The use of a Third Party Proxy in Achieving GSM Anonymity

Neil J. Croft and Martin S. Olivier

Abstract—Mobile communications have grown tremendously over the last decade; however little attention has been directed to addressing privacy concerns around mobile interactions. Few mobile subscribers are aware that their serving GSM Network holds sensitive information regarding ever aspect of the mobile users interactions which is monitored, logged and could potentially be compromised. Such information includes personal banking details, place of residence, location, movement and — in particular — with whom the user interacts on a daily basis.

Sender anonymity refers to the ability of a sender of a message to remain anonymous. Receiver anonymity refers to the ability to contact a receiver, while the receiver remains anonymous or pseudonomynous.

This paper focuses on how sender and receiver anonymity can be obtained in a GSM network through the use of a Trusted Third Party Proxy. Emphasis is placed on shifting the control and collection of personal information away from a subscriber's serving GSM network. This is based on the fact that violations of privacy are known to frequently perpetrated by individuals who are 'insiders' and authorised to access sensitive information. By allowing anonymous calls where the GSM network cannot obtain call details, this insider threat is effectively eliminated.

Our solution still provides for appropriate billing even though calls can be made anonymously..

Index Terms—Anonymity, Privacy, Trusted Third Party

I. INTRODUCTION

PRIVACY refers to the ability of the individual to protect personal information. Privacy occurs in many forms. Anonymity, for example, is the privacy of identity [8]. The Global System for Mobile communications (GSM) [1] is a popular digital cellular Network that provides privacy to its subscribers: GSM, for example, encrypts voice communication, and it allows for the user to control whether a called party gets the caller's phone number (known as Call Line Identity or CLI). However, GSM requires that a subscriber trusts his/hers service provider with details of calls made and received. It is well known that many violations of privacy occur when insiders in some trusted organisation violate the trust placed in them and use their authorised permissions to misuse private information. It is entirely possible that such misuse of information could occur within a GSM service provider.

In traditional data communication networks, various schemes to ensure anonymity have been proposed where most are based on Chaum's so-called Mix [3]. Schemes have been proposed that enables anonymous Web browsing, anonymous sending of email, as well as other applications [7]. Often these schemes ensure anonymity (or pseudonymity) through the use of public key encryption or are based conceptually around the use of a proxy. Often third parties are used to provide the desired level of anonymity, where such a party may be fully or partially trusted based on how much critical information is disclosed to it.

In order to operate, GSM clearly needs identifying information: users should be charged for outgoing calls and incoming calls should reach the appropriate phone. The Home Location Register (HLR) is a database within a GSM network that contains permanent and temporary data for all registered users. Permanent data would include the user's profile while temporary data could include the current location of a user. When a subscriber switches on his or her mobile device, the International Mobile Subscriber Identity (IMSI) is used for connection to the network. The initial connection is the only time the IMSI is used, as after the connection the network assigns the subscriber a temporary identifier known as the Temporary Mobile Subscriber Identity (TMSI), thus hiding a user identity from eavesdroppers. The TMSI has local purpose, as the temporary identifier is valid only for a specific area. If the subscriber moves to another area, the network allocates the subscriber a new TMSI. The main purpose of the TMSI is to retain the anonymity of the subscriber since the IMSI can reveal the subscriber's true identity. Within the HLR, the IMSI/TMSI of a subscriber is mapped to their Mobile Station International ISDN Number (MSISDN) or mobile number. This information is primarily used for billing purposes. It is important to note that the IMSI/TMSI provides a certain degree of subscriber communications anonymity as well as subscriber anonymity in authentication; however this does not provide for network anonymity, where you network operator monitors all activity performed in the domain as all actions linked to a single alias. In the GSM environment, the single alias most commonly used is the mobile number (MSISDN) associated with the subscriber.

Sender anonymity refers to the situation where the originator of the communication wishes to keep his or her identity private. *Receiver anonymity* refers to the case where we wish to enable calls to a persistent pseudonym.

Indormation and Computer Security Architectures Laboratory, Department of Computer Science, University of Pretoria. Email: molivier@cs.up.ac.za Tel 012-420-2052 Fax 012-362-5188

As stated, our aim is to enable sender and receiver anonymity in a GSM network.

The following example illustrates the real-world requirement of GSM sender anonymity. A person "tips off" authorities about a crime and subsequently wishes to remain anonymous for safety reasons.

The following example illustrates the necessity for GSM receiver anonymity. A person places an advertisement in a local newspaper in order to sell goods. However, the goods will only be on sale for a week after which the seller does not wish to be contacted further on the contact number displayed in the advert. The seller achieves true GSM receiver anonymity through the use of an alias (in this case a virtual mobile number). This virtual number may be purchased from a third party or allocated to the user on request. The validity of the assigned virtual number is set to expire (at the third party) after a week. Subsequently the mapping of the virtual number to the seller's real mobile number or identity is relinquished.

This paper focuses on the hiding of personal aspects of the subscriber's identity to its serving GSM network. Our specific aim is to propose a mechanism that enables a user of a mobile handset to make and receive calls where the service provider cannot determine the identity of the other party involved in the call. More formally, we investigate the possibility of achieving sender and receiver anonymity in GSM. This is achieved through the use of our proposed modelled Trusted Third Party (TTP) Privacy Proxy. Obviously, our model should still allow the network to bill the appropriate party for services rendered even though the network is unaware of the other party involved in a call.

The primary intention of the paper is to describe the high-level operation of the TTP, rather than to consider details of implementation.

Key aspects of our modelled approach include Personal Control and Identity Management. These constitute two of the four layers presented in the layered architecture for privacy-enhancing technologies [2]. Personal control is the guarantee that an individual's personal information is only divulged in accordance with the individual's privacy policy. The goal is to only release private information if the request is compatible (or at least to a negotiated level of agreement) with that of the owner's privacy policy. Identity management includes the possibility of acting anonymously and pseudonymously to hide aspects of an individual's true identity.

There are indeed other privacy concerns in GSM (such as the ability to always locate a subscriber). Those issues will, however, not be addressed in this paper. Furthermore, it should be noted that most aspects of the proposed model are not limited to GSM, but are, in fact, generic. Our decision to base the model on GSM has been influenced by the availability of a consistent set of terminology and the fact that the larger research area within which the current paper is situated does focus on aspects that are specific to GSM.

This paper is structured as follows: Section 2 provides background of technologies used in achieving sender and receiver anonymity in various technologies. Section 3 investigates sender and receiver anonymity in the GSM realm. Section 4 develops the proposed modelled approach to achieving true subscriber anonymity through the use of a Trusted Third Party (TTP) Proxy in GSM. Section 4 concludes the paper.

II. Sender and Receiver anonymity

The technology for email anonymity, also known as anonymous remailers [7, 8, 10], has addressed the problems of achieving both email sender and receiver anonymity. An anonymous remailer is merely a third party proxy that strips away a user's real identity when sending or receiving mail and replaces this information with pseudo anonymous information, also known as a persona or alias.

Chaining is simply a technique to achieve more robust security by sending a message through several anonymous remailers, so that the second remailer sees only the address of the first remailer and not the address of the originator [8]. The advantage of chaining lies in the knowledge that every remailer must be compromised in order to trace the original sender of the message.

The technology for web browsing anonymity [11], which employs cryptographic engines [12], allows for a user to browse the web in a personalized, simple, private and secure fashion by making use of generated aliases and maintaining pseudoanonymous relationships with multiple servers.

Some work has addressed the need for untraceable authentication protocols suitable for mobile subscribers [6]. However this does not undermine the fact that the mobile subscriber's serving network still maintains and monitors personal interactions of its subscribers.

III. Sender and Receiver anonymity in GSM

We apply a similar approach to that used in remailers and consistent anonymous web access within the GSM environment. Mobile subscriber sender and receiver anonymity are achieved through the use of a Trusted Third Party Privacy Proxy. Our solution will also make use of aliases to realize sender and receiver anonymity. An alias in the GSM realm is simply a unique identifier assigned to a mobile subscriber. The alias will resemble an MSISDN, but could, in principle be identified with the TTP. One possibility is to use a special prefix (e.g. 085 in South Africa) to indicate an alias served by a TTP.

A number of problems exist in the GSM environment where sender and receiver anonymity is concerned. There are three major issues that arise.

One problem is that a subscriber needs to be reached at any moment; the serving network always needs to know the location of the mobile user in order to route incoming calls to the user. Hence in a two way communication, although the receiver may not know the identity of the sender, the underlying network possesses location information of both in order to establish and maintain an open communications channel.

The second problem is that someone's mobile number (contact details), once known, is considered public information; i.e. once the mobile number of someone is known it can be disclosed to many others via different mediums without the consent of the owner.

The third problem — and perhaps the most pertinent difference between GSM and other forms of communication — is that GSM conversations have to occur in real-time and are billed based on time, contract options and (sometimes) distance. The sender must be linked to one particular identifiable entity so that within a time frame (usually once a month) all network events conducted by the user are summed and the monetary equivalent calculated thereof. The service provider holds its subscribers accountable for their network-related actions and presents each user with an itemized bill (usually at month end).

There are a number of requirements that must be met in order to realize true GSM sender and receiver anonymity:

- Each sender and receiver must (in principle) be able to create a large number of anonymous identities (aliases), such that the network will be unable to map any of these identities to the same sender or receiver unless for the purpose of billing — i.e. identities must be incomparable.
- The sender and receiver are empowered to control all anonymity requirements if need be, leaving influential basic anonymity requirements to the serving GSM network.

At present, the only degree of anonymity that is controlled by the user is where the sender may choose to disclose his/her identity by allowing "own number sending" from the mobile device when contacting a particular receiver. At the receiver end, the identity of the caller will be unknown.

Anonymity clearly holds implications for reputation and trust: in many cases a receiver would decide whether or not to accept a call (and sometimes whether or not to make a call) on whether the receiver (or caller) is able to identify the caller (or receiver) before establishing the connection. Clearly, when anonymity (or even pseudonymity) is used, it is up to the prudence of the receiver whether to accept or deny an incoming call. Similarly, whether a call is made depends to some extent on knowing whom one is calling. As a practical example of the latter case, consider the implications from buying an item from someone for whom one only has a temporary number available; since one may not be able to contact the seller after the transaction, one may be afraid of proceeding with the transaction. Furthermore, sender and receiver anonymity in GSM will be subscriber influenced and maintenance intensive; such conscious safeguarding may provide a greater level of aggravation to the user opposed to benefit gained.

In Figure 1 we define an actions map underlining GSM communication governing privacy, enforced by a sender on a receiver or vice versa. These actions are administered through Personal Control and Identity Management. They include the following: access, deny, disclose, utilize, anonymize, depersonalize and repersonalize. Influenced by trust and reputation, identity is enforced locally by a user. The GSM pseudo anonymity actions map provides a generic solution in achieving anonymity. The underlying GSM network can play a substantial role in control and maintenance, thus eliminating subscriber involvement for basic privacy requirements, such as ensuring that that the communications channel is secure.

From Figure 1, the four quadrants represent different situations where a sender may be known or unknown to a receiver and vice versa. All four quadrants are administered by Personal Control and Identity Management. For example we assume a communication channel may be established where the receiver is known to the sender, however the sender is unknown to the receiver. The receiver trusts the anonymous sender enough to allow the creating of a communications channel. The sender may choose action "disclose", revealing the sender's true identity. The true identity in this case would include the sender's mobile number and possibly other personal information.

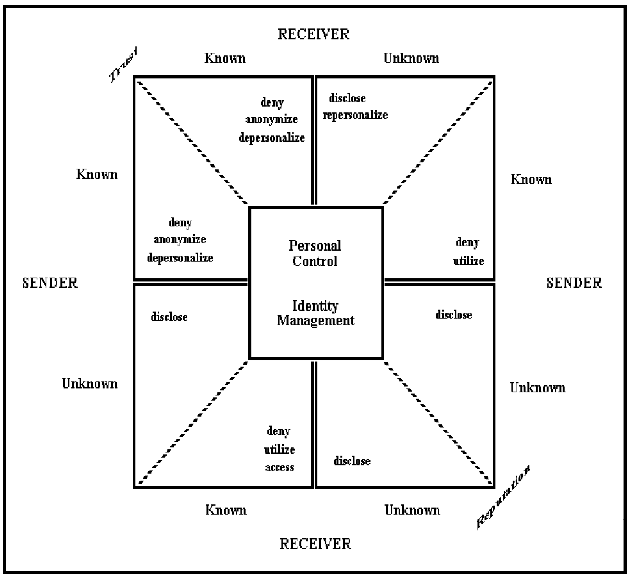

Figure 1 GSM pseudo anonymity actions map

IV.

This section describes our model for using a trusted third party to achieve sender and receiver anonymity in GSM.

It is relatively straightforward to achieve sender anonymity through the use of a TTP: Using CLI preferences, one can call the TTP but withhold one's MSISDN from the TTP. One then has to somehow inform the TTP of the intended recipient of the call. Technically, this is easily achieved by using Dual-tone Multi Frequency (DTMF) signals to communicate this number with the TTP. The TTP can then complete the call by calling the number entered by the original caller. Since the TTP does not have access to the CLI of the original caller, it cannot compromise the privacy of the caller — to the called or any other party.

A number of issues, however, remain with this proposed solution; the most important issues are security of the proposed solution and billing.

The major security issue relates to the requirement that the call should be anonymous not only to the recipient, but also to the network. (If anonymity was only required towards the called party, simply not sending one's own number would have sufficed.) One's service network will know that a TTP has been called. We also have to assume that the network is familiar with the process of sending the eventual called party's MSISDN using DTMF (or other means). The network will thus, in principle, be able to establish whom the call is made to, by eavesdropping on the connection. In defence of the technique, it is worth pointing out that such eavesdropping does not happen routinely (as logging of dialled numbers usually does) and it requires a perpetrator to monitor the connection when the call is made. (Again, note that the actual connection is encrypted, but we are assuming an attacker on the inside of the GSM network as the current threat). The proposed solution will thus be adequate for many purposes, but would not be absolutely secure. Below we will consider another alternative that eliminates this problem.

Since the TTP does not (and should not) know the identity of the caller, the TTP is not in a position to bill the caller for services rendered. In the general case, the TTP will have no agreement with the called party and will not be able to bill him or her either. The only solution therefore is to bill the caller's network. This implies that calls to the TTP should be billed at a premium rate (by the usual service provider). This could have the undesirable effect of attracting more attention to the specific call, than other "normal" calls would have attracted, but this does not seem to be a critical weakness. The fact that the billed rate would cover the call costs to the TTP, the TTP's service charge as well as the call from the TTP to the eventual recipient, means that the call will be relatively expensive; however in cases where hiding the CLI from the called party is not sufficient, a higher call rate would probably be acceptable. A bigger concern with the proposed billing approach is the fact that the cost of calling the TTP would best be based on a known cost for the call from the TTP to the called party. This clearly implies that one cannot have an indefinite sequence of TTPs through which the call is to be routed to better protect privacy. Remember that this process, known as chaining, is indeed often used where privacy is to be protected.

We now turn our attention to receiver anonymity. In this case the TTP clearly needs to know the identity of the receiver — otherwise it will not be able to route calls to the receiver. Therefore the receiver is required to register with the TTP before using the service and to provide a real number where the recipient can be contacted. Therefore some trust in the TTP is required.

When registering, the recipient receives one or more aliases. Depending on the intended application, an alias could be used to work for a limited time or an extended period.

The fact that the contact number of the recipient is known to the TTP could be alleviated by using chaining: The contact number given to a TTP could be an alias registered at a second TTP, where the second TTP knows the real MSISDN. This can be repeated as often as required. To associate the alias at the first TTP with the real MSISDN would require collusion between the two (or more) TTPs.

Two options exist for billing: Charging the caller is an option. Calls to aliases can be charged at a premium rate as was suggested above for sender anonymity. However, since the recipient is known to the TTP, it is also possible to adopt a different billing model, where the caller is charged for a normal call and the recipient for the second half of the connection. Even where the recipient is not entirely known to the TTP (for example, when the contact details given were an alias at a second TTP) it is still possible to charge the recipient: The recipient can easily buy "vouchers" anonymously (at a normal shop) and use these to "recharge" his or her account at the TTP, without revealing any true identifying data to the TTP. In fact, this second billing model is the appropriate one to use when using chaining: The network will not know through how many TTPs a call will eventually be routed and therefore cannot bill in an appropriate manner for the call. The recipient can, in contrast, quite easily pay for each (anonymized) leg of the call.

Finally, consider the integration of sender and receiver anonymity: As presented above, it is obvious that the two approaches are simple to integrate. This solves the problem (referred to earlier) that the service provider is, in principle able, to breach sender anonymity if it eavesdrops when the caller enters the recipient's MSISDN. If an alias is used for the recipient, the service provider will be able to infer much less than would otherwise have been the case.

An integrated solution also offers an interesting confidentiality versus convenience trade-off: Assume that two parties are communicating with one another using both sender and receiver anonymity. Using the (combined) solutions offered above, the CLI of both parties will be hidden from the TTP. If, however, the CLI is revealed to the TTP the TTP will be able to translate the incoming CLI to the alias it associates with the CLI and use this alias as the CLI of the outgoing call. This would enable an anonymous call to be made and will allow the called party to (automatically) return the caller's call. Both parties will be pseudonymous towards each other, as well as the network. However, in this case the TTP will know the real contact details of both communicating parties. While this possibility was not specifically excluded by the problem statement at the beginning of this paper, this could indeed be a concern. Chaining is one possible solution for this, but the billing approach described for a sender anonymous call described above cannot deal with this option. A simple extension to the billing approach for receiver anonymous calls given above, will solve the billing problem introduced here.

V. Conclusion

This paper considered an approach to facilitate anonymous and pseudonomynous calls in a GSM network through the use of a TTP. It was demonstrated that the suggested approach can support sender and receiver anonymity and viable approaches to billing have been given. As noted in the introduction, the proposed technique uses little that is specific to GSM networks (except some terms, the fact that encryption is used and the fact that own number sending can be dynamically controlled by the user) and it could be applied to telephone networks in general. Our intention is, however, to consider anonymity and pseudonymity in the broader context of GSM networks, including its application for messaging and packet radio services — and hence the decision to cast this paper in the GSM environment. Consideration of these other facets of GSM is, however, left for future research.

Legal and forensic implications of the proposed technique will also be considered in future research.

REFERENCES

[1] M. Rahnema, “Overview of the GSM Systems and Protocol Architecture”, IEEE Communications Magazine, April 1993.

[2] M. S. Olivier, “A Layered Architecture for Privacy-Enhancing Technologies”, in Proceedings of the Third Annual Information Security South Africa Conference (ISSA2003), J. H. P. Eloff, H. S. Venter, L. Labuschagne, and M. M. Eloff (eds.), Sandton, South Africa, July 2003.

[3] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms”, Communications of the ACM, Volume 24, Number 2, Pages 84-88, February 1981.

[4] N. J. Croft, “Secure Interoperation of Wireless Technologies”, Masters Dissertation, University of Pretoria, October 2003.

[5] R. Molva, D. Samfat, G. Tsudik, ”Authentication of Mobile Users”, IEEE Network Magazine, Special Issue on Mobile Communications, March/April 1994.

[6] R. Molva, D. Samfat, N Asokan, “Untracability in Mobile Networks”, Communications of the ACM, 1995

[7] D. Goldschlag, M. Reed, P. Syverson, “Onion routing for anonymous and private internet connections”, Communications of the ACM (USA), Volume 42, Number 2, Pages 39-41, 1999.

[8] I. Goldberg, D. Wagner, E. A. Brewer, “Privacy-enhancing technologies for the Internet”, In IEEE COMPCON ’97, pages 103-109, IEEE, February 1997.

[9] A. Bacard, “Anonymous Remailer FAQ”, 1996, Web reference: http://www.well.com/user/abacard/remailer.html

[10] L. Cotrell, “Mixmaster & Remail Attacks”, 1995, Web reference: http://www.obscura.com/~loki/remailer/remailer-essay.html

[11] E. Gabber, P. B. Gibbons, D. M. Kristol, Y. Matias, A. Mayer, “Consistent, yet anonymous, web access with LPWA”, Communications of the ACM, Volume 42, Number 2, Pages 42-47, February 1999.

[12] E.Gabber, P. B. Gibbons, D. M. Kristol, Y. Matias, A. Mayer, “On secure and Pseudonymous Client-Relationships with Multiple Servers”, ACM Transactions on Information and System Security, Volume 2, Number 3, Pages 390-415, November 1999.

Neil J Croft received his Bachelor of Science and Honours degrees in Computer Science at the Rand Afrikaans University in 2000 and 2001 respectively. He has recently completed his master’s degree at the University of Pretoria. He is currently employed at a local GSM network operator. His research interests include security, privacy and communication protocols within wireless environments.