等级安全系统中的一种新型访问控制方案

张建民,刘贤德,徐海峰
ZHANG Jian-min,LIU Xian-de,XU Hai-feng

华中科技大学 光电子工程系,武汉 430074
Huazhong University of Science and Technology,Wuhan 430074,China
E-mail:zjm1996@163.com

ZHANG Jian-min,LIU Xian-de,XU Hai-feng.New scheme for access control in hierarchy security systems.Computer Engineering and Applications,2007,43(16):156-158.

Abstract: It is significant in fact that access control schemes in hierarchy.In this paper,an access control scheme based on Hwang-Yang scheme has been proposed.It solves the security issues in Hwang-Yang scheme by using Chinese remainder theorem.This scheme needs smaller storage than Hwang-Yang scheme and its keys generation and derivation is more simple and efficient too.

Key words: hierarchy security system;access control;Chinese remainder theorem

摘 要:等级系统中的访问控制问题有着重要的实际意义。在 Hwang-Yang 方案的基础上提出了一个新的基于等级系统访问控制方案,该方案不仅利用中国剩余定理解决了 Hwang-Yang 方案中的安全问题,而且所需的储存空间更少,密钥的生成和导出的效率更加高效。

关键词:等级安全系统;访问控制;中国剩余定理
文章编号:1002-8331(2007)16-0156-03 **文献标识码**:A **中图分类号**:TP309

1 引言

在等级访问控制系统中,用户以及他所拥有的信息是严格分成安全等级的,等级高的用户类成员可以访问等级低的用户类的信息,而不允许等级低的用户类成员访问等级高的用户类信息。Akl 和 Tallor[1]第一次将密码技术应用于等级系统的安全访问控制,他们基本思想是:等级高的安全类用户可以利用自己私有的秘密信息和系统的公共信息导出等级低的安全类密钥,而等级低的安全类用户不能导出等级高的安全类密钥,从而实现了利用密钥分配进行等级系统的访问控制。

Akl-Tallor 的方案的优点是密钥产生和导出的算法简单,缺点是当系统中安全类的数目增多时,系统需要存储的公共信息量很大,而且添加/删除一个安全类或改编一些类的权限时,所需的计算量很大,后来许多工作者作了大量工作来改进 Akl 的方案,减少了系统需要存储的公共信息量,但没有解决安全类的动态管理问题[2],有的虽然解决了安全类的动态管理,但导出密钥时需要很大的计算量[3]。Harn and Lin 在文献[4]中提出中采用自第底向上的密钥生成方式,这样系统在实际应用中需要存储的公共信息较 Akl 的方案大大减少。后来 Hwang 和 Yang 在文献[5]中对 Harn-Lin 方案进行了改进,该方案不仅减少了所有的存储空间,运算性能也有所改进,而且也支持安全类的动态管理。然而 Wang 和 Laih 在文献[6]中指出了 Hwang-Yang 方案存在安全性问题。本文在 Hwang-Yang 方案的基础上提出了一个新的访问控制方案,该方案不仅解决了 Hwang-Yang 方案中安全问题,而且运算性能也有很大的提高。

2 等级系统访问控制的基本概念

假设 $C=\{C_1,C_2,\cdots,C_n\}$是等级系统中全部的安全类构成的集合,"≤"是 C 上的一个的偏序关系,如有 $C_j\leqslant C_i$,则表示安全类 C_i的安全级别高于 C_j,所以 C_i可以访问 C_j中的信息,反之则不行。当不存在 C_k使得 $C_j\leqslant C_k\leqslant C_i$成立,称 C_i是 C_j的直接前趋,C_j是 C_i的直接后继。否则称 C_i是 C_j的间接前趋,C_j是 C_i的间接后继。图 1 是一个等级系统偏序集的哈斯图,在图中 C_5是 C_{500}和 C_{502}的直接前趋,而 C_2是 C_{500}和 C_{502}的间接前趋。直接前趋和间接前趋合称为前趋,直接后继和间接后继合称为后继。如果 C_i和 C_j具有相同的直接前趋,则称 C_i和 C_j互为兄弟,如图 1 中 C_8到 C_{500}都互为兄弟。如果 C_i没有后继则称 C_j为叶结点,图 1 中 C_8到 C_{1000}都是叶结点。如果 C_i和 C_j都是叶节点且互为兄弟,则它们组成一个叶兄弟组。如图 1 中 C_8到 C_{1000}之间叶结点组成一个叶兄弟组。如果一个叶结点没有兄弟结

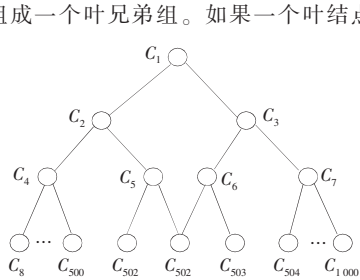

图 1 一个等级系统偏序集的哈斯图

作者简介:张建民(1970-),男,博士研究生,主要研究方向:BACnet 控制网络,控制网络安全;刘贤德,教授,博士生导师。

点,这里认为该叶结点自成一个叶兄弟组,如图1中C_{502}就自成一个叶兄弟组。

3 基于中国剩余定理的访问控制方案

假设等级系统中有n个安全类:$C_1,C_2,\cdots,C_n$,CA(Central Authority)是一个中央授权机构,它为每一个安全类用户生成秘密密钥和公共参数,一个安全类用户可以使用这些公共参数计算得到后继安全类用户的秘密密钥,进而可以访问后继安全用户类用户的信息。

3.1 中国剩余定理

设$m_1,m_2,\cdots,m_k$是两两互素,则同余方程组:$x\equiv b_k(\mathrm{mod}\,m_k)$ $i=1,2,\cdots,k$对模$M=m_1,m_2,\cdots,m_k$有唯一解:$x=\sum_{i=1}^{k}b_iM'_iM_i(\mathrm{mod}\,M)$。其中$M_i=M/m_i$,$M'$是满足$M'_iM_i\equiv1(\mathrm{mod}\,m_i)$。

3.2 密钥和公共参数算法

中央机构CA为每个安全类生成秘密密钥和公共参数的算法如下:

(1)CA秘密选择两个大素数p和q,计算出$n=pq$,p和q对所有用户保密,而n可以向用户公开;

(2)计算n的欧拉数$\Phi(n)=(p-1)(q-1)$;

(3)CA从$[2,n-1]$中选择一个与n互素的数K_0,K_0用来生成用户密钥;

(4)CA从$[2,\Phi(n)-1]$中选择m个素数$e_1,e_2,e_3,\cdots,e_m$,用公式$e_id_i=1\Phi(n)$分别计算出$d_1,d_2,d_3,\cdots,d_m$,d_i对所有的用户保密,而e_i可以对所有用户公开,(e_i,d_i)分别作为非叶结点C_i的秘密参数和公开参数;其中,m为系统中非叶结点的个数;

(5)计算非叶结点C_j的密钥K_j和公共信息PB_j:

$$K_j=K_0^{\prod d_l \bmod \phi(m)} \bmod n \tag{1}$$

$$PB_j=\prod e_l \tag{2}$$

其中d_l,e_l是C_j所有后续节点C_l的参数;

(6)计算叶结点密钥和公共信息:

假设$C_{i1},C_{i2},\cdots,C_{ik}$组成一个叶兄弟组,它们的共同直接前趋是$C_{j1},C_{j2},\cdots,C_{jt}$。

CA为该兄弟组的每个成员生成一个密钥$K_{i1},K_{i2},\cdots,K_{ik}$,同时CA还生成一个密钥$BK_i$作为该叶兄弟组的一个秘密参数。

叶兄弟组中每个叶结点公共参数为:

$$PB_{il}=K_{il}\oplus H(BK_i,C_{il}) \tag{3}$$

另外叶兄弟组的所有成员还有一个公用的公共参数:

$$BP_i=r_{j1}M'_{j1}M_{j1}+r_{j2}M'_{j2}M_{j2}+\cdots+r_{jk}M'_{jt}M_{it}(\mathrm{mod}\,M) \tag{4}$$

其中$M=e_{j1}e_{j2}\cdots e_{jt}=e_{j1}E_{j1}=e_{j2}E_{j2}=\cdots=e_{jt}E_{it}$,$E'_{jl}E_{jl}\equiv1(\mathrm{mod}\,e_{jl})$

$r_{jl}=BK_i\oplus K_{jl}$

其中$(e_{j1},K_{j1}),(e_{j2},K_{j2}),\cdots,(E_{jt},K_{jt})$是该叶兄弟组直接前趋$C_{j1},C_{j2},\cdots,C_{jt}$的公共参数和密钥,$H(x)$是单向哈希函数。

CA计算完各结点秘密密钥和公共参数后,公开所有的公共参数PB_i,e_i和BP_i,并把各个结点密钥K_i通过安全通道发送给对应的安全类用户。

3.3 密钥导出算法

等级系统中的任意一个安全类用户可以使用密钥导出算法计算其后继安全类用户的秘密密钥。安全类用户C_i获得其后继C_i的秘密密钥的过程如下:

假设安全类用户C_i的秘密密钥为K_i,公共参数PB_i;后继C_j的公共参数PB_j。如果后继U_j的是叶结点公共参数还包括BP_j。

(1)如果C_j是非叶结点

$$K_j=K_i^{(PB_i|PB_j)} \bmod n \tag{5}$$

(2)如果C_j是叶结点

第一步:计算C_j的一个直接前趋C_t的密钥K_t

$$K_t=K_i^{(PB_i|PB_t)} \bmod n \tag{6}$$

第二步:求出r_i

$$r_j=BP_j \bmod (e_t) \tag{7}$$

第三步:求出C_j所在叶兄弟组的秘密参数BK_j

$$BK_j=r_j\oplus K_t \tag{8}$$

第四步:根据K_t求出K_j

$$K_j=PB_j\oplus H(BK_j,C_j) \tag{9}$$

其中(PB_t,e_t)为C_j一个直接前趋C_t的公共参数。

3.4 安全类的动态管理

若要在一个现有的等级安全系统中添加一个安全类C_{n+1}:

(1)如果安全类C_{n+1}是非叶结点且它的直接后继中没有叶结点

这时CA给该新加的用户类生成(e_{n+1},d_{n+1}),计算出它的密钥K_{n+1}和公共参数PB_{n+1},同时更新它所有前驱的公共参数和密钥;

(2)如果安全类C_{n+1}是非叶结点且它的直接后继中有叶结点

CA除了执行(1)中的运算外,还要更新直接后继中叶结点所在叶兄弟组的公共参数BP_j;

(3)安全类C_{n+1}是叶结点且有兄弟结点

CA只需给该类分配一个密钥K_{n+1},并计算出它的公共参数;

(4)安全类C_{n+1}是叶结点且但没有兄弟结点

CA除了执行(3)中的运算外,还要更新它所有前驱的公共参数和密钥。

若要在一个现有的系统中删除一个安全类:

(1)如果删除的安全类是叶结点且没有兄弟,这时该删除安全类的直接前驱C_i就成为叶结点,CA给C_j生成一个密钥,根据C_j的直接前趋计算C_j的公共参数KP_j和叶兄弟组公用公共参数BP_j,并更新C_j所有前趋的密钥和公共参数;

(2)如果删除的安全类是叶结点而且有兄弟,这种情况CA只需要把该安全类的相关信息从系统删即可,此时对系统中其它安全类没有影响;

(3)如果删除的安全类是非叶结点且它的直接后继中没有

叶结点，这时情况 CA 把该安全类的相关信息从系统删除外，还要更新该安全类的所有前趋的密钥和公共参数；

(4)如果删除的安全类是非叶结点且它的直接后继中有叶结点，这时除了执行(3)中的运算外，还有更新它的直接后继中叶结点所在叶兄弟组的公共参数 BP_j。

4 方案性能分析

4.1 安全性能分析

本方案对等级系统安全类的处理分为两部分：第一是对非叶结点安全性的处理，第二是对叶结点安全类的处理。系统对非叶结点安全类的处理与 Hwang-Yang 方案中一样，这方面的安全性 Hwang-Yang 在文献[3]指出，只要系统的保密信息不泄露，就可以防止用户进行非法访问。Hwang-Yang 方案中的安全问题是由叶结点安全类的密钥生成方法引起的，为了减少素数的个数，Hwang-Yang 方案中采用类似 R.centti 等在文献[7]中的方法，把叶结点按照一定的规则分组，每组分配一定数目的素数，其中每个叶结点只拥有这些素数的一个真子集，并保证每两个叶结点拥有的素数真子集不同，这样每组所需素数的个数小于该组中叶结点的个数。S.Y Wang 等在文献[6]指出，该方案中同组的几个叶结点安全类的用户可以勾结起来，计算出同组其它叶结点安全类密钥。为了解决此问题，本文所提出的方案中叶结点的密钥是由 CA 直接分配，所以可以防止 Hwang-Yang 方案中几个叶结点安全类用户勾结其起来去进行越权访问。

本方案中对叶结点安全类信息的访问，要首先计算出叶结点的直接前趋的密钥，否则非法用户即使根据公共参数由公式(7)：$r_j=BP_j \bmod (PB_t)$，也无法用公式(8)：$BK_j=r_i \oplus K_i$ 计算出叶结点所在叶兄弟组的秘密参数 BK_j。从公式(9)：$K_j=PB_j \oplus H(BK_j, C_j)$ 可以看出，由于哈希函数 $H(x)$ 的单向运算性，即使叶结点安全类用户，也无法根据自己的密钥 K_j 和公共参数 PB_j 计算出秘密参数 BK_j，从而可以防止一个叶结点安全类的用户去非法访问其它叶结点安全类的信息。

4.2 空间复杂度和时间复杂度

设等级系统中共有 n 个安全类，Hwang-Yang 方案需要 x 个素数，本文提出的方案需要 y 个素数，从文献[3]中的公式(5)可以看出，x 除了包括非叶结点的个数外，还包括其它两项，而 y 只包括等级系统中非叶结点的个数，所以 y 大于小 x，例如对于图 1 的情况，x=42，而 y=7。Hwang-Yang 方案密钥生成算法的复杂度为 $O(x)$，密钥导出算法的复杂度为 O(1)，公共信息最大值为 $\prod_{i=1}^{x} e_i$，需要的存储空间复杂度为 $O(nx)$。而本文方案密钥生成算法的复杂度为 $O(y)$，密钥导出算法的复杂度为 O(1)，公共信息最大值为 $\prod_{i=1}^{y} e_i$，需要的存储公共参数空间复杂度为 $O(ny)$。综上所述，本文的访问控制方案较 Hwang-Yang 的方案具有较高的时间和空间效率。

5 结论

随着计算机资源，信息资源的共享的需求扩大，访问控制日益重要，在一些诸如政府、军队等部门，用户被严格地分成安全等级，为了在这种环境中充分共享资源，许多研究者做了大量工作，以实现访问控制。本文在 Hwang-Yang 方案的基础上提出了一个新的等级系统的访问控制方案，它不仅解决了 Hwang-Yang 方案的安全问题，而且与 Hwang-Yang 方案相比，需要更少的存储空间，密钥的导出也更为高效。

(收稿日期：2006 年 9 月)

参考文献：

[1] Akl S G,Taylor P D.Cryptographic solution to a problem of access control in a hierarchy[J].ACM Trans on Computer System,1983,1(3):239-247.

[2] Machinnon S T,Taylor P D.An optimal algorithm for assigning cryptographic keys to control access in a hierarchy[J].IEEE Trans compter,1985,34(9):797-802.

[3] Laih C S,Hwang T L.A branch oriented key management solution to dynamic access control in a hierarchy[J].IEEE Trans on Software Engineering,1991,17(3):422-429.

[4] Harn L,Lin H Y.A cryptographic key generation Scheme for multilevel data security[J].Computers & Security,1990,9.

[5] Hwang M S,Yang W P.Controlling access in large partially ordered hierarchies using cryptographic keys[J].The Journal of Systems and Software,2003,67:99-107.

[6] Wang S Y,Laih C S.Cryptanalysis of Hwang-yang scheme for controlling access in large partially ordered hierarchies[J].The Journal of System and Software,2005,65:189-192.

[7] Canetti R,Garay J,Itkis G,et al.Multicast security:a raxonomy and some efficient constructions[C]//IEEE INFOCOM'99,Mar,1999:708-716.

(上接 141 页)

[2] Lee B,Kim H,Kim K.Strong proxy signature and its applications[C]//Proc of the 2001 Symposium on Cryptography and Information Security(SCIS'01),2001:603-608.

[3] Shum K,Wei V-K.A strong proxy signature scheme with proxy signer privacy protection[C]//Eleventh IEEE International Workshop on Enabling Technologies:Infrastucture for Collaborative Enterprises (WETICE'02),Pittsburgh,Pennsylvania,USA,2002:55-56.

[4] Sun H-M,Hsieh B-T.On the security of some proxy signature schemes Crytology ePrint Archive,Report 2003/068[R/OL].[2003].http://eprint.iacr.org.

[5] Lee Narn-Yih,Lee Ming-Feng.The security of a strong proxy signature scheme with proxy signer privacy protection[J].Applied Mathematics and Computation,2005,161:807-812.

[6] 曹正军，刘木兰.数字签名方案中的孤悬因子和冗余数据[J].计算机学报，2006,29(2):249-255.