP tunnel, which means al kinds of traffic from the subscribers, e.g. DNS queries, zone transfers and NTP syncs. Most likely GPRS operation and maintenance traffic goes over it, by HTTP, telnet or FTP. This is if no dedicated network for operation and maintenance is present. By default the GTP is not encrypted which means the traffic carried over it is transparent[14][25].

In the signalling plane, GTP specifies a tunnel control and management protocol that allows the SGSN to provide GPRS network access for a MS. Signalling is used to create, modify and delete tunnels[28].

In the transmission plane, GTP uses a tunnelling mechanism to provide a service for carrying user data packets. The choice of path is dependent on whether the user data to be tunnelled requires a reliable link or not.

The GTP protocol is implemented only by SGSNs and GGSNs. No other systems need to be aware of GTP's presence. GPRS MSs are connected to an SGSN without being aware of GTP. It is assumed that there will be a "many-to-many" relationship between SGSNs and GGSNs. A SGSN may provide service to many GGSNs. A single GGSN may associate with many SGSNs to deliver traffic to a large number of geographically diverse mobile stations.

3.6 Interworking between GPRS networks

The primary reason for the interworking between the GPRS networks is to support roaming GPRS subscribers [21]. This so subscribers will be able to access from other operators GPRS networks to their home network, that means from VPLM to the HPLMN. A general model for GPRS network interworking is shown in Figure 3.7.

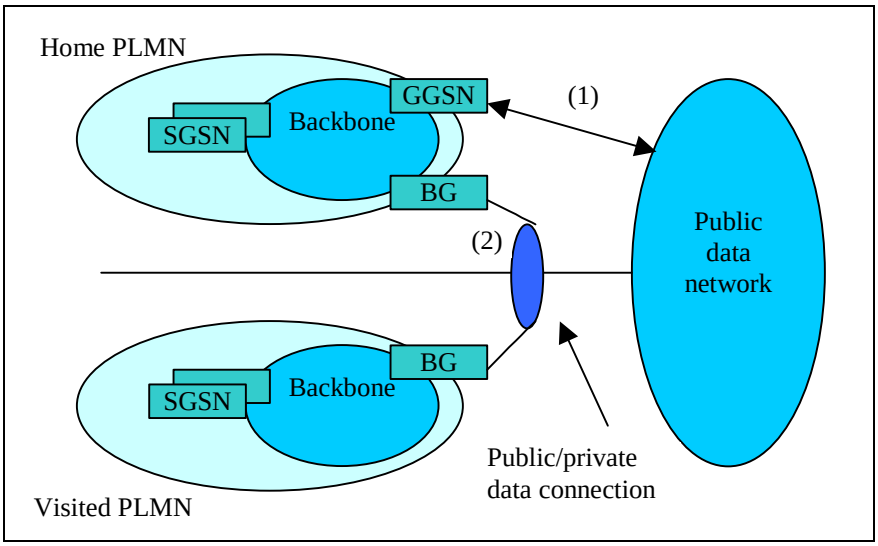

Figure 3.7 Interworking GPRS networks

GPRS networks are connected to each other via interoperator backbone networks [10]. The inter-PLMN link may be any packet data network (1), e.g. Internet, or a dedicated link (2). Dedicated link may be chosen to fulfill QoS requirements of a certain protocol. Each GPRS operator may support IPSec and accompanying specification for authentication and encryption as a basic set of security functionality in its border gateways. However, other security protocols may be selected by a bilateral agreement between the GPRS operators.

3.7 Interworiking GPRS PLMN and Packet Data Networks

The GPRS are supporting interworking with Packet Data Networks (PDN) that is based on the Internet Protocol. These interworked IP networks can be either the Internet or Intranets. GPRS has the opportunity to operate with IPv4 and the new IPv6. As mention earlier and shown in Figure 3.8, the interworking point with IP networks is at the Gi interface [10][21].

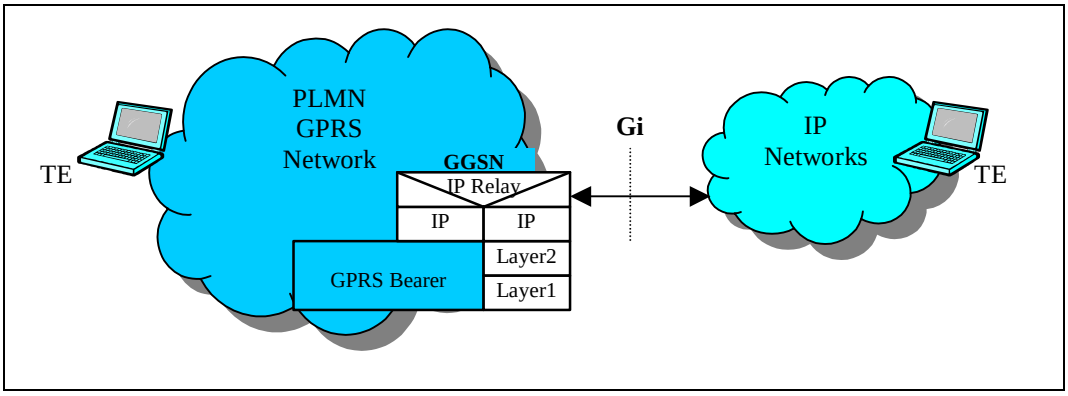

Figure 3.8 IP network interworking

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 3.8. The Layer1 and Layer2 protocols are operator specific and are negotiated between e.g. a GPRS operator and an external IP network operator.

The access to Internet, Intranet or ISP through GPRS may involve specification such as: user authentication, user's authorization, end to end encryption between MS and Intranet or ISP and allocation of dynamic address belonging to the PLMN, Intranet or ISP addressing space. For this purpose GPRS PLMN may offers either direct transparent access to the Internet, or a non-transparent access to the Intranets or ISP.

Transparent access to the Internet

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 for packet forwarding between the Internet nodes and the GGSN and as well to map packet within the GGSN.

The MS need not to send any authentication request at the PDP context activation. And the GGSN do not need to participate in the user authentication or authorization processes.

The user authentication and encryption of the user data are done within the "Intranet protocol" if either of them is required. This is shown in Figure 3.9 where the communication is between a GPRS PLMN and an Intranet. The figure also shows that the security is ensured on an end-to-end basis between MS and the intranet by the "Intranet protocol". The communication between GGSN and the Intranet may be performed over any network e.g. Internet, and there is no specific secure protocol between GGSN and the Intranet. IPSec is an "Intranet protocol" that can be used to offer the GPRS user to communicate over insecure public networks securely.

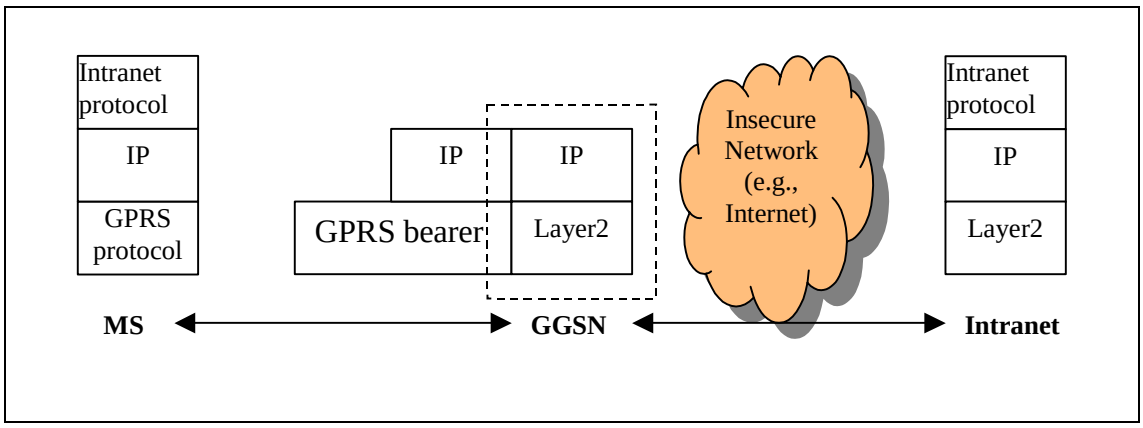

Figure 3.9 Transparent access to an Intranet

Non-Transparent access to an Intranet or an ISP

When non-transparent access to an Intranet or ISP is used, the MS is given an address, which belongs to the address space of the intranet or ISP. In the same way as the transparent access, the address is either a static address given at subscription time or a dynamic address given at PDP context activation. This received address is used for packet forwarding within the GGSN, the Intranet or the ISP. This again requires a link between the GGSN and an address allocation server belonging to the Intranet or the ISP. This server may be based on, e.g. RADIUS or DHCP [10][21].

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 request user authentication and configuration from a server like, RADIUS as shown in Figure 3.10.

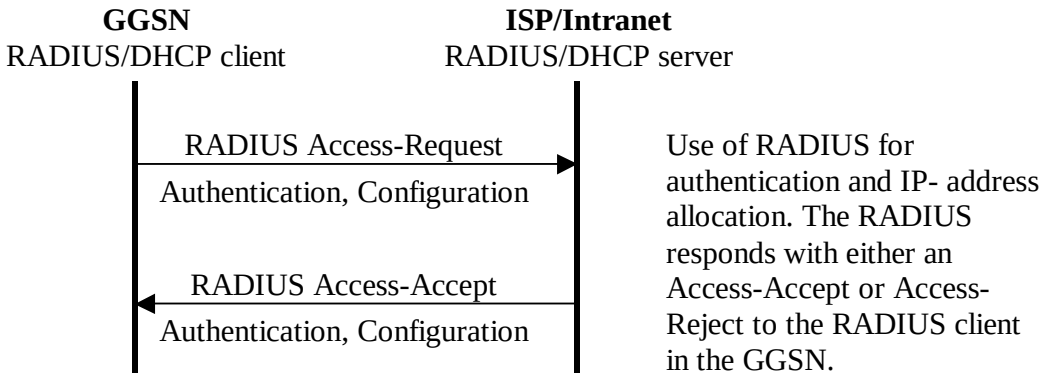

Figure 3.10 Authentication and Configuration request between GGSN and Intranet or ISP

It is also possible to do the authentication and configuration procedure by using RADIUS and DHCP. RADIUS is responsible for the authentication request, after the authentication request the DHCP handles the configuration procedure, as illustrated in Figure 3.11.

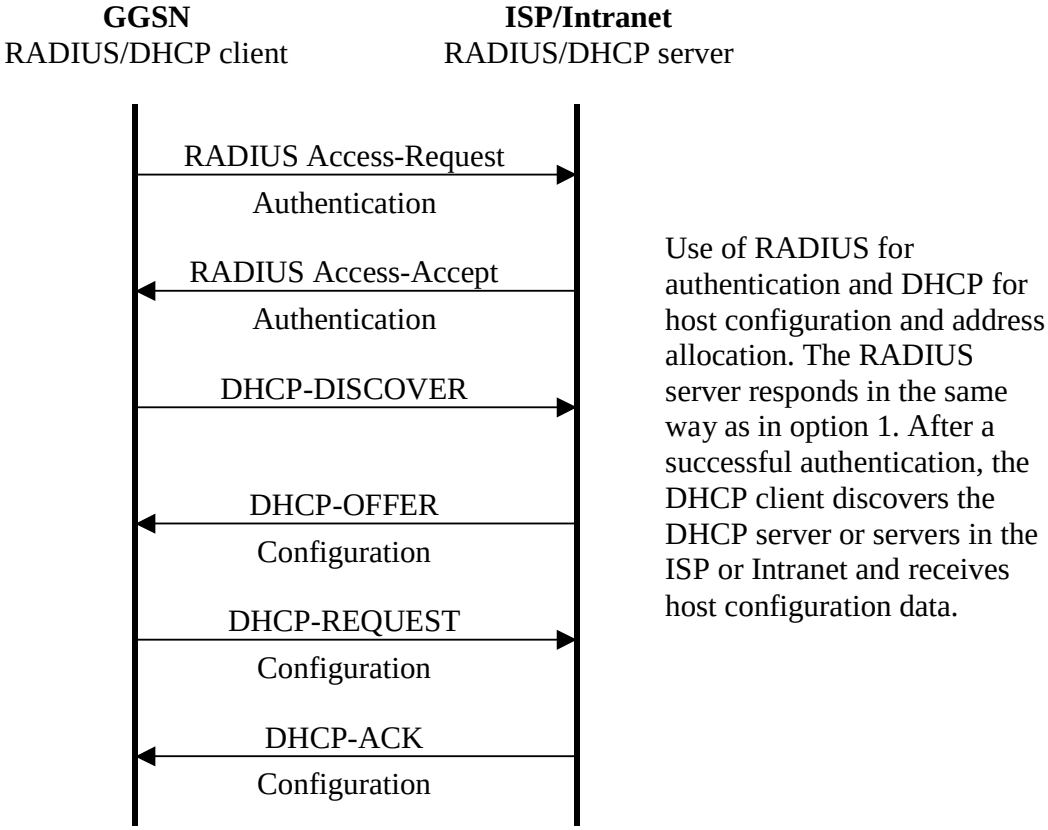

Figure 3.11 Authentication and Configuration request between GGSN and Intranet or ISP

The connection between the GPRS network and ISP can be arranged over any network, even an insecure one, such as the 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 [10],[21].

4 Security threats to the GPRS

4.1 Intro

The threats to the GPRS are very different from the Circuit Switched GSM. The security threats to the GSM are quite limited, there are not many hackers that can or will crack the obscurity SS7 protocol. The GPRS system are a much more exposed to intruders, because of it IP based backbone. It is a lot of people that have thoroughly knowledge about the TCP/IP in proportion to the SS7 [8].

Intruders to the GPRS system can be people or organization that attempts to breach the confidentiality, integrity, availability or otherwise attempts to abuse the GPRS in order to compromise services, defraud users or any parts in the GPRS system [4].

4.2 Terminal and the SIM card

Integrity of data

The mobile phone may deal with some of the same threats as a normal computer that is connected to a network have, e.g. the Internet. Intruders to a mobile phone or a terminal may modify, insert or delete application or data stored in the terminal. This can be compared when a computer are getting a “virus” that attacks the system. Not only the terminal but also the SIM is a possible target to the integrity of the data in the same way as the terminal. It can also result that the access to the terminal or the SIM can be obtained either locally or remotely.

Stolen terminal and SIM card

Since the mobile phones are much smaller and lighter than a computer, it makes it much more easier to steal. There are two scenarios regarding stolen mobile equipment, use of stolen terminal without the SIM and use of terminal with the SIM card inserted. A stolen terminal without the SIM card result in loss to the owner with respect to the value of the terminals since the charging and billing is related to the SIM card. If the stolen terminal includes a valid SIM card, then the loss is greater until the operator disables the SIM card [7]. A disabled terminal are not useless, the possibility to manipulate the identity of the terminal and get access to services that an operator offers exist. The way to do this is to modify the IMEI of the terminal and than insert a valid SIM card in the terminal.

Borrowed terminal and SIM

Another threat is use of borrowed terminal and SIM. Users who have been given authorization to the equipment may misuse their privileges perhaps by exceeding agreed usage limitations [4].

Eavesdrop, masquerade or manipulate

The SIM –terminal interface are also having threats with intruders eavesdropping data, intruders masquerade as a SIM or a terminal in order to intercept data and intruders that modify, insert, replay or delete user traffic or in other words manipulate the data.

Confidentiality of user data and authentication data

Confidentiality of user data and authentication data in the SIM card together with confidentiality of certain user data in the terminal may be threats for the owner. Intruders may get access to personal user data stored by the user in the terminal or the SIM card, this might be telephone books and messages belonging to the user. When it comes to the confidentiality of the authentication data in the SIM card, the intruders are probably interested to access authentication data stored by the service provider, like the authentication key.

Cloned SIM card

To get the authentication key, the intruders probably have to clone the SIM card. The fastest way to do this is to physically have the SIM card, but it is also possible to clone the SIM card over the Air. If they have the opportunity to have a cloned SIM card, they might want to listen to the real subscribers call or even make calls that would be billed to the original subscriber account [23].

Non-type approved terminals and defective equipment

Non-type approved terminals and defective equipment can be a source to disturbing the network's performance and may affect the quality of service offered to other subscribers [7].

4.3 Interface between the MS and the SGSN

The significant point of attack between the MS and the SGSN is actually the radio interface or the air interface between the terminal equipment and the BSS. Threats related to the air interface can be separated in four different parts. These four parts are; unauthorized access to the data, threats to the integrity, denial of service and unauthorized access to service [4].

Unauthorized access to the data

User traffic, signalling data or control data are information intruders may eavesdrop on the air interface. The signalling data or the control data are information that can be useful to conducting active attacks on the GPRS system and give the intruders access to secure management data.

It is possible for intruders to masquerade as a network element, e.g. a BTS and intercept user traffic, signalling data or control data over the air interface.

Intruders may observe the time, rate, length, sources or destination of messages in order to get access to the information. This is a passive way to analyse the traffic. Intruders may actively initiate communication sessions and then observe in the same way as the passive traffic analysis to obtain access to information.

Threats to the integrity

Manipulation of user traffic, signalling data or control data may occur in an accidental or a deliberate manner. The integrity is exposed if the traffic and the data in any way are modified, inserted, replayed or deleted.

Denial of service attacks

To jam users traffic is a physical intervention of denying someone the services. The user traffic, signalling data and control data are by jamming prevented from being transmitted over the air interface. Another way to prevent the information or data to be transmitted is by including specific protocol failures. It is possible for intruders to induce these failures by physical meanings.

Another way to deny services is by masquerade as a network element and then prevent the user traffic, signalling data or control data from being transmitted.

Unauthorized access to services

A possibility for an intruder to get unauthorized access to services can be by masquerading as a BST towards a user and then hijacking the users connecting after authentication has been established.

4.4 GPRS backbone

The threats to the backbone are as mention in the beginning of the chapter 2.3 dealing with many of the same threats as the air interface. Threats that are described between the MS and the SGSN are also threats to wired parts in the backbone. These threats may be unauthorized access to data, threats to the integrity, denial of services and unauthorized access to services.

An important threat to the backbone are that trusted sources are misusing their privileges to attack the PLMN backbone or from the PLMN backbone. Since it has been estimated that the lion's part of all network attacks come from trusted sources [14]. That means that it is exposed that attacks are being initiated from the PLMN backbone, and people with access to the PLMN have a good opportunity to initiate such attacks.

It is not obvious that the IP based PLMN backbone is only dedicated to GPRS traffic. A possibility is that the PLMN backbone is operating on top of the already existing core network. The core IP network might then carry various types of traffic nodes in the GPRS network might be addressable from a large community of people, in fact from the whole Internet. Traffic that may pass the core network is of course the GPRS Tunnelling Protocol, but also other IP based protocols such as DNS queries and NTP syncs.

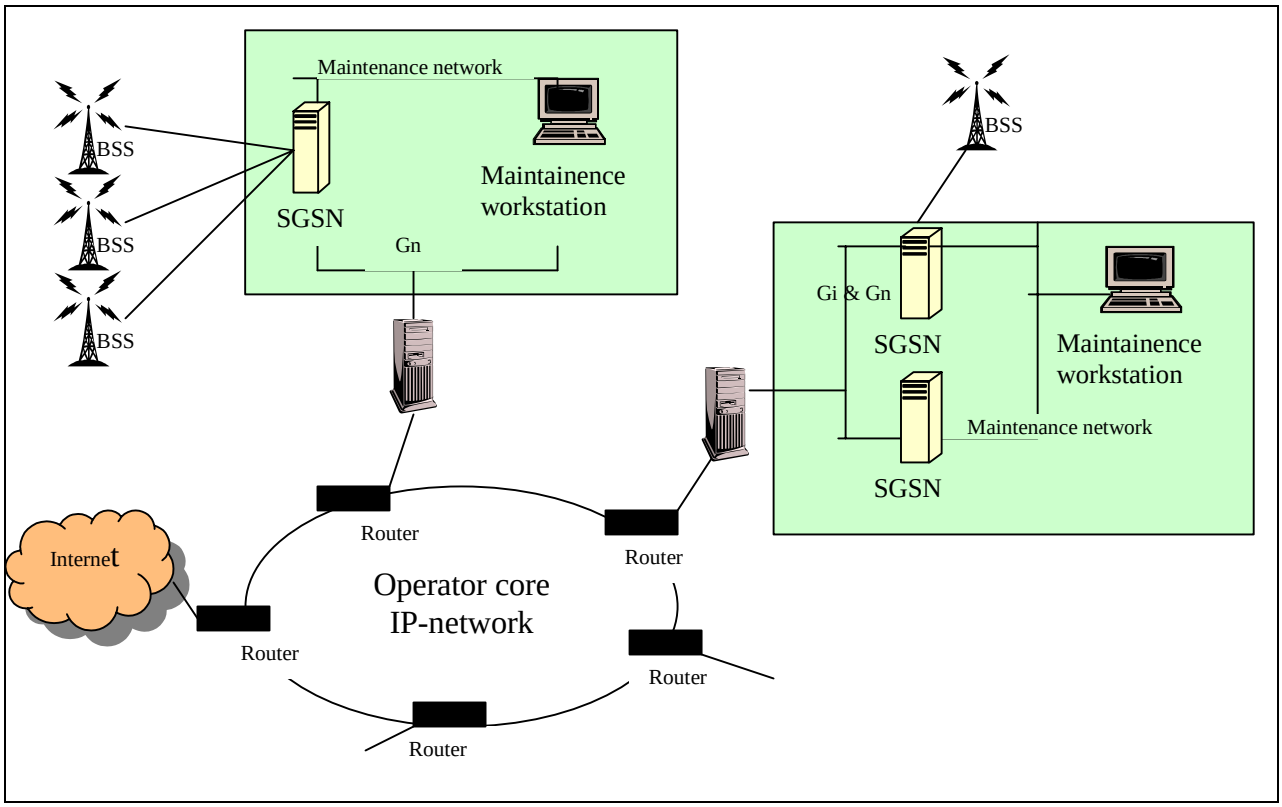

Figure 4.1 Operator using existing IP- network as PLMN

Since the GTP protocol is not encrypted by default it is easy for a person that have access to the intermediate node between the GGSN and SGSN to eavesdrop e.g. the traffic of the GPRS subscribers.

Another threat related to the PLMN backbone is how to handle the operations and maintenances of its NE. As shown in the figure 4.4 it is possible to have maintenance workstation to administrate such problems. The interface should be protected against intruders from e.g. the Internet in case of any insecure ports are opened such as 20 and 21 for FTP and 8888 for node administration via HTTP. The interface for operations and maintenances are not standardized, but is an interface that is a supplementary from Ericsson given the name Gom [14].

4.5 Interworking between GPRS networks

The security between different GPRS operators depends on the reliability to each other. Are the other operators to be trusted or not? As mention in the security chapter, there are different bilateral agreements between the GPRS operators.

Like the treats related to the backbone, the threats between GPRS operators are in many way the same. The opportunity for trusted people in the different network to misuse the position and export actions like:

- Eavesdropping
- Masquerading
- Traffic analysis
- Manipulation
- Denial of service

The fact that the different operators actually are competing for the same subscribers, this means that they also can constitute a threat to each other. A PLMN might want to hurt or attack the other operators network or subscribers in order to make the subscribers change operator.

One relevant contingency is to make denial of service attacks. The attacking operator may prevent, by physical intervention subscribers traffic, from being transmitted or delaying transmission on purpose. This may be done while the subscribers are using the visited or attacking network, or it can be attacked outside from the visiting network against the subscribers home networks. One physically way to intervene such attacks is to inducing protocol with failures so the network cannot handle the protocol in a right manner.

4.6 Interworking GPRS PLMN and Packet Data Networks

To protect the GPRS system against hackers or intruders that want to hurt or utility the GPRS system from an external network, like Internet are essential. A hacker that breaks into from an external IP-network can in many ways be a threat to the data confidentiality, integrity or availability.

People that are trying to get access inside the GPRS system from an external network are often doing this to show their technical skills and gain reputation in the hackers' environment. The purpose of the attack might be to cause harm to the GPRS system or steal information. After they have stolen the information they have the opportunity to sell the information in order to receive money [11].

A hacker could also cause huge bills for the GPRS users. Since the GPRS billing is based on the amount of transferred and received data. It may be possible to cause harm for the GPRS users by sending large spam e-mails from the external network or to create a virus located at users MS. This virus may have a property to send dummy packets from the MS without the user even knowing it [10].

The GGSN has the opportunity to use either static or dynamic routing. When dynamic routing is used, it is relatively easy to launch a denial of service attack against the GGSN, by giving the GGSN false routing information [14].

5 Security testing of the GPRS system

5.1 Background

In this chapter we will describe a security test that were performed at Ericsson AS in Grimstad. In order to get an understanding of what kind of threats and the level of work that is put into it, we will try to explain how a hacker prepare before an attack[28].

5.2 How to prepare for a hack

While there is no easy recipe to hacking, most system intrusions can be divided into four steps. Depending on techniques involved or level of difficulty, there could be less or more, but these four steps should give an idea on how hackers with some experience would prepare a system intrusion:

1. Learn as much as possible about the target before the attack. The techniques involved can be passive to bordering on mini-attacks themselves. Plan out the goals for the attack. Then use the knowledge gained to develop a plan, no matter how small or quick the hack is.

2. Initial access to the system. This step has to be considered as the real attack part. This could be anything from ftp access to a sendmail bug to logging in as a "regular" user. If successful, it should either create an opportunity for indirect or direct access to the system.

3. Full system access. At this level most goals developed can be carried out. This will most likely involve password file retrieved for cracking, trojan installed, secret file copied, etc. So this stage usually involves either taking advantage of a bug that allows higher privileges to be obtained, taking advantages of miss configured system parameters, or a combination of both.

4. Tracks are covered and backdoors installed. System logging is doctored to remove traces of the attack and what was done during the attack, and either defence are lowered or files are tampered with, to allow quicker and easier access. Some experienced hackers even patch the system to keep less experienced hackers out of the system (who might possibly tip off a Sys Admin). Once step four is complete, hackers will refer to this system being owned.

In order to get an overview of the information about GPRS out amongst people whose interest is hacking, have we browsed sites and newsgroups with focus on this subject. And the impression we have is that there is not much information out there. But if someone has any information on GPRS they usually has a very good overview of it. When it comes to hacking in general there is a lot of information and tools, and some of the information gives an impression of comprehensive knowledge on the different systems. Even though the information today on the GPRS system is not very broad, we see that the interest of GSM is great. It is therefore likely to believe that GPRS, which is based on a well-known

architecture and components, will be a popular target for attacks. The fact that the billing for system usage is usually high will be a factor that accelerates the eagerness to hack the system.

5.3 The security test lab

5.3.1 Background

Ericsson AS has a test lab dedicated for testing the security of the system. It is fully equipped with all of the system components including user traffic. Since the GPRS system is in continuous development it is impossible to guarantee that the components are completely without faults. It is therefore important to have defined levels of risks with procedures for what action to take for each level[29].

Four Risk and danger levels are defined [29]:

1. High: any vulnerability that allows an attacker to gain immediate access into a machine, to gain superuser access, or to bypass a firewall.
2. Medium: any vulnerability that provides information, degrades performance, or has a high potential of giving system access to an intruder.
3. Low: any vulnerability that provides information that could potentially lead to a compromise.
4. None: No vulnerability was detected. Lowest possible risk, but this does not guarantee total security.

If a test returns a danger level “high” or “medium” it is consider as it failed the test. With the danger level “low” and “none” the test is considered as passed. Even thou a test is considered as passed on risk level “low” it does not mean it can be forgotten, the exploitation of a “low” risk vulnerability can be a used as a part in a larger means.

The CGSN platform is built out of standard components, including the operating system. The Unix operating system Solaris from Sun is used in addition to VxWorks. Solaris is widely used on desktop workstations and on server installations. It is in the latter capability it is used in the CGSN. It is a multi-user system and is well suited to perform tasks that require well-defined access rights. VxWorks is a real-time operating system used in systems where time is essential [17].

Solaris is commonly used in desktop workstations and on server installations, and GPRS is based IP technology, which both are well-known systems for persons with bad intents. This and the fact that information for e.g. billing will be situated here, make the probability for an attack high.

5.3.2 The test lab

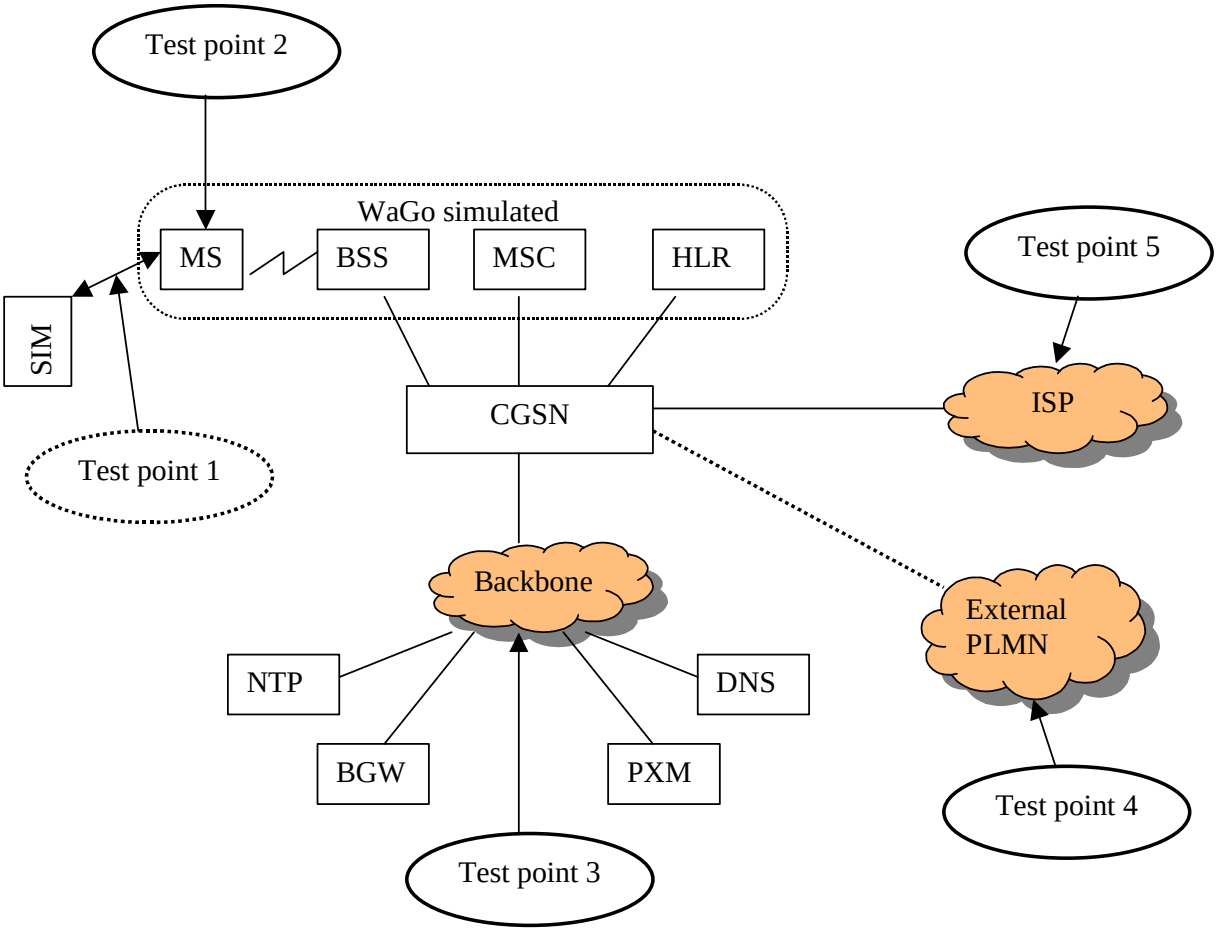

Figure 5.1 Overview of the test point

A security laboratory (Sec Lab) will be connected to a GPRS network, external PLMN, MS and ISP for testing. This security lab consists of different hardware and software components that will be used as tools for testing the security of the different GPRS system parts. We have defined 5 points where the security of the system can be exploited.

Test point 1

This security test point is not included in Ericsson's test lab, nevertheless it is a point where security can be jeopardised. The vulnerability of this point is described more in detail in chapter 4.2.

Test point 2

This security test point is from an MS. This MS is a Solaris based computer, which is connected to the Sec Lab backbone network as a gateway. All other computers in the Sec Lab are connected through the gateway.

Test point 3

This security test point is on the backbone network of the GSN. The test will be executed directly towards the NEs.

Test point 4

This security test point is from an external PLMN. The Sec Lab will be connected to an external PLMN network as one of the host in PLMN for testing.

Test point 5

This security test point is from an ISP. The Sec Lab is connected as a host in the ISP. The ISP is connected to the router interface (Gi) of the CGSN.

5.3.3 Test environment

In the SecLab, different types of security test tools are implemented. In order to stay up to date when new security flaws are discovered is it profitably to use commercial available security test tools. When new security flaws are discovered is it possible to add the check for this new flaw to the tool. In addition many of these test tools offer users the ability to customise tests and write their own test scripts. The software tools we used and will describe here, are called Nessus and Ethereal. In addition to those two, we also participated in some tests with tools from ISS. The tools from ISS are not freely distributed. But the ISS security tools are considered to be among the most comprehensive there is. More information on the ISS tools in appendix B.

Nessus Security Scanner

Nessus is security scanner software, which will check remotely a given network and determine whether bad guys may break into it, or misuse it in some way. It will detect all services on any port and attempt to exploit the vulnerability. The scanner is built inn a way where every test is like a plugin. This makes it possible to customise a test or add your own test.

Ethereal
Ethereal is a free network protocol analyser for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.

When we used the test lab at Ericcson AS in Grimstad, we run tests on the system with two test tools:

- Nessus Security Scanner (For scanning on network level)
- Ethereal (a network protocol analyser for Unix and Windows)

Examples of security holes are like wrong file permission, absence of root or users password, bugs in services in the OS [29].

5.3.4 The Security test with Nessus on RPC (Remote Procedure Call) vulnerability.

Since the security test may contain information that is considered confidential by Ericsson, it is removed from the main report. The results from the test are in Appendix 1, which will be made available on request and approval from Ericsson or Lars Line.

6 Protecting the different GPRS parts

6.1 Introduction

The meaning of protecting or preventing different part in the GPRS system is also about avoiding attacks to the system. We will in this chapter focus on the possibilities to avoid security attacks to the GPRS system.

6.2 Subscriber authentication

Subscription is checked during the GPRS attach procedure and also during the PDP Context Activation procedure. The GGSN implicitly checks its internal context related to the destination address for each mobile terminated packet. If there is a context associated with the PDP address the packet shall be forwarded to the MS, otherwise the packet shall be discarded or rejected depending on the implemented protocol [21].

The SGSN authenticates the subscriber when attaching to the system. This authentication is done so the system will be able to properly bill the subscriber. When the subscriber is connected, he will be able to e.g. send and receive SMS messages. The subscriber is authenticated again when the PDP context is activated. This authentication is done to make sure the user is allowed to the network he is trying to connect to. This double authentication may seem extraneous but it is a security measures that protect the GPRS subscriber. Actually it is also protecting the network and the service provider against undesirable subscribers [14].

To further increase the security of the authentication procedure it is possible to use one-time passwords in the GPRS systems in the same way it is done in the regular dial-up connections. Normally an external device such as an electronic key ring is used to generate this password. This password is sent to the server that checks the password against a special RADIUS server capable of handling one-time passwords. An external device might be needless in a GPRS system. Instead the MS can be used. E.g. before the subscriber activates the PDP context he sends an SMS message to a specific telephone number. The message includes a pin code and the name of the PDP context that the subscriber want to use. The server that receives the message checks if the pin code is correct. If so, the server sends an SMS message in response to the subscriber with a one-time password. The subscriber then uses the one-time password when activating the PDP context. Another solutions would be to use the storing capabilities in the MS to store pre-generated one-time password that can be unlocked with a pin code.

Protecting the GPRS system with use of firewalls

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks . In the GPRS view of using firewalls there are lots of places where firewalls are needed in order to secure the system. The operators want to protect the GPRS equipment, the subscribers need end user security, and directly connected companies want to protect their vital Intranet resources. The GPRS operators may also want to disallow some bandwidth-demanding protocols, this to ensure that a group of singles subscribers do not consume so much bandwidth that other subscribers are noticeably affected [14].

From the GPRS operators point of view there are two main purposes witch should be protected against attacks originated from the Internet [14]. This is the GPRS equipment and the mobile terminals, this also include protections of subscribers information or other information that are stored in the GPRS network or in the mobile terminal.

Or as the ETSI describe how the network control screening should be performed [21]:
The PLMN administration and or the GPRS service provider shall set basic screening functionality, if applicable, e.g. firewall to reduce the risk of fraud and misuse. This is to ensure the integrity of the network and to protect subscribers.

Between the GGSN and the external IP network the following assumptions are valid in generic case [21]:

- A firewall is configured by the GPRS operator. In general, all applications that are using IP as the underlying protocol are supported, but the GPRS operator may restrict their usage. In most cases it is necessary to restrict access from external IP networks to the GPRS network.

- A Domain Name Server is managed by the GPRS operator or it can be managed by the of the external IP network operator.

- From the GPRS network's point of view, the allocation of a dynamic IP address is done by the GGSN. The GGSN may allocate these addresses by itself or use an external device such as a DHCP server. This external device may be operated by an external organisation such as an ISP or Intranet operator.

Where the Firewall, DHCP and DNS are placed is illustrated in Figure 6.1.

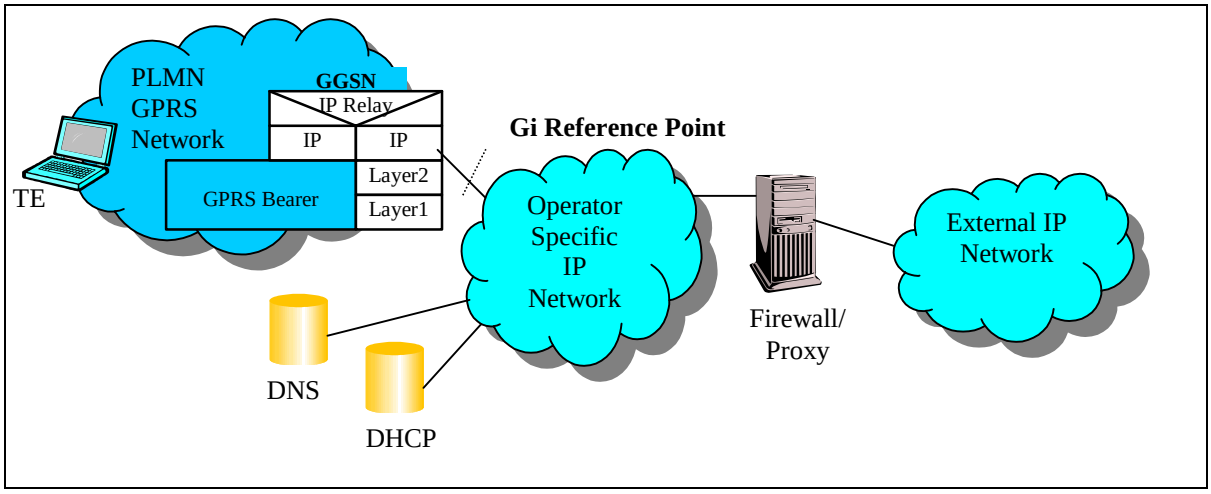

Figure 6.1 GPRS Network connected to External IP Network

The Figure 6.1 shows that a firewall is used to protect the GPRS network. The operator may consider that only traffic initiated from the MS and not from the Internet should pass through the firewall. This is done for two reasons, to restrict the traffic in order to protect the MS from attacks and also to protect the MS from receiving unrequested traffic. Unrequested traffic may be unwanted for the

subscribers since they are paying for the traffic received as well. To be able to only allow traffic that is initiated from the MS a firewall that is capable of stateful inspection is needed [14].

GPRS system is more complicated compared to normal office environments. Normal offices have an open network on the inside and are connected to the outside through a firewall. This implies that the personnel and departments on the internal network trust each other since the traffic between them does not pass through the firewall. In the GPRS system it is not possible to assume that the mobile subscribers belonging to the same GGSN should trust each other. As shown in Figure 6.2 MS A and MS B can reach each other without passing through a firewall placed between the GGSN and the Internet if the two connecting tunnels do not utilise APN routing [14].

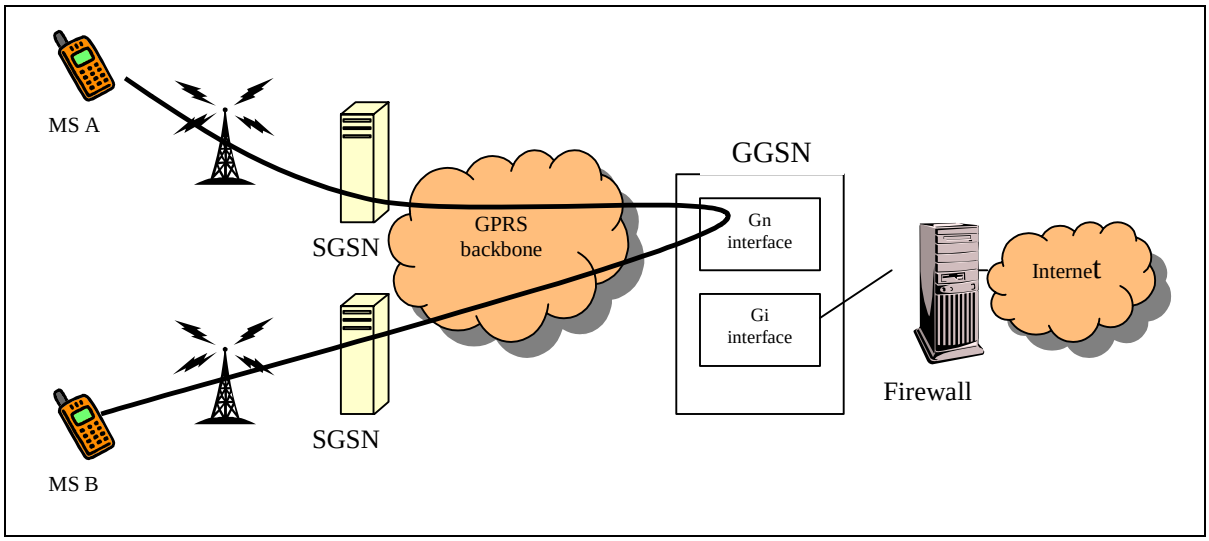

Figure 6.2 MS A access MS B without passing through a firewall

APN routing is one of two ways to route traffic from and to the GSN node [15]. APN routing and routing decision is taken on the basis of which MS APN network the packet arrives from. When APN routing is used the connection between the GGSN and the external network must be a point to point connection like a IPSec tunnel, a PPP link or a dedicated Virtual Circuit e.g. ATM VC. The other way is to use Normal IP Routing that is using normal routing protocol like OSPF and normal routing algorithms.

Figure 6.3 illustrate both APN routing and Normal IP Routing. If Normal IP Routing is used the GGSN will use normal IP forwarding policy for the MS. The GGSN looks at the destination IP address in the packet and forward the packet to the router that have the lowest cost towards the Internet host. This could lead to that the packet is being forwarded to R2 through the ISP 2 network even though the MS actually belongs to the ISP 1.

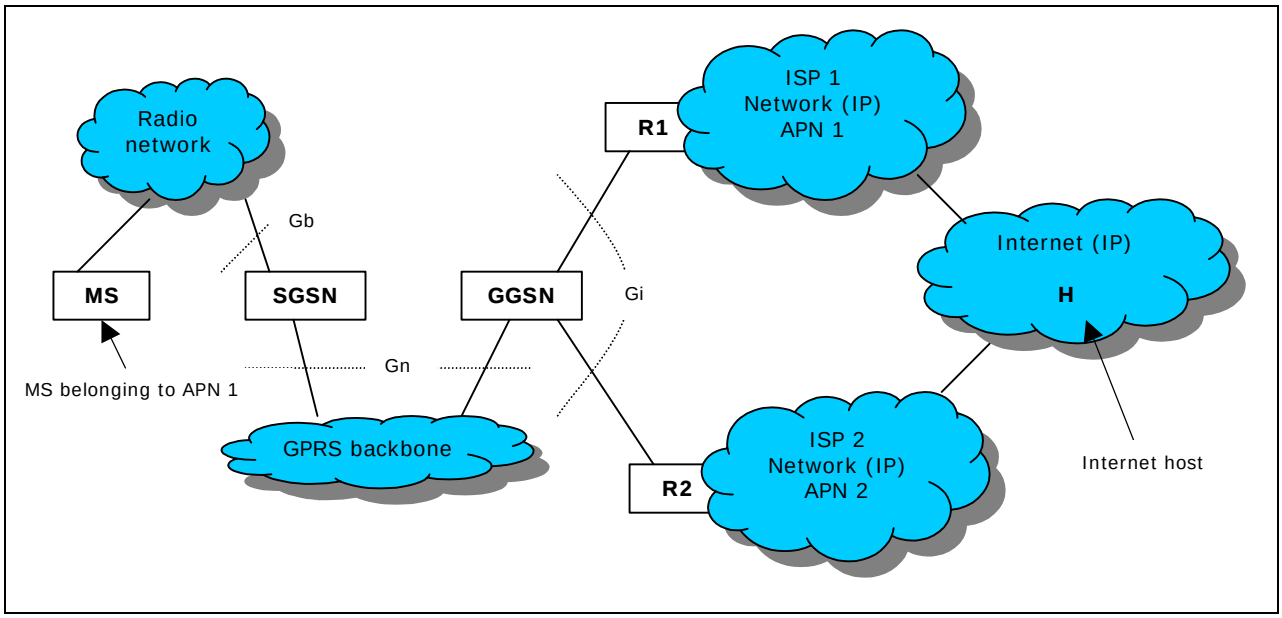

Figure 6.3 APN Routing and Normal IP Routing

If APN Routing is used, then the GGSN will base the forwarding decision upon which external network the MS belongs to. This means that the IP packets from the MS always will be forwarded to the R1 through ISP1 for then to reach the Internet host.

Because the MSs are behind the firewall between the GGSN and the Internet other devices such as SGSN, DNS servers and O&M workstations in the operators network will not protected against the MSs. The packet filters in the GGSN and the external firewall should be configured to drop MS packets addressed to those interfaces. This is not just a problem when operator uses a combined network, but also when operator uses separate Gi network. This is because the Gi interface itself and the backside of the firewall will be addressable at the IP level.

A good solution is to use firewalls and healthy network designs where all the different networks interface are separated from each other. Figure 6.4 Possible network designs for operators using existing IP-network as PLMNshow how a network designs for operators using their existing IP-network as the PLMN. From the figure point of view the firewall has five interfaces the operators core IP-network interface, Gi, Gn, Gom and Gp interface [14].

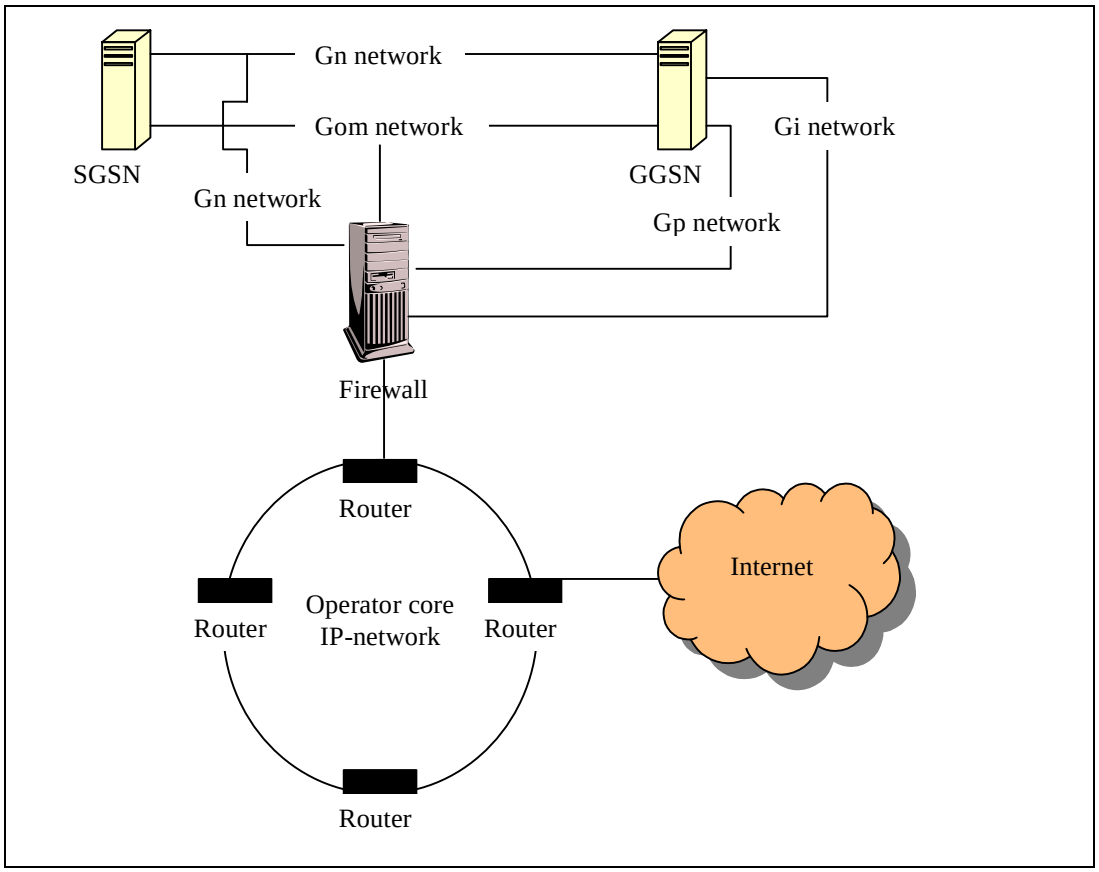

Figure 6.4 Possible network designs for operators using existing IP-network as PLMN

The use of firewall from a Gi interface point of view is a challenge when use of APN routing. If the firewall not understand APN routing a dedicatied firewall for each of the connections is needed. This connection could e.g. from the GGSN to the internet, ISP's or a company dedicated connection. The figure 7.x.x5 illustrate how this can be done. Multiple firewalls can be used to get redundant connections to a network, the placement of two firewall from the GGSN to the Internet is illustrating this.

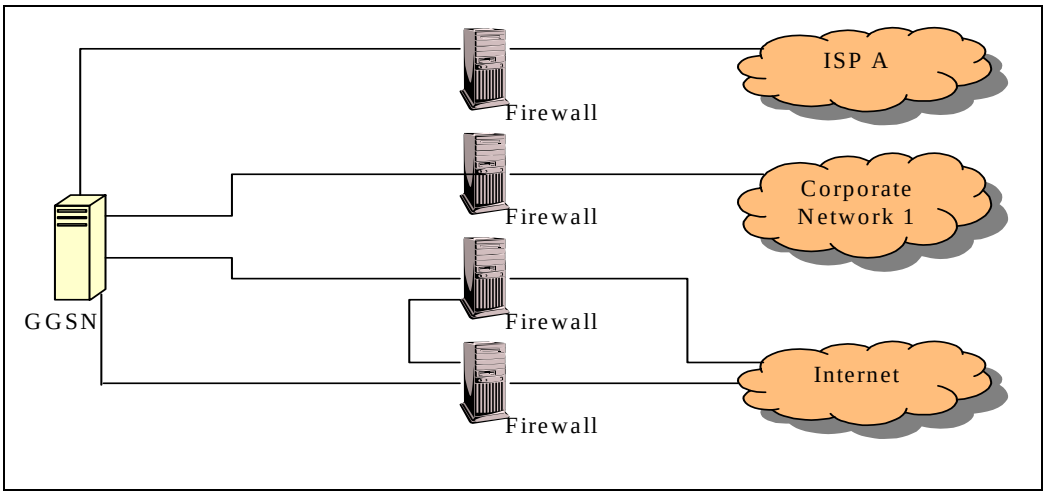

Figure 6.5 Firewall and APN routing

6.3 Virtual Private Networks

In a firewall server it is typically installed some VPN software [22]. A VPN is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocol and security procedures. It can be seen as private network over a public network, e.g. the Internet. Using VPN involves encryption of data before sending it through a network and decryption of the data at the receiving end. IPSec is the most common protocol that is used to achieve a VPN in the GPRS system, the IPSec is described in more details later. Secure virtual connections are created between two machines, a machine and a network or two networks. In the GPRS point of view the machine can actually be the MS. To use a VPN instead of leasing a dedicated line can save a lot of money for the different companies.

In the GPRS system there are different places where the VPN technique can be used. It is possible for a mobile client to establish an end-to-end VPN tunnel from the MS to a corporate network. In a costumers point of view, and end-to-end VPN connections, provide the best security since the traffic goes encrypted the whole way and is show inFigure 6.6.

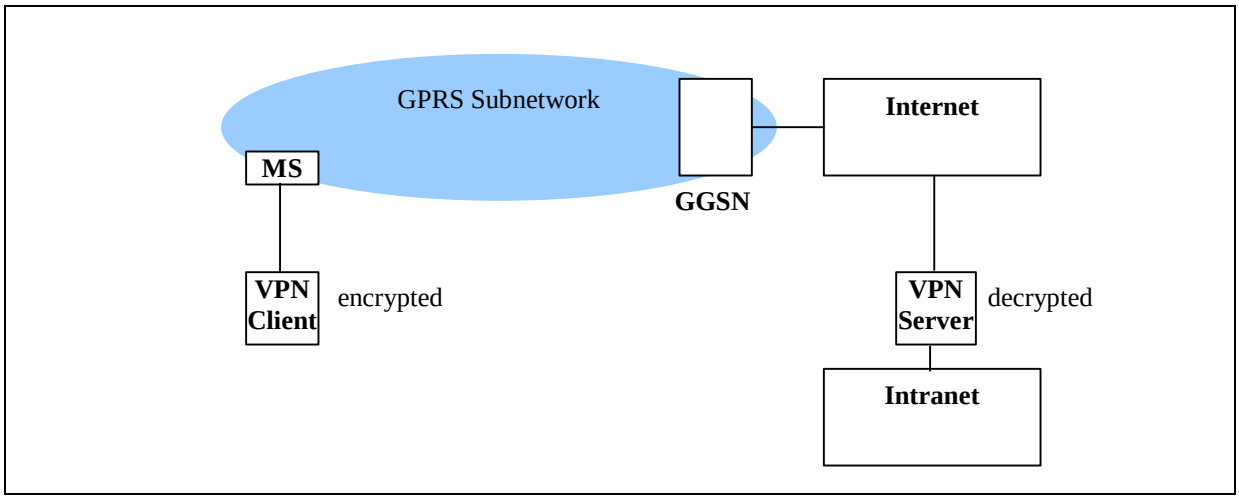

Figure 6.6 End-to-end VPN connection setting [11]

End-to-end VPN is a good solution for the users, but this might be a problem or in conflict with LEAs wishes. This is because the LEA through use of LIN can require user data and other network related information whenever wanted, and this can be difficult to fulfil when end-to-end VPN is used.

Another use of VPN is to use VPN between the GGSN and the corporate Intranet. That means the security from the MS to the Gi interface is leaved on behalf of the GPRS operators, and this will also make it easier to fulfil the requirements from the LEA. Since the encryption algorithm in the GGSN often has a limit of 56-bit [14]. The operators may use additional hardware outside the GGSN, e.g. firewall or other device that is capable of VPN tunnelling to get a more secure VPN. This should probably be done since a cryptographic algorithm with 56-bit keys is considers not strong enough in most of today's situations.

No security is by default provided in the GTP to protect the communication between different GPRS operators [25]. As mention in the chapter about interworking between GPRS operators the protecting from another network can be basted on different security functions in the Border Gateways. A security mechanism that may be considered is for example IP Security.

6.4 IP Security - IPSec

GPRS operators may support the security protocol IPSec. IPSec consists of several open standards and its purpose is to ensure security private communication over IP networks. E.g. inside GPRS backbone, between different GPRS Networks and over the Internet. It is based on standards developed by the Internet Engineering Task Force (IETF). IPSec ensures confidentiality, integrity and authentication of data communications across an insecure, public IP network [10].

IPSec offers encryption and authentication on network layer. It provides an end-to-end security solution in the network architecture itself. Thus the end systems and applications do not need to know how to handle security issues. Encrypted packets look like ordinary IP packets and thus they can be easily routed through any IP network, such as GPRS or the Internet, without the intermediate network nodes know about encryption. The only devices that know about the encryption are the end points. This feature greatly reduces both implementation and management costs.

IPSec consists of a pair of protocols that implement the available security services. These two protocols are the Authentication Header (AH) and the Encapsulating Security Payload (ESP). The AH provides access control, connection message integrity, authentication and antireplay protection. The ESP support the same services as the AH plus confidentiality. These two protocols can be used by themselves or together to provide exactly the mix of services that the user wants [24].

IPSec can operate in two different modes, this is transport mode or tunnel mode. The transport mode can only be used when both the source and the destination system understand IPSec. In most case IPSec is used in tunnel mode allowing the implementation of the IPSec in the network architecture without modifying the operating system or any applications on PCs, servers, and hosts. This is also the situation in GPRS [10].

Figure 6.7 illustrates IPSec in transport mode. In transport mode, it is only the IP payload that is encrypted. The original IP header is left intact. This mode has the advantage of adding only a few bytes to each packet.

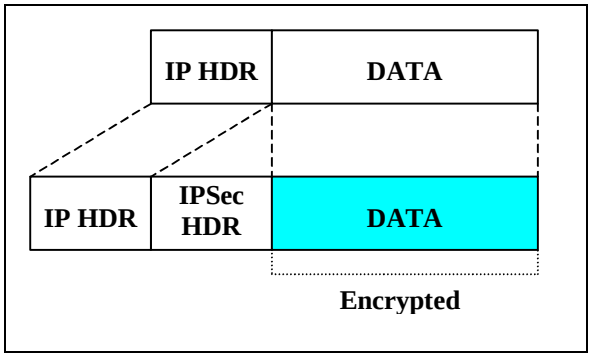

Figure 6.7 IPSec transported mode

In Figure 6.8 IPSec is operating in tunnel mode. When tunnel mode is used, the entire original IP datagram is encrypted. The original IP header and the data becomes the payload in a new IP packet.

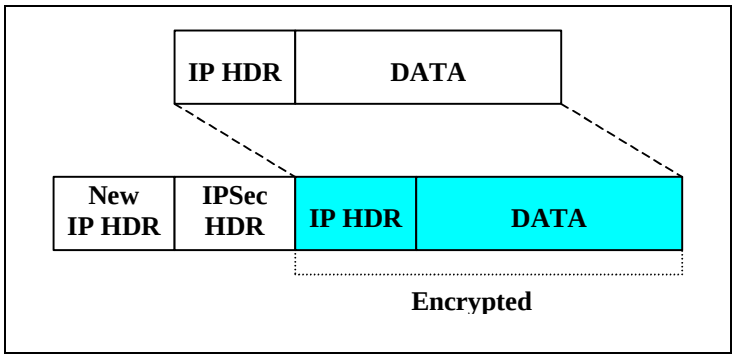

Figure 6.8 IPSec tunneled mode

7 Security result and result to the test

7.1 Introduction

This chapter consists of the results from each of the five issues in the theoretical part. The chapter also includes the results from the test that was done at Ericsson.

7.2 Terminal and SIM card

The mobile phone user decides himself or herself how to take care of it. The owner of the mobile phone is responsible for making the phone a difficult target for a thief. It is also necessary for the owner to have a secure access to the terminal. It should not be easy to modify or get access to the local stored data in the mobile phone or get access to external data stored in e.g. an Intranet, through the terminal.

How to handle the IMEI stored in the ME in a secure way is a challenge for both the manufactures of the ME and the different operators.

The possibility to clone SIM card and get the secret authentication key Ki, is realistic and should be taken into consideration.

7.3 Between the MS and the SGSN

Eavesdropping is a security breach that has to be taken into consideration. And it calls for the operators to choose good algorithms to be used for securing the interface between the MS and the SGSN.

Information over the radio path allowing a listener to derive the identity of the subscribers should not be transmitted in clear text.

7.4 GPRS Backbone

It is the PLMN operators decision to protect the backbone. As mentioned before, a fair share of all known intrusions are accomplished from inside or inside information, e.g. an employee or former employee. The fact that the GPRS backbone often is the same as the corporate backbone makes it important to protect it. The GTP offers an option for encryption, but it is not encrypted by default. The operation and maintenance of the different nodes can be done remotely and it is an operators choice who and how this is done.

7.5 Interworking between GPRS networks

The security between different PLMN operators are based on bilateral agreements.

BG's are used to protect the PLMN network from other PLMN networks.

7.6 Interworking GPRS PLMN and external networks

In view of the fact that there are many people that have thorough knowledge about the IP protocol, intruders from an external network such as the Internet imply a real threat to the GPRS system.

A firewall between the GGSN and the external network should be used to protect operators network and the subscribers against intruders. A stateful inspection capable firewall should be used.

The operators should consider using static routes to avoid denial of service attack against the GGSN. This is because it is relatively easy to give the GGSN false routing information when dynamic routing is used.

7.7 Test results

Since the security test results may contain information that is considered confidential by Ericsson, it is removed from the main report. The results from the test are in Appendix 1, which will be made available on request and approval from Ericsson or Lars Line.

8 Discussion

8.1 Introduction

From the results in chapter seven, this chapter is a discussion on these results.

8.2 Terminal and SIM card

The normal way to protect the ME and the SIM card is by letting the user type a PIN-password before the user is getting permission to use the ME and accessing the SIM card. Another method to identification and access control to the terminal is by biometrics, like eye features, fingerprints, voice recognition and signatures [7]. The owner of the terminal has to make sure that the phones are left in a secure modus, so a thief does not get access to the data stored in the terminal or access to an Intranet if the connection to the Intranet is established and opened. A possible solution to this problem might be to disable the connection regularly so the subscriber has to reactivate and again perform authentication to the Intranet. It is not obvious that a user who has been given access to the terminal does not take advantage of it and misuse the terminal to access local or external data that is available.

The manufactures treat of the IMEI has not been strict enough. This has done it easier for a thief to modify the IMEI in the ME and introduce the ME with a valid SIM card for the network. Another opportunity is to use an already existing IMEI number and introduce the ME with a SIM card for a new PLMN. Some PLMN can detect if there are duplicate IMEI in their network. If the PLMN notice that there are two phones with the same IMEI connected to the network, the PLMN can close the account for both the legitimate subscriber and the attacker. This is done because the PLMN cannot distinguish between the legitimate and the fake subscriber.

The IMEI should be stored in the ME in a way that makes it easy to read, but very difficult and meaningless to change. This means that not only the manufactures, but also the different operators should treat the IMEI so it is complicated to introduce ME with illegal IMEI to the network. It should be hard for stolen and non-type approved ME that do not conform to the telecommunication standards to be connected to the network. This should also be a wish from the operators view, since the operators are concerned if the non-type approved ME is disturbing the system. A non-type approved ME may give a drop of quality of services for other legal subscribers and perhaps result in loss of subscribers using the services. Witch again has influence for the operator's reputation and earnings.

The possibility for attacker to retrieve the authentication key, Ki, from the SIM card and then clone the SIM card is probably one of the biggest threats to the security in GPRS. A security research group from the Smartcard Developer Association and the ISAAC discovered a flaw in the COMP128 algorithm that effectively enabled them to retrieve the secret key, Ki, from a SIM [23]. The attack was performed on a SIM card they had physical access to. When this attacks was performed, they actually had to have access to the SIM card for at least eight hours. This time is greatly reduced since the equipment to do such attacks and the SIM cards has been considerably improved. The time to get physically access to a SIM card is actually now less than ten minutes, which is very realistic.

The attack was based on a chose-challenge attack by a PC that made about 150.000 challenge to the SIM and the SIM generated the SRES and the session key, Kc, based on the challenge and the secret key. This could be done since the COMP128 algorithm is broken in such a way that it reveals information about the Ki when appropriate RAND are given as arguments to the A8 algorithm. Why it now takes less then ten minutes to perform such attacks, is because the SIM card and the smartcard reader which is connected to the PC, is able to perform this with a much higher rate.

To get the Ki by attacks over-the-air and then clone the SIM should also be possible from the SDA and ISAAC point of view. The over-the-air attack is based on the fact that the MS is required to response to every challenge made by the GPRS network. This is different from the UMTS system where the network is responding the MS. Over-the-air attacks can be done with a false BTS bombing the MS with challenges and re-construct the secret key from these responses. One problem is that the MS has to be available to the attacker over the air for the whole time it takes to conduct the attack. It is possible to split the attack in smaller parts. One way to do this is to just tease the phone for a short time every day on the victim's way to work. Since the time it takes to clone the SIM card is much faster, is it more difficult for the victim to notice that the battery level has changed. This is because the phone is using more battery when it is exposed for an attack.

An opportunity with cloned SIM card is that an attacker is only interested in listening to the calls of the subscriber. To do so the attacker can stay passive and invisible to the GPRS network and just listen to the call of the subscriber. Since the attacker is invisible to the network, the network cannot notice that there are two identical phones connected and the account of the subscribers is not closed.

A corrupt GPRS dealer is a possible attacker that would make cloned SIM cards. The corrupt employee would do so e.g. to sell cloned cards to a third parties who wish to stay anonymous and do not want to buy valid SIM cards or sell it to a certain customer so the customer can eavesdrop on the owner's calls.

The cloned SIM card is usable until the subscribers gets a new SIM card, this can actually be for a very long time since it is not often the subscribers are receiving a new SIM card from the operators, and the time does not play a part when it is the GPRS dealer that is cloning the SIM card.

8.3 Between the MS and SGSN

The interface between the MS and the SGSN is amongst the most exposed elements in GPRS. It is therefore vital that it is strongly protected. As mentioned earlier the GPRS system offers services on the radio path to give the user a secure and reliable service with confidentiality of the user identity, confidentiality of user data and confidentiality of signalling information elements and connectionless user data.

In order to take care of the secure and reliable services for the users, the GPRS system use authentication and data encryption between the MS and the SGSN. In the GPRS authentication procedure the same algorithm is used as in the GSM system, this algorithm is the A3 and the A8. Unfortunately the COPM128 algorithm that is used by the most operators for the A3 and A8 is broken. How the weakness in COMP128 is exploited is described over in the terminal discussion. The operator or the standardisation organisation can develop new algorithm to improve the security. Since the algorithm is stored in the SIM card,

the network operator can make the changes themselves and does not need to involve the hardware or software manufacturers. Other networks operator does not have to know anything about the different algorithm used, this because the triplets that are transferred to the visited network include the RAND and the SRES. SRES is the answer from the MS that is compared with the SRES in the visited network to confirm a right authentication.

In relation to the data encryption between the MS and the SGSN a new A5 algorithm has been implemented. This algorithm is not publicly known, but if it became so, the GPRS system would be more vulnerable for manipulation and eavesdropping.

It is also difficult to fulfil that the identity of the subscribers should not be transmitted in clear text. A false BTS can e.g. catch up an Attach Request from a MS or it can transfer an Identity Request to the MS. The false BTS can from the response, get the IMSI and the IMEI, which again could be used to eavesdrop the subscriber.

8.4 GPRS backbone

The GPRS backbone connects a large part of the elements in the GPRS system and is therefore a part that will be attractive for intruders. The GPRS operator has to work out security measurements so it is prepared to meet this threat. If the backbone is not dedicated to GPRS traffic but also the operators corporate backbone, it might carry many types of traffic and be addressable for a lot of people, maybe the whole of the internet. To minimize the risk for external attack on the backbone, is it important to be able to identify and validate the traffic on it. The use of firewalls on the BG can help accomplice this. But this will only protect it for traffic from the outside. The traffic from the backbone itself and from MSs will not be filtered trough the BG firewall.

In cases where someone gets access to this network they will be able to eavesdrop on the GPRS traffic going on it. The use of GTP encryption might lower this risk. The GTP is not encrypted by default but the use of this function has to be considered in cases with combined networks. The backbone carries also operation and maintenance information that has to be protected. With valid rights this kind of work can be carry out from any point of the network. With the use of tunnels and IPSec from dedicated point in the network to the NE the risk of someone seeing this traffic is minimized. However by using dedicated points in the network with secure connections to the NE for this kind of work, the flexibility of the system will be more limited. On the other hand we have the problem with lawful interception. This problem arises primarily if the user traffic on the backbone is strongly encrypted, in which will cause difficulties for the authorities that lawfully should have access to the traffic to get it.

The NE is usually built out of commonly known elements for IP based networks. One example is the SGSN who in the case of Ericsson is running the Sun Solaris operating system. These kinds of systems are well known and are shipped with many pre-installed components. Many of these components are not required and used in the GPRS system, but nevertheless they represent a security risk since some have faults so they can be misused to get access to the rest of the operating system. Removing this kind of services will eliminate the chance for exploitation. But it may also make it harder to access the system. There are also services in use that carries security risks, this kind of services has to be monitored closely to avoid cases of exploitation.

8.5 Interworking between GPRS networks

Normally all data and signalling between the GPRS operators are transmitted via BGs. The different packets that arrives the BG should fit to the bilateral agreements between the operators. The packet filters in the BG should be configured to drop packets addressed to those interfaces and network elements that is not according to the agreements.

Even if the different operators have some kind of co-operation, they are actually competing about the same subscribers. But we have never heard of, or were able to find, any information about that this is considered as a threat to the operators or to the security in the GPRS.

8.6 Interworking GPRS PLMN and external networks

Newspapers sometimes brig articles on hackers that has got inside a system that is expected to be secured, especially if hackers have got access inside e.g. a banks data system. These data systems are protected by firewalls from the Internet, but hackers are able to get pass the firewall and get the opportunity to make damage to system. Since the GPRS system is connected to the Internet in the same way, hackers that are attacking the bank from the Internet are also a threat to the GPRS system. An important rule to fight the hackers is to have a practical procedure to upgrade the security systems to handle well-known security problems. It is also important that the security system give a notice if some intruders are trying to break into the system [26].

Since the GGSN have more than just Internet connections, but also connections like leased lines, virtual circuits and VPN tunnels, it makes it hard to use a standard, off the shelf, firewall solution. In fact it should also handle different types of interface, e.g. Ethernet and ATM. In the chapter protecting the different GPRS parts we have looked how to handle the complexity of placing firewalls more thorough.

Even if the operators should consider using static routes, it is also a question about how to achieve redundant connections from GGSN to an external network. To achieve redundant connections it is mandatory to use dynamic routing. This is because when dynamic routing is used the router knows much more about how the traffic flow is, and can than route the traffic where it is most practical.

8.7 Test discussion

Since the security test discussion may contain information that is considered confidential by Ericsson, it is removed from the main report. The results from the test are in Apendix 1, which will be made available on request and approval from Ericsson or Lars Line.

9 Conclusion

The user of the mobile phone is responsible to look after the phone, but it is possible to improve the security related to the terminal. This means that the manufactures have to take the IMEI more serious and that the operators make the possibility to clone SIM card more difficult. This may result in upgrading the software and the hardware not only in the ME and the SIM card, but also the operator's network. It is not a huge problem for the subscribers to buy a new mobile phone to get the right configuration on it, this is because the user change their mobile phone rapidly. The investment might be more expensive for the manufactures and operators.

Because the decryption take place in the SGSN and not in the BTS, and a new A5 ciphering algorithm has been implemented, the security has been improved. But it is possibility to get the identity of the subscribers e.g. by use of false BTS. This again can lead to eavesdropping on the user traffic. Subscribers should not trust the security of the GPRS network when transferring confidential data more than he does using the Internet for the same transfer.

The GPRS backbone is vulnerable for attacks from several points. The fact that it is based on well-known technologies, like the SGSNs operating system, only increases this risk. The subscriber traffic is only encrypted between the MS and SGSN, in other words it will pass through the backbone in clear. The GTP offers encryption but this feature is optional and not used by default. In the case of protecting the backbone, it is important to continuously monitor the traffic and improve the security mechanisms.

It is not possible to exclude that a operator could be a threat for another operator, but agreements is a obligation to offer the subscribers each other services. BG are used to give protection between the operators.

Because the threats from external network, and the fact that there are more people that knows the IP protocol architecture, it is necessary to have strong focus of protecting the system with firewalls.

Even if dynamic routing can lead to denial of service attacks, dynamic routing also give a better performance when there are many subscribers using the network. This is a consideration that the operators should keep in mind when choosing static or dynamic routing.

The test we ran indicated that the system we tested could be vulnerable for intrusion. Since well exploited safety breaches in a system in all likelihood will be included in a system attack, is it important to remove or fix faults as soon this are discovered. Information that could be misused was also revealed when looking at the packet stream on the backbone. Mechanisms for secure transportation of information on the backbone should also strongly be considered used. Since a extensive group of people has access to the network, the way access rights are handled is crucial.

References

[1] ETSI TS 100 929:
Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 V6.1.0 Release 1997)

[2] ETIS EN 300 920:
Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 V7.1.1 Release 1998)

[3] ETSI TS 100 614:
Digital cellular telecommunications system (Phase 2+); Security management (GSM 12.03 V8.0.0 Release 1999)

[4] ETSI TS 121 133:
Universal Mobile Telecommunication System (UMTS); 3G Security; Security Threads and Requirements (V3.1.0 Release 1999)

[5] ETSI TS 133 120:
Universal Mobile Telecommunication System (UMTS); 3G Security; Security Principles and Objectives (V3.0.0 Release 1999)

[6] 3G TS 33.102:
3G Security; Security Architecture (V3.4.0 Release 1999)

[7] UMTS Security Architecture (USECA)

[8] Lecture notes from IKT2315 “Signaleringsprotokoller og mobilitet”

[9] General Packet Radio Service (GPRS): Architecture, Protocols and Air Interface. http://zzz.com.ru/art61.html

[10] Authentication and Security in GPRS Environment: An Overview, Lasse Huovinen, Helsinki University of Technology

[11] GPRS Security – Security Remote Connections over GPRS, Jussi Rautpalo, Helsinki University of Technology

[12] GSM and GPRS Security, Chengyuan Peng, Helsinki University of Technology

[13] GPRS System Survey, Student Text, Ericsson

[14] Ericsson GPRS Security Solutions

[15] GSN Routing, Ericsson

[16] Gi/Gn Engineering Guidelines, Ericsson

[17] Securing GSN, Ericsson

[18] ETSI TS 100 922:

Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM); Functional characteristics (GSM 02.17 V8.0.0 Release 1999)

[19] ETSI TS 101 106:
Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements (GSM 01.61 V6.0.1 release 1997)

[20] ETSI TS 100 508:
Digital cellular telecommunications system (Phase 2+); International Mobile station Equipment Identities (IMEI) (GSM 02.16 V7.2.0 release 1998)

[21] ETSI TS 101 348:
Digital cellular telecommunications system (Phase 2+); GPRS; Interworking between the Public Land Mobile Network (PLMN) supporting GPRS and Packet Data Networks (PDN) (GSM 09.61 V7.2.0 Release 1998)

[22] www.whatis.com

[23] GSM Interception, Lauri Pesonen, Helsinki Univerity of Technology

[24] “Computer Networks”, second edition written by Larry L. Peterson & Bruce S. Davie

[25] ETSI EN 301 347:
Digital cellular telecommunications systems (Phase 2+); GPRS; GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (GSM 09.06 V7.5.1 release 1998)

[26] USA kongress rystet:
Selv militære IT-systemer mangler varsel mot inntrengere, Eirik Rossen, 06.04.2001
http://digitoday.no/digi98.nsf/pub/dd20010406122402_ero_46675669

[27] Telecom nr 13/01

[28] www.nmrc.org

[29] Ericsson Security Testing

[30] www.sun.com

[31] www.iss.ie/is.htm

[32] www.iss.ie/ss.htm

[33] http://documents.iss.net/literature/SystemScanner/S242_UG.pdf

Abbreviations

AH	Authentication Header
APN	Access Point Name
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
BG	Border Gateway
BSC	Base Station Controller
BSS	Base Station Sub-System
BTS	Base Transceiver Station
CIA	Confidentiality, Integrity and Authentication
CGSN	Co-located GPRS Support Node
CKSN	Ciphering Key Sequence Number
CS	Circuit Switched
DNS	Domain Name System
DoS	Denial of Service
EIR	Equipment Identity Register
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FAC	Final Assembly Code
FW	Firewall
FR	Frame Relay
FTP	File Transfer Protocol
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSN	GPRS Support Node
GTP	GPRS Transport Protocol
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	Internet Protocol with security extension
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
LEA	Law Enforcement Agency
LIG	Lawful Interception Gateway
LLC	Logical Link Control
MCC	Mobile Country Code
ME	Mobile Equipment
MM	Mobility Management
MNC	Mobile Networks Code
MS	Mobile Station
MSC	Mobile (services) Switching Center
MSIN	Mobile Subscriber Identity Number
MT	Mobile Termination
NE	Network Element

NMSI	National Mobile Station Identification number
NTP	Network Time Protocol
OSPF	Open Shortest Path First
O&M	Operations & Maintenance
PDN	Packet Data Network
PDP	Packet Data Protocol
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PS	Packet Switched
PSTN	Public-Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAI	Routing Area Identity
RAND	RANDom number
RPC	Remote Procedure Call
Sec Lab	Security Laboratory
SGSN	Serving GPRS Support Node
SGSNn	Serving GPRS Support Node new
SGSNo	Serving GPRS Support Node old
SIM	Subscriber Identity Module
SMS	Short Message Service
SNR	Serial NumbeR
SRES	Signed RESponse
SS7	Signalling System number 7
TA	Terminal Adapter
TAC	Type Approval Code
TCP	Transmission Control Protocol
TE	Terminal Equipment
TLLI	Temporary Logical Link Identity
TMSI	Temporary Mobile Subscriber Identity
VC	Virtual Circuit
VLR	Visitor Location Register
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network

Glossary

Chipering

Chipering is a method of encrypting text, in which a cryptographic key and an algorithm are applied to a data stream to produce chipertext.

Session management

Session management. A user may have several subscribed contexts, any of the contexts can be activated or deactivated independently

Buffer Overflow Attacks
The most common kind of DoS attack is simply to send more traffic to a network address than the programmers who planned its data buffers anticipated someone might send. The attacker may be aware that the target system has a weakness that can be exploited or the attacker may simply try the attack in case it might work [22].

COMP128
A one-way function that is currently used in most GSM networks for A3 and A8. Unfortunately the COMP128 algorithm is broken so that it gives away information about its arguments when queried appropriately. This is an undesired and unacceptable side effect in a one-way function [23].

DHCP - Dynamic Host Configuration Protocol
DHCP is a communications protocol that lets network administrators manage centrally and automate the assignment of IP addresses in an organization's network [22].

Hijacking
Hijacking is a type of network security attack in which the attacker takes control of a communication. In one type of hijacking also known as a man in the middle attack, the perpetrator takes control of an established connection while it is in progress [22].

LLC - Logical Link Control
LLC is a protocol which is responsible to maintain communication channel between an individual mobile station and the GPRS core network across the radio interface [10].

PDP - Packet Data Protocol
PDP is any protocol which transmits data as discrete units known as packets, e.g., IP [1].

PDP address - Packet Data Protocol address
PDP address is used to point a particular PDP entity. In GPRS PDP address may be dynamic or static. The operator gives dynamic address during PDP context activation. Static address is assigned permanently at subscription time [10].

PDP context - Packet Data Protocol context
Each PDP address is described by an individual Packet Data Protocol context in the MS, SGSN, and GGSN. Every PDP context exists independently in the states active or inactive. The PDP context must be active for data transmission using that PDP address [10].

RADIUS – Remote Authentication Dial-In User Service
RADIUS is a client or server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point [22].

Appendix A ..... Confidential

Since the security test may contain information that is considered confidential by Ericsson, it is removed from the main report. The results from the test are in Apendix 1, which will be made available on request and approval from Ericsson or Lars Line.

Appendix B

Rits Information Security Solutions Ltd.

ISS Internet Scanner

ISS's Internet Scanner is the network security industry's preferred solution for network vulnerability analysis and decision support. Internet Scanner focuses on the single most important aspect of organisational network risk management – identifying and addressing technical vulnerabilities. Internet Scanner performs scheduled and selective probes of your network's communication services, operating systems, key applications, and routers in search of those vulnerabilities most often used by unscrupulous threats to probe, investigate, and attack your network. Internet Scanner then analyses your vulnerability conditions and provides a series of corrective action, trends analysis, conditional, and configuration reports and data sets [31].

ISS System Scanner

System Scanner provides host-based security assessment analysing security weaknesses not visible to network scanning. While the Internet Scanner determines vulnerabilities by scanning devices at the network level, System Scanner detects vulnerabilities internally on the system level through an System Scanner agent resident on network devices [32].

System Scanner agents are the software components that are installed on the computer that you want to scan. You usually control these agents using the System Scanner console's graphical user interface. A single console can manage large numbers of agents throughout an enterprise [33].

These System Scanner agents allow a security policy to be implemented, managed and controlled across an enterprise from a central point. Each security risk is prioritised by System Scanner based on its relative severity. Once a system has been secured, System Scanner locks down that system's configuration with a digital fingerprint, making it easier to detect unauthorised tampering. System Scanner agents are available for Windows NT and many popular UNIX platforms.