Forward-Secure Multi-signatures

N.R. Sunitha[1] and B.B. Amberker[2]

[1] Dept. of Computer Science & Engg., Siddaganga Institute of Technology, Tumkur, Karnataka, India
[2] Dept. of Computer Science & Engg., National Institute of Technology, Warangal, Andhra Pradesh, India

Abstract. In many applications a document needs to be signed by more than one signer. When a signature depends on more than one signer we call it a multi-signature. Further, ordinary digital signatures have an inherent weakness: if the secret key is leaked, then all signatures, even the ones generated before the leak, are no longer trustworthy. Forward-secure digital signatures were proposed to address this weakness, they ensure that the past signatures remain secure even if the current secret key is leaked. We propose to apply the concept of Forward-Security to multi-signatures. The basic signature scheme that we have considered is ElGamal Signature scheme which is based on discrete log problem. We initially make this signature scheme forward-secure and then apply it to multi-signatures. By this all signers of the document can guarantee the security of document signed in the past even if their secret key is exposed today. An adversary will not be able to forge a multi-signature unless the secret key of all the signers are compromised in the same time period, which is practically not possible. Further, we propose two types of Forward-Secure multi-signatures : Forward-Secure Parallel multi-signatures and Forward-Secure Serial multi-signatures.

Once a user switches to use forward-secure signatures in place of ordinary signatures, he can easily extend it to use it as a multi-signature. In all applications where parallel or serial multi-signatures are used, the corresponding forward-secure multi-signatures can be used.

Keywords: Digital Signature, ElGamal Signatures, Serial multi-signature, Parallel multi-signature, Forward-Security, e-banking.

1 Introduction

The standard notion of digital signature [1, 2, 3, 4, 5] security is extremely vulnerable to leakage of the secret key which over the lifetime of the scheme may be quite a realistic threat. Indeed if the secret key is compromised any message can be forged. All future signatures are invalidated as a result of such a compromise and furthermore no previously issued signatures can be trusted. Once a leakage has been identified some key revocation mechanism may be invoked but this does not solve the problem of forgeability for past signatures. Asking the signer to reissue all previous signatures is very inefficient and moreover requires

M. Parashar and S.K. Aggarwal (Eds.): ICDCIT 2008, LNCS 5375, pp. 89–99, 2008.

trusting the signer. For example it is very easy for a dishonest signer to leak his secret key in order to repudiate a previously signed document. Furthermore changing the schemes keys very frequently is also not a practical solution, since frequently registering new public keys and maintaining them in a place that is both publicly accessible and trusted is a difficult task.

Forward-secure signature schemes, first proposed by Anderson in [4] and formalised by Bellare and Miner in [5] are intended to address the above limitation. A forward-secure digital signature scheme [5, 6, 7, 8, 9, 10, 11, 12] is a method for creating digital signatures signed with secret keys changing with time periods, all of which can nevertheless be verified by the verifier using the same public key. An adversary with access to this public key and the secret key of some time period, will be unable to forge signatures for an earlier time period. Thus, given the secret key for any time period, it is hard to compute any of the previously used secret keys. (It is important for the signer to delete the old secret key as soon as the new one is generated, since otherwise an adversary breaking the system could easily get hold of these undeleted keys and forge signatures.) Therefore a receiver with a message signed before the period in which the secret key gets compromised, can still trust this signature, for it is still hard to any adversary to forge previous signatures.

As many applications require multiple signers to sign the same document, we propose to apply the concept of forward-security to multi-signatures. A multi-signature scheme [13, 14, 15, 16] enables a group of signers to produce a compact, joint signature on a common document. Once a user switches to use forward-secure signatures in place of ordinary signatures, he can easily extend it to use it as a multi-signature. In all applications where parallel or serial multi-signatures are used, the corresponding forward-secure multi-signatures can be used. Using Forward-secure multi-signatures all signers of the document can guarantee the security of document signed in the past even if their secret key is exposed today.

In Section 2, we make the ElGamal signature scheme Forward-secure. In Section 3, we apply this forward-secure scheme for a group of signers who need to sign the same document. Here we discuss i) Forward-secure parallel multi-signatures that ensure forward-security of the document and allow each signer to sign the same document separately and independently. Such signatures can be used in signing contracts / approving the minutes of meeting where more than one person is required to sign the same document and can be signed independently. ii)Forward-secure serial multi-signatures that ensure forward-security of the document and allow signers to sign the same document serially and does not need to predetermine the signing order. Such signatures can be used where one signer signs the document only after another signer responsible for the document signs it. In Section 4, we give the security analysis of our scheme by considering the possible attacks against the multi-signature scheme and in Section 5, we discuss the forward-security of our scheme. Lastly in Section 6, we conclude the paper.