一种针对层次结构的安全动态存取控制方案*)

A Secure Dynamic Access Control Scheme for the Hierarchy Structure

施荣华

(中南大学信息科学与工程学院 长沙 410075)

Abstract Based on both the Rabin's scheme and the Chinese remainder theorem, this paper presents a secure access control scheme for the hierarchy structure. Compared to the existing access control schemes, the scheme's key generation algorithm and derivation algorithm of successor's keys are simple. In the scheme, the predecessor not only can efficiently derive secret keys of its successors, but also can withstand the attack of collusion. The scheme's dynamic feature is perfect. Moreover, each security class in hierarchy structure can freely select/change his own key without altering other keys present in the system.

Keywords Hierarchy structure, Rabin's scheme, Chinese remainder theorem, Dynamic access control, Key derivation algorithm

一、前言

在多用户计算机系统中,经授权对共享资源进行存取控制是很重要的。存取控制问题可以用一种用户层次结构描述[1]。层次结构中的存取控制问题本质上是密钥分配方案的选择问题[2]。

1983 年,AKL 和 TAYLOR 首先给出了一种基于层次结构的存取控制方案[3]。在该方案中,在 t_i 整除 t_j(记为 t_i/t_j)的前提下,当且仅当 $sc_j \leqslant sc_i$,可为每一个安全类分配一可公开的整数 t_i,那么,sc_i 可按 $sk_i = (\mathrm{mod\ m})\ sk_0^{t_i}$ 计算出密钥 sk_i。这里 sk_0 是认证中心(CA)密钥;m 是一对保密的大素数的积。如果 $sc_j \leqslant sc_i$,则 t_j/t_i 是一个整数并且 sc_i 能按下式导出 sc_j 的保密密钥 sk_j:

$$sk_j = sk_0^{t_j} = sk_i^{t_i * (t_j/t_i)} = sk_i^{(t_j/t_i)} (\mathrm{mod\ m})$$

相反,若 sc_j 与 sc_i 之间不存在关系"$\leqslant$",则 t_i/t_j 就不是一个整数并且不能导出 sk_j。

Akl-Taylor 方案的优点是密钥生成和密钥推导算法相当简单。然而存在几个缺点。首先,当层次结构中安全类的数量大时,得要求大量的存贮空间来存放公开参数 t_i;其次,动态特性不好,为了在已有系统中实现像加/减安全类及关系这样的动态存取操作,得重建整个系统;第三就是改变密钥相当困难。

于是,Mackinnon 针对 Akl-Taylor 方案给出了一种改进的方案[4],该方案的目的是减少 t_i 的值,进而减少存放 t_i 的存储空间。后来,Harn 提出了另一种改进方案,该方案使用自底向上方法来代替 Akl-Taylor 的方案中自顶向下的方法来生成密钥。结果这两种改进方案中 t_i 的值的确要比 Akl-Taylor 方案中的小。但这两种改进方案的动态特性都不好。除非改变密钥,不然在已有的用户层次结构系统中动态加/减安全类是不可能的。

为解决在已有的用户层次结构中能动态加/减安全类及用尽可能小的空间来保存公开参数信息 t_i,又出现了几种密钥分配方案[5~7]。但在这些方案中,拥有较高级别安全通行证的用户得反复执行密钥生成过程导出那些非直接后继者用户的密钥,并且导出的密钥有时是无效的。因此,为保证导出密钥的有效性,又产生了一些其它方案[8~10]。在这些方案中,允许用户改变他们的密钥并能有效地导出属于后继者的密钥,但计算又相当复杂。

为克服上述各类方案的缺点,本文基于 Rabin 方案和中国剩余定理给出了一种针对层次结构的安全存取控制方案。

二、Rabin 方案和中国剩余定理

2.1 Rabin 方案

1979 年,Rabin 提出一种针对 RSA 公钥系统的修正方案[12]。在该方案中,有一对加密密钥(b,m)和一对解密密钥(p,q)。Rabin 方案的关键是选择一对保密大素数(p,q)(即解密密钥),并令 $m = p * q$。加密计算:

$$C = \mathrm{E}(M) = M(M+b) \bmod m \qquad (1)$$

其中:M 是明文,C 是密文。解密计算:

$$M = -b/2 \pm \sqrt{(-b/2)^2 + C} \bmod p$$

$$M = -b/2 \pm \sqrt{(-b/2)^2 + C} \bmod q$$

显然,在 Rabin 方案中,加密函数是一个二次多项式,计算的是两个大素数(p,q)积的模;解密函数是一个平方根函数以计算这两个大素数(p,q)之一的模。

如果用户要导出密钥 SK(即明文 M),首先他得有解密过程的保密数据 p、q。换句话说,系统的安全性取决于两个大素数积的因式分解的计算难度,只要找到大素数对(p,q),就可攻破该方案。于是,为了保护系统的安全性,我们得给每一个安全类分配一个不同素数对。可按 Dirichlet 定理[12]生成不同的素数对。

根据 Dirichlet 定理,设 $b \geqslant 1$,则存在一整数 $r \geqslant 1$ 使得$(r * 2^b + 1)$是一个素数,也存在另一个整数 r' 使得$(r' * 2^b - 1)$是另一个素数。

在系统安全的前提下,为了生成自己的密钥(p,q),每一个安全类应拥有两个保密数据(r,r')及一个公开数 b。然而针对 u_i 来讲,占有其他所有后继者的信息元(r_j,r'_j)就像占有后

*)国家自然科学基金项目(批准号:60173041)和铁道信息科学与工程开放实验室项目(批准号:TDXX0205)资助。施荣华 教授,现从事计算机通信保密和计算机网络的研究工作。

继者的密钥(p_j,q_j)一样是不方便也是不安全的。因此，我们采用中国剩余定理来解决这一问题。

2.2 中国剩余定理[13]

设$n_1,n_2,\cdots,n_k$是两两互素的k个正整数，即$\gcd(n_i,n_j)=1(i\neq j)$。并令：$N=\prod_{i=1}^{k}n_i$。又设$r_1,r_2,\cdots,r_k$是k个正整数，则同余方程$x=r_i(\mathrm{mod}\ n_i),(i=1,2,\cdots,k)$，针对模$N$有唯一解：

$$x=\sum_{i=1}^{k}r_iy_i(\mathrm{mod}\ N)$$

其中：$y_i=h_i*(N/n_i)$，并且满足$y_i=1(\mathrm{mod}\ n_i)$

三、存取控制方案描述

在我们的方案中，密钥SK与识别码ID联接代替Rabin方案加密过程式(1)中的信息M，于是等(1)变换成：

$$C=(SK\amalg ID)((SK\amalg ID)+b)\bmod m \qquad (2)$$

其中："Ш"表示"联接"操作。显然，密钥SK能从式(2)中求得。

3.1 密钥生成算法

我们假定已有系统在用户层次结构中有n个安全类$sc_1,sc_2,\cdots,sc_n$。针对每一个安全类sc_i生成其密钥sk_i的算法如下：

Step 1：随机选取n个尽可能小的两两互素的素数$n_1,n_2,\cdots,n_n$。即$\gcd(n_i,n_j)=1(i\neq j)$。

Step 2：计算$N=\prod_{I=1}^{n}n_i$。

Step 3：用前序周游方式从层次结构中取一结点sc_i。

Step 4：认证中心(CA)为安全类sc_1随机选取三个正整数r_i、r_i'及b_i。

Step 5：CA再选择h_i使得$y_i=(N/n_i)*h_i(1\leqslant i\leqslant n)$，并满足$y_i=1(\mathrm{mod}\ n_i)$。

Step 6：CA再针对$sc_j\leqslant sc_i$计算每一个安全类sc_i的导出信息：

$$x_i=\Sigma_j(r_j\amalg r_j')*y_j-(r_i\amalg r_i')*y_i(\mathrm{mod}\ N)$$

Step 7：当安全类sc_i接收到数据(r_i,r_i',y_i,x_i)及其拥有的公开参数(b_i,n_i)时，执行以下步骤：

①计算$p_i=(r_i*2^{b_i}+1),q_i=(r_i'*2^{b_i}-1)$，并让$m_i=p_i*q_i$。并秘密保存$p_i$、$q_i$及$m_i$。

②为了方便，先选择一个密钥sk_i，再把sk_i与其相应的识别码ID_i联接，并让：$M_i=sk_i\amalg ID_i$，这里：$1\leqslant M_i\leqslant m_i-1$。

③计算公开信息$C_i=M_i*(M_i+b_i)\bmod m_i$。

Step 8：重复Step 3-Step 8步至直周游完层次结构的所有结点。

3.2 密钥导出算法

借助于sc_i任何后继者sc_j的公开信息$(b_j,n_j,c_j,)$，sc_i能导出其密钥sk_j，sc_i再用sk_j对sc_j拥有的信息体进行解密。sc_i推导sc_j的密钥sk_j的算法如下：

Step 1：计算$(r_j\amalg r_j')=x_i\bmod n_j$，并从中分别提取$r_i$与$r_i'$；

Step 2：计算$p_j=(r_j*2^{b_j}+1),q_j=(r_j'*2^{b_j}-1)$；

Step 3：计算四个平方根：

$$M_j=-b_j/2\pm\sqrt{(-b_j/2)^2+C_j}\bmod p_j$$

$$M_j=-b_j/2\pm\sqrt{(-b_j/2)^2+C_j}\bmod q_j$$

Step 4：按识别码ID_j，从明文$M_j=(SK_j\parallel ID_j)$中提取sk_j。

四、方案的动态存取控制特性描述

存取控制操作主要包括增加/删除安全类、增加/删除关系及改变密钥。

4.1 增加安全类

假定要加入新的安全类sc_{n+1}到已有层次结构系统中，CA修改的只是前驱的那些安全类sc_i的x_i，在该系统中所有其它密钥不变。CA执行以下几步：

Step 1：按中国剩余定理的要求，选择一个新的素数n_{n+1}，并证$N=N*n_{n+1}$；

Step 2：选择h_{n+1}使得$y_{n+1}=(N/n_{n+1})*h_{n+1}$，并满足$y_{n+1}=1(\mathrm{mod}\ n_{n+1})$；

Step 3：随机选取三个正整数r_{n+1},r_{n+1}'及b_{n+1}使得：

$$p_{n+1}=(r_{n+1}*2^{(b_{n+1})}+1)$$

$$q_{n+1}=(r_{n+1}'*2^{(b_{n+1})}-1)$$

并令：$m_{n+1}=p_{n+1}*q_{n+1}$；

Step 4：针对sc_{n+1}的所有前驱sc_i，CA增加新的安全类sc_{n+1}之后，使$x_i=x_i+(r_{n+1}\amalg r'_{n+1})*y_{n+1}(\mathrm{mod}\ N)$；

Step 5：计算：$x_{n+1}=\Sigma_{j\in J}(r_j\amalg r_j')*x_j-(r_{n+1}\amalg r'_{n+1})*y_{n+1}(\mathrm{mod}\ N)$。

其中：$J=\{j|(sc_j\leqslant sc_{j+1})\wedge\neg(sc_j\leqslant sc_i)\}$；

Step 6：计算：$C_{n+1}=(M_{n+1})*(M_{n+1}+b_{n+1})(\mathrm{mod}\ m_{n+1})$

其中：$M_{n+1}=sk_{n+1}\amalg ID_{n+1}$

4.2 删除安全类

为了在已有层次结构系统中删除安全类sc_k，CA将执行以下几步操作：

Step 1：$N=N/n_k$；

Step 2：CA删除sc_k之前，针对sc_k的所有前驱sc_i，计算：

$x_i=x_i-(r_k\amalg r_k')*y_k(\mathrm{mod}\ N)$；

Step 3：删除sc_k的保密数据(r_k,r_k',y_k,x_k)和公开参数(b_k,n_k)。

4.3 增加关系

假定在用户层次结构中sc_a与sc_b之间加入一个新的关系，使得$sc_a\geqslant sc_b$，则CA要执行以下几步：

Step 1：对$sc_b\leqslant sc_a$和$sc_j\leqslant sc_b$，计算：

$$x_a=x_a+(r_b\amalg r_b')*y_b+\Sigma_{j\in J}(r_j\amalg r_j')*y_j(\mathrm{mod}\ N)$$

其中：$J=\{j|(sc_j\leqslant sc_b)\wedge\neg(sc_j\leqslant sc_a)\}$

Step 2：针对有关系$sc_a\leqslant sc_i$的所有安全类sc_i，执行：

$$x_i=x_i+\Sigma_{j\in J}(r_j\amalg r'_j)*y_j(\mathrm{mod}\ N)。$$

其中：$J=\{j|(sc_j\leqslant sc_a)\wedge\neg(sc_b\leqslant sc_i)\wedge\neg(sc_j\leqslant sc_i)\}$

4.4 删除关系

假定要在用户层次结构中sc_a与sc_b之间删除一个关系，则关系$sc_b\leqslant sc_a$就不存在了。CA删除关系$sc_b\leqslant sc_a$之前，得执行以下几步：

Step 1：针对$sc_b\leqslant sc_a$和$sc_j\leqslant sc_b$，计算：

$$x_a=x_a-(r_b\amalg r'_b)*y_b-\Sigma_{j\in J}(r_j\amalg r'_j)*y_j(\mathrm{mod}\ N)$$

其中：$J=\{j|(sc_j\leqslant sc_b)\wedge\neg(sc_j\leqslant sc_a)\}$

Step 2：针对有关系$sc_a\leqslant sc_i$的所有安全类sc_i，计算：

$$x_i=x_i-\Sigma_{j\in J}(r_j\amalg r'_j)*y_j(\mathrm{mod}\ N)$$

其中：$J=\{j|(sc_j\leqslant sc_a)\wedge\neg(sc_b\leqslant sc_i)\wedge\neg(sc_j\leqslant sc_i)\}$

显然，CA仅需针对$sc_b\leqslant sc_i$重新计算公开参数x_i，而不用改变其它已有参数。

4.5 改变密钥

若要把安全类sc_i的密钥sk_i变成sk'_i，则仅需把公开信息

C_i 修改成：

$C_i=(sk_i' \amalg ID_i)((sk_i'+ID_i)+b_i)\bmod m_i$。而所有其它密钥或信息元不需要修改。

五、存取控制方案的安全特性分析[12~15]

在所给存取控制方案的密钥推导过程中，拥有秘密信息的任何安全类 sc_i 都能容易地导出其后继者的有效密钥；而仅知其前驱的公开信息(b_i,n_i,b_i)的后继者，要推导出其前驱的密钥，就得求解因子分解这一难题。

在层次结构系统中处于较低层的用户企图联合起来推导出较高层用户的密钥。由密钥生成算法的第(6)步，我们知道一些安全类的所有后继者仅能联合起来使用他们拥有的所有(r,r')和 y 获取该安全类的 x，即使他们获得了他们的前驱的 x，也不能获取该前驱的密钥 sk。因为他们只有在获知前驱的相应保密数据(r,r')之后，才能获取其前驱的密钥。

由 Dirichlet 素数定理，当 $b\geqslant 1$ 时，我们可以选择确定的正整数对(r,r')。于是，在我们的方案中应考虑如何选择这两个正整数(r,r')。

设(r,r')是两个 10 位数的正整数，于是，整个穷尽搜索空间需要 10^{20}位。假定每天针对 m_i 能搜索的空间是 10^{10}位，则整个计算时间是 10^{10}天。这样，所给方案的安全性取决于经仔细挑选所得的(r,r')。另外，可以把模数 n_i 选得小一点，因为这个值在我们的存取控制方案中是保密的，而不象 Rabin 方案，这个模数 n_i 是公开的。

参 考 文 献

1 San J K. Asingle-key access control scheme information protection system. Information Science, 1990, 51(1):1～11

2 Ham L, Lin H Y. A cryptographic key generation scheme for multilevel data security. Computer & Security, 1990, 9(3):539～546

3 Akl S G, Taylor P D. Cryptographic solution to a problem of access control in a hierarchy. ACM Trans. Comput. syst., 1983, 1(3):239～247

4 Mackinnon S T, Taylor P D, Meijer H, Akl S G. An optimal algorithm for assigning cryptographic keys to control access in a hierarchy. IEEE. Trans. comput, 1985, C-35 (9): 797～802

5 Sandhu R S. Cryptographic implementation of a tree hierarchy for access control. Inf. proc. lett., 1988, 27: 95～98

6 Chang C C, Hwang R K, Wu T C. Cryptographic key assignment scheme for access control in a hierarchy. Inf. Syst., 1992, 17(3): 243～247

7 Chang C C, Buehrer D J. Access Control in a hierarchy using a one-way trapdoor function. Comput. Math. with Appl., 1993, 26(5):71～76

8 Tsai H M, Chang C C. A Cryptographic implementation for dynamic access control in a user hierarchy. Comput. Secur., 1995, 14(2):857～959

9 Wu T C, Wu T S, He W H. Dynamic access control scheme based on the Chinese remainder theorem. Comput. Syst. Sci. Eng., 1995, 10(2):92～99

10 施荣华. 一种有效的动态密钥对分配方案. 小型微型计算机系统, 1997, 18(12):55～88

11 Rabin M O. Digitized Signatures and public-key function as intractable as factorization; [Technical Report]. MIT/ LCS/ TR-213 MIT Lab. For Computer Science, 1979

12 Ribenboim P. The book of prime number records, 2nd edn., Springer-Verlag, 1989

13 卢开澄. 计算机密码学. 清华大学出版社, 1998

14 施荣华. 一种针对 RSA 的冗余二进制算法. 计算机科学与技术学报(英文刊), 1996, 11(4):417～419

15 施荣华. 一种基于 Harn 数字签名的双向认证访问控制方案. 计算机学报, 2001, 24(4):400～404

(上接第 91 页)

表 3 各个项目的领先单位

单位	QA(28)	Web(23)	CLIR(16)	Filtering(13)
BBN Technologies			1	
CMU (卡内基－梅隆大学)				2
Fudan University(复旦大学)			3	3
Queens College, CUNY	2			
Justsystem Corp.		1		
MSRCN (微软中国研究院)			2	
MSRBR (微软英国研究院)				1
University De Neuchatel		3		
Ricoh(理光公司)		2		
Southern Methodist U.	1			
Waterloo University(滑铁卢大学)	3			

参 考 文 献

1 Lawrence S, Giles C L. Accessibility of Information on the Web. Nature, 1999, 400:107～109

2 Tomorrow's Top Five Software Categories, BYTE, Sep. 1995. 68～69

3 陈至立. 抓住机遇，加快发展，在中小学大力普及信息技术教育. 在全国中小学信息技术教育工作会议上的报告, 2000

4 Vooheers E M. Overview of the Seventh Text Retrieval Conference (TREC-8). http://trec.nist.gov, 2000

5 Voorhees E. Presentation to the Text REtrieval Conference (TREC-9)Gaithersburg, MD, USA, 2000

6 Robertson S, Hull D. the TREC-9 Filtering Track Final Report. In:Proc. of the Ninth Text Retrieval Conference(TREC-9), 2001