Chapter 16
Cryptography in Electronic Mail

Hosnieh Rafiee
Hasso Plattner Institute, Germany

Martin von Löwis
Hasso Plattner Institute, Germany

Christoph Meinel
Hasso Plattner Institute, Germany

ABSTRACT

Electronic Mail (email) is a very important method of communicating across the Internet, but the protocols used to handle emails during transmission, downloads, and organizational processes are not secure. Spammers and scammers misuse these protocols to propagate spam or scams across the Internet for advertising purposes or to gain access to critical data, such as credit card information. Cryptographic approaches are applied as a tool to help in securing email components, such as the header, data, etc. This chapter classifies the approaches used according to the protection mechanisms provided to the email components, and it also briefly describes these approaches. Because scammers are continually trying to crack current algorithms, the most recent improvements in email security using cryptography are covered in this discussion. An explanation is given as to the need for verifying both receivers and senders in this process. Finally, the authors examine how the use of these approaches will work in IPv6 as compared to IPv4.

INTRODUCTION

In computer terms, email (e-mail) is short for electronic mail. It is a current method of transmitting data, text files, digital photos, and audio and video files from one computer to another over the internet. This phenomenon did not become popular until 1990 and now it is a major business in personal communications. Compared to sending mail via the post office in the traditional way (snail mail), email is faster and cheaper. Messages can be sent at any time to anywhere and the recipient can read it at his or her convenience. The same message can be sent to multiple recipients at one time and the message can be forwarded without having to retype it.

Early email was not invented; it just evolved. Early email was just a small advance on what we know these days as a file directory—it just put a message in another user's directory in a spot where

DOI: 10.4018/978-1-4666-4030-6.ch016

they could see it when they logged on. Just like leaving a note on someone's desk.

The first documented email system was MAILBOX, used at the Massachusetts Institute of Technology. Another early program used to send messages, on the same computer, was called SNDMSG (Tomlinson, 1971).

Some of the mainframe computers of this era might have had up to one hundred users - often they used what are called "dumb terminals" to access the mainframe from their work desks. Dumb terminals just connected to the mainframe—they had no storage or memory of their own and all work was done by the remote mainframe computer.

Today, a standard protocol called Simple Mail Transfer Protocol (SMTP) (Klensin, 2008) is used to send and receive mails and transport them across multiple networks (SMTP relay) by establishing a two-way transmission channel between a SMTP client and server over the internet or networks.

Here, two problems are encountered. The first is related to spamming. Spam mail is unsolicited email. It is also known as "junk" email that is typically not wanted by the user who is receiving it. The second is related to scamming. Scam mail is an email that is also unsolicited, but is attempting to acquire money or personal information from the recipient. Spammers and criminals profit from the use programs that misuse the SMTP protocol.

The U.S. Congress passed a law (15 USC Chapter 103, 2011) in 2003 that was designed to curb spam. This law makes it illegal to send messages that use deceptive subject lines and false return addresses, providing fines for as much as 6 million dollars and possible prison terms for violators. The law states that all messages, solicited or unsolicited, must have a valid postal address and an opt-out mechanism so that recipients can prevent future email solicitations. The email system is also vulnerable to hackers who can attach malicious programs to an email in hopes of infecting other computers whose resources they can then use in further attacking scenarios. This could damage the reputation of Internet Service Providers (ISPs) and/or expose critical personal information to criminals.

Email remains the most important application on the internet and is the most widely used facility that the internet has. Now more than 600 million people internationally use email. One can thus see how important it is to make it as secure as possible.

This chapter focuses on the use of cryptographic approaches to resolve the security issues inherent in SMTP. Reference will be made to many different possible cryptographic approaches based on what part of the total message they address; envelope or content. Each approach will be classified accordingly. Thus, there are cryptographic approaches for securing the SMTP envelope, such as verifying the users' authenticity to reduce spam and forged messages, and for securing the content of the message to prevent exposing critical data, such as credit card information, etc. to criminals. The necessity of verifying receivers, as well as senders, in order to avoid forged messages, will also be discussed. We start with a short introduction about electronic mail, SMTP, and problems of misusing SMTP. We discuss the advantages and disadvantages of these approaches and then introduce the most recent improvements and modifications made to enhance these approaches. Finally, we describe how to use these approaches in future internet networks, i.e., IPv6.

ELECTRONIC MAIL (EMAIL)

Email Object

An electronic mail message (or email for short) is a digital message that can be transferred over communication networks. An email consists of two components (Klensin, 2008):

- **Envelope:** The envelope is something that an email user will never see since it is part of the internal process by which an email is routed. It's added automatically by your