A Strong User Authentication Protocol for GSM

Özer Aydemir

TÜBİTAK UEKAE İLTAREN Research Center
06100 Ankara TURKEY
ozer.aydemir@iltaren.tubitak.gov.tr

Ali Aydın Selçuk

Dept. of Computer Engineering, Bilkent University
06800 Bilkent Ankara TURKEY
selcuk@cs.bilkent.edu.tr

Abstract

Traditionally, the authentication protocols for cellular phone networks have been designed for device authentication rather than user authentication, which brings certain limitations and restrictions on the functionality of the system. In this paper we propose a user authentication protocol for the Global Standards for Mobile (GSM) which permits the use of weak secrets (e.g. passwords or PINs) for authentication, providing new flexibilities for the GSM users.

Keywords: *Wireless network security, GSM, user authentication, strong password protocols.*

1. Introduction

Mobile telephone networks are becoming more popular everyday, and the *Global System for Mobile* (GSM) is the most commonly used standard for mobile communications with more than one billion users worldwide [5]. GSM defines the services, functional/subsystem interfaces, and protocol architecture for digital mobile radio networks. Identity of a GSM subscriber is established by the *subscriber identity module* (SIM). For authentication, GSM relies on a symmetric encryption key embedded in the SIM card [3, 6, 11].

One of the reasons for preferring device authentication in GSM rather than user authentication is humans' inability to remember strong secrets; they tend to choose weak secrets such as short PINs, dictionary words, birthdays as passwords, which are vulnerable to dictionary attacks. Two early solutions to that problem are the Encrypted Key Exchange (EKE) protocol [1] and Gong et al.'s protocol [4], which have several extensions [2, 7, 8, 10, 12]

In this work we have designed a new strong user authentication protocol for GSM, in order to bring some flexibilities to GSM users. Mobile users can redirect their calls, reach their accounts without their SIM card, or easily disable their accounts without interacting with the operator of the service provider.

We give an overview of strong password protocols in Section 2. Section 3 reviews the current GSM authentication protocol. Section 4 presents the new user authentication approach to GSM; Section 5 presents the experimental results on the protocols; and finally Section 6 concludes the paper.

The notations common to the rest of the paper are as follows:

Π_i : Password of user i

$E_x\{p\}$: Public key encryption of plaintext p with the key of x

K(p): Symmetric key encryption of plaintext p with key K.

2. A Review of Strong Password Protocols

Assume that two parties Alice and Bob try to establish a secret, authenticated session key for their communication. The only secret they share is a user password Π, which is vulnerable to dictionary attacks. The aim of strong password protocols is to authenticate the user while protecting the password against dictionary attacks by online eavesdroppers. Two early works in this category are the EKE protocol of Bellovin and Meritt [1] and the protocol of Gong et al. [4]. Both protocols aim to authenticate the parties of

0-7695-2362-5/05 $20.00 © 2005 IEEE

communication and protect the user's password against eavesdroppers.

2.1 Encrypted Key Exchange

The Encrypted Key Exchange (EKE) protocol provides secure authentication between user and a server using a weak secret. There are two main classes of the EKE protocol; one based on public key encryption, the other on Diffie-Hellman key exchange.

EKE is a generic protocol and can be used with any public key scheme with minor modifications [1]. Even though EKE is a secure user authentication protocol with weak secrets, generating per session public-private key pairs and doing private key operations on client side make it infeasible to use with computationally restricted devices.

In 2002 Zhu et al. presents a variant of RSA-EKE for mobile devices [13]. The proposed protocol eliminates the need for per session RSA key generation. However, an "interactive step" included against e-residue attacks brings additional computational costs on both the server and client sides.

2.2 Protocol of Gong at al.

Another influential work on strong user authentication with weak passwords is a proposal by Gong et al. [4]. This solution contains a trusted third party which is continuously available online, as in Kerberos. The parties in the system authenticate each other by the help of the trusted server. In this protocol, unlike EKE, there is no need to generate fresh public/private key pairs per session, but there is a need for the trusted server's public key to be known to all parties.

3. Review of Authentication in GSM

GSM contains three entities in a session: a mobile subscriber (cellular phone), visiting location register (VLR), and home location register (HLR). Alice's SIM card contains a secret authentication key K_A and unique "International Mobile Subscriber Identity" (IMSI). A3, A5 and A8 algorithms are used in authentication, where A3 and A8 are one-way functions and A5 is a symmetric encryption function [6].

Fig. 1 illustrates the authentication protocol of GSM for the first connection attempt of the mobile subscriber to a certain VLR. K_A and K_t respectively are permanent and temporary key of Alice (mobile client). Alice sends her unique identity to VLR, VLR passes this identity to HLR in order to inform it that Alice wants to log in to the system. HLR generates a random number RAND, calculates temporary authentication key K_t for consecutive attempts, and the *security result* SRES that is equal to K_A and RAND encrypted with A3. VLR passes RAND to the mobile client and keeps K_t and SRES. Alice calculates SRES and sends it to VLR. If SRES sent by Alice is equal to SRES sent by HLR then VLR sends TMSI encrypted with K_c to the mobile client to be used in consecutive authentication attempts without the need of contacting the HLR.

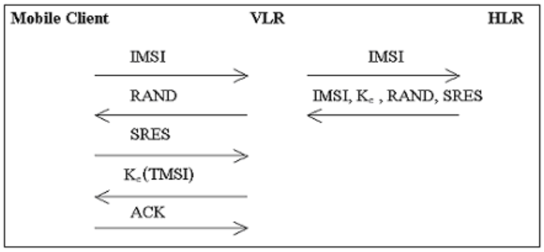


Figure 1. GSM Authentication using IMSI

4. A User Authentication Protocol for GSM

In this section, we describe the GSM User Authentication Protocol (GUAP). The current GSM authentication scheme uses a cryptographic authentication key embedded in the SIM card of the device. By the new approach, the user can authenticate with her password instead of the embedded key. Using passwords instead of embedded keys breaks the dependency on the SIM card during authentication. Users will be able to reach their accounts without their SIM cards, via any cellular phone, Internet, or a special network. Users can reach their address book, redirect their calls, or get their personal information without the need of either SIM card or giving their personal information to operators of the service provider.

GSM authentication protocol resembles the approach of Gong et al. [4] in certain ways. Both schemes are based on three entities, and in both cases the third entity is a trusted server whose public key is known by all parties. Unlike Gong et al.'s protocol, in GSM authentication, VLR is an automated non-human entity, which is able to remember strong secrets. Another difference is in regard to the use of timestamps. Clock synchronization may be a crucial problem in GSM authentication, which can be solved by generating random nonces for freshness guarantee of the sessions.

GUAP is illustrated in Fig. 2. Mobile user wants to be authenticated to HLR via VLR, using her password Π. A random nonce, RAND, is generated by VLR per session and provides freshness guarantee for the session. Three random nonces generated by the mobile client are n_1, n_2 and c; n_1 proves the correct decryption of HLR in the fifth message, n_2 masks the session key k, c protects the first message against replay by adversary.

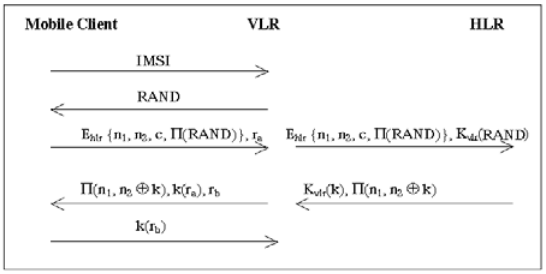

Mobile Client
VLR
HLR
IMSI
RAND
$E_{hlr}\{n_1, n_2, c, \Pi(RAND)\}, r_a$
$E_{hlr}\{n_1, n_2, c, \Pi(RAND)\}, K_{vlr}(RAND)$
$\Pi(n_1, n_2 \oplus k), k(r_a), r_b$
$K_{vlr}(k), \Pi(n_1, n_2 \oplus k)$
$k(r_b)$

Figure 2. User authentication approach to GSM

The protocol starts with the client's authentication request by sending its unique identity (IMSI) to VLR. VLR generates and sends a random number RAND to Alice. Alice generates three random nonces n_1, n_2 and c, and encrypts RAND with her password. She then encrypts n_1, n_2, c, and Π(RAND) with HLR's public key and sends it to VLR with a random challenge r_A. VLR takes the message and encrypts the RAND with its symmetric key, and sends it with HLR's portion of the message to HLR. HLR, knowing VLR's symmetric key, decrypts the message, then asymmetrically decrypt the message come from Alice, finally decrypts Π (RAND) to get RAND, if both RAND are equal then HLR is sure about VLR's and Alice's identities. HLR generates a session key for VLR and Alice, encrypts it with VLR's symmetric key for VLR, and encrypts the masked session key ($n_2 \oplus k$) and n_1 with Alice's password, then sends both messages to VLR. VLR decrypts its portion of the message to get session key k, encrypts the challenge r_A with k sent by Alice in first message, forwards Alice's portion of message with the response to her challenge and a new challenge r_B. Alice decrypts the message coming from HLR and gets the session key k. She then responds to VLR's challenge. In consecutive sessions Alice and VLR can use the generated session key k without need of re-authentication.

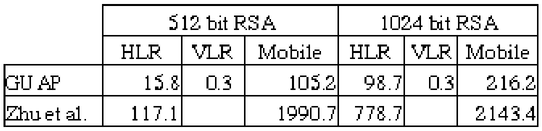
The existence of the correct n_1 value in the fifth message indicates that it is the HLR that has decrypted the first message and sending this output. The random nonce n_2 protects HLR's response encrypted by Π against dictionary attacks on Π by an attacker who gets to know k or by VLR. The issue here is a dictionary attack by someone who knows k and hence can guess n_1 and n_2. Random c protects first message against regeneration by VLR: Again a malicious VLR or an adversary that has compromised a past session key k, can choose a candidate password Π′ and decrypt the message of mobile client to get candidate n_1' and n_2'. Without the confounder c, the adversary can generate a candidate first message. If the candidate message is equal to real message then the password guess is correct [4].

In the protocol VLR is not a user entity, hence it is able to remember and perform its operations with a strong cryptographic key K_{vlr}. This reduces the computational cost of Gong et al.'s protocol. The only asymmetric key operation done by the mobile client is a public key encryption in the first message. If RSA is used here, then the public exponent of the key pair can be fixed to a small prime, reducing the computations on the client side.

5. Experimental Results

In order to test the efficiency of GUAP we carried out several simulation experiments. The HLR and VLR are simulated on a 2.4 GHz Pentium IV machine, and the mobile client runs on Sun's KToolbar v.2.0 simulation toolkit [14]. The simulations are implemented in Java2 Standard Edition (J2SE) for HLR and VLR, and in Java2 Mobile Edition (J2ME) for the mobile client. The cryptographic functions are inherited from the Bouncy Castle Lightweight Crypto API [15] for both J2SE and J2ME.

Table 1. Average CPU time (in milliseconds)



	512 bit RSA			1024 bit RSA		
	HLR	VLR	Mobile	HLR	VLR	Mobile
GU AP	15.8	0.3	105.2	98.7	0.3	216.2
Zhu et al.	117.1		1990.7	778.7		2143.4

The simulation results show that the GUAP computations can be carried out efficiently in a reasonable time by all the parties, either with 512- or

1024-bit RSA. The load on the VLR is particularly low, as a result of the design decision to use symmetric key encryption between the VLR and HLR.

Zhu et al.'s protocol seems to be significantly slower. However it must be noted that this protocol was designed for a somewhat more restricted setting where the mobile device does not have a priorly established trust with the server and cannot have the server's public key installed securely beforehand. Nevertheless, we included it in the simulation experiments due to its significance as the only strong password protocol designed specifically for constrained mobile devices.

6. Conclusion

GSM is widely used over the world. If user authentication becomes possible for mobile users, everybody will be able to reach their accounts without their SIM card. People can redirect their calls through Internet, or reach their accounts through anybody's phone only by entering their username and password. We have presented a strong user authentication protocol for GSM that permits user authentication to the standard. Our protocol is inspired by strong authentication protocols for weak secrets [1, 4]. Our main goal is to break the dependency on SIM cards for authentication in GSM and to make the standard more flexible for users. The design takes into consideration the computational restrictions of the mobile subscribers. It also enables authentication of VLR by both mobile subscriber and HLR. Besides; easy, fast, and trusted key disabling can be obtained by a minor extension to our protocol.

As a final remark we would like to note that our protocol, although designed for GSM, is not a particularly specific to GSM and can easily be adopted to any other mobile protocol where a user device authenticates itself to its home server via a local base station.

References

[1] S.M. Bellovin and M. Meritt, "Encrypted Key Exchange: Password based protocols secure against dictionary attacks", in *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, May, 1992, pp.72-84.

[2] S.M. Bellovin and M. Meritt, "Augmented Encrypted Key Exchange: A password based protocol secure against dictionary attacks and password file compromise", Technical Report, *AT&T Bell Laboratories*, 1994

[3] ETSI/TC Recommendation GSM 03.20, *Security Related Network Function*, version 3.3.2,
January1991.

[4] L. Gong, T.M.A. Lomas, R.M. Needham, J.H. Saltzer, "Protecting poorly chosen secrets from guessing attacks", *IEEE Journal on Selected Areas in Communication*, Vol.11, No:5, June 1993, pp. 48-656.

[5] http://www.gsmworld.com/news/statistics/index.shtml

[6] Hung-Yu, Lein Harn and Vijay Kumar, "Authentication protocols in wireless communications", I*CAUTO' 95*.

[7] D. Jablon, "Strong password only authenticated key exchange", *ACM Computer Communications Review*, October 1996.

[8] S. Lucks, "Open Key Exchange: How to defeat dictionary attacks without encrypting public keys", *Proc. of the Security Protocols Workshop*, LNCS 1361. Springer-Verlag, Berlin, 1997.

[9] P. MacKenzie and M. K. Reiter. "Networked cryptographic devices resilient to capture", *International Journal of Information Security*, November 2003.

[10] R. Perlman and C. Kaufman, "PDM: A new strong password based protocol", *Proceedings of the 10th USENIX Security Symposium*, August 2001.

[11] M. Rahnema, "Overview of the GSM system and protocol architecture", *IEEE Communications Magazine* pp. 92-100, April 1993.

[12] T. Wu, "Secure remote password protocol", *Proceedings of the Internet Society Symposium on Network and Distributed System Security*, pp.97-111, 1998

[13] F.Zhu, D.S. Wong, A.H. Chan, R.Ye., "Password Authenticated Key Exchange based on RSA for Imbalanced Wireless Networks", ISC 2002, Sao Paolo, Brazil.

[14] KToolbar, A toolkit for J2ME, http://java.sun.com/j2me

[15] Lightweight Crypto API, Bouncy Castle, http://www.bouncycastle.org