Zeitschrift: Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri

Band: 70 (1992)

Heft: 3

Artikel: The security of Natel D GSM

Autor: Rueppel, Rainer A. / Massey, James L.

DOI: https://doi.org/10.5169/seals-873978

The Security of Natel D GSM

Rainer A. RUEPPEL and James L. MASSEY, Zurich

1 Introduction

The 'Groupe Spécial Mobile' (GSM) was established in 1982 to formulate the specifications for a Pan-European mobile cellular system. The GSM recommendations are published by the European Telecommunications Standards Institute (ETSI). In Switzerland, the GSM services are called Natel D GSM, and a pilot system has been installed for Telecom 91 (October 1991) in Geneva. In spring 1993, Natel D GSM services will officially begin.

A mobile communications service presents some special security problems. For instance, it is no longer possible to identify a user by the physical line installed between the user's premises and the local exchange. Providing user authentication for a user who is allowed to connect into the network at any point he wishes can only be accomplished with cryptographic means.

2 Threats

The following threats are basic in a mobile communication environment:

1. Loss of confidentiality
   Since GSM uses a radio path to communicate between a mobile subscriber and the base station, anyone can (in principle) tune into a conversation and listen to whatever information is communicated. This threat is very real, as illustrated by the fact that lawyers and doctors in the US are prohibited by law to discuss clients and cases over a car phone.
2. Illegitimate use of service
   A basic problem of every (telecommunication) service is to ensure proper billing. It must not be possible for nonauthorized users to use or to block any of the network's resources. Additionally, it must not be possible for authorized users to impersonate a different user and to make calls on his account. As a consequence, authorized users must be properly identified.
3. Traceability
   Even if the communication between the mobile station and the base station is encrypted, it may be possible from listening to the signalling information on the radiopath to determine the routes and moving patterns of a targeted person. Ensuring untraceability of a subscriber somewhat conflicts with the goal of user authentication. One solution to this problem is to assign temporary random pseudonyms to the subscribers.

3 Security Services

In order to counter the particular threats identified for mobile radio communication, GSM has specified the following security services:

1. user authentication
2. user pseudonyms
3. data confidentiality

31 User Authentication

To avoid identity misuse and to ensure proper billing, users are authenticated each time that they connect to the network. The mechanism used is a challenge-and-response protocol. The user first sends his international mobile subscriber identity (IMSI), the network then challenges the subscriber with a random number (RAND) from a random number generator (RNG). The subscriber has to meet the challenge by sending back a so-called signed response (SRES). SRES is obtained by applying the authentication algorithm A3, parametrized by the user's personal authentication key K_i, to the random number RAND. *Figure 1* illustrates the basic authentication protocol.

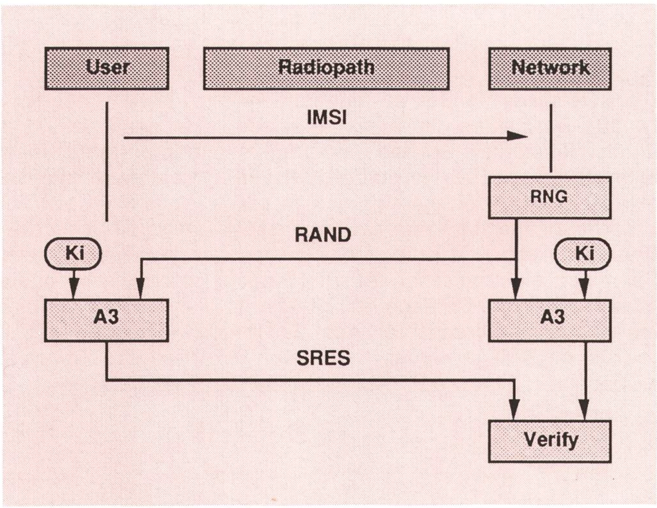

Fig. 1 Basic authentication protocol

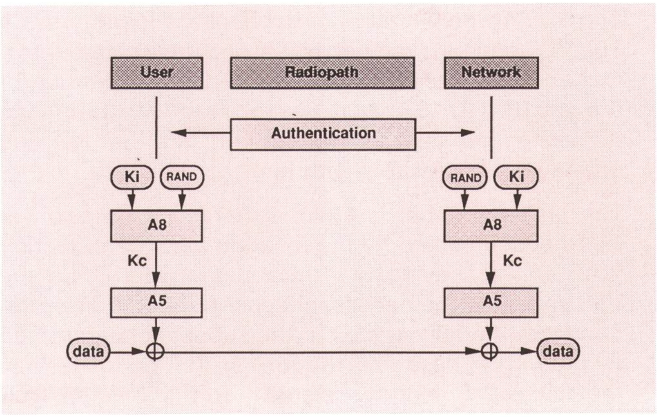

Fig. 2 Encryption of radio path

To relieve the network nodes from the tasks of generating random numbers and computing signed responses and/or to avoid that the network nodes need to know the user's personal authentication key K_i, this security-related information is precomputed by the authentication center and stored in the home location register (HLR) and, possibly, in a visited location register (VLR).

The visited network needs not know anything about the user's authentication key K_i or about the authentication algorithm (A3) employed in the user's home network. Instead, the visited network requests the authentication information (and the encryption key) from the home network of that user.

32 Data Confidentiality

To counter passive eavesdropping attacks, the radio communication is encrypted with a stream cipher (algorithm A5). The key K_c to be used with the stream cipher is derived from RAND and the subscriber authentication key K_i using the key generating algorithm (A8). The key generation takes place in the SIM, and the encryption key K_c needs not be transmitted over the radio path. Of course, before the confidentiality service can be activated, proper user authentication has to take place *(Fig. 2)*.

To activate the confidentiality service, the network sends a ciphering command mode message to the mobile station. Upon reception of this message, the mobile station begins to encipher. To avoid compatibility problems, the encryption algorithm A5 is fixed for the whole of GSM. It is placed in the nonpersonal part of the mobile station, which is called the mobile equipment.

33 User Pseudonyms

To avoid the possibility that an eavesdropper can trace a subscriber based on the identification information exchanged at connection establishment, user pseudonyms are introduced. A user pseudonym is a temporary identity that is assigned to a user after proper authentication *(Fig. 3)*. The value of the so-called temporary mobile subscriber identity (TMSI) is chosen by the network and transmitted to the subscriber in encrypted form. The TMSI is a local identity and valid only in a given location area. The user can initiate the request for a new TMSI. When a user enters a new location area, he can identify himself with his true identity (IMSI) or with his pseudonym (TMSI), which now must be accompanied by the corresponding location area identity (LAI) to allow the network to request the information necessary for authentication. Once the identity of the user has been established, a new TMSI can be allocated.

4 Security Management

The security management is that part of the network management concerned with operations that are outside normal instances of communications but are needed to support and control the security aspects of those communications. The task of the security management is the control and distribution of security-relevant information for

1. providing security services to the users
2. controlling access to the network nodes
3. reporting security-relevant events

Security management is not concerned with the passing of security-relevant information within the protocols at connection establishment.

41 User Enrollment

At subscription time, each user obtains from the administrative center a personal number called international mobile subscriber identity (IMSI) and a personal security module called the subscriber identity module (SIM). The SIM contains among other things:

1. the IMSI of the subscriber
2. the subscriber authentication key K_i
3. the authentication algorithm A_3
4. the personal identification number (PIN) of the subscriber

The SIM may be a chipcard or a plug-in module. It serves to provide secure storage of all personal and secret user data and to compute authentication responses

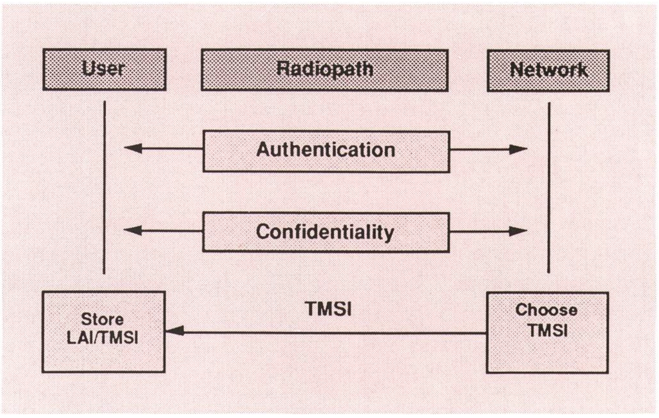

Fig. 3 Assignment of a user pseudonym

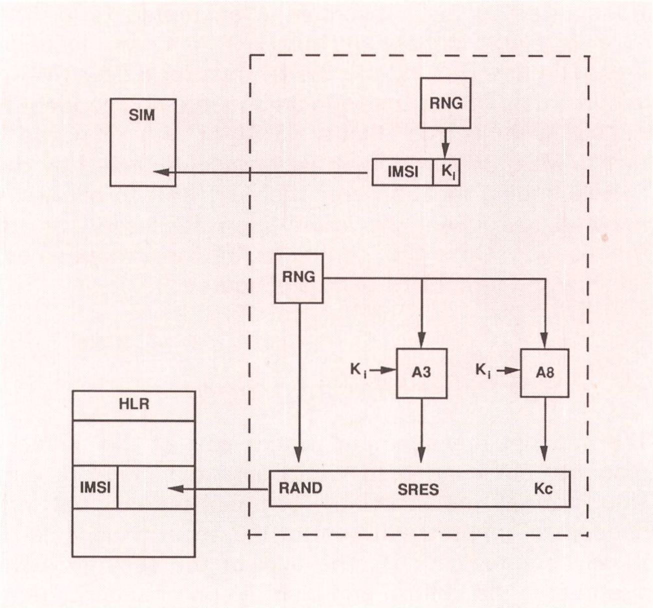

Fig. 4 Tasks of the authentication center

and encryption keys. The SIM must be inserted into the mobile equipment (ME) which contains the radio transmitter/receiver and the encryption algorithm. The SIM personalizes the ME to give a functional mobile station (MS). The GSM services can be used, once the IMSI has been activated in the HLR.

42 The Authentication Center

The entity which is responsible for all security-related aspects is the authentication center (AuC). It has two basic tasks *(Fig. 4):*

1. For each user in its security domain, the authentication center has to generate a personal authentication key (K_i) and associates it with the user's identity (IMSI).
2. For each user in its security domain, the authentication center has to generate the set of authentication data and encryption keys (RAND, SRES, K_c). These sets are transferred to the HLR upon request.

43 The Home Location

Each user has associated his home location area (HLA). That is the subnetwork where the user's permanent address is located and where the user is permanently registered in the home location register (HLR). The HLR stores for each user in its domain, the set of authentication elements and encryption keys (RAND, SRES, K_c) generated by the authentication center.

44 The Visited Location

If a user visits a new subnetwork, the security-related information pertaining to that user has to be transferred to that subnetwork. The visited location register (VLR) serves to temporarily store all security-related information of such visiting users. *Figure 5* illustrates the authentication of visiting mobile stations.

The VLR may obtain that information in one of two ways:

1. The visiting mobile station declares its identity IMSI. The VLR requests the necessary security-related information from the HLR of that user. Upon reception of the set (RAND, SRES, K_c) associated with that user, the visited subnetwork can authenticate the user and communicate securely with him.
2. The visiting mobile station declares its pseudonym TMSI accompanied by the location area identification (LAI) of the previously visited subnetwork. Then the VLR requests the necessary security-related information from the former VLR in the subnetwork identified by the LAI. In case that the former VLR no longer has the necessary security-related information, the HLR will supply the set (RAND, SRES, K_c) to the VLR directly.

   To authenticate a user's identity, the VLR sends the challenge RAND via the switching center and the BS to the user and receives the response SRES. After successful authentication, the VLR generates a pseudonym TMSI and sends that TMSI and the corresponding encryption key to the mobile switching center for further use.

5 Discussion

The GSM security architecture offers a confidentiality service. This service has certain limitations. First of all, it applies only to the radio access link. Thus, there is no end-to-end security. Once the messages have left the

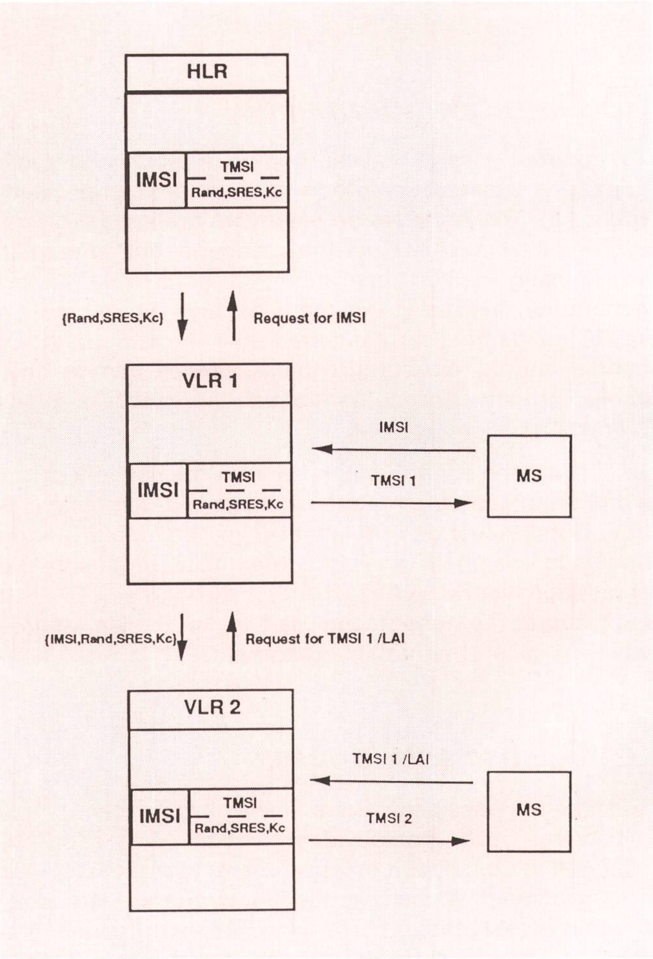

Fig. 5 Authentication of visiting mobile stations

radio path and entered the telephone network, they travel unencrypted. A passive wiretap may succeed here. Also, there is no privacy from the network operator. This problem is aggravated when calls are made from a mobile station in a foreign country and the messages are routed via more than one network operator. The GSM security architecture offers user pseudonyms to achieve untraceability. Again, this feature applies only to the radio access link. The network operator(s) know(s) the true identity of the users; in fact, the network assigns the pseudonyms to the users; hence, the network operator can trace a user if he decides to do so. The algorithms used with GSM are all confidential. Whereas the authentication algorithm A3 and the key generation algorithm A8 are considered a national matter, it is only possible to change the encryption algorithm A5 with the approval of all network operators. Algorithms A3 and A8 could, in principle, be chosen independently by the administration or company operating the mobile network. But typically the network operators will rely on the proposals for A3 and A8 that can be obtained from MOU. Although all these algorithms are confidential, a large number of people will know them. Thus, every puplic land mobile network operator is advised to assess what level of security he is actually offering to his subscribers and what responsibilities and liabilities he is taking.

6 Conclusion

GSM is a step in the right direction. Only recently has the necessity for security services in the public telecommunications environment been acknowledged. But for the next generation of mobile radio systems, it seems desirable to provide truly asymmetric security services in the sense that the users needn't trust the network to generate and maintain their secrets securely. Rather, the users may choose their own secrets and pseudonyms and may authenticate themselves to the network without giving away their secrets. This creates the possibility for true end-to-end confidentiality.

Glossary

A3	authentication algorithm
A5	signalling data and user data encryption algorithm
A8	ciphering key generating algorithm
AUC	authentication centre
GSM	groupe spécial mobile
HLR	home location register
IMSI	international mobile subscriber identity
K_c	ciphering key
k_i	individual subscriber authentication key
LAI	location area identity
MS	mobile station
MSC	mobile services centre
PIN	personal identification number
PLMN	public land mobile network
RAND	random number
SIM	subscriber identity module
SRES	signed response
VLR	visitor location register

Bibliographie

[1] *Stadelmann T.* Natel D GSM, Pan-European Mobile Communication System. Bern, Techn. Mitt. PTT 69 (1991), 9, p. 383.

[2] ETSI/TC GSM, Recommendations 2.09, 3.20, 12.xx.

Addresses of Authors

Dr. Rainer A. Rueppel
R^3 Security Engineering
Bahnhofstrasse 242
8623 Wetzikon

Prof. James L. Massey
Institut für Signal- und
Informationsverarbeitung
ETH-Zentrum
8092 Zürich

Zusammenfassung

Die Sicherheit von Natel D GSM

Wie jede Mobilkommunikationsumgebung bietet Natel D GSM auch einige besondere Sicherheitsprobleme. Die Autoren befassen sich mit diesen Gefährdungen und erläutern die Sicherheitsdienste, die zu ihrer Lösung spezifiziert wurden. Sie zeigen, wie diese Dienste im «Sicherheitsverwaltungs»-Teil der GSM-Netzverwaltung ablaufen, und behandeln schliesslich Sicherheitsaspekte des Gesamtsystems, das sowohl die Funkstrecke als auch einen Teil des Telefonnetzes umfasst.

Résumé

La sécurité du système Natel D GSM

Comme tout système de communication mobile, le Natel D GSM soulève aussi certains problèmes relatifs à la sécurité. Les auteurs passent en revue les dangers à envisager et expliquent les services de sécurité susceptibles d'y remédier. Ils montrent comment ces services s'intègrent dans la gestion des réseaux GSM, dans l'entité dite «gestion de la sécurité», et traitent le système en général sous l'aspect de la sécurité qui comprend aussi bien le circuit radioélectrique qu'une partie du réseau téléphonique.

Riassunto

Natel D GSM: il problema della sicurezza

Come per ogni sistema di comunicazione mobile anche per il Natel D GSM quello della sicurezza è un problema particolare. Gli autori se ne occupano e illustrano i «servizi di sicurezza» specificati per risolverlo; mostrano quindi come tali servizi vengono svolti nella parte della gestione della rete GSM riservata alla sicurezza; trattano infine gli aspetti concernenti la sicurezza del sistema globale, vale a dire della tratta radioelettrica e di una parte della rete telefonica.

Summary

The Security of Natel D GSM

The Natel D GSM System, as any mobile communications environment, presents some special security problems. The authors illustrate these threats and comment on the security services specified to solve them. They show how the services are treated in the «Security Management» part of the GSM network management, and finally assess the overall security of the system, including radio path and telephone network.