Anonymous Mobile Conference Calls

N.J Croft and M.S Olivier
Information and Computer Security Architectures (ICSA) Research Group
Department of Computer Science
University of Pretoria
Pretoria
South Africa
Email: ringtingting@gmail.com

***Abstract*— This paper describes an architecture and protocol for making anonymous mobile conference calls. A number of examples exist where multiple users may wish to communicate in an anonymous manner, such as anonymous virtual support groups (e.g Alcoholics Anonymous).**

Anonymous group identification schemes coupled with the novel idea of *Virtual Numbers*, allows for identification to a conference call facility where access control is permitted based on the concept of "proof of knowledge" of an individual.

The goal is to design an anonymous multi-user conference call *architecture* that includes zero-knowledge proof group identification and a private *communication-efficient protocol* in mobile conference call environments.

Our approach focuses on the Global System for Mobile Communication (GSM). Previous work on the use of a Trusted Third Party (TTP) Privacy Proxy for achieving GSM communication anonymity and anonymous channelling and billing in GSM provides the basis for multi-user anonymous mobile conference facility.

The underlying components of the serving GSM network remain unchanged.

I. Introduction

The Global System for Mobile communications (GSM) is a popular digital circuit switched network [1] that provides privacy to its subscribers [2] and facilitates conference calls. In the current GSM system, the conference call is supported by call holding and multiparty supplement service [3]. In this mechanism, however, the conference members are limited to five in general [4]. Another approach recommended in the GSM specification to support multi-user conference calls is Group Call Service [5]. This approach resolves the limitation of conference member (participant) number; however, restrictions by service area and the scope of the application still remain.

Anonymity is the state of being not identifiable within a set of subjects, the so-called *anonymity set* [6]. In certain circumstances an individual may wish to participate anonymously in a group activity. A good example of this is someone who participates in a personal support group such as Alcoholics Anonymous. Given the trend in communicating more and more using technology rather than face-to-face, a need exists to provide anonymous conference calling facilities in a voice network. One approach to achieving sender and receiver anonymity in a GSM network is through the use of a Trusted Third Party (TTP) Privacy Proxy [7]. This allows subscribers to remain anonymous from each other and provides abstraction from the serving GSM network. GSM requires that a user trusts his or her serving network [7] with details of calls made. Therefore, an anonymous mobile conference call architecture is achievable only if communication is anonymous from participants in the conference group and from the serving GSM network.

Recent work on anonymous channelling in GSM [8] provides user anonymity from its serving network. This anonymous ticket-based protocol allows users to hide their identity from the serving GSM network while performing accountable GSM network events, such as a mobile call. A required extension of anonymous channelling is that the network still retains the ability to bill a user when using these anonymous channels [9].

Anonymous identification schemes allow a user to identify themselves to a verifying authority in a secure way without revealing their identity or secret key. Such anonymous identification is vital in a conference facility where a subscriber authenticates to a conference call facility without revealing identity. Virtual Numbers [7], used later as means of access control, play a significant role in identification and call recovery of an anonymous subscriber to the conference call facility proposed in this paper. Incomparability of identities is realized through the creation of a large number of anonymous identities; Virtual Numbers fulfil this requirement. By placing a call to a Virtual Number, access to a conference call facility is granted if the calling party should be permitted to place the call.

This paper encompasses, combines and adapts previous work on privacy enhancing mobile communication techniques in order to create this anonymous mobile conference call facility. This call facility is intended to be useful within the constraints imposed by the GSM system.

We propose an *anonymous mobile conference call architecture* and devise a private *communication-efficient protocol*.

Our decision to position our work in the GSM context is based on the popularity of GSM and its wide spread adoption in comparison to other mobile communication networks such as Universal Mobile Telecommunications System (UMTS). In addition, work reported on in this paper forms part of a larger privacy and security project [2], [7], [9]–[11] set in the GSM and next generation wireless communication context.

Cimato et al. [12] previously described an anonymous group communication protocol in mobile networks. However, every user in the network must perform a membership test and key recovery in order to find out whether or not they are a participant in a conference call. This approach is not feasible due to the large number of GSM subscribers and the possibility of numerous concurrent conference calls.

This paper is structured as follows: Section II covers a brief overview of GSM. Section III illustrates our proposed Anonymous Conference Call Architecture. We investigate the privacy requirements in providing an anonymous mobile conference facility and detail an approach in fulfilling these requirements. Section IV investigates a private communication-efficient protocol used in the anonymous mobile conference call architecture. Finally Section V concludes this paper.

II. Background

This section briefly reviews those aspects of GSM (the Global System for Mobile Communication) and related technologies that are important to place the remainder of this paper into context.

GSM is a popular mobile communication standard issued by the European Telecommunications Standards Institute (ETSI) [13]. The GSM architecture consists of Mobile Stations (MSs) and Base Transceiver Stations (BTSs) [2]. BTSs are connected to a Base Station Controller (BSC), which in turn, is connected to a Mobile Switching Centre (MSC). The MSC has an interface to one or more BSCs and to external networks. The Home Location Register (HLR) database contains information (including location information) on every subscriber in the GSM network. The Visitor Location Register (VLR) database, contains information on subscribers visiting its location area. The AuC is the subscriber Authentication Centre and contains a shared secret authentication key, denoted by $(\mathbf{K_i})$ [14], with the MS. GSM networks collect personal communication information required for the billing and charging of its subscribers [9]. Through analysis of a user's movements and various network activities patterns of private user activities are known by the serving GSM network. One approach to achieving GSM anonymity is through the use of a Trusted Third Party (TTP) Proxy [7].

GSM has a comprehensive Security Model. This model is based on three well-known algorithms (A3, A5, A8) each having a specific purpose. The A3 algorithm is primarily used in verifying the authenticity of the GSM subscriber during sign-on to the GSM network. We utilize the A3 algorithm later in this paper.

The Dual Tone Multi-Frequency (DTMF) signalling is used extensively in GSM and other telephony systems for call signalling. A user may cause a DTMF tone to be generated by depression of a key in the Mobile Station (MS) [15]. Interactive Voice Response (IVR) is a computerized system that allows a GSM subscriber to select an option from a voice menu and otherwise interface with a computer system. Generally, the system plays pre-recorded voice prompts to which the person presses a key to respond. We utilize these technologies later in the paper as a means for establishing a conference call facility from an initiator, also referred to as a *dominant*.

III. Anonymous Mobile Conference Call Architecture

A GSM mobile conference call is a synchronous collaboration session, in which users can initiate or join an existing conference call facility. We define two varieties of conference call scenarios, namely an *Invited* conference call facility and a *Public* conference call facility. Invited conference calls refer to those conference calls that only if invited, one could attend. On the other hand, a public conference call facility suggests that anyone can attend, for example a support group conference call.

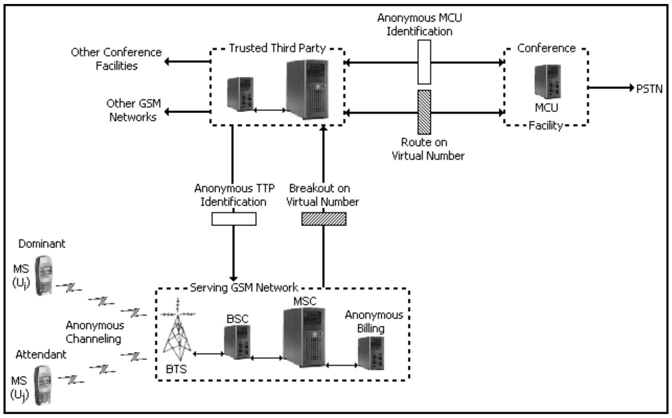

Fig. 1. Anonymous Mobile Conference Call Architecture

The Anonymous Mobile Conference Call Architecture proposed in this paper is depicted in Figure 1. It consists of Mobile Stations (MSs) where U_i refers to the conference call initiator (the dominant) and an attendant denoted by U_j, the serving GSM network (Base Transceiver Station, Base Station Controller, Mobile Switching Centre and Anonymous Billing amongst others), a Trusted Third Party (TTP) Privacy Proxy and a Media Control Unit (MCU) or Conference Facilitator. In most part the TTP and MCU may exist as one entity but are decoupled for illustration and practical purposes. The TTP's responsibilities include filtering and forwarding calls between the MCU and the serving GSM networks. The MCU's roles include conference facility creation, media translation and control conversion for attendants in a conference call facility. The MCU may also have an external interface to a Public Switched Telephone Network (PSTN).

This section reviews the most important technologies used in our anonymous mobile conference call architecture and (to be used below in our private communication-efficient protocol).

A. Anonymous Channelling over GSM

The first technology we explore in our architecture is that of anonymous channelling. The intention is to hide the identity of a GSM user from a visited network as well as from the home network where the user is registered. The visiting network cannot determine details of the user and the home network — which already has the details — cannot trace the user on the visiting network. As illustrated in Figure 1 it is to be used in the Anonymous Conference Call Architecture between any MS participating in the call and its serving network.

The protocol we use is one recently proposed by Peinado [8]. It is an authentication protocol that allows anonymous channelling over GSM. The protocol is based on the generation of *Temporal Keys*, denoted by $\mathbf{TK_i}$, and the utilization of prepaid tickets. The main objective of this new protocol is to allow the legal subscribers anonymous access to the GSM network's resources [8]. The anonymity provided allows any authorized subscriber to access the GSM network, while completely hiding the subscriber's true identity to the serving VLR. Therefore the associated user location information is irrelevant to the serving GSM network.

In anonymous GSM channelling, mutual authentication between the MS and the serving GSM network is provided without any modifications in the underlying GSM architecture. In the same way, every user has its own secret key K_i which is shared with the Home Location Register (HLR) (network user database store). The protocol is based on the generation by the HLR of a *Temporal Key* $\mathbf{TK_i}$. The *Temporal Key* allows the Visitor Location Register (VLR) (temporary network user database store) to authenticate the subscriber without further connections to the HLR, and having no knowledge of shared secret key K_i.

The protocol is divided into two parts, namely the ticket issuing phase and the utilization of these prepaid tickets, where the ticket is generated by the HLR [8].

The ticket is defined as follows:

$$(Auth_{VLR}; TK_i; T_{exp}) \tag{1}$$

where $Auth_{VLR} = A3(K_i; T)$ and $TK_i = A3(K_i, T_{exp})$. T and T_{exp} represent the current time and expiry time respectively. We choose to utilize this ticket later in our communication-efficient protocol for an invited conference call facility.

A further requirement is that the serving GSM network retains the ability to bill the anonymous subscriber. In earlier work [9] we expanded the protocol of anonymous channelling in GSM by allowing an accurate yet accountable procedure for anonymous billing.

B. Trusted Third Party Privacy Proxies

The second technology used in our architecture is Trusted Third Party Privacy Proxies. Figure 1 illustrates where it is positioned in the architecture.

A Trusted Third Party (TTP) Privacy Proxy is an external entity to the serving GSM network operator.

In this paper the TTP's main purpose is to act as a facilitator in hiding personal details of the mobile user's intensions and actions from their serving GSM network as well as referring control of conference facilities away from the serving GSM network. The need for using a TTP is evident from the fact that the serving GSM network controls communication information, for example who the user is calling and for what purpose. To illustrate, if a user phones an anonymous support group, the serving network can infer the reason for the call (based on the dialed number).

Numerous distributed TTP Proxies and MCUs may exist; thus the serving GSM network requires TTP identification and the TTP requires MCU identification.

In order to retain anonymity during the entire process, registration takes place in an anonymous manner. Anonymous communication between the TTP and serving GSM network and the TTP and MCU, is achievable through various possible privacy-enhancing techniques such as Mixes [16] and Onion Routing [17]. The TTP may employ such privacy-enhancing techniques on behalf of participants in conference calls such as Codec-Hopping [10] enhancing security and privacy of voice communication. See the protocol described in section IV for the approach followed in this paper.

C. Virtual Numbers

The third technology used in our architecture is Virtual Numbers. A Virtual Number can best be described as a valid numbering plan. It is a number that conforms to number prefixing and minimum and maximum digit length requirements. The GSM network may choose to allocate and assign a virtual number for a specific purpose. In a crisis situation a short number — that is easier to remember than a long number — may, for example, be assigned to a crisis call centre. When the virtual number is dialled it is rerouted to the real number. As another example a virtual number may be assigned to a disaster relief fund and set at a premium charge rate. Income derived from the premium-rated service may the be donated to the fund. A form of Virtual Numbers already exists with the inception of mobile “short code” numbers.

A Virtual Number may be purchased for use from a TTP or from the serving GSM network.

In this paper we use the concept of virtual numbers to map to a TTP service and conference facility. The conference dominant will acquire the number from a TTP and distribute it to potential participants. The attendants will then call this number to participate in the conference call. The details of the protocol to be used will be given below.

D. Anonymous Identification Schemes

A subscriber must identify himself to the conference facility in an anonymous manner. Such anonymous identification is vital in a conference facility where a subscriber authenticates to a conference call facility without revealing identity. Most anonymous identification schemes are based on the concept of zero-knowledge proofs, which we again use later in our invited conference call facility. We are specifically interested in the case where it is necessary to identify a user as a member of a group, without (typically) identifying the user.

E. Anonymous Group Identification Schemes

The last technology used in our architecture is concerned with anonymous identification. Some identification schemes are based on the number-theoretic problem of quadratic residuosity modulo a composite integer. One such example is the general paradigm of zero-knowledge proofs which proves the knowledge of an identity without revealing any information about it [18]. The basic idea of the *zero-knowledge paradigm* is that it is not used to prove existence of witnesses but rather “knowledge about knowledge” [19]. The concept of zero-knowledge proofs was first introduced by Goldwasswer et al. [17] such that a user can convince a polynomial bounded verifier of identity whilst not relinquishing any information that would otherwise identify the user. Take for example U whose goal is not to prove that X belongs to Y but to show that it knows the status or relationship that exists between X and Y. A verifier V thus only obtains U’s state of knowledge and no information with respect to U.

In this paper anonymous *group* identification is required as a conference facility consists of two or more attendants.

Formally, a group identification scheme is a method that allows a user of a system or member of a group denoted by $G = \{M_1, \ldots, M_i\}$ to convince a third party that they in fact belong to the Group. The additional property of being anonymous requires that the scheme is firstly secure and secondly that the member (M_x) of the group (G) does not reveal its identity to the Group at any stage in the communication process.

A group identification scheme is a distributed protocol executed by a trusted participant, usually referred to as the Centre (denoted by C), many participants called the Users (denoted by U_i), and another trusted participant, called the Verifying Authority (denoted by V_{auth}). The group identification scheme is divided into two phases, namely the *Initialization phase* and the *Identification phase*. This illustrates an efficient zero-knowledge group identification for a single user. In our case a single mobile user identification is required to the group (multi-user) conference call.

One way of achieving zero-knowledge proofs is by exploiting the properties of Blum integers. For more detail on Blum Integers and its properties please refer to [20] and [21]. [22] presents a communication-efficient group identification scheme whose security property is based on the computational difficulty of factorizing Blum integers. We adapt this group identification scheme for use in our communication-efficient protocol for an invited conference call facility. It is imperative that we outline the group identification scheme phases as this has a direct impact on our invited conference call facility setup.

1) Initialization Phase: The Centre C generates a Blum integer x. C distributes to each user U_i an integer y_i and w_i where y_i is a quadratic residue modulo x and w_i is the square root of x. The initializing protocol which Centre C performs is as follows [23]:

1) Uniformly choose n-bit primes p,$q \equiv 3 \bmod 4$ and set $x = pq$.
2) For $i = \{1, \ldots, m\}$ uniformly choose $w_i \in Z_x^*$ and compute
$y_i = w_i^2 \bmod x$; set $public\_key_i = (x, y_i)$ and send $secret\_key_i = w_i$ to user U_i;
3) Set $public\_key = (public\_key_1, \ldots, public\_key_m)$;
and output $(public\_key, (secret\_key_1, \ldots, secret\_key_m))$.

2) Identification Phase: Informally, a user U_i identifies itself to the verifying authority V_{auth} by providing knowledge about the secret key associated with the U_i public key. The secret key is received during the initialization phase. It is important to note: user U_i has a $1/2$ chance of cheating in this protocol and thus the protocol must be repeated a number of times to be confident in his knowledge of the secret key.

IV. Private Communication-Efficient Protocol

Recall from Section III that we defined two varieties of anonymous mobile conference call scenarios, namely: *Invited* and *Public* conference call facility.

A. Public Mobile Conference Call Facility

Figure 2 illustrates the public mobile conference call setup. As described in [5], a calling service subscriber or calling dominant dials a particular short code or address at call setup, in this case, the MCU’s associated mobile subscriber ISDN number (MSISDN) [14]. This call may be charged by the serving GSM network operator at a premium rate. Upon an initiate conference call setup request an Interactive Voice Response (IVR), at the MCU, guides the dominant through the steps in creating a conference call facility. DTMF (refer to Section II) allows the conference call initiator to communicate with this specially configured network services, during a voice connection [14], in establishing the conference call facility. The MCU generates and sends a Virtual Number to the TTP. It is then the responsibility of the TTP to distribute this VN and related conference call descriptor to any connected GSM networks, so that the network will know to route calls using the VN to the TTP. After GSM network publication of the VN and available associated conference call facility, any MS $(U_1 \ldots U_i)$ may place a call to the VN and become a attendee of the conference facility. The MCU manages the conference facility creation (session establishment), media translation and control conversion for joining attendants in a conference call facility. The dominant may revoke the conference call facility or alternatively, after an expiry time, the MCU may revoke the VN. After this MS $(U_i \ldots U_i)$ will be unable to call the conference call facility on this VN.

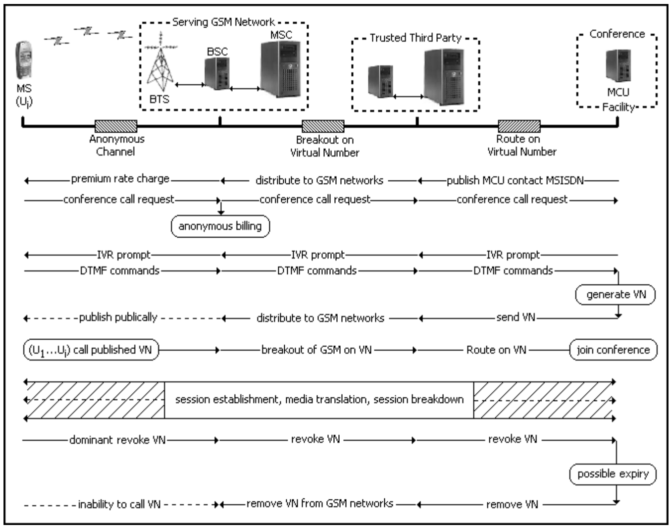

Fig. 2. Anonymous Public Mobile Conference Call Facility Protocol

B. Invited Mobile Conference Call Facility

In an invited mobile conference call facility, we choose to make use of anonymous group identification schemes combining identity from the anonymous channelling ticket. The Temporal Key (TK_i) holds the relationship to the restricted conference call facility. This "proof of knowledge" contained in the Temporal Key linked to a VN is sufficient in anonymously identifying the attendant when requesting access to the conference facility. It is important to note that such a direct association may hold sufficient proof and therefore nullifies the requirement in repeating the identification phase (refer to III-E.2 of the protocol. Remember that there is a 50% chance of cheating in this protocol). The protocol may be repeated a number of times to show a higher confidence in knowledge of a secret key.

The ticket used $(Auth_{VLR}; TK_i; T_{exp})$ for anonymous channelling remains unchanged where TK_i, now through zero-knowledge proof, contains sufficient knowledge regarding the established conference facility. We define a zero-knowledge proof Temporal Key which is structured as follows:

$$zkTK_i = A3(K_i; T_{exp}; secret\_key_i; VN) \qquad (2)$$

where $secret\_key_i = w_i$ (refer to Section III-E.1) relating to a Blum Integer generated at the MCU, and VN is the Virtual Number assigned by the MCU. Thus, through the zero-knowledge Temporal Key $(zkTK_i)$, there is a private relationship between the MS (U_i) and the VN. The U_i identifies itself to the verifying authority — in this case the MCU — by providing knowledge about the secret key associated with the U_i public key contained within its zero-knowledge Temporal Key $(zkTK_i)$. Furthermore, MS (U_i) may be involved in numerous conference facilities over a period of time and may continually require access to specific conference call groups. We define a zero-knowledge proof Temporal Key for access to multiple conference facilities which is structured as follows:

$$zkTK_i = A3(K_i; T_{exp}; \{(C_{1_{secret\_key_i}}; VN_1); \ldots; (C_{M_{secret\_key_i}}; VN_M)\}) \qquad (3)$$

where $\{(C_{1_{secret\_key_i}}; VN_1); \ldots; (C_{M_{secret\_key_i}}; VN_M)\}$ represents the set of secret keys associated with conference facilities $\{C_1; \ldots C_M\}$ linked to individual Virtual Numbers $\{VN_1; \ldots VN_M\}$.

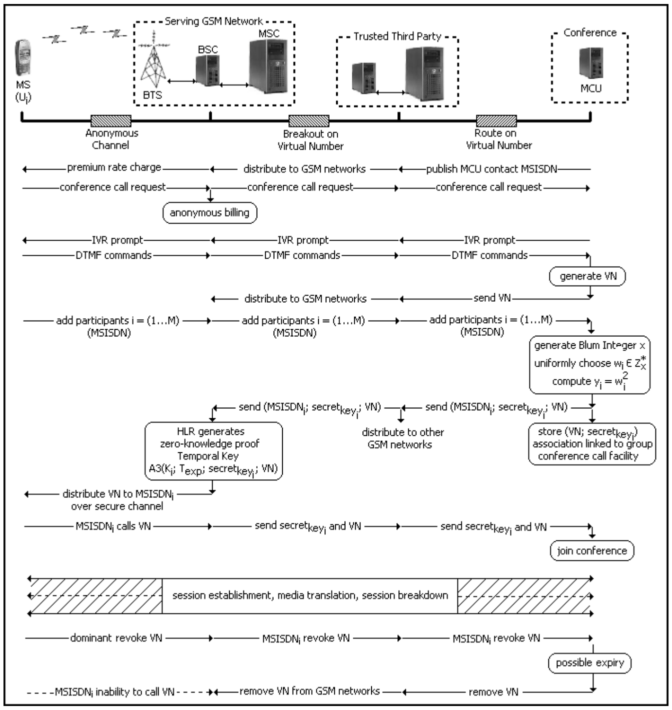

Fig. 3. Anonymous Invited Mobile Conference Call Facility Protocol

Figure 3 illustrates the invited mobile conference call facility protocol. Like in the public conference call scenario, a dominant dials a particular short code or address at call setup (the MCU's associated MSISDN). The dominant again uses DTMF commands in establishing the conference facility. Using DTMF, attendants are added by their mobile numbers $(MSISDN_i)$. The MCU generates a Blum Integer x, uniformly choosing $w_i \in Z_x^*$ and computes $y_i = w_i^2 \bmod x$. The MCU sends the $MSISDN_i$, $secret\_key_i$ and Virtual Number (VN) to the TTP and stores the $(VN; secret\_key_i)$ association linked to the invited group conference call facility. It is then the responsibility of the TTP to distribute this triplet to the serving GSM network of the $MSISDN_i$. The HLR of the serving GSM network generates a zero-knowledge Temporal Key $(zkTK_i)$ for $MSISDN_i$. The VN and conference facility descriptor is distributed over a secure channel to the $MSISDN_i$, for example using secure SMS [11]. Thereafter, the attendants in the invited conference call facility may call the assigned VN. The $secret\_key_i$ is retrieved from the serving GSM network and used in conjunction with the VN for anonymous group authentication to the restricted conference call facility. The dominant may revoke the conference call facility or the participant may revoke the VN linked to $MSISDN_i$.

V. Conclusion

In this paper we provided an anonymous mobile conference call architecture and private communication-efficient protocol. We outlined various key aspects including anonymous group identification schemes, anonymous channelling and billing in GSM, Trusted Third Party (TTP) proxies and Virtual Numbers (VNs). Our anonymous mobile conference call architecture encompasses these privacy elements allowing for both an invited and public conference facility where both attendant and network anonymity is achieved. Future work includes a formal communication-efficient protocol security and privacy analysis.

References

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

[2] N. Croft, "Secure interoperations of wireless technologies," Masters Dissertation, University of Pretoria, School of Computer Science, October 2003.

[3] M. Mouly and M. Pautet, "The GSM system for mobile communications, cell & sys," 1992.

[4] L. Chin, J. Wen, and T. Liu, "The Study of Interconnection of GSM Mobile Communication System Over IP Based Network," *VTC*, pp. 2011–2015, 2001.

[5] 3GPP, *Technical Specification Group Services and System Aspects; Voice Group Call Service (VGCS); Stage 1*, ts 02.68 v8.2.1 ed., 3rd Generation Partnership Project, July 2005.

[6] A. Pfitzmann and M. Köhntopp (Hansen), “Anonymity, unobservability, pseudonymity and identity management — a proposal for terminology,” *LNCS, Springer-Verlag*, vol. 2009, pp. 1–9, 2000.

[7] N. Croft and M. Olivier, “Using a Trusted Third Party Proxy in achieving GSM Anonymity,” in *South African Telecommunication Network and Applications Conference*. SATNAC, September 2004.

[8] A. Peinado, “Privacy and authentication protocol providing anonymous channels in GSM,” *Computer Communications*, vol. 27, no. 17, pp. 1709–1715, May 2004.

[9] N. Croft and M. Olivier, “Using compatible keys in achieving subscriber privacy channelling for billing in GSM Networks,” in *INC*, 2005.

[10] ——, “Codec-Hopping: Secure and Private Voice Communication in Bandwidth Constrained Networks,” in *SecPerU, Workshop on Security an Privacy in Pervasive Ubiquitous Computing*, Santorini, Greece, April 2005.

[11] ——, “Using an approximated one-time pad for securing Short Message Service (SMS),” in *South African Telecommunication Network and Applications Conference*. SATNAC, September 2005.

[12] S. Cimato, P. D’Arco, and I. Visconti, Eds., *Anonymous Group Communication in Mobile Networks*. Springer, 2003.

[13] *Recommendation GSM 02.09; Security related network functions*, European Telecommunications Standard Institute, ETSI, June 1993.

[14] H. V. J. Eberspacher and C. Bettstetter, *GSM Swithing, Services and Protocols*, Second ed. Wiley, 2001.

[15] 3GPP, *Technical Specification Group Core Network; Support of Dual Tone Multi-Frequency (DTMF) signalling*, 3rd ed., 3rd Generation Partnership Project, Janruary 2005.

[16] D. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[17] S. M. S. Goldwasswer and C.Rackoff, “The Knowledge Complexity of Interactive Proof Systems,” *SIAM*, vol. 18, pp. 186–208, 1989.

[18] A. Bar-Noy and Z. Naor, “Establishing a Mobile Conference Call Under Delay and Bandwidth Constraints,” in *INFOCOM*. IEEE, 2004.

[19] D. Chaum, Ed., *Demonstrating That a Public Predicate Can Be Satisfied Without Revealing Any Information About How*. Proceedings of CRYPTO, 1986.

[20] M. Blum, A. de Santis, S. Micali, and G. Persiano, “Non-Interactive Zero-Knowledge,” *SIAM Journal of Computing*, vol. 20, no. 6, pp. 1084–1118, December 1991.

[21] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*. New York: John Wiley and Sons, 1960.

[22] A. D. Santis, G. D. Crescenzo, and G. Persiano, “Communication-efficient anonymous group identification,” in *5th ACM Conference on Computer and Communications Security (ACM CCS98)*, vol. 3-5, San Francisco, California, U.S.A., 1998, pp. 73–82.

[23] A. F. U. Feige and A. Shamir, “Zero-Knowledge Proofs of Identity,” *Journal of Cryptography*, vol. 1, pp. 77–94, 1988.

Neil Croft Neil Croft is a PhD Computer Science student at the University of Pretoria. His research interests include security and privacy in current and next generation wireless communication networks. He completed his Masters degree at the University of Pretoria in October 2003 and undergraduate studies at the Rand Afrikaans University in 2001.