第31卷 第24期 计 算 机 工 程 2005年12月
Vol.31 № 24 Computer Engineering December 2005
·博士论文· 文章编号：1000—3428(2005)24—0030—03 文献标识码：A 中图分类号：TP393.08

一种基于可信度计算的集成身份认证与访问控制的安全机制

曾剑平，郭东辉
(厦门大学物理系EDA实验室，厦门 361005)

摘 要：提出了一种基于主体可信度计算的集成身份认证和访问控制的安全机制，当主体的可信度下降到某个值之后，采用一次性口令认证方法对主体进行重新认证。该安全机制能有效提高访问控制模型对冒充用户访问的检测及控制能力。
关键词：访问控制；身份认证；可信度；分布式系统

A Security Mechanism Integrating Authentication with Access Control Based on Certification Factor

ZENG Jianping, GUO Donghui
(EDA Lab, Dept. of Physics, Xiamen University, Xiamen 361005)

【Abstract】 A new kind of security mechanism integrating authentication with access control based on certification factor is proposed. When the subject's certification factor decreases to a certain value, a one-way password authentication is required. This security mechanism can effectively improve the ability of access control model to detect and control a pseudo-user.
【Key words】 Access control; Authentication; Certification factor; Distributed system

访问控制是OSI网络安全体系结构的一类安全服务[1]，其目的是对主体访问客体的行为进行合法性判断，并允许或禁止这种行为的发生。然而这种安全性的一个重要前提是假设用户身份是真实的，即用户身份的表示与用户本人是一致的。而目前确定用户身份最常见的方法是采用基于用户名及密码的身份认证机制。然而，在访问控制应用中，特别是在分布式系统中，这种方式经常会带来的安全问题是：某个用户的身份信息被他人非法获取或破译，使得主体被非法用户冒充而进入系统，从而使访问控制模型失去安全作用，造成信息安全性大大降低。

目前针对这个问题的解决办法是采用审计或入侵检测的方法[2]。然而这些方法是一种事后检测的方法，冒充用户对客体的操作已经发生，其造成的后果在很多情况下是很难弥补的。目前正在发展中的实时入侵检测技术则往往因为误报或漏报[1]而造成用户操作上的不方便或忽略了安全隐患。本文提出一种折中的安全机制，将身份认证与访问控制这两种安全服务有效地结合起来。通过建立主体的可信度计算方法，实时检测主体的可信度变化，当它下降到某个设定的值之后，采用一次性口令[4]方法对主体的身份进行重新认证。同时在一次性口令实现中结合了基于公开密钥的密码序列处理，因此，能否通过一次性口令认证就反映了用户身份的可信度。

1 集成身份认证与访问控制的安全机制

身份认证是保证用户身份合法性及唯一性的方法，而访问控制的有效性也需要建立在合法主体的基础之上。有效地将两者结合起来，发挥各自的优势，能提高整个系统的安全性与灵活性。

目前将这两种安全机制结合起来的方法主要是基于会话定时的重新认证机制，这种机制大量用于Web服务器对用户的控制。其缺点是没有根据主体执行的环境采取合适的措施，而是采用统一的一个定时时间来强制用户重新进行身份认证。因此，这些安全机制对冒充用户的鉴别及控制能力是很弱的。

为了方便后续的描述，本文约定如下的符号表示：s表示主体，o表示客体。并作如下的定义：

定义1 访问会话（Access Session）：主体s通过访问控制模型许可之后，进入客体o所在的应用模块到s退出这个模块为止，此过程在计算机中的逻辑映像称为一次访问会话。

本文提出的集成机制有效地提高了检测及控制冒充用户访问的能力。这个集成机制的基本原理如图1所示，由身份认证、访问控制模型、可信度计算、可信度控制、重新认证及一次性口令管理等功能组成。

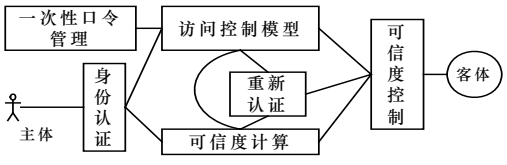

图1 集成身份认证与访问控制的安全机制

这个安全机制中的各个功能描述如下：

（1）身份认证。采用基于用户名及密码的身份认证方式，允许或限制用户进入应用系统。它向访问控制模型提供一个经过认证的、

基金项目：国家自然科学基金资助项目(60076015)；国家人事部留学人员创业基金资助项目
作者简介：曾剑平（1973－），男，博士生，主研方向：信息安全，分布式系统；郭东辉，教授、博导
收稿日期：2004-11-08 **E-mail**：zeng_jian_ping@hotmail.com

并且代表用户身份的用户名，同时身份认证需要为可信度计算模块提供计算主体可信度所需要的信息，包括认证时间、认证地点以及运行环境的相关信息。

(2) 访问控制模型。访问控制模型对主体的访问请求进行判断，得到是否允许访问的结论。同时需要为可信度计算模块提供在每个访问行为前提下，对主体可信度的计算的信息，包括主体请求、访问会话中的环境信息等。

(3) 可信度计算。可信度计算对身份认证及访问控制模型提供的信息动态计算主体的可信度，它随着所得到的信息而变化，可信度是一个位于[-1，1]区间的值。-1 表示主体绝对不可信，而 1 表示主体绝对可信。

(4) 可信度控制。可信度控制根据主体当前的可信度及访问控制模型判断结果，决定主体的访问请求是否继续，以及是否要求对主体进行重新认证。

(5) 重新认证。按照一次性口令的认证方式，通知访问控制模型对主体进行重新认证。

(6) 一次性口令的管理。主要完成当前访问会话的一次性口令的生成，将生成的一次性口令加密并发送给客户端。

2 可信度计算

2.1 可信度计算方法

主体可信度是这个安全机制的核心，它可以通过以下几种途径来计算:

(1) 根据主体在进行身份认证时所获得的信息来计算。这些信息包括主体通过认证的时间、主体的认证位置、以及主体所在的客户机信息等。

(2) 根据主体在访问客体时所表现出来的属性计算。这些属性可以是在某个客体上的停留时间、在客体上的资料输入方式等。

(3) 通过预测主体访问客体的序列来计算。预测主体下一步访问中选择某个客体的可能性，可以作为主体可信度计算的参考值。

下面分别详细描述这 3 类可信度计算方法。

2.2 规则型可信度计算

前两类计算途径使用的是规则型的信息，可以归结为 IF – THEN 形式的规则表示，即

IF E THEN H CF(H,E)

这里的 E 表示证据,即上述方法中所获得的信息或属性; H 为结论，表示为 OWN(s)，即某个访问会话中的主体 s 确实是用户本身。因此该规则可以解释为: 证据 E 发生的前提下，那么主体 s 确实是用户本身，这个规则的可信度为 CF(H,E)。

计算主体的可信度就是求解结论可信度 CF(H)的过程。根据可信度理论[5]，CF(H)的计算方法可用以下计算公式:

(1) 证据不是肯定存在的

$$CF(H)=CF(H,E)*\max\{0,CF(E)\} \quad (1)$$

(2) 证据是合取连接的，即

$$E=E1\wedge E2\wedge\cdots\wedge En$$

$$CF(E)=\min\{CF(E1),CF(E2),CF(E3),\cdots,CF(En)\} \quad (2)$$

(3) 证据是析取连接的，即 $E=E1\vee E2\vee\cdots\vee En$

$$CF(E)=\max\{CF(E1),CF(E2),CF(E3),\cdots,CF(En)\} \quad (3)$$

(4) 多条规则，具有相同结论的

$$CF_1(H)=CF(H,E)*\max\{0,CF(E1)\}$$

$$CF_2(H)=CF(H,E)*\max\{0,CF(E2)\}$$

则合成的可信度为

$$CF_{i2}(H)=\begin{cases}CF_1(H)+CF_2(H)-CF_1(H)\times CF_2(H), & CF_1(H)\ge 0 \text{ and } CF_2(H)\ge 0\\ CF_1(H)+CF_2(H)+CF_1(H)\times CF_2(H), & CF_1(H)<0 \text{ and } CF_2(H)<0\\ CF_1(H)+CF_2(H), & \text{others}\end{cases} \quad (4)$$

在上述公式中，需要先求得规则可信度 CF(H,E)和证据的可信度 CF(E)，才能计算 CF(H)。而对于规则可信度 CF(H,E)，一般是采用人为的判断决定它的取值。证据的可信度的计算方法，解释如下。

在上述两类计算途径中，有的证据可信度可以用精确的值来表示，有的则需要用模糊值才能表达，如“主体在晚上登录系统”。因此，规则的描述需要支持模糊信息的表达。同时称系统在某个具体的身份认证过程或访问会话中获得的证据为事实值。则在计算事实值对应的结论可信度时，需要将事实值模糊化，并运用模糊运算得到结论的可信度。假设某个事实值为 V_e，算法如下:

算法 1 计算事实值的可信度

如果与之匹配的规则中的证据是采用模糊数表示的

设对应的模糊概念为 Y，它的论域为 U，则模糊概念 Y 可以用一个隶属度函数 $u_y(x)$ 来表示。

则事实值 V_e 对应的可信度 $CF(E)=u_y(Ve)$

否则求得相应规则中的证据 ER 与 V_e 之间的相对距离（偏差）:

$$|D_{er-ve}|=\frac{f(ER)-f(V_e)}{f(ER)}$$

其中 f(x)是证据 x 对应的属性值的一种评价函数

事实值 V_e 对应的可信度 $CF(E)=|D_{er-ve}|$

求得 CF(E)和 CF(H,E)之后，就可以根据式(1)～式(4)计算不同规则和事实值条件下的主体可信度 CF(H)。

2.3 访问序列下的主体可信度计算

主体在访问会话过程中所表现出来的可信度，可以通过对客体访问序列的分析计算得到。根据可能性－概率一致性原理，可能性与概率存在某种线性关系，而可信度 CF=MB-MD，其中 MB、MD 可以用概率来解释[5]。因此，事件的可能性在某种程度上也是反映了它的可信度。这是本文的计算访问序列下主体可信度的依据。

可以通过计算某一时刻主体所访问的客体相对于所有可能的客体的可能性，并作为主体的当前可信度，而这种可能性可以通过对访问序列进行预测分析来计算。下面具体描述基于 Markov 模型[6]的计算方法。

设在某个时刻 t 的主体所处的状态 $H(t)=[h_1,h_2,\ldots,h_n]$，因为主体在一个访问会话中不可能同时访问不同的客体，所以 $h_1,h_2,\ldots,h_n$ 中只有 1 项不等于 0。假设 Markov 模型对应的概率转移矩阵为 A，A^1 表示对应的 1 步概率转移矩阵，依次类推，A^n 表示 n 步概率转移矩阵。则在已知 t 时刻的访问序列情况下，计算 t+1 时刻主体可信度的算法如下:

算法 2 计算 t+1 时刻主体的可信度算法

输入: t 时刻主体的可信度 $CF_t(H)$，t+1 时刻被访问的客体 o_j

处理:

计算 t 时刻状态对 t+1 时刻的预测结果: $V_1(t+1)=H(t)\times A^1$，计算 t-1 时刻状态对 t+1 时刻的预测结果: $V_2(t+1)=H(t-1)\times A^2$，依次类推。

计算 t+1 时刻的综合预测值:

$$V(t+1)=a_1\times V_1(t+1)+a_2\times V_2(t+1)+\cdots+a_n\times V_n(t+1)$$

$$=a_1\times H(t)\times A^1+a_2\times H(t-1)\times A^2+\cdots+a_n\times H(t-n+1)\times A^n$$

其中，$\sum_{i=1}^{n}a_i=1$，a_i 表示过去的每个预测值对 t+1 时刻的影响因子。

则相应地可以得到 t+1 时刻主体的可信度的更新值: $CF_{t+1}'(H)=V(o_j)$

根据式 (4) 计算 t+1 时刻主体的可信度，即

$$CF_{t+1}(H)=\begin{cases}CF_t(H)+CF_{t+1}'(H)-CF_t(H)\times CF_{t+1}'(H), & CF_t(H)\ge 0 \text{ and } CF_{t+1}'(H)\ge 0\\ CF_t(H)+CF_{t+1}'(H)+CF_t\times CF_{t+1}'(H), & CF_t(H)<0 \text{ and } CF_{t+1}'(H)<0\\ CF_t+CF_{t+1}'(H), & \text{others}\end{cases}$$

输出: t+1 时刻主体的可信度 $CF_{t+1}(H)$

3 基于可信度的控制

其主要功能是根据不同的可信度值，对主体的行为进行适当的控制，目标是尽量减少判断错误，同时又能拒绝大部分的冒充用户访问。本文采用重新认证的方法解决这个问题。

为了避免重新认证时，采用与首次身份认证所使用的密码一样，增加认证的可信性，这里使用一次性口令认证方法。一次性口令的优点是对于窃听者或主机上密码文件的窃取具有很好的抵抗能力，因为密码只在一段时间内有效，而且即使获得了当前的密码，也不可能知道下一次的密码。但它的缺点也是明显的，例如在分布式环境下，所生成的密码序列的反馈很不方便。一次性口令认证方法有多种实现形式，主要有 Lamport 方案、Dellcore 方案、时钟同步方案、挑战响应方案。由于 Lamport 可以不使用手持鉴别器，实现上相对简单。因此，本文以 Lamport 方案为基础，结合公钥加密算法，使得在分布式环境下密码序列能安全地反馈给客户端。

一次性口令认证的两个关键参数是：初始口令或某一个秘密串 R 和所要生成的一次性口令个数 N。在通常情况下，这两个参数是由客户端提出的。本文中，R 可取主体的身份认证时设置的密码，N 则由主机随机生成。则一次性口令的生成及反馈算法描述如下：

算法 3 一次性口令生成及反馈算法

输入：秘密串 R、一次性口令个数 N，用户的公共密钥 PK，私有密钥 MK

处理：

置循环变量 m=0，保存 N 个一次性口令的数组 OP[N]，P=R

OP[m] = Hash(P)，其中 Hash(x)是一个哈稀函数，它是一种单向函数

P= OP[m]， m=m+1

FB = FB + P，这里是指将两个字符串连接起来

重复执行(2)～(3)步骤，直到 m=N-1

主机用用户的公共密钥 PK 对生成的密码串加密，得到 FC = Encry(FB,PK)，并将结果 FC 发送给客户端

在客户端，主体使用自己的私钥 MK 将接收到的串 FC 解开，得到 FB=Dencry(FC,MK)。从而可以得到本次访问会话过程中可以使用的 N 个密码序列。

输出：

N 个一次性口令

由于私钥 MK 是由用户自己保管的，并且不在网络上传输，不会被其他人非法获取，因此拥有相应的私钥就代表了该主体确实是用户本人，即用户的可信度为 1。

用户主体得到 N 个一次性口令之后，即可用来进行身份的重新认证，基于可信度的访问控制算法描述如下：

算法 4 基于可信度的访问控制算法

输入：主体的当前可信度 CF(H)，保存 N 个一次性口令的数组 OP[N]

处理：

如果 $0 < CF(H) \le 0.5$，则

启动重新认证机制，要求主体按照一次性口令的规则，输入当前的密码 Pass；

如果 Pass = OP[N]，则

置主体可信度 CF(H) = 1；

否则

置主体可信度 CF(H) = -1；

N = N –1

如果 $CF(H) > 0.5$，则

允许主体的访问行为继续进行，可信度 CF(H)不变

如果 $CF(H) \le 0$，则

不允许主体的访问行为继续进行，用户需要退出本次的访问会话重新登录并接收一次性口令。

输出：

是否允许继续访问

主体的当前可信度 CF(H)

4 安全机制的实例

本文提出的安全机制将身份认证和访问控制模型结合起来，利用算法 1、算法 2 实时计算在每个事件情况下的用户可信度，并使用算法 4 对访问控制模型的访问决策进行控制。从而可以在可信度动态变化的情况下对主体的访问行为进行控制。图 2 是实际运行中的主体可信度与在不同时刻所发生的事件的变化关系。曲线 A 表示了用户在多次认证失败的情况下，进行一次性口令认证时的可信度变化；曲线 B 表示了用户在访问客体过程中可信度下降时进行一次性口令认证的情况；曲线 C 表示了正常用户在访问会话过程中的可信度变化情况。

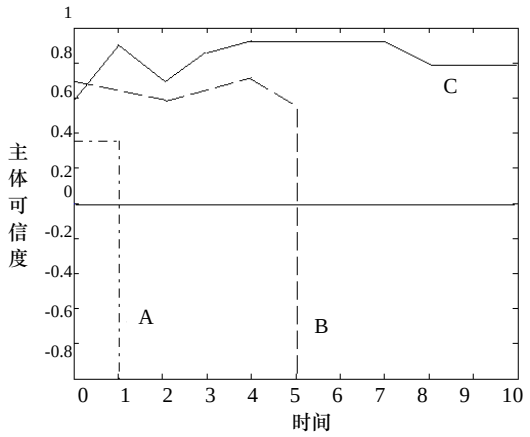

图 2 事件触发下的可信度变化

5 结束语

确保访问控制模型安全性的一个主要前提是用户身份的真实性，但是基于简单的用户名/密码身份认证方式容易受到各种攻击，造成某个主体的身份信息被他人非法获取或破译，主体被非法用户冒充而进入系统，从而使访问控制模型失去安全作用。本文提出了一种基于主体可信度计算的集成身份认证和访问控制的安全机制，当主体的可信度下降到某个值之后，采用一次性口令认证方法对主体进行重新认证。该安全机制能有效提高访问控制模型对冒充用户访问的检测及控制能力。保证访问控制模型在用户身份不确定情况下的安全性仍然具有较高的安全控制能力。

参考文献

1 中国信息安全产品测评认证中心编著. 信息安全理论与技术. 北京：人民邮电出版社, 2003

2 钟 诚, 赵跃华. 信息安全概论. 武汉：武汉理工大学出版社, 2003-08

3 Haller N, Metz C, Nesser P, et al. A One-time Password System. RFC2289, 1998-02

4 邵力军, 张 景, 魏长华. 人工智能基础. 北京：电子工业出版社, 2000-03

5 陆汝钤. 人工智能. 北京：科学出版社, 2002-02

6 李裕奇. 随机过程. 北京：国防工业出版社, 2003-08