Combining Mediated and Identity-Based Cryptography for Securing E-Mail

Sufyan T. Faraj Al-Janabi and Hussein Khalid Abd-alrazzaq

College of Computer, University of Anbar,
Ramadi, Iraq
sufyantaih@ieee.org, hu_albasri@yahoo.co.uk

Abstract. This work aims to exploit a distinguished method of the public key cryptography which is known as Identity-Based Cryptography (IBC) to solve the usability problem of secure e-mail systems. The public key is taken from general information (such as e-mail address) of the recipient and thus does not require access to any certificate to validate the key. To increase the system strength, the identity-based cryptography is combined with mediated cryptography to enable the cancelation of any key that is being exposed or suspicious. In addition, all the operations of decryption and signature are controlled (without the ability to fraud or detect secret) by the authorized person to prevent hackers and non-authorized parties from using or manipulating of the system. This proposal includes the deployment of the combined method for Mediated Identity-Based Cryptography.

Keywords: e-mail security, identity-based cryptography, mediated RSA, public-key infrastructure.

1 Introduction

Email is one of the essential applications of the Internet. More than a hundred million electronic messages traverse the world's computer networks every day, most of this electronic mail is vulnerable. Securing email has always been an important issue and a subject of growing concern for the researchers and the users, where the volume of email grows continuously. Various standards and products have been created. Securing E-mails with encryption is introduced broadly by many experts, and they are successful in security matters. Several algorithms are designed for encryption and decryption. But intruders or hackers are still trying to find solutions in order to break these algorithms and retrieve the plaintext. For this reason, it is always desirable to find better ways to raise the security level for email and eliminate the increased risk of hackers.

Most of available secure e-mailing systems relies on public key cryptography for key management and signature issues. However, most people continuously fail in protecting themselves, despite the long time that has passed on the availability of systems that based on public-key infrastructure (PKI). The main reason for this is that PKI is just too difficult for the average user. A well-known difficulty with the use of public key cryptographic systems is the verification and distribution of the public

E. Ariwa and E. El-Qawasmeh (Eds.): DEIS 2011, CCIS 194, pp. 1–15, 2011.

keys. Therefore; it requires a tremendous overhead in terms of setting up a public key. A relatively new trend of research in this direction is to use Identity-Based Cryptography (IBC) in securing e-mail systems so that to make them easier for use by users. IBC facilitates easy introduction of public key cryptography by allowing an entity's public key to be derived from an arbitrary identification value, such as email address. Thus, it greatly reduces the need for public key certificates. However, IBC techniques are not compatible with popular public key encryption algorithms. On the other hand, mediated cryptography or mediated RSA (mRSA) achieves simple splitting of RSA private key between the user and a Security Mediator allowing fine-grained control of users' security privileges. However, mediate cryptography relies on public key certificates to manage public keys. In this paper, we present an interesting combination of IBC and mediated cryptography for securing e-mail systems. In addition, a secure e-mail system based on this hybrid security technique has been developed and tested.

The remaining of this paper is organized as follows: Section 2 contains some background of public key cryptography. Section 3 presents theoretical background of IBC. Then, a general description of the proposed system is given in Section 4. The proposed hybrid security techniques is described in Section 5. Next, Section 6 outlines the operation of the system. Finally, the paper is concluded in Section 7.

2 Public Key Cryptography

Public key cryptography requires the receiver's public key. As a consequence, before sending any message, the sender should obtain this public key. Moreover, he should make sure that the public key he obtains is indeed the correct one. This introduces two important steps in real life implementation, fetching the public key and verifying it. It may seem that the second step is the difficult one. However, there is a simple solution that allows one to verify a public key is public-key certificates. At the most basic level, a public-key certificate is simply a message that asserts: "The public key of user Bob is upk_B", to make sure that the certificate is genuine. It needs to be signed [1].

To use a public key that is contained in a digital certificate, a user queries the public repository where the certificate can be found and retrieves the certificate. Because a public key may be valid for quite a while, it is often necessary to check such a public key for validity before using it. A much more difficult problem when using such certificates is the management of trust. This is related to what guarantee can be given to trust the owner of the verification key [2].

2.1 Public Key Infrastructure

The Public Key Infrastructure provides the digital certificates that can identify the individual's identity. The digital certificate is used to offer level of security that means each person must present the digital certificate which contains the public key to check from the identity. PKI is the combination of hardware, software, encryption technology, people, and policies. The PKI consist of many parts, which are [2, 3]:

- *Certification Authority (CA):* CA is to oversee the generation, distribution, renewal, revocation and suspension of the digital certificates.