An Architecture for more Privacy in Mobile Communication Systems

Uwe G. Wilhelm
Ecole Polytechnique Fédérale de Lausanne
Département d'Informatique
CH-1015 Lausanne (Switzerland)
wilhelm@lse.epfl.ch

Abstract

The privacy of users of mobile communication systems is not very well protected within currently existing systems, such as GSM, D-AMPS or JDC. This is illustrated with the example of GSM.

We propose the *modular architecture* (MARC) for mobile communication, which separates network services from privacy relevant services, by introducing the notion of *anonymous communication* on the level of the underlying network. The two approaches (GSM and MARC) are then compared with the help of a formalization of privacy, which is based on properties that can be identified as having an impact on privacy. We conclude that MARC is more flexible and does provide a better protection of the privacy of its users according to the formalization of privacy presented in the paper.

1 Introduction

Communication has always had a considerable impact on our society. This observation will become especially true for the products that enable mobile communication due to their ubiquitous presence. These systems are currently receiving an increasing amount of attention from various authors, most of which identify an urgent need for strong mechanisms to protect the privacy of their users. Such mechanisms, however, are only rudimentarily developed in currently existing systems (such as GSM[1], D-AMPS[2], or JDC[3]), which threaten the privacy of their users with the large amount of –possibly confidential– data that is generated within them.

Since it is impossible to decide, whether a certain piece of data contains confidential information, we have to make the assumption that all data concerning a person is confidential. Our concern is amplified by the fact that data can be stored easily for arbitrary periods of time and that some data may gain importance over time[4]. We therefore conclude that in order to protect the privacy of a user, all of the data generated by a mobile communication system must be well protected.

[1] Global System for Mobile Communications, Europe

[2] Digital-Advanced Mobile Phone Service, USA

[3] Japanese Digital Cellular, Japan

[4] The entire business of popular media profits from this fact.

This protection is usually provided by laws and implemented by the providers of mobile communication systems. However, even though we generally assume that these providers (such as national phone companies) are trustworthy, we can not assume the same for their employees. The fact that laws will provide threats to deter most people from abusing the data that is available to them, might not be enough to prevent data abuse in the case when the benefits for the offending person outweigh the threats. This problem becomes even more difficult since data abuse is inherently hard to detect and since it is very difficult to prove that it happened in the first place.

From this we conclude that it is insufficient to increase the security and the protection of privacy by merely improving the security mechanisms that protect a system against threats from outside intruders. We advocate that the basic architecture of a mobile communication system has to be improved, in order to provide an inherently better protection of the privacy of its users.

Recent articles in the domain of telecommunications have identified the need to restructure the architecture of modern communication systems (both mobile and fixed) in order to cope with the new tasks and responsibilities of future communication systems. While Garrahan *et al* [GRKK93] only identify the advantage of the independence of network operators from equipment suppliers, Rapeli [Rap95] further develops this idea, by proposing the separation of service provision (i.e., high level services) and network operation. In this paper we want to take their ideas even further and propose an architecture that is more general and flexible than current architectures, with the added advantage that our architecture can provide a better protection of the privacy of its users. We will refer to this architecture as the *modular architecture* (MARC).

Our suggestion is to restructure the architecture of mobile communication systems, by separating network services that handle basic communication with the mobile users from privacy relevant services that handle confidential data. This separation can be realized by introducing the notion of *anonymous communication* on the level of the network, which means that users do not identify themselves to the network provider.

The paper is organized as follows. In Section 2 we introduce our formalization of privacy. Then in Section 3 we describe the architecture of GSM. Next in Section 4 we present the modular architecture. In Section 5 we will compare the protection of privacy in the two architectures according to the formalization in Section 2. Finally, Section 6 concludes the paper.

2 A Formalization of Privacy

The issue of privacy is rather complicated, since it does not lend itself to simple or precise mathematical definition. Several proposals for a definition can be found in the literature, such as one of the earliest by Warren and Brandeis [WB90]: privacy is "the right to be let alone". However, we do not want to enter a philosophical discussion about privacy, which would – due to the disparate opinions of each person – probably not lead to applicable results. The definition we will use for this issue is more pragmatic.

We consider the issue of privacy in the very wide context of an interaction, which we understand to mean any form of transaction (e.g. purchase, bank transaction) or communication between multiple parties. Our approach will establish some basic privacy relevant properties that can easily be identified as having an impact on the privacy of the involved persons. These properties are then investigated within different protocols for a given interaction, in order to compare the privacy provided by these protocols. In this Section we will establish these privacy relevant properties, which will be used for the comparison in Section 5.

A basic hypothesis is that a person, who does not interact with another person or institution, has ultimate privacy, since he does not disclose any information about himself whatsoever. Obviously such a behaviour limits the possible actions of this person far too much. However, we conclude from this hypothesis that privacy is closely tied to information disclosure and that an interaction, in which less personal information is disclosed provides more privacy. Thus we postulate **minimal disclosure** as our first privacy relevant property. If we can identify the minimal amount of information that has to be disclosed by the participating parties in a given interaction (which is usually a very difficult task), then we assume that a protocol for this interaction that discloses only this minimal amount of information provides the best protection of the privacy of the participants.

Another related privacy relevant property tries to assess to which degree the user has control over the information about himself that is disclosed in a given interaction. This property is very similar to the one identified by Schoeman in [Sch84]. There are basically three cases, in which the user does not have control over the disclosed information. First, an intermediate entity, that facilitates or enables the interaction might add additional information to an interaction; e.g. in the ISDN phone service, phone companies routinely send the telephone number of the caller to the callee (caller id service). Second, the other party refuses to conduct the interaction on the basis of the minimal information; e.g. a shop might refuse to accept a credit card transaction without some additional proof of identity or a company might refuse to hire a person without having complete access to his medical records. Third, the other party can obtain additional information from the context of the interaction; e.g. the time when or the location where the interaction took place. We conclude that the more **control** a person has over the disclosed information, the better he can protect his privacy.

For most forms of interaction, it is inevitable to disclose personal information, e.g. a bank has information about the financial situation of its customers. In these cases, it is necessary to **trust** the other party not to abuse this personal information or to disclose it to some third party without the consent of the involved person. This trust can stem from the existence of regulating laws, that threaten to punish such a behaviour or from the fear of bad publicity, if violations of the trust become publicly known. In order for the issue of publicity to have some influence on the behaviour of the other party, it is further necessary to have the possibility to choose among different alternatives; this is presently being worked on in the area of telecommunications, with the demonopolization in many european countries.

In summary, we will assess the protection of privacy in a protocol for some interaction, by examining the following privacy relevant properties:

- minimal disclosure
- control
- trust

This enumeration of properties is not complete and one could surely find many other important properties to assess. However, in the context of mobile communication, the proposed properties are sufficient to conduct a meaningful evaluation of the protection of privacy available to the users of such a communication system. We will demonstrate this in Section 5 by comparing two different architectures for mobile communication systems: GSM (Global System for Mobile Communications) and the modular architecture for anonymous mobile communication.

3 The Architecture of GSM

Due to the extensive amount of available documentation and the quite elaborate security features implemented in GSM (Global System for Mobile Communications), we have chosen this system as an example of currently existing mobile communication systems.

We will present an overview of the general architecture and then examine some of the mechanisms we are interested in with a special regard to privacy issues. For a detailed description of GSM, we refer the reader to [MP92].

3.1 An Overview

GSM is a very complex system, and can be described from several different points of view. In this overview we are not interested in the technical details of its implementation, but only in the high level entities in the system (called sub-systems) and their interaction. The sub-systems of GSM are presented in Figure 1 and will be explained below.

A subscriber, we will call him Bob, can access the system via a Mobile Station (MS), which consists of a personalized Subscriber Identity Module (SIM) and the Mobile Equipment (ME). The SIM holds all

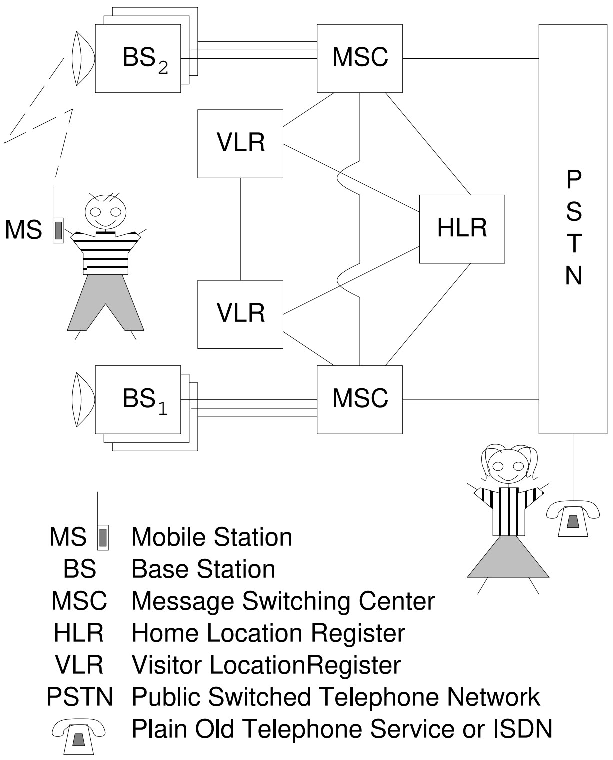

Figure 1: The architecture of the GSM mobile communication system

the personal data concerning the subscriber such as his International Mobile Subscriber Identity (IMSI) and his personal key K_i that is used for authentication and session key management. The ME is completely interchangeable between multiple subscribers, and serves only as interface between the subscriber and his SIM on one side, and the fixed network on the other side.

The Base Stations (BS) are the access point for the users within a given cell. They communicate with the ME of a subscriber via a radio channel and provide the link to the Message Switching Center. The Message Switching Center (MSC) coordinates-ordinates the calls to and from mobile subscribers. A MSC usually serves several BSs and is in contact with the external networks (i.e., the fixed telephone system – PSTN). The Visitor Location Register (VLR) is a database that temporarily stores subscription data for those subscribers currently located in the service area of the corresponding MSC(s) as well as data on the exact location of these subscribers. A VLR may serve several MSCs, but they are often co-located within a single site, since they have a rather close interaction. The Home Location Register (HLR) is the permanent repository for subscription data (i.e., subscribed services, billing information) and it holds data about the current location of a subscriber. One of the important functional entities within the HLR is the Authentication Center (AuC), which is the repository of the key K_i on the network side. (The authentication in GSM is based on a shared key approach.)

3.2 Location Control

Assume that Bob is roaming within the coverage area of a GSM provider. In order to remain reachable for other users, Bob has to register his current location with the system; in GSM the responsible database is the HLR. If Bob is moving from the coverage area of BS_1 to the coverage area of BS_2 (see Figure 1), his MS will sense this location change by measuring the signals from the different BSs and register this information with the system as follows (we assume that BS_1 and BS_2 are connected to different MSCs; otherwise the HLR is not involved in the location change). A schematic representation of the message exchange is depicted in Figure 2.

Upon registering with BS_2, Bob will identify himself to the MSC, by sending his IMSI (in GSM there is an elaborate mechanism to avoid sending this identifier as a clear message over the radio channel). The MSC will then contact Bob's HLR (which is encoded in his IMSI), in order to obtain a challenge-response pair[5] for authentication, together with a session key and will then send the challenge to Bob's MS. The MS uses the challenge to calculate the response and the session key, which both depend on the secret subscriber key contained in the SIM (Subscriber Identity Module) within Bob's MS and returns the response to the MSC. Now the MSC verifies whether the response obtained from Bob is identical to the one obtained from the HLR. If this is the case, then Bob is authenticated to the MSC, and both share a secret session key K_s, which is used to establish a protected channel between them. The MSC finally informs Bob's HLR of the fact that Bob is registered in its domain and will receive Bob's subscription data, which it stores in the VLR associated with the MSC.

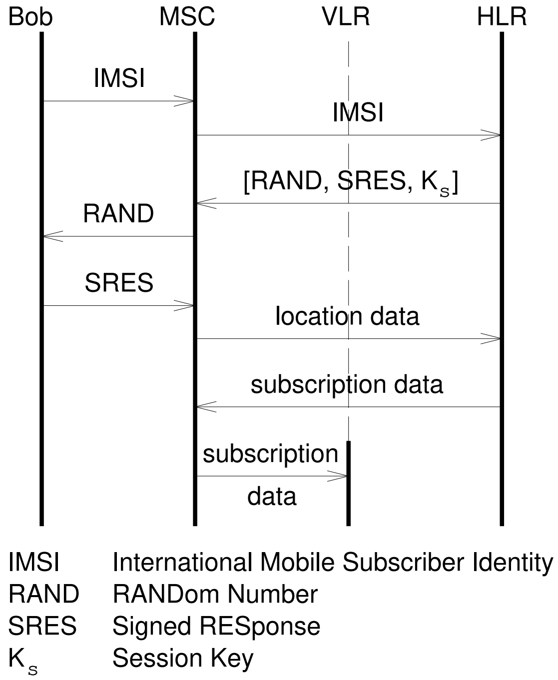

Figure 2: Location update and authentication in GSM

Assume now that another user, we will call her Alice, tries to set up a conversation with Bob. She dials Bob's number, in

[5]In GSM the two values are called RAND and SRES.

which the corresponding GSM provider is encoded. Her switching station will contact Bob's HLR and obtain the MSC, with which Bob is registered. This MSC has a fixed address within the network, so that Alice's call can be routed to the corresponding MSC. The MSC will now contact Bob (maybe with some further information stored in the associated VLR) and complete the communication channel between Alice and Bob.

In the described interaction, which uses only the basic functionality of GSM, the GSM provider does obtain a lot of information about Bob. Here is a summary of the information obtained:

- Bob's identity (authenticated)
- Bob's location (a trace of locations is possible)
- Bob's communications (the entire list of communications is stored for accounting purposes)

We consider all of this information as confidential and, hence, necessary to protect.

4 The Modular Architecture

The basic idea of the *modular architecture* (MARC) is the separation between network services that handle basic communication with the mobile users and privacy relevant services that handle confidential data. The service offered by the network service provider consists solely of the provision of an *anonymous communication platform* (ACP), which allows a mobile user to communicate with other entities in the system, without identifying himself to the network service provider. The ACP constitutes the basic communication facility, upon which all other services are implemented. The privacy relevant services are isolated into Protected Servers, implemented by independent providers on top of the ACP. These independent providers are considered to be at least as trustworthy as the communication service providers, but we hope that competition and laws will create an environment of high trust, comparable to the one in which banks operate. Any interaction between a mobile user an a Protected Server can be secured with any suitable encryption algorithm [DH79, Sch94].

We now want to define the ACP and then continue to identify the privacy relevant service, which is necessary to create a working mobile communication system. Figure 3 gives an overview of the proposed architecture, which will be explained in more detail below.

4.1 The Anonymous Communication Platform

The basic architecture of the ACP (see Figure 3) is very similar to the architecture of GSM presented in Section 3. The user has a Mobile Station (MS), which contains all the necessary personal information about the user (e.g. identity of the user and encryption keys). This MS can be subdivided into a personalized Subscriber Identity Module (SIM) and some exchangeable Mobile Equipment (ME). The ME is able to communicate with any Base Station (BS) that is within its radio coverage. Several BSs are connected to a Message Switching Center (MSC) which can route calls to other entities in the network via the PSTN (or any other available network). However, upon communicating with a MSC, the MS does not reveal the identity of its user, but remains anonymous. This anonymity constitutes the most basic concept of the ACP.

There are no databases like the VLR or HLR in the ACP; due to the anonymity of

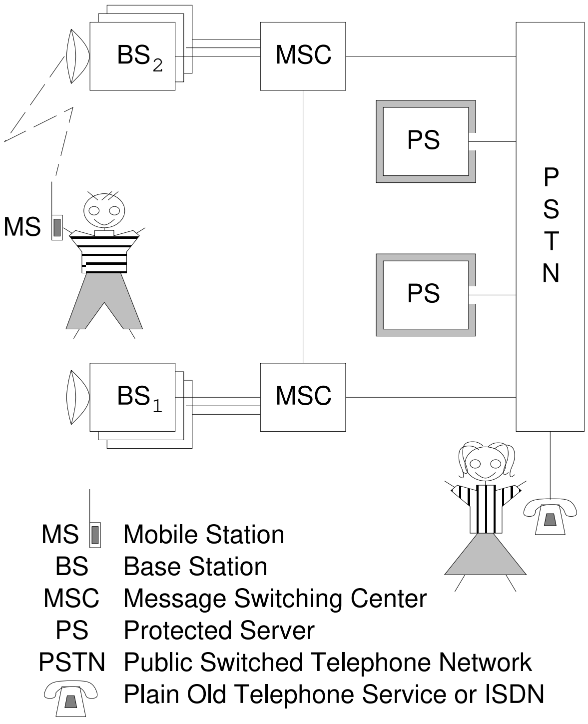

Figure 3: MARC – a modular architecture for mobile communication systems

the users, there is no such information available.

Another important concept of the ACP is the *temporary address* (TA), assigned to a MS. It is assigned by the MSC upon request of a local MS. The TA is valid throughout the entire communication network and can be used to address the MS, to which it is assigned to, as long as the MS is still reachable by the MSC that assigned the TA. We assume that the TA contains no decipherable information for any entity outside the ACP, concerning the location of the MS it is assigned to. This can be accomplished by encrypting the TA with a key that is only known to the ACP provider.

The functionality offered by the ACP is as follows:

- it will assign a TA to a MS upon request;
- it will deliver messages addressed to a TA to the associated MS (if reachable);
- it will transport a message with a valid address (this can be a static address of a well-known service or a TA of some other mobile user) from a MS to its destination;
- it will set up a regular communication channel[6] between two entities with valid addresses.

This functionality is also very similar to that of GSM and could therefore be implemented using the same hardware. With the described ACP, it is possible to support calls from mobile users to stationary entities (we assume that a stationary entity can be located with a regular telephone number). However, in order for mobile users to be reachable, we have to introduce an additional service (*anonymous call set-up*), which will be discussed in Section 4.3.

4.2 Accounting

A very important question in the context of anonymity is, how the ACP provider can recover the payment for his services. This problem deals with the economical aspects of a mobile communication system.

The ACP provider offers a service to its users, for which it has to charge them based on their usage of this service. Since the ACP has no information about the identity of a certain user, this issue can not be solved by simply accumulating the amount of data transferred and charging the user after a certain period of time as in existing systems. The solution proposed for this problem is to use *anonymous electronic cash* [CFN88].

In this approach, a user is required to pay for each piece of data that he wants to send

[6] The system might offer several types of communication channels with different QoS requirements, as in GSM.

over the network immediately, by including the necessary amount of *electronic cash* in the message. In order to reduce the number of payments for the case of an established communication channel, the user could pay the necessary amount of *electronic cash* for a certain time unit in advance. There is a considerable amount of research going on in this area, such as the ESPRIT project CAFE [BBC+94], which describes an *anonymous electronic cash* system with special protocols for "paying phone ticks, i.e., many payments of very small amounts to the same payee in very fast succession".

The usage of *anonymous electronic cash* prevents all problems concerned with defrauding of the ACP provider, since it can verify each payment immediately, before providing the service. The users on the other hand have to trust the ACP provider to perform the service for which they paid in advance; this, however, can be controlled by independent institutions and is not considered a serious problem.

4.3 Privacy Relevant Services

In MARC, the privacy relevant services are implemented within Protected Servers (PS) on top of the ACP (see Figure 3) and thus completely decoupled from the ACP. Nevertheless, the services of the PS can be implemented by the ACP provider, but also by independent companies, which may offer lower prices, better services, or better protection of the confidential information with which they deal. Thus, MARC contains the structure of existing systems as a special case, but is open for new providers.

This constitutes a layered approach, which is a widely accepted tool to control software complexity. Furthermore, this approach requires the precise definition of interfaces to access the services of the PS and prevents any optimization within the system that could compromise the protection of privacy. (The problems concerning the robustness of algorithms for security described in [And] are also applicable to algorithms for privacy.)

Since MARC is structured to prevent internal optimization, it does have a greater communication overhead. The advent of a widespread utilization of fiber-optics in the fixed networks with both high bandwidth and low communication delays, allows us to assume that the communication overhead does not constitute a serious limitation of our architecture, but much rather a reasonable price to pay for the intended benefits.

As an example of a privacy relevant service we will discuss the Location Service (LS), which is necessary to transform MARC into a full-fledged mobile communication system. This service implements the *anonymous call set-up*, which is similar to the task of the HLR in GSM. To illustrate its functionality, we will discuss a small example.

Assume that Bob, a mobile user, has subscribed to the service of some LS provider. He will send periodic location updates, which contain his current TA, to his LS provider. These location update messages are encrypted and authenticated with an algorithm suitable for this purpose, on which Bob and his LS provider have agreed in advance. Note, that the LS is a static entity with a well-known address, so the ACP can easily route the message to the LS.

This approach reverses the responsibilities for location update, which are under the control of the network provider in GSM. In MARC, the user (or rather his MS) is responsible for the accuracy of the location information. This gives the user a direct control over the location information stored in his LS, which can be used to optimize the location strategy with elaborate user profiles and to increase the protection of his privacy (see Section 5).

If another user, we call her Alice, tries to call Bob, she dials Bob's number, in which his LS is encoded. Her switching station will contact Bob's LS and obtain Bob's TA. With the information contained in this TA, the switching station will then set up the communication channel between Alice and Bob.

Again we want to look at the information obtained during the interaction by the various participants. The information obtained by the ACP provider is the following:

- Bob's location
- Bob's communications

However, since Bob did not identify himself to the ACP, this information can not be linked to Bob, and constitutes no confidential information. Furthermore, since Bob requests a new TA any time he enters the area of another MSC, there is no trace of his locations possible (other than with extensive traffic analysis). The information obtained by the LS provider is the following:

- Bob's identity (authenticated)
- Bob's TAs (a trace of these TAs is possible)
- Bob's incoming communications (outgoing communications do not have to pass via the LS)

Note, that the TA does not contain any decipherable information for the LS provider concerning the location of the user. Thus, MARC achieves a *separation of information* on identity and locality. The ACP holds information about the location of the participants in a conversation, but has no information about their identity (unless a participant is associated with a fixed address); whereas the LS provider and the participants know the identity of the participants, but have no information about their location[7]. The property of *separation of information* is one of the central reasons for the improved protection of privacy in MARC and is discussed in the following Section.

5 An Evaluation of Privacy in Mobile Communication

The interactions, in which we are interested for this evaluation, are the examples for location update and call set-up given in Section 3.2 and Section 4.3. We will investigate each privacy relevant property in both presented architectures and discuss the advantages and disadvantages. We want to remark that the concerns that we have about the protection of privacy in GSM are in no way restricted to this system in particular, but are applicable to other mobile communication systems as well.

Due to the close interaction of privacy and encryption, we want to discuss some of the related issues in Section 5.4.

5.1 Minimal Disclosure

As is obvious from the given examples, MARC discloses less information to each participating party than GSM. Thus, we conclude that GSM does not adhere to the principle of minimal disclosure. GSM is so intricate that it is inherently difficult to assess the amount of information necessary to provide a certain service.

In MARC, the network service provider obtains no information at all, other than from the context of the interaction. This

[7]Exceptions for law-enforcement agencies would have to be regulated by laws.

amount could be further reduced with the techniques given in [Cha88, CB95], for the price of a much higher communication overhead.

Any other information that is disclosed, is entirely under the control of the user. Thus, we conclude that MARC does support the principle of minimal disclosure; the implementation of this principle is up to the user or his MS (Mobile Station).

5.2 Control

In GSM, all the information transmitted during a given interaction is defined in the GSM specification and under the complete control of GSM. The amount of confidential information produced and stored in the system depends entirely on the policy of the GSM provider. The user has no influence on this policy, no control over the actual implementation, and very often no knowledge about the contents of this policy at all. Thus, a user has no control over the information that is disclosed about him during a given interaction.

In MARC, the user has complete control over each message that is sent over the network and, thus, on the content and the information disclosed in this message. For example, a user will identify and authenticate himself to his bank in order to conduct a transaction on his account; but he would not identify himself to a bank in order to obtain foreign exchange information.

Since the network – as the only intermediate party – has no information about a user (other than the location of the user, which it is supposed to keep secret), no additional information can be disclosed in the interaction. Again, the only information over which the user has no control, is the information contained in the context of the interaction (e.g. time).

Another aspect of control is linked to user profiles, which are a collection of additional information about a user, intended to be used for optimization of the system. To our knowledge, no existing mobile communication system keeps such profiles – but they are subject to extensive research [IB93, KVP94].

In GSM, such profiles would be kept by the GSM provider. In MARC, they would be handled by the MS, under the control of the user. A user could continuously update his profile, based on information exclusively available to him (e.g. instruct his MS that he will remain stationary for a long period of time, in which he expects many incoming calls).

We do not expect a user to exercise all the means to control the behaviour of the system. This could entirely be managed by the software within the MS, which can be customized according to the requirements of the user.

5.3 Trust

Users do not always have the choice between many different service providers. The investment in the infrastructure of a mobile communication system is so high, that the number of providers is usually rather low. This restricts the influence of publicity on the behaviour of the service provider.

Due to the complexity and sheer size of mobile communication systems, they require a large number of employees for regular operation and maintenance. These employees have more or less restricted rights to access the data within the system. As experiences in insurance companies, banks, and other large institutions have shown, there exists a high risk that an unauthorized person gains access to confidential data [Smi93, Rot92].

The providers of mobile communication systems are usually not very sensitive to privacy issues[8], since they are preoccupied with the very demanding task of providing this service at all. Their basic concern is to provide a functional and profitable service and any additional functionality that is not immediately necessary for the operation of the service is just added complexity.

The issues above suggest that the question of trust is not about the trustworthiness of the service provider itself, but about its ability and willingness to protect the confidential data in its databases from access by third parties.

We assume that the laws that regulate the usage of this data, which are already in place today, will also be applicable to MARC, which has the following additional advantages. The providers of the privacy relevant services (PS providers) will require few, highly skilled, and well paid employees, which are less prone to abuse the information available to them, because they have more to loose if caught in the act. Due to the smaller investment necessary to provide such a service, we assume a considerable amount of competition. This gives the users the possibility to choose between several PS providers. The PS providers will be under surveillance by the media, independent experts, and competitors. Finally, as a result of the separation of information, the PS providers have less information about a user than current GSM providers.

5.4 Encryption

We assume that any interaction between a mobile user (or his MS) and a PS (Protected Server) within MARC is secured by strong encryption and authentication algorithms (see [Sch94]). This assumption is viable, since all the protocols for this interaction have to be newly defined. However, in order to provide real privacy, the content of a conversation has to be encrypted as well (preferably end-to-end). This issue is entirely dependent on the availability of these mechanisms in the fixed network and, thus, deliberately left open.

If the fixed network provides a reasonably strong encryption mechanism (which might also be used for mutual authentication of the communicating parties), then we assume that this mechanism can also be implemented in the MS. In this case, there is no special encryption mechanism for the protection of the messages, transmitted over the radio channel between the MS and the BS (Base Station), necessary.

If one of the participants does not support encrypted communication, the radio channel has to be protected against eavesdroppers. This can either be handled similar as in GSM: the user establishes (via some PS) a shared key with the ACP, the contents of the conversation is encrypted by the MS, sent over the radio channel to the BS, decrypted by the BS, and sent in clear over the network. However, a better solution would be to decouple this task from the ACP and implement it in a PS, which acts as a proxy for the mobile user in such an interaction.

6 Conclusion

The paper has introduced a formalization of privacy, which is based on several properties that can be identified as having an impact on privacy. This formalization constitutes a tool that allows us to reason about the privacy in a given interaction between multiple parties.

We then describe two architectures for mobile communication: GSM (Global Sys-

[8] According to Mouly and Pautet [MP92], one of the reasons to make the explicit functional distinction between the HLR and the AuC in GSM, was to sensitize operators and manufacturers to the security issue.

tem for Mobile Communications) and the *modular architecture* (MARC). The main idea of MARC is the separation of network services that handle basic communication with the mobile users from privacy relevant services that handle confidential data. This separation can be realized by introducing the notion of *anonymous communication*, which allows the isolation of privacy relevant services into protected servers outside the control of the network service provider.

With the help of the introduced formalization of privacy, we argue that MARC provides a better protection of privacy than currently existing systems for mobile communication, such as GSM.

The given description of MARC is still rather vague and leaves many problems of an actual implementation open (such as handover, lack of end-to-end encryption in fixed communication systems, network incompatibilities, or conflicting interests of various standardization organizations). Nevertheless, we are convinced that the ideas, on which MARC is based are "a step in the right direction" — towards a communication infrastructure with a better protection of personal privacy.

References

[And] R. J. Anderson. Making smartcard systems robust. to appear in *Cardis 94*.

[BBC+94] J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. de Rooij, B. Schoenmakers, M. Schunter, L. Vallee, and M. Waidner. The ESPRIT project CAFE – high security digital payment systems. In *European Symposium on Research in Computer Security*, Lecture Notes in Computer Science. Springer-Verlag, 1994.

[CB95] D. A. Cooper and K. P. Birman. Preserving privacy in a network of mobile computers. Technical Report 95-1490, Cornell University, 1995.

[CFN88] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. In *Proceedings of Crypto*, pages 319–327, Berlin, 1988. LNCS, Springer-Verlag.

[Cha88] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1, 1988.

[DH79] W. Diffie and M. E. Hellman. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67(3):397–427, March 1979.

[GRKK93] J. J. Garrahan, P. A. Russo, K. Kitami, and R. Kung. Intelligent network overview. *IEEE Communications Magazine*, 31(3):30–36, Mar 1993.

[IB93] T. Imielinski and B. R. Badrinath. Wireless mobile computing: Solutions and challenges in data management. Technical Report DCS–TR–296, Department of Computer Science, Rutgers University, New Brunswick, NJ 08903, 1993.

[KVP94] P. Krishna, N. H. Vaidya, and D. K. Pradhan. Static and dynamic location management in distributed mobile environments. Technical Report 94-030, Department of Computer Science, Texas A&M University, U.S., jun 1994.

[MP92] M. Mouly and M.-B. Pautet. *The GSM System for Mobile Communications.* Palaiseau, France, 1992.

[Rap95] J. Rapeli. UMTS: Targets, system concept, and standardization in a global framework. *IEEE Personal Communications*, 2(1):20–28, Feb 1995.

[Rot92] J. Rothfeder. *Privacy for Sale.* Simon & Schuster, New York, 1992.

[Sch84] F. D. Schoeman. Privacy: Philosophical dimensions of the literature. In F. D. Schoeman, editor, *Philosophical Dimensions of Privacy.* Cambridge University Press, 1984.

[Sch94] B. Schneier. *Applied cryptography.* Wiley, New York, 1994.

[Smi93] H. J. Smith. Privacy policies and practices: Inside the organizational maze. *Communications of the ACM*, 36(12), December 1993.

[WB90] S. D. Warren and L. D. Brandeis. The right to privacy. In *Harvard Law Rev. 4*, pages 193–220. 1890.