分布式应用中的多级安全密钥管理

卿斯汉,蒙 杨,刘克龙
(中国科学院软件研究所,中国科学院信息安全工程研究中心,北京 100080)

摘 要: 本文提出一种分布式应用中的多级安全密钥管理体制,该体制采用 BELL-LaPadula 模型作为多级安全存取控制策略,利用中国剩余定理,引入"主密钥因子","次密钥因子","写入因子",构造会话密钥的共享信息,该体制具有高效,安全,动态的特点. 这种体制有广泛的应用前景,有效的解决了网上会议,网上讨论等实际应用中的密钥管理问题.

关键词: 密钥管理; 多级安全系统; 中国剩余定理; 分布式应用
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2001) 02-0269-03

Key Management for Multilevel Security in Distributed Applications

QING Si-han, MENG Yang, LIU Ke-long
(*Institute of Software, The Chinese Academy of Sciences, Engineering Research Center for Information Security Technology, The Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract: A key management scheme for multilevel security in distributed applications is presented. The scheme adopts BELL-LaPadula model as multilevel access control policies. We use Chinese Remainder Theorem, introduce the notions of first-secret-key-element, second-secret-key-element and writing-element, and construct sharing information of session key. The scheme is efficient, secure and dynamic. At the same time, there are many practical applications involving the scheme for key management such as meeting in the network and talking in the network etc.

Key words: key management; multilevel security system; Chinese remainder theorem; distributed application

1 引言

随着计算机网络特别是 internet 的出现,多级安全的分布式应用成为一研究热点,所谓多级安全,指用户被分成不同的具有一定安全级别的组,不同的组具有不同的安全级别. 同时,不同安全级别的用户之间的消息流动须符合一定的安全存取控制策略. 由于分布式应用的安全最终通过对用户之间消息的加密来完成,所以加密传递的消息还得满足相应的存取控制策略,从而需要相应的密钥管理技术. 对于类似问题的研究始于八十年代,最早提出这个问题的并且提出解决方法的是文献[1],但是由于当时应用背景的限制,早期的研究主要针对数据库和操作系统. 由于受不断激增的应用的刺激,关于分布式应用中的多级安全存取控制策略的研究[2~5]成为一个热点,也有一些类似问题的研究[6~8],但是这些发布体制主要缺点有两个: (1) 所依靠的安全策略使得分组管理与密钥管理脱离; (2) 这些分发体制主要依靠计算不同安全类别之间的关系参数实现,这种实现降低了效率.

本文采用基于 BELL-LaPadula[8] 模型的安全控制策略,利用安全标签技术,使得分组管理与安全等级管理结合起来. 利用中国剩余定理进行密钥管理,通过发布会话密钥的共享信息来发布会话密钥,每次只需计算一次共享信息即可,该体制高效,安全,同时作到了密钥管理与安全管理的尽可能的分离. 以下就安全控制策略,密钥管理进行详细叙述,最后对本体制的效率与安全进行了分析.

2 多级安全存取控制策略

在多级安全存取控制研究中[7],常用的策略是把不同用户分成不同的安全级别,然后根据用户所属安全级别进行密钥发布,但是它有明显的缺陷: 比如在一个实际企业内部办公网中,人事组主管与财务组主管的安全级别应该是一样的,但是人事组主管不能随意得到财务组主管的消息,反之亦然.

本文利用 BELL-LaPadula 模型中安全标签的概念,存取控制才采用橘皮书中 *B* 级操作系统中强制存取控制策略概念,引入主体 (subject),客体 (object),支配 (dominance). 主体对客体可以进行的操作是读,主客体安全由安全标签来表示. 而每一个安全标签是由两部分组成: 安全等级,分类集. 安全等级是有大小之分的,而分类集是由无大小概念的分类组成. 在以下用 h 表示安全等级,用 c 表示分类集,用 $h_i \le h_j$ 表示 h_j 安全等级高于 h_i. 标签用 l_{ij} 表示,其中 i 代表安全等级,j 代表分类集,则 l_{ij} 表示安全等级为 h_i 分类集为 c_j 的标签,用 $l_{ij} \le l_{tl}$ 表

收稿日期: 1999-06-02; 修回日期: 2000-08-18
基金项目: 自然科学基金 (No. 69673016)

示标签 l_{tl} 支配 l_{ij},则 $l_{ij} \leq l_{tl}$ 的必要条件是:

$$h_i \leq h_t, c_j \subseteq c_i$$

在分布式应用中,操作主体指用户,所有用户都具有一安全标签. 而客体指用户之间传送消息的载体,如文件,邮件,目录,在网上的广播消息等等,其安全标签指产生消息的用户安全标签. 同时所有的用户分成不同的组,而所有组按其管理关系构成一树状结构,上一级的组能够读取其子孙组产生或拥有的消息. 以图 1 为例,某应用中用户划分得到的组有 $g_i, 1 \leq i \leq 5$;组之间的等级关系如图,以 d_i 表示 g_i 的子孙集,则 $d_0 = \{g_i | , 1 \leq i \leq 5\}$, $d_1 = \{g_3, g_4\}$. 很显然,子孙的子孙集是该子孙的祖先的子孙集的子集. 设 g_i 的安全等级为 $h_i, 0 \leq i \leq 5$,则子孙组的安全等级一定比祖先组的低,否则该分组是错误的,在本例中, $h_i \leq h_0, 1 \leq i \leq 5$, $h_5 \leq h_2$, $h_3 (h_4) \leq h_1$. 则对任意 $1 \leq i \leq 5$, $(h_i, c_i = (\{g_i\} \cup d_i))$ 构成一安全标签 l_{ii},这样每一个组对应一安全标签,所有的安全标签的全体构成一标签树. 以 g_0, g_1 为例分析其安全策略和相应的消息流向:

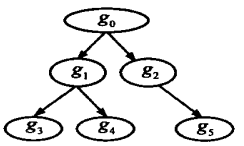

图 1 分组构成的树

由于 $h_1 \leq h_0$ 并且 $c_1 \leq c_0$,所以 $l_{11} \leq l_{00}$,则 g_0 可以存取 g_1 的消息. 反之不成立.

显而易见,任何组的标签一定支配其子孙组的标签. 这样上一级的组一定能读取其子孙组的消息. 反之一定不成立. 所以采用标签树符合多级用户的存取控制要求.

3 密钥管理办法

在该密钥管理体制中,跟其他类型的管理体制一样,有一可信任的第三方 KDC(密钥分发中心)来产生和分发密钥. 以下用 $E[\cdots]$ 表示公钥加密函数, $D[\cdots]$ 表示相应的解密函数, KDC 的公钥为 PK,相应的私钥为 SK, KDC 采用的加密算法和 PK 公布出来. 同时,设该体制中共有 T 个安全级别, L 个范畴,则对任意安全标签 $l_{tl} (t \leq T, l \leq L)$,其具有一密钥管理的代理 a_{tl}.

3.1 密钥因子产生办法

对任意安全标签 $l_{tl} (t \leq T, l \leq L)$,其代理 a_{tl} 随机选择素数 s_{tl},随机选择 k_{tl},使得 $k_{tl} < s_{tl}$,然后将 (s_{tl}, k_{tl}) 用 PK 加密传送到 KDC,然后计算 k_{tl}^{-1},使得 $k_{tl}^{-1} k_{tl} = 1 (\mathrm{mod}\ s_{tl})$,把 (k_{tl}^{-1}, s_{tl}) 称为 l_{ij} 的密钥因子,在我们的体制中,标签密钥因子的改变主要是指改变 k_{tl}^{-1}, s_{tl} 并不经常改变. 所以把 k_{tl}^{-1} 称为主密钥因子,把 s_{tl} 称为次密钥因子. KDC 选择 KDC 的关于 l_{tl} 的密钥 v_{tl},最后 KDC 计算会话密钥的上限 mr. 其过程如下:

$a_{tl} \rightarrow$ KDC: $c = E[PK, s_{tl}, k_{tl}]$

KDC 解密 c,得到 s_{tl}, k_{tl}

KDC 随机选择素数 v_{tl},使得 $v_{tl} <> s_{ij}$,其中 s_{ij} 是 l_{tl} 的祖先标签 l_{ij} 的次密钥因子.

KDC 计算 $mr = \lfloor \min(s_{tl}) / \max(k_{tl}) \rfloor$

3.2 会话密钥的产生

安全标签 l_{tl} 产生会话密钥的过程如下:

向 KDC 提出请求, KDC 选择一会话密钥 r_{tl},使得 $r_{tl} < mr$

构造一元同余方程组,其中未知数 m_{tl} 为 l_{tl} 的会话密钥共享信息

For l_{tl} 及其祖先标签 l_{ij}

begin

$$m_{tl} = k_{ij} r_{tl} (\mathrm{mod}\ s_{ij}) \quad (1)$$

end

随机选择 $w_{tl} < v_{tl}$,构造方程

$$m_{tl} = w_{tl} (\mathrm{mod}\ v_{tl})$$

据中国剩余定理(CRT)容易求解此同余方程,此方程组的解 m_{tl} 关于模 $\prod_{ij} s_{ij} v_{tl}$ (s_{ij} 为 l_{tl} 的祖先标签的次密钥因子)唯一. KDC 将 m_{tl} 以及有关的必需信息签名发布出来.

3.3 会话密钥的推导

设安全标签 l_{ij} 为 l_{tl} 或 l_{tl} 的父标签, l_{ij} 从 KDC 得到密钥 r_{tl} 的共享信息 m_{tl},由于, $m_{tl} = k_{ij} r_{tl} (\mathrm{mod}\ s_{ij})$.

则 $r_{tl} = k_{ij}^{-1} m_{tl} (\mathrm{mod}\ s_{ij})$ 容易得到.

3.4 会话密钥的改变

先看看利用中国剩余定理求解同余方程(1)的过程:

令 $Q_{tl} = \prod_{ij} s_{ij} v_{tl}$ (s_{ij} 为 l_{tl} 或 l_{tl} 的祖先标签的次密钥)

$M_{ij} = Q_{tl} / S_{ij}$, $M_0 = Q_{tl} / v_{tl}$

$y_{ij} M_{ij} \equiv 1 (\mathrm{mod}\ S_{ij})$

$e_{ij} = M_{ij} y_{ij}$

$y_0 M_0 \equiv 1 (\mathrm{mod}\ v_{tl})$

$O_{tl} \equiv M_0 y_0$

$C_{tl} \equiv (\sum_{ij} e_{ij} k_{ij}) r_{tl} + O_{tl} W_{tl} \quad (\mathrm{mod}\ Q_{tl})$

令 $h_{tl} = (\sum_{ij} e_{ij} k_{ij}, O_{tl})$,称 h_{tl} 为 l_{tl} 的写入因子,在密钥因子产生时生成,在 KDC 中保存. 若 KDC 要改变会话密钥为 w'_{tl},随机选择 w'_{tl},使得 $w'_{tl} < v_{tl}$,在每次改变会话密钥时只需计算

$$c_{tl} \equiv (r'_{tl}, W'_{tl}) h_{tl}^{T} \quad (\mathrm{mod}\ Q_{tl})$$

这种产生会话密钥方法特别适合会话密钥动态生成.

3.5 用户密钥因子的改变

某一标签 l_{tl} 把主密钥因子 k_{tl} 改变为 k'_{tl},用户首先根据(3.1)把该值传送至 KDC, KDC 需计算

$y_{tl} M_{tl} \equiv 1 (\mathrm{mod}\ S_{tl})$

$e_{tl} = M_{tl} y_{tl}$

对 l_{tl} 及所有子孙标签 l_{ij},计算

$$h'_{ij} = h_{ij} + (e_{tl} (k'_{ij} - k_{ij}), 0)$$

则标签 l_{ij} 的写入子密钥为 h'_{ij}

通过上面的计算过程可以看到,主密钥的改变主要计算一个线性同余方程. 如果标签 l_{tl} 的次密钥 s_{tl} 改变,则需要重新计算所有子标签的同余方程组,才能得到所有子标签的写入因子. 同时,即使非法用户窃取次密钥,由于不知道主密钥因子而无法得到会话密钥. 由此可以看出,引入主密钥因子可以提高计算的效率,同时没有降低系统的安全性能.

3.6 安全标签的管理

3.6.1 增加一安全标签

如果该标签的安全等级已存在,也就是为某一标签增加一个子标签. 同样,该子标签选择其密钥因子, KDC 为其产生写入因子. 如果再为该标签增加子孙标签,同样只需为这些子

标签产生写入因子.从过程看,增加这种标签不影响任何已存在的标签的写入因子.而这种类型的标签增加是最主要的形式.如果该标签的安全等级不存在,比如在已存在的安全等级之间增加一安全等级,则需要重新计算该标签的所有子孙标签的写入因子.由于这种重新计算只发生在该标签的子孙标签,也就是重新计算其子孙标签相对应的中国剩余定理.同时,这种类型的标签增加不是标签增加主要的形式.

3.6.2　删除一安全标签

某一安全标签被删除后,由于所有子孙标签要有一新的父标签,其所有子孙标签的写入因子都需重新计算.而不影响其他的任何标签.总之,任何标签的改变只需计算其子孙标签相对应的写入因子.同时,由于标签的改变并不经常发生.所以从整体上说,安全标签的管理不影响系统的效率.

4　效率与安全性分析

4.1　效率分析

在写入因子产生时,每一个安全标签需要利用中国剩余定理求解一个同余方程,在一安全标签变化以后,需要为其每一个子标签利用中国剩余定理求解一同余方程.在每次产生会话密钥时,只需计算不多于(安全标签对应节点的高度) *2 次乘法和几次加法.而用户主密钥因子的改变,只需一个求逆运算,而次密钥因子的改变,需求解一关于次模逆运算.而在推导会话密钥时,只需计算几次乘法.

4.2　安全性分析

4.2.1　外部攻击

如果一非法用户仅有安全标签 l_{tl}密钥共享信息 m_{tl},而他的安全标签不是 l_{tl}或其父标签,由于他不知道 l_{tl}或其任何父标签的密钥因子,所以是无法得到 l_{tl}的会话密钥.同时,即使该非法用户得到 l_{tl}或其父标签的次密钥因子或主密钥因子中的一个,也是无法计算得到 l_{tl}的会话密钥.

4.2.2　内部攻击

如果一用户得到 l_{tl}密钥共享信息 m_{tl},而他的安全标签 l_{ij}是 l_{tl}或其父标签.则他企图通过其子标签的密钥共享信息得到其祖先标签的会话密钥.由于祖先标签的会话密钥只在下式中用到　$c_{tl} \equiv (\sum_{ij} e_{ij}k_{ij})\, r_{tl} + O_{tl}w_{tl} \pmod{Q_{tl}}$

要计算得到祖先标签的密钥,需计算得到 h_{tl},由于 (Q_{tl}, w_{tl}) 未知,所以计算未经模 Q_{tl}运算的 $(\sum_{ij} e_{ij}k_{ij})\, r_{tl} + O_{tl}W_{tl}$是不可能的,即使得到 h_{tl},由于未知数太多,无法得到其任何祖先标签的会话密钥.

如果一非法用户想利用一个子孙标签的多次密钥共享信息,他只能得到以下的方程组

$$c_{tl}^{(0)} \equiv r_{tl}^{(0)} h_{tl} + O_{tl}w_{tl}^{(0)} \pmod{Q_{tl}} \quad \cdots\cdots$$
$$c_{tl}^{(1)} \equiv r_{tl}^{(1)} h_{tl} + O_{tl}w_{tl}^{(1)} \pmod{Q_{tl}}$$

从方程组可以看出,每增加一个方程,要增加两个未知数,所以多个方程能得到的信息与一个方程是一样多的.

如果一非法用户想利用多个子孙标签的会话密钥,只能得到以下的方程组

$$c_{tl} \equiv r_{tl}h_{tl} + O_{tl}w_{tl} \pmod{Q_{tl}}$$
$$c_{ij} \equiv r_{ij}h_{ij} + O_{ij}w_{ij} \pmod{Q_{ij}} \quad (l_{ij}\text{为 } l_{tl}\text{的子孙标签})$$

从方程组看,每一个方程具有不同的未知数.增加方程得不到任何更多的信息.

以上分析可知,即使多个子孙标签联合攻击,也无法得到其父标签的密钥.

5　结论

本文提出的多级安全密钥管理体制,采用基于 BELL-La-Padula 模型的安全存取控制策略,适合分布式应用中安全存取控制,每一个用户具有一安全标签,而非简单的属于某一个安全类别,通过安全标签之间的支配关系来产生会话密钥的共享信息,而非产生安全类别之间的关系.本文引入主密钥因子与次密钥因子以及写入因子,在产生会话密钥时,只需计算几次乘法与加法,其速度与效率是显而易见的.同时使得密钥管理与标签管理尽可能的分离,是其他同类密钥管理体制无法比的.同时其安全性也是非常高的.在实际的实现中,可采用主密钥因子的位数是次密钥因子的位数删除一半,这样会话密钥的长度与主密钥因子的长度相当;每一个安全标签的代理可以是一个组用户,负责产生密钥因子,计算会话密钥,在同组用户之间分发会话密钥.

参考文献:

[1] L. harn, H. Y. Lin. A cryptographic keys generation scheme for multi-level data security [J]. Computer security, 1990, 9: 539 - 546.

[2] Vincent Nicomette and Yves deswarte. A multilevel security model for distributed object systems [J]. Proceedings in Computer Security, Esorics 96.

[3] R. s. sandhu and P. samarati, Access control: principles and practies [J]. IEEE communications, 1994, 32(9): 40 - 48.

[4] Takayuki Tachikawa, Hiroaki Higaki, Makoto Takizawa. Purpose-oriented access control model in object-based systems [A]. In Proceedings ACISP'97 [C], 1997, 7: 38 - 49.

[5] G. Horng. A key management approach for access control in user hierarchies [J]. Proc. Of International Computer symposium, Hsinchu, Tai-Wan, 1994: 439 - 444.

[6] H. M. Tsai, C. C. Chang. A cryptogaryphic implementation for dynamic access control in a user hierarchy [J]. compute and security, 1995, 14: 159 - 166.

[7] Chu-Hsing Lin. Dynamic key management schemes for access control in a hierarchy [J]. Computer comminication, 1997, 20(15): 1381 - 1385.

[8] D. Bell and L. Lapadula. Secure computer systems: unified exposition and multics interpretation [R]. Tech. Rep. MTR-2997, MITRE Co., 1975, 7.

作者简介:

卿斯汉　博士生导师,1939 年生,主要研究领域是信息安全理论与技术

蒙　杨　博士生,1972 年生,主要研究领域:信息安全理论与技术