Efficient Identity-Based Protocol for Fair Certified E-mail Delivery

Zhenfeng Zhang[1,2], Jing Xu[1,3], and Dengguo Feng[1,2]

[1] State Key Laboratory of Information Security
[2] Institute of Software, Chinese Academy of Sciences, Beijing 100080, P.R. China
[3] Graduate School of Chinese Academy of Sciences, Beijing 100039, P.R. China
zfzhang@is.iscas.ac.cn

Abstract. Certified e-mail delivery has become one of the basic requirement in performing business transactions over the Internet securely. How to construct efficient fair protocols for certified e-mail delivery is of great interest. The notion of identity based cryptosystem has attracted much interest since its introduction by Shamir in 1984, as it eliminates the need of certificates and simplifies the key management. In this paper, we propose a fair protocol for certified e-mail delivery based on identity-based signatures. A semi-trust third party (TTP) is involved in our protocol to ensure fairness, who does not need to store anything except its own private-key. There is no need for an additional registration between users and TTP. The proposed scheme is the first identity-based protocol with such a concise frame and is computation- and communication-efficient.

Keywords: Fair exchange, Certified E-mail, Security protocol, Identity-based signature.

1 Introduction

Communication by e-mail has become a vital part of everyday business and has replaced most of the conventional ways of communicating. The basic e-mail security services include the provision of privacy (only the intended recipient can read the message) and authentication (the recipient can be assured of the identity of the sender). Cryptographic mechanisms for providing these security services have been applied in Internet mail systems, such as S/MIME [24] and PGP [25]. In addition to sender authentication and message privacy, S/MIME can also provide a signed receipt service. A signed receipt from the recipient (requested by the sender) serves as a non-repudiable proof of receipt for a specific e-mail. However, the return of this receipt relies on the willingness of the recipient to honor the sender's request and provides no protection to the sender if the recipient chooses not to sign and return the acknowledgement after having read the message. In other words, this technique does not truly provide non-repudiation of the receipt security service.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 200–210, 2005.

Important business correspondence may require certified e-mail delivery service, analogous to that provided by conventional mail service. For a viable certified e-mail service, the following security properties are needed:

- Non-repudiation of origin - the recipient must have a way of proving that a specific e-mail indeed originates from the sender;
- Non-repudiation of receipt - the sender must have a way of proving that the recipient has indeed received a specific e-mail;
- Strong fairness for the exchange - the recipient should obtain a specific e-mail if and only if the sender obtains a receipt for it.

By now, certified e-mail delivery (CEMD) has become one of the central problems in performing business transactions over the Internet securely and can be applied in numerous e-commerce transactions. Briefly speaking, this is the problems of how two mutually distrustful parties can fairly exchange a sender's valuable e-mail for a receiver's digital signature representing a proof of reception. A CEMD protocol [13, 17] shall provide strong fairness to ensure that the recipient receives the e-mail if and only if the sender receives the receipt.

The most practical and efficient approach to the fair exchange problems is to make use of an off-line trusted third party (TTP) to help the participants with the exchange. By this approach, the exchanging parties attempt to exchange their respective items themselves, i.e. without any involvement of the TTP. Should any dispute arise during the exchange process due to a party's misbehavior or a network failure, TTP is invoked to recover the disputed items and restore fairness.

Recently, a new category of off-line TTP-based fair exchange protocols has been proposed based on a cryptographic primitive called *verifiable and recoverable encryption of a signature* (VRES) [1, 2, 3, 4, 8, 10, 11, 14]. The VRES represents a digital signature encrypted in such a way that a receiver of the VRES can verify that it indeed contains the correct signature without obtaining any information about the signature itself (verifiability). The receiver can also verify that a designated TTP can help to recover the original signature from the VRES, in case the original signature sender refuses to do so (recoverability).

In SAC'04, Nenadic et al. [21] proposed a new RSA-CEMD protocol for the two communicating parties to fairly exchange an e-mail message for an RSA-based receipt. The main contribution of their work is a novel RSA-based method for the verifiable and recoverable encrypted signature, which is utilized as a crucial primitive to construct their RSA-CEMD protocol. The proposed protocols has been used as a main cryptographic primitive in the Fair Integrated Data Exchange Services (FIDES) project [22] provided for E-commerce transactions. However, as a building block, their VRES scheme was shown to be insecure recently by [23]: an adversary can easily generate a valid VRES which cannot be recovered by the designated TTP, and hence the proposed certified e-mail delivery protocol can not guarantee the claimed fairness.