GSM SECURITY: A description of the reasons for security and the techniques

Charles Brookson

The purpose for security

GSM is the 900 MHz radio system using a common world-wide standard. The system use by PCN (DCS 1800) is technically identical, except for the frequency. It allows full roaming from operator to operator if mutual bilateral agreements are in place.

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.

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.

Printed and published by the IEE, Savoy Place, London WC2R 0BL, UK.

GSM MoU Security Rapporteur, British Telecommunications plc, United Kingdom.

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.

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 judgement must be made of the cost and effectiveness of the security measures.

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.
- ***Signalling Protection*** So that sensitive information on the signalling 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 Signalling 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 signalling and messages to provide privacy (A5 series algorithms).

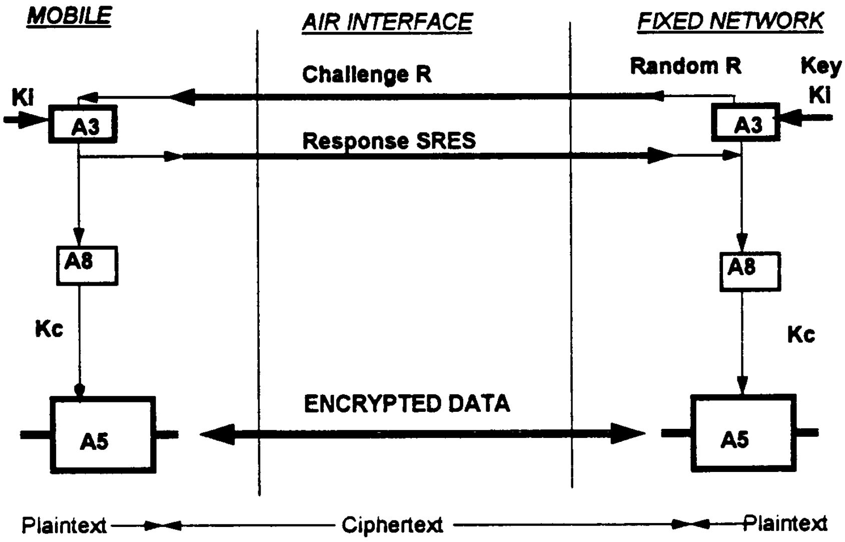

Figure 1. Encryption for GSM

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 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.

The above policy means that operators may use only the appropriate algorithm in base stations. The intention is to minimise export controls on mobiles, where future generations of mobiles shall support A5/1, A5/2 and no encryption. The protocols to support are available in GSM.

Conclusions

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.

GSM is the first time a complete system has been taken to international standard status with security techniques and features. The lessons learnt of the challenges and difficulties have been of use to other subsequent developments (such as CT2 and DECT), as well as non radio applications. Both the customer and operators have significant benefits over the previous generations of land mobile offerings.

Acknowledgements

Acknowledgements are due to the Director of Security and Investigation of British Telecommunication plc for permission to publish this paper.