http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (6): 1217-1221, 2010
ISSN 1812-5638

A Solution of Secure User-to-SP Messaging Using Identity-Based Cryptography

[1,2]Yu Dingguo, [3]Chen Nan and [1]Tan Chengxiang
[1]Department of Computer, Tongji University, Shanghai 201804, China
[2]School of Information, Shaoxin University, Shaoxin 312000, China
[3]School of Qianjiang, Hangzhou Normal University, Hangzhou 310012, China

Abstract: To exploit the popularity of SMS as a secure business bearer protocol and offer the security services such as confidentiality, integrity, authentication and non-repudiation. In this study, we propose a solution of secure user-to-SP messaging using Identity-Based Cryptography (IBC). It is an application layer protocol for mobile terminal and SP and a network independent solution. It does not need any change in the network's infrastructure and simultaneously provides some secure attributes. Since, it selects MSISDN numbers as identity and deploys elliptic curves and a symmetric encryption algorithm; it has great computational and storage advantages over the traditional Public Key Certificate (PKC) cryptography while simultaneously providing the most feasible security services. This solution will help commercial companies and government authorities, who need confidential information transmitted over the air, such as banks providing mobile bank service, policemen exchanging data of criminals, etc, to build secure SMS messaging.

Key words: Mobile telecommunication, Secure data communication, SMS, Public key cryptography, Elliptic curve cryptography

INTRODUCTION

Mobile telecommunication handsets and networks are developing rapidly in recent years. At the end of 2009, the worldwide number of mobile users was over 4.3 billion people (GSM World, 2010). Short Message Service (SMS) is a store-and-forward, easy to use and low cost service. While it is mainly used for the personal communications, it has also been used in applications where the other party is an information system, such as remote control of the apparatus (Werff *et al*., 2005), m-banking and m-payment (Dukić and Katić, 2005). It is popular used for data bearer/service within GSM, CDMA and other cellular networks and will be more popular in the future.

The GSM with the greatest worldwide number of users suffers from many security problems (Siddique and Amir, 2006). In the GSM, only the airway traffic between the Mobile Station (MS) and the Base Transceiver Station (BTS) is optionally encrypted with a weak and broken stream cipher (A5/1 or A5/2) (Toorani and Shirazi, 2008). The GSM network access security uses A3/A8 (COMP128 actually used in GPRS) authentication algorithm to authenticate each Subscriber Interface Module (SIM) card which attempts to connect to the GSM network and it depends on a shared secret key between SIM card and the GSM Authentication Center (AUC), the secret key is embedded into the SIM card during manufacture and it is also securely replicated into the AUC (Zhao *et al*., 2008). Transmission of the short messages between SMSC and phone is via the Signaling System Number 7 (SS7) within the GSM Mobile Application Part (MAP) framework. The problem with GSM MAP is that it is an unencrypted protocol allowing employees within the mobile operator's network that has access to SS7 network to eavesdrop or modify SMS messages (Hassinen, 2003). The SMS messaging has some extra security vulnerabilities due to its store-and forward feature and the problem of fake SMS that can be conducted via the Internet. When a user is roaming, the SMS content passes through different networks and perhaps the Internet that exposes it to various vulnerabilities and attacks (Toorani and Shirazi, 2008).

To exploit the popularity of SMS as a secure business bearer protocol, it is necessary to enhance its functionalities to offer the security services such as confidentiality, integrity, authentication and non-repudiation. However, such requirements are not provided by the traditional SMS messaging (Toorani and Shirazi, 2008).

In some literatures, most solutions use symmetric key cryptography or public key certificate cryptography to provide secure messaging. Toorani and Shirazi (2008) provided an elliptic curve-based public key solution to

Corresponding Author: Yu Dingguo, Department of Computer, Tongji University, No. 4800 Caoan Road, Shanghai, 201804, China

build secure application layer protocol as a secure bearer in the m-payment systems, but it has some disadvantages such as store, grant and maintenance of certificates. Zhao *et al*. (2008) proposed a solution for secure messaging channel using identity-based cryptography. It does not require a large storage on mobile terminal side and provides end-to-end security. But it is short of an availability authentication mechanism before exchanging secure message with each other. Croft and Olivier (2005) made use of an approximated one-time pad scheme to encrypt SMS messages between two mobile phones, it has limitation in this mechanism. It does not ensure end-to-end encryption because there is a decryption occurring within the mobile network so that another one-time pad can be created for the receiving phone to decrypt the message. Because the message is required to be decrypted within the mobile network, there is a dependency on the network infrastructure. Ratshinanga *et al.* (2004) proposed a secure SMS protocol which uses public and symmetric key cryptography and password authentication strategy. In terms of the cryptographic algorithms, they use 1024-bit RSA for the public key algorithm and 128 bit AES/CTR for symmetric key and block cipher mode algorithm and SHA-1 for the hash algorithm. It needs more computation on mobile terminal.

IDENTITY-BASED CRYPTOGRAPHY

Identity-based cryptography: Identity-Based Cryptography (IBC) is a form of public key cryptography for which the public key can be an arbitrary including email address, phone number and username. The concept was first introduced by Shamir (1984). The IBC can be classified into: Identity Based Encryption (IBE), Identity Based Signature (IBS) and Identity Based Authenticated Key Agreement protocol. After the concept was first suggested, IBS schemes were sooner founded, but IBE scheme remained a more challenging problem. Based on properties of pairings of a bilinear map on elliptic curves was suggested, which is the first fully functional, efficient and provably secure identity-based encryption scheme (Boneh and Franklin, 2001).

Nowadays most identity-based cryptosystems are built on Elliptic Curve Cryptography (EEC). Compared to RSA, EEC is more efficient in general. For example, Chang and Stebila (2002) showed that for a security level of 2048-bit RSA, ECC outperformed RSA in every aspects; for a security level of 1024-bit RSA, ECC outperformed RSA in scenarios such as in mobile telecommunication networks. Compared to traditional PKI, identity-based cryptography also saves storage and transmission of public keys and certificates, which is especially attractive for devices used in mobile telecommunication networks.

Bilinear pairings: A bilinear map is denoted $\hat{e}: G_1 \times G_1 \rightarrow G_2$ between two cyclic groups G_1, G_2 of order q for some large prime q, where G_1 is the group of points of an elliptic curve over F_p and G_2 is a subgroup of $F^*_{p^2}$. A cryptographic bilinear map utilizes its properties of bilinear, non-degeneration and computability (Dutta *et al*., 2004; Baek *et al*., 2004):

- **Bilinear:** $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for $P, Q \in G_1$and $a, b \in Z^*_q$
- **Non-degenerate:** $\hat{e}(P,P) \in F_{p^2}$ is an element of order q and in fact a generator of G_2. In other words, $\hat{e}\ (P, P) \in \neq 1$
- **Computable:** Given $P, Q \in G_1$ there is an efficient algorithm to compute $\hat{e}(P, Q)$

Why choosing identity-based cryptography: Basically, there are three alternatives to use for a solution of secure messaging system. Each of them has its advantages and disadvantages.

Symmetric key cryptography: The keys are short and the algorithms are highly efficient, these are particularly suitable for mobile devices. However, the SP needs to maintain n pairs of keys if there are n users. Each user needs to maintain a key with the SP.

Public Key Certificate (PKC) cryptography: Mature algorithms such as RSA exist for the PKC system and an infrastructure for grant and maintenance of certificates has come into existence. However, this cryptography requires much computational and storage resources to calculate and store public/private keys. A mobile device may not be able to provide the required services. Furthermore, the SP needs to maintain n certificates if there are n users. Each user needs to maintain a certificate of the SP.

Identity-Based Cryptography (IBC): The computational resource requirement is comparable to PKC for the same size of keys. However, it requires shorter keys to obtain the same security level as compared to the size of the key for traditional PKC cryptography. Moreover, it does not require extra transmission and storage of public keys. The SP needs to maintain n keys if there are n users. Each user needs to maintain nothing for the SP.

According to the analysis above, we can see that the PKC cryptography is not suitable for secure messaging, because of their much computational and storage resources to calculate and store public/private keys and the symmetric key cryptography is not suitable for it too, because it does not meet the secure requirement of integrity, authentication and non-repudiation etc. The advantage of identity-based cryptography is that there is no need to propagate public keys before communication and thus there is no need to store the keys as well. Therefore, we choose identity-based cryptography in present solution.

SOLUTION SYSTEM SETUP

Identity: In GSM, the primary user identity is the International Mobile Subscriber Identity (IMSI) number. Note that the IMSI number is not the subscriber number (the so-called MSISDN number). The MSISDN number is a telephone number with full international prefix and is associated with the IMSI number in the operative databases. The MSISDN numbers are public information, while the IMSI number is intended for the system's internal identification and routing purposes. Each SP has a unique short number that is publicly known to mobile users (Zhao *et al*., 2008). For a mobile user we choose his MSISDN (for a SP, we choose the short number) as the identity to be used in identity-based cryptography, because the receiver's number is known to the sender whenever sending a message to a receiver and the sender's number is known to a receiver whenever a message is received.

System parameters: In the identity-based cryptography, the user's public key is easily calculated from his identity, while a user's private key can be calculated for him by a trusted authority, called Private Key Generator (PKG). The identity-based cryptography needs a setup phase in which system parameters are built and distributed to its users. These parameters include system public key, master key, private key of each user and algorithms to be used for hash, encryption and decryption.

In the setup stage, the PKG specifies a group G_1 generated by $P \in G_1^*$ and the bilinear pairing ê: $G_1 \times G_1 \rightarrow G_2$. It also specifies hash functions $G:\{0,1\}^* \rightarrow G_1^*$ to map variable identity strings to points in G_1 and chooses hash functions H_1: $G_2 \rightarrow \{0, 1\}^l$, where l denotes the length of a plaintext and $H_2:\{0,1\}^* \times G_1 \rightarrow Z_q^*$. The PKG then picks a master key s umiformly at random from Z_q^* and computes a public key $P_{pub} = sP$. For a mobile user or SP, when they give their identity (MSISDN or a short number) string $ID \in \{0, 1\}^*$ to PKG, the cryptographic scheme builds an initial private key d_{ID} as $d_{ID} = sQ_{ID}$ where $Q_{ID} = G(ID)$. Then the mobile user or SP gets its private key d_{ID} and the system parameters paras = $(G_1, G_2, \hat{e}, l, P, P_{pub}, G, H_1, H_2)$ from the PKG (Fig. 1).

When user A sends a secure SMS message to user B (A or B can be the SP), it encrypts and authenticates the message as follows:

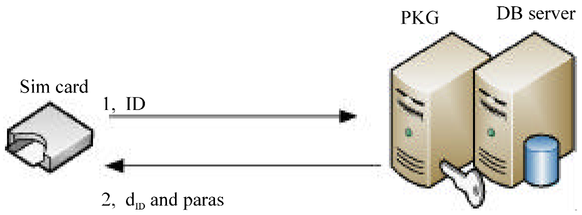

Fig. 1: Distribute private key and system parameters

- A first generates the public key Q_B of user B, $Q_B = G(ID_B)$, ID_B is the MSISDN or short number of user B
- A encrypts the message $M \in \{0, 1\}^l$ and outputs the cipher text C as $C = (U, V) = (rP, M \oplus H_1(\hat{e}(Q_B, P_{pub})^r))$, where r is chosen at random from Z_q^*
- A signs the message with its own private key d_A and outputs the signature S as: $S = (U; V) = (rQ_A, (r+H_2(C, U))d_A)$, where r is chosen at random from Z_q^* . The encrypted message C and signature S are put into the payload field of the SMS packet M' =<C, S>, then sending M' to receiver B

At the receiver B's side, the message is verified and decrypted as follows:

- B first generates the public key Q_A of user A, $Q_A = G(ID_A)$, the ID_A is the MSISDN or short number of sender derived from the packet header
- B verifies the validity of A's signature S = (U; V) by checking whether $\hat{e}(P,V) = \hat{e}(P_{pub}, U + H_2(C,U)Q_A)$. If so, the message is processed further, otherwise, discard the message
- For the received message C = (U; V), B decrypts it by computing $M = V \oplus H_1(\hat{e}(d_B, U))$, , d_B is a private key of user B

Implement and use of the system: We designed and implemented a secure user-to-SP SMS messaging system according to the solution for one police business information system in 2008 at Shanghai. The architecture of system as Fig. 2 shows. It includes secure mobile terminal, GSM modem, secure gateway, database server and application servers. The secure gateway sends or receives secure message from or to secure mobile terminal by using GSM modem.

The secure mobile terminal installed an add-on Message Management Toolkit which developed with Java 2 Micro Edition (J2ME). It includes user's private key, system parameters and some functions such as encryption, decryption, fragments and reassembles of messages and system setting etc. The Message

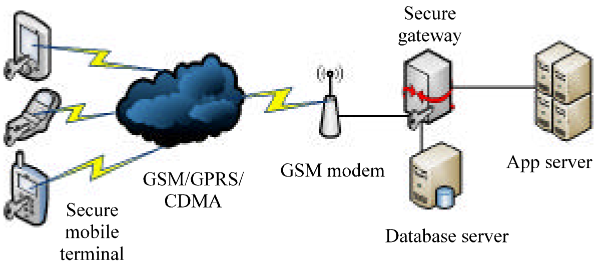

Fig. 2: The architecture of system

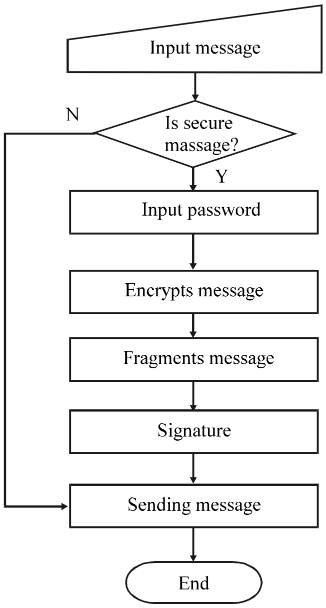

Fig. 3: The work flow of secure mobile terminal sending message

Management Toolkit does not change the traditional message input/output interfaces in the mobile terminal, but is built on top of them. It is like a new message management interface, where by the user receives and sends all messages. The user chooses an option to read or send a secure message or plain text message. On the SP side, a corresponding application runs on the secure gateway, the application encrypts all messages before sending to GSM modem and decrypts all messages coming from GSM modem. The secure gateway provides services to application servers by web services.

Figure 3 shows the work flow of the secure mobile terminal sending message. Figure 4 shows the work flow of the secure mobile terminal receiving message. On the SP side, the secure gateway has a corresponding work flow. In all this communication, the network operator has an access to only the encrypted text. Anyone who has intercepted the traffic, both from the air, or by getting into the network operators network, will also see only the encrypted messages and cannot get the clear text.

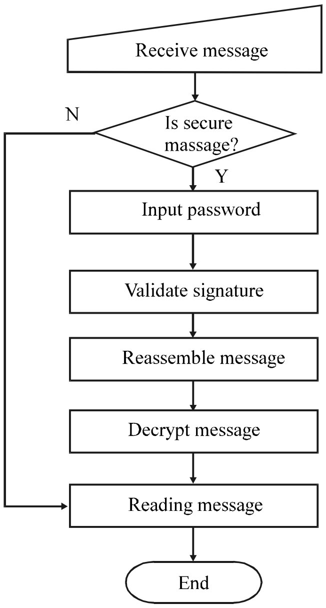

Fig. 4: The work flow of secure mobile terminal receiving message

DISCUSSION ABOUT SECURITY OF THIS SYSTEM

In present solution, it selects MSISDN numbers as identity and deploys elliptic curves and a symmetric encryption algorithm. It has great computational and storage advantages over the traditional Public Key Certificate (PKC) cryptography while simultaneously providing the most feasible security services such as confidentiality, integrity, authentication and non-repudiation, etc.

Hereunder, some security attributes of the solution are briefly described.

Confidentiality: The confidentiality is completely resided in the secrecy of session key since the system uses a strong block cipher. The session key differs for different sessions and is derived from the private keys of the participants. The Unknown Key-Share (UKS) attack is thwarted because the identifier of sender is involved in derivation of session key. There are only two ways to defeat the confidentiality: finding the private key of receiver, or having both of the private key of sender and randomly integer r. Deducing the corresponding r of R is generally in deposit of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) that is computationally infeasible with the chosen domain parameters.

Authentication: The implicit authentication is provided as the receiver verifies the signature.

Integrity: The hash value of message, concatenated with some variable parameters is involved in the signature generation. The integrity is guaranteed by the security attributes of the deployed hash function and also the unforgeability of the signature.

Non-repudiation and unforgeability: It is computationally infeasible to forge the signature of the sender without having her private key.

The solution provides confidentiality, authentication, integrity and non-repudiation, etc. security attributes. It effectively prevents the some attacks previously available on SMS such as identity impersonation, message forgery and tampering.

CONCLUSION

In this study, we present a solution to build secure communications channel for user-to-SP SMS messaging using identity-based cryptography and implement the system. This solution will help commercial companies and government authorities, who need confidential information transmitted over the air, such as banks providing mobile bank service, policemen exchanging data of criminals, etc., to build secure SMS messaging.

ACKNOWLEDGMENT

This study is supported by the National High Technology Research and Development Program of China (863 Program), No. 2006AA01Z438.

REFERENCES

Baek, J., J. Newmarch, R. Safavi-Naini and W. Susilo, 2004. A survey of identity-based cryptography. Proceedings of the 10th Annual Conference for Australian Unix Users Group, (AUUG'04), Springer-Verlag, pp: 95-102.

Boneh and Franklin, 2001. Identity-based encryption from the weil pairing. Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Aug. 19-23, Springer-Verlag, London, UK., pp: 213-219.

Chang, G. and Stebila, 2002. Performance analysis of elliptic curve cryptography for SSL. Proceedings of the ACM Workshop on Wireless Security, Sept. 28, ACM, New York, USA., pp: 87-94.

Croft, N. and M. Olivier, 2005. Using an approximated one-time pad to secure short messaging service (SMS). Proceedings of the Southern African Telecommunication Networks and Applications Conference, (SATNAC'05), Champagne Castle, South Africa, pp: 71-76.

Dukić, B. and M. Katić, 2005. m-Order-payment model via SMS within the m-banking. Proceedings of 27th IEEE International Conference on Information Technology Interfaces, June 20-23, ITI, pp: 93-98.

Dutta, R., R. Barua and P. Sarkar, 2004. Pairing-based cryptographic protocols: A survey. Cryptology ePrint Archive Report 2004/064, 2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.2043.

GSM World, 2010. Market data summary. http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm.

Hassinen, M., 2003. Secure SMS messaging using quasigroup. University of Kuopio, Finland, Tech. Report. http://www.cs.uku.fi/research/publications/reports/A-2003-1/page187.pdf.

Ratshinanga, H., J. Lo and J. Bishop, 2004. A security mechanism for secure SMS communication. Proceedings of South African Institute of Computer Scientists and Information Technologists, (SAICSIT'04), Computer Science Department, University of Pretoria, South Africa, pp: 736-744.

Shamir, A., 1984. Identity-based Cryptosystems and Signature Schemes. Lecture Notes Comput. Sci., 196: 47-53.

Siddique, S.M. and M. Amir, 2006. GSM security issues and challenges. Proceedings of the 7th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, July 19-20, IEEE Computer Society, Washington DC, USA., pp: 413-418.

Toorani, M. and A.A.B. Shirazi, 2008. SSMS-A secure SMS messaging protocol for the m-payment systems. Proceedings of Computers and Communications, July 6-9, Marrakech, pp: 700-705.

Werff, M.V., X. Gui and W.L. Xu, 2005. A mobile-based home automation system. Proceedings of 2nd IEEE International Conference on Mobile Technology, Nov. 15-17, Guangzhou, pp: 1-5.

Zhao, S., A. Aggarwal and S. Liu, 2008. Building secure user-to-user messaging in mobile telecommunication networks. Proceedings of Wireless Telecomunications Symposium, April 24-26, Pomona, CA, pp: 151-157.