Mobile Authentication Scheme Using SMS

Minglei Shu, Chengxiang Tan, and Haihang Wang
College of Electronics & Information Engineering, Tongji University, Shanghai, China, 201804
shuminglei@yahoo.com.cn , cxtan@trimps.ac.cn, wanghh@sh163.net

Abstract

Identity authentication is the first line of defense in the security application system to access the mobile network resources. However, as the means of attacking become variety, new requirements have been brought forward for the technology of identity authentication. To improve performance of mobile authentication, this paper presents a novel mobile authentication scheme, which transmits message encrypted with digital certificate to implement authentication between the mobile phone and the server. Theoretical analysis and experiments indicate the scheme satisfies security, non-repudiation and mutual authentication.

Keywords: Mobile Authentication, SMS, Non-repudiation, Mutual Authentication

1. Introduction

Accompany with the rapid growth of mobile technology, more and more mobile terminals, such as personal digital assistants (PDAs), smart phones, are used in our lives, and have brought huge convenience to us. At the same time, security problems also have been brought to our lives. These problems have hold back many potential applications of mobile technology. It will make great important significance for the development of mobile services to prevent the security risk.

Identity authentication is the first line of defense in the security application system to access the mobile network resources. It plays an important role in the mobile security area, because system provides the users that have passed through the identity authentication with corresponding application services. However, due to wireless network's feature of being open and the deficiencies of wireless protocol, more and more means of attack have been offered, it is easier to carry out malicious attacks of snooping, replay, disguise and so on[1]. Therefore it is an important and basic research topic to put forward efficient authentication scheme.

This paper presents a novel mobile authentication scheme to improve performance of mobile authentication. Our scheme transmits message encrypted with digital certificate to implement authentication between the mobile phone and the server. Short messaging service (SMS) messaging with digital signature can be used as a way to strongly authenticate a user and provide non-repudiation [2]. Moreover, at the end of the year of 2008 there will be almost 5 hundred million mobile phone users in China, the most part of which use smart phones, so it is completely feasible to apply the programs given by the paper.

The rest of this paper is structured as follows. In Section 2 previous proposed approaches are given, section 3 describes overview of our scheme, in section 4 authentication protocol using SMS of this paper is presented, section 5 shows comments of the scheme and implementation, finally conclusions are drawn in section 6.

2. Related work

Several studies of mobile authentication using SMS messages have been made. A protocol was described for mobile payment for vending machines in [2]. It uses the Public Key Infrastructure (PKI) provided by the Finnish Population Register Centre to encrypt messages, and then transmits messages between the two smart phones to mutually authenticate. The scheme must obtain the certificate from Finnish Electronic Identification via radio waves which may be insecurely, and the scheme also has a drawback about the timestamp.

A system to encrypt, send and receive text messages securely with a mobile phone was presented in [3]. The system uses one encryption based on symmetric algorithm and a shared secret password between the sender and the recipient.

A two-factor authentication scheme was proposed in [4]. It possesses a Bluetooth-enabled handheld device to enforce authentication based on weak

978-0-7695-3729-0/09 $25.00 © 2009 IEEE
DOI 10.1109/SSME.2009.43

credentials. The working prototype of its scheme is lacking so that the effective performance figures can not be obtained, and the security of its encryption scheme need further to be proven.

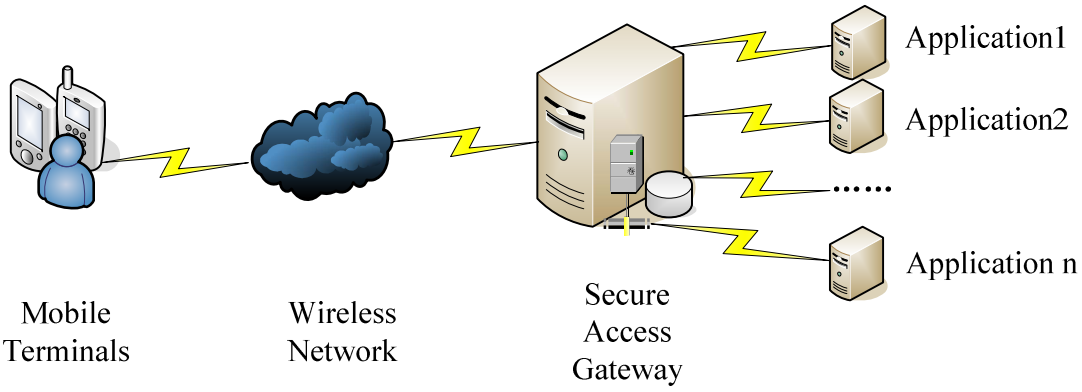

Figure 1. The topology of system

3. System overview

Our system mainly consists of two parts: mobile terminals and secure access gateway (GW). Figure 1 illustrates the topology of system.

Mobile terminals: they are the mobile devices which are computationally capable of running the programs. The programs may be software running in PDAs or smart phones, or as hardware integrated into SIM Tool Kit (STK).

Secure access gateway: It is consists of access authentication server and database management server. Authentication server makes sure that legitimate mobile terminals can access the system accurately. Database management server records the online state of mobile terminals, user information and authority certificate. The card holder's public keys and the GW's private key are stored in the database management server. Each terminal stores the private key of its own and the public key of the GW. In the ordinary course of event, the keys are fixed and unchanging. However, when we update the key of the gateway or a terminal, it must be finished via a secure channel.

After the success of authentication, special services, such as accessing the data of corporate LAN, surfing the internet, or carrying out commerce transactions, can be provided for mobile terminals.

4. Protocol for SMS authentication

The authentication is started by the terminal, and then GW and the terminal check the validation factor (VF) of each other. VF is a fixed-size one-way hash value produced by a hash function. Public key cryptography and symmetric key cryptography are used to encrypt or decrypt packets.

The Protocol's specific content is as follow, and it is also shown in figure 2:

1) The terminal generates one VF named Nc
2) The terminal encapsulates Nc with connection request message to produce SMS_AUTHENTICATION_REQ1, which will be sent later to GW to start authentication.
3) Once GW gets SMS_AUTHENTICATION_REQ1, the preliminary check will begin. The information, including mobile phone number, International Mobile Equipment Identity (IMEI) and the mobile phone's login status, is searched in the database. If the information is not stored in the database, or this terminal has logined, protocol will abort.
4) Secure access gateway generates one VF named Ns and one session key named Ks
5) Nc，Ns and Ks are signed using the private key of GW
6) The data of step 5 is encrypted using the mobile phone's public key recorded in database to produce SMS_AUTHENTICATION_ACK1, which will be sent later to mobile terminal
7) On receipt of SMS_AUTHENTICATION_ACK1, the terminal signs this message with the terminal's private key
8) The data of step 7 is decrypted using the public key of GW to obtain Nc', Ns and Ks
9) If Nc=Nc', the terminal encrypts Ns with key Ks to acquire SMS_AUTHENTICATION_REQ2, which will be sent later to GW. Otherwise the verification fails.
10) After receiving SMS_AUTHENTICATION_REQ2, GW decrypts the message to obtain Ns'.
11) If Ns= Ns', the verification succeed. Message of finishing authentication, called SMS_AUTHENTICATION_ACK2, is sent to the

terminal. Finally the login status is recorded in the database.

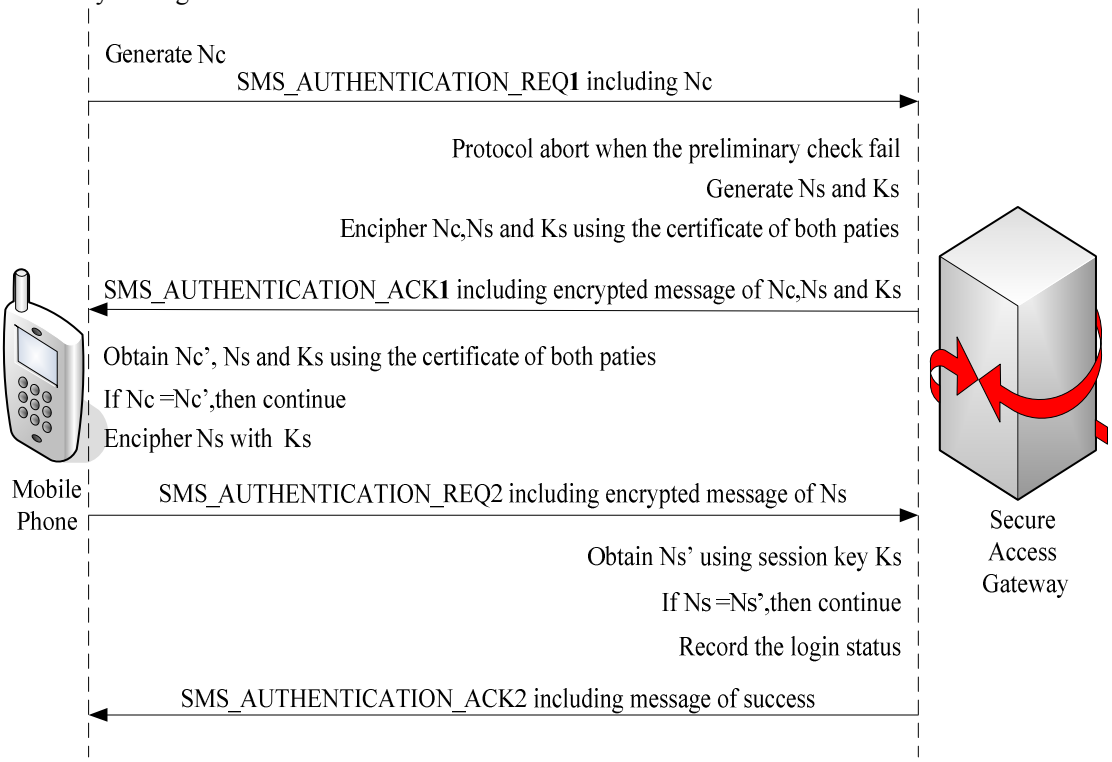

Figure 2. SMS authentication protocol

5. Security analysis and implementation

The scheme uses PKI technology based on digital certificate to verify identity. PKI can deliver solid end-to-end security across the networks, which ensure our scheme's safety [5]. Besides, the security of our scheme will be examined as follows.

1. The scheme introduces session key mechanism to achieve replay-attack resistance.

An eavesdropper may intercept the logon message from mobile terminal and replay them [6]. But according to the scheme, such messages from the eavesdropper will be abandoned as the rejected data, because the session keys Nc and Ns vary with the new authentication.

2. The scheme resists secret key guessing attack.

The hash function produces a fixed-size one-way hash value of one random number, and the hash value is used as VF. Obviously, it is too computationally intensive to crack hash algorithm.

3. The scheme resists reflection attack.

The attacker may capture the first request SMS_AUTHENTICATION_REQ1 and congest the line of the next authentication message from legitimate mobile terminals. Nevertheless, our scheme demands the private certificate of each other should be used to finish mutual authentication in the following steps, so the attacker can not be legitimate users in this way.

4. The scheme resists signer verification attack.

The attacker may verify the signature with public key, and if the signature passed the verification, it would make the leakage of mobile users' information, which is harmful to information security. In our scheme, MS_AUTHENTICATION_ACK1 is encrypted using the mobile phone's public key and signed using the private key of GW, that meanings the attacker can acquire nothing after capturing MS-_AUTHENTICATION_ACK1.

5. The scheme resists parallel session attack.

In our scheme, during the whole authentication process, the legality or authenticity is attested after each communication between mobile terminals and GW. The attacker can't obtain any information to counterfeit the GW or mobile terminals after session hijacking.

6. The scheme provides perfect non-repudiation.

The private key of terminal user is stored in the storage of terminal, and undoubtedly it is forbidden to keep a duplicate by others. Therefore, terminal user is the only one owning the private key. Surely it is the same with GW. That means non-repudiation can be provided perfectly.

7.The scheme can provide high security for communication after the successful authentication.

We can encrypt messages between mobile terminals and GW with session keys, which will be certain to thwart the replay attack because one session key only can be used at a time.

An application which implements our protocol has been developed. The hardware system of the application is a combination of smart phone with the feature of programmability, PC server used as secure access gateway and GSM modem. We chose Windows Server 2003 Enterprise Edition and Windows Mobile 5.0 as the operating systems, and used Java 2 Micro Edition (J2ME) as the programming platform. J2ME is a wonderful development platform for mobile applications. Within J2ME, Mobile Information Device Profile (MIDP) is defined as an industrial standard profile and can provide much technical support for mobile manufacturers [7].

The results of experiments indicate the scheme satisfies security, non-repudiation and bidirectional authentication, which accord with theoretical analysis.

6. Conclusions and future work

A mobile authentication scheme using SMS has been presented in this paper. The scheme uses PKI to provide bidirectional authentication and non-repudiation, uses session key to provide high security. We also developed an application to assess the scheme, and the results kept identical with our expectation.

Future work will focus on studying mobile authentication scheme using Multimedia Message Service (MMS). MMS will replace SMS totally, so it is significant to research how to use audio file or video file transmitted via radio waves to certify identity.

7. References

[1]G. Racherla, D. Saha, “Security and Privacy Issues in Wireless and Mobile Computing”, Proceedings of 2000 IEEE International Conference on Personal Wireless Communications, Dec 17-20, 2000, pp.509-513.

[2]H. Marko, H. Konstantin, “Strong Mobile Authentication”, Proceedings of 2nd International Symposium on Wireless Communication Systems, Sept 5-7 2005, pp.96-100.

[3]M. Hassinen, “SafeSMS - end-to-end encryption for SMS messages”, Proceedings of the 8th International Conference on Telecommunications, June 15-17, 2005, pp.359-365.

[4]D. P. Reberto, M. Gianluigi, A. S. Maurizio, “A Two-Factor Mobile Authentication Scheme for Secure Financial Transactions”, Proceedings of the International Conference on Mobile Business (ICMB’05), July 11-13, 2005, pp. 28-34.

[5] R. Perlman, “An Overview of PKI Trust Models”, IEEE Network, 1999, 13(6), pp. 38-43.

[6] S. Goel, R. Negi, “Secret Communication in Presence of Colluding Eavesdroppers”, Proceedings of Military Communications Conference 2005 (MILCOM 2005). Oct 17-20, 2005, pp.1501-1506.

[7]Sun Microsystems Inc: J2ME API Documentation. http: // java.sun.com/