动态(1,t,n)门限群签名方案

蓝才会
(西北师范大学 数学与信息科学学院,甘肃 兰州 730070)

摘 要:针对现有门限群签名的主要弱点:难以抵御部分成员的合谋攻击以及成员加入和注销需大量改变参数,结合了将签名成员分等级的思想,提出了一种新的动态 $(1,t,n)$ 门限群签名方案。该方案能有效地克服这些缺点,当成员加入或注销时,系统本身的参数和其他成员的密钥保持不变,并且还能追查签名者。

关键词:知识签名;门限签名;合谋攻击
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)01-0175-03

Dynamic $(1,t,n)$ Threshold Signature

LAN Cai-hui
(College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China)

Abstract: Many existing threshold group signature schemes have the weaknesses that they are difficult to resist the conspiratorially attack from part of members, and they change a lot of parameters when group members added or deleted. According to the concept of class in some signature application, propose a new dynamic $(1,t,n)$ threshold signature. The new scheme not only can avoid those weaknesses, but also can find out the subscriber after the event.

Key words: knowledge signature; threshold signature; conspiracy attack

0 引 言

群签名方案首次由 Chaum 和 Van Heyst 提出[1],在群签名方案中,每个成员都可以代表整个群体签名。考虑到某些应用需要群体中某些给定子集才可以代表整个群体签名,从而就有了门限签名方案[2~5];但有时有的应用更特殊,比如某个董事会由一名董事长和 n 名董事组成,一项提案要获得通过,必须有董事长和其余 $t(t<n)$ 名以上董事同意才行,并且若董事长不同意,则提案一定通不过。在这个例子中,董事长就是一名特权成员,正基于这种需求,提出一种 $(1,t,n)$ 门限签名方案。

该方案不仅能满足上述需要,而且克服了目前已提出的许多门限群签名方案的一些问题,其中最主要的缺点就是:部分成员可以合谋得到系统的秘密参数;群成员加入或注销时,需要大量改变系统参数和旧群成员的参数;门限值固定以及发生纠纷后,无法追查签名者。

收稿日期:2007-03-15
基金项目:甘肃省自然科学基金资助项目(3ZS051-A25-042)
作者简介:蓝才会(1977-),男(畲族),江西永丰人,硕士研究生,研究方向为信息安全、现代密码学。

1 方案的描述

方案采用了离散对数和知识签名的密码体制[6],包括初始化、门限签名的产生和签名验证三部分。初始化主要由一个可信中心 CA 负责选择系统参数和秘密参数;门限签名产生阶段主要包括一个特权成员签名、$t(t<n)$ 个普通成员(u_i)的签名以及一个群服务者(Clerk)把个人签名合成为群签名;签名验证负责验证群签名。

1.1 初始化

1)CA 首先选择 p 是一个安全的大素数,g,h 是 Z_p 中的乘法群 Z_p^* 的两个生成元。然后选择 a_0,b_0 作为私钥,计算 $y=g^{a_0},z=h^{a_0}g^{b_0}$,并且把 y,z 作为公钥发布。最后,选择一个安全的单向 Hash 函数和二个秘密多项式 $f(x)$ 和 $g(x)$:

$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_tx^{t-1}\bmod p$$

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\bmod p$$

2)CA 在 Z_p^* 中选取互异的 n 个数 x_i,计算 $f(x_i)$ 和 $g(x_i)$,通过安全信道传送 $f(x_i)$ 和 $g(x_i)$ 给普通成员 $u_i(i=1,2,\cdots,n)$,公布 $x_i,y_i=g^{f(x_i)}\bmod p$ 和 $z_i=h^{f(x_i)}g^{g(x_i)}\bmod p$。

3)CA 在 Z_p^* 中选取互异的 $n-t+1$ 个值 $x_j'(j=1,2,\cdots,n-t+1)$ 且不等于第二步所选择的 x_i,计算

$f(x_j') = d_j$，同时通过信道把 d_j 传送给特权成员，公布 x_j'。

1.2 门限签名的产生

假设有 t 个成员，不妨设为 $U_t = \{u_1, u_2, \cdots, u_t\}$ 和特权成员同意对消息 M 进行签名，则每个成员 $u_i \in U_t$ 完成以下步骤产生签名。

1) 每个成员 $u_i \in U_t$ 随机选择 $r_{1i} \in Z_p^*$，$r_{2i} \in Z_p^*$，计算：

(1) $t_{1i} = g^{r_{1i}} \bmod p$

(2) $t_{2i} = g^{r_{2i}} h^{r_{1i}} \bmod p$

(3) $c_i = \mathrm{Hash}(y \| z \| g \| h \| t_{1i} \| t_{2i})$

(4) $s_{1i} = r_{1i} - c_i f(x_i) \bmod p$

(5) $s_{2i} = r_{2i} - c_i g(x_i) \bmod p$

将 t_{1i}, t_{2i} 传送给其他普通成员和特权成员，$(c_i, s_{1i}, s_{2i}, y_i, z_i)$ 发送给特权成员。

2) 特权成员首先验证：

(6) $c_i = \mathrm{Hash}(y \| z \| g \| h \| g^{s_{1i}} y_i^{c_i} \| g^{s_{2i}} h^{s_{1i}} z_i^{c_i})$

当式(6)成立，且满足 $y_i \neq y_j, z_i \neq z_{j(i \neq j)}$ 以及 y_i 和 z_i 能在 CA 公布的参数中找到，再随机选 r_1, r_2 计算：

(7) $t_1 = g^{r_1} \bmod p$

最后将 t_1, t_2 传送给参与签名的普通成员 u_i。

3) 普通 u_i 收到 t_{1i}, t_{2i}, t_1, t_2 后，计算：

(8) $T_1 = t_1 \prod_{i=1}^{t} t_{1i} \bmod p$

(9) $T_2 = \prod_{i=1}^{t} t_{2i} \bmod p$

(10) $C = \mathrm{Hash}(g \| h \| y \| w \| T_1 \| T_2 \| M)$

(11) $s_i^1 = r_{1i} - C \times f(x_i) \times \prod_{j=1, j \neq i}^{t} \frac{-x_j}{(x_i - x_j)} \times \prod_{k=1}^{m-t+1} \frac{-x_k'}{(x_i - x_k')} \bmod p$

(12) $s_i^2 = r_{2i} - C \times g(x_i) \times \prod_{j=1, j \neq i}^{t} \frac{-x_j}{(x_i - x_j)} \bmod p$

将 C, s_i^1, s_i^2 发送给合成者。

4) 特权成员收到 t_{1i}, t_{2i}，计算：

(13) $T_1' = t_1 \prod_{i=1}^{t} t_{1i} \bmod p$

(14) $T_2' = \prod_{i=1}^{t} t_{2i} \bmod p$

(15) $C' = \mathrm{Hash}(g \| h \| y \| w \| T_1 \| T_2 \| M)$

(16) $s = r_1 - C' \times \sum_{j=1}^{n-t+1} d_j \times \prod_{i=1, i \neq j}^{n-t+1} \frac{-x_i'}{x_j' - x_i'} \times \prod_{k=1}^{t} \frac{-x_k}{x_j' - x_k} \bmod p$

5) 合成者收到所有的 C, s_i^1, s_i^2, C', s 后，首先验证：

(17) $C = C'$

(18) $(z^C) \times \prod_{i=1}^{t} g^{s_i^2} h^{s_i^1} h^s \bmod p = T_2$

当式(16)，(17)成立，然后计算：

(19) $S_1 = s + \sum_{i=1}^{t} s_i^1 \bmod p$

(20) $S_2 = \sum_{i=1}^{t} s_i^2 \bmod p$

则信息 M 的门限签名为 (C, S_1, S_2, M)。

1.3 门限签名的验证

签名验证者首先计算：

(21) $R = g^{S_1} y^C \bmod p$

(22) $T = g^{S_2} h^{S_1} z^C \bmod p$

然后验证：

(23) $C = \mathrm{Hash}(g \| h \| y \| w \| R \| T \| M)$

如果式(23)成立，则 M 的门限签名 (C, S_1, S_2, M) 有效。

1.4 身份识别

由于特权成员一定参加了签名，这里的身份识别就是在发生争执的情况下确定成员的身份，那么可以通过特权成员来判别某个化名的成员是否参加了这次签名。如需要识别成员的真实身份时，就把特权成员所掌握的信息 y_i 送给 CA，CA 根据保存的信息能识别出真实签名人的身份，也就是说本方案具有追踪性。

2 正确性证明

1) 签名验证人可以通过式(23)来验证门限签名的有效性。

证明：

$$R = g^{s_1} y^C = g^{s + \sum_{i=1}^{t} s_i^1} \bmod p\, y^C =$$

$$g^{r_1 - C' \times \sum_{j=1}^{n-t+1} d_j \times \prod_{i=1, i \neq j}^{n-t+1} \frac{-x_i'}{x_j' - x_i'} \times \prod_{k=1}^{t} \frac{-x_k}{x_j' - x_k} + \sum_{i=1}^{t} (r_{1i} - C \times f(x_i) \times \prod_{j=1, j \neq i}^{t} \frac{-x_j}{(x_i - x_j)} \times \prod_{k=1}^{n-t+1} \frac{-x_k'}{(x_i - x_k')})} \bmod p\, y^C$$

$$= g^{\sum_{i=1}^{t} r_{1i} + r_1 - Ca_0} \bmod p\, (g^{a_0})^C$$

$$= g^{\sum_{i=1}^{t} r_{1i} + r_1} \bmod p = T_1$$

同理可证 $T = T_2$；

于是有 $C = \mathrm{Hash}(g \| h \| y \| w \| R \| T \| M)$。

2) 签名合成者可以通过式(17)和式(18)来验证个体成员的合法性。

证明：式(17)只要没有成员和合成者篡改，显然是成立的。

$$(z^C) \times \prod_{i=1}^{t} g^{s_i^2} h^{s_i^1} h^s =$$

$z^{C}g^{\sum_{i=1}^{t}s_i^2}h^{s^1+\sum_{i=1}^{t}s_i^1} = z^{C}g^{-Cb_0+\sum_{i=1}^{t}r_{2i}\bmod p}h^{-Ca_0+r_1+\sum_{i=1}^{t}r_{1i}\bmod p}\bmod p = g^{Cb_0}h^{Ca_0}g^{-Cb_0+\sum_{i=1}^{t}r_{2i}\bmod p}h^{-Ca_0r_1+\sum_{i=1}^{t}r_{1i}\bmod p}\bmod p = g^{\sum_{i=1}^{t}r_{2i}\bmod p}h^{r_1+\sum_{i=1}^{t}r_{1i}\bmod p}\bmod p = T_2$

所以在每一个成员和特权成员诚实的情况下式(19)成立。

3) 特权成员可以通过式(6)来验证签名成员的身份。

证明:$g^{s_{1i}}y_i^{c_i} = g^{r_{1i}-c_if(x_i)\bmod p}g^{f(x_i)c_i}\bmod p = g^{r_{1i}}\bmod p = t_{1i}$

$g^{s_{2i}}h^{s_{1i}}z_i^{c_i}\bmod p = g^{r_{2i}-c_ig(x_i)\bmod p}h^{r_{1i}-c_if(x_i)\bmod p}h^{f(x_i)c_i}g^{g(x_i)c_i}\bmod p = g^{r_{2i}}h^{r_{1i}}\bmod p = t_{2i}$

所以 Hash($y \| z \| g \| h \| t_{1i} \| t_{2i}$) = Hash($y \| z \| g \| h \| g^{s_{1i}}y_i^{c_i} \| g^{s_{2i}}h^{s_{1i}}z_i^{c_i}$),即式(6)成立。

3　安全性分析

该方案的安全性是建立在离散对数和知识签名体制[6]之上的,这两种体制的安全性已被广泛认可,而且该方案可以抵制伪造攻击、合谋攻击以及易注销和加入成员等。

1)能抵制合谋攻击:因为任何签名都必须特权成员参与才能形成,利用特权成员来抵御非特权成员的合谋攻击。假设 n 个普通成员都是恶意成员,虽然可以重构出秘密多项式 $g(x)$,但是他们也不能重新构造群的秘密多项式函数 $f(x)$。因为要构造 n 阶的多项式,就必须有 $n+1$ 个秘密参数 $f(x_i)$,然而 n 个恶意群成员合谋也只有 n 个秘密参数 $f(x_i)$,所以他们不能重新构造群的秘密多项式函数 $f(x_i)$。恶意群成员如企图从求出的 b_0 去求 a_0 通过 y 和 z,需解离散对数问题,或通过 $s = r_1 - C' \times \sum_{j=1}^{n-t+1} d_j \times \prod_{i=1,i\neq j}^{n-t+1} \frac{-x_i'}{x_j' - x_i'} \times \prod_{k=1}^{t} \frac{-x_k}{x_j' - x_k} \bmod p$ 求 d_j,由于 r_1 是特权成员选择的随机数和存在 $m-t+1$ 个未知数 d_j,所以不可能求出每个 d_j。

2) 能抵制伪造攻击:在不知道私钥的情况下,根据知识签名体制的安全性我们知道,不可能伪造签名。就算是合成者通过接受到的参数 C, s_i^1, s_i^2, C', s 来伪造攻击也是不可能:如果通过 s_i^1, s_i^2, s 来求 $f(x_i), d_j$,由于方程中的 $r_{1i}, r_{2i}, r_i, f(x_i), d_j$ 都是未知数,一个方程中有两个或两个以上的未知数,所以求不出来,如果通过 S_1, S_2 求随机数之和,由于 $f(0)$ 和 $g(0)$ 不知道,根据知识签名可知 Clerk 也不能伪造。

3) 新成员 u_{n+1} 加入,CA 只需要为新成员选择三个随机整数 x_{n+1} 和 f' 以及 x_{n-t+2}'(要求和初始化中的 2)、3) 相同),并令 $f(x_{n+1})' = f'$,计算 $g(x_{n+1}), y_{n+1} = g^{f(x_{n+1})'}, z_{n+1} = h^{f(x_{n+1})'}g^{g(x_{n+1})}, f(x)' = f(x) + A(x-a_0)(x-x_1)\cdots(x-x_m)\bmod p$(其中 $A = \frac{f(x_{n+1})' - f(x_{n+1})}{\prod_{i=1}^{n} x_{n+1} - x_i}\bmod p$,显然有:$f(x_i)' = f(x_i)_{(1\leqslant i\leqslant n)}, f(0)' = f(0)$ 和 $d_j = f(x_j')'$,且将 $f(x_{n+1})', g(x_{n+1})$ 秘密传送给 u_{n+1},而 $d_{n-t+2} = f(x_{n-t+2})'$ 秘密发送给特权成员,同时公布 y_{n+1}, z_{n+1} 和 r_{n-t+2},而不需更改其他成员的密钥和参数。如果安全性要求不高,可以直接将 $g(x_{n+1}), f(x_{n+1})'$ 秘密传送给 u_{n+1} 即可。

4) 当注销某个群成员 u_i 时,CA 只需从公开参数中把 y_i, z_i 删除即可。

5) 当门限值 t 变成 t',当 $t' < t$ 时,只需要另选 $(t - t')$ 个 x_k'',且要求不同于 x_i 和 x_j',把计算的 $f(x_k'')$ 秘密传送给特权成员,同时公布 x_k'';当 $t' > t$ 时,CA 只需另选 $t' - 1$ 次多项式 $g(x)'$,要求 $g(0)' = g(0)$,计算 $g(x_i)'$ 并秘密传送给 u_i。

4　效率分析

方案能有效地实现成员的加入和注销,如果文献[5,7]要实现成员的加入和注销,首先需要重新选择多项式和私钥,然后重新计算普通成员和特权成员的私钥和公钥,再把相关的信息公布或秘密传送给相关成员。而本方案中,当成员加入时,只需计算一个多项式,再计算新加入成员的相关信息和特权成员的一个秘密值和对应的公开值即可,当成员注销,不需要作任何计算,只需把注销成员的相关信息删除,相比节省了计算时间和带宽。

5　结束语

这是一种 $(1,t,n)$ 门限签名方案,适用于那些需要一名决策者的情况,决策者拥有一票否决权和部分决定权,其他成员拥有部分决定权。事实上,这类情况在实际生活中是很多的。方案的安全性是建立在离散对数和知识签名体制之上,通过分析,方案可以抵制伪造攻击、合谋攻击,注销和加入成员不需要改变大量参数和签名者密钥以及可以动态地改变门限值。

参考文献:

[1] Chaum D, Van Heyst E. Group signatures[C]//In: Davies D

(下转第 180 页)

入侵数据有 4 大类,24 小类。分别是:DOS(Denial of Service) 攻击,例如 SYN 洪流;U2R(未授权的提升权限)攻击,例如各种缓冲区溢出攻击;R2U(未授权的远程登录) 攻击,例如猜测密码;PROBING 攻击,例如端口扫描。根据 Pal 等[7]的从聚类有效性角度考虑,设置 m 取值为[1.5,2.5],后续试验中 m 取 2.1 效果较好,故本算法令 $m = 2.1$。

2.2 样本的选取及实验结果

以随机方式重新建立 6 个样本集,每个集合包含 1000 个正常实例和 100 个入侵实例。在算法实现过程中忽略类标识属性,其仅供算法结果分析之用。实验样本集结构如表 1 所示。

表 1 实验数据结构

	实例数	正常实例数	入侵实例数	攻击类型数	分类攻击数
数据集 1	1100	1000	100	22	4
数据集 2	1100	1000	100	20	4
数据集 3	1100	1000	100	3	2
数据集 4	1100	1000	100	4	2
数据集 5	1100	1000	100	3	3
数据集 6	1100	1000	100	8	3

表 2 为仿真实验结果,其中包含两个重要检测性能参数:

表 2 实验结果

	正常实例数	入侵实例数	检测率	误检率
数据集 1	999	49	49%	0.1%
数据集 2	1000	41	41%	0%
数据集 3	986	100	100%	1.4%
数据集 4	994	50	50%	0.6%
数据集 5	1000	100	100%	0%
数据集 6	944	20	20%	5.6%
平均值	999.83	60	60%	1.283%

(1)检测率:$D_r = n_i/N_i$ 表示入侵行为的检测比例,其中 n_i 为检测出的入侵实例数目,N_i 为数据集中入侵实例总数。

(2) 误检率:$F_r = (N_i - n_i)/N_n$ 表示误将入侵判断为正常行为的比例,其中 N_n 表示数据集中正常实例数目。

这两项指标能充分反映算法的检测能力。在仿真实验中,入侵实例与正常实例之比为 10∶1 ,而平均检测率仍大于 50%,平均误检率保持约 1.3%。这充分表明算法对于未知攻击检测的可行性和有效性。

3 结 论

文中针对网络入侵的异常检测问题,利用基于模糊 C-均值聚类算法进行入侵检测。由于网络流量样本一般具有混合性属性,因此给出了一种新型的基于属性值范围的加权相似性度量方法。最后,利用 KDD Cup 1999 数据集对该算法进行了实验。实验结果表明,此算法异常入侵检测问题是可行、有效的,具有良好的可扩展性。

参考文献:

[1] 唐正军.网络入侵检测系统的设计与实现[M].北京:电子工业出版社,2002.

[2] 胡昌振.网络入侵检测原理与技术[M].北京:北京理工大学出版社,2006.

[3] Han Jiawei, Kamber M. Data Mining Concepts and Techniques [M]. [s.l.]: Morgan Kaufman, 2001.

[4] 罗 静,董 晟,华 鹏.一种基于克隆的模糊 C-均值入侵检测方法[J].微机发展,2004,14(3):107-109.

[5] 高新波.模糊聚类分析及其应用[M].西安:西安电子科技大学出版社,2004.

[6] KDD99. KDD99 cup dataset[DB/OL]. 1999. http://kdd.ics.uci.edu/databases/kddcup99.

[7] Pal N R, Bezdek J C. On clustering for the fuzzy c-means model[J]. IEEE Trans FS, 1995, 3(3): 370-379.

(上接第 177 页)

W, ed. Advances in Cryptology - EUROCRYPT'91. Berlin: Springer-Verlag, 1991: 257-265.

[2] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[3] Desmedt Y, Frankel Y. Threshold cryptosystems[C]//In: Advances in Cryptology - Crypto89, Lectures Notes in Computer Science 435. Berlin : Springer-Verlag, 1989: 307-315.

[4] Desmedt Y, Frankel Y. Shared generation of authenticators and signatures[C]//In : Advances in Crytology. Crypto'91. Berlin: Springer-Verlag, 1991: 457-469.

[5] Wang G. On the security of the Li-Hwang-Lee-Tsai threshold group signature scheme[C]//In: Proceedings of Information Security and Cryptology (ICISC 2002). Berlin: Springer-Verlag, 2003: 75-89.

[6] Camenisch J, Stadler M. Efficient Group Signature Schemes for Large Groups[C]//Advances in Cryptology - CRYPTO'97. [s.l.]: Springer-verlag, 1997: 410-424.

[7] 郭兴阳,张 权,唐朝京.一种动态门限群签名方案的安全性分析[J].国防科技大学学报,2005,27(4): 71-74.