An attack on an ID-based multisignature scheme

Chris J. Mitchell

Technical Report
RHUL–MA–2001–9
19 December 2001

Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Abstract

A serious weakness is identified in the ID-based structured multisignature scheme of Lin, Wu and Hwang.

1 Introduction

A cryptanalytic attack on the ID-based structured multisignature scheme of Lin, Wu and Hwang, [1], is described below. This attack enables one user from a group of users to forge multisignatures on arbitrary messages. This enables the forgery of both partial multisignatures and 'complete' multiignatures for the entire 'group' of users. The attack requires only two known multisignatures created by the group concerned.

The notion of Lin, Wu and Hwang, [1], is used throughout. Note in particular that, in line with [1], the word group is used to mean the defined collection of individuals authorised to create a multisignature. It has no relationship to the standard mathematical notion of a group.

2 The attack

First suppose a user wishes to be able to forge user u's contribution to a multisignature. For simplicity suppose $u = u_1$ for some serially ordered group of signers $(u_1, u_2, \ldots, u_n)$. Note this initial attack applies to the serial signing version of the scheme.

The attacker first arranges for two messages, m, m' say, to be multisigned. These messages can be chosen arbitrarily except that they must satisfy

$$\gcd(h(m), h(m')) = 1.$$

The probability that this will be true for arbitrary messages m and m' is good, and if it does not hold then a multisignature on a third message will very probably be sufficient. Then, there will exist integers a and b such that

$$ah(m) + bh(m') = 1.$$

(Finding such a and b is simple using the Euclidean algorithm).

When user u_1 computes the multisignatures on messages m and m', the following values are computed and made public:

$$S_1 = \alpha^{k_1 h(m)} \bmod N$$

and

$$S_1' = \alpha^{k_1 h(m')} \bmod N.$$

Suppose the attacker has these values and has computed a and b as above. The attacker can now compute

$$\begin{aligned}(S_1)^a (S_1')^b \bmod N &= \alpha^{ak_1 h(m) + bk_1 h(m')} \bmod N \\ &= \alpha^{k_1} \bmod N\end{aligned}$$

The value $\alpha^{k_1} \bmod N$ can now be used to forge a partial multisignature for user u_1 on any message of the attacker's choice.

Using precisely the same reasoning, two 'complete' multisignatures for the same user group (in the serial signing case) can be used to forge arbitrary numbers of multisignatures on messages of the attacker's choice. Similar attacks apply to the parallel and 'mixed' versions of the multisignature scheme.

3 Concluding remark

Since this note was first written, one of the authors of [1] (Chih-Yin Lin) has devised a modified version of the scheme which resists the attack described above. For details of this revised version please contact Professor Lin at `lincy@iim.nctu.edu.tw`.

References

[1] C.-Y. Lin, T.-C. Wu, and J.-J. Hwang. ID-based structured multisignature schemes. In B. De Decker, F. Piessens, J. Smits, and E. Van Herreweghen, editors, *Advances in Network and Distributed Systems Security*, pages 45–59. Kluwer Academic Publishers, Boston, 2001.