I J C T A, 9(26) 2016, pp. 267-273

A Study of Secured E-Mail Security System Using Certificateless Cryptography and Domain Name System

A. Joseph Amalraj[1] and J. John Raybin Jose[2]

ABSTRACT

Email security is the most challenging aspect in the internet world. Email security plays an important role to provide the security to email event. To improve security and efficiency, most email system adopt Public Key Infrastructure (PKI) as the mechanism to implement security, but public key infrastructure based systems suffer from expensive certificate management and problems in scalability. This paper proposes an implementation of a practical, secure email system based on certificateless cryptography, which uses Domain Name System (DNS). Identity Based Cryptography (IBC) is another method. The main objective of this approach is awareness of email security and its requirements to the common computer users. A number of cryptographic techniques are developed for achieving secure communication. The proposed mailing system is secure against standard security model.

Keywords: Encryption, Decryption, Computer Security, Cryptography, Certificate-less cryptography, Domain name system, Identity based cryptography, Multi-factor authentication, Public key infrastructure, Securing Data, Hacking.

1. INTRODUCTION

Cryptography plays a major role in a science of secret writing. It is the art of protecting information by transforming and technology application. The main reason for using email is probably the convenience and speed with which it can be transmitted, irrespective of geographical distance. Now a day's our entire globe is depending on internet and its application to protecting national security. Cryptography is used to ensure that the contents of a message are very confidentiality transmitted and would not be altered.

Cryptography provides number of security goals to ensure of privacy of data, on-alteration of data and so on. The idea of encryption and encryption algorithm by which we can encode our data in secret code and not to be able readable by hackers or unauthorized person even it is hacked. The main reason for not using encryption in email communications is that current email encryption solutions and hard key management.

This paper proposes a secured email system in an open standard as an alternative technology for eliminating the problems with PKI and identity-based cryptographic mailing systems [4, 16]. This system key details and multi-factor user authentication for secure user authentication with the system.

Related works on existing email security systems and an introduction to certificate-less cryptography are described in Part 2. Part 3 describe the design of the proposed system. Part 4 describes the implementation of the system. The security features of the paper are described in Part 5. Finally, conclusions are given in Part 6.

[1] Research Scholar, Computer Science, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India. *E-mail: softwarejoseph@gmail.com*

[2] Professor & Head, Department of Information Technology, Bishop Heber College, Tiruchirapalli, Tamil Nadu, India. *E-mail: johnraybinjose@gmail.com*

2. LITERATURE REVIEW

2.1 Secure Email Security Systems

Email security systems are based on Identity-Based Cryptography/Public Key Infrastructure schemes [8, 9]. The mentioned security functions are implemented by these methods, of which the most important ones are S/MIME and PGP [3] uses hash functions and public key encryption algorithms; for example RSA and MD5 algorithm to enable encryption for content-protection and digital signature for non-repudiation. RSA [12] public keys are attached as PGP certificates along with the message. This trust mode of PGP is only suitable for small-scale groups and is not suitable for large-scale groups or user environments. Due to the difficulty of certificate management in PKI and S/MIME cannot ignore tedious operations, such as certificate revocation, verification, and so on. This result is lower efficiency compared with Elliptic Curve Cryptography (ECC) [2, 14] with the same level of security. The scheme also suffers from the problem of key escrow, where a central trusted authority issues a private key to a user. Because a central authority is responsible for private key generation, it is able to work as an authorized user and could maliciously decipher the incoming encrypted text or generate false signatures. They classified into two groups based on the private key generation technique

(i) Multiple authority approach and

(ii) User chosen secret key information approach.

The secret key exchange protocol based system is also not suited for email systems because a receiver of the email system may not always be online.

Domain Keys Identified Mail (DKIM) [10] permits users to claim some responsibility for a message by associating it with a domain name that they are authorized to use. This claim is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. A new concept called Lightweight Signatures for Email (LES) [1], proposed by Ben Adida, David Chau, Susan, is an extension to DKIM. The scheme described as "An End-to-End Secure Mail System Based on Certificateless Cryptography in the Standard Security Model" [17] based on of Certificateless Public Key Cryptography (CL-PKC) [18]. Therefore, efficient email security systems are in great need. This paper proposes a secure email system using certificateless cryptography as an alternative technology for eliminating the problems with Public Key Infrastructure and Identity Based Cryptography based mailing systems.

2.2 Certificateless Public Key Cryptography

The concept of Certificateless Public Key Cryptography (CL-PKC) is introduced by Al-Riyami and Paterson [18] in 2003, to overcome the key escrow problem of Identity Based Cryptography. In CL-PKC, a trusted

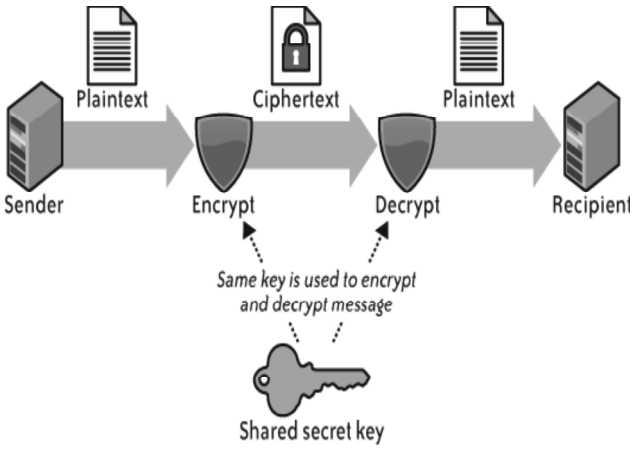

Figure 1: Secret Key Cryptography

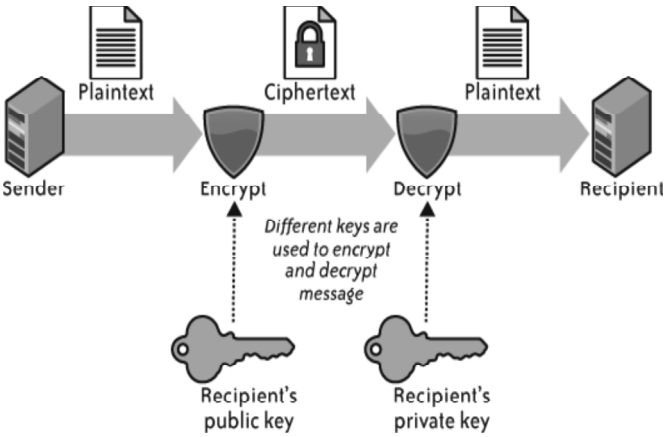

Figure 2: Public Key Cryptography

third party, called the Key Generation Center (KGC), supplies a user with partial private key. While compared to identity based public key cryptography (IDPKC), the trust assumptions regarding the trusted third party in this scheme are significantly reduced. Using this scheme, the replacement of a public key of a user in the system by the KGC is equivalent to certificate by PKI system.

3. SYSTEM DESIGN

The proposed secure email system should securely exchange email messages, easy to use and make use of the existing secure email standards, and it should be applied without making significant changes to email communication system.

- The first question to be answered is whether to apply security to both the email client and server, or just one of them. Any change in the email servers is not recommended, since this implies that all the email servers around the world should be updated to implement the new change.
- The analysis of the current encryption schemes shows that different aspects of the key distribution technology have related directly to the digital certificates management complexity.
- Thus, CLPKC represents an excellent replacement to the existing email security technology and it will be adopted in the design of this system.

3.1 Building Blocks

A user public key issue server issues public keys for users. The functionality of the user public key issue service may be implemented as part of the KGC server for small user base domains. During the user registration phase, the system asks for an email address system and a password and a secret value. To keep the secret value with the safer and we propose a usb security key token to store the secret with password protection.

Multi-factor authentication is now a requirement for effective secure authentication. Multi-factor authentication is commonly mentioned as (*e.g:* Password, PIN No, ATM Card, Smart Card, Security Token, Biometric materials such as fingerprint, palm pattern lock)

For an efficient security system, it is recommended to use “authentication methods that depend on more than one” (*i.e*. “Multi-factor” authentication). Biometric, which refers to physiological and behavioral characteristics of human beings because of its uniqueness and immutability. For the fingerprint system the user has to be enrolled with the user public key server authentication to verify the current captured image with the previously recorded fingerprint.

3.2 User Public-Key Distribution

Domain Name System has been proposed as a public-key infrastructure with Domain Key Identified Mail (DKIM) [2] by the Internet Engineering Task Force (IETF). In the DKIM reserves the domain key for every domain with an MX record. Our proposed system uses the same technique as in DKIM for specifying the address of the user public key issue server of the domain.

3.3 Domain Set Up

In the basic domain setup with email address alice@a.com, will obtain her partial secret key from a key server to her domain a.com. The detailed setup procedure of the domain is defined as follows and Figure 3 shows the domain setup.

- Choose an identity-based signature scheme from the various schemes.
- Generate a master key pair for this scheme.

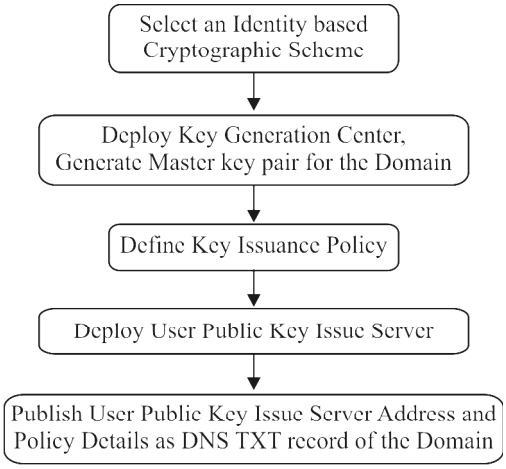

Figure 3: The domain setup

- Define key issuance policy for the system.
- Publish the user public key issue server details and policy as a DNS TXT record corresponding the MX record for a.com

3.4 Domain Policies

Domain policies decides to deploy an email security system, it simply needs to create a key server and a user public key distribution server for the domain and specify this server address in the appropriate DNS record. Policy determines the domain's requirements on its email users as well as its guarantees to any recipients. Three external sign policy values are used as below.

None

Person may sign emails. If the signature and verification fails, no warning header will be added by the recipient email signature verification system.

Basic

Person may sign emails with key issued by this key server. If the signature and verification fails, a warning header will be added by the recipient email signature verification system.

Strong

Person are required to sign all of their emails with a key issued by this domain. The message will be rejected if verification fails.

3.5 The Proposed System

The working of the security functionality is based on how the internal and external domain policies are specified for the domain. Figure 4 explain basic operation of the security functionality is as follows.

Signing Method

1. Request a partial private key from the KGC to generate the private key for client.
2. Sign the encrypted mail along with the fields FROM, TO, SUBJECT, TIMESTAMP to produce the signature using client private key.
3. The timestamp used in the signature in SMTP and email client sends email using SMTP.

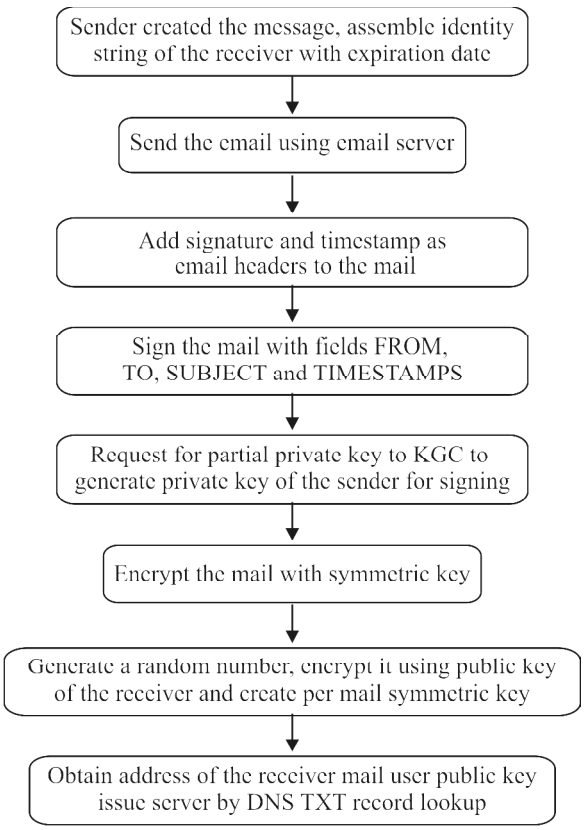

Figure 4: Sending secure mail

Signature Verification Method

Figure 5 explain the steps involved in receiving the secure mail. They are,

1. Download the secure mail from the mail server to the Email client.
2. Obtain the address of the User Public Key issue server for the domain a.com, by DNS TXT record lookup.
3. Recreate the message M that was signed, using the declared FROM, TO, SUBJECT fields the email body and the TIMESTAMP is declared.

4. IMPLEMENTATION OF THE PROPOSED SECURE EMAIL SYSTEM

The prototype system was developed using the C++ programming language. To implement the IBC protocol, there is a need for a cryptographic library that can provide both

Elliptic Curve Cryptography (ECC) and bilinear pairing functions. All of the basic encryption functions, such as setup, extract, encrypt and decrypt functions, were developed using the C++ language. Security services for the email client were implemented as an extension to the Mozilla email client using Javascript and the C++ library.

5. RESULTS AND DISCUSSION

The proposed system is secure against the standard security model because it is based on the Elliptical Curve Discrete Function and Hash function standard cryptographic primitives. Likewise the other more security properties provided by solution are.

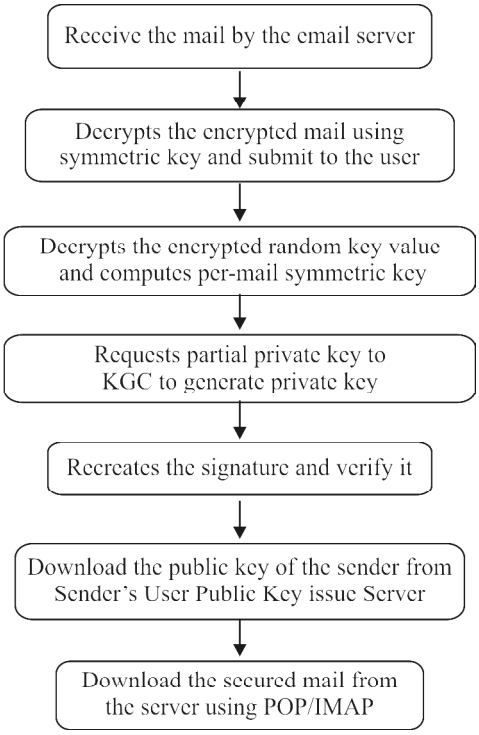

Figure 5: Receiving secure mail

1. End-to-End User Authentication

In proposed mailing security mail system uses the Certificateless Public Key Cryptography with the binding technique for both sender and receiver will authenticate each other using a pairing operation.

2. Sender and Receiver without Interact Using Key Agreement

The sender and receiver of the proposed system compute the shared secret key using their own secret values. Therefore, the proposed system is secure against the man-in-the-middle type attack.

3. Forward and Backward Secrecy

In the proposed system the random number has the feature of Perfect Forward and Backward Secrecy, which is always fresh and unrelated to any past or future sessions.

4. Confidentiality of the Message

Every mail content is encrypted by a symmetric crypto system which guarantees the confidentiality of the message and symmetric key can only be decrypted by the receiver.

6. CONCLUSION

This paper proposed an end-to-end secure mailing system based on certificate-less public key cryptography, with DNS as the mechanism to publish a user's public key server address. This avoids a man-in-the-middle attack to obtain details of encryption /decryption key and hence contents of the email. Probably the proposed mail system is based on Elliptic Curve Cryptography, which is very efficient compared and free from the heavy burden of certificate management of PKI/PGP based systems. Moreover, the proposed system is based on standard cryptographic primitives and which makes it secure against the standard security model.

REFERENCES

[1] B. Adida, D.Chau, S.Hobenberger, and R.L.Rivest "Lightweight email signatures (extended abstract)", *International Conference on Security and Cryptography for Networks*, **20(1)**, 288-302, 2006.

[2] D. Boneh and M. Franklin, "Identity-based encryption form the weil pairing", in *Advance in Cryptology*, **37**, 213-229, 2011.

[3] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer, Open PGP Message Format, Technical Report RFC 2440, Nov.1998.

[4] S. Chatterjee and P. Sarkar, Identity-based Encryption, Springer Science+Business Media, LLC, 2011.

[5] L. Chen, K. Harrison, N. Smart and D. Soldera, "Applications of multiple trust authorities in pairing based cryptosystems", in *International Conference on Infrastructure Security* **12(5)**, 260-275, 2002

[6] T. Chen and S. Ma, "A secure email encryption proxy based on identity-based cryptography", in *International Conference on Multi Media and Information Technology* **10(6)**, 284-286, 2008.

[7] S.S.M Chow, "Removing escrow from identity-based encryption", in Public Key Cryptography **11**, 256-276, 2009.

[8] M. Cooper, Internet X.509 Public Key Infrastructure (Latest Draft), IETF Internet Drafts, Jan.2005.

[9] M. Crispin, Internet Mail Access Protocol, Technical Report RFC 1730, Dec 1994.

[10] D. Crocker, T. Hansen, and M. Kucherawy, Domain keys Identified Mail (DKIM) Signatures, Technical Report 6376, Sep 2011.

[11] D. Eastlake, Domain Name System Security Extensions, Technical Report RFC 2535, Mar 1990.

[12] B.A. Forouzan, Cryptography and Network Security, India: Tata McGraw Hill Publishing Company Limited, 2007.

[13] Fortinet, Forti Mail Identity Based Encryption, Jan.2014 (http://www.fortinet.com)

[14] M. Franklin and D. Boneh, "Identity based encryption from the weil pairing", *Journal of Computing*, **32(3)**, 586-615, 2003.

[15] E. Gerck, Secure Email Technologies X.509/PKI, PGP, IBE and Zmail. A Usability and Security Comparision, ICFAI University Press, **55(1)**, 171-196, 2007.

[16] C. Gu and Y. Zhu, "New efficient searchable encryption schemes from bilinear pairings", *International Journal of Network Security*, **10(7)**, 25-31, 2010.

[17] M. Hassouna, N. Mohamed, B. Barry, and E. Bashier, "An end-to-end secure mail system based on certifticateless cryptography in the standard security model", *International Journal of Computer Science* Issues, **10(3)**, 264-272, 2013.

[18] A. R. Sattam and P. Kenneth, "Certificateless public key cryptography a full version", in Asiacrypt'03, LNCS 2894, Springer, **20(4)** 452-473, 2003.