高技术通讯 2010 年 第 20 卷 第 7 期:668 ~ 673

doi:10.3772/j.issn.1002-0470.2010.07.002

基于风险评估的电子飞行包系统访问控制模型①

杨宏宇② 李 伟 吕宗平

(中国民航大学计算机科学与技术学院 天津 300300)

摘 要 对电子飞行包(EFB)系统的安全访问控制问题进行了研究。提出了一种基于风险评估的 EFB 系统访问控制模型,设计了包含上下文模块、访问控制模块、风险评估模块的模型框架,定义了模型的元素和控制流程,通过上下文信息模块和基于 D-S 证据理论的风险评估模块为访问控制决策提供依据,采用基于阈值比较的访问控制决策算法和访问控制策略动态调整机制实现访问控制决策。实验结果证明该模型能有效满足 EFB 系统的安全访问需求。

关键词 电子飞行包(EFB),访问控制,风险评估,D-S 证据理论,阈值比较

0 引 言

电子飞行包(electronic flight bag,EFB)[1,2]是民航信息技术领域的一项最新技术,EFB 系统的应用将民航飞机驾驶舱的数字信息传输与管理提高到一个新水平。EFB 可完成飞行准备阶段的各种计算和检查,提供飞行过程中的实时飞行性能、油料计算等功能并供飞行人员实时查询[1,2]。在 EFB 系统中,数据访问控制是一项关键的安全技术,它能在保证合法用户访问资源的前提下有效限制用户对关键资源的访问。由于 EFB 系统的数据访问控制直接关系到飞行安全和空防安全,因此对该系统的访问控制安全性要求极高。

EFB 系统中与飞行相关的数据来源于航空公司、机场和数据服务提供商的资源系统,由于航班任务存在差异,每次飞行前 EFB 系统需要访问的资源系统有所不同。目前广泛使用的是基于角色的访问控制[3]。EFB 系统的数据源系统多样,是典型的分散授权管理和集中访问控制系统,故采用基于角色的访问控制机制将会导致用户、角色、权限的映射关系极为庞杂、效率不佳且难以监控,无法满足 EFB 系统用户权限随时间、任务和环境的不同而变化的需求;另一方面,也会导致对整个系统风险的量化评估存在较大困难,使得系统的整体风险无法控制。为此,本文引入了风险评估模块,建立了一种灵活可变、指标量化、适应 EFB 系统需要的访问控制模型,以满足 EFB 系统的访问安全性需求。

1 相关工作

传统的访问控制技术主要包括自主访问控制、强制访问控制(如 Bell-Lapadula)和基于角色的访问控制(如 ARABC02、CL03[3])。近年来又出现了基于策略、基于任务、基于工作流、基于信任度等的多种访问控制模型[4],以提高访问控制机制的灵活性和适应性,解决工作流系统、P2P 网络环境、普适计算、虚拟企业、网格等领域的访问控制问题。

文献[5]提出了一个针对协同环境下 CAD 模型的多层次动态的安全访问控制模型,利用多层次的权限模型实现了产品模型的多粒度访问控制,通过引入权限的依赖关系及权限状态迁移概念,实现了权限的动态授权管理。该模型的权限层次划分、权限依赖关系定义等预处理过程非常繁琐,较容易出现错误。该模型针对 CAD 领域,不能直接应用于信息系统。文献[6]提出了一种访问控制模型,引入上下文信息对访问请求操作可能产生的后果赋予不同的权重,给出在可用性、完整性、机密性方面的损失值并计算得到访问请求操作的风险值,通过比较结果给出访问决策。但该模型并未给出确定损失值的具体方法,风险计算方法不能准确反映评估因素间的相互冲突和评估因素对总体风险值的实际影响。

① 863 计划(2006AA12A106),国家自然科学基金(60776807),天津市科技支撑计划重点项目(07ZCKFGX01700)和中国民航科技基金(RKXZY0814)资助项目。

② 男,1969 年生,博士,教授;研究方向:网络与信息安全;联系人,E-mail: yhyxlx@hotmail.com

(收稿日期:2009-04-01)

文献[7]将 Dempste-Shafer (D-S)理论引入信息安全的风险评估过程,弥补传统评估方法在解决不确定性信息上的不足。该文献论证了 D-S 理论在进行信息安全风险评估上的优越性,但并未涉及其在访问控制方面的应用。文献[8]提出了一种基于收益与风险的访问控制模型,针对数据修改和读访问请求操作,分别给出其收益和风险向量,以有向图描绘信息传递的过程,通过收益值和风险值比较做出访问控制决策。该模型中收益和风险向量的计算过程依赖于对该有向图的实时调整和分析,因此具有较高的算法复杂度,在实现方面困难较大。

2 模型设计

2.1 访问控制模型框架

由于 EFB 系统结构复杂,各数据资源子系统分布部署,且在具体实现上有较大差异,因而对访问控制系统的安全性要求较高。因此,EFB 系统的访问控制模型应满足通用性强、流程简单、指标量化且充分考虑环境因素等要求。根据上述要求,本文提出了一种基于风险评估的 EFB 系统访问控制模型,其框架如图 1 所示。EFB 系统访问模型主要包含三个模块:上下文模块、访问控制模块、风险评估模块。

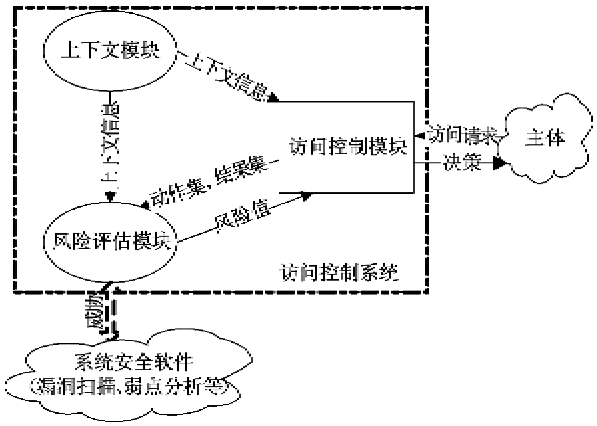

图 1 访问控制模型框架

上下文模块负责收集用户与系统的状态及环境信息,综合分析后形成上下文信息,为访问控制模块和风险评估模块提供依据。上下文信息的主要内容包括网络连接情况、通信成本及带宽、资源位置、用户状态与所在地点、正在进行的活动等。访问控制模块是整个模型的核心,负责接收用户对于资源的访问请求,进行分析,收集相关参数并发送给风险评估模块。在收到风险评估的结果之后,做出相应的决策并最终返回给用户。风险评估模块是整个模型的关键,它负责收集影响当前系统风险的因素,结合访问控制模块及上下文模块发来的相关信息,通过计算最终得出风险等级及危害程度。

2.2 控制流程

为准确描述基于风险评估的 EFB 系统访问控制模型对用户访问请求的控制流程,在详细分析图 1中模型框架各模块的数据交换过程及依赖关系的基础上,定义模型元素如下:主体(Subject)——用户(飞行人员或地面人员)或某段程序;资源(Resource)——可被访问的飞行数据对象,依据资源重要性可将资源划分为极重要资源(Ⅰ类)、重要资源(Ⅱ类)、一般资源(Ⅲ类)三种类型;操作(A)——主体要求对资源所进行的动作;结果序列(O)——某个动作可能产生的全部后果的集合,将对访问操作整体风险产生影响;上下文属性——EFB 系统中与访问控制相关的环境因素(如时间、地点、通信方式、网络状态、操作类型、资源状态等),由上下文模块对系统环境抽取得到;上下文序列(S)——全体上下文属性的集合,用于描述 EFB 系统当前的环境信息。各属性的不同取值构成上下文序列的不同状态,如 S_1 =(白天,机场,使用机场地面网络,网络状态空闲,进行飞行数据读操作,数据文件较小)。

在 EFB 访问控制模型中,本文设计的系统访问控制流程如图 2 所示。

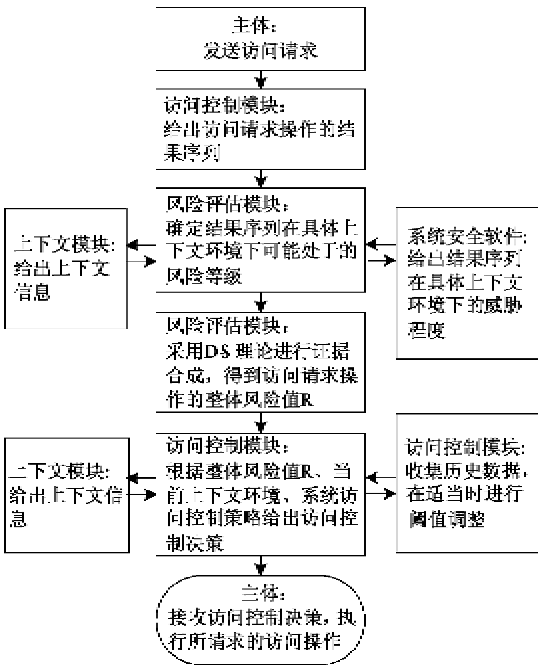

图 2 EFB 系统访问控制流程图

3 风险评估

风险评估是 EFB 系统访问控制模型的关键模块。信息系统风险的复杂性、关联性和多样性导致评估过程中存在大量的不确定性[9,10],因此采用合适的方法对不确定性进行处理则成为 EFB 系统访问控制模型的一个关键问题。

D-S 理论可以对不确定性进行量化描述,并可对多来源获得的不同证据及他们之间的冲突进行有效融合[11],因此在信息安全风险评估中取得了较好的效果。本文采用 D-S 理论对主体访问请求操作的风险进行评估,为访问控制决策提供准确的依据。Shafer 提出改进合成法则,采用"折扣率"的方法有效降低证据间的冲突[11]。本文采用这一改进合成法则进行了证据合成与风险计算。

3.1 风险评估指标体系

为便于应用 D-S 理论进行风险评估,需要首先构建影响访问请求操作风险的各项基本因素的评估指标。基于访问控制模型框架,本文建立了 EFB 系统的风险评估指标体系(如图 3 所示),将指标状态集作为识别框架 Θ。在 EFB 系统中,最常用的操作是对飞行数据的只读访问,因此 Θ 中的动作仅以数据读操作为对象进行说明。

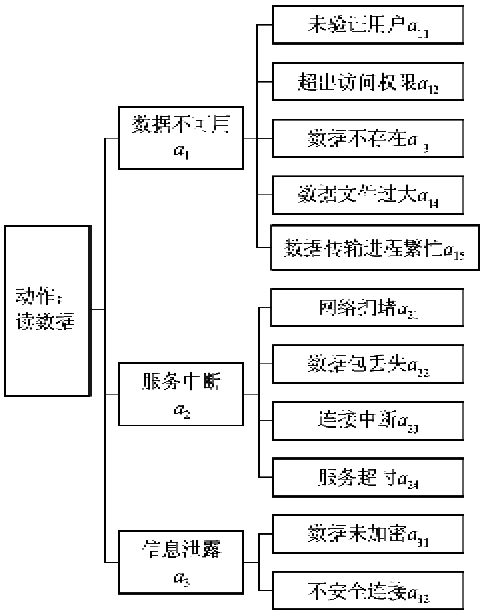

图 3 EFB 系统的风险评估指标体系

$A = \{a_1, a_2, a_3\}$:设当前请求进行的访问操作为读数据,其可能导致的结果为:数据不可用、服务中断、信息泄露,则访问请求操作的综合风险 A 被分解为 a_1, a_2, a_3 三个影响因素,即指标 A 可分解为 a_1, a_2, a_3 三个子指标,a_i 对应的权重为 $\omega_i (i = 1,2,3)$。

$A_1 = \{a_{11}, a_{12}, a_{13}, a_{14}, a_{15}\}$:$a_1$ 可能处于 5 种上下文环境中,每种上下文环境可能处于不同的风险等级,分别对应不同的基本可信度值,其基本可信度分配函数为 m_{1j}。a_{1j} 对应的权重为 $\omega_{1j} (j = 1,2,3,4,5)$。同样可定义指标子集 A_2 和 A_3 及其元素对应的权重。

$X = \{x_1, x_2, \cdots, x_k\}$ 为风险评估指标体系评语集[7],$x_h (h = 1,2,\cdots,k)$ 为具体评语,即所处的风险等级[12],如:X = {极高风险(x_1),很高风险(x_2),高风险(x_3),中等风险(x_4),低风险(x_5),很低风险(x_6),极低风险(x_7)}。$m_{ij}(x_h)$ 表示子元素 a_{ij} 关于 $x_h (h = 1,2,\cdots,k)$ 的基本可信度。

3.2 Dempster 合成法则

得到 EFB 系统的各评估指标关于评语集 X 的基本可信度分配后,按照 Dempster 合成法则[11]对其进行合成,给出访问请求操作的整体风险。另外,合成过程也可以减少系统的不确定性,得到准确结果。

Dempster 合成法则:设 m_1 和 m_2 是同一识别框架 Θ 上的 2 个基本可信度分配函数,则可用 $m = m_1 \oplus m_2$ 表示 m_1 和 m_2 的合成,称为 m_1 和 m_2 的直和,计算如下:

$$m(A) = \begin{cases} 0 & (A = \varnothing) \\ \dfrac{\sum\limits_{A_i \cap B_j = A} m_1(A_i) m_2(B_j)}{1 - K} & (A \neq \varnothing) \end{cases} \tag{1}$$

其中 $K = \sum\limits_{A_i \cap B_j = \varnothing} m_1(A_i) m_2(B_j)$。多个基本可信度分配函数的合成按上式依次进行。

3.3 改进后的合成法则

各指标的基本可信度分配(即证据)间可能存在冲突,导致合成结果不准确,因此需要采用改进的 Dempster 合成法则[11]减小冲突对评估结果的影响,以满足 EFB 系统访问控制模型对风险评估模块的精确性要求。改进后的合成法则为各个证据分配了不同的权重。设证据集为 $E = \{E_1, E_2, \cdots, E_n\}$,证据 E_i 权重系数为 ω_i,则所有的权重系数组成了证据的权重向量 $W = (\omega_1, \omega_2, \cdots, \omega_n)$,满足 $\omega_i \in [0, 1]$ 且 $\sum\limits_{i=1}^{n} \omega_i = 1$。权重系数反映了证据在合成过程中

的重要程度。

首先,在识别框架内为各命题分配基本可信度值,并建立证据的权重向量 $W = (\omega_1, \omega_2, \cdots, \omega_n)$。其次,设 $\omega_{\max} = \max\{\omega_1, \omega_2, \cdots, \omega_n\}$,可得证据基本可信度的"折扣率" $\alpha_i (0 \leqslant \alpha_i \leqslant 1)$, $(1 - \alpha_i) = \omega_i / \omega_{\max}, i = 1,2,\cdots,n$。利用"折扣率"按如下方法调整识别框架内所有命题的基本可信度,得到调整后的基本可信度分配函数:

$$m_i'(A_k) = (1 - \alpha_i) m_i(A_k) \tag{2}$$

$$m'(\Theta) = (1 - \alpha_i) m(\Theta) + \alpha_i \tag{3}$$

式中 $k = 1,2,\cdots,d_i$, d_i 为证据 E_i 提供的识别框架中非 Θ 基本可信度个数。$m'(\Theta)$ 代表调整后对于不确定性的基本可信度。改进后的信度函数为

$$Bel'(A) = \sum_{B \subseteq A} m'(B) \quad (\forall A \subseteq \Theta) \tag{4}$$

最后,将各证据的所有命题调整后的基本可信度值 $m_i'(A_k)$、$m'(\Theta)$ 代入公式(1),构成新的证据合成公式。

在访问请求操作风险评估中, $m_{ij}'(x_h)$ 代表调整之后 a_{ij} 对风险等级 x_h 的基本可信度分配。应用改进的 D-S 合成规则对 $m_{ij}'(x_h)$ 进行合成,可以得出 a_i 对风险等级 x_h 的基本可信度分配 $m_i'(x_h)$,通过进一步合成得到某个访问请求操作对风险等级 x_h 的可信度分配 $m'(x_h)$。

3.4 风险计算

在基于风险评估的 EFB 系统访问控制模型中,访问控制决策的制定依赖于精确量化的风险评估结果。根据访问请求操作对风险等级 x_h 的可信度分配 $m'(x_h)$ 和风险危害程度,计算得到访问请求操作的风险量化指标[7]。

设 $P(X) = \{p(x_1), \cdots, p(x_k)\}$ 为专家关于指标体系评语集 X 给出的风险事件一旦发生所造成的危害程度。$p(x_h)(h = 1,2,\cdots,k)$ 为对应于风险等级 x_h 的危害程度平均值,其取值范围为 $0 \leqslant p(x_h) \leqslant 1$。

由于 x_h 的子集都是单个元素,则由式(4)得访问请求操作对风险等级 x_h 的信度函数为

$$Bel'(x_h) = m'(x_h) \quad (\forall x_h \subseteq \Theta) \tag{5}$$

由此可以得到访问请求操作的整体风险值为

$$R = \sum_{h=1}^{k} P(x_h) Bel'(x_h) \tag{6}$$

4 访问控制策略

4.1 策略描述

访问控制策略是描述 EFB 系统的安全需求而指定的对用户行为进行约束的一整套严谨的规则,用以确定主体是否对客体拥有访问权限。EFB 系统采用基于风险评估的访问控制策略,以满足系统对较高访问安全性的需求。

在基于风险评估的 EFB 系统访问控制模型中,系统管理员制定的访问控制策略以访问控制策略表的形式表示。当风险评估模块给出的访问请求操作风险值小于访问控制策略表中相应阈值时,则允许对资源的访问,否则拒绝访问。

4.2 阈值设定

阈值是预先设定的风险值,体现了 EFB 系统对资源访问所造成的风险的容忍度。阈值的设定是为了达到资源利用率与系统受威胁程度的平衡。设对某资源的所有访问请求中,有 30% 的操作风险值大于 0.9,则阈值 0.9 保证资源利用率为 70%,系统风险低于 0.9。

阈值的初始值根据系统模拟试运行获取的数据进行设定,其过程如下:首先,设定初始阈值为 1,即允许一切访问请求。其次,设经过一段时间的模拟试运行后,测得在上下文序列 S_1 中对Ⅰ类资源进行读操作的访问数据(表 1)。

系统管理员根据以上数据和资源重要性,在系统风险和资源利用率中进行权衡,决定阈值大小。例如,系统管理员在访问控制策略表中设定该项的阈值为 0.8,即保证资源利用率为 70%,系统风险低于 0.8。最后,按照以上方法依次设定访问控制策略表的其他各项阈值,形成访问控制策略表。

4.3 访问控制决策过程

在基于风险评估的 EFB 系统访问控制模型中,风险评估模块计算访问请求操作的风险值 R,并将其发送给访问控制模块。访问控制模块根据待访问资源类型、访问请求操作类型、主体的上下文环境在访问控制策略表中查找对应阈值,将 R 值与阈值比

表 1 读操作的访问历史数据

风险值	<0.1	0.1~0.2	0.2~0.3	0.3~0.4	0.4~0.5	0.5~0.6	0.6~0.7	0.7~0.8	0.8~0.9	>0.9
访问请求次数	1	2	10	15	9	15	10	8	20	10

较,若 R 小于阈值则允许访问,否则拒绝访问。

访问控制模块记录一段时间内对某项资源的访问请求次数和所有访问请求操作的风险值,统计分析后对访问控制策略进行动态调整。

对时间段 T 内,在上下文序列 S_1 下请求对Ⅰ类资源进行读操作的历史数据进行分析,结果如图4所示。设当前访问控制策略表中该项阈值为0.7,由图3可以看出资源利用率偏低,对EFB系统的性能造成了不利影响。因此,系统管理员可以采取以下措施加以调整:(1)调高阈值至0.8,保证较高的资源访问率;(2)保持阈值不变,采取措施减少当前系统中存在的威胁、弱点等不安全因素,使得风险评估模块给出的访问请求操作风险值降低到小于阈值的水平,保证较高的资源利用率。

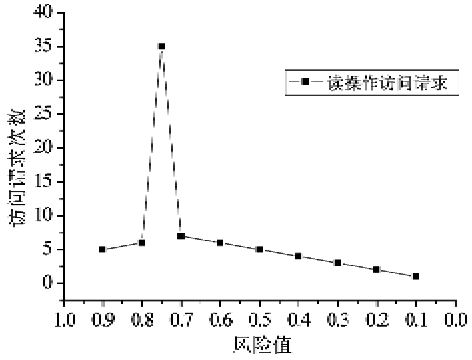

图4 读操作访问控制统计

5 实验与分析

为了验证EFB访问控制模型的有效性,应用本文提出的模型对图3所示的指标体系进行风险评估。实验过程如下:

(1)确定各指标基本可信度。确定各层权重及 a_{ij} 关于 $x_k(k=1,2,\cdots,k)$ 的基本可信度 $m_{ij}(x_h)$,其中 Θ 表示不确定性。$m_{ij}(x_h)$ 的值可通过风险评估模块与系统安全软件的交互确定,权重值可由层次分析法(analytic hierarchy process, AHP)得到,如表2所示。

表2 风险评估指标体系基本可信度分配

动作	结果	权重 ω_i	上下文信息	权重 ω_{ij}	基本可信度 x_1	x_2	x_3	x_4	x_5	x_6	x_7	Θ
访问动作:读数据	数据不可用 a_1	0.19	未验证用户 a_{11}	0.252	0.2	0.3	0.1	0	0.1	0.1	0.2	0
			超出访问权限 a_{12}	0.254	0	0.2	0.1	0.1	0.1	0.1	0.2	0.2
			数据不存在 a_{13}	0.093	0.15	0.1	0.3	0.2	0	0.1	0	0.15
			数据文件过大 a_{14}	0.187	0	0.1	0.15	0.2	0.1	0.1	0.3	0.05
			数据传输进程繁忙 a_{15}	0.214	0.1	0.2	0.1	0.1	0.3	0	0.1	0.1
	服务中断 a_2	0.29	网络拥堵 a_{21}	0.176	0	0	0.1	0.2	0.3	0.2	0.1	0.1
			数据包丢失 a_{22}	0.213	0.1	0.1	0.2	0.1	0.2	0.1	0.05	0.15
			连接中断 a_{23}	0.325	0.2	0.2	0.1	0.1	0.1	0.1	0.1	0.1
			服务超时 a_{24}	0.286	0.2	0.1	0.1	0.2	0.1	0.3	0	0
	信息泄露 a_3	0.52	数据未加密 a_{31}	0.437	0	0.1	0.1	0.3	0.1	0.2	0.1	0.1
			不安全连接 a_{32}	0.563	0.3	0.1	0.1	0.2	0	0.1	0.1	0.1

(2)计算调整后的基本可信度。计算“折扣率”$(1-\alpha_i)$,并由式(2)和式(3)计算用“折扣率”加以调整后的基本可信度值。

(3)数据合成。利用式(1)依次对 $m'_{ij}(x_h)$ 进行数据合成,得到 $m'_i(x_h)$。

(4)计算访问请求操作的基本可信度分配。对基本可信度分配数据重复步骤(2)和步骤(3)的处理过程,得到调整后的 a_i 对风险等级 x_h 的基本可信度分配 $m''_i(x_h)$ 和合成后的访问请求操作A对风险等级 x_h 的基本可信度分配 $m''(x_h)$,结果如表3所示。

(5)计算信度函数。用式(5)计算访问请求操作的信度函数,得 $Bel''(x_1)=m''(x_1),\cdots,Bel''(x_7)=m''(x_7)$。

表3 合成结果

$m''(x_h)$							
x_1	x_2	x_3	x_4	x_5	x_6	x_7	Θ
0.232	0.118	0.089	0.268	0.026	0.133	0.093	0.042

(6)计算安全风险值。设 $P(X)=\{p(x_1),p(x_2),p(x_3),p(x_4),p(x_5),p(x_6),p(x_7)\}=\{1,0.85,0.7,0.55,0.4,0.25,0.1\}$,由公式(6)计算得到访问请求操作可能存在的风险值为0.5953。

(7)访问控制决策。访问控制模块根据访问请求操作风险值 R、主体的上下文环境,并根据 EFB 系统的访问控制策略给出最终的访问控制决策,完成访问控制系统与主体的对话过程。系统访问控制策略如表 4 所示。表 4 给出了数据访问动作在不同上下文序列下的风险阈值,通过风险值 R 与阈值的比较给出访问控制决策。

表 4 Ⅰ类资源访问控制策略

访问动作	上下文信息序列				
	S_1	S_2	S_3	S_4	S_5
读数据	<0.5	<0.6	<0.8	<0.3	<0.2
修改数据	<0.3	<0.4	<0.9	<0.7	<0.1
删除数据	<0.8	<0.9	<0.7	<0.2	<0.1

设当前上下文序列为 S_1,待访问资源为极重要资源(Ⅰ类),由上述步骤计算得到的读操作风险值 R 大于阈值,给出的访问控制决策为"拒绝该主体的访问请求"。

6 结 论

电子飞行包(EFB)系统涉及飞行安全,对访问控制与系统风险的要求较高,本文提出的基于风险的访问控制机制较好地满足了 EFB 系统在系统风险可量化、访问权限与上下文环境密切相关、访问控制机制灵活性强等方面的要求。通过实验分析表明,本文提出的访问控制模型及流程适合 EFB 系统的需要,应用 D-S 理论进行风险评估可有效解决各指标间的相互冲突,减少由此带来的系统不确定性,得到的量化评估结果为访问控制决策的制定提供清晰可靠的依据。未来的工作将集中于加强访问控制策略与风险评估过程中各指标基本可信度分配的自适应性及提高访问控制模型的效率方面。

参考文献

[1] Theunissen E, Koeners G J M, Roefs F D, et al. Evaluation of an electronic flight bag with integrated routing and runway incursion detection functions. In: Proceedings of the 24th Digital Avionics Systems Conference, Washington, DC, USA, 2005.1: 4.E.1-41-11

[2] 吕小平. 电子飞行包(EFB)系统介绍.中国民用航空, 2007, 10 (82): 47-50

[3] 杨秋伟,洪帆,杨木祥等.基于角色访问控制管理模型的安全性分析.软件学报, 2006, 17 (8): 1804-1810

[4] 林闯,封富君,李俊山.新型网络环境下的访问控制技术.软件学报, 2007, 18 (4): 954-966

[5] 方萃浩,叶修梓,彭维等.协同环境下 CAD 模型的多层次动态安全访问控制.软件学报, 2007, 18(9): 2295-2305

[6] Diep N, Hung L, Zhung Y, et al. Enforcing access control using risk assessment. In: Proceedings of the 4th European Conference on Universal Multiservice Networks, Toulouse, France, 2007. 419-424

[7] Gao H, Zhu J, Li C. The analysis of uncertainty of network security risk assessment using Dempster-Shafer Theory. In: Proceedings of the 12th International Conference on CSCW in Design, Xi'an, China, 2008. 754-759

[8] Zhang L, Brodsky A, Jajodia S. Toward information sharing: benefit and risk access control (BARAC). In: Proceedings of the IEEE 7th International Workshop on Policies for Distributed Systems and Networks, London-Ontario, Canada, 2006. 9-13

[9] 周傲英,金澈清,王国仁等.不确定性数据管理技术研究综述.计算机学报, 2009, 32(1):1-16

[10] 张永铮,方滨兴,迟悦等.用于评估网络信息系统的风险传播模型.软件学报, 2007, 18(1):137-145

[11] 段新生. 证据理论与决策、人工智能. 北京:中国人民大学出版社, 1993. 6-36

[12] 计算机信息系统安全保护等级划分准则[GB 17859-1999]. 北京:质检总局, 1999

An access control model for electronic flight bag systems based on risk assessment

Yang Hongyu, Li Wei, Lu Zongping

(School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300)

Abstract

This paper studies the secure access control issues of electronic flight bag (EFB) systems. A risk assessment based access control model for EFB systems is proposed. An access control model framework with the modules of context, access control and risk assessment is given, and the elements and the control procedure of the model are defined. The parameters for access control decision can be obtained through the context module and the Dempster-Shafer theory based risk assessment module. Then the access control decision can be achieved through the threshold comparison based access control decision algorithm and the dynamic adjustment mechanism of access control strategies. The experimental result demonstrates that this access control model can effectively meet the secure access requirements of EFB systems.

Key words: electronic flight bag (EFB), access control, risk assessment, Dempster-Shafer theory, threshold comparison