http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

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

Information Technology Journal 6 (3): 435-440, 2007
ISSN 1812-5638
© 2007 Asian Network for Scientific Information

Identity Based Encryption Using mRSA in Electronic Transactions

[1]S. Rajalakshmi and [2]S.K. Srivatsa
[1]Department of Computer Science and Engineering,
Sri Chandrasekharendra Saraswathi Viswa Maha Vidyalaya,
(Deemed University), Enathur, Kanchipuram-631 561, Tamil Nadu, India
[2]Department of Electronics, Anna University, MIT Campus,
Chromepet, Chennai-600 040, Tamil Nadu, India

Abstract: This research studies the latest research concept in Computer Security namely Identity Based Cryptography. To start with, the paper gives an introduction to the concept called Identity Based Encryption with Mediated RSA and then applies this concept to do secure transactions through Internet. The research also highlights on the future work that can be carried over in this area.

Key words: Identity Based Encryption (IBE), Identity based cryptography with mediated RSA (IB-mRSA), Security Mediator (SEM), electronic transaction, Certifying Authority (CA)

INTRODUCTION

It was unanimously agreed in the cryptography community for a long time that the only way for two parties to establish secure communications was to first exchange a secret key of some kind. Using this secret key and an encryption algorithm, the sender encrypts the message. The receiver using the same secret key and the corresponding decryption algorithm decrypts the message. However, the Public Key Cryptography (PKC) Scheme introduced by Diffie and Hellman (1976) gave the concept that the sender and receiver need not use the same secret key for encryption and decryption. In fact, the sender uses a key called public key to encrypt and the receiver uses a different key called private key, for decryption. This concept revolutionized the cryptography research. This also introduced the concept of Digital Signature (Rivest *et al*., 1978). Though there are number of algorithms available to implement the PKC, the main problem lies in the distribution of the Public key. This is done by a Certification Authority (CA), which distributes the Public Key of a user in the form of a signed certificate. This leads to the issues of certificate management like revocation, distribution, storage and verification.

Identity Based Public Key Encryption is a solution to these problems. Identity Based Encryption is a scheme, in which, an entity's public key is derived directly from certain aspects of its identity, for example, an IP address belonging to a network host, or an e-mail address associated with a user.

In Shamir (1984) gave the concept of Identity Based Encryption (IBE). Shamir's original motivation for identity-based encryption was to simplify certificate management in e-mail systems. Xuhua Ding and Gene Tsudik have introduced a simple Identity Based Cryptography with Mediated RSA (IB-mRSA) (Ding and Tsudik, 2003). In this scheme, a simple identity based cryptosystem developed atop some Mediated RSA (mRSA) (Boneh *et al*., 2002) has been proposed. Mediated RSA is a practical and RSA compatible method of splitting an RSA private key between the user and a security mediator called a SEM. Neither the SEM nor the users know the factorization of the RSA modulus and neither can decrypt/ sign message without the other’s help. Built on top of mRSA, the IB-mRSA blends the features of identity based and mediated cryptography.

This study makes use of the IB-mRSA scheme to do electronic transaction (William Stallings, 2003) in a secure manner. Transactions over Internet have become a common feature now a day. However, the question remains how secure these transactions are. A solution to this has been proposed in this paper using the concept of IB-mRSA.

OVERVIEW OF IDENTITY BASED ENCRYPTION SCHEMES

Boneh and Franklin introduced Identity Based Encryption Schemes using Bilinear Pairing Scheme as a mathematical primitive (Boneh and Franklin, 2001). This

Corresponding Author: S. Rajalakshmi, 18B/10, Nagareeswarar Koil Street, Kanchipuram-631 502, Tamil Nadu, India
Tel: 91-44-67275543

followed Identity Based Signature scheme based on Bilinear Pairing by Cha and Chaeon (2003). These schemes use Private Key Generators (PKG) for generating the private keys based on the identity and hence have the problem called Key-Escrow Problem. That is, as the PKG issues the private key based on its master key, the PKG knows the private key and is able to decrypt or sign any message. To overcome this Key Escrow Problem, Boneh and Franklin, (2001) suggested that the master key may be distributed to number of PKGs and the user obtains the partial private keys from various PKGs and forms his/her whole private key. However, this multiple PKGs cause lot of communication and computational cost and hence are not desirable. Ding and Tsudik (2003) have introduced a simple Identity Based Cryptography with Mediated RSA (IB-mRSA) in which the Key Escrow Problem does not exist.

OVERVIEW OF IDENTITY BASED MEDIATED RSA (IB-mRSA)

Mediated RSA (mRSA) involves a special entity, called a SEM, which is an on-line partially trusted server. A user must obtain an identity-based token from the SEM. Without this token, the user cannot use his key to decrypt or sign a message. Revocation of keys can take place as in RSA. A single SEM serves many users. SEM's presence is invisible to other users. In signature mode, mRSA yields standard RSA signatures and in decryption mode, mRSA accepts plain RSA-encrypted messages. The main idea is to divide the RSA private key into two parts: one is given to the user and the other given to the SEM. The two parts of the keys are to be used to sign/decrypt the message. Also the key cannot be derived knowing the half key. In the IB-mRSA scheme proposed by Dan Boneh *et al.* (2002) the sender makes use of the public key derived from the receiver's identity.

IB-mRSA KEY GENERATION PROCESS

In the scheme given in IB-mRSA, the initialization phase sets up the RSA modulus for all users in the same system. A Certifying Authority CA does this. First, CA chooses, at random, two large primes p' and q' such that p = 2p'+1 and q = 2q'+1 are also prime. Then it computes n = p*q. There is a high probability that a randomly chosen number in Zn is relatively prime to $\phi(n)$. For any user X, the public exponent 'e' is constructed as the output of F (ID_x), where F is a mapping function. It is represented as a binary string of the same length as the RSA modulus with the least significant bit set. These ensure that 'e' is odd and, with overwhelming probability, relatively prime to $\phi(n)$. The private key 'd' is split into two between the user and the SEM.

ALGORITHM IB-mRSA KEY GENERATION (EXECUTED BY CA)

Suppose k (even) is the security parameter.

- Random k/2-bit primes: p'; q' are generated such that p = 2p' +1; q = 2q'+1 are also prime.
- $n \leftarrow pq$
- For each user X:

    - $k' \leftarrow k - | F(ID_x)| -1$
    - $e_x \leftarrow f(ID_x) = 0^{k'} || F(ID_x)|| 1$
    - $d_x \leftarrow 1/e_x \bmod \phi(n)$
    - $d_{x,u} \leftarrow^{r} Z_n - \{0\}$
    - $d_{x;sem} \leftarrow (d_x - d_{x,u}) \bmod \phi(n)$

Thus the CA sets up the public/private key-pair and commumicates $d_{x;sem}$ to the SEM and $d_{x,u}$ to the user. It also distributes the system-wide certificate, which contains along with usual fields the common modulus n. It will not contain the real public key. For the sake of compatibility with other RSA implementations including plain RSA and m-RSA, the CA may upon request issue an individual certificate to a user. The encryption is done as in plain RSA. To encrypt a message, the sender needs the recipient's identity such as email address and its organization certificate having common modulus n.

ALGORITHM FOR IB-mRSA ENCRYPTION

- e← IB- mRSA.key(recipient's identity)
- n is retrieved from organization certificate;
- Message m is encrypted using standard RSA encryption with (e; n) as the public key

The recipient's public key certificate is not required for the sender to encrypt.

Since the key is derived from the receiver's unique identifier, the sender does not need a certificate to ensure that the intended receiver is the correct public key holder. Furthermore, instantaneous revocation provided by mRSA obviates the need for the sender to perform any revocation checks.

ALGORITHM FOR IB-mRSA DECRYPTION

First step:

- USER: m' ←encrypted message
- USER: send m'to SEM

Second step:

- In parallel:
- SEM :

- If USER revoked return (ERROR)
- PDsem← $m'^{dx,sem}$ mod n
- Send PDsem to USER
- USER:
- PDu← $m'^{dx,u}$ mod n

Third step:

- USER: m← (PDsem * PDu) mod n
- USER: return (m)

Thus IB-mRSA provides identity-based encryption along with revocation. Also usage of mRSA decryption technique gives security to the message. Now we will see how this technique can be extended to electronic transactions.

OVERVIEW OF ELECTRONIC TRANSACTION

Whenever a customer tries to buy some product using his existing credit card or payment infrastructure in an open network such as Internet, he always encounters the problem of security. Secure communication must be ensured among all parties involved in the transaction. Privacy in the case of customer's payment card must be ensured. The scheme described here tries to solve this problem.

THE PARTICIPANTS IN THIS SCHEME ARE AS FOLLOWS

Purchaser: The purchaser or the consumer or the customer places the order through the Internet. He makes use of the payment card issued by various banks for payment.

Retailer: The retailer or the merchant sells goods or services to the consumer.

Issuer: This is a financial institution like a bank which provides the payment card to the purchaser

Payment bank: This is a financial institution with which the retailer establishes an account.

Security mediator (SEM): This is an online trusted server, which gives the identity-based security to the electronic transaction.

Certifying Authority (CA): The CA sets up public/private key-pair for all the users like merchants, banks and distributes the same to the SEM and users. It also issues the system-wide certificate, containing the common modulus n.

SECURITY ISSUES IN ELECTRONIC TRANSACTIONS

The purchaser gets the payment card issued by a bank. Then he goes through the Internet to purchase certain goods. Once he goes through various retailers' information, he decides on a particular retailer to place the order. He sends the order list to the retailer and after going through the order, the merchant accepts the order and sends an acknowledgment. Then the purchaser sends the information about the order placed by him along with the payment details to the merchant. However, the merchant should not get the credit card details of the purchaser, which is sent along the payment details. To make sure that the purchaser does not lie about the order, the order and the corresponding payment information are to be sent together. The security scheme takes care of the issue that, the merchant gets only the order information and the bank gets the payment information. The purchaser using the respective public keys of the merchant and the bank encrypts the order details and payment details. He then concatenates the two along with a random number and sends to the merchant. The merchant sends the same to the SEM. The SEM verifies the validity of the merchant and the bank. The SEM using the part of the private keys of the merchant and the bank decrypts the order details and payment details and sends them to the merchant and the bank, respectively. The merchant makes use of the part of his private key and decrypts the order details and uses it to get the order details along with the decrypted message received from the SEM. Similarly the bank gets the payment details after decrypting the payment details with partial private key and making use of the decrypted message from SEM. So the scheme takes care that the merchant gets the order details only and the bank gets the payment details only. Also they are sent together by the purchaser to avoid conflict. The scheme also uses the Identity based cryptography so that no third party is involved in generating the public keys. The actual working of the scheme is described below.

ELECTRONIC TRANSACTION USING IB-mRSA

Sequence of events: 1. The customer opens an account. The customer obtains a payment card through any bank that supports the Security Mediator.

The customer receives the keys: The public key e_c based on the identity of the customer and private key pairs $d_{c,u}$ and $d_{c,sem}$ are created by the certifying authority. The keys are distributed to the customer and SEM. The common modulus n is available with the certificate.

Merchants create web sites and have their own keys: The merchants interested in online sales create their web sites with details of goods/services to be sold. The certifying authority generates the private key pairs with the common modulus n using the identity of merchant and bank. The CA creates the private key pairs $d_{o,sem,}$ to be used by the SEM and $d_{o,u}$ by the merchant for retrieving the order details and $d_{p,sem,}$ to be used by the SEM and $d_{p,u}$ to be used by the bank for retrieving payment details.

The customer places the order: The customer goes through the merchant's web site to select items and determines the price. The customer then sends the list of items to be purchased to the merchant who in turn sends the order form containing the list, their price, total price and an order number (r).

The order and the payment details are sent: The customer creates the messages M_o containing the order detail and M_p containing the payment details to be sent to the merchant and bank after authentication and encryption and sends them together to the merchant.

The merchant requests payments authorization: The merchant sends the payment information to the payment bank, which verifies the customer and sends the authorization to the merchant.

The merchant confirms the order and delivers the goods: The merchant sends confirmation of the order to the customer and sends the delivery.

The merchant requests the payment: The merchant sends a request to the payment bank, which makes the payment with the help of the issuer.

IB-mRSA ELECTRONIC TRANSACTION PROTOCOL

The order and payment details are generated by the customer as M_o and M_p where $M_o \leftarrow od || r || R$ and $M_p \leftarrow pd || r || R$, R being a random number.

The customer creates hash of M o and M_p and signature as follows:

- Customer sends h_o =h (M_o) and h_p =h (M_p) to SEM

In parallel: SEM

- Checks for the validity of the customer.
- Calculates part of the signature Pcsemo = ($h_o{}^{dc,sem}$) mod n and sends it to the customer
- Calculates part of the signature Pcsemp = ($h_p{}^{dc,sem}$) mod n and sends it to the customer

Customer:

- Calculates part of the signature Pco = $h_o{}^{dc,u}$ mod n
- Calculates part of the signature Pcp = $h_p{}^{dc,u}$ mod n
- Calculates the signature S_o = (Pcsemo * Pco) mod n
- Calculates the signature S_p = (Pcsemp * Pcp) mod n

The customer obtains the IB- mRSA public keys $e_{o,}$ based on the merchant's identity and e_p, based on the on the bank's identity. The common modulus 'n' is retrieved from the organization certificate.

The customer encrypts the messages M_o to obtain M'_o using (e_o, n) as public key and M_p to obtain M'_p using (e_p, n) as the public key with Standard RSA algorithm. The encrypted messages M'_o and M'_p concatenated with S_o and S_p respectively for verification are sent to the merchant.

The merchant takes up the messages and performs the following:

- Merchant gets the encrypted messages M'_o and M'_p and S_o and S_p
- Merchant sends M'_o and M'_p to SEM
- Merchant sends M'_p to the bank along with S_p

In parallel: SEM

- Checks for the validity of the Merchant and Bank
- Calculates Pdsemo = ($M'_o{}^{do,sem}$)mod n and sends it to the merchant
- Calculates Pdsemp = ($M'_p{}^{dp,sem}$)mod n and sends it to the bank

Merchant:

- Calculates Pdo = $M'_o{}^{do,u}$ mod n
- Calculates M_o = (Pdsemo * Pdo) mod n
- Calculates h_o =h (M_o)
- Decrypts the signature S_o with the public key of the customer $e_c \leftarrow$ IB- mRSA.key(customer's identity) and standard RSA decryption and compares it with $h_{o.}$

Bank:

- Calculates Pdp = $M'_p{}^{dp,u}$ mod n
- Calculates M_p = (Pdsemp * Pdp) mod n
- Calculates h_p =h (M_p)
- Decrypts the signature S_p with the public key of the customer $e_c \leftarrow$IB- mRSA.key(customer's identity) and standard RSA decryption and compares it with h_p

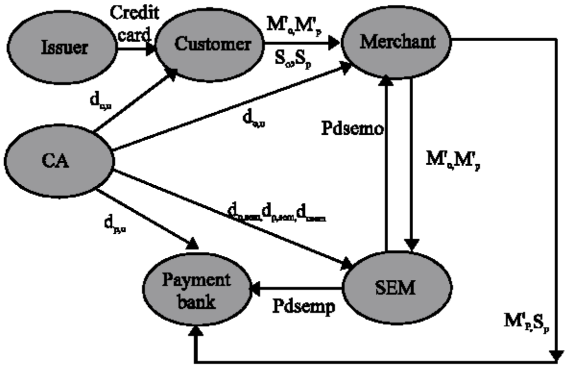

Fig. 1: IB-mRSA secure electronic transaction-protocol overview

Thus, the merchant, bank and SEM together check for the authentication of the customer and get the required messages after decryption. The merchant and the bank verify the signature of the customer on the order and payment details.

The merchant sends the goods/services to the customer and the customer acknowledges with the transaction id with a signature as above. Then the merchant sends this acknowledgment along with a capture request consisting of payment amount and transaction id to the payment bank.

The bank verifies the signature of the customer and matches the transaction id with the earlier message. Then the payment is made to the merchant.

Thus, the customer sends the encrypted order details and payment details along with the corresponding signed messages. The merchant decrypts the order details and verifies the signature for the same (Fig. 1).

The bank decrypts the payments details and verifies the signature for the same. The order details are not known to the bank and payment details are not known to the merchant. The two are sent together to avoid any confusion regarding the order and payment combination. The Security Mediator takes care of the payment through the payment bank to the merchant once the order is released. Also, the SEM authenticates the customer as well as the merchant.

SECURITY ANALYSIS IN ELECTRONIC TRANSACTIONS USING IB-mRSA

The security issues are resolved as follows:

- Integrity-the contents are encrypted with the corresponding public keys of merchant and bank and hence it is ensured that they reach the concerned people as sent. The random number R generated by the customer and the transaction id generated by the merchant accompany the messages. The merchant/bank can check the random number and transaction id after decryption and if there is any modification, the sender can be alerted.
- Authenticity-the customer sends the message with a signature signed using its private key along with the SEM, which authenticates the customer. If the customer is revoked, then the SEM gives an error message. The merchant and bank decrypt the signed messages using the corresponding public keys. By this, the customer authenticates himself to the merchant and bank. The merchant sends the goods/services to the customer and the merchant receives the signed acknowledgment of the customer. This acknowledgment is again verified by the merchant and bank for authenticity.
- Confidentiality-the message is encrypted using IB-mRSA method and hence is kept secret. The content of the message is decrypted together with SEM and the merchant and hence is meaningless to anyone other than the sender and receiver.

CONCLUSIONS

The purchaser gets the payment card issued by a bank. Then he goes through the Internet to purchase certain goods. Once he goes through various merchants' information, he decides on a particular merchant to place the order. He sends the order list to the merchant and after going through the order, the merchant accepts the order and sends an acknowledgment. Then the purchaser sends the information about the order placed by him along with the payment details to the merchant. However, the merchant should not get the credit card details, of the purchaser, which is sent along the payment details. To make sure that the purchaser does not lie about the order, the order and the corresponding payment information are to be sent together. The security scheme takes care of the issue that, the merchant gets only the order information and the bank gets only the payment information. The purchaser using the respective public keys of the merchant and the bank encrypts the order details and payment details. He then concatenates the two along with a random number and sends to the merchant. The merchant sends the same to the SEM. The SEM verifies the validity of the merchant and the bank. The SEM using the part of the private keys of the merchant and the bank decrypts the order details and payment details and sends them to the merchant and the bank, respectively. The merchant makes use of the part of his private key and decrypts the order details and uses it to get the order details along with the decrypted message received from the SEM. Similarly, the bank gets the payment details afters decrypting the payment details with partial private key and making use of the decrypted message from SEM. So, the scheme takes care that the merchant gets the order details only and the bank gets the payment details only. Also, they are sent together by the purchaser to avoid conflict. The scheme also uses the Identity based cryptography so that no third party is involved in generating the public keys.

REFERENCES

Boneh, D. and M. Franklin, 2001. Identity based encryption from weil pairing, proceedings of advances in cryptology-Crypto2001 LNCS (lecture notes in computer science) Intel. Assoc. Cryptologic Res. Springer-Verlag, 2001, pp: 2139: 213-229.

Boneh, D., X. Ding and G. Tsudik, 2002. Identity-Based Encryption using Mediated RSA, in The 3rd Workshop on Information Security Applications, Jeju Island, Korea, Aug.,

Cha, J.C. and J.H. Cheon, 2003. An Identity-based Signature from Gap Diffie-hellman Groups, Public Key Cryptography- Proceedings of PKC 2003, Springer-Verlag, LNCS., 2567: 18-30.

Ding, X. and G. Tsudik Simple Identity Based Cryptography with Mediated RSA in the Cryptographer's Track RSA Conference, 2003.

Diffie, W. and M. Hellman, 1976. New Directions in Cryptography, IEEE Transactions on Information Theory, pp: 22: 644-654.

Rivest, R.L., A. Shamir and L.M. Adleman, 1978. A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Communications of the ACM., pp: 21: 120-126.

Shamir, A., Identity Based Cryptosystems and Signature Schemes, Proceedings of Advances in Cryptology –Crypto 84, LNCS, Springer-Verlang, 1984, pp: 196: 47-53.

Stallings, W., 2003. Cryptography and Network Security Principles and Practice, Prentice-Hall of India Private Limited, 3rd Edn.