GSM (and PCN) Security and Encryption

Charles Brookson

The purpose for security

All frauds result in a loss to the operator. It is important to recognise that this loss may be in terms of:

- No direct financial loss, where the result is lost customers and increase in use of the system with no revenue.
- Direct financial loss, where money is paid out to others, such as other networks, carriers and operators of 'Value Added Networks' such as Premium Rate service lines.
- Potential embarrassment, where customers may move to another service because of the lack of security.
- Failure to meet legal and regulatory requirements, such as License conditions, Companies Acts or Data Protection Legislation.

The objective of security for GSM system is to make the system as secure as the public switched telephone network. The use of radio at the transmission media allows a number of potential threats from eavesdropping the transmissions. It was soon apparent in the threat analysis that the weakest part of the system was the radio path, as this can be easily intercepted.

The GSM MoU Group produces guidance on these areas of operator interaction for members. The technical features for security are only a small part of the security requirements, the greatest threat is from simpler attacks such as disclosure of the encryption keys, insecure billing systems or corruption ! A balance is required to ensure that these security processes meet these requirements.

At the same time a judgment must be made of the cost and effectiveness of the security measures.

Limitations of security

Existing cellular systems have a number of potential weaknesses that were considered in the security requirements for GSM.

The security for GSM has to be appropriate for the system operator and customer:

- The operators of the system wish to ensure that they could issue bills to the right people, and that the services cannot be compromised.

- The customer requires some privacy against traffic being overheard.

The countermeasures are designed:

- to make the radio path as secure as the fixed network, which implies anonymity and confidentiality to protect against eavesdropping;
- to have strong authentication, to protect the operator against billing fraud;
- to prevent operators from compromising each others' security, whether inadvertently or because of competitive pressures.

The security processes must not:

- significantly add to the delay of the initial call set up or subsequent communication;
- increase the bandwidth of the channel,
- allow for increased error rates, or error propagation;
- add excessive complexity to the rest of the system,
- must be cost effective.

The designs of an operator's GSM system must take into account the environment and have secure procedures such as:

- the generation and distribution of keys,
- exchange of information between operators,
- the confidentiality of the algorithms.

Descriptions of the functions of the services

The security services provided by GSM are:

- ***Anonymity*** So that it is not easy to identify the user of the system.

- ***Authentication*** So the operator knows who is using the system for billing purposes.

- ***Signaling Protection*** So that sensitive information on the signaling channel, such as telephone numbers, is protected over the radio path.

- ***User Data Protection*** So that user data passing over the radio path is protected.

Anonymity

Anonymity is provided by using temporary identifiers. When a user first switches on his radio set, the real identity is used, and a temporary identifier is then issued. From then on the temporary identifier is used. Only by tracking the user is it possible to determine the temporary identity being used.

Authentication

Authentication is used to identify the user (or holder of a Smart Card) to the network operator. It uses a technique that can be described as a "Challenge and Response", based on encryption.

Authentication is performed by a challenge and response mechanism. A random challenge is issued to the mobile, the mobile encrypts the challenge using the authentication algorithm (A3) and the key assigned to the mobile, and sends a response back. The operator can check that, given the key of the mobile, the response to the challenge is correct.

Eavesdropping the radio channel reveals no useful information, as the next time a new random challenge will be used. Authentication can be provided using this process. A random number is generated by the network and sent to the mobile. The mobile use the Random number R as the input (Plaintext) to the encryption, and, using a secret key unique to the mobile Ki, transforms this into a response Signed RESponse (SRES) (Ciphertext) which is sent back to the network.

The network can check that the mobile really has the secret key by performing the same SRES process and comparing the responses with what it receives from the mobile.

User Data and Signaling Protection

The response is then passed through an algorithm A8 by both the mobile and the network to derive the key Kc used for encrypting the signaling and messages to provide privacy (A5 series algorithms).

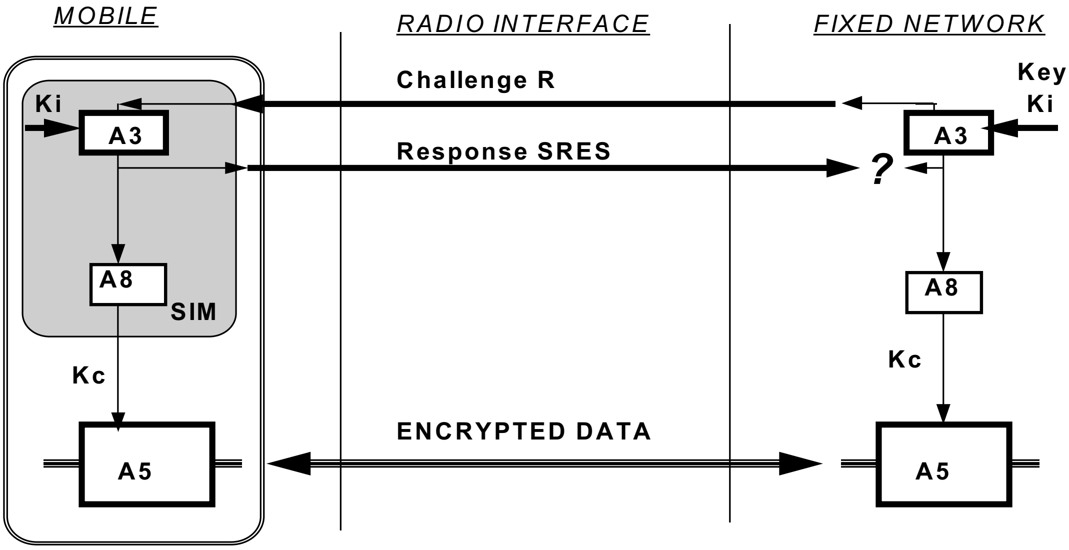

Figure 1. Encryption for GSM

Implementation and Roaming

The authentication algorithm A3 is an operator option, and is implemented within the smart card (known as the Subscriber Interface Module or SIM). So that the operators may inter-work without revealing the authentication algorithms and mobile keys (Ki) to each other, GSM allows triplets of challenges (R), responses (SRES) and communication keys (Kc) to be sent between operators over the connecting networks.

The A5 series algorithms are contained within the mobile equipment, as they have to be sufficiently fast and are therefore hardware. There are two defined algorithms used in GSM known as A5/1 and A5/2. The enhanced Phase 1 specifications developed by ETSI allows for inter-working between mobiles containing A5/1, A5/2 and unencrypted networks. These algorithms can all be built using a few thousand transistors, and usually takes a small area of a chip within the mobile.

World-wide use of the algorithms

There are now three different possibilities for GSM, unencrypted, and use of the A5/1 algorithm or the A5/2 algorithm to secure the data. This arose because the GSM standard was designed for Western Europe, and export regulations did not allow the use of the original technology outside Europe. The uses of the algorithms in the network operator's infrastructure are controlled by the GSM Memorandum of Understanding Group (MoU) according to the formula below:

- The present A5/1 algorithm can be used by countries which are members of CEPT.
- The algorithm A5/2 is intended for any operators in countries that do not fall into the above category.

Export controls on mobiles are minimal, and the next generation of mobiles will support A5/1, A5/2 and no encryption. The protocols to support the various forms of A5 (up to seven) are available in GSM.

Loss areas

There are a number of areas that can be exploited, the most likely intention of all the techniques is the ability to make money at the lowest cost possible.

Technical fraud

Technical fraud is where a weakness of the system is exploited to make free calls. For example, Call Forwarding or Conference Call facilities may be used to give reduced price services to customers from a stolen mobile. These are often known as 'Call Sales Offices'. Hackers are occasionally able to gain access and exploit a weakness in the switching or billing system and gain the ability to make calls or financial advantage.

Technical fraud can be minimised by designing in the features from the start.

Procedural fraud

Procedural fraud results from the exploitation of business processes, where a flaw or weakness can be used to gain money. It may be possible for example to get free calls from a stolen mobile, and sell the calls on for a lower cost than any legitimate network operator.

Procedural frauds are minimised by designing processes so that losses can be stopped by the use of correct policies, flows of information, and taking the opportunity to create a fraud away from the attacker or employee.

Procedural measures are usually the easiest and most cost effective to introduce, Technical measures are expensive, especially when retrospective modification of equipment is required !

Comparison with other frauds

Many of the techniques that can be used to commit fraud on a conventional telecommunications network can also be used for a mobile network. Analogue mobile phone systems were subject to being eavesdropped, and the phones could be cloned so that bills were paid by the owner of the original mobile phone.

Many of these analogue problems can be overcome by using fraud engines, which are described later. But it is often easier to design the technical measures in from the start. Existing cellular systems have a number of potential weaknesses that were considered in the security requirements for GSM.

Networks such as GSM, with international roaming and interactions with other operators, offer other opportunities for exploitation. GSM has been designed to offer various technical solutions to prevent misuse, such as strong authentication, together with anonymity and encryption of the signaling and data over the radio. However, all systems are dependent on secure management and procedures, and lapses in these areas will have a severe impact on the resilience of the business process to fraud.

Other GSM security mechanisms

SIM Card

There is always the possibility (we have no knowledge) that the SIM card can be compromised. This is considered unlikely, especially as some operators use their own version of A3. Keys Ki and the matching IMSI could be compromised by someone selling the information for money.

IMEI

In GSM the customer subscription and authentication capability is contained within a smart card (SIM, Subscriber Identity Module). Any mobile will take on the identity of a subscriber by insertion of a smart card. The mobiles now become attractive items to steal, as they can be used with another SIM card.

To prevent this, GSM has specified an International Mobile Equipment Identifier (IMEI). Although to an operator, at first evaluation, it may seem as the stolen mobiles have no effect, as they do not affect a subscription, there will be problems with an increase in customer facing staff to handle esquires, and a possibility that GSM handsets are expensive to insure.

An Equipment Identity Register (EIR) exists in each network, with Black, White and Grey Lists for stolen or non type approved mobiles, valid mobiles and mobiles that need tracking respectively. Grey lists are for local tracking of mobiles within a network.

GSM has defined a procedure so that approved, lost or stolen mobile IMEIs can be communicated to all other operators. A Central Equipment Identity Register has been (CEIR) proposed. Type approval authorities issue white list numbers (random ranges of valid IMEIs) to mobile manufacturers, and manufacturers inform the CEIR when the mobiles are released to market. All operators are able to post their black lists to the CEIR, and in return collect a consolidated list of all operators black and white lists.
By this method stolen or invalid mobiles can be quickly barred throughout the world.

Roaming
International roaming problems are minimised by the use of two procedures:

- Rapid exchange of billing information by means of EDI
- Notification of the home network of the visitor when the visitor has exceeded a certain billing limit.

Other security related considerations

Credit Checking
Where it is possible to gain service without full credit checking, or verification of the identity of the customer. In some countries, credit checking is not available. Marketing demands for 'instant satisfaction' from the point of sale may also be counterproductive in this respect, although not for a legitimate customer.

Other procedures that need to be carefully designed in are:

- Distribution techniques for the Smart Cards and equipment,
- Polices for the selective barring of areas and other features that can be exploited for fraud, such as 'premium service' lines.
- Checks and balances in internal procedures, such that collusion is required before any crime can be committed.

General IT security to prevent misuse
Supporting the fraud engines, there must be a proper environment to prevent security failures. A typical example of the framework that could be adopted is that in British Standard BS7799. This will also meet enable an operator to meet relevant legal and regulatory requirements.

The Code covers the areas of:

- Security Policy,
- Security Organisation,
- Assets classification and control
- Personnel security
- Physical and environmental security
- Computer and network management
- System access control,
- System development and maintenance,
- Business continuity planning,
- Compliance.

Measurement and Fraud Detection

A properly designed billing system can be used to detect fraud patterns from usage. Different types of fraud often produce a distinct pattern that can be detected, but this is sometimes not obvious from simple inspection of the call records.

It is obvious however, that what we need to detect are:

- Multiple calls at the same time,
- Large variations in revenue being paid to other parties,
- Large variations in the duration of calls, such as very short or long calls,
- Changes in customer usage, perhaps indicating that a mobile has been stolen or is being abused,
- Monitor the usage of a customer closely during a 'probationary period'.

There are some commercial systems on the market that can provide these features. These 'Fraud Engines' enable patterns in billing data to be analysed, and give time for swift effective action.

With fraud detection capability, and security procedures in place, it is possible to minimise the effect of fraud on a billing system.

Summary

GSM provides a basic range of security features to ensure adequate protection for both the operator and customer. Over the lifetime of a system threat and technology change, and so the security is periodically reviewed and changed. The technical security features must be properly supported by procedures to ensure complete security. The security provided by GSM is well in advance of similar mobile radio systems, and should ensure that it remains at the front of the field for some time to come.

However, it is vitally important that these capabilities are designed in from the start, as they will have an impact on the system requirements. Business cases should show the effect of fraud and the costs of protection.