Distributing Security-Mediated PKI Revisited *

Jong-Phil Yang[1], Kouichi Sakurai[1], and Kyung Hyune Rhee[2]

[1] Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-0053, Japan
{bogus, sakurai}@itslab.csce.kyushu-u.ac.jp
[2] Division of Electronic, Computer and Telecommunication Engineering, Pukyong National University, 599-1, Daeyeon3-Dong, Nam-Gu, Pusan 608-737, Republic of Korea
khrhee@pknu.ac.kr

Abstract. The SEM approach to PKI offers several advantages, such as immediate revocation of users' signing ability without CRLs and compatibility with the standard RSA. However, it has a weakness against denial of service attack caused by breaking down or being compromised. G. Vanrenen et al. proposed a distributed SEM approach to overcome the weakness. However, it does not provide the desirable properties such as instant availability and immunity against denial of service attack, due to inadequate usage of threshold cryptography and proactive secret sharing. In this paper, we point out its structural shortcomings and propose a modified version.

Keywords: Certificate Status Information, Reliability, Fault-tolerance.

1 Introduction

Without doubt, the promise of public key infrastructure (PKI) technology has attracted a significant amount of attention in these days. The IETF PKIX Working Group is developing the Internet standards to support an X.509-based PKI. A certificate is a digitally signed object binding a set of attributes to a public key. The correctness of the trust decisions a relying party makes depends on the assumption that the entity knowing the matching private key possesses those properties. When this binding ceases to hold, this certificate needs to be revoked, and this revocation information needs to propagate to relying parties, lest they make incorrect trust judgments regarding that public key. There are well-known standard mechanisms to solve the revocation of the certificate such as Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP), and non-standard mechanisms such as delta CRL, indirect CRL, Certificate Revocation Tree (CRT) and Certificate Revocation System (CRS) [4][8].

* This work was partially supported by IT Scholarship Program supervised by Institute for Information Technology Advancement (IITA) & Ministry of Information and Communication (MIC) in Republic of Korea, Grant No. R01-2006-000-10260-0 from the Basic Research Program of KOSEF, and Strategic International Cooperative Program, Japan Science and Technology Agency (JST).

A.S. Atzeni and A. Lioy (Eds.): EuroPKI 2006, LNCS 4043, pp. 31–44, 2006.

In [3], Boneh et al. proposed a mechanism to fast certificate revocation centered around the concept of an on-line semi-trusted mediator (SEM). The basic idea of SEM is as follows. To sign or decrypt a message, a client must first obtain a message-specific token from its SEM. Without this token, the user cannot accomplish the intended task on the message. To revoke the user's ability to sign, SEM just stop issuing tokens for that user's future request. The SEM approach to PKI offers several advantages like immediate revocation of users' signing ability without Certificate Revocation Lists (CRLs) and compatibility with the standard RSA. However, it has a weakness against denial of service attack caused by breaking down or being compromised. To overcome the weakness, G. Vanrenen et al. proposed a distributed SEM approach based on threshold cryptography and proactive secret sharing [5]. However, it does not provide the desirable properties such as instant availability and immunity for denial of service attack, because of inadequate usage of threshold cryptography and proactive secret sharing.

Our Contributions
This paper introduces firstly the structural shortcomings of G. Vanrenen et al's proposal according to the following topics.

- Efficiency and meaning of performing a proactive secret sharing.
- Immediacy of the distributed SEM approach.
- Specifying the number of servers in the distributed SEM approach.

Then, we derive new requirements to address the shortcomings of G. Vanrenen et al.'s proposal and to design a modification of the distributed SEM approach. We introduce additionally two new cryptographic tools to satisfy new requirements. Finally, we design a modification of the distributed SEM with respect to the new requirements. Our modification has the following benefits: *removal of both insecurity and ambiguity, efficient and timely signing or decrypting, strong against denial of service attack and meaningful proactive secret sharing with the simplified procedure.*

Organizations
The remainder of this paper is organized as follows. Section 2 reviews the original SEM approach and the distributed SEM approach. We discuss notable problems of the distributed SEM and present requirements for designing a modified version in section 3. We present two cryptographic tools and design a modification of the distributed SEM in section 4. Section 5 discusses the security and the desirable properties of our modification. We conclude in section 6.

2 Related Work

2.1 SEM: Semi-trusted Mediator

In [3][17], the SEM system is based on a variant of RSA called as mediated RSA (mRSA). As in RSA, each user has a public key (e, N) and the corresponding