in: Günter Müller, Kai Rannenberg (Ed.): Multilateral Security in Communications, Addison-Wesley-Longman 1999, 349-364.

Protection in Mobile Communications

Hannes Federrath

Dresden University of Technology, Department of Computer Science, D-01062 Dresden, Germany

E-Mail: federrath@inf.tu-dresden.de

1 Introduction

In recent years mobile communication has surpassed all expectations. Availability virtually everywhere in Europe, increasingly favorable prices and world-wide service speak for themselves. Mobile voice communication has become a mass product.

GSM (Global System for Mobile Communication) is the best known and most widely used mobile communication standard. It is a European development, which has also found global acceptance. Unfortunately, the advance of security standards has not kept pace with the dissemination of mobile communication.

In spite of this, the security functions which prevent eavesdropping and unauthorized use are emphasized by the mobile phone companies. Frequently (almost always), the fact that encryption is restricted to the radio transmission is concealed. Disputes between a user and the mobile phone company concerning billing cannot be resolved on a formal basis (e.g. digital signatures of the billing data).

The existing mobile communication networks are not safer than the fixed telephone networks. They only offer protection against the new forms of abuse which arise as a result of mobility.

1.1 What data does the mobile user create?

In their advertisements, the network carriers do not talk about the data collected and processed. However, the user leaves behind a large trail of private data:

1. As soon as the mobile phone is switched on, it registers with the network carrier. The identity of the user (international mobile subscriber identity, IMSI, respectively temporary mobile subscriber identity, TMSI), the serial number of the mobile phone and data concerning the current location is transmitted to network internal databases (home location register, HLR, and visitor location register, VLR).
2. Regardless of whether the user is actually making a call or not, the stored location data is updated from time to time (periodic location updating) in order to check the reachability of the mobile phone. When leaving the current location area a location update is necessary, in order to be able to continue to connect calls to the mobile user. This signaling of location updates is transparent to the mobile user, i.e. he does not know when it happens.[1] Table 1 gives an overview of typical updating intervals.

Table 1. Typical periods for periodical location updating

network carrier	country	periodic location updating time constant
D1	Germany	6 hours
D2	Germany	4 hours
E+	Germany	12 hours
ITINERIS	France	6 minutes
MERCURY	England	30 minutes to 4 hours
SPRINT	USA	30 minutes
SWISSCOM	Swiss	2 hours

see http://www.ii-mel.com/interception/mobile_tracegb.htm

3. Each attempted call to a mobile phone is logged and stored by the network carrier, regardless of whether a connection was established or not.
4. The security protocols which have been implemented (encryption, authentication, authorization check) can be „broken“ (e.g. with the IMSI

[1] To check when a (periodically) location updating request is sent by the mobile phone, the user can place his mobile phone very close to a portable transistor receiver and wait until a typical noise („tzzz“) is audible.

Catcher, c.f. section 2.1 or as a result of implementation weakness) – without having to break the underlying cryptography.

Some of the data mentioned above is needed for the functionality of the network, for example the current location; other measures are aimed at repairing malfunctions, for instance, the transmission of the serial numbers of mobile phones.

In order to ensure the interoperability of the equipment from different manufacturers, network carriers and service providers, many mechanisms and protocols have been defined in national, European and international standards. One of these standards is GSM [ETSI_93]. However, if one wants a concrete answer to the question of which data is stored by a network carrier for how long, examining these standards alone is not sufficient. One example is the „backup“ of locations. Table 2 gives an overview of how long different network carriers store the locations of their mobile users. From a technical point of view there is no reason to store a „history“ of locations permanently or for a long time. For purposes of optimization locations only need to be stored temporarily during the optimization process.

Table 2. „Backup“ time of locations

network carrier	**country**	**„history“ of locations stored**
D1	Germany	–
D2	Germany	2 days
E+	Germany	2 days
ITINERIS	France	–
MERCURY	England	–
SFR	France	15 days
SPRINT	USA	–
SWISSCOM	Swiss	7 days

see http://www.ii-mel.com/interception/mobile_tracegb.htm

1.2 Security functions of the GSM

As background to a better understanding of the attacks on the GSM network which are described later, the following gives a brief introduction to the security functions available in GSM. The following functions exist:

- access control by means of a personal smart card (called subscriber identity module, SIM) and PIN (personal identification number),
- authentication of the users towards the network carrier and generation of a session key in order to prevent abuse.
- encryption of communication on the radio interface, i.e. between mobile station and base station,
- concealing the users' identity on the radio interface, i.e. a temporary valid identity code (TMSI) is used for the identification of a mobile user instead of the IMSI.

The cryptographic algorithms which are used to generate and change the TMSI and for encryption and authentication are kept secret (and, in part, remain secret). They are based on symmetric cryptography, i.e. both the network carrier and the mobile user (more precisely, the user's smart card) share a secret key Ki (unique for each user). All security parameters (encryption key, authentication data) are derived from Ki.

Fig. 1 shows the interaction of the security functions using the example of a location update, without describing it in detail. [MoPa_92], for example, contains a detailed presentation of the security functions and protocols of GSM.

2 Security problems and known attacks on GSM

We now describe some known security problems and attacks on GSM. The IMSI Catcher described in section 2.1 discloses the identities of all users within a radio cell, while the attackers described in sections 2.2 and 2.3 attempt to make phone calls at the expense of other users. Section 2.4 describes which data is collected for billing.

The security problems and their solutions concerning the protection of locations are introduced in section 3.

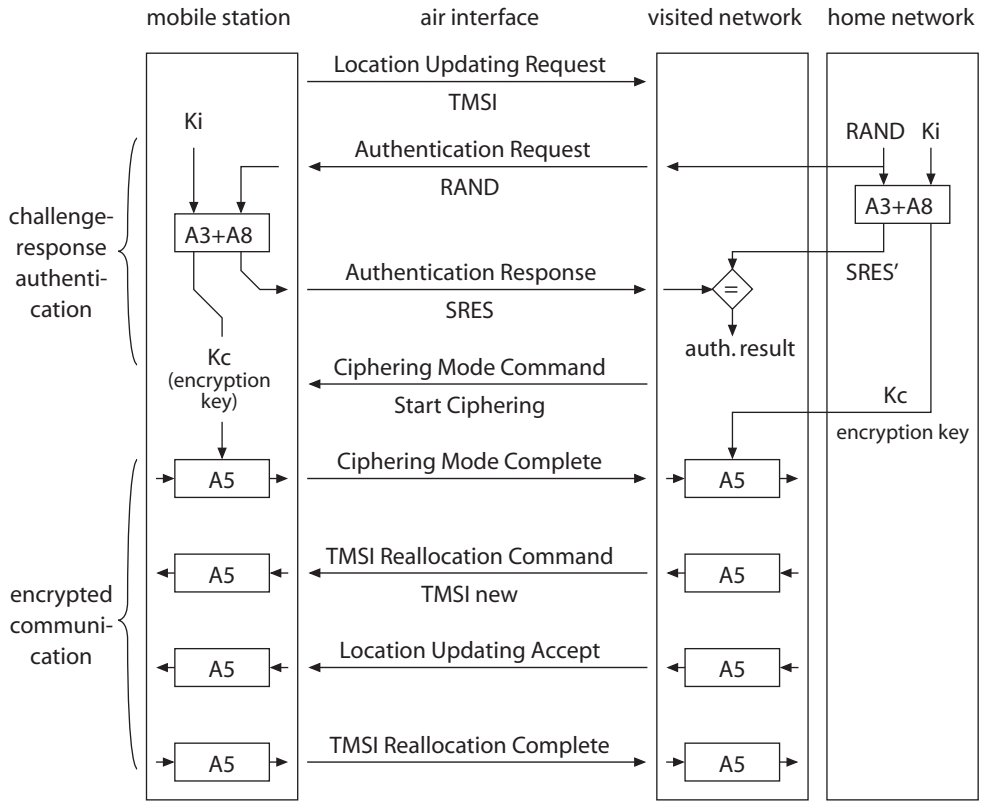


Fig. 1. Use of the security functions of GSM (simplified)

2.1 IMSI Catcher

The name of the IMSI Catcher refers to the abbreviation for the network-internal call number IMSI (international mobile subscriber identity). By directly utilizing „weaknesses“ in the authentication protocols of GSM, it is possible to determine the IMSIs of all users of a radio cell, i.e. the target of an attacker is to determine the identities of mobile users.

The IMSI Catcher is even capable of signaling to the mobile phone that it should discontinue using encryption on the radio link, i.e. between the mobile phone and the base stations.

The type of attack which the IMSI Catcher launches is very simple and is referred to as a man-in-the-middle-attack. It behaves like a base station towards the mobile phone and in relation to the „genuine“ base station of the network carrier it behaves like a mobile phone (see Fig. 2).

Such an attack could have been easily prevented if in place of a one-sided authentication (the mobile phone only authenticates to the network carrier, see Fig. 1) mutual authentication (both users to network and network to users) had been used. Unfortunately, the GSM standard only defines a one-sided authentication.

The technical expenditure for the use of mutual authentication would have been only slightly higher.

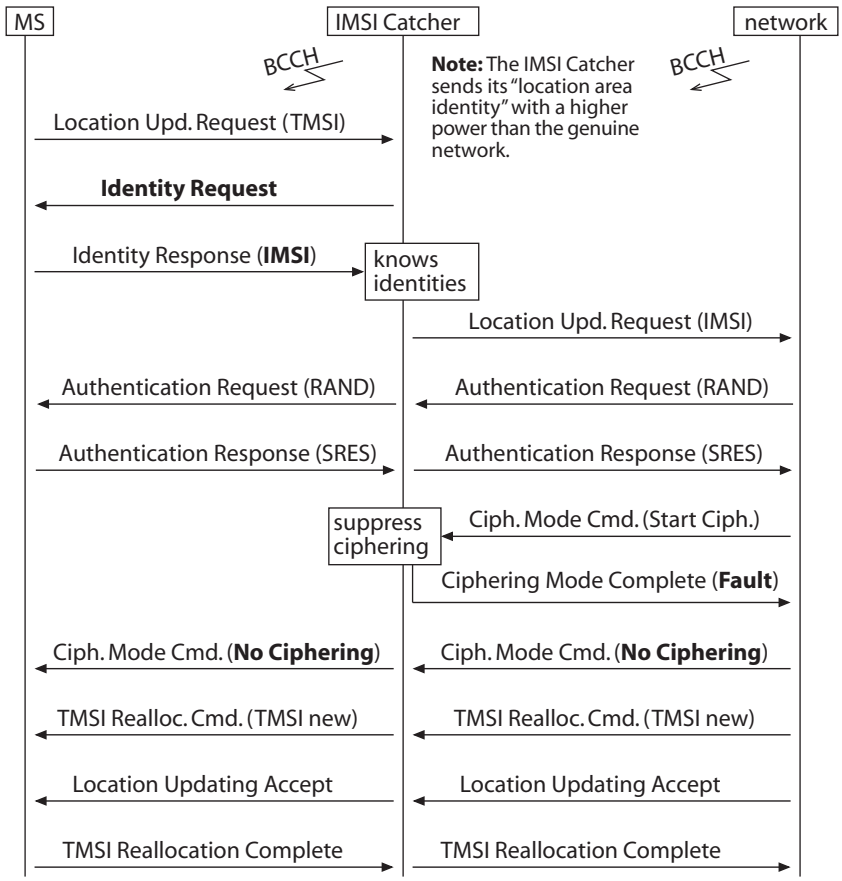


Fig. 2. Catching of IMSIs and suppression of encryption

2.2 SIM Cloning

In addition to the monitoring of users described in the preceding section, the question arises of whether it is possible to make unauthorized phone calls at someone else's expense. The challenge-response authentication of GSM (see

Fig. 1) is intended to prevent this abuse. Unfortunately, the specifications of the cryptographic algorithms are not public. However, documents related to an algorithm COMP128 have been made available. COMP128 implements both A3 and A8. It is published in the Internet, e.g. under http://www.scard.org/gsm/a3a8.txt. After some weaknesses of COMP128 were discovered, the following attack was possible. The attacker has to be in the possession of the smart card and the PIN of the mobile user, at whose expense he wants to make phone calls, for a short time. The attack is executed offline, i.e. without communication to the GSM network. The secret key Ki can be determined after approximately 150,000 requests to the smart card. As a result, it is then possible for the attacker to provide the correct response (SRES) online to the challenge (RAND).

It would now be possible for the attacker to make a „copy“ of the smart card. This attack was revealed by Marc Brienco (Smart Card Developers Association), Ian Goldberg and Dave Wagner (both University of California, Berkeley) and is published in the Internet under http://www.isaac.cs.berkeley.edu/isaac/gsm.html.

It may have been possible to avoid the attack if the algorithm had been published and reviewed by the security community.

Depending on the smart card reader and computer which are used, at present the attack takes about 8 to 12 hours to perform. Since the attack is based on a weakness of COMP128, it only works with smart cards of operators who use exactly this algorithm. A list of operators, who do *not* use COMP128, can be found in the Internet under http://www.scard.org/gsm/.

2.3 Interception of authentication data

It is not possible to make calls at the expense of others with the attack described above exclusively with information intercepted from the radio interface. In the following attack described in [Ande_97], however, this is possible.[2]

---

2 The motivation for Anderson‘s efforts was the advertisement of a service provider, which offered to transfer 10,000 DM to a non-profit organisation, if someone succeeded in making phone calls at the expense of a certain GSM call number. The

Many network carriers connect their base stations by (non-public) radio links. The goal of this procedure is to communicate as much as possible via their own communication links in order to decrease costs. These radio links are usually not encrypted.

If a user registers (location updating) at a base station, he is requested to authenticate himself. The network then creates authentication information (called authentication triple RAND, SRES, Kc) from the individual Ki. The creation of this data is processed in the authentication center, located at the home network operator (see Fig. 1). Since the challenge-response authentication protocol is processed in the mobile switching center which is being visited, the authentication triple has to be transmitted from the home network operator to the visited network operator. If the authentication triple is transmitted over a (usually) un-encrypted radio link, an attacker can eavesdrop and record the information. In the actual authentication request the attacker only needs to answer (respond) to the RAND with the SRES he has just intercepted and he will be authenticated.

2.4 Billing and privacy

As long as the processing of data is the responsibility of one operator alone, he will be able to make his own decisions to a large extent. Otherwise, legal regulations (e.g. privacy laws) apply. A **billing record** in GSM contains at least the following data:

- number of the subscriber who made the call,
- number of the subscriber called,
- location identifier consisting of the switching center, location area and cell identifier,
- trunk group (the physical line, through which the switching center connects the call),
- serial number and type of the mobile terminal used,
- beginning, end, duration of the call,

---

appropriate smart card was deposited with a lawyer. By the time the described attack was published, the service provider had already withdrawn the advertisement.

- cause for the termination of the call (e.g. normal end, interference, recognition of a stolen device, failure of a network component),
- volume of transmitted data (data services only).

At the billing center the billing records have to be sorted and attached to the appropriate user. It is important that the billing data also contains the location identifiers of a connection. Thus, the subsequent localization of users is possible.

Since the periodic messages for location updating can lead to an increased signaling load in the mobile network, the creation of so-called „**location updating records**“ is intended for billing purposes — at least technically. A location updating record contains the old and new location of the user, as well as the appropriate time. Such a location updating record is ideally suitable for the monitoring and tracking of users.

A possible means of preventing the collection of data is the use of pre-paid mobile phone cards. Pre-paid phone cards are not supported directly by GSM, although appropriate offers from network carriers are available. However, they operate with shadow accounts on the basis of a pre-paid amount. Such cards cannot be bought anonymously (at least not in Germany).

Unfortunately, no functions are implemented in GSM which guarantee the user that the invoice is correct. In a dispute the user is has to depend on the fair trading practices of the network carrier.

3 Movement profiles and their prevention

Generally — as a result of the spread of mobile communication — we can assume that the ability to observe users, i.e. who said or did what and when, will be expanded by the question „where?“.

It is frequently claimed that the network carrier needs to know, where a user is currently located, since incoming (i.e. mobile terminating) calls have to be connected to the current location of the user.

However, in normal operation the creation of movement profiles (i.e. permanent location tracking) should be prevented. According to legal regulations, creating movement profiles is prohibited, although it is technically possible. The user should be able to decide to whom he wants to entrust his data.

Even if a user wants to protect himself from tracking by the network carrier, all existing mobile communication networks prevent this. Since the locations of the users are stored, the network carrier can access the data at any time and create movement profiles.

There are occasions, however, when the localization of users can be quite helpful or even life-saving, e.g. in case of an accident.

3.1 Administration of locations

Normally, a network carrier is not primarily interested in collecting data about his users, in order to abuse this data. On the contrary, the less data which is required to provide a service, the lower costs for processing and, particularly, for protection are.

Table 3. Procedures for the prevention of movement profiles (selection)

1. Broadcast method
Avoidance of location data storage and broadcasting (paging) of call requests over the entire area supplied by the mobile network.
2. Group pseudonyms [KFJP_96]
A group of individual users is summarized under a common group pseudonym. The locations of individual users are anonymous within the group.
3. Explicit trustworthy storage of locations
Storing of location data in a trustworthy environment under the control of each mobile user (e.g. a box or a smart card in a special telephone plug socket, attached to the fixed telephone of the user) or with help of a trusted third party (trust center).
4. Temporary pseudonyms (TP method) [KeFo_95, KFJP_96]
Storing of location data in the network, however under a temporary changing pseudonym, and linking of the pseudonym with the identity via a trustworthy environment. This procedure is based on explicit trustworthy storage (see 3.), however, it is more efficient.
5. Co-operating chips [Fede_99]
Storing of location data in tamper-resistant hardware, e.g. a smart card, which is the counterpart to the smart card in the mobile phone. This method can be combined with explicit trustworthy storage (see 3.) and temporary pseudonyms (see 4.).
6. Mobile Communication-MIXing [FeJP_96, Fede_99]
Storing of locations in the network protected with cryptography. Additionally, this procedure prevents the monitoring and observation of calls.

The procedures presented in Table 3 avoid the processing of location data by the network carrier — without restricting the user in his mobility.

The most important concepts in these procedures are:

- Pseudonyms are used as registration numbers of users instead of identities (call numbers).
- Tamper-resistant, trustworthy devices for the storage of confidential data (in particular locations) are used instead of location databases.
- Concepts for the protection of traffic data, e.g. MIXes, are used.
- Special addressing mechanisms, so-called implicit addresses, are used.

3.2 Basic concepts and procedures

In the following we describe a selection of the basic concepts and procedures introduced in section 3.1. For a detailed description of all procedures see the original publications [KeFo_95, KFJP_96, FeJP_95] or [Fede_99].

GSM – no protection of locations

To reach a mobile user (e.g. with an incoming call) the network carrier stores the location of mobile users in data bases (HLR and VLR). When an incoming call arrives for a mobile user the network carrier requests the data bases for the current location of the user (see Fig. 3a).

Since all data base entries are stored under the identity (ID, concretely the call number) of the user, movement profiles can be created by the network carrier very easily — simply by continuously looking up the data bases.

Explicit trustworthy storage – secure but high costs

We assume that a user wants to protect himself by using a trustworthy environment (Table 3, item 3) in the fixed network and storing his locations directly there (see Fig. 3b). If, however, he is located far away from his home residence (more precisely, home location area), e.g. on another continent, in extreme cases the current location identifier will have to be signaled over long distances of the fixed network. This incurs high costs.

In order to deal with this situation, in GSM the location data base is divided. One part of the data base is located in the home residence of the user (home location register, HLR), the other part of the location information is created

and stored in the area being visited (visitor location register, VLR). A VLR serves a large area, therefore, only a change of the VLR area has to be signaled to the HLR. Cell changes are signaled to the VLR without signaling to the HLR.

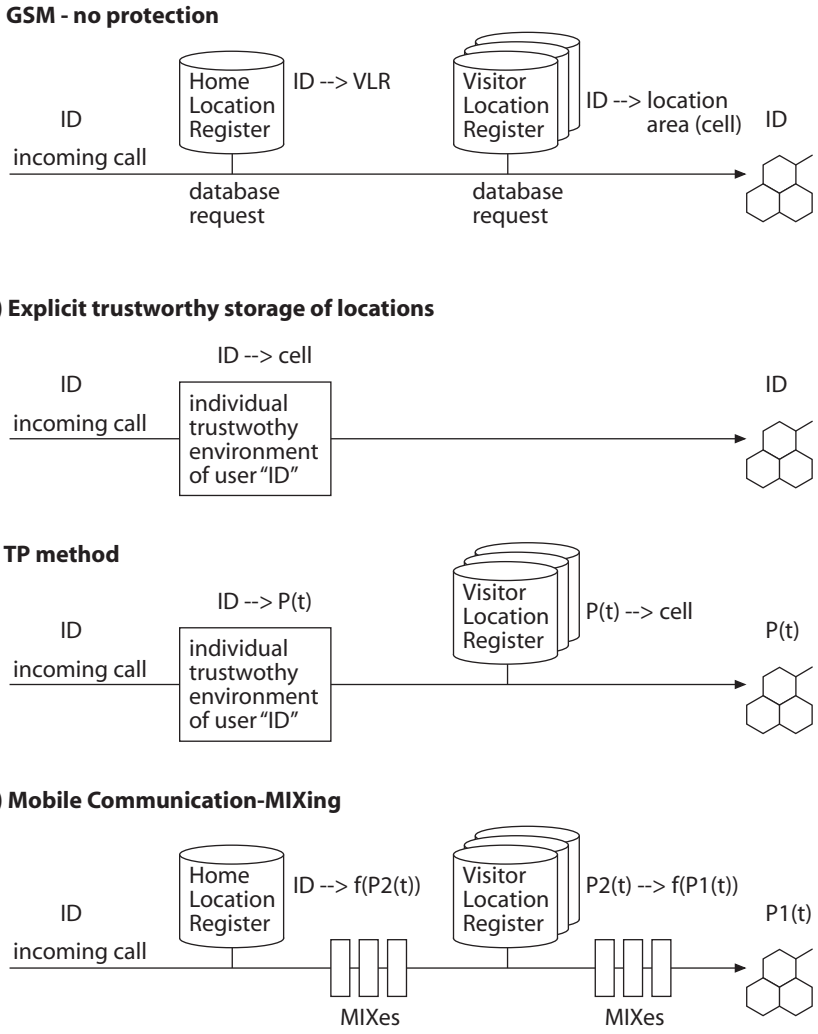


Fig. 3. Connection establishment a) with GSM, b) with explicit trustworthy storage, c) with the TP method, d) with the Mobile Communication MIXing

Pseudonyms in mobile communication

Pseudonyms are used as registration numbers for users instead of identities (call numbers). They work as a linking feature between users and their actions — without disclosing the identity of the user. They are adaptable to the degree

of anonymity desired by a user. For a general overview about the usage and variants of pseudonyms see [PWP_90, PfWa_87].

Pseudonyms for the protection of locations appear to all participants (including the network carrier) like random numbers. Only the user who wants to protect his location knows the association between his identity and his pseudonym.

The TP method [KeFo_95, KFJP_96] (temporary pseudonyms, Table 3, item 4) makes use of such pseudonyms.

TP method

In the TP method (see Fig. 3c) the locations are no longer stored under the ID but under a changing pseudonym P(t). Each change of location is registered under a new pseudonym, and the old one automatically expires after a certain time. Since the pseudonym cannot be linked to a call number, not even by the network carrier, no movement profiles can be generated.

When an incoming call arrives the network carrier requests the trustworthy environment for its current pseudonym, then requests the data bases for the location of the pseudonym P(t) and routes the call to the visiting cell.

In the TP method cell changes need not be announced to the trustworthy environment. The synchronization of the pseudonyms is only checked from time to time (i.e. in the range of minutes to hours) From a technical point of view, especially in the trustworthy environment, this creates problems. It could impair availability, since the user cannot be reached if his trustworthy area has „crashed“ or has been directly attacked.

Mobile Communication-MIXing

It would be desirable to achieve the protection of the location without an individual trustworthy environment. Mobile Communication-MIXing [FeJP_96] (Fig. 3d) offers a solution for this. Special computers, so called MIXes, are switched into the communication line.

The concept of MIXes was introduced for the first time in 1981 by David Chaum [Chau_81]. Chaum's concept was developed for E-Mail, and is, unfortunately, not directly applicable for connection oriented communication. Therefore, adaptations of the basic MIX concept were introduced. In [PfPW_91] a modification for the Integrated Services Digital Network (ISDN)

was introduced. Mobile Communication-MIXing is an additional adaptation in order to apply it in mobile communication networks.

MIXes conceal the relationship between incoming and outgoing messages.[3] MIXes must be implemented, installed and operated independently from the network carrier. Usually, several MIXes are switched in series. Thus, an attacker must either control all MIXes (i.e. crack them) or he must have fed all messages to the system himself, in order to unmask a certain communication relationship.

Implicit addressing for the protection of the recipient

None of the suggested methods for the protection of the location work properly if the identity (call number or other personal identifiers) is transmitted during the paging procedure. In GSM a temporary valid paging code, the temporary mobile subscriber identity (TMSI), is transmitted. It is used to prevent localization through the interception of the radio signals.

If the user wants to protect himself from localization by the network carrier, a so-called implicit address has to be used in place of the TMSI. Implicit addresses enable the user, and only the user, to detect a message intended for him (e.g. connection requests and incoming calls). Implicit addresses are generated with cryptographic procedures.

4 The „costs“ of additional security

The question of the expenditure of such location protection arises, since the development of mobile phones and mobile computing technology is still

---

3 MIXes store incoming messages until sufficient messages from sufficient different senders are available, change their appearance (i.e. coding) and change the order (resorting) of outgoing messages. The kernel function of a MIX is the change of message coding. It is based on public key cryptography, e.g. on the well-known RSA encryption system. In order to prevent attacks by re-sending (replay) of messages, MIXes have to check at the first whether a certain message has already been mixed. In order to prevent attacks by linking of incoming and outgoing messages by means of their length, all incoming messages should have the same length, likewise all outgoing messages.

going on. The Universal Mobile Telecommunication System (UMTS) is one development for the next (referred to as „3rd“) generation of mobile communication.

The bottleneck of a mobile radio system is the air interface. Thus, it is worth discussing the expansion of the message length of the new procedures in comparison to GSM. In Fig. 4 the typical message lengths for establishing communication in GSM, the TP method and Mobile Communication-MIXing (MC-MIXing) are shown and compared. A detailed assessment of all procedures can be found in [Fede_99].

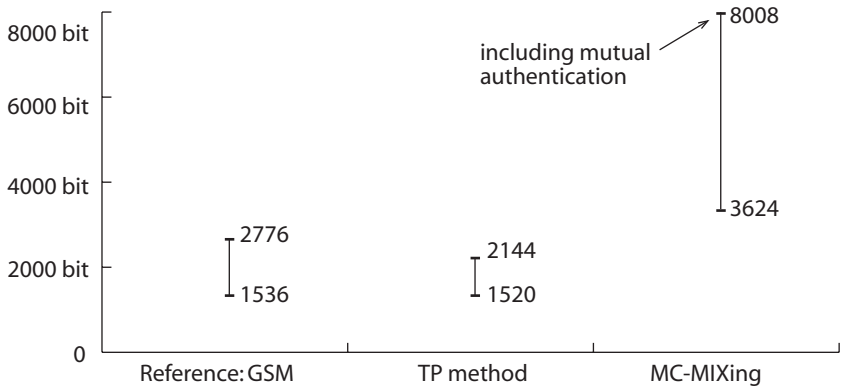


Fig. 4. Message lengths or - intervals of the connection establishment messages

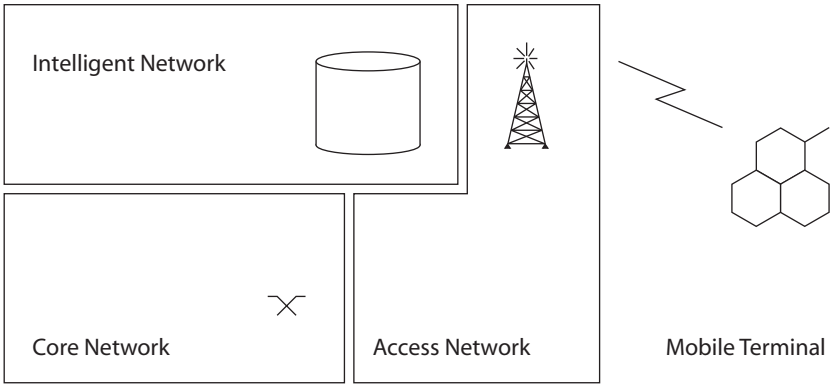
In the TP method the additional expenditure for protection is relatively insignificant, however, it introduces high expenditure in advance, since each user has to purchase a „trustworthy box“, which is installed, for example, to his fixed telephone socket at home. In addition, there are costs for the „re-routing“ of each call to the mobile user.

With Mobile Communication-MIXing there is no additional expenditure for the box (or the additional costs for re-routing), but the public key encryption procedures which are applied to calls from and to the mobile phone result in higher expenditure. Initially, this large expansion of the messages may appear to be a serious problem. However, if we take into account the fact that this public key encryption will be standardly applied in 3rd generation mobile networks, the expansion becomes relative. Note, that in the GSM no pubic key cryptography is used.

5 What will the future bring? — UMTS!

With its modular structure UMTS is already suitable for supporting concepts such as those which have been described. Three parts, i.e. the components access network, the intelligent network and the core (or fixed) network, are considered appropriate as the architectural base for UMTS [Mitt_94] (see Fig. 5).

Fig. 5. The architectural concept of UMTS



According to this architecture, the fast and flexible implementation of new services is achieved by the concept of the intelligent network. The mobility functions (e.g. location registration and location update) are also implemented. The core network is realized by means of broadband ISDN (B-ISDN). The interface to the mobile user forms a special access network, which is coupled directly to the B-ISDN. Thus, UMTS is no longer „the“ mobile network, but a „network of networks“.

In order to be able to use the variety of services and transmission techniques offered, the development of a multi-functional personal communication terminal (personal Communicator for so-called „terminal mobility“) is necessary. It combines all the mobility options in one terminal. Additionally, UMTS will provide multi-functional terminals installed at a wide range of (public) places in order to facilitate so-called „personal mobility“.

The Universal Mobile Telecommunication System has to unite and combine the existing mobile radio networks (GSM, cordless systems, paging services, etc.) within a common platform. UMTS supports new services with higher data rates, better speech quality and even the capability for multimedia services. However, no special features which would allow users to protect their

location information are planned. Thus, the question arises of whether UMTS still offers options for the installation of the procedures described above.

Unfortunately, no strong preventive measures against the creation of movement profiles have been designated in the standardization of UMTS. To a certain extent the situation has even been intensified, in contrast to the GSM, by the introduction of so-called advanced location management procedures with the aim of increasing efficiency. As long as the standardization process for UMTS remains open, there are still opportunities to define appropriate location protection functions. The installation of appropriate security functions after standardization has been completed would result in higher costs and unnecessary compromises.

References

Ande_97 Ross Anderson: GSM hack – operator flunks the challenge. Risks-Forum Digest 19/48 (1997).

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

ETSI_93 ETSI: GSM Recommendations: GSM 01.02 - 12.21. February 1993, Release 92.

Fede_99 Hannes Federrath: Sicherheit mobiler Kommunikation. DuD Fachbeiträge, Vieweg, Wiesbaden 1999.

FeJP_96 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy. in: R. Anderson (Ed.): Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996, 121-135.

KeFo_95 Dogan Kesdogan, Xavier Fouletier: Secure Location Information Management in Cellular Radio Systems. IEEE Wireless Communication System Symposium 95, Proceedings, Long Island (1995), 35-46.

KFJP_96 Dogan Kesdogan, Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Location managment strategies increasing privacy in mobile communication. in: Sokratis K. Katsikas, Dimitris

Gritzalis (Ed.): Informations Systems Security, IFIP SEC '96 Conference Committees, Chapman & Hall, London, 1996, 39-48.

Mitt_94 Hakan Mitts: Universal Mobile Telecommunication Systems - Mobile access to Broadband ISDN. in: W. Bauerfeld, O. Spaniol, F. Williams (Ed.): Broadland Islands ´94, Connecting with the End-User, 1994, 203-209.

MoPa_92 Michel Mouly, Marie-Bernadette Pautet: The GSM System for Mobile Communications. A comprehensive overview of the European Digital Cellular Systems. ISBN 2-9507190-0-7, published by the authors, 1992.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead. 7th IFIP International Conference on Information Security (IFIP/Sec '91), Elsevier, Amsterdam 1991, 245-258.

PfWa_87 Andreas Pfitzmann, Michael Waidner: Networks without user observability. Computers & Security 6/2 (1987) 158-166.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.