GPRS Security

Charles Brookson December 2001

"Quis Custodiet Ipsos Custodes." - "Who will guard the guards?"
Juvenal's Satires, circa 120 AD

GPRS offers a number of security enhancements over existing GSM security. The standards themselves also offer technical features, which a network operator may choose to use. As well as these features, there are additional security technical features that may be used from proprietary and other industry organizations.

Much more important than the underlying technical features, is to ensure that they are used correctly (or even used at all!), and that all the other aspects of good security are also put in place.

Naturally, since the only secure system is one that is never turned on, and since the desire is to have a working system, both the operator and the users of GPRS must decide on which security measures to use themselves against security attacks and frauds. All these will be have to be based on a risk analysis of the security threats, and the operator should attempt to identify cost-effective solutions to the various security issues. This paper discusses these issues.

1 Security features of GPRS

The technical security offered by GPRS is very similar to that offered by GSM. Identity Confidentiality, Identity authentication, Confidentiality of both the user data and signaling (between the mobile and GPRS serving node – SGSN), and in addition to the GSM standard the security of the GPRS backbone. The detailed security of GPRS is contained within the 3GPP standards [1], but an overview is useful to understand and is described below.

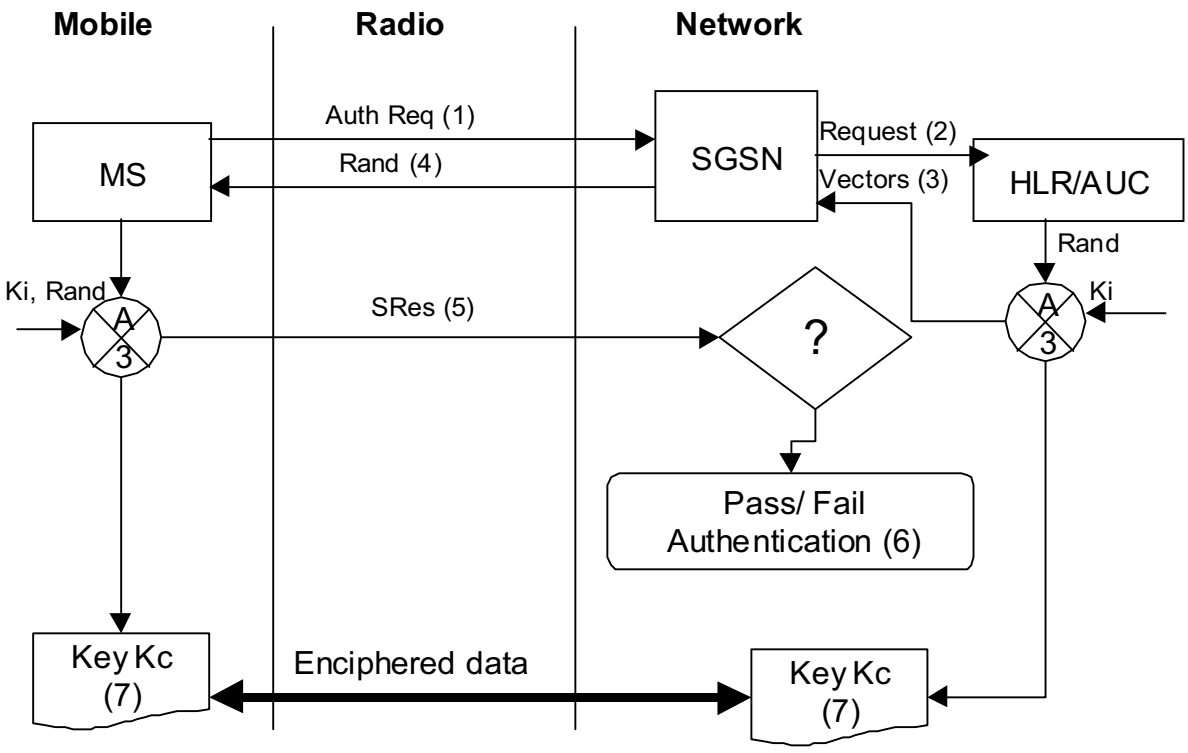

Figure 1.: Authentication and key derivation

Referring to Figure 1 above, the following are the stages for security in GPRS:

1) The Mobile Station (MS) sends an authentication request to the network. This arrives at the SGSN and is sent on to the

2) Home Location Register (HLR) and Authentication Center (AuC). Which generates triplets. These triplets consist of a Random Number (RAND), Signed Response (SRES) and encryption key GPRS-Kc. The first two are used as a challenge and response to authenticate the smart card in the mobile station (or more precisely, that the card has the right key Ki which is associated with the identity (IMSI) and card).

The key Kc is used to encrypt all the data between the MS and SGSN. GPRS-Kc and SRES are calculated from RAND using the authentication algorithm A3/8. This authentication algorithm may be individual for each operator, as only the derived triplets are sent when roaming, and other operators need not know the authentication algorithm.

3) The triplets of vectors (RAND, SRES, and GPRS-Kc) are sent to the SGSN, which sends RAND to

4) The MS. The MS (and Smart Card or SIM) then uses the same authentication algorithm A3/8 to calculate SRES and GPRS-Kc. SRES is sent back to

5) The SGSN, which compares the SRES, returned to it, and the SRES in the authentication triplets.

Charles Brookson

6) If they are identical, then the MS must have the correct authentication algorithm A3/8 and Ki, and therefore is judged to be genuine.

7) Both the MS and the SGSN also have GPRS-Kc, and both use this key to encipher the session between the MS and SGSN.

It is interesting to note that if the MS does not have Ki or the authentication algorithm, it cannot then calculate Kc and the encryption fails. This should prevent someone hijacking a call in progress, as there is an 'implicit authentication' throughout the session, assuming that no other party can derive Kc. Not all the data on this link will be enciphered, as some of the data will need to be used between the MS and SGSN, and so must be left in clear.

A description of the security services offered by GPRS is described below.

1.1 Identity Confidentiality

The objective of Identity Confidentiality is to provide privacy to the subscriber, so it will be difficult to identify the person from their signal over the radio and connections to the SGSN. The identity of the user as an IMSI is avoided where possible, and a temporary identity known as Temporary Logical Link Identifier (TLLI) is used. The TLLI is accompanied by a Routing Area Identity (RAI) to avoid ambiguities. The relationship between the TLLI and IMSI is held within a database in each SGSN.

Where possible the signaling confidentiality is also used to protect identity, such as dialed digits and addresses.

1.2 Identity Authentication

Identity authentication is specified in [2]. Authentication is performed within the SGSN. Pairs of Random Numbers and Signed responses (RAND & SRES) are obtained from the HLR/ AUC and stored within the SGSN.

As in GSM, the challenge (RAND) and response (SRES) are compared by the SGSN to decide if the smart card to be identified has the correct authentication algorithm for A3 and the correct key Ki.

1.3 User and signaling data confidentiality

The user data and signaling key GPRS-Kc is derived by using function A3/8 as in GSM. A 64 bit key called GPRS-Kc is derived. Synchronization is performed by a Ciphering Key Sequence Number GPRS-CKSN, which is described in [3].

Synchronization is ensured by ensuring that GEA is driven by INPUT and DIRECTION bits. Not all the signaling bits can be enciphered, for example Routing Area Update Request message.

1.4 The algorithms

There are seven GPRS Encryption Algorithms (GEA) allowed for in the GPRS specifications, of which two (GEA1 and GEA2) have already been defined by ETSI

SAGE. GEA2 was defined about a year later than GEA1 and was an improvement, which was allowed by the easing of export control legislation.

Negotiation of the GEA in use happens between the mobile and network at the start of the call. Similar considerations to those in GSM for the A5 algorithm allow for new authentication and encryption algorithms to be introduced within the lifetime of the standards.

2 End to end security connections for Services

GPRS does not itself offer end to end security. There are many proprietary and other standards that cover methods of methods of end to end encryption such as those from the WAP forum [5] [6]. Other methods, such as the Internet security protocols covered by IPsec may also be used [7]. Organizations may also set up Virtual Private Networks, and be able to access company information over encrypted links [8].

Some of these techniques do not protect the information from the operator or user, so if you are a third party offering valuable services you will need to study carefully the various possibilities for a scheme that may suit your application.

If they are used, a user may have multiple identities to access various services, such as for shopping, banking, or booking a golf teeing time. These identities will probably only be stored in a terminal, and therefore have also to be protected in some way.

3 Network security

A GPRS network will be based on an Internet packet system. As such it is open to the same security issues as any Internet network from attack.

Care will need to be taken in the design of the network; to ensure those sensitive parts of the infrastructure (such as billing data, encryption keys, and identities) cannot be compromised. There may also be legal constraints, such as data privacy or lawful interception requirements, that mean that encryption, access control or Interception may have to be included within the infrastructure.

Particular attention should be paid to the key management, such as the transportation and storage of keys. With the knowledge of these (such as the individual user key, Ki), an attacker may be able to clone a terminal or service, and bill to it.

4 The Internet

GPRS is designed to connect users to the Internet. Gateways and serving nodes as well as customers will all have Internet addresses, and others networks will also know these. Network mapping software, which easily available can be used to look at the network configuration. For example, terminals within an operator’s network are inside the firewall and therefore, unless the network is properly configured, may have access to the infrastructure.

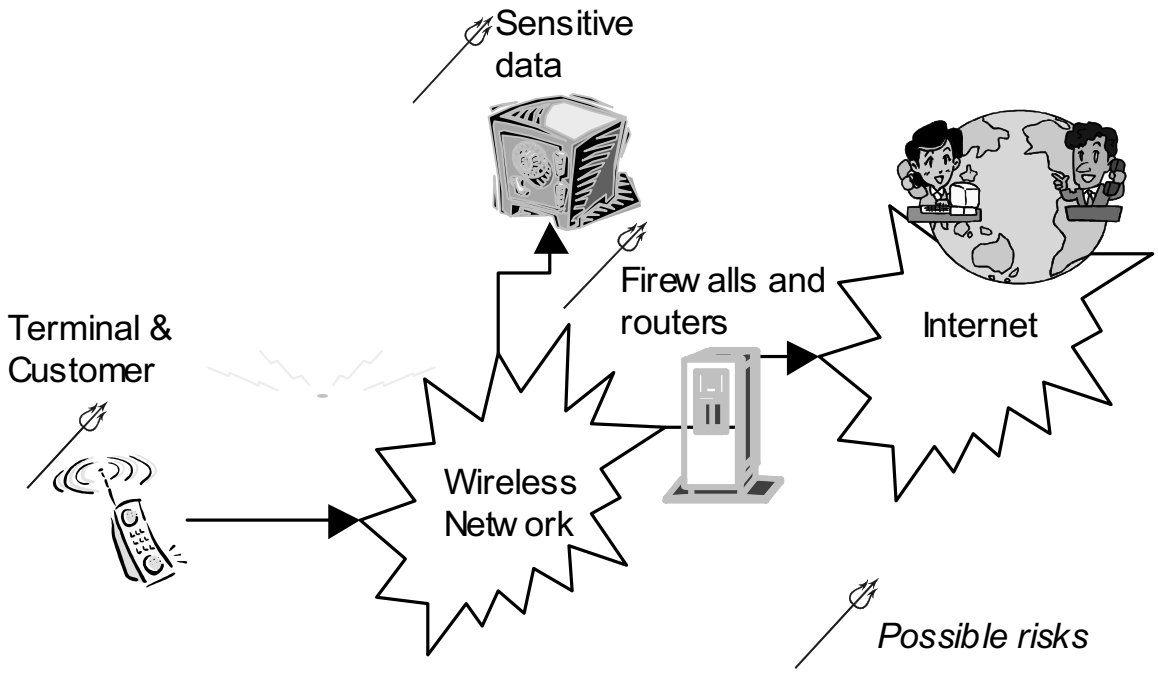

Figure 2.: Internet security issues

Figure 2 shows some of these concerns. Customer's terminals are threatened by rogue code, such as viruses or Trojans. Firewalls and routers must be kept up dated to stop intrusion, and sensitive information such as encryption keys and customer information must be protected. Finally, network information flowing over the Internet must be protected. These security issues are discussed below.

All the Internet security concerns, such as Denial of Service attacks against network nodes and customers are possible. These include the possibility of the compromise of both customer and network data stored on the terminals and infrastructure.

Security concerns that have come to attention in the Internet World must now be considered for the GPRS network. Techniques will include Firewalls, Router control, address translation and hiding and encryption of sensitive data.

The operator will need to now become an Internet security specialist to protect against the attacks and threats that can be expected, as well as updating the software and firewalls continuously to protect the integrity of the network and information against the latest attacks.

Version control of the software will become more important, as will be the ability to test new hardware and software before it brought into service on a live system.

The customer must also be kept informed about the new risks that they face, such as downloading untrusted software and updates to their terminals, browsing untrusted sites on the Internet, or opening email attachments. The nature of the business will change. Wireless operators will now become Internet Information Service Providers, and inform the customer the risks and methods so that both of them may better protect themselves.

5 Viruses and trojans

Terminal equipment will be probably 'always on', and will also be equipped with software like Internet browsing and email services. This means that they will be open to attacks from viruses, trojans, worms and so on.

The use of smart applications and software, which can execute computer code, will be attractive to the virus writers of the world, and allow code to be downloaded to terminals. Such software could perform similar tricks to existing Internet attacks, such as monitoring usage, down loading files, making calls unknown to the user etc.

There will no doubt have to be a range of antivirus software developed to meet these needs. These will be of particular attraction as there is the capability to make revenue from these attacks; ways of doing this are discussed in the potential frauds.

Terminals may have the ability to update their operating systems, and these could also be tampered with to perform unwanted functions. This more likely in the future, with software radios and devices where much of the software is driven by a computer.

Users of cable modems and other similar devices, which are always connected to the Internet, have lead to an increase in various attacks, for example Back Orifice, which allows someone to run your computer remotely without your knowledge. This will also be true of GPRS terminals. Firewalls and similar techniques will have to be used to prevent this type of attack, even on the terminals.

6 General security considerations

An important part of security within a Company is to ensure that all the general security is handled correctly.

This will mean setting up an organization responsible for security, and giving it authority from the management board. The issues that will need to be covered are Pollicies, Information, Electronic Security, Business Security, People Security, Physical Security, Investigations and Fraud.

A useful source of guidance is an International Standards Organization (ISO) standard called "Information technology. Code of practice for information security management" [4]. This covers the areas of:

Compliance
To ensure the systems and processes comply with legal requirements, such as data privacy.

Personnel Security
To ensure personnel are adequately informed and educated in the use and management of security.

Security Organization
To ensure that adequate resources and policies exist for the education, ownership and outsourcing of security.

Asset Classification and Control
To ensure that information and systems are appropriately marked and protected.

Business Continuity Planning
To ensure that in case of interruption, there are plans and procedures in place to ensure that the business processes may continue.

Security Policies
To have supporting policies for information security

Computer & Network Management
To ensure there is adequate protection of networks and computers within a business.

System Access Control
To ensure controls for access to information and electronic resources throughout the business.

System Development and Maintenance
To ensure secure development of software, the use of authentication, privacy and integrity techniques.

Physical and Environmental Security
To protect the assets and information from physical harm.

7 Fraud issues

Fraud is carried out where there is monetary gain to be made. It is difficult to predict what frauds will practical in GPRS, as they will depend on:

- Charging mechanisms,
- Billing mechanism,
- Services offered,
- Technical weaknesses the processes,
- Business weaknesses in the processes.

There are quite a few possible ways of gaining revenue from frauds, and this may make GPRS attractive to a fraudster – Telecommunications crime is a very big business. For example, if the provider of a service is able to get revenue by content charging when a customer views a page or uses a service, then they may be tempted to load rogue software into a customer's terminal to force the terminal to view that content.

Another example would be if the rogue service could force the terminals to make connections to premium rate or infoline services, where the provider of such services gets a share of the revenue. Software could also be introduced to seize the identity of the user of the terminal for use in banking or e-commerce services.

It is possible to develop Fraud Detection Systems (FDS) that will notify you when a fraud is taking place. But to do this you must have first found the fraud and identified the 'fingerprint' as series of rules (for example short calls to certain addresses). So, all FDSs have a weakness that you must have first identified a fraud. It is by far better to build the possibility in the process to protect against the fraud! It is none too clear how an FDS will work on a packet based system, and development work is just starting in this area.

Some FDS also try to work out the rules, so allowing the FDS to detect new patterns that may predict a fraud. Probably a combination of rules based and learning is the ideal solution.

Billing between operators will be on the basis of either the length of time of the connection, or the amount of data sent. This will make it harder to ascertain the types of frauds, as for example; the destination of addresses used will not be transferred between operators.

An issue is likely to be the use of dynamic addressing, where an Internet address is allocated to a user from a pool when it is required, and then returned. This will make it hard to identify a user, especially when the link between the user and address is not retained for a long time.

8 Finally

When developing a product or service it is very important to study the whole business process for a potential of misuse. GSM systems in the past have suffered from these problems, such as prepaid based on insecure mechanisms. The same will be true of GPRS.

So GPRS is secure, providing you have thought about the issues, and have taken the right management and technical decisions.

References:

[1] 3GPP TS43.020 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security related network Functions. Note: This was called GSM 03.20.

[2] 42.009 Security Aspects. Note: This was called GSM 02.09

[3] 44.008 Mobile radio interface layer 3 specification Note: This was called GSM 04.08

[4] BS ISO/IEC 17799:2000, BS 7799-1:2000 Information technology. Code of practice for information security management

[5] WAP Transport Layer End-to-end Security WAP-187-TLE2E-20010628-a from www.wapforum.org.

[6] WAP Transport Layer Security WAP-261-WTLS-20010406-a

[7] See the Internet Engineering Task Force, www.ietf.org.

[8] See Certicom on www.certicom.com.