一个强前向安全的代理签名方案

张 波 徐秋亮
(山东大学南校区计算机科学与技术学院,济南 250061)
E-mail:zbsdu@mail.sdu.edu.cn

摘 要 在Kan Zhang不可否认代理签名方案的基础上,通过引入私钥演化机制,提出了一个强前向安全的代理签名方案,攻击者即使在第i时段入侵系统,也无法伪造以前或以后时段的代理签名,方案的安全性基于离散对数的难解性。

关键词 数字签名 代理签名 强前向安全

文章编号 1002-8331-(2006)09-0109-02 **文献标识码** A **中图分类号** TP309

A Strong Forward-Secure Proxy Signature Scheme

Zhang Bo Xu Qiuliang
(College of Computer Science and Technology, Shandong University, Ji'nan 250061)

Abstract: Based on Kan Zhang's nonrepudiable proxy signature scheme, a strong forward secure proxy signature scheme is proposed by introducing the mechanism of key evolving. Even if the malicious attacker can intrude the system at period i, he can not forge the proxy signature in other periods. The security of our scheme relies on difficulty of solving discrete logrithm problem.

Keywords: digital signature, proxy signature, strong forward-security

1 引言

根据Kerckhoff假设,密码体制的安全性完全依赖于密钥的安全性。密钥泄漏对于一个密码体制的安全性来说是致命的。

为了减轻密钥泄漏所带来的严重后果,Anderson在文献[1]提出了前向安全签名的概念。Bellare和Miner在文献[2]中第一次给出了前向安全签名的正式定义,并基于A.Fiat和A.Shamir的签名方案给出了两个前向安全签名方案。前向安全的基本思想是:在普通签名算法中加入密钥进化算法。密钥进化算法将公钥的生命期分为T个时段,公钥在这T个时段总保持不变,私钥随着时段的推进而不断更新。在前向安全签名方案中,攻击者即使在t时段入侵系统获得签名密钥,也无法伪造之前的签名。即使密钥因泄漏而被撤销,系统在t时段之前所做的签名依然有效。正是由于这一显著特点,前向安全签名受到了人们很多的关注。但是前向安全存在这样的隐患:攻击者在得到t时段的私钥后,可以伪造本阶段或者以后阶段的签名,因为所有的安全措施只有在发现私钥泄漏后才进行,在攻击者得到私钥到签名者发现私钥泄漏这段时间里,攻击者可以保持静默并和签名者进行同样的私钥更新,整个签名体制都暴露在攻击者的攻击之下,这样仍然会产生很大的损失。产生上述缺陷的主要原因是私钥更新阶段本身,目前的前向安全方案的私钥更新算法一般采用以下两种策略:一是用计算的方式直接计算得出新的私钥,二是预先生成私钥,采用存储或计算的方法再次获得。显然,这两种方式在私钥泄漏后均没有办法阻止攻击者进行同样的密钥更新。M.Burmester和V.Chrissikopoulos在文献[4]中提出了"强前向安全"的概念,认为在保证前向安全的同时,不应该让攻击者具有和合法签名者同样的私钥更新能力。必须使攻击者在获得t时段签名密钥的前提下,不能伪造以后时段的签名。这种安全性可理解为"双向安全性",采用M.Burmester和V.Chrissikopoulos的说法,本文也称其为"强前向安全性"。M.Burmester和V.Chrissikopoulos在提出"强前向安全"概念的同时,给出一个方案,该方案通过CA参与密钥更新来阻止攻击者。一旦攻击者获得密钥并进行更新,CA会发现两份密钥更新申请,进而确定出现私钥泄漏的情况,通过这样的方法,可以在私钥泄漏的情况下,把攻击者的伪造能力控制在一定的时间内,从而降低系统损失。但这种通过可信中心进行密钥更新的方法,实际上难以实现。

代理签名是由M.Mambo等在文献[5]中提出来的一个签名概念,原始签名人因为某种原因不能进行签名时,便将签名权交给代理人(如秘书)对文件进行签名。这种签名在电子交易、移动代理等环境中应用很广。代理签名中也存在代理人私钥泄漏的问题。代理人私钥泄漏会导致恶意用户伪造代理签名,从而对代理人构成诬陷,并使原始签名人的利益受损。代理人以往的签名会随之失效。可以看到,在代理签名过程中,原始签名人与代理签名人有着相同的利害关系,正是利用了这一点,本文首次提出一个强前向安全的代理签名方案。此方案能减轻私钥泄漏带来的损失,能保证在私钥泄漏前的签名都是有效的,通过原始签名人与代理签名人合力产生代理签名钥,尽早察觉私钥泄漏的情况,从而实现强前向安全。

2 强前向安全的代理签名方案

2.1 初始化阶段

选择大素数p,q而且$q|p-1$,令g为$GF(p)$的生成元,且

基金项目:国家自然科学基金资助项目(编号:60373026);山东省自然科学基金资助项目(编号:Y2003G02)
作者简介:张波(1981-),男,硕士研究生,主要研究方向为信息安全。徐秋亮(1960-),男,教授,博士生导师,研究领域为密码学与信息安全。

$g|q$,在此签名方案中,原始签名人 Alice 和代理签名人 Bob 的密钥有效期分为 T 个时段。

Alice 和 Bob 分别随机选择整数 x_{A_0}, x_{B_0} 作为初始私钥,$1<x_{A_0}, x_{B_0}\leqslant q$,计算相应公钥为:$y_A=g^{x_{A_0}^{2^{T+1}}} \bmod p$,$y_B=g^{x_{B_0}^{2^{T+1}}} \bmod p$,则 Alice 得到公私钥对的初始值$(y_A, x_{A_0})$,Bob 得到公私钥对的初始值$(y_B, x_{B_0})$,系统公钥为$(p, q, T, y_A, y_B)$,$h:\{0,1\}^* \to Z_p^*$是一个安全 hash 函数。

2.2 代理签名人私钥进化算法及代理签名钥的产生

在这里我们采用了 Kan Zhang 不可否认代理签名方案中的代理签名钥生成协议,并且将代理签名人的私钥作为最终实际代理签名钥的一部分。具体实现如下:

(1)系统进入 i 时段$(0<i<T)$时,Alice 利用 $i-1$ 时段的密钥 $x_{A_{i-1}}$ 计算 $x_{A_i}=(x_{A_{i-1}})^2 \pmod{p-1}$,并立即从系统中删除 $x_{A_{i-1}}$,Bob 使用 $i-1$ 时段的密钥 $x_{B_{i-1}}$ 计算 $x_{B_i}=(x_{B_{i-1}})^2 \pmod{p-1}$,并立即从系统中删除 $x_{B_{i-1}}$。这时原始签名人和代理签名人的密钥对分别是$(y_A, x_{A_i})(y_B, x_{B_{i-1}})$。

(2)Alice 选择$\overline{k_i} \in_R Z_q$,计算$\overline{r_i}=g^{\overline{k_i}} \bmod p$,将$\overline{r_i}$传送给 Bob。

(3)Bob 选择 $k_i \in_R Z_q$,计算 $r_i=g^{k_i}\overline{r_i} \bmod p$,如果 $r_i \notin Z_q^*$,则重新选择 k_i,计算 r_i,将满足属于 Z_q^* 的 r_i 传送给 Alice。

(4)Alice 计算$\overline{s_i}=r_i x_{A_i}^{2^{(T+1-i)}}+\overline{k_i} \bmod q$,将$\overline{s}$传送给 Bob。

(5)Bob 计算 $s_i=\overline{s_i}+k_i \bmod q$,验证等式 $g^{s_i}=y_A^{r_i} r_i$,如果等式成立,接受 s_i。并计算代理签名钥 $x_{p_i}=x_{B_i}^{2^{(T+1-i)}}+s_i \pmod{p-1}$。

2.3 代理签名

在阶段 i,对要签名的任意消息 m,Bob 选择 $k_p \in_R Z_q$,计算 $r_p=g^{k_p} \bmod p$ 和 $s_p=k_p+x_{p_i}h(m, r_p, r_i, i) \bmod p-1$,然后将$(m, r_p, r_i, i, s_p)$传送给签名接受者或者签名验证者。

2.4 代理签名验证

签名接受者或签名验证者验证签名:$g^{s_p}=r_p(y_B y_A^{r_i} r_i)^{h(m, r_p, r_i, i)} \bmod p$,如果成立,则接受签名,这是因为:

$$g^{s_p}=g^{k_p+x_{p_i}h(m, r_p, r_i, i)}=r_p(g^{x_{p_i}})^{h(m, r_p, r_i, i)}=r_p(g^{x_{B_i}^{2^{T+1-i}}+s_i})^{h(m, r_p, r_i, i)}=$$
$$r_p(y_B y_A^{r_i} r_i)^{h(m, r_p, r_i, i)} \bmod p$$

3 新方案的安全性及有效性分析

可以看到,上述方案的代理签名钥产生,采用了 Kan Zhang 不可否认代理签名方案中代理签名钥产生协议的思想,上述强前向安全的方案具有下列性质:不可伪造性:只有代理签名者可以产生合法的代理签名,原始签名人 Alice 如果要假冒代理签名人 Bob 的签名,必须通过 $y_B y_A^r r=g^{x_p} \bmod p$ 计算 x_p,这是一个离散对数问题。可验证性:代理签名钥为原始签名人 Alice 和代理签名人 Bob 联合产生,Bob 在没有得到 Alice 的委托下,不能产生合法的签名,只要签名验证合法,即可认定 Alice 授权 Bob 进行代理签名。代理权可撤销性:代理签名人 Bob 无法独立产生代理签名钥,原始签名人 Alice 可以随时中止更新密钥的活动,从而达到撤销代理权的目的。强前向安全性:每个阶段的代理签名密钥是在原始签名人 Alice 和代理签名人 Bob 合力下产生的,在每个时段开始 Alice 和 Bob 都要进行密钥的更新,攻击者在 i 时段进入系统,要产生第 i 时段之前(不妨设为 $i-1$ 时段)的签名,意味着攻击者必须通过 $r_{i-1}=g^{k_{i-1}}\overline{r_{i-1}}=g^{k_{i-1}}g^{\overline{k_{i-1}}}=g^{k_{i-1}+\overline{k_{i-1}}} \bmod p$ 计算 $k_{i-1}+\overline{k_{i-1}}$ 计算,才能得到 $i-1$ 时段代理签名密钥,这同样需要求解离散对数问题。要产生第 i 时段之后的签名,则要同 Alice 进行通信,更新密钥,这样 Alice 会接收到来自 Bob 和攻击者两个私钥更新的请求,察觉出系统受到攻击,代理签名钥的更新阶段顺利完成保证了系统的安全性,从而达到强前向安全的目的。

4 结论

本文提出的新方案在代理签名的基础上,利用简便高效的密钥进化算法,通过原始签名人和代理签名人合作产生代理签名钥,实现了强前向安全的代理签名方案,它可以有效地保护密钥,最大限度减少密钥泄漏带来的损失,保护原始签名人和代理签名人的利益。(收稿日期:2005 年 11 月)

参考文献

1.R Anderson.Two remarks on public key cryptology[C].In:Fourth Annual Conference on Computer and Communications Security,ACM,1997

2.M Bellare,S miner.A forward-secure digital signature scheme[C].In:Advances in Cryptology-Crypto'99,volume 1666 of Lecture Notes of Computer Science,1999:431-448

3.Amos Fiat,Adi Shamir.How to prove yourself:Practical solutions to identification and signature problems[C].In:Advances in Cryptology-CRYPTO'86,volume 263 of Lecture Notes in Computer Sicence,1986:186-194

4.Mike Burmester,Vassillios Chrissikopoulos.Strong Forward Security[C].In:IFIP-SEC 2001 Conference,Kluwer Academics Publishers,2001:109-119

5.M Mambo,K Usuda,E Okamato.Proxy signature:Delegation of the power to sign messages[C].In:IEICE Trans Fundamentals,1996

6.K Zhang.Nonrepudiable proxy signature schemes.Manuscript,1997

(上接 95 页)

memory system[C].In:Proc the 38th IEEE International CompCon Conference,1993:528-537

4.Lenoski D,Laudon J,Gharachorloo Ketal.The directory based cache coherence protocol for the DA SH multiprocessors[C].In:Proc ISCA'90,Seattle,1990:148-158

5.Bailey S,Barton J,Lasinski Tetal.The NAS Parallel Benchmarks[R].NASA:Technical Report 103863,1993