

面向普适计算的动态多级安全访问控制方案

刘 丁

(陕西师范大学, 陕西 西安 710062)

摘 要: 提出一种面向普适计算的动态多级安全访问控制新方案, 形式化描述了访问控制的构成要素, 定义了动态访问控制策略, 最后给出了授权实现算法. 方案既保证了授权的动态性, 又增强了访问控制的安全性, 更适合于普适计算环境.

关键词: 普适计算; 访问控制; 上下文; 多级安全; 安全级

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)01-0102-04

A New Scheme for Pervasive Computing-Oriented Dynamic Multi-Level Security Access Control

LIU Ding

(Shaanxi Normal University, Xi'an 710062, China)

Abstract: The paper presents a new scheme for pervasive computing-oriented dynamic multilevel security access control. The elements, dynamic access control mechanism are discussed respectively, at last the paper bewrote the authorization algorithm. Compared to the existing authorization models, the scheme we brought forward can insure dynamic authorization, and provides high security for the access control as well. The scheme is more suitable for pervasive computing environment.

Key words: pervasive computing; access control; context; multi-level security; secure label

1 引言

随着普适计算研究和应用的不断深入, 普适计算的安全性已经成为普适计算的一个基础问题. 访问控制(access control)是针对越权使用系统资源的防御措施, 通过限制对关键资源的访问, 防止非法用户的侵入或合法用户的不慎操作而造成的破坏, 从而保证系统资源受控地、合法地使用, 它是确保计算机系统安全的核心技术之一. 传统静态的基于身份的访问控制理论和方法已经不能满足普适计算环境的需要, 迫切需要研究新理论和新方法^[1].

多级安全(Multi-Level Security, MLS)保护的主要是信息的安全性, 它用来保障信息不会被非法阅读、修改和泄漏. 在多级安全系统中, 所有信息都

有一个安全级(secure label), 安全策略要求, 为了合法地得到某一信息, 用户的安全级必须大于或等于信息的安全级, 并且该信息属于用户的信息访问类别. 如何既能使多级安全思想融入到普适计算环境(即多级安全性动态化), 又能简化访问控制的授权和认证, 是构建文中的思想出发点. 针对普适计算访问控制的特点, 提出一种面向普适计算的动态多级安全访问控制方案^[2].

2 动态多级安全访问控制构成要素

定义 1 普适实体. 普适计算环境中参与活动的所有硬件接口设备, 称为普适实体, 记为 E , $E = \{E_r, E_s\}$, 其中, 需要请求某种服务的实体称为请求实体 E_r , $E_r = \{E_{r1}, E_{r2}, \dots, E_{rm}\}$; 为请求实体提供

某种服务的实体称为服务实体,记为 $E_s, E_s = \{E_{s1}, E_{s2}, \dots, E_{sn}\}$. 根据应用上下文的不同,系统中的某一实体,既可以是 E_r ,也可以是 E_s .

定义2 实体安全级. 普适计算环境下的任何实体都要求被赋予一定的安全级别,称为实体安全级,记为 L .

$L = \{\text{less_low}, \text{low}, \text{more_low}, \text{medium}, \text{less_high}, \text{high}, \text{more_high}\}$

实体安全级的划分粒度具有一定弹性,可根据普适计算系统的实际应用需求来确定.

通常在信息系统安全级别表示中,安全级可以离散地表示(如定义2),也可以用连续的实数值表示,并有一个上界和下界,即用模糊区间值表示.后者虽然更符合普适计算环境的不确定性,但如何界定同一区间内不同实数所代表的安全级大小,在理论和方法上还有待于进一步研究.文中采用离散形式来表示.

定理1 实体安全级集合 L , 其中 $\langle L, \leq \rangle$ 是一个偏序集, $\text{less_low} \leq \text{low} \leq \text{more_low} \leq \text{medium} \leq \text{less_high} \leq \text{high} \leq \text{more_high}$. 其中, $\leq$ 构成了偏序关系.

定义3 实体安全级函数定义为 $\text{entityLabel}(E) = L^E$, 其中, 函数 $\text{entityLabel}(E)$ 称为实体 E 的安全级函数, 完成实体到安全级的映射.

定义4 普适计算环境上下文是用户环境和应用环境以及和访问控制决策相关的信息集, 也称为面向普适计算的上下文环境^[3].

用户在普适计算系统中处于核心的、非从属地位, 这就决定了计算机应该更加主动, 不应该再将用户的信息输入或操作行为作为系统运行的唯一动力源, 必须要求普适计算系统具有自适应性, 即在用户不发出服务请求的情况下, 动态地进行授权和认证. 普适计算系统进行自适应活动的唯一依据就是上下文环境, 上下文所涵盖的用户环境和应用环境以及和访问控制决策相关的信息, 在普适计算访问控制中起着决定性的关键作用.

普适计算环境中的上下文大致分为3类:

- (1) 环境上下文: 时间、位置等环境因素;
- (2) 设备上下文: 移动终端、传感器节点等设备特性;
- (3) 用户上下文: 表情、动作、习惯等.

上下文感知是当前普适计算的研究热点和难点之一, 尤其涉及到用户相关的上下文信息, 不能定量地获取, 需要依据用户的历史数据来进行综合的判

定, 系统必须具备一定的自学习能力. 因此, 文中讨论的主要利用环境上下文的时空属性(即时间、位置)信息来对普适主体进行动态授权.

时间作为重要的上下文信息, 是实现动态访问控制的重要约束条件之一. 时间的表示包括连续时间和离散时间两种, 为简单起见, 文中以离散时间为讨论对象, 连续时间讨论与此类似. 设 $T = \{t_0, t_1, \dots\}$ 是离散时间轴上的所有点构成的无限集合. 离散时间轴上的不间断点构成的集合称为区间时间, 记为 $[t_s, t_e]$, 其中 $t_s, t_e \in T$, 并且 $t_s \leq t_e$. 周期时间用序偶 $([t_s, t_e], P)$ 表示, 其中 P 是周期时间表达式, 表示周期时间区间的无限集合. 离散时间轴上的连续点构成的集合 $[t_s, t_e]$ 称为时间区间, $t_e - t_s$ 表示其长度, 用 length 表示, $\text{length} = \lfloor t_e - t_s \rfloor$.

定义5 设 $C_1, C_2, \dots, C_n, C_d$ 是日历, 周期时间表达式 P 定义为

$$P = \sum_{i=1}^n O_i \cdot C_i \triangleright r \cdot C_d$$

其中, $O_1 = \text{all}$, $O_i \in 2^N \cup \{\text{all}\}$, $C_i \subseteq C_{i-1}$, $i = 1, 2, \dots, n$, $C_d \in C_n$ 是时间区间的长度单位, N 是自然数集合, $r, n \in N$, 符号 $\triangleright$ 左端表示周期时间表达式所代表的时间区间左端点的集合, 右端表示日历 C_d 的时间步长, r 代表日历的个数. 例如, $\text{all} \cdot \text{year} + \{2, 5, 11\} \cdot \text{month} + 3 \cdot \text{day} \triangleright 10 \cdot \text{day}$, 表示分别以每年的2、5和11月份的第3天开始计时, 持续时间为10天^[4].

定义6 $\forall [t_s, t_e] \in T \times T, t \in T$ 是时间点, $[t_s, t_e]$ 是时间区, 周期时间表示的时间点集合定义为 $\text{timeSet} = ([t_s, t_e], P)$. 例如周期时间表达式 $P = \text{all} \cdot \text{month} + \{1, 5\} \cdot \text{day} + 9 \cdot \text{hour} \triangleright 1 \cdot \text{hour}$ 表示, 每月1日9点至10点和5日9点至10点, 则 $\text{timeSet}([2009/1, 2009/2], P) = \{2009/1/1: 9, 2009/1/5: 10, 2009/2/1: 9, 2009/2/5: 10, 2009/3/1: 9, 2009/3/5: 10\}$.

普适实体位置的感知和定位, 是实现普适计算机动态授权的另外一个关键的约束. 在这方面研究中, 涌现了很多感知物体空间位置的技术, 比如超声波、全球定位系统(GPS)、IEEE 802.11、RFID、超宽带(UWB)、基于射频信号到达时间差定位(TDoA)、智能地板(smart floor)传感器定位等等. 具体选择哪种技术, 要根据实际普适应用环境、成本、计算精度等诸多因素来综合考虑, 文中不对具体的定位技术进行评论. 因此以下讨论假定普适实体的上下文位置信息总是可以获得的.

定义 7 空间点(space point)是离散三维空间中的点,定义为 $\text{point} = (x_i, y_i, z_i)$, $i \in N$.

空间点是时空访问控制模型中常采用的基本空间因素,一般表示为二维或三维坐标.

定义 8 空间点的集合是离散的三维空间中所有点的集合,定义为

$$\text{pointSet} = \sum_{i=1}^n (x_i, y_i, z_i), i \in N.$$

定义 9 空间任意两个离散点之间的距离用函数 distance 表示,定义为

$$\text{distance}((x_i, y_i, z_i), (x_j, y_j, z_j)) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2}, i, j \in N.$$

3 普适动态多级安全访问控制方案

定义 10 普适请求实体 E_r 是一个五元组,服务实体 E_s 是一个四元组,定义如下

$$E_{ri} = (op_{ri}, L_i, t_{si}, t_{ei}, \text{point}_i), i \in N$$

$$E_{sj} = (op_{sj}, L_j, P_j, \text{point}_j), j \in N$$

其中, L 为普适实体的安全级; $[t_s, t_e] \in T \times T$, t_s 是请求实体得到服务实体授权的起始时间点, t_e 是请求实体拥有权限的中止时间点; point 是普适实体的空间坐标; op_r 为请求实体的权限集合变量,接受来自服务实体 E_s 的服务权限赋值; op_s 为服务实体 E_s 可提供的服务权限集合; P 为权限的生命周期,在一定的周期内, E_r 授权有效,超出周期时间约束时,权限强行撤销.

定义 11 授权模板是一个三元组 $au = (E_r, E_s, rw)$. 其中, E_r 、 E_s 分别是请求实体和服务实体, $rw \in (\text{read}, \text{write})$. 授权模板依据多级安全规则进行授权,授权规则如下:

当且仅当请求主体 E_r 的安全级大于等于服务实体 E_s 的安全级时,请求实体 E_r 被授予 read 权限,拥有此权限,请求实体即可获得服务实体所提供的服务权限集合 op_s ; 当且仅当请求主体 E_r 的安全级小于等于服务实体 E_s 的安全级时,请求实体 E_r 被授予 write 权限,则服务实体会拒绝请求实体获得服务权限集合 op_s 的要求. 即

if ($\text{entityLabel}(E_r) \geq \text{entityLabel}(E_s)$) $\Rightarrow (rw = \text{read})$

then $op_r = op_s$

else $op_r = \text{null}$.

3.1 动态访问控制策略

策略 1 实体安全级函数 $\text{entityLabel}(E)$ 完成实体到安全级的映射. 其中, 服务实体 E_s 的安全级

相对稳定, 始终处于激活态, 而请求实体 E_r 的安全级一开始处于休眠态.

策略 2 只有请求实体 E_r 处在服务实体 E_s 许可的空间范围之内时, 其安全级才能被激活.

策略 3 处于激活态的请求实体 E_r 的安全级, 其存在生命周期, 一旦超出周期时间限制, 其安全级会重回休眠态.

普适计算环境中, 存在大量的普适服务实体, 比如, 大量的传感器、计算设备、跟踪定位设备等, 这些实体的安装位置相对固定, 出于简单考虑, 在构建普适多级安全环境时, 为这些设备赋予稳定的安全级. 而作为最重要的定位目标——人(往往携带定位单元, 如智能手机、PDA、笔记本电脑等)具有很强的移动性, 其安全级要依据上下文来动态授予或撤销.

普适请求实体 E_r 的安全级经安全级函数 $\text{entityLabel}(E)$ 映射后, 安全级就处于休眠状态, 它的状态是时空敏感的, 即随上下文(位置、时间)动态变化, 变化依据策略 2 和策略 3 实施, 安全级处于休眠态的请求实体不能进行授权. 只有当请求实体处于服务实体限定的空间范围之内时, 其安全级才能被激活, 此时可以进行授权. 而一旦请求实体脱离服务实体限定的区域时, 请求实体安全级会被挂起, 只有再次满足空间约束条件后, 其安全级才会被重新激活. 请求实体安全级被激活后, 存在生命周期, 超出周期时间限定后, 实体安全级会再次回到休眠状态. 图 1 为请求实体安全级状态转换图^[5].

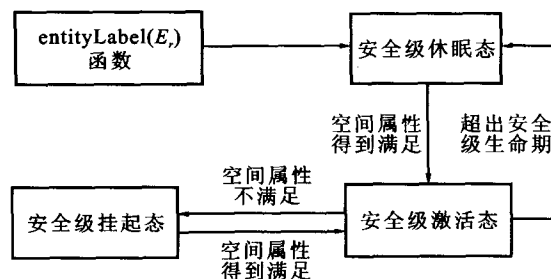


图 1 请求实体安全级状态转换图

3.2 动态多级安全访问控制算法

动态多级安全访问控制是当普适请求实体(通常为携带定位单元的用户)进入普适环境时, 系统依据预先定义的动态访问控制策略, 对是否允许执行用户请求作出决策. 动态访问控制算法描述如下. 其中, 变量 D 是服务实体 E_s 的空间约束限定距离, 此距离变量的值由不同的服务实体 E_s 决定, 例如, 只有当请求实体和服务实体空间直线距离小于等于 D 时, 请求实体的安全级才可以被激活. 变量 P 是权

限生存周期,即请求实体获得服务实体提供的权限集合 op_s 后,权限在此周期约束之内有效.请求实体 E_r 的空间坐标为 (x_i, y_i, z_i) ,服务实体 E_s 的空间坐标为 (x_j, y_j, z_j) .

Step1 依据函数 $\text{entityLabel}(E)$ 计算系统中实体的安全级,将请求实体 E_r 放进休眠队列 $\text{dennedQueue} = \{E_{r1}, E_{r2}, \dots\}$,将服务实体 E_s 放入激活队列 $\text{activeQueue} = \{E_{s1}, E_{s2}, \dots\}$,其中服务实体的安全级始终处于激活态,位于激活队列中;

Step2 如果 $\text{Distance}((x_i, y_i, z_i), (x_j, y_j, z_j)) \leq D$,则将该请求实体 E_r 放入激活队列, $\text{activeQueue} = \{E_{rj}, E_{s1}, E_{s2}, \dots\}$,同时转 Step 3,否则继续跟踪实体,重复 Step 2;

Step3 如果 E_r 的安全级 L_i 大于等于 E_s 的安全级 L_j ,依据授权规则对请求实体 E_r 授权,否则转 Step 6;

Step4 计时器 count 开始计时,开始时间点放入时间变量 t_s 中,系统当前时间点放入时间变量 t_e 中;

Step5 如果 $|[t_e - t_s]| \leq P$,则转 Step 5,重复检测时间约束,否则将该请求实体从激活队列 activeQueue 中删除,同时转 Step 6;

Step6 停止.

4 结束语

文中以满足普适计算环境下访问控制授权的动态不确定性特点作为研究出发点,通过引入多级安

全思想,提出一种新的面向普适计算的动态多级安全访问控制方案.在此方案中,普适系统中请求实体的安全级是上下文敏感的,安全级的激活或休眠受到请求实体的时空属性(时间、位置)限制.当请求实体处于服务实体限定的位置区域内时,系统依据多级安全授权策略进行授权,而权限具有一定的生存周期.通过文中定义的授权策略,既实现了普适计算环境所要求的动态授权,同时又兼具多级安全信息系统的优点,增强了访问控制的安全性,进而确保了此方案更适用于普适计算环境.

参考文献:

- [1] Weiser M. Hot topics: ubiquitous computing[J]. Scientific American, 1991, 265(3):94-104.
- [2] Patrikakis C, Karamolegkos P. Security and privacy in pervasive computing [J]. IEEE Pervasive Computing, 2007, 6(4):73-75.
- [3] 王小明,赵宗涛. 基于角色的时态对象存取控制模型[J]. 电子学报, 2005, 33(9):1634-1638.
- [4] 付争方,王小明,窦文阳,等. 基于信任授权的模糊访问控制模型[J]. 微电子学与计算机, 2007, 24(9):29-31.
- [5] 武鹏,梁英,陈皓,等. 一种基于策略的跨自主域访问控制模型研究[J]. 微电子学与计算机, 2008, 25(9):7-10.

作者简介:

刘丁男, (1981-), 硕士, 助教. 研究方向为信息安全、普适计算.

(上接第101页)

6 结束语

文中介绍并实现了一种高速的 SD/SDHC/MMC 控制器设计, AHB 接口的采用使其作为 IP (intellectual property) 核的可复用度大大提升. 该设计已通过了 FPGA 验证, 并将用于某款自主知识产权的 SOC 芯片中.

参考文献:

- [1] SD Association Technical Committee. SD Specifications part 1: physical layer specification version 1.0[S]. SD Group, 2000.

- [2] SD Association Technical Committee. SD specifications part 1: physical layer specification version 2.0[S]. SD Group, 2006.
- [3] SD Association Technical Committee. SD specifications part A2: SD host controller simplified specification version 2.0[S]. SD Group, 2007.
- [4] Bhasker J. Verilog HDL 综合实用教程[M]. 孙海平, 译. 北京:清华大学出版社, 2004.

作者简介:

王宁男, (1983-), 硕士研究生. 研究方向为数字集成电路设计与验证.