计算机科学 1995 Vol. 22 №. 3

基于欧拉定理的文件保护方案

林宣雄 李怀祖 张文修
(西安交通大学管理学院 西安 710049)

摘 要 This paper proposes a new mechanism for access control based upon Euler's theorem. With this mechanism, once access privileges of object are assigned to subjects, then the locks and keys, corresponding to the objects and subjects, respectively, can be decided automaticaly. And when an access attempt is made, the subject access right upon an object can attained by simple calculation with his key and its lock without retrieving any table. So it is a reasonable access control method.

关键词 Information security, Euler's theorem, Access control.

一、引 言

建立在单机单用户环境下的信息系统，其信息保护比较容易实现，在分时多用户环境下，其信息保护的实现就相对复杂一些，而在网络共享、集中/分布式环境下，其信息保护所涉及的范围广、所需考虑的问题多，是一个复杂的系统工程。本文讨论在UNIX环境下以TCP/IP为互连协议的网络系统的信息保护。

信息保护可以归结为文件保护，规定文件的密级，确定用户的权限，允许授权用户访问合适的文件，阻止非授权用户的越权、侵权访问就实现了对文件中信息的保护。

UNIX系统使用了控制信息码技术来实现文件的接入控制(Access Control)，在UNIX中，按文件将主体(Subject)分为三类，即文件主、与文件主同组的用户以及其它用户。这样当用户分组有交叉时就出现了问题，主要缺点是不能对个别用户限定接入权，因而常会使某些原来不想让其接入某文件的用户，由于其所在组有权接入而导致接入该文件。本文提出了一个新的基于欧拉定理的接入控制方法，每一个合法用户被赋予一个数字钥，每一个受保护的文件被给定一个数字锁。通过简单的运算，用户接入某文件的接入权限就能够被决定。这样在UNIX环境下，在SHELL级上实施这种接入控制，就能确保整个系统的信息安全。

二、基于接入控制矩阵的抽象模型

在UNIX系统中，共享是不可避免的，重要的是让系统知道对系统中每一个受保护的客体(Object)，每个主体具有的接入权。接入控制矩阵(图1)能够表示主体与客体之间的各种接入关系。

用户 \ 文件	File 1	File 2	File 3	File 4	File 5
User 1	R	W	O	—	O
User 2	W	R	R	O	R
User 3	R	O	—	O	R
User 4	R	—	R/W	R	—

R:读，W:写，O:文件主，—:没有接入关系

图1 简单的接入控制矩阵

在图1中有4个用户(Subject)、5个文件(Object)。User1是File3的拥有者，User2可以读该文件，User4可以读写该文件，File4由User2和User3共同拥有，User1可以将File3的写权限授给User2，User1也可以请求User2和User3给予File4的读权限。改变接入控制矩阵中权限的过程就称做动态的接入控制或者说是接入控制矩阵的动态使用。

图1所示的接入控制矩阵规定了各个用户对于每一个文件的接入权限，文件主对于文件既有读写权，也具有授予权，而某用户对某文件既不是拥有者

林宣雄 在职博士生，主要从事计算机安全、信息系统安全和计算机网络等研究。李怀祖 博士生导师，主要从事决策理论、决策专家系统方面的研究。张文修 博士生导师，主要从事模糊数学与集值随机过程及信息论与或然逻辑等的研究。

又没有读写权，表明该用户不可接入该文件，即没有最低的接入权限。如果系统中有 n 个文件，m 个用户就可以构成一个 n 列 m 行的接入控制矩阵。对于拥有众多用户、众多文件的系统，相应的接入控制矩阵就变得非常大，文[1][2][3]提出了几种不同的实现技术。

三、钥-锁机制

钥-锁机制可以用图 2 来描述。

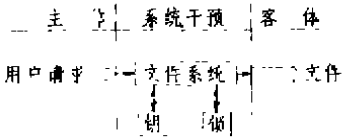

图 2 钥-锁机制

对于每个用户，其访问文件的每一个企图都被系统所截获并进行合法性检查。截获和检查的过程对用户是透明的。文件系统为每个文件分配一个锁，当一个用户加入到系统中的时候，系统就要决定其对已存文件的接入权限。系统为每一个用户产生一个钥，有了这个钥，用户就可以在规定的权限内访问文件。

表 1 给出了一个有 5 个用户、6 个文件的简单系统的接入控制矩阵。用户 i 访问文件 j 的请求仅当其权限与矩阵中的(i,j)项的属性值 a_{ij} 匹配时才被允许。

表 1 $A_{5,6}$ 接入控制矩阵

用户 i \ 文件 j	1	2	3	4	5	6
1	2	4	1	4	4	0
2	1	2	2	1	2	1
3	2	0	3	3	3	0
4	1	4	2	1	2	3
5	3	0	4	2	2	1

0：不可接入，1：执行，2：读，3：写，4：文件主

Wu 和 Hwang[3]设计了一种接入方法。在这种方法中，每个用户都被分配一个 n 位的数字钥 K_i，每个文件被分配一个 n 位的数字锁 L_i。当 $K_i * L_j \geqslant a_{ij}$ 时，接入被允许。这里钥值和锁值的乘积是域 GF(t)中的内积。t 是大于接入控制矩阵中所有属性值和文件个数的最小素数。在表 1 中，所有属性值 $a_{ij}<5$，文件个数等于 6，因而 t=7。

如果选择 5×5 非奇异的具有伪随机入口的矩阵 K(如下所示)：

$$K=\begin{bmatrix}4&2&1&3&0\\5&0&1&2&0\\3&4&0&1&3\\2&0&1&3&4\\2&1&1&1&4\end{bmatrix}$$

那么就可以确定 5 个用户的数字钥为：

$K_1=(4,2,1,3,0)$；$K_2=(5,0,1,2,0)$；

$K_3=(3,4,0,1,3)$；$K_4=(2,0,1,3,4)$；

$K_5=(2,1,1,1,4)$。

为了决定文件的数字锁，可以假定文件 j 的数字锁为 $L_j=(x_{j1},x_{j2},x_{j3},x_{j4},x_{j5})$。对于文件 1 的锁可以得到以下 5 个方程式：

$$2\equiv 4x_{11}+2x_{12}+1x_{13}+3x_{14}+0x_{15}\pmod 7$$
$$1\equiv 5x_{11}+0x_{12}+1x_{13}+2x_{14}+0x_{15}\pmod 7$$
$$2\equiv 3x_{11}+4x_{12}+0x_{13}+1x_{14}+3x_{15}\pmod 7$$
$$1\equiv 2x_{11}+0x_{12}+1x_{13}+3x_{14}+4x_{15}\pmod 7$$
$$3\equiv 2x_{11}+1x_{12}+1x_{13}+1x_{14}+4x_{15}\pmod 7$$

在 GF(7)中解上述方程式得 $L_1=(4,2,3,0,1)$，类似地可以求得 $L_2=(1,1,2,1,2)$；$L_3=(6,1,1,3,2)$；$L_4=(2,5,1,2,1)$；$L_5=(3,2,6,1,2)$；$L_6=(2,0,3,1,0)$。

当根据接入控制矩阵决定了用户的钥和文件的锁后，系统就可以根据用户的钥来决定是否可以接入某个文件。即判定 $K_i * L_j$ 是否等于矩阵中第(i,j)项的值，若等于则接入，否则予以拒绝。

这种方法有三大缺点：(1)存贮钥和锁的空间超过原始接入控制矩阵所占的空间；(2)钥-锁操作繁琐；(3)构造钥和锁并不简单。

四、基于欧拉定理的钥-锁机制

Wu 和 Hwang 的方法占用空间大，钥锁构造和操作费时繁琐，为此本文提出了一个简单省时且占空间少的钥锁构造和操作的方法。该方法中的接入控制矩阵与 Wu 和 Hwang 所使用的接入控制矩阵相同，只是构造用户钥、文件锁以及计算用户对于文件的接入权限的方法不一样。用户接入权限由 $\lfloor K_i/L_j \rfloor \pmod n$ 决定，其中 K_i(自然数)为用户 i 的钥，L_j(自然数)为文件 j 的锁，n 为文件个数，$\lfloor\ \rfloor$ 为舍去取整操作(例$\lfloor 1.9 \rfloor=1$)。这是一种基于欧拉定理的钥-锁方法。

定理 4.1(欧拉定理) 设 a,b 互素，即(a,b)=1，则有

$$a^{\varphi(b)}\equiv 1\pmod b \qquad (1)$$

其中 $\varphi(\cdot)$ 为欧拉函数。

证明　见华罗庚"数论导引"，(科学出版社)。

定理 4.2　设 $A_{m\times n}$ 是接入控制矩阵，矩阵中第 (i,j) 项 a_{ij} 是用户 i 对于文件 j 的接入权限，这里 $i=1,2,\cdots,m$，$j=1,2,\cdots,n$，设 $L=\{L_1,L_2,\cdots,L_n\}$ (L_i 是自然数，$i\leqslant n$) 是文件锁的集合，$(L_i,L_j)=1,\forall i,j\in 1,2,\cdots,n$，且 $i\neq j$，$\mathrm{Min}\{L_j\}\geqslant n>\mathrm{Max}\{a_{ij}\}$。其中 $i=1,2,\cdots,m$，$j=1,2,\cdots,n$，如果取

$$K_i=\sum_{j=1}^{n}N_{ij}\cdot n\cdot\Big(\prod_{\substack{i=1\\ i\neq j}}^{n}L_i\Big)^{\varphi(L_j)}\quad(i\leqslant m)\qquad(2)$$

则有

$$a_{ij}\equiv\lfloor K_i/L_j\rfloor(\mathrm{mod}\ n)\quad(i\leqslant m,j\leqslant n)\qquad(3)$$

其中 $N_{ij}=\left\lceil\frac{a_{ij}\cdot L_j}{n}\right\rceil$，$\lceil\ \rceil$ 为舍入取整操作(例 $\lceil 1.1\rceil=2$)。

证明(略)

例　假设一个简单的系统，有 4 个用户，3 个文件，其接入控制矩阵如表 2 所示。

表 2　$A_{4\times3}$ 接入控制矩阵

文件 j / 用户 i	1	2	3
1	1	2	1
2	2	0	1
3	0	2	1
4	2	1	0

根据定理 4.2，为文件选择两两互素的锁，$L_1=3$，$L_2=4$，$L_3=5$，由式(2)可计算用户 1 的钥如下：

$$K_1=\sum_{j=1}^{3}N_{1j}\cdot 3\cdot\Big(\prod_{\substack{i=1\\ i\neq j}}^{3}L_i\Big)^{\varphi(L_j)}$$

$$=\sum_{j=1}^{3}\left\lceil\frac{a_{1j}\cdot L_j}{3}\right\rceil\cdot 3\cdot\Big(\prod_{\substack{i=1\\ i\neq j}}^{3}L_i\Big)^{\varphi(L_j)}$$

$$=127641$$

用户 2,3,4 的钥同样可由式(2)计算得到：

$K_2=126816$；$K_3=126441$；$K_4=3750$。

由钥和锁就可以计算接入权限：

$a_{11}=\lfloor K_1/L_1\rfloor=\lfloor 127641/3\rfloor=42547\equiv1(\mathrm{mod}3)$

$a_{12}=\lfloor K_1/L_2\rfloor=\lfloor 127641/4\rfloor=31910\equiv2(\mathrm{mod}3)$

$a_{13}=\lfloor K_1/L_3\rfloor=\lfloor 127641/5\rfloor=25528\equiv1(\mathrm{mod}3)$

$a_{21}=\lfloor K_2/L_1\rfloor=\lfloor 126816/3\rfloor=42272\equiv2(\mathrm{mod}3)$

$a_{22}=\lfloor K_2/L_2\rfloor=\lfloor 126816/4\rfloor=31704\equiv0(\mathrm{mod}3)$

⋮

由定理 4.2 所计算的用户钥的数值较大，如果变(2)式为

$$K_i\equiv\sum_{j=1}^{n}N_{ij}\cdot n\cdot\Big(\prod_{\substack{i=1\\ i\neq j}}^{n}L_i\Big)^{\varphi(L_j)}(\mathrm{mod}\ n\prod_{i=1}^{n}L_i),$$

则可使 K_i 的值大大变小，从而使计算简单，但结果不变，其证明略。

继续延用上述例子，因为 $n\prod_{i=1}^{n}L_i=3\times\prod_{i=1}^{3}L_i=3\times3\times4\times5=180$，所以 $K_1'\equiv K_1(\mathrm{mod})80>\equiv127641(\mathrm{mod}\ 180)\equiv21(\mathrm{mod}\ 180)$，$K_2'\equiv K_2=(\mathrm{mod}\ 180)\equiv126816(\mathrm{mod}\ 180)\equiv96(\mathrm{mod}\ 180)$，$K_3'\equiv K_3(\mathrm{mod}\ 180)\equiv126441(\mathrm{mod}\ 180)\equiv81(\mathrm{mod}\ 180)$，$K_4'\equiv K_4(\mathrm{mod}\ 180)\equiv3750(\mathrm{mod}\ 180)\equiv150(\mathrm{mod}\ 180)$，以新钥 K_i' 重新计算如下：

$a_{11}=\lfloor K_1'/L_1\rfloor=\lfloor 21/3\rfloor=7\equiv1(\mathrm{mod}3)$

$a_{12}=\lfloor K_1'/L_2\rfloor=\lfloor 21/4\rfloor=5\equiv2(\mathrm{mod}3)$

$a_{13}=\lfloor K_1'/L_3\rfloor=\lfloor 21/5\rfloor=4\equiv1(\mathrm{mod}3)$

$a_{21}=\lfloor K_2'/L_1\rfloor=\lfloor 96/3\rfloor=32\equiv2(\mathrm{mod}3)$

$a_{22}=\lfloor K_2'/L_2\rfloor=\lfloor 96/4\rfloor=24\equiv0(\mathrm{mod}3)$

⋮

可见，它们的结果相同。

参考文献

[1]G. S. Graham, et al., Protection Principles and Practice, Proc. of AFIPS 1972 SJCC40, P. 417-429

[2]T. Y. Hwang, et al., An aceess control mechanism for computer system resources, Proc. of intl. Computer Symposium, 1980, Taipei, China

[3]M. L. Wu and T. Y. Hwang, Access control with single key-lock, IEEE Transactions on Software Engineering SE-10(2)(1984)

(上接第 24 页)

机器学习的程序中应当加入有关的元知识。

参考文献

[1]Thomas. E. Hill,《现代知识论》，中国人民大学出版社翻译出版，1989 年

[2]Abelson, R. P., The structure of belief systems. In R. C. Schank and K. M. Colby (Eds.), Computer models of thought and language. San Francisco: Freeman, 1973

[3]Abelson, R. P., Differences between belief and knowledge systems, Cognitive Science 3, 1979

[4]康德,《纯粹理性的批判》，三联书店，1957 年版