Fighting E-Mail Abuses: The EMPE Approach

Massimiliano Pala and Antonio Lioy

Politecnico di Torino
Dip. di Automatica e Informatica
Torino, Italy
{massimiliano.pala, lioy}@polito.it

Abstract. Electronic mail is one of the most used and abused service in today communication. While many efforts have been made to fight e-mail abuses, no effective solution has yet been developed. Furthermore new technologies (e.g. wireless roaming) and new user needs (e.g. mobility) completely break the existing e-mail authentication techniques based on network topology. In this paper we present the E-Mail Policy Enforcer system (EMPE) which provides a method to cryptographically bind the identity of the original sender of an e-mail to the message body by combining digital signatures and transport level authentication data.

1 Introduction

Electronic mail is used by millions of people for work, personal contact, or simply for any other activity that requires fast communication. Due to the importance it has acquired in business it is considered a critical and inestimable service by enterprises and professionals. Unfortunately it is also one of the most abused Internet services. Perhaps no problem plagues the Internet as deeply as that of unsolicited junk e-mail, or spam. The word spam comes from an old Monty Python skit [1] where some people are unable to have a conversation because of a noisy "Spam" song coming from the nearby table. The term became connected with computers in 1985 [2] when somebody annoyingly typed the word "spam" on a MUSH (Multi-User Shared Hallucination role playing game) on all the connected users' terminals.

Perhaps the first traced spam took place in May 1988 and it is named the "JJ incident" [3]. An even earlier example known as "the dinette set heard 'round the World" [4] consisted in only two posts sent to *net.general* which is seen everywhere.

Today the e-mail system is subject to a variety of abuses, this includes not only spam, but also viruses and worms. According to RFC-2505 [5], spam is the mass sending of unsolicited e-mail. However, it is not easy to establish what "unsolicited e-mail" is. In fact some e-mail addresses are meant to be public, e.g. addresses used to provide products support or help desk services, addresses of professionals or Public Administrations, and all of them should be able to receive mail from everyone.

Many attempts have been made to stop spammers by law. Many countries have laws that prohibit or regulate bulk sending of e-mail messages, but still

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 130–144, 2006.

no positive results have been achieved. In most cases laws address specifically commercial advertisements. To apply any existing law, however, it should be possible to trace back the real sender of the message. Unfortunately the biggest flaw in today e-mail system is that messages do not retain strong authentication information from the sending Mail Transfer Agent (MTA) to the receiving one. Consequently the electronic envelope is subject to the same problems as in traditional mail where the receiving post office has no means to verify if the sender printed on the envelope is real or forged. This problem is exploited by spammers to disguise their identities.

Another recently used technique, that is becoming ever more popular among spammers, is the so called *prefix hijacking* attack. By using the lack of security in the Internet routing protocol [6], spammers are able to impersonate whole sets of unallocated IP addresses as originating points when sending spam. In fact the Internet routing infrastructure is actually subject to different type of attacks (e.g. blackholling, redirection, subversion) and current counter measures are either generally ineffective (route filtering) or too heavyweight to deploy (S-BGP [7,8]). After sending unauthorised e-mails, then, attackers disappear by restoring original routes.

An important aspect to be analysed is the economics of e-mail abuses. Internet subscribers world-wide are unwittingly paying an estimated 10 billion euro a year in connection costs just to receive "junk" e-mails, according to a study undertaken for the European Commission in 2001 [9]. The high volume of messages exchanged because of spam and viruses raises costs for every subject involved in the e-mail delivery process, by requiring additional CPU power, disk storage and network bandwidth. Moreover this situation pushes users and enterprises to buy additional services and software, e.g. anti-spam or anti-virus products. The e-mail abuse has therefore opened a new market which is still growing.

The solution presented in this paper, i.e. *E-Mail Policy Enforcer* (EMPE), addresses the e-mail abuse problem by providing a tool to enforce strong authentication on message contents. The rest of the paper is organised as follows. In section 2 and 3 we analyse existing solutions and proposed standards. In section 4 we detail the EMPE architecture, while in section 5 we discuss issues related to EMPE deployment. Section 6 describes possible enhancements to our solution and future work.

2 Present Solutions

The Simple Mail Transfer Protocol (SMTP) [10] and the Internet Message Format [11], which represent the underlying communication standards for the e-mail system, were designed for open communication, and consequently authentication was not a priority during their design. Moreover these standards allow to configure a server to relay mail (i.e. by acting as an SMTP client to the next SMTP server after having accepted an e-mail from a user or another MTA), thus making it difficult to identify and track the original sender of a message. Therefore malicious users could forge the message contents with false or dangerous data.