Identity-based Cryptography for Securing Mobile Phone Calls

Matthew Smith, Christian Schridde, Björn Agel, Bernd Freisleben
Department of Mathematics and Computer Science, University of Marburg
Hans-Meerwein-Str. 3, D-35032 Marburg, Germany
Email: {matthew, schriddc, agel, freisleb}@informatik.uni-marburg.de

Abstract

In this paper, an identity-based key agreement system for mobile telephony in GSM and UMTS networks is presented. The use of telephone numbers as public keys allows the system to piggyback much of the security overhead for key management to the existing GSM or UMTS infrastructure. The proposed approach offers solutions to the problems of multi-domain key generation, key distribution, multi-domain public parameter distribution and inter-domain key agreement.

1 Introduction

Since current encryption schemes in GSM (2G) and UMTS (3G) only encrypt calls between the mobile phone and the base station, an attacker positioned anywhere in the network between the two base stations can usually intercept calls without great difficulty. Furthermore, since GSM base stations are not authenticated, an attacker can pose as a base station and intercept phone calls in the vicinity using an IMSI catcher [1]. Due to backwards compatibility and UMTS coverage issues, most UMTS devices allow network fallback to GSM, opening up UMTS devices to the same Man-In-The-Middle Attacks (MITMA) that afflict GSM networks.

To prevent the such attacks, end-to-end protection of mobile phone calls is required. Conventional Public Key Infrastructure (PKI) based solutions are too complex both for the network providers and for the users. A simple approach is required that can be implemented by network providers independently of each other and which does not introduce added complexity for end users. Identity-based cryptography (IBC) [2], [3], [4] promises to offer an approach to end-to-end encryption for mobile telephone calls in which the telephone numbers of the call participants are used as the public keys to secure the communication channel, thus making the cryptographic security procedure as easy as making a telephone call. The use of telephone numbers as public keys has two major benefits. Firstly, since the caller knows the number to be called, the caller also automatically knows the public key and does not need a separate public key look-up or certification infrastructure. Secondly, telephone numbers are easy to understand, such that there is no need to educate users to understand the link between a telephone number, a public key and/or its certificate.

In this paper, a new identity-based key agreement system is introduced that focuses on the issues to be solved when implementing IBC for mobile telephony. The protocol allows two mobile phones to perform a session key agreement over an unsecured channel and between different providers using telephone numbers as public keys. Using the created session key, a symmetric encryption of all call data can be performed. Solutions to the problems of multi-domain key generation, key distribution, multi-domain public parameter distribution and inter-domain key agreement are presented.

The paper is organized as follows. Section 2 introduces the IBC protocol. Section 3 addresses implementation issues. Section 5 discusses related work. Section 6 concludes the paper and outlines areas for future research.

2 Protocol

2.1 Algorithmic Overview

The identity-based key agreement protocol *SSF* (Secure Session Framework) consists of four main algorithms: **Setup**, **Extract**, **Build SIK**, and **Compute**.

2.2 Key Agreement

The **Setup** algorithm (Fig. 1) is only performed once by the ID-PKG to create both the master secrets as well as the public parameters.

Public, Shared Parameters. *The public, shared parameters (PSP) of a domain* **D** *of the key agreement protocol* SSF *is the quadruple* $PSP = (N, G, R, H(\cdot))$.

The **Extract** algorithm (Fig. 2) is used by the ID-PKG to create the identity key (i.e. the private key) for a given identity.

The **Build SIK** algorithm (Fig. 3) is executed by the participating devices.

The random integer r_{ID} is generated with a secure number generator to make r_{ID} unpredictable. The private identity key is used in combination with this randomly chosen integer and the generator in such a way that it is not possible to extract the identity key from the SIK. This is due to the fact that the multiplications are performed in the ring $\mathbb{Z}_{\mathbb{N}}$ and the result set of a division in the ring $\mathbb{Z}_{\mathbb{N}}$ is so large that the extraction of the identity key is infeasible. The SIK is then sent over an unsecured channel to the other party and vice versa. The SIK must be greater than zero to prevent a trivial replacement attack where an attacker replaces the SIKs with zero which in turn would make the session key zero as well. Any other replacement attacks lead to invalid session keys.

The final step of the key agreement process is the computation of the session key using the **Compute** algorithm (Fig. 4) that is executed by the participating devices. By applying the inverse of the hash value of the opposite's identity, the involved identity key is canceled out. Only if both endpoint addresses match their identity keys, a valid session key is created.

For a more information on the *SSF* protocol, the reader is referred to [6].

2.3 Key Agreement Between Domains

The ID-PKG determines the public, shared parameters, and all entities that receive their identity key for their IDs from this generator can establish a key agreement among each other. Since telephone network providers are in charge of managing the MS information of their customers autonomously, it is desirable that they also manage the security information autonomously, meaning that they must be allowed to operate their own ID-PKG without having to cooperate with other providers. The management infrastructure, such as HLRs and AuC, can then simply be extended by the required additional data.

In the proposed cross-domain key agreement algorithm, each device only needs a single identity key, and the ID-PKGs do not need to agree on common parameters or participate in any form of hierarchy. Consider two domains D_1 and D_2 and their public parameters $(N_1, G_1, R_1, H_1(\cdot))$ and $(N_2, G_2, R_2, H_2(\cdot))$, respectively. Every parameter can be chosen independently. The case that $(R_2, \varphi(N_1)) > 1$ or $(R_1, \varphi(N_2)) > 1$ is not critical, since no R-th roots must be computed regarding the other domain's modulus. The two moduli N_1 and N_2 were chosen according to the requirements stated in the **Setup** algorithm, i.e. the computation of discrete logarithms is infeasible in $\mathbb{Z}_{N_1}$ and $\mathbb{Z}_{N_2}$, respectively.

In the following, an entity $\mathsf{E}_{\mathsf{ID}_1}$ from D_1 wants to communicate with $\mathsf{E}_{\mathsf{ID}_2}$ from D_2. The algorithm for cross-domain key agreement is shown in Fig. 5. In step 1, the common shared public parameters are the element-wise product of both sets of domain parameters. In step 2, entity $\mathsf{E}_{\mathsf{ID}_1}$ extends its identity key using the Chinese-Remainder Theorem. In step 3, entity $\mathsf{E}_{\mathsf{ID}_1}$ extends its hash identifier also using the Chinese-Remainder Theorem. The procedure for entity $\mathsf{E}_{\mathsf{ID}_2}$ is analog, only the indices change from 1 to 2. Key agreement is then performed using the extension of the original algorithm shown in Fig. 6.

3 Implementation Issues

In the following, several issues for deploying the proposed system in practice are discussed.

3.1 Distribution of Public Parameters

To distributed the public parameters, the idea is to integrate them into the GSM/UMTS lookup mechanism and carry the information over the SS7 [7] protocol. Since there already is lookup functionality to locate the HLR of a MS and the current location of the MS, a flag can be attached to the request message, stating that the public parameters of the MS should be sent piggybacked to the response. The flag is used, since the public parameters only need to be queried for the very first call to a MS of a particular provider. All subsequent calls to the same or other MS of the same provider do not need a further public parameter lookup. In the case of UMTS, this is reasonably secure since the BTS must authenticate itself to the MS and thus an active MITMA is prevented that could otherwise tamper with the public parameters. The passive MITMAs still possible with UMTS are not a danger to the transfer of the public parameters since they are

Setup - The **Setup** algorithm is executed by the ID-PKG.
Input: $k \in \mathbb{N}$
Step 1: Choose an arbitrary integer $R > 1$ from $\mathbb{Z}^+$.
Step 2: Generate two primes, P and Q, of bit length k with the following properties:
1. The prime factorization of $(P-1)$ contains a large prime P'
2. The prime factorization of $(Q-1)$ contains a large prime Q'
3. $\gcd(\varphi(PQ), R) = 1$, where $\varphi(\cdot)$ is the Totient Function.
Step 3: Compute the product $N = PQ$
Step 4: Choose a generator G of a subgroup $\mathbb{G}$ of $\mathbb{Z}_N$ whose order contains at least one of the primes P' or Q' such that the Computational Diffie Hellman Assumption (CDHA) [5] holds in $\mathbb{G}$.
Step 5: Choose a cryptographic collision-resistant hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_{\mathbb{N}}$.
Output: $PSP = (N, G, R, H(\cdot))$, $SP = \{P, Q\}$

Figure 1. Setup algorithm

Extract - The **Extract** algorithm is executed by the ID-PKG.
Input: PSP, SP, ID
Let ID be a given identity. The algorithm computes $d_{\mathsf{ID}} \equiv H(\mathsf{ID})^{1/R} \pmod{N}$. The integer d_{ID} is called the *identity key* and is given to the entity E_{ID}.
Ouput: d_{ID}

Figure 2. Extract algorithm

Build SIK - The **Build SIK** algorithm is executed by the entity E_{ID}
Input: PSP, d_{ID}
Step 1: Choose a random integer r_{ID} from $\mathbb{Z}^+$.
Step 2: Compute $SIK_{\mathsf{ID}} \equiv G^{r_{\mathsf{ID}}} \cdot d_{\mathsf{ID}} \pmod{N}$.
SIK_{ID} is the SIK (session initiation key) for the identity string ID that belongs to entity E_{ID}.
Output: SIK_{ID}

Figure 3. Build SIK algorithm

Compute - The **Compute** algorithm is executed when two parties perform a key agreement.
Input for $\mathsf{E}_{\mathsf{ID}_1}$: $\mathsf{E}_{\mathsf{ID}_2}$, PSP, SIK_{ID_2}, r_{ID_1}
Input for $\mathsf{E}_{\mathsf{ID}_2}$: $\mathsf{E}_{\mathsf{ID}_1}$, PSP, SIK_{ID_1}, r_{ID_2}

When $\mathsf{E}_{\mathsf{ID}_1}$ receives the session initiation key from $\mathsf{E}_{\mathsf{ID}_2}$, it calculates
$(SIK_2^R \cdot H(\mathsf{ID}_2)^{-1})^{r_{\mathsf{ID}_1}} \equiv ((G^{r_{\mathsf{ID}_2}} \cdot d_{\mathsf{ID}_2})^R \cdot H(\mathsf{ID}_2)^{-1})^{r_{\mathsf{ID}_1}} \equiv G^{Rr_{\mathsf{ID}_1} r_{\mathsf{ID}_2}} \equiv S \pmod{N}$

When $\mathsf{E}_{\mathsf{ID}_2}$ receives the session initiation key from $\mathsf{E}_{\mathsf{ID}_1}$, it calculates
$(SIK_1^R \cdot H(\mathsf{ID}_1)^{-1})^{r_{\mathsf{ID}_2}} \equiv ((G^{r_{\mathsf{ID}_1}} \cdot d_{\mathsf{ID}_1})^R \cdot H(\mathsf{ID}_1)^{-1})^{r_{\mathsf{ID}_2}} \equiv G^{Rr_{\mathsf{ID}_1} r_{\mathsf{ID}_2}} \equiv S \pmod{N}$

Output: $H(S)$, the common session key for $\mathsf{E}_{\mathsf{ID}_1}$ and $\mathsf{E}_{\mathsf{ID}_2}$.

Figure 4. Compute algorithm

Cross-Domain Key Extension (from the view of participant $\mathsf{E}_{\mathsf{ID}_1}$)
Input: PSP_1, PSP_2, d_{ID_1}
Step 1: Calculate the common, shared, public parameters: $PSP_{1,2} = (N_1 \cdot N_2, G_1 \cdot G_2, R_1 \cdot R_2, H_2(\cdot))$.
Step 2: Use the Chinese-Remainder Theorem to calculate the integer $\widetilde{d}_{\mathsf{ID}_1}$:

$$\widetilde{d}_{\mathsf{ID}_1} \equiv d_{\mathsf{ID}_1} \pmod{N_1} \text{ and } \widetilde{d}_{\mathsf{ID}_1} \equiv 1 \pmod{N_2}$$

Step 3: Use the Chinese-Remainder Theorem to calculate the integer $\widetilde{H_1}(\mathsf{ID})$:

$$\widetilde{H_1}(\mathsf{ID}_1) \equiv H_1(\mathsf{ID}_1)^{R_2} \pmod{N_1} \text{ and } \widetilde{H_1}(\mathsf{ID}_1) \equiv 1 \pmod{N_2}$$

Step 4: Build $eSIK_{\mathsf{ID}_1}^{(1,2)} \equiv (G_1 \cdot G_2)^{r_{\mathsf{ID}_1}\widetilde{d}_{\mathsf{ID}_1}} \pmod{N_1 N_2}$
Output: $eSIK_{\mathsf{ID}_1}^{(1,2)}$, the cross-domain session initiation key.

Figure 5. Cross-Domain Key Extension algorithm

public anyway. In the case of GSM, this form of public parameter distribution holds the risk of an attacker with an IMSI catcher replacing the public parameters with his own on the first call made to a provider by a MS. However, this attack only works on the very first call ever placed to a provider and will be detected as soon as the MS calls someone else at the same provider after the attack due to a public parameter mismatch.

3.2 Distribution of the Identity Keys

The most critical element in all IBEs or PKIs in key escrow mode is the distribution of the identity keys (private keys) and the prevention of identity misbinding. In a mobile phone scenario, identity keys can be placed on the SIM card during manufacturing. Since the deployment process of SIM cards is already set up to include sensitive personal information, adding the identity key to the SIM is not difficult. If there is no requirement for key expiration, this is most likely the best solution, since the identity key is never transmitted over a public network and thus the risk of compromise is minimized. However, if a more flexible online system is required, the novel structure of the presented algorithm allows this as well. If the public parameters of the provider for a MS can be placed on the SIM during manufacturing, the presented system offers a secure way to transmit identity keys securely over an insecure network. When a MS first connects the the network, it requests its identity key from its home provider. Since this message exchange is security critical, the messages must be protected. To this end, the client creates a session key that is encrypted using the public parameter N (N can be used in the same way as an RSA public key) of the provider. The session key can only be decrypted by the provider who then uses the session key to encrypt the identity key of the MS using AES, and sends it to the client. Since even an active MITMA cannot compromise this message exchange, because it is not in possession of the P and Q to decrypt the session key, the transfer of the identity key is secure. This novel online distribution of identity keys allows key expiration (see below) to be implemented without a significant overhead, since no further security infrastructure or out-of-band communication is required. The algorithm implemented for this approach is shown in Fig. 7.

3.3 Key Expiration

Another practical issue of mobile phone call encryption is the fact that telephone numbers are reused. In the presented identity-based solution, natural key expiration techniques can be used to cope with telephone number reuse. Boneh et al. [3] showed how keys can be given a lifetime, which allows natural expiration of the identity key. This is done by the internal concatenation of the ID, in our case the telephone number, with a date. The same technique can be used in our solution. Thus, when a customer releases a telephone number and it is reused, the next customer will have a different identity key based on the current date. Since telephone number reuse is time-delayed in any case, this time frame can be used as the key lifetime to ensure that each successive owner lies in a new lifetime slot. With the techniques introduced in this paper, a frequent automatic in-band key distribution can be safely executed and thus key renewal is far less of a problem. Additionally, key expiration also reduces the risk of identity key theft, since the attack window

Cross-Domain: Compute SK algorithm
Input for $\mathsf{E}_{\mathsf{ID}_1}$: ID_2, $PSP_{(1,2)}$, $eSIK^{(1,2)}_{\mathsf{ID}_2}$, r_{ID_1}, $\widetilde{H_2}(\mathsf{ID}_2)$
Input for $\mathsf{E}_{\mathsf{ID}_2}$: ID_1, $PSP_{(1,2)}$, $eSIK^{(1,2)}_{\mathsf{ID}_1}$, r_{ID_2}, $\widetilde{H_1}(\mathsf{ID}_1)$
When $\mathsf{E}_{\mathsf{ID}_1}$ receives the session initiation key from $\mathsf{E}_{\mathsf{ID}_2}$, it calculates
$\left(((G_1 \cdot G_2)^{r_{\mathsf{ID}_2}} \widetilde{d}_{\mathsf{ID}_2})^{R_1 \cdot R_2} \widetilde{H_2}(\mathsf{ID}_2)^{-1}\right)^{r_{\mathsf{ID}_1}} \equiv (G_1 \cdot G_2)^{R_1 R_2 r_{\mathsf{ID}_1} r_{\mathsf{ID}_2}} \equiv S \pmod{N_1 \cdot N_2}$
When $\mathsf{E}_{\mathsf{ID}_2}$ receives the session initiation key from $\mathsf{E}_{\mathsf{ID}_1}$, it calculates
$\left(((G_1 \cdot G_2)^{r_{\mathsf{ID}_1}} \widetilde{d}_{\mathsf{ID}_1})^{R_1 \cdot R_2} \widetilde{H_1}(\mathsf{ID}_1)^{-1}\right)^{r_{\mathsf{ID}_2}} \equiv (G_1 \cdot G_2)^{R_1 R_2 r_{\mathsf{ID}_1} r_{\mathsf{ID}_2}} \equiv S \pmod{N_1 \cdot N_2}$
Output: S, the common session key for $\mathsf{E}_{\mathsf{ID}_1}$ and $\mathsf{E}_{\mathsf{ID}_2}$

Figure 6. Cross-Domain Compute SK algorithm

Identity Key Request and Submit algorithm.
Input: $PSP \in \mathbb{N}$
Step 1 (E_{ID}): Choose an arbitrary integer w from $\mathbb{Z}^+$.
Step 2 (E_{ID}): Compute $c \equiv w^R \pmod{N}$.
Step 3 (E_{ID}): Send c to ID-PKG.
Step 4 (ID-PKG): Compute $D \equiv R^{-1} \pmod{\varphi(N)}$
Step 5 (ID-PKG): Compute $c^D \equiv w \pmod{N}$.
Step 6 (ID-PKG): $C \leftarrow AES_{enc}(w, d_{\mathsf{ID}_A})$.
Step 7 (ID-PKG): Send C to entity E_{ID}.
Step 8 (E_{ID}): $d_{\mathsf{ID}_A} \leftarrow AES_{dec}(w, C)$
Output: d_{ID_A}

Figure 7. Identity Key Request and Submit

is restricted to a small time interval.

4 Experimental Results

In this section, experimental results of the presented identity-based cryptographic security solution for mobile phone key agreement are presented. The experiments were run on a Nokia N82-1 and a Nokia N95-1 both with an ARM-11 CPU with 330 MHz running Symbian 9.2 FP1. Both the performance of the key agreement and the ensuing symmetric AES encryption were measured. To gain a robust mean, all experiments were performed 100 times. For the key agreement, the following parameters were examined: the modulus - with N = 512, 1024, 2048 and 4096 Bit, the random exponent - with r_{ID} = 64, 128, 256 and 512 Bit and the chosen public parameter R = {3, 17, 513, 65537}. The numbers chosen for R were selected to give an overview of the performance of the algorithm based on the size of R. R can be chosen arbitrarily by the ID-PKG according to the setup algorithm (Step 2.3). For example, Table 4 contains the mean time for the key agreement operations of the 100 trial runs computed using a fixed modulus of N = 2048 with r_{ID} and R in the rows and columns.

2048-Bit Modulus				
bitsize of r_{ID}	R			
	3	17	513	65537
64-Bit	622	670	670	700
128-Bit	1192	1186	1208	1169
256-Bit	2320	2421	2334	2435
512-Bit	4577	4559	4582	4575

Table 1. Measurements (milliseconds)

The main contribution to the computational time is the random exponent. The public random number R selected by the provider does not have a significant effect due to the fact that the computational time of the algorithm depends on the number of $1's$ in the binary representation of the number and the used random numbers all contain two binary $1's$. The random number R is not security critical for $R > 3$. Key agreement with a 2048-bit modulus and 128 or 256-bit random exponents has acceptable run times for current devices. Once a session key has been established, a symmetric encryption of the call using AES 256 is executed. The encoding block was set to 4096 Byte which contains at least 256 ms (depending on the compression) of audio data. On the N95-1 and N82-2 it only takes an average of 24.1 ms to encrypt the block, so the phones can easily cope with the real time encryption of the voice data.

5 Related Work

Kumar et al. [8] present an IBC based approach to mutual authentication and key agreement for GSM networks. Unlike our proposal, Kumar et al. use the IMSI number as the public identity key. The security

of the protocol relies on a secure channel to the HLR and VLR (Phase 1, Steps 2 and 3). Both these design decision have drawbacks. Firstly, using the IMSI as the public key means the users must trust the infrastructure to show them the correct binding between telephone number and IMSI number, since most users do not know their own IMSI, let alone the IMSI of other users. Secondly, the communication channels between the MS and the HLR and VLR are not considered to be secure and must be handled by the presented solution.

There are other approaches such as the Cryptophone [9] that applies the ZFone [10] VoIP security mechanism to mobile phones. ZFone executes a standard Diffie-Helmann key agreement (which is vulnerable to an active MITMA), but then displays a hash of the generated session key to both users. One user must then read out the hash to the other user, who can then see if the key agreement was compromised, since if a MITMA attack has taken place, the hash values are different. While preventing simple MITMAs, the ZFone solution is somewhat cumbersome, since users must read out hash values to each other. It also does not prevent impersonation attacks or voice based MITMA attacks. While the latter might seem difficult, recent events have shown how easy such attacks can be performed. A voice imitation artist made a phone call to a German politician professing to be a colleague and successfully lead the fake conversation and published the recording to Youtube. Such low tech principles can easily be used to break the ZFone security by simply overlaying the voice imitator reading the compromised session key whenever the user is asked to read out the hash. The key distribution system proposed by Okamoto [11] extracts its identity information in a similar manner as in our scheme, but does not address the case of key agreement between different domains.

6 Conclusions

In this paper, an identity-based key agreement system for mobile telephony in GSM and UMTS networks was presented. The approach offers solutions to problems of multi-domain key generation, key distribution, multi-domain public parameter distribution and inter-domain key agreement. Experimental results based on a Symbian implementation for the Nokia smartphones N95-1 and N82-1 were presented showing that current smartphones are powerful enough to run the presented system.

Future work will include simulated large scale deployment and scalability studies to quantitatively evaluate the administrative benefit of using the presented identity-based approach compared to a traditional PKI. Finally, user-studies will be performed to further evaluate the benefits to the non-tech savvy end user.

References

[1] U. Meyer and S. Wetzel, "A Man-In-The-Middle Attack on UMTS," in *WiSe '04: Proceedings of the 3rd ACM Workshop on Wireless Security*. New York, NY, USA: ACM, 2004, pp. 90–97.

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Advances in Crytology - Crypto 84, Lecture Notes in Computer Science*, vol. 196, pp. 47–53, 1984.

[3] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM Journal of Computation*, vol. 32, no. 3, pp. 586–615, 2003.

[4] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," in *Proc. of the 8th IMA International Conference on Cryptography and Coding*. Springer-Verlag, 2001, pp. 360–363.

[5] F. Bao, R. H. Deng, and H. Zhu, "Variations of Diffie-Hellman Problem," in *International Conference on Information and Communications Security*, 2003, pp. 301–312.

[6] C. Schridde, M. Smith, and B. Freisleben, "An Identity-Based Key Agreement Protocol for the Network Layer," in *SCN - The 6th Conference on Security and Cryptography for Networks*, vol. 5229. Lecture Notes in Computer Science, Springer-Verlag, 2008, pp. 409–422.

[7] L. Dryburgh and J. Hewett, *Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Applications*. Cisco Press, 2003.

[8] K. P. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, "Mutual Authentication and Key Agreement for GSM," in *ICMB '06: Proceedings of the International Conference on Mobile Business*. Washington, DC, USA: IEEE Press, 2006, p. 25.

[9] "Cryptophone," HTTP://WWW.GSMK.DE/.

[10] "ZFone," HTTP://ZFONEPROJECT.COM/.

[11] E. Okamoto, "Key Distribution Systems Based on Identification Information," in *CRYPTO '87: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*. London, UK: Springer-Verlag, 1988, pp. 194–202.