一种基于单向函数的双重认证存取控制方案 [1]

施荣华

(长沙铁道学院电子系 长沙 410075)

摘 要 本文基于单向函数针对信息保密系统提出了一种双重认证的存取控制方案。该方案与已有类似方案相比要更安全一些，因为在该方案中，用户保密密钥不仅用来计算对所需访问文件的存取权，也用于认证需访问保密文件的请求用户的合法性。该方案能够在动态环境中执行像改变存取权和插入 / 删除用户或文件这样的存取控制操作，而不影响任何用户的保密密钥。此外，该方案还具有建立简单的特点。

关键词 Diffie-Hellman 分钥方案，单向函数，双重认证，存取控制，信息保密系统

中图号 TN918.1

1 引 言

一个信息保护系统主要由以下几部分组成 [1]: (1) 一组主体； (2) 一组客体； (3) 一个存取控制矩阵。在存取控制矩阵中每一个元素 (i,j) 表示主体 i 对客体 j 的存取权。从表 1 中可以看出，用户 1 对文件 5 无任何访问权；用户 4 对文件 2 有改写权等。近些年来，有关学者提出了几种实现访问控制矩阵的方案 [1-4] 。在这些方案中，信息保护系统要经过复杂的计算才能建立起来，更不能容忍的是整个建立起来的信息保护系统在动态环境中，像改变访问权和插入 / 删除用户或文件等，要不断进行重建。这些方案的另一个普遍缺点是建好的信息保护系统不能抗击伪装者的攻击，也就是说不能对需要访问保护文件而请求进入系统的用户进行认证。本文为克服上述缺点，提出了一种基于单向函数的双重认证访问控制方案。

表 1 拥有 4 个用户和 5 个文件的存取控制矩阵

	文件 j					
用户 i	1	2	3	4	5	
1	4	4	1	2	0	1: 可读
2	2	2	1	0	3	2: 可写
3	0	1	4	3	3	3: 可执行
4	1	2	0	0	4	4: 可读、可写、可执行

2 单向函数和 Diffie-Hellman 公钥方案

2.1 单向函数的含义 单向函数 F 可以这样定义 [5,6]: (1) 在 F 的值域内，对于任意给定的 $x, F(x)$ 是容易计算的； (2) 对于某 x, 按 $y=F(x)$ 决定 y, 要找到 x 在计算上是不可行的，除非知道在设计函数 F 中所用的特殊信息。 Diffie-Hellman 公钥方案就是一著名的基于计算离散对数问题的单向函数。

[1] 1995-04-03 收到， 1996-06-26 定稿
铁道部青年科学基金项目资助课题

2.2 Diffie-Hellman 公钥方案 [7]　设 P 是一个大的素数，a 是一个本原元 (mod p)。设 k 是密钥，对应于 k 的公钥 y 可以这样计算：

$$y = a^k \bmod p. \tag{1}$$

显然，要根据 y 计算出 k 来就等同于在域 GF(p) 中计算离散对数问题，是非常困难的。

Diffie-Hellman 公开密钥分配方案，可以用来构造一个由两个通信者所共享的密钥。设 k_a 是用户 A 的密钥，y_a 是用户 A 的公钥。同样，设 k_b 是用户 B 的密钥，y_b 是用户 B 的公钥。根据 (1) 式，用户 A 和用户 B 所共享的密钥：

$$k_{ab} = a^{k_a k_b} \bmod p = y_b^{k_a} \bmod p = y_a^{k_b} \bmod p. \tag{2}$$

3 双重认证存取控制方案

3.1 信息保护系统的建立　设在信息系统中有 m 个用户，n 个文件。令 a_{ij} 是用户 i 对文件 j 的访问特权。先按 Diffie-Hellman 公钥方案为系统和用户分配各不相同的密钥和相应的公钥。　设 k_s 是系统的密钥，y_s 是系统的公钥；让 t_i 是用户 i 的密钥，y_i 是用户 i 的公钥。用户的密钥由它们自己保留。设 q 是比所有 a_{ij} 中最大值还要大的数。

过程建立

第一步　计算由系统和用户 i 所共享的密钥

$$k_{si} = y_i^{k_s} \bmod p, \quad i = 1, 2, \cdots, m; \tag{3}$$

第二步　计算

$$r_{ij} = ((k_{si} + j) \bmod q) \oplus a_{ij}, \quad i = 1, 2, \cdots, m; j = 1, 2, \cdots, n; \tag{4}$$

这里 $\oplus$ 是“异或”运算符。

第三步　将 y_i 和 r_{ij} 放入共同信息表中 ($i = 1, 2, \cdots, m$;　$j = 1, 2, \cdots, n$)。

过程建立的主要目的是构造由系统和用户所共享的密钥。与此同时，这些共享密钥也确定了各个用户的访问权 (针对每一个文件)。执行完过程建立后，可得表 2。

表 2 系统管理的共用信息表

	文件 j				
用户 (i, y_i)	1	2	⋯	⋯	n
$(1, y_1)$	r_{11}	r_{12}	⋯	⋯	r_{1n}
$(2, y_2)$	r_{21}	r_{22}	⋯	⋯	r_{2n}
⋮	⋮	⋮	⋯	⋯	⋮
⋮	⋮	⋮	⋯	⋯	⋮
(m, y_m)	r_{m1}	r_{m2}	⋯	⋯	r_{mn}

3.2 用户请求的合法性检验　共用信息表一旦建立起来，用户 i 就能给出他的密钥 k_i，请求系统以特权 a_{ij}^* 去存取所需的文件 j。检验用户 i 请求合法性的过程如下：

过程认证　(k_i, i, j, a_{ij}^*):

第一步　系统重新计算用户与系统的共享密钥

$$k_{si} = y_i^{k_s} \bmod p. \tag{5}$$

第二步 系统检查是否有

$$k_{si} = y_s^{k_i} \bmod p \tag{6}$$

来认证请求用户 i, 若不等，则拒绝用户 i 的请求并结束。

第三步 系统计算用户 i 对文件 j 的存取特权：

$$a_{ij} = ((k_{si} + j) \bmod q) \oplus r_{ij}. \tag{7}$$

第四步 系统检查用户 i 提供的对文件 j 的特权 a_{ij}^* 是否与 a_{ij} 相同。若相同，则接收请求；否则拒绝请求。

利用“异或”运算的特性，(7) 式明显可由 (4) 式导出。借用于共享公共密钥，过程认证不仅用于计算存取特权，而且也用于拒绝一些企图非法访问保护文件的入侵。根据过程认证，如果某个入侵者伪装成用户 i 并请求系统存取特定的保护文件，他得先给出正确密钥 k_i 以便通过过程认证第一步的测试。而根据 Diffie-Hellman 公钥方案，要由 y_i 计算出 k_i 的困难性等于在 GF(p) 域中计算离散对数的困难性。于是，过程建立和过程认证构造出一个使得 $r_{ij} = F(k_i, y_s, a_{ij})$, $a_{ij} = F(k_s, y_i, r_{ij})$ 的单向函数。

3.3 双重认证存取控制方案的运作实例 下面的例子说明了过程建立和过程认证是怎样运作的。

考虑一个拥有存取控制矩阵如表 1 所示的信息系统，并设 $a = 2, p = 19, q = 5, k_s = 4, k_1 = 2, k_2 = 3, k_3 = 5, k_4 = 7$ 。根据 (1) 式可算出： $y_s = 16, y_1 = 4, y_2 = 8, y_3 = 13, y_4 = 14$; 根据 (2) 式可算出： $k_{s1} = 9, k_{s2} = 11, k_{s3} = 17, k_{s4} = 17$ 。系统执行过程建立之后，便可得到共用信息表 3 。系统依据表 3, 由 (7) 式可计算出用户 i 对文件 j 的访问权 a_{ij} 。如：

$$\begin{aligned} a_{22} &= (((y_2^{k_s} \bmod p) + 2) \bmod q) \oplus r_{22} = (((8^4 \bmod 19) + 2) \bmod 5) \oplus 1 \\ &= ((11 + 2) \bmod 5) \oplus 1 = 3 \oplus 1 = (011)_2 \oplus (001)_2 = (010)_2 = 2 \end{aligned}$$

显然与表 1 中的 a_{22} 相符。同理，也可用 (7) 式来检验其它的权限 (a_{ij}) 。

表 3 实例中的公用信息表

	文件 j				
用户 (y, y_i)	1	2	3	4	5
(1, 4)	4	5	3	1	4
(2, 8)	0	1	5	0	2
(3, 13)	3	5	4	2	1
(4, 14)	2	6	0	1	6

4 双重认证方案的动态存取控制特性

现在，考虑我们的双重认证方案在动态环境的存取控制特性。分别说明如下：

第一 把用户 i 对文件 j 的存取权改为 a_{ij}^* 。系统只要计算： $r_{ij}^* = (((y_i^{k_s} \bmod p) + j) \bmod q) \oplus a_{ij}^*$, 并把公用信息表的变元 r_{ij} 改为 r_{ij}^* 即可。

第二 从系统中删除用户 t 。系统只要删除 y_t 和从公用信息表中删除所有的 $r_{tj} (j = 1, 2, \cdots, n)$ 即可。

第三 从系统中删除文件 t 。系统只要从公共信息表中删除所有 $r_{it} (i = 1, 2, \cdots m)$ 即可。

第四 把文件 t 插入到系统中。系统先计算： $r_{it} = (((y_i^{k_s} \bmod p) + t) \bmod q) \oplus a_{it}$ $(i = 1, 2, \cdots, m)$. 再把所算得的所有 r_{it} 填入公用信息表中即可。

第五　把一用户 t 插入到系统中。系统先分配一特定的密钥 k_t 给用户 t 并计算出相应的公钥 y_t 。然后计算： $r_{tj}=(((y_t^{k_s} \bmod p)+j) \bmod q) \oplus a_{tj}$　$(j=1,2,\cdots,n)$ 。再把所计算得的所有 r_{tj} 填入公用信息表中即可。为安全起见，系统为用户 t 分配的密钥 k_t 不应是系统中已分配出去的密钥。

5　双重认证存取控制方案的复杂性说明

我们的双重认证存取控制系统的建立仅需要 (k_s-1) 次乘法，一次加法，两次模运算和一次“异或”操作。为了检验一次存取请求，它仅需要 $[(k_s-1)+(k_i-1)]$ 次乘法，一次加法，两次模运算和一次“异或”操作。

参　考　文　献

[1] Chang C C. On the design of a key-lock-pair mechanism in information protection systems, Bit, 1986, 26(4): 410–417.

[2] Chang C C. An information protection scheme based upon number theory, The Computer Journal, 1987, 30(3): 249–253.

[3] Jan J K. A single key access control scheme in information systems. Information Science, 1990, 51(1): 1–11.

[4] Laih C S, Harn L, Lee J Y. On the design of single-key-lock machanism base on Newtens interpolating polynomials. IEEE Trans. on SE, 1989, SE-15(5): 1135–1137.

[5] Williams H C. Computationally, 'hard' problems as a source for cryptosystems, In secure Conmmnmications and Asymmetric Cryptosystems, AAAS selected Symposium 69. Colorado: Westview Press, 1982, 11–39.

[6] 施荣华. 一种基于牛顿插值方法的动态密钥分配方案. 长沙铁道学院学报, 1994 年 12 月 (增刊): 45–49.

[7] Diffie W, Hellman M E. New directions in Cryptography IEEE Trans. on IT, 1976, IT-22(6): 644–654.

AN AUTHENTICATION-DOUBLED ACCESS CONTROL SCHEME BASED ON ONE-WAY FUNCTION

Shi Ronghua

(*Changsha Railway University, Changsha* 410075)

Abstract　Based on a one-way function, this paper proposed an authentication-doubled access control scheme for information protection system. The scheme is safer than the previously proposed schemes. In the scheme, the user's secret key is used not only for computing the corresponding access privilege to the intended file, but also for authenticating the requesting user not to illegitimately access the protected file. The scheme can perform the access control in dynamic environments, such as change access priviledges and insert/delete users or files. Beside, the scheme is simple to establish.

Key words　Diffie-Hellman public key distribution scheme, One-way function, Authentication-doubled, Access control, Information protection system

施荣华：　男，1964 年生，副教授，现从事计算机网络与计算机通信保密的教学和研究工作.