ISSN 2319 - 6629

Volume 1, No.1, August- September 2012

International Journal of Wireless Communications and Networking Technologies

Available Online at http://warse.org/pdfs/ijwcnt01112012.pdf

A Secure Email System Based on Identity Based Encryption

Suresh Kumar B.[1], **Jagathy Raj V. P.** [2]

[1],Sree Chitra Thirunal Institute for Medical Sciences and Technology, Thiruvananthapuram, India,
suresh@sctimst.ac.in

[2] School of Management Studies, Cochin University of Science and Technology, Kochi, India,
jagathy@cusat.ac.in

ABSTRACT

Now a days, email has become the most widely communication way in daily life. The main reason for using email is probably because of the convenience and speed in which it can be transmitted irrespective of geographical distances. To improve security and efficiency of email system, most of the email system adopt PKI and IBE encryption schemes. However, both PKI and IBE encryption schemes have their own shortcomings and consequently bring security issues to email systems. This paper proposes a new secure email system based on IBE which combines finger print authentication and proxy service for encryption and decryption.

Keywords : IBE, Secure Email System, Fingure Print Authentication

1. INTRODUCTION

With rapid developments in communication technologies based on computer and internet, communications via emails has become more and more widespread. However, traditional email protocol is insecure since the message is transmitted in plain text. If someone wants to interpret, copy or even alter emails, they can do it with relative ease. Individual privacies such as bank transactions, commercial secrets, even countries intelligence information are being delivered through emails and thus contents of emails are now more valuable than ever. Therefore, the security of emails has raised more concerns. The secure messaging system has three benefits: keeping sensitive information private, preventing anyone from tampering with the contents of the message and authenticating the identity of both the message sender and receiver.

Recently, many secure email systems are brought out and most of these systems are based on Public Key Infrastructure (PKI) or Identity Based Encryption (IBE) [1], [2]. Most popular systems using these technologies are S/MIME [3] and PGP [4]. Implementing PKI or IBE based on cryptographic system are facing a challenge of lacking the exact connection between cryptographic key and legitimate users. In PKI scheme, certificates are not easily located; there needs strict online requirement; validating policy is time-consuming and difficult to administer; certificate leaking issues and difficulty in exchanging keys. In IBE system, it is difficult to prove self-identity to Private Key Generator (PKG) and authenticate email sender's identity.

In this paper proposes a novel security system using proxy system [5], IBE and biometric [6] authentication. It needs no public key management and proxy service can automatically decrypt encrypted mails. If only email ID is used for IBE encryption, the decryption private keys can be requested on demand by proxy if biometric verification is already done to prove user's identity.

Biometrics, which refers to distinctive physiological and behavioral characteristics of human being, is more reliable means of authentication than traditional password or token based system. Finger print is the most widely used biometrics because of its uniqueness and immutability.

The rest of the paper is organized as follows. At first IBE system is introduced. Then the proposed system is introduced. At last, security of the proposed system is analyzed.

2. IDENTITY BASED CRYPTOGRAPHY

2.1 Identity-based Encryption Backgrounds

The idea of identity based public key scheme was proposed by Adi Shamir in 1984[1]. The purpose of IBE is to reduce the cost of public key certificate management. Instead of generating and using public/private key pair in a public key crypto system such as RSA, Shamir conceived the idea of using a user's name or email address as a public key, with the corresponding private key is generated by a trusted key generating center or Private Key Generator (PKG). Since users public key is based on some publically available information, that uniquely represents the user, an identity based crypto system can do away with public key directory maintenance and certificate management. In 2001, Boneh and Franklin[7] presented the first practical and secure IBE solution. It strengthened the IBE research rhythm again.

2.2 Identity-based Encryption - Mathematical Backgrounds

Let G1 and G2 be two groups of order q for some large prime q. The IBE system makes use of a bilinear map $\hat{e}$: G1 × G1 → G2 between these two groups. The map must satisfy the following properties:

1. *Bilinear*: A map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is *bilinear* if $\hat{e}\,(aP, bQ) = \hat{e}\,(P,Q)^{ab}$ for all $P,Q \in G_1$

and all $a; b \in Z$.

2. Non-degenerate: The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2. Since G_1, G_2 are groups of prime order this implies that if P is a generator of G_1 then $\hat{e}\,(P, P)$ is a generator of G_2.

3. Computable: There is an efficient algorithm to compute $\hat{e}\,(P,Q)$ for any $P,Q \in G_1$.

A bilinear map satisfying the three properties above is said to be an admissible bilinear map.

Bilinear Diffie-Hellman Assumption :- On a bilinear pairing $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$, the BDH Problem is that given $<P,aP,bP,cP>$ where $a,b,c \in Zq^*$, computing $\hat{e}(P, P)^{abc}$ is a NP hard problem.

The master key s and public parameter P are generated by the Private Key Generator Center (PKG) when the IBE system initialized. Multiplicative point sP could be published because that given sP and P, the master key s can not be deduced under the BDH problem assumption.

Suppose user A wants to send a message to user B, A selects a random r, computes a session key k using the following bilinear paring:

$$k = pair\ (r\bullet ID_B,\ s\bullet P)$$

A uses k to encrypt the message m, and sends to B as well as $r\bullet P$.

While receiving, the user B reconstructs the session key k using his private key $s\bullet ID_B$ and $r\bullet P$ from A, with the following bilinear pairing:

$$k = pair(\ s\bullet ID_B,\ r\bullet P)$$

B uses k to decrypt the received encrypted message to get the original message m.

If the email address of users are mapped into public points using Hash functions, identification of user is by the biometric way, and the email server acts as the PKG to manage master key, then the proxy based secure email system using IBE can be easily developed.

3. SYSTEM DESIGN AND IMPLEMENTATION OF PROPOSED SECURE EMAIL SYSTEM

An IBE based secure email system is proposed with the architecture illustrated in Figure 1.

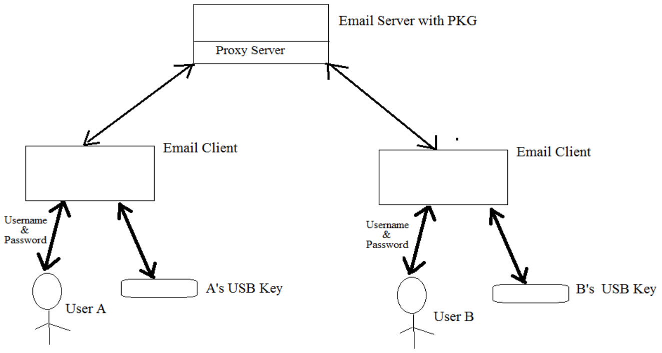

Figure. 1: Architecture of Secure email system

The USB key has fingerprint sensor and USB token. This device is able to capture fingerprint image. The email client software compares the finger print captured with the image already stored in the PKG system during authentication. If authentication is successful, email client communicates with the proxy service, which is an interface between email client and combined system of PKG and email server. The proxy service will handle all encryption and decryption services.

The sender and receiver are both the registered users in the

system. They can transparently send and receive encrypted emails by the proxy service. The work flow of the proposed system for two users distributed in two different secure domains is shown below.

(1) Alice in domain A composes a new email to Bob in domain B.

(2) The proxy service generates a random but secure key K for email contents symmetric encryption. It requests an IBE public key for the receiver's email address as its identity and uses it to encrypt the encryption key, forming a digital encapsulation for each email.

(3) The encapsulated secure email is sent over the network to the destination email server as normal email delivery and stores the message in the encrypted form in domain B.

(4) When the receiver (Bob) access his email using email client by authenticating user name, password and USB key, the proxy service in the domain B will requests for Bob's private key from PKG using the credentials it holds to authenticate. Once getting the private key from PKG over secure channel, such as SSL, the proxy can finally decrypt the email automatically and pass the decrypted message to the email client.

(4) Eventually Bob can read the email online in domain B using email client, without need to know and do anything about encryption operations.

There are 5 key modules designed for the system. The main functions of each module are described as follows:

A. Security System Setup

To initialize the system, establishing communicatiod)with email server and issue IBE related public parameters including Hash function manage master key, key generation, storage, update, backup, restore etc.

B. User Management

To provide management services for user registration, authentication, updation etc. Assume user *A* wants to send a email to user B. User *A* should register at PKG. PKG writes public parameters and *A*'s personal parameters in *A*'s USB key. While registration, PKG system verifies user's identity by inspecting documents such as passport, driving license etc. which can prove his real identity. Then PKG system captures *A*'s finger print, collect relevant personal public parameters etc. The finger print is transformed to finger print templates and store in PKG system and USB key along with personal public parameters.

C. Email Secure Agent (Proxy service)

This communicates between PKG system and Email server. This agent encrypt/decrypt email content, request PKG for private keys on behalf of email server/client.

D. PKG Management

To manage private key request, response and update, securely distribute private keys by communicating to USB keys using Email Client and verify private key with the details available in PKG database and USB key while authentication.

E. Email Client

Email client is a software module of the proposed system and manipulated by user directly. The various sub functions of email client are local login authentication, initiate encryption/decryption(request to proxy service), inter-communication with USB-key and PKG system. When a user wants to login the email client, he needs to pass the local authentication such as username and password with his USB key. Email client authenticates the user's legitimacy by comparing fingerprint template stored in USB key, currently acquired image of user's fingerprint and if PKG system is currently available online, then the fingerprint stored in PKG is also taken. If one user does not have USB key or the USB key does not belong to him, he will be rejected by the email client system.

4. OPERATION

For illustrating the operation of the proposed system, we propose the following steps.

a) User *A* register at PKG system and obtain his USB-key-A.

b) User *A* uses USB-key-A along with his username and password to login in the email client system, compose email, and sends the email via internet.

c) User *B* register at PKG and obtain his USB-key-B.

d) User *B* receives the email from email server via internet. The email client will notice B that a new mail arrived. Then email client will verify the USB key finger print, user authentication such as username and password by communicating with PKG system. If proper authentication is done, then email client communicates with proxy server for decrypting the email content on the fly while retrieving email from the email server.

5. SECURITY DISCUSSION

By using the proposed system, it is very easy to find the proper user identity by using USB key and is very secure. It is also possible to verify the identity of sender by contacting to PKG as email client automatically sends user's identification data to PKG.

6. CONCLUSION

In this paper, we presented a secure email system based on IBE, proxy service and fingerprint authentication. Email proxy provides online service, doing email encryption/decryption on behalf of registered users. In the system, we use USB key to keep secret data and help completing the relevant encryption process. The USB key can only be used by its legitimate owner. Thus the system ensures proper authentication with legitimate users.

REFERENCES

1. Shamir A. **Identity based cryptosystems and signature schemes**. Advances in cryptology, Springer, Lecture Notes in Computer Science, Volume 196/1985, pp. 47-53, 1985.
2. S. Chatterjee and P. Sarkar. **Identity-Based Encryption**, Springer Science+Business Media, LLC 2011
3. *S/MIME version 3 message specification*, RFC2633
4. *Open PGP Message format*, RFC2240.
5. Zhe Wu, Jie Tian, Liang Li, Cai-ping Jiang and Xin Yang. **A Secure Email System Based on Fingerprint Authentication Scheme,** Intelligence and Security Informatics, pp. 250 – 253, 2007
6. Tieming Chen and Shilong Ma. **A Secure Email Encryption Proxy Based on Identity-Based Cryptography**, Proceeding of IEEE, 284-286, 2008
7. Franklin M. and Boneh D. **Identity based Encryption from the Weil,** Journal of Computing, 32(3):586-615,2003.