两个前向安全的代理签名方案的安全性分析 *

夏祥胜[1,2], 洪 帆[1], 崔国华[1]
(1. 华中科技大学 计算机学院 信息安全系, 武汉 430074; 2. 武汉工业学院 计算机系, 武汉 430023)

摘 要: 针对最近一些学者提出的前向安全的代理签名方案和改进的前向安全的代理签名方案,给出了这两种代理签名方案的安全性分析,并指出它们是不安全的,均不具备前向安全性质。当代理人的私钥泄露后,前向安全的代理签名方案不能抵抗伪造攻击;而改进的前向安全的代理签名方案对攻击者来说仅利用公开的信息就可以实施伪造攻击。

关键词: 前向安全; 代理签名; 伪造攻击; 安全分析
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2009)02-0709-02

Security analysis of two forward secure proxy signature schemes

XIA Xiang-sheng[1,2], HONG Fan[1], CUI Guo-hua[1]
(1. *Dept. of Information Security, College of Computer Science, Huazhong University of Science & Technology, Wuhan* 430074, *China*; 2. *Dept. of Computer, Wuhan Polytechnic University, Wuhan* 430023, *China*)

Abstract: Recently, some researchers proposed a forward secure proxy signature scheme and an improved forward-secure proxy signature scheme. This paper analyzed the security of the two proxy signature schemes and pointed out they were insecure and had not the characteristic of forward security at all. The first scheme couldn't resist forgery attack while the secret key of the proxy signer was lost. If adversary knew some public information of the second scheme, he/she could forge proxy signature.

Key words: forward security; proxy signature; forgery attack; security analysis

代理签名是指原始签名人将自己的签名权利委托给代理签名人,由代理签名人代表原始签名人产生代理签名,其有效性由验证人验证和确认。自 Mambo 等人于 1996 年首次提出代理签名方案[1,2]以来,人们对代理签名的研究非常关注,取得了丰富的成果,已提出了许多代理签名方案,如代理环签名[3]、代理多重签名[4]、门限代理签名[5]等。一个代理签名至少应满足可验证性、不可伪造性、可区分性、不可否认性等安全性质。代理签名在电子现金、电子投票、移动代理及电子商务等方面有广泛的应用。但是,代理签名密钥或私钥的泄露,将会给系统带来灾难性的后果。为了将损失降低到最小,人们提出前向安全的签名机制来解决此类问题,其本质是数字签名的风险控制。1997 年,Anderson 首次提出前向安全的概念[6],前向安全数字签名的基本方法是把签名密钥的有效期(如一年)分成 T 个周期,在每个周期内使用不同的签名密钥产生签名,而验证签名的公钥在整个有效期内保持不变。即使当前周期的签名密钥被泄露,此周期之前所产生的签名依然有效。从而大大减轻了由于签名密钥泄露而给系统带来的损失。2005 年,王晓明等人首次将前向安全的概念引入代理签名体制[7],提出了一个前向安全的代理签名方案;2007 年,张晓敏等人提出了一个改进的前向安全的代理签名方案[8]。引入前向安全机制构造前向安全的签名方案成为研究热点之一[9,10]。

本文详细分析了文献[7,8]的方案,发现它们都不具有真正的前向安全特性。王的方案虽然实现了授权密钥的前向安全,但当代理人的私钥泄露后,任何人均可以实施伪造攻击,从而不具有真的前向安全性质。张的方案企图对代理人的私钥进行进化,以弥补王的方案只对代理签名密钥进化的不足,但仍然不具备前向安全的性质,是不安全的;攻击者甚至不用知晓代理签名人的私钥,亦可成功实施伪造攻击。

1 前向安全数字签名相关知识

1.1 文献[7]给出了前向安全的形式化定义

定义 若存在一个单向签名密钥更新算法 KeyUd,使得签名人可以在第 i 时间段将签名密钥由 σ_{i-1} 更新为 $\sigma_i = \mathrm{KeyUd}(\sigma_{i-1})$,并在不同的时间段内使用不同的签名密钥 σ_i 生成签名 $\mathrm{sign}(\sigma_i, m)$($m$ 是消息),而任何验证人均可用固定的公钥 y 及时间段的编号 i 验证等式 $\mathrm{ver}[y, i, \mathrm{sign}(\sigma_i, m), m] = \mathrm{true}$ 成立,则签名 $\mathrm{sign}(\sigma_i, m)$ 为一个前向安全数字签名。

1.2 前向安全数字签名的密钥进化过程

前向安全数字签名实现的一个关键问题是密钥进化,即寻找一个单向签名密钥更新算法 KeyUd,使得签名人可在第 i 时间段将签名密钥由 σ_{i-1} 更新为 $\sigma_i = \mathrm{KeyUd}(\sigma_{i-1})$。但目前构造方法单一,大多数基于模合数平方剩余难题[11,12],利用式 $\sigma_i = \sigma_{i-1}^2 \bmod n$(其中 n 为合数)将第 $i-1$ 时间段签名密钥 σ_{i-1} 更新为第 i 时间段签名密钥 σ_i。由于模合数平方剩余难题,即使 σ_i 泄露,也很难推出 σ_{i-1},从而保证签名的前向安全性。如

收稿日期: 2008-05-09; **修回日期**: 2008-07-26 **基金项目**: 国家自然科学基金资助项目(60403027);国家"863"高科技研究发展基金资助项目(301-1-3)

作者简介:夏祥胜(1968-),男,湖北武汉人,博士研究生,主要研究方向为数字签名理论、现代密码学(xiaxiangsheng@126.com);洪帆(1942-),女,教授,博导,主要研究方向为现代密码学、安全模型与访问控制;崔国华(1947-),男,教授,博导,主要研究方向为现代密码学、密钥管理.

何寻找更多单向密钥更新算法 KeyUd 来构造前向安全数字签名方案,仍将是一个值得研究的问题。

2 对王晓明等人所提方案的安全性分析

2.1 王晓明等人的前向安全代理签名方案

1)初始化阶段 系统选择一个安全的单向散列函数 $h(\cdot)$和安全的大素数 p_1、p_2、p'_1、p'_2、q 满足:$p_1 = 2qp'_1 + 1$, $p_2 = 2qp'_2 + 1$, $p_1 = p_2 = 3 \bmod 4$;令 $n = p_1p_2$,在模 n 的平方剩余集合中选择一个 q 阶生成元 g,公布(n,q,g,h)。原始签名人 A 的身份标志为 ID_A, A 随机选择 $k_A \in [1,n]$作为私钥,计算 $y_A = g^{k_A} \bmod n$ 作为公钥,选择(e,d)满足 $\gcd(e,\Phi(n)) = 1$, $ed \equiv 1 (\bmod \Phi(n))$,公布$(ID_A, Y_A, e)$。代理签名人 B 的身份标志为 ID_B, B 随机选择 $k_B \in [1,n]$作为私钥,计算 $y_B = g^{k_B} \bmod n$ 作为公钥,公布(ID_B, y_B)。

2)授权过程 A 选择时间周期 $1,2,\cdots,T$ 和代理终止时间 t,计算 $\sigma_0 = y_B^{k_A} \bmod n$ 以及 $Y = (\sigma_0^{2^{T+1}} y_A^{ID_B})^{-e} \bmod n$,公布 B 为其代理签名人及参数$(T,Y,t,ID_B)$。B 计算 $\sigma_0 = y_A^{k_B} \bmod n$ 并验证等式 $Y = (\sigma_0^{2^{T+1}} y_A^{ID_B})^{-e} \bmod n$ 是否成立,如果等式成立,则 σ_0 为代理签名密钥。

3)前向安全的代理签名产生过程 在第 j 个签名周期开始时,B 计算 $\sigma_j = \sigma_{j-1}^2$作为该时段的签名密钥,并删除前一个时段的签名密钥 σ_{j-1},$1 \leqslant j \leqslant T$。设待签名消息为 m,B 随机选择 $\alpha_j, \beta_j \in [1,n]$,计算 $r = g^{\alpha_j 2^{T-j+1}} \bmod n$, $z = \sigma_j g^{\beta_j} \bmod n$, $u = h(j \| m \| r_2 \| t)$, $s = \alpha_j - \beta_j e - k_B u \bmod q$,则前向安全的代理签名为$[j,(m,s,u,z,t)]$。

4)前向安全的代理签名的验证 验证人收到$[j,(m,s,u,z,t)]$后,首先验证 t 是否超过代理终止时间 t 如果超过,则认为签名无效;否则计算 $r' = (g^s z^e y_B^u)^{2^{T-j+1}} Y(y_A^{ID_B})^e \bmod n$,然后验证等式 $u = h(j \| m \| r' \| z \| t)$是否成立,若成立则代理签名有效。

2.2 对王晓明等人的前向安全代理签名方案的分析

该方案对 σ_0 进行进化是没有意义的。因为代理人 B 的私钥 k_B 在整个签名过程中并没有被删除,一旦泄露,任何人都可以像 B 一样计算 $\sigma_0 = y_A^{k_B} \bmod n$,进而可以伪造任意时段 j'的代理签名。分析如下:

如果代理人 B 的私钥 k_B 泄露,那么攻击者 C 就可以计算 $\sigma_0 = y_A^{k_B} \bmod n$,因为 $\sigma_{j'} = \sigma_0^{2^{j'}}$ 所以攻击者 C 就可以伪造任意时段 j'的代理签名密钥。在周期 j',C 随机选择$\overline{\alpha_{j'}}$、$\overline{\beta_{j'}}$计算:

$$\bar{r} = g^{\bar{\alpha}_{j'} 2^{T-j'+1}} \bmod n,\ \bar{z} = \sigma_0^{2^{j'}} g^{\bar{\beta}_{j'}} \bmod n$$

$$\bar{u} = h(j' \| m' \| \bar{r} \| \bar{z} \| t),\ \bar{s} = \bar{\alpha}_{j'} - \bar{\beta}_{j'} e - k_B \bar{u} \bmod q$$

则$[j'(m',\bar{s},\bar{u},\bar{z},t)]$为有效的代理签名,即$[j',(m',\bar{x},\bar{u},\bar{z},t)]$能通过验证人的验证。证明如下:

$$\bar{r}' = (g^{\bar{s}} \bar{z}^e y_B^{\bar{u}})^{2^{T-j'+1}} Y(y_A^{ID_B})^e =$$

$$(g^{\bar{\alpha}_{j'}} g^{-\bar{\beta}_{j'} e} g^{-k_B \bar{u}} \sigma_0^{2^{j'}} e g^{\bar{\beta}_{j'} e - k_B \bar{u}})^{2^{T-j'+1}} Y(y_A^{ID_B})^e =$$

$$g^{\bar{\alpha}_{j'} 2^{T-j'+1}} \sigma_0^{2^{T+1} e} (\sigma_0^{2^{T+1}} y_A^{ID_B})^{-e} (y_A^{ID_B})^e =$$

$$g^{\bar{\alpha}_{j'} 2^{T-j'+1}} \bmod n = \bar{r}$$

故

$$\bar{u} = h(j' \| m' \| \bar{r} \| \bar{z} \| t) = h(j' \| m' \| \bar{r}' \| \bar{z} \| t)$$

所以,$[j',(m',\bar{s},\bar{u},\bar{z},t)]$为有效的代理签名,攻击者 C 的伪造攻击成功。

因此,一旦代理签名人 B 的私钥 k_B 泄露,任何人都可以伪造代理签名,不诚实的代理人也可以否认他的真实签名,声称是其他人伪造他的签名,从而使代理签名不再具有不可伪造性、可区分性、不可否认性等安全性质。另外,即使像原始签名人一样知道 σ_0,不知道 k_B 也无法伪造代理签名,因此对 σ_0 进化是没有意义的。

3 对张晓敏等人所提方案的安全性分析

张方案是对王方案的改进,张晓敏等人认为王方案没有对代理签名者的私钥作进化,导致当代理签名者的私钥泄露后不具有前向安全性;但没有给出详细的证明,并提出了一个对代理签名者的私钥作进化的改进方案。张晓敏等人声称他们的方案具有真的前向安全性质,本文的分析显示张方案也不具有前向安全性。

3.1 张晓敏等人的改进的前向安全代理签名方案

1)系统初始化 n、p_1、p_2、p'_1、p'_2、q、g、$h(\cdot)$如王方案所述,$v \in Z_n^*$ 是一随机数,x_A、$x_B \in Z_n^*$ 分别是原始签名者和代理签名者的私钥; $y_A = x_A^{-v} \bmod n$, $y_B = x_B^{-v} \bmod n$ 分别是对应的公钥,系统将密钥有效期划分为 T 个时段,系统的公开参数是$(n, y_A, y_B, v, q, g, h(\cdot), T)$。

2)授权过程 原始签名者 A 选择代理终止时间 t,指定 B 为其代理签名者,然后计算 $a = g^{x_A} \bmod n$,公开(t, a, ID_B);如果代理签名者 B 愿意接受代理则计算并公布 $b = g^{x_B} \bmod n$。原始签名者 A 计算 $\sigma = b^{x_A} \bmod n$ 以及 $Y = \sigma^{-v2^{T+1}} y_A^{-1} \bmod n$,并公布 Y;代理签名者 B 计算 $\sigma = a^{x_B} \bmod n$,并验证 $Y = \sigma^{-v2^{T+1}} Y_A^{-1} \bmod n$ 是否成立,如果等式成立则接受 A 的授权。

3)前向安全的代理签名产生过程 在第 i 个周期开始时,代理签名者 B 首先进行密钥进化,计算 $x_{B_i} = x_{B_{i-1}}^2 \bmod n$,并立即删除 $x_{B_{i-1}}$,其中 $x_{B_0} = x_B$。

设签名消息为 m,B 选择 $k_i, \alpha_i, \beta_i \in_R Z_n^*$,计算:$r = g^{k_i} a_i \bmod n$, $w = g^{2^{T-i+1}} \bmod n$, $z = x_{B_i} \sigma^{2^i} g^{\beta_i} \bmod n$, $u = h(i \| m \| w \| r \| z \| t)$, $s = \alpha_i - \beta_i v - k_i u \bmod q$,消息 m 的前向安全的代理签名为(i,m,r,s,z,u,t)。其中 t 是签名时间。

4)前向安全的代理签名的验证 验证人收到(i,m,r,s,z,u,t)后,首先验证 t 是否超过代理终止时间 t,如果超过,则认为签名无效;否则计算 $w' = (g^s z^v r^u)^{2^{T-i+1}} y_A y_B^{2^{T+1}} Y \bmod n$,然后验证等式 $u = h(i \| m \| w' \| r \| z \| t)$是否成立,如果成立,则认为签名有效。

3.2 对张晓敏等人的改进前向安全代理签名方案的分析

该方案存在安全隐患,攻击者甚至在不知晓代理人私钥的情况下也可假冒代理人实施伪造攻击。由于 Y, y_A, y_B, T 公开,攻击者可以伪造任意周期 j 的代理签名,分析过程如下:

设签名消息为 m',在周期 j 攻击者选择 $k_j, \alpha_j \in_R Z_n^*$,计算

$$\bar{r} = g^{k_j} \bmod n,\ \bar{w} = g^{2^{T-j+1} \alpha_j} y_A y_B^{2^{T+1}} Y \bmod n,\ \bar{z} = 1 \text{(这里 } \bar{z} \text{ 取正整数 1)}$$

$$\bar{u} = h(j \| m' \| \bar{w} \| \bar{r} \| \bar{z} \| t'),\ \bar{s} = \bar{\alpha}_j - k_j \bar{u} \bmod q$$

其中 t'是签名时间。则$(j,m',\bar{r},\bar{s},\bar{z},\bar{u},t')$为有效的前向安全的代理签名。下面证明$(j,m',r,s,z,u,t')$能够通过验证人的验证。

(下转第 718 页)

享,用以验证服务器身份和向服务器加密传输数据),比较现有方案的开销有较大节省。

e)运行效率高。本方案生成的随机数 R_U、R_S 仅用于 hash 计算和身份验证,不需要其他存取,大大减少了服务器的开销,提高了服务器的运行效率。

f)验证强度提高。虽然运算次数和服务器开销减少,但验证强度较以前有所提高。客户端有 $PK_i(A)?$、$H_s=?h_i(R_S \| H'_i)$ 两次对服务器的验证;服务器端有 $H'_i \in ?list$、$SK(PK(H_{ss}, R_U))$、$H_{ss}=?h_i(H'_s R_U)$ 三次对客户端的验证。

g)登录灵活。并不像借助计数器的协议,用户只能使用特定的客户端才能通过认证,只要有识别指纹装置的客户端都可以。

4 结束语

本文在不降低安全性的前提下,基于挑战/应答模式,结合 hash 函数和公开密钥设计了一种新的能有效适用于网络环境的一次性身份认证方案。相比现有的挑战/应答的一次性口令方案,其能有效地克服现有方案开销大的弱点,减少加密算法和 hash 函数的计算次数,并且实现简单、执行效率高,可与应用系统(特别是安全系统如防火墙)集成,用于应用系统本身的身份认证,以增强应用系统的安全性。

参考文献:

[1] 孙克强,刘嘉勇,丁光华. 基于 Hash 函数和对称加密算法的一次性口令方案[J]. 信息与电子工程. 2007,5(6):449-452.

[2] AGI I, GONG Li. An empirical study of secure MPEG video transmission[C]//Proc of Symposium on Network and Distributed Systems Security. Washington DC: IEEE Computer Society, 1996:137-144.

[3] MAP LES T B, SPANOS G A. Performance study of a selective encryption scheme for the security of networked, real-time video[C]//Proc of the 4th International Conference on Computer Communications and Net-works. Washington DC: IEEE Computer Society, 1995:2-10.

[4] 王春枝,唐皓. 一种新型的一次口令机制与实现[J]. 科技文汇,2006,2(2):187-188.

[5] 汤鹏志,李黎青,左黎明. 基于 SHA 的一次性口令认证技术[J]. 华东交通大学学报, 2005,22(2):55-59.

[6] 王滨,张远洋. 一次性口令身份认证方案的分析与改进[J]. 计算机工程, 2006,32(14):149-150.

[7] 张宏,陈志刚. 一种新型一次性口令身份认证方案的设计与分析[J]. 计算机工程, 2004,30(17):112-114.

[8] 陈航,周剑岚,冯珊. 基于 SHA 和 RSA 算法实用有效的双向身份认证系统[J]. 计算机安全,2006,4(3):6-8.

[9] 刘刚,司渐美. 对一个双向身份认证方案的改进[J]. 计算机安全,2006,10(5):7-8.

[10] 刘涛,严楠,甘洁静. 基于 RSA 算法动态相互身份认证的设计[J]. 安徽工程科技学院学报,2006, 21(1):29-33.

[11] 宋金秀,杨秋翔. 一种一次性口令身份认证方案的设计与分析[J]. 山西电子技术, 2007(4):62-63.

[12] 李涛,曾英,甄姬娜. 一种新的基于动态口令的远程双向认证[J]. 信息安全,2007,23(11):38-40.

[13] 王涛,谢冬青,周洲仪. 一种新的双向认证的一次性口令系统 TAO-TP[J]. 计算机应用研究,2005,22(9):128-130.

[14] SHI Chang-gui, WANG Sheng-yi, BHARGAVA B. MPEG video encryption in real-time using secret key cryptography[C]//Proc of International Conference on Parallel and Distributed Processing Techniques and Applications. 1999: 2822-2828.

(上接第 710 页)

验证人收到 $(j,m',\bar{r},\bar{s},\bar{z},\bar{u},t')$ 后,首先验证 t' 是否超过代理终止时间 t,如果超过,则认为签名无效,否则计算:

$$\bar{w}'=(g^{\bar{s}}z^{\bar{r}}\bar{r}^{\bar{u}})^{2^{T-j+1}}y_A y_B^{2^{T+1}} Y \bmod n =$$
$$(g^{\bar{\alpha}_j}g^{-k_j\bar{u}}1^{v}g^{k_j\bar{u}})^{2^{T-j+1}}y_A y_B^{2^{T+1}} Y \bmod n =$$
$$g^{2^{T-j+1}\alpha_j}y_A y_B^{2^{T+1}} Y \bmod n = w$$

所以,等式 $u=h(j \| m' \| w' \| r \| z \| t')$ 成立,即 $(j,m'r,s,z,u,t')$ 能够通过验证人的验证,攻击者的伪造攻击成功。

因此,对张方案不用知晓任何私有信息,任何人都可以直接伪造代理签名,不诚实的代理人也可否认他的真实签名,声称是其他人伪造他的签名,从而使代理签名不再具有不可伪造性、可区分性、不可否认性等安全性质。张方案不仅不具有前向安全性质,且已不具备一般代理签名的安全性质,存在非常严重的安全隐患。

4 结束语

本文分别分析了由王晓明和张晓敏提出的两个前向安全代理签名方案的安全性,发现它们都不具有真的前向安全性质,均不能抵抗伪造攻击。张方案甚至已不具备一般代理签名的安全性质,攻击者可以无条件地实施伪造攻击。目前,大多数前向安全数字签名方案[13,14]并不具备真的前向安全性质,如何设计一个真的前向安全的签名方案仍是一个值得研究的困难问题。

参考文献:

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans on Fundamentals, 1996, E79-A(9): 1338-1354.

[2] MAMBO M, USUDA K, OKAMOTO E. Proxy signature for delegating signing operation[C]//Proc of the 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996: 48-57.

[3] ZHANG Fang-guo, SAFAVI-NAINI R, LIN C Y. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings[J/OL]. 2003. http://eprint iacr. org/2003/104.

[4] YI Li-jiang, BAI Guo-qing, XIAO Guo-zhen. Proxy multi-signature scheme: a new type of proxy signature scheme[J]. Electronics Letters, 2000, 36(6): 527-528.

[5] HSU C L, WU T S, WU T C. New nonrepudiable threshold proxy signature with known signers[J]. Journal of Systems and Software, 2001,58(9): 119-124.

[6] ANDERSON R. Two remarks on public key cryptology[C]//Proc of the 4th ACM Conference on Computer and Communications Security. New York: ACM Press, 1997: 151-160.

[7] 王晓明,陈火炎,符方伟,等. 前向安全的代理签名方案[J]. 通信学报,2005,26(11): 38-42.

[8] 张晓敏, 张建中. 一个改进的前向安全的代理签名方案[J]. 计算机工程, 2007, 33(21):140-141.

[9] KOZLOV A, REYZIN L. Forward-secure signature with fast key update[C]//Proc of the 3rd Interatinal Conference on Security in Communication Network. Berlin: Springer-Verlag, 2002:241-256.

[10] 李如鹏,于佳, 李国文,等. 高效撤销成员的前向安全群签名方案[J]. 计算机研究与发展, 2007,44(7):1219-1226.

[11] 王晓明, 符方伟, 张震,等. 前向安全的多重数字签名方案[J]. 计算机学报, 2004,27(9):1177-1181.

[12] 冯华熹,冯登国. 一个基于双线性映射的前向安全门限签名方案[J]. 计算机研究与发展,2007, 44(4): 574-580.

[13] 谭作文,刘卓军. 一个前向安全的强代理签名方案[J] . 信息与电子工程,2003, 1(4): 257-259.

[14] 秦波,王尚平,王晓峰,等. 一种新的前向安全可证实数字签名方案[J]. 计算机研究与发展, 2003, 40(7): 1016-1020.