Untraceability of mobile Internet users

Carlos Molina–Jiménez and Lindsay Marshall

Department of Computing Science, The University of Newcastle upon Tyne, U.K.
{Carlos.Molina, Lindsay.Marshall}@newcastle.ac.uk

Abstract. Current mobile telecommunications providers conceal the records gathered about their subscribers from other subscribers and non–subscribers but not from the mobile telecommunications providers themselves. Thanks to the availability of these records, mobile telecommunications providers can easily trace their subscribers and learn about their habits, movements and whereabout. This means that the subscribers' right to individual privacy is not fully observed. We believe that this problem is caused by the use of a centralized billing system and the use of permanent, personal and universal numbers which are used for incoming and outgoing calls and is hard–wired to the mobile internet devices.

In this paper, we argue that a centralized single bill and the use of a universal personal number are not convenient for several applications. We suggest a flexible billing system and the use of mobile internet devices provided with the traditional personal and universal number, and with a mechanism for negotiating a random, impersonal, temporary number. The flexible billing system allows the user to pay locally for the services while the random, impersonal, temporary number is used for outgoing, anonymous calls, whenever the user wishes to access a service without taking the risk of being traced and having his or her right to individual privacy compromised.

1 Introduction

Today's Internet computers and services are accessed mainly from office computers tethered to coaxial cables and from home PCs tethered to telephone wires. Because of this, an Internet user can gain access to the Internet only when he is in his office or at home, but not when he is outdoors. In other words, today's Internet is *confined*. Fortunately, this limitation is likely to be overcome soon (in three to five years) with the integration of the third generation (3G) mobile phone networks into the Internet. This will result in an truly *ubiquitous* Internet.

Thanks to their integration with terrestrial and satellite networks 3G networks provide unlimited communication. A user of a 3G device will be able to communicate with tethered Internet machines and other 3G devices *anywhere—anytime*. By anywhere—anytime communication it is understood that the communication will happen regardless of the time and the current physical location of the communicating parties. A 3G device is a cross between a mobile phone and a pocket–sized computer and is called a Mobile Internet Device (MID) or a Wireless Internet Device (WID).

Currently, 3G networks are still being deployed, yet experts in the communication market predict that they will reach the masses in Asia, Western Europe and North America in less than five years. This means that pretty soon Bob (the user of a MID) will be able to reach Alice (another MID user) and a great variety of services regardless of his current physical location.

So far so good as it seems that Bob will have everything reachable at the touch of a button while on the move. However, the fact that Bob can reach Alice and electronic services from anywhere and at anytime raises issues of the right to individual privacy because this also implies that Bob can be traced anywhere–anytime by people by whom he does not want to be traced, secretely and against his will. The main concern here is that for law abiding reasons Bob might not wish to disclose information about his habits, movements and whereabouts to some of the people and services with which he communicates from his MID. The issue here is a consequence of the trace left behind by electronic devices. Thanks to this trace, Bob's travelling pattern can be deducted from the roaming data collected by his mobile telecommunications provider. Similarly, Bob's movements and whereabouts can be deduced from records kept by his banker [1].

The aim of this paper is to discuss how the right to individual privacy of users of MIDs is compromised because of the traceability of these devices; and to introduce anonymity as a possible and simple solution to this issue.

2 The elements of the ubiquitous Internet

Although it is still being deployed, it is not difficult to predict that a ubiquitous Internet will look (when fully deployed) like the picture shown in Fig. 1. The four parties (subscribers, mobile telecommunications providers, service providers, and eavesdroppers) shown in the picture are, in our opinion, the main parties involved in the issue of the right to individual privacy.

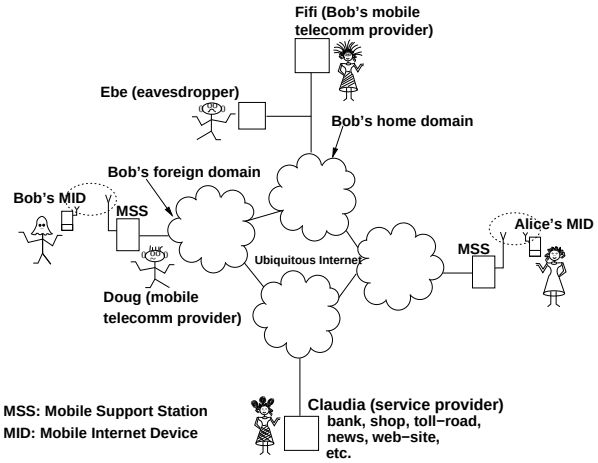

Fig. 1. A mobile user's scenario

2.1 Subscribers

A subscriber is a person that signs a long–term contract with a mobile telecommunications provider on the following terms: First, he or she is granted access to an extensive range of basic mobile telecommunications services exclusive to subscribers. Naturally, the signing of this contract implies that the subscriber provides the mobile telecommunications providers with sensitive personal data

(name, home address, employment, etc.). Second, he agrees to pay the bills he incurs whenever he accesses these telecommunications services, on a postpaid basis —monthly, for example.

Notice that in this work, we are excluding users of the so–called Pay & Go mobile phones from our definition of subscribers. The justification for this is that these users pay their mobile telecommunications providers on a pre–paid basis; consequently, they are not required to sign contracts with their mobile telecommunications providers.

It is worth mentioning that some authors make a distinction between subscribers (the person that owns the subscription and pays the bill) and users (the person who makes use of the services). Normally, the subscriber and the user are the same person, but not always [2]. This distinction is irrelevant for this discussion. Hence, for the sake of simplicity we will assume that the subscriber and the user are the same person and regard the two terms as synonymous.

In Fig. 1 Bob and Alice are two subscribers:

- Bob owns both the MID he is holding and a subscription to Fifi's mobile telecommunications network.
- Similarly to Bob, Alice owns the MID she is holding and a subscription to some mobile telecommunications network. Notice that Alice's telecommunications provider is not specified in the picture, it can be Fifi, Doug or anybody else.

2.2 Mobile telecommunications providers

A mobile telecommunications provider offers basic telecommunications services (phone answering services, caller identification, call forwarding, call transfer, roaming, single billing, location of mobile user, etc.) to her subscribers.

Being a mobile telecommunications provider, Fifi owns and has full control of what are called the Home Location Register (HLR) and the billing centre [3] of her network. In her HLR, she stores the personal data related to each or her subscribers (international mobile subscriber identity, subscriber's phone number in the mobile network, authentication keys, services allocated to the subscriber, etc.). This data is used during the authentication process and service granting. Similarly, in her billing centre, she stores personal data related to each subscriber (name and home address, for example) and records about service usage.

In the picture shown in Fig. 1 we have two mobile telecommunications providers.

- Fifi is a mobile telecommunications provider. Bob is one of her subscribers. Thus, from the subscription point of view, one can say that Fifi *owns* Bob. Hence she has full control over Bob's records. For Fifi, Bob is *her* subscriber and for Bob, Fifi's network is his *home domain* or *home network*.
- Doug is another mobile telecommunications provider. In the snapshot shown, Bob is currently visiting Doug's network. Consequently, for Bob, Doug's network is a *foreign domain*.

2.3 Service providers

A service provider offers remote services to the subscribers of mobile networks. Examples of such services are: banking, information (news, whether, knowledge databases, etc.), road tolling and road use pricing, shopping, bargain–hunting, auction–bidding, gambling, gaming, televoting, on–line counselling, etc. A service

provider has nothing to do with the provision of the mobile telecommunications services —this is the responsibility of the mobile telecommunications provider. In Fig. 1 Claudia is a service provider. Technically speaking, the services offered by Claudia can be offered by Fifi and Doug as well. For example, it is conceivable that apart from being a mobile telecommunications provider, Fifi offers bank services so that Bob's shopping bill is sent directly to his phone bill instead of involving complex bank transactions. However, this might be regarded as a monopoly practice and might not be allowed because of government regulations.

2.4 Eavesdroppers

An eavesdropper is an unscrupulous individual that meddles with the services offered by, or over, a network with the intention of committing illegal or unethical actions (frauds, for example). He can be anybody (a subscriber or a non–subscriber) who can gain access to the network. Ebe is the unwanted fellow in the picture shown in Fig. 1—he is an eavesdropper. He is shown using a desktop workstation for eavesdropping on Fifi's network, yet he can be anywhere in the ubiquitous Internet. He can be in possession of a MID and eavesdrop on Doug's network, for instance.

3 Mobility

One of the services to be provided by the ubiquitous Internet is *user mobility*. As its name suggests, a user of this service, Bob, for example, will be free to move around within the ubiquitous Internet and make outgoing calls on his own account (the one he has with Fifi's network) from any terminal located at his home, office, shops, restaurants, cinemas, taxis, buses, airplanes, etc. and of course, his MID.

Another dimension of mobility on the ubiquitous Internet is *terminal mobility* and is defined as the possibility of moving a terminal from one logical (possible geographical) location into another while still being able to access the same services. The main idea here is that users of MIDs will be able to move around (within the same network or from one network into another) without losing contact with the services in which they are interested.

Because we believe that users like Bob will always carry with them their MIDs when they are outdoors, and because of the technical characteristic of mobile and wireless devices discussed in Section 12.1, in this work we will focus on terminal mobility only and exclude user mobility. This means that regardless of his current geographical location, Bob accesses the Internet only from his MID. Terminal and personal mobility is discussed at large in [2, 4].

4 The watchful mobile telecommunications providers

Protection of data sent over communication lines is not a new topic. In the civilian field, the telecommunications industry is credited with being one of the pioneers.

Traditionally, the main aim of the mobile telecommunications providers has been to protect their networks from fraudsters. Consequently, in their view, the potential enemy is a member of the public (subscribers and non–subscribers) from whom the company and their customers must protect their money and other sensitive information (sensitive personal data, for instance) that can be considered confidential. Because of this, current mobile telecommunications providers offer, or have plans for offering, the following security services:

authentication of users Before given full access to resources, the system must identify the user (by means of a PIN number, for example) and ascertain that the user is actually who he or she claims to be.

non–repudiation Once a message is sent the sender cannot deny that the message was sent by him. Similarly, when a message is received, the receiver cannot deny that she received it.

data integrity A message in transit over the communications link or stored on disk will never be modified or deleted by an unauthorized individual.

data confidentiality Unauthorized individuals will never gain access to the contents of messages in transit over communications links or stored on disk.

A concept that deserves some comments here is the *Temporary Mobile Subscriber Identity* (TMSI) of the GSM system. The TMSI is an alias assigned to a mobile device by the system with the intention of preventing intruders from identifying the subscriber. Unfortunately, this number is assigned only after a successful authentication. This means that the mobile telecommunications provider always knows the real identity of the subscriber [5].

As can be seen from the above discussion, the subscribers' right to individual privacy is not in the mobile telecommunications providers' interest—they do not protect their subscribers' sensitive data from the mobile telecommunications providers' themselves. In other words, they take for granted that they have the right to gather, store, process and use the data about their subscribers. This assumption is grounded on the belief that mobile telecommunications providers are considered a trustworthy authority, consequently, their customers should not have reasons for concern. In the past, when customers used mobile telecommunications services for voice communication only, this assumption was reasonable. However, this situation has changed. With the increase in the number of services that involve the use of mobile telecommunications networks, a concern about the use and abuse of personal–sensitive data in possession of mobile telecommunications providers has been expressed. Ideally, these records should be used only for billing and accounting, however, because they are handily available and possess commercial value, they might be used for other purposes as well.

We believe that the time to review the traditional approach has come. It is time to redraw the picture of the mobile phone user and his potential unwanted observers. If the mobile telecommunications providers and service providers have means for knowing and collecting records about Bob's movements and whereabouts and without his consent, there is no reason for excluding them from the group of potential unwanted observers.

5 Untraceable mobility and unwanted observers

Bearing in mind that Bob is interesting in using his MID for accessing all services available on the ubiquitous Internet we can now identify what information he is interested in protecting and his potential unwanted observers.

In Section 4, we pointed out that traditional systems for data protection, deployed by mobile telecommunications providers are oriented to preventing frauds. Fraud prevention is certainly essential, however, in our view, data protection must be extended to prevent mobile telecommunications providers and service providers from gathering and storing data about the habits, movements and whereabouts of the users of the ubiquitous Internet. Unfortunately, this is not happening with current mobile telecommunications providers. In addition

to the data protection services mentioned in Section 4, we consider that mobile telecommunications providers should offer their customers (the users of the ubiquitous Internet) mechanisms for untraceable mobility.

By *untraceable mobility*, we have in mind that the user of a MID can travel around the ubiquitous Internet accessing its services without disclosing to anybody (the mobile telecommunications providers and service providers included) his or her habits, movements and whereabouts.

It is worth noting that the issue of untraceable mobility is discussed in Giuseppe Ateniese et al.[1]. However, we depart from Giuseppe Ateniese et al. in that we do not consider it necessary that Bob's mobile telecommunications provider is always aware of Bob's current location. As a side comment, it is interesting to notice that, these authors use the term *mobile anonymity* as synonymous with untraceable mobility. We prefer not to do so, because we believe that anonymity has to do with identities and not with user movements or locations.

With this arguments in mind, we suggest that the list of Bob's potential unwanted observers of his habits, identity, movements and whereabouts must include the following characters:

- Ebe, the eavesdropper
- Fifi and Doug, the mobile telecommunications providers
- Claudia, the service provider
- Alice, the receiver

The key point here is to depart from the traditional view over data protection in mobile networks in order to consider that for certain applications, some users of the ubiquitous Internet in possession of MIDs will count their mobile telecommunications providers and service providers as unwanted observers.

Protection from eavesdroppers is normally achieved by using cryptographic techniques which are based either in the use of secret or public keys [6, 7].

How to protect a MID user from his or her mobile telecommunications provider and service providers is an issue that needs to be explored. This is not a trivial issue. Thus, from now on we will concentrate only on the discussion of mobile telecommunications providers and leave service providers for a separate paper.

6 Billing in mobile networks

Billing is at the heart of mobile networks. Consequently, the functionality of all services offered by, or over, the network and the satisfaction or dissatisfaction of its subscribers much depends on how the charges are collected, the bill presented and the payment performed.

6.1 Single bill and charge collection

The billing system in current mobile networks are an evolution of those used in the old wire–line networks which were designed to meet the telephone companies' needs of monopoly. Accordingly, with this old way of making business, Bob *belongs* to Fifi's (see Fig. 1). Bob is Fifi's *catch*, so she will do everything possible in order to keep him within the limits of her domain so that all charges he incurs are sent to his account in Fifi's network. Since Bob is Fifi's subscriber, Fifi has full control over Bob's data: both the data he provides at subscription time

and his billing records. If Bob travels and incurs charges in foreign networks (in Doug's, for example) he still receives a single bill.

At first glance, a single bill looks like a reasonable idea. It sounds more practical for Bob to subscribe to a bundle of telecommunications services and receive a single bill from them rather than receiving several ones. For marketing telecommunications services and for Bob's domestic accountings a single bill sounds convenient. However, this convenience should not be taken for granted. It is probably a good idea to stop for a while and discuss what negative side effects a single bill might bring to Bob's right to individual privacy. This will help to identify the situations where a single bill might not be convenient.

6.2 Negative side effects of a single bill

A single bill seriously goes against Bob's right to individual privacy. Regardless of the services that Bob uses, Fifi always gets involved (see Section 4). Whenever Bob connects to the Internet (through Fifi's or Doug's network), he must authenticate himself to Fifi before he is granted full access to the ubiquitous Internet. Also, when he initiates a call, Fifi's network activates what is known as the *Calling Party Identification* (CPI) in order to collect data related to the call, such as subscriber's name and number, date and duration of the call. All this information is sent (over the signaling system [6]) to Fifi's billing centre where it is used for billing Bob at the end of the month or end of the agreed upon period. Moreover, the CPI record is used in the implementation of other services. Among other uses, it is used for presenting the called party with the caller's identification [8].

From the above discussion it follows that Fifi always has the means to collect records about Bob's habits, movements and whereabouts because her billing system receives this information from Doug and other mobile telecommunications providers visited by Bob. The result of this is that, if Bob uses his MID for supporting his favourite TV–star in a televoting show, Fifi will know about it. Similarly, if Bob travels to Cancun and from there he calls Alice three times a day and without receiving any call from her, Fifi will know that Bob has fallen for Alice. If Bob uses his MID for bidding in a goat–cheese auction, Fifi will know that Bob is a goat–cheese eater. If Bob uses his MID for paying his toll at the Forth Bridge, Fifi will know that Bob went by car to Edinburgh last weekend, and so on.

We argue that a single bill works well in some situations, namely, in situations where the right to individual privacy is not a concern. Hence, we should not adopt it precipitately without considering other alternatives. Recall that a single bill is not what we use for paying for goods and services in conventional commerce. In the following sections we will elaborate on our novel alternative that takes into consideration the issue of the right to individual privacy and is based on the use of anonymous e–cash and anonymous communications.

7 Anonymity as a means for protecting individual privacy

From the discussion presented in Sections 5 and 6.2, it should be clear that Bob's concern is about giving away sensitive personal data to Fifi—his mobile telecommunications provider— simply because, though she is considered a trusted third party, he does not trust her. He does not want to take any risk of having his right to individual privacy compromised.

In reality, the issue here is not about giving away sensitive personal data to an untrusted party, but about giving away sensitive personal data together with

the name of the individual or with enough information to link these two pieces of information together. Breach of individual privacy occurs only when both the individual's name and his or her sensitive personal data are collected together by an untrusted and unauthorized party. As long as Fifi does not find the means for associating and recording these two pieces of information Bob has no reason for being worried about his individual privacy. The idea is simple: if Bob gives aways his name, he must not give away his personal sensitive data; similarly, if for any reason he has to give away his sensitive personal data, he must conceal his name. From the second statement, it follows that a reasonable and simple approach to protecting the right to individual privacy of the ubiquitous Internet is by means of anonymity.

It is important to notice that by *the name of the individual* we mean the real name of the individual (Robert James Smith, for example), or other identifying number uniquely assigned to him such as driver's licence number or social security number, IP–address of a single–user machine, for example, and naturally, his home telephone number, International Mobile Subscriber Identity and International Mobile Equipment Identity. Likewise, symbols and images uniquely belonging to the individual, such as a finger print, voice print, DNA or a photograph, can also be regarded as the name of an individual. An informative discussion about absolute identification is presented in [9].

8 Anonymity and untraceability of cash

In today's societies, most people are happy and feel comfortable with using different methods of payment for different services. Currently, we use cash, credit and debit cards; likewise, we use prepaid cards, cheques, electronic fund transfers, money orders, coupons and other methods of payment [10]. Each of these alternatives has specific properties that make them suitable in certain cases but unsuitable in others; the purchaser and the merchant agree upon one of them depending on the nature of the transaction.

From the perspective of the right of the purchaser to protect his right to individual privacy these different methods can be divided into two groups:

- anonymous
- non–anonymous

Cash is the only method of payment that offers complete anonymity and untraceability. One can argue that prepaid cards like those used to operate public phone boxes and prepaid phones are anonymous and untraceable as well. This is true only if the purchaser uses cash to pay for the prepaid card. Under the same restrictions, coupons can be considered anonymous and untraceable as well. The rest of the payment methods mentioned are traceable, consequently, they do not protect the right to individual privacy.

Promoters of e–commerce consider that e–commerce will not reach the masses before potential e–shoppers like Bob are provided with terminals capable of protecting their right to individual privacy. If this is true, the idea of a single bill with a postpaid payment appears inconvenient as postpaid payments are not anonymous nor untraceable. It seems clear that for e–commerce to be successful we need to provide Bob's MID with a mechanisms for sending anonymous e–cash whenever he decides to access an Internet services without compromising his right to individual privacy. The problem with anonymous e–cash is that it can be sent only from anonymous terminals. We argue that what we need is pre–payments rather than post–payments. In other words, we need anonymous MIDs

with anonymous e–cash in and ready to be used for low–value transactions, that is, something functionally equivalent to having conventional cash in our pockets.

9 Unauthenticated access to services

Without any doubt, after considering the discussion presented in Section 6.2, Bob will ask whether it is possible for him to use his MID for accessing a service in which he is interested but without Fifi knowing about it. We believe that for a great variety of services the answers to Bob's question is a categorical yes.

With today's mobile telecommunications providers, it is common practice that access to network services is granted only after authentication. This paradigm is based on the assumption that even when the user of a MID is away from his home domain he still needs to access data (personal files, local data bases, local Web pages, etc.) and services (name, file, Web, mail servers, etc.) which are available only in or through his home domain. Because of this, whenever a user accesses a service he always needs to contact his home domain and authenticate himself so that the service is granted and a single bill issued.

This assumption is certainly justifiably, however, we argue that there are several applications where a MID can work perfectly well without using data and services from its home domain, i.e. without contacting it. For example, Bob does not need any support from his home domain to download Web pages into his MID, post information to an e-mail list or listen to the news as long as these services and Bob's connection to his foreign domain are free or Bob finds a means for paying for them locally.

The main idea here is that Bob can use his MID to access services from the ubiquitous Internet without telling his mobile telecommunications provider where Bob is and without telling anybody (the owner of the service he is using, for instance) who he is and where he is coming from. The core issue here is the payment.

10 Flexible charging without authentication

To prevent his mobile telecommunications provider from tracing him, Bob needs a flexible billing system. Thus it is reasonable for Fifi to give Bob the opportunity to choose how he wishes to pay for using a given service in the ubiquitous Internet. For some services (when he does not care about being observed by Fifi) Bob may be happy to be charged at his subscription account. However, in some situations he might prefer to pay locally and anonymously so that his right to individual privacy is not put at risk. For example, if he goes to Cancun and from there he calls Alice who is on holiday in Rio, Bob could choose between being billed when he returns to Newcastle (his home city) or pay anonymous e–cash to Doug —the mobile telecommunications providers he connects to in Cancun. After all, if we assume that Fifi's network in not in the path between Cancun and Rio, there are no reasons for Fifi to take part in the arrangement of the call. Bob's authentication is not an issue because as long as Doug is paid by Bob for the communications services, he should not care about Bob's identity.

The key idea here is that instead of contacting Fifi to ask her whether Bob has a subscription there and whether he is entitled to the services he is requesting, Doug can just check whether Bob can pay locally, that is, whether Bob can provide in advance the right amount of money for the service he demands. This should be enough for Doug. Doug can ask Bob for an advance payment in the form of anonymous e–cash, for example.

11 Random temporary, impersonal and non–universal numbers

One of the aims of third generation systems is the provision of user mobility. To authenticate mobile users, promoters, manufacturers and standard makers are considering to provide each MID with a globally unique and permanent identifier (IP address, International Mobile equipment Identity and International Mobile Subscriber Identity Number, for example). This identifier is assigned to the mobile user by his mobile telecommunications provider on a long–term–basis and remains permanent regardless of the mobile user's current physical and logical location. In other words, it is personal and uniquely identifies the the mobile user. Let us call it a **universal number**. The intention is to use this universal number for incoming and outgoing calls.

There is no room for doubts that this approach has several benefits. However, we argue that it should not be adopted without considering its consequences.

For incoming calls there are not doubts that Bob will be happy to receive messages on his terminal from his office, family, friends and other people from whom he wants to hear. However, this is not necessarily true for outgoing calls. There are situations where Bob may not want to initiate a call from his universal number provided by Fifi as this can bring undesirable side effects, like unwanted junk e–mail. This observation motivated us to propose a new paradigm, namely, a MID capable of switching into two different modes (see Fig. 2):

- MID with universal number provided by Fifi
- MID with a random, temporary, impersonal number

The crucial point here is that Bob switches his MID into the second mode whenever he does not want to put his right to individual privacy at risk. The appealing side of this mode is that before gaining access to the ubiquitous Internet, Bob does not need to contact Fifi for authentication, because of this, he does not need to disclose his identity to anybody, that is, he remains anonymous. For this to be possible, he pays locally (the owner of the mobile network to which he is connected) for the charges he incurs. For this purpose, he can use anonymous e–cash.

As shown in the figure, the random, temporary, impersonal number (TmpId) Bob uses is assigned by the owner of the mobile network at which he is currently located; by Doug if Bob is currently visiting his network. Naturally, nothing prevents Bob from requesting a TmpId from Fifi so that he can visit his own network as an anonymous user.

12 Implementation

A protocol for assigning a TmpId to a MID has already been published [11, 12]. In this protocol the anonymous user pays locally for his anonymous communication session using anonymous e–cash. Originally, the protocol was validated using SPIN [13]. Recently, it was programmed in Java and its suitability for practical implementation tested [14]. As of this writing, the Java code is being ported to *HP Jornada 720* and *Compaq iPAQ* personal digital assistants with a *Buffalo AirStation* wireless access point.

The crucial point of the protocol is that the TmpId is assigned anonymously. This means that Bob does not need to reveal his identity to anybody to obtain a TmpId for his MID. Once Bob's MID is in possession of a TmpId, Bob can use it (to call Alice for example and a counsellor at an Alcohol & Drug Abuse

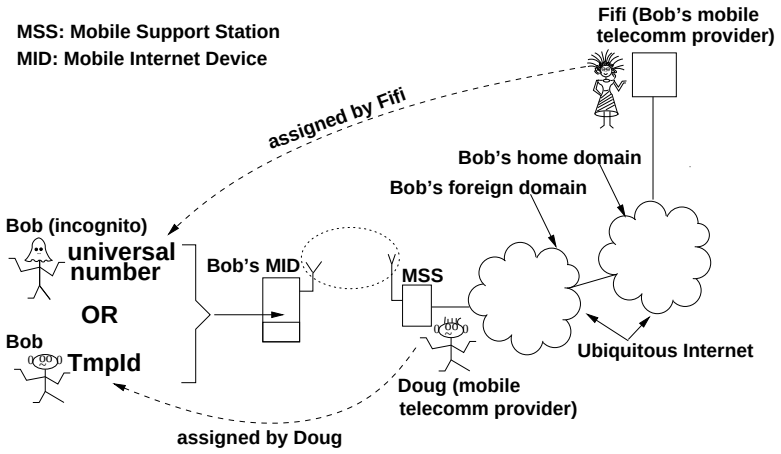

Fig. 2. A multinumber MID.

Clinic, for instance) with certainty that because his identity is not exposed, his right to individual privacy is fully protected. Naturally, if Bob needs to pay for the services he accesses, he uses anonymous e–cash, as discussed in Section 10.

It is worth commenting that, the TmpId is valid only for the duration of the anonymous communication session and that the original protocol does not support hand–off.

12.1 Anonymous communication using MIDs

In the protocol presented in [11], Bob uses a personal digital assistant as a MID for initiating his anonymous communications. The use of a wireless and mobile device instead of a wired desktop computer is not casual but a significant factor in this protocol. In accordance with the arguments presented in [12], true anonymous messages can be sent only from mobile devices to which TmpIds can be assigned. Ironically, the wireless facilities that help the mobile telecommunications providers to trace their mobile users can be used for protection against them.

In fact, any mobile device that permits the changing of their universal identifiers (IP address, MAC address, international mobile subscriber identity, etc.) without major difficulties (via software, for example) can be used. As has been observed by Arbaugh [15], most current wireless cards do. If this is true, there is not reason for not having mobile phones and other mobile devices boasted as MIDs, with similar facilities. Naturally, for a commercial implementation we would need that current mobile support stations (mobile phone base stations, for instance) run the protocol presented in [11] so that they are able to assign TmpId to MIDs, on request. We believe that this does not sound unreasonable since there is room for commercial applications here. Notice that the disposable SIM cards available in some countries (take for instance, Italy) that are valid only for a certain period of time (one year, for example) are a kind of temporary impersonal numbers inserted into mobile handsets. Why not make this service more flexible by changing the mobile handset number by software rather than by hardware?

It is important to notice that we assume a large number of MID users requesting anonymous services since with our approach, the protection of Bob's

right to individual privacy depends on how anonymous he remains after using a TmpId. Likewise, the degree of anonymity offered by any anonymizer it is hardly absolute but depends of its number of users [16].

13 Are conventional services surveillance–free?

After all this long discussion one cannot help asking whether the provision of this rather complicated protocols and expensive technology aimed at protecting our right to individual privacy is justifiable; it might happens that Bob is extremely paranoid about being observed through the electronic traces left behind by his MID; if this is true, he might feel very tempted to throw his MID out and resort to conventional means of accessing services. Regrettably, this might not be the best solution for certain services simply because regardless of our own personal preference we are living in an electronic world full of video–cameras; we are filmed wherever we go; there are claims that in cities in the United Kingdom a person is filmed over 100 times a day on average once he or she leaves the privacy of his or her home. Accordingly, Bob will be filmed if he decides to go personaly to the bookstore or the library to get a book about an embarrassing disease. In cases like this, the facilities for accessing services remotely seems highly valuable. In the example mentioned above, Bob can order an electronic version of the book or call the counselling service anonymously from the comfort of his house.

We are aware that anonymity is a topic that has triggered the hottest debates and divided the intellectual community into supporters and detractors because it can be used for good and bad purposes. We will not elaborate on this issue because it has already been discussed in several papers [17, 18, 19].

We believe that rather than putting aside Internet technology due to fear of negative side–effects in critical applications, we have to provide our electronic gadgets and electronic services with the necessary facilities to protect our right to individual privacy and to learn how to use them properly. For example, rather than thinking about how to ban anonymous communications from the Internet, we should be thinking about how to build services with both anonymizing and disanonymizing facilities; so that honourable individuals can use them for protecting their right to individual privacy and malevolent ones are caught red–handed [17]. In other words, we believe in electronic solutions for electronic problems.

14 Conclusions

If our predictions are correct, the current confined Internet will be converted into an ubiquitous Internet in less that five years. There will be great variety of services to be accessed from mobile internet devices. Many of the mobile internet users will be reluctant to make a full use of these services unless their right to individual privacy is fully observed. Current mobile telecommunications providers do not guarantee complete individual privacy as their billing records allow them to know all about the habits, movements and whereabouts of their subscribers. The centralized charge collection, the postpaid monthly, single, billing system, and the use of a universal personal number for outgoing and incoming calls leaves the subscriber without hopes of using his mobile internet device without putting into risk his or her right to individual privacy.

The provision of the full right to individual privacy in the ubiquitous Internet is not only desirable but possible as well. A more flexible billing system based on the use of local, on–the–fly payments by anonymous e–cash stored in a device

capable of connecting to the ubiquitous Internet by using a random, temporary, impersonal number is a possible solution to this issue.

References

[1] Giuseppe Ateniese, Amir Herzberg, Hugo Krawczyk, and Gene Tsudik. Untraceable mobility or how to travel incognito. *Computer Networks*, 31(8), 1999.

[2] Jan Thorner. *Intelligent Networks*. Artech House, 1994.

[3] Siegmund M. Redl, Matthias K. Weber, and Malcolm W. Oliphant. *GSM and Personal Communication Handbook*. Mobile Communications Series. Artech House, 1998.

[4] Nadège Faggion and Thierry Hua. Personal communications services through the evolution of fixed and mobile communications and the intelligent network concept. *IEEE Network*, 12(4), Jul/Aug 1998.

[5] Asha Mehrotra. *GSM System Engineering*. Mobile Communications Series. Artech House, 1997.

[6] Vijay K. Garg and Joseph E. Wilkes. *Wireless and Personal Communications Systems*. Prentice Hall PTR, Upper Saddle River, NJ, 1996.

[7] William Stallings. *Network Security Essentials: Applications and Standards*. Prentice Hall, 2000.

[8] Warren Hioki. *Telecommunications*. Prentice Hall, third edition, 1998.

[9] Simson Grafinkel. *Database Nation. The death of privacy in the 21st century*. O'reilly, 2000.

[10] Treese G. Winfield. *Designing systems for Internet commerce*. Addison-Wesley, 1998.

[11] Carlos Molina-Jiménez and Lindsay Marshall. Anonymous and confidential communications from an IP addressless computer. In *Handheld and Ubiquitous Computing, Proceedings of the First International Symposium, HUC'99*, Karlsruhe, Germany, Sep 1999. Springer. Lecture Notes in Computer Science, 1707.

[12] Carlos Molina-Jiménez and Lindsay Marshall. True anonymity without mixes. In *The Second IEEE Workshop on Internet Applications (WIAPP '01)*, San Jose, Ca. US, Jul 2001. IEEE Computer Society.

[13] Gerard J. Holzmann. *Design and Validation of Computer Protocols*. Prentice Hall, 1991.

[14] James Jillian. Anonymity on the internet. MSc dissertation, University of Newcastle upon Tyne, Department of Computing Science, August 2001.

[15] William A. Arbaugh. Your 802.11 wireless network has no clothes. http://www.cs.umd.edu/ waa/wireless.html, March 2001.

[16] Clay Shields and Brian Neil Levine. A protocol for anonymous communication over the internet. In Sushil Jajodia and Pierangela Samarati, editors, *Proceedings of the 7th ACM Conference on Computer and Communications Security*, Athens, Greece, November 1–4, 2000. ACM Press.

[17] Carlos Molina-Jiménez and Santosh Shrivastava. Understanding anonymity. Draft available on request from the authors at the Department of Computing Science. University of Newcastle upon Tyne, September 2001.

[18] Bruce Schneier. *Secrets & Lies. Digital Security in a Networked World*. John Wiley & Sons, Inc., 2001.

[19] Mike Godwin. *Cyber Rights: Defending Free Speech in the Digital Age*. Times Book, 1998.