Chapter X

Electronic Mail Security

Electronic Mail Security

In previous chapters of this book, crypto systems, security mechanisms, and security services have been discussed and reviewed as separate crypto modules. In Chapters 10 to 14, how these crypto modules are used to provide network security will be discussed.

Electronic mail enables users to exchange messages using computer communications facilities, but sending an e-mail message is like sending a postcard that anyone can read as it travels from post office to post office. When an e-mail message travels from one e-mail server to another, the e-mail is first stored in an e-mail server before it is sent to the next e-mail server.

A way to protect e-mail is by using writer-to-reader security in which the message is encrypted at the sender station and deciphered at the receiver station. There are several ways to make e-mail secure. Pretty Good Privacy (PGP) and Secure MIME (S/MIME) are presented in this chapter.

Objectives

- Be able to explain PGP security services work
- Know S/MIME Message Formats
Introduction

When a company sends a document using regular mail, employees may go to the extreme to safeguard the information by delivering the mail directly to the post office and using certified delivery, or by using courier companies. However, employees do not hesitate to send highly sensitive and confidential information, such as a business report or sales forecast, using e-mail. E-mail is the most used network-based application, but it is the least secure. Companies spend millions of dollars in hardware and security intrusion software, but very few encipher their e-mail communications.

To send and receive e-mails a user needs to be connected to an e-mail server. When a message is sent, the e-mail server receives and stores the message, and then sends it to another e-mail server that does the same. E-mails travel through many servers and each one keeps a copy of the message. Users cannot erase the e-mail on all those servers, so the copy of the e-mail stays in the server until the server owner decides to erase it. There are companies that have found a niche in developing specialized software that supposedly erases e-mail from all the servers where the e-mail has been archived.

A way to protect e-mail is by using writer-to-reader security in which the message is encrypted using privacy enhanced mail (PEM), MIME Object Security Services (MOSS), X.400, PGP, and S/MIME. PGP, which is a specification and a product, and S/MIME, which is a protocol, are compatible with Internet mail and work with Eudora e-mail, Netscape Messenger, and Microsoft Outlook.

Pretty Good Privacy (PGP)

PGP, developed by Phil Zimmermann, is a crypto system that uses data compression and symmetric and public-key cryptography. By compressing the data before it is encrypted, PGP strengthens cryptographic security because most cryptanalysis techniques use plaintext patterns to try to break the cipher.

The following steps describe the PGP encryption algorithm (Zimmermann, 2000):

1. The sender generates a session by entering a word or password in his/her computer using the keyboard or mouse. PGP uses the content and timing of user keystrokes and mouse movements to generate a random message encryption key. The message encryption key is a one-time secret key used to encipher the message by encrypting it with a symmetric encryption algorithm.

2. The message is hashed using SHA-1 and signed using DSA or RSA with the sender’s private key creating a digital signature.

3. The cleartext message is concatenated with the digital signature, and the result is compressed using a compression package called ZIP.

4. The ZIP compressed cleartext message and digital signatures are enciphered with a symmetric algorithm (Cast-128, IDEA, or 3DES) using the one-time secret key generated previously by the sender.
A Research on Students' Perceptions on a B-Learning English Environment to Improve Written Skills

Ana María Pinto-Llorente, Mª Cruz Sánchez-Gómez and Francisco José García-Peñalvo (2018). Multidisciplinary Perspectives on Human Capital and Information Technology Professionals (pp. 179-201).

www.igi-global.com/chapter/a-research-on-students-perceptions-on-a-b-learning-english-environment-to-improve-written-skills/198257?camid=4v1a