Available online at www.sciencedirect.com
ScienceDirect
Computers and Electrical Engineering 33 (2007) 88–93
Computers and Electrical Engineering
www.elsevier.com/locate/compeleceng

Insider attacks on multi-proxy multi-signature schemes

Lifeng Guo [a,*], Guilin Wang [b]

[a] State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China
[b] Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613, Singapore

Received 9 January 2006; received in revised form 6 June 2006; accepted 30 August 2006
Available online 21 December 2006

Abstract

In 2004, Hwang and Chen demonstrated new multi-proxy multi-signature schemes that allow a group of authorized proxy signers to sign messages on behalf of a group of original signers. Later, Lyuu and Wu pointed out Hwang et al.'s schemes were not secure and then proposed a modified scheme. They claimed that their modified schemes were secure. But in this paper we show a new attack on the Lyuu–Wu et al.'s schemes. Moreover, the original Hwang–Chen's schemes are also vulnerable to this insider attack. Furthermore, we point out some improvements for the Lyuu–Wu scheme and Hwang–Chen schemes according to Wang et al.'s methods [Wang GL, Han XX, Zhu B. On the security of two threshold signature schemes with traceable signers. In: Applied Cryptography and Network Security (ACNS 2003). Lect Notes Comput Sci (LNCS), vol. 2846, Springer-Verlag; 2003. p. 111–222]. These improvements can resist our insider attack.

Keywords: Proxy signature; Multi-proxy; Multi-signature; Insider attack

1. Introduction

The concept of the proxy signature scheme was first proposed by Mambo et al. [10,11] in 1996. A proxy signature scheme allows a signer to delegate the signing capability to a person, called a proxy signer, to sign on behalf of an original signer. For the group-oriented applications, the threshold proxy signature scheme is proposed. A (t,n) threshold proxy signature scheme is a variant of the proxy signature scheme in which the proxy signature key is shared by a group of n proxy signers in such a way that any t or more proxy signers can cooperatively employ the proxy signature key to sign messages on behalf of an original signer, but $t-1$ or fewer proxy signers cannot. So far, there have been many threshold proxy signature schemes [7,8,12,14,16,18]. In 2000, Hwang and Shi [4] proposed a multi-proxy signature scheme. In fact, a multi-proxy signature scheme is a special threshold proxy signature scheme in which only the cooperation of all the proxy signers can generate proxy signatures on behalf of the original signer. At the same time, some proxy multi-signature schemes were proposed [5,17]. That is, the group of original signers authorize one person as their proxy

* Corresponding author.
E-mail addresses: lfguo@amss.ac.cn (L. Guo), glwang@i2r.a-star.edu.sg (G. Wang).

0045-7906/$ - see front matter
doi:10.1016/j.compeleceng.2006.08.003

signer. In [6], a new kind of proxy signature scheme, multi-proxy multi-signature schemes were proposed. In the multi-proxy multi-signature schemes, only the original signer group can authorize the proxy signer group to sign message. Subsequently, Lyuu and Wu [9] analyzed the security of Hwang et al.'s schemes. They claimed that Hwang's schemes are vulnerable to insider attack. That is, a malicious proxy signer can forge a multi-proxy multi-signature for a message secretly while participating in a normal message signing process with other proxy signers. Furthermore, they proposed modified schemes and claimed their schemes were secure.

In this paper, we demonstrate an insider attack on the Lyuu–Wu schemes. A malicious proxy signer can forge a valid multi-proxy multi-signature. At the same time the Hwang–Chen [6] schemes are also vulnerable to this attack.

The rest of this paper is organized as follows. Section 2 reviews the Lyuu et al.'s multi-proxy multi-signature scheme and demonstrates our security analysis on their scheme. Section 3 simply analyzes the Hwang–Chen's scheme. Furthermore, we point out some improvements for the Lyuu–Wu scheme and Hwang–Chen schemes. These improvements can resist our insider attack. The conclusion is drawn in Section 4.

2. Insider attack on Lyuu–Wu multi-proxy multi-signature schemes

In the Lyuu–Wu scheme, they only modified the Hwang–Wu scheme without a clerk. But the same modifications can be applied to the scheme with a clerk and obtain the same results. In this section, we first review the Lyuu–Wu scheme. Then we proceed with the security analysis on the Lyuu–Wu scheme.

2.1. Review of the Lyuu–Wu schemes

In [9], Lyuu and Wu showed two multi-proxy multi-signature schemes: one needs the help of a clerk, whereas the other does not. Both schemes use the same calculations to generate the proxy certificate and signatures. Here we only review the scheme without a clerk in this subsection. Our attack also works against the scheme with a clerk. The scheme without a clerk has two types of participants: the original signers $\{U_1, U_2, \ldots, U_n\}$ and the proxy signers $\{P_1, P_2, \ldots, P_m\}$. The scheme can be divided into four phases: system set-up, proxy certificate generation, multi-proxy multi-signature generation, and multi-proxy multi-signature verification. We describe Lyuu–Wu's multi-proxy multi-signature scheme as follows.

2.1.1. System set-up phase

The proposed scheme parameters are listed as follows:

$N = p_1 p_2$ a public odd integer, where p_i are large primes such that each $p_i - 1$ has a large prime factor q_i;
$Q = q_1 q_2$ a public integer;
g a public integer with order Q in Z_N^*;
h a public one-way hash function;
ID_{u_i} the unique ID of the original signer U_i;
ID_{p_j} the unique ID of the proxy signer P_j;
$x_{u_i} \in Z_Q^*$ the secret key of the original signer U_i;
$y_{u_i} = g^{x_{u_i}} \bmod N$ the certified public key of the original signer U_i;
$x_{p_j} \in Z_Q^*$ the secret key of the proxy signer P_j;
$y_{p_j} = g^{x_{p_j}} \bmod N$ the certified public key of the original signer P_j;
w the proxy warrant that specifies the public proxy details such as $\mathrm{ID}_{u_i}, \mathrm{ID}_{p_j}, y_{u_i},$ and y_{p_j}.

2.1.2. Proxy certificate generation phase

In this phase, all proxy signers $P_1, P_2, \ldots, P_m$ cooperate with all original signers $U_1, U_2, \ldots, U_n$ to generate the proxy certificate (K, V) as follows: