Chapter 15
Enhancing Security at Email End Point:
A Feasible Task for Fingerprint Identification System

Babak Sokouti
Tabriz University of Medical Sciences, Iran

Massoud Sokouti
Shahid Beheshti University, Iran

ABSTRACT

Although email security needs more attention, a small amount of research has been conducted. Most of the security properties that can be applied to the email messages are based on encryption and digital signatures. The cryptography techniques that can be both symmetric and asymmetric algorithms cannot prove the identity of the sender and receiver in the real world, which is related to the end point security. Additionally, these techniques are not capable of preventing the spams, scams, and spoofing attacks. A new secure email system based on fingerprint identification is proposed to overcome the recognition of the real identity of the email sender and receiver. This method uses the user's username and password hashes, their full name and personal image, and fingerprint hashes along with the email message hash. The proposed method is successfully evaluated against security, maintenance, operational, and privacy issues.

INTRODUCTION

Electronic mail or email is a popular form of communication between computer users. This has led it to forcefully get used to hosting the malware, for example, viruses, spam email, Trojans and other phishing scams. The use of email will allow attackers (Garfinkel, Margrave, Schiller, Nordlander, & Miller, 2005)—an entry wedge as a means of getting personal information—if the person trusts the received email. Sometimes sensitive data is transmitted clearly in Internet.

DOI: 10.4018/978-1-4666-4030-6.ch015

This allows the messages to be intercepted or to be read by an unauthorized person; also messages can be re-created, altered and sent to the recipient from an unauthorized sender (Garfinkel, et al., 2005). By using cryptographic techniques a secure channel can be created for protecting the email contents; this is the only way used to protect the messages from previous years. Nowadays, although encryption and signing messages based on cryptography are integrated into email client software, small numbers of messages are transmitted securely (Gutmann, 2004).

Some of the standards of securing emails are PEM (Privacy Enhanced Mail), MIME (Multipurpose Internet Mail Extensions), S/MIME (Secure/Multipurpose Internet Mail Extensions)), PGP (Pretty Good Privacy) and PKCS#7 (Public Key Cryptography Standard #7). These are being used to provide security services such as confidentiality, data origin authentication, message integrity and non-repudiation of origin. By using these standards within the email process, a digital signature can be added to email to provide the authenticity of the sender to make a message tamper resistant and encrypting makes it undecipherable by anyone else (Garfinkel, 2003; Housley, 1989).

These techniques are all based on the asymmetric or public key cryptography in which we do not need to share a secret key between sender and receiver. The public and private key pair production is done by special mathematical formulas in which the private key can be used for both decrypting and signing processes and the public key for both encrypting and verifying processes. The security of this system is totally relying on the key management issue, i.e. by compromising the private key or by altering the public key the whole sensitive data will be revealed to an unintended person.

Up to now, protecting the email content by providing the related security service is being presented which has its own pros and cons in special situations. Now at this stage it is critical to see how previous methods can solve it. In this chapter, a new email security model is presented to answer this question that none of the previous methods can solve this problem. Though the security of the communication channel is being discussed, the real authenticity of the endpoints (sender and receiver) is not provided. This can be resulted in the threats such as Spam emails and Phishing threats or even a non-repudiation security service issue.

Suppose a simple scenario in which Alice (Sender), Bob (Intended Receiver), and Sarah (Secretary Receiver) are included. Alice signs or/and encrypts the message by her private key and sends it to Bob's email address. Sarah, as Bob's secretary receiver, knows the Bob's Public key as she is his trusty secretary, receives the message, verifies or/and decrypts the message. The message is very urgent and Bob should also have a reply to Alice's email. For some reasons, Sarah forgot to tell Bob about the received message. After some days, Alice asks Bob about the reply of her message and Bob does not know about the email she is talking about as Sarah has not informed him. Now, the problem is how Bob will know whether the email sent to him has been deleted or read while he did not get informed.

In this situation, a means is needed to reveal the real authenticity of the message receiver/sender as cryptographic techniques are just a combination of ASCII characters and are not based on an individual's characteristics. Biometrics technology is the most common way of determining the identity; for solving this problem a biometric solution is used to authenticate individuals for which fingerprint identification is more reliable and user-friendly than other biometric features (Jain, Ross, & Prabhakar, 2004).

A fingerprint recognition system consists of a fingerprint sensor input, feature extractor, a database of stored fingerprint features, and decision making section. Finally, the system will make the comparison between the input data and the stored