Design and Implementation of an Inline Certified E-mail Service

Stelvio Cimato[1], Clemente Galdi[2], Raffaella Giordano[3], Barbara Masucci[2], and Gildo Tomasco

[1] Dipartimento di Tecnologie dell'Informazione, Universitá di Milano, Via Bramante 65, 26013 Crema (CR), Italy
cimato@dti.unimi.it

[2] Dipartimento di Informatica ed Applicazioni, Universitá di Salerno, Via S. Allende, 84081 Baronissi (SA), Italy
clegal, masucci@dia.unisa.it

[3] Italsime s.p.a. Via Cinthia 25, Parco S. Paolo, 80126, Napoli (NA), Italy
giordano.r@italsime.it

Abstract. Nowadays, e-mail has become one of the most widely used communication medium. Because of its characteristics of inexpensivity and rapidity in the delivery of messages, e-mail is increasingly used in place of ordinary mail. However, the e-mail service exposes users to several risks related to the lack of security during the message exchange. Furthermore, regular mail offers services which are usually not provided by e-mail, and which are of crucial importance for "official" events.

Certified e-mail tries to provide users with additional guarantees on the content and the delivery of the messages, making e-mail equivalent and in some cases more convenient than the ordinary paper-based mail service. In literature, several distributed protocols for certified e-mail have been proposed, relying on an inline trusted third party (TTP) to ensure the fairness of the protocol. In such protocols, the TTP is actively involved in each message exchange. In this paper we provide a novel inline certified e-mail protocol which satisfies all the most important requirements which have been discussed for certified e-mail. Furthermore, we discuss a prototype implementation of our protocol targeted to the Windows platform.

1 Introduction

The electronic mail service allows users connected to the Internet to exchange messages containing text or multimedia files. The ease of use of e-mail clients as well as the spreading of the Internet and its associated services has determined a large diffusion of the e-mail service. E-mail is more and more used in place of ordinary mail. However, the use of e-mail in official events poses some problems. Indeed the actual e-mail service is based on the Simple Mail Transfer Protocol (SMTP [2]) which offers no guarantees on the delivery and the authenticity of the messages. Compared to the ordinary mail service, the e-mail is much less

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 186–199, 2005.

reliable: it gives the sender no evidence of having sent a message as well as no return receipt. Furthermore, whenever an e-mail message is received, there is no assurance on the identity of the originator of the message. Even the transmitted message could be eavesdropped over its path from the origin to the destination, and its content could be manipulated or corrupted by a malicious adversary.

Some e-mail clients (e.g., Microsoft Outlook) provide a Read Receipt request facility. Recipients may receive a request for a response to be sent, but they may decline to send the acknowledgement, or could set a switch to forbid confirmations of such a request. Other e-mail clients may simply ignore the request for a receipt. Indeed, such systems give no guarantee that the sender will receive a receipt when the recipient has displayed the message.

IETF RFC 2298 [1] defines a MIME content-type for message disposition notifications (MDNs). An MDN can be used to notify the sender of a message of any of several conditions that may occur after successful delivery, such as display of the message contents, printing of the message, deletion (without display) of the message, or the recipient's refusal to provide MDNs. However MDNs are not enough to satisfy all the properties usually guaranteed by the regular mail service, because they are easily forgeable.

Exploiting the digital nature of the transaction, it is possible to devise methods and techniques that enhance the capabilities of the message transfer protocol, obtaining the same or even additional guarantees with respect to the paper-based counterpart. One example of such guarantees is the following. A registered mail service allows the sender to prove that she sent *a message* at a specific time to a specific destination. Notice that nothing can be said about the *content* of the message sent. In a digital world, the sender may be able to prove that she sent a *message with a specific content* to a destination.

Certified e-mail protocols basically provide the following property: user Bob receives an e-mail message from user Alice if and only if the latter receives a receipt for this communication, i.e., a proof that the message has been delivered to the recipient. The receipt is such that the recipient cannot deny having received the message. Along with this property, many certified e-mail protocols provide other features like confidentiality of the message, proof of integrity, and so forth. Temporal authentication is, in some cases, e.g., patent submissions, a strict requirement. Enhancing e-mail systems with temporal authentication could simplify such kind of applications by reducing them to the simple operation of sending an e-mail. In Section 2 we describe in more detail the most important properties that have been identified in the literature as being crucial for certified e-mail systems.

Recently a lot of research has been dedicated to the problem of designing certified e-mail protocols. Most of the protocols that have been studied involve a trusted third party (TTP for short) which is delegated by the participants to control the behavior of the parties, assist them during the exchange of messages, and resolve any dispute, if necessary. According to the role played by the TTP, protocols have been classified as *inline* or *optimistic*. In inline protocols [10, 28, 17, 23], the TTP is actively involved in each message exchange: both