DOI:10.3876/j.issn.1000-1980.2020.03.014

跨域云环境下基于动态异构网络的风险访问模型

文 静[1,2],袁家斌[1],王诗璇[1],魏利利[3]

(1.南京航空航天大学计算机科学与技术学院,江苏 南京 211106;
2.淮阴师范学院计算机科学与技术学院,江苏 淮安 223300;3.中国兵器工业第二〇八研究所,北京 102202)

摘要:针对在动态异构网络中传统的访问控制机制复杂度高、灵活性差、数据安全性支持不足的问题,提出一种引入风险管理机制的多级安全访问模型。为每一个域设定动态风险阈值,对发起访问的主体和被访问的客体进行风险预审核。在设定的访问周期内对访问次数、累计访问风险值、最大访问风险值进行比较并给出限制条件,对频繁发起访问的低风险主体给予风险预支额度,在未透支风险额度的情况下允许其进一步访问。访问结束后,会动态调整本域风险阈值,使之具有一定的动态适应性。

关键词:多级安全;访问控制;动态风险阈值;风险预支;历史访问记录;异构网络
中图分类号:TP309 **文献标志码**:A **文章编号**:1000-1980(2020)03-0284-07

Risk access model based on dynamic heterogeneous network in cross-domain cloud environment

WEN Jing[1,2], **YUAN Jiabin**[1], **WANG Shixuan**[1], **WEI Lili**[3]

(1. *College of Computer Science and Technology*, *Nanjing University of Aeronautics and Astronautics*, *Nanjing* 211106, *China*;
2. *College of Computer Science and Technology*, *Huaiyin Normal University*, *Huaian* 223300, *China*;
3. *NO.* 208 *Research Institute of China Ordnance Industries*, *Beijing* 102202, *China*)

Abstract: Aiming at the high complexity, poor flexibility and security problem in the traditional cross-domain access under the dynamic heterogeneous network environment, this paper proposed a multi-level security access model that introduced the risk management mechanism, where a dynamic risk threshold is set for each domain and a risk pre-audit is performed on both subject and object of the access. The model compares the number of access, the cumulative access risk values, and the maximum value within the set access period and then stipulates restriction conditions. For low-risk entities that frequently initiate access, a risk advance limit is offered, and further access is allowed in case of non-overdraft risk limit. After the access, the risk threshold of the domain will be adjusted dynamically to make it a certain dynamic adaptability.

Key words: multi-level security; access control; dynamic risk threshold; risk advance; access history record; heterogeneous network

作为大数据的基础平台和支撑技术的云计算而言[1-2],云中的访问控制所涉及的资源可能由于云的分布式特点而位于不同域,这就构成了一个巨大而复杂的异构数据环境[3]。针对分布式异构环境下跨域安全互操作,要求能实现信息资源的安全共享[4]。当前在云端实现信息安全共享的主流方式是访问控制,访问控

基金项目:国家重点研发计划(2017YFB0802303);国家自然科学基金面上项目(61571226);南京市产学研合作后补助项目计划(201722025)

作者简介:文静(1978—),女,副教授,博士研究生,主要从事信息安全与无线传感器网络研究。E-mail:grace@hytc.edu.cn

引用本文:文静,袁家斌,王诗璇,等.跨域云环境下基于动态异构网络的风险访问模型[J].河海大学学报(自然科学版),2020,48(3):284-290.
WEN Jing, YUAN Jiabin, WANG Shixuan, et al. Risk access model based on dynamic heterogeneous network in cross-domain cloud environment[J]. Journal of Hohai University(Natural Sciences),2020,48(3):284-290.

制主要有基于角色的访问控制、基于任务的访问控制和基于属性的访问控制 3 种[5]。在传统的分布式环境下,其访问控制模型中的主体一般只需一次授权即可使用,对环境的动态变化适应性较差。但是在云环境下,异构网络具有动态变化的特性,节点或边的变化会对当前的风险识别及跨域访问造成影响[6-7]。不确定性和动态性是多自治域环境的特点,保证数据资源安全性是安全策略的基本要求,二者之间的矛盾给多自治域环境中互操作带来许多风险和安全隐患[8-9]。目前针对动态异构网络中的访问控制机制未能较好地利用历史访问信息,限制高风险的节点访问,也没有对风险值进行实时更新,自适应性较弱[10]。

Lyu 等[11]提出了一个云服务下基于图形工具的安全风险评估模型,可以清晰描述云服务的虚拟化安全风险场景,准确评估虚拟化安全风险因素,其方法能够较好地模拟云服务中复杂的动态安全问题。Zheng 等[12]针对云模型不适用于非正态分布的问题,提出了一种基于均匀分布的一维后向云算法,建立了一种可信度评估指标,并将其应用于云中可信度评估,然而该算法仅适用于单个云环境的情况。Uikey 等[13]提出了一种可扩展的访问控制体系结构和授权机制,该机制为多领域云环境下的资源管理策略提供了一个灵活的框架,但是该方法没有考虑到风险的因素。Dos-Santos 等[14]针对传统访问控制模型无法满足特定安全要求的问题,提出了一种基于 XACML 扩展的风险管理框架,然而该框架没有考虑到访问双方的历史信息。Laleh 等[15]提出了一种针对用户行为的风险评估模型,认为如果用户行为与“正常行为”的差异越大则风险越大,然而在云环境中,定义完整的“正常行为”几乎是不可能的。从已有的文献来看,较少考虑到访问记录对于风险的影响,无法适应异构跨域访问。拒绝频繁访问的操作没有考虑允许低风险高优先级的主体访问请求。

本文针对大数据云平台分布式异构环境下节点跨域访问风险问题,考虑到多个安全管理域的特点,建立跨域的访问控制模型,将自适应的风险动态阈值运用于带有记忆分量的多级安全模型中,对发起访问的主体和被访问的客体进行风险预审核,在本次访问请求结束后,无论访问是成功还是失败,管理节点都会实时调整本域风险阈值,使之具有一定的动态适应性,从而提高访问的灵活性,降低访问的风险,保证系统的安全性。

1　风险访问模型

分布式环境下的节点具有较强的动态性和不确定性,节点的风险值会随着访问历史记录及时间的变化而改变。本文的风险量化采用定量和定性相结合,随着历史访问次数的增加,风险值会变得越来越客观。模型涉及的风险值主要包含节点的风险值和域风险值。节点风险值由初始风险值、历史风险值和频率风险值组成。域风险值由本域指定的管理节点保存。当本域节点产生变化时需要对域风险值进行实时调整和更新。域中节点的风险值表示为$r_i(i=1,2,\cdots,m)$,m 为域 d 中的节点总数。

1.1　模型概述

云中任意自治域中的主体向域中客体发出访问请求。首先,由管理节点主观设置风险阈值初始值赋予所属域管理节点。访问过程中需要将主体在访问周期内访问次数计数器的值和设定的最大访问次数进行比较,如果该值小于设定的最大访问次数则可以进入下一步;否则该节点将被定义为频繁访问节点,需要判断节点是否为低风险节点。如果该节点为低风险节点,则由本域管理节点分配预支风险值进入下一步。当该节点的风险值小于访问域和被访问域设定的风险阈值,被访问域中的客体才会对主体的访问请求做出反馈。当访问请求结束后,不管本次访问请求成功与否,访问发起域和被访问域的域管理节点都需要对本次访问操作相互做出评价,各域管理节点根据评价值修改本域风险阈值。

1.2　初始风险值

节点的初始风险值记为$r_{\text{ini}}\in[0,1]$,根据访问类型、被访问资源的敏感程度等多评测因素由管理节点主观的综合设定。此项指标虽然对节点风险值具有一定的主观性和静态性影响,但是由于后期将受到历史访问记录r_{his}的影响,节点的风险值将会变得越来越客观和动态。设风险因素集为 $U_{\text{F}}=[u_1,u_2,\cdots,u_l]$,其中 l 代表风险因素的个数。定义权重集为 $A_{\text{F}}=[a_1,a_2,\cdots,a_l]$,其中$a_l$ 表示第 l 个风险因素的权重,并且满足非负性与归一性,即$a_i\geqslant 0(i=1,2,\cdots,l)$, $\sum_{i=1}^{l} a_i=1$。对风险的评价集为 $V_{\text{F}}=[v_1,v_2,\cdots,v_k]$,$k=7$,其中$v_k$ 由低到高分别表示拒绝、高风险、低风险、中等风险、低安全、高安全和允许访问。隶属度矩阵 $\boldsymbol{Q}=(q_{ij})_{l\times k}$,其中 $q_{ij}=v_{ij}/\sum_{j=1}^{k} v_{ij}(i\in[1,l],j\in[1,k])$ 表示因素u_i对评语v_j的隶属度,从而可得初始风险函数:

$$r_{ini}(s)=\frac{\sum_{i=1}^{k} v_i b_i}{\sum_{i=1}^{k} b_i} \tag{1}$$

式中:b_i——评价结果向量 $\boldsymbol{B}$ 中第 i 个评价结果。

1.3 历史风险值

历史访问记录是评估节点风险的重要信息,对节点间交互的历史访问记录进行综合与分析,得出每一个节点的历史风险值。可以将历史风险值r_{his}分为两部分,即直接访问风险值r_{his1}和间接访问风险值r_{his2}。

1.3.1 直接访问风险值r_{his1}

r_{his1}表示历史直接访问累计的风险值。H_{ij}表示主体 s_i 申请访问客体o_j的总次数,S_{ij}表示节点间直接交互过程中成功的次数,F_{ij}表示节点间直接交互过程中失败的交易次数,无法确定交互是否成功或者失败的次数用U_{ij}来表示,显然$H_{ij}=S_{ij}+F_{ij}+U_{ij}$。直接访问风险值可表示如下:

$$r_{his1}=\begin{cases}1-\dfrac{S_{ij}}{H_{ij}} & H_{ij}\neq 0\\ 1 & H_{ij}=0\end{cases} \tag{2}$$

在访问周期内,为使直接风险值更加客观,设定 t 为风险更新的时间片,很明显 $t<t_{d\text{-}p}$,$t_{d\text{-}p}$为当前域 d 管理节点设定的时间周期。节点 i 对直接风险值进行周期为 t 的更新。设在t_n至t_{n+1}时段($t_{n+1}=t_n+nt,n\geqslant 0$),管理节点根据近期历史访问记录对$t_n$时刻的直接风险值进行更新,得到$t_{n+1}$时刻的风险值,$r_{his1}$的计算修正如下:

$$r_{his1}=\frac{(1-\mu)S_{ij}+\mu\Delta S_{ij}}{H_{ij}} \tag{3}$$

式中:ΔS_{ij}——本访问周期交互成功的次数;μ——由本域管理节点设置的更新权重,如果 ΔS_{ij}大于本访问周期交互失败的次数,则约定 $\mu\in(0.5,1)$,否则 $\mu\in(0,0.5)$。

1.3.2 间接访问风险值r_{his2}

被询问节点 k 必须和询问节点 i 有过安全的历史交易,节点可信,可以表示为如下形式:$P_{ij}=\{k\mid S_{ik}+F_{ik}>0,r_{his1}(J_{req_{i,k}})>0\}$($J_{req_{i,k}}$表示主体节点 i 对客体节点 k 历史访问的函数),则间接访问风险函数可表示为

$$r_{his2}=\begin{cases}\dfrac{\sum_{k\in P_{ij}} r_{his1}(x_{ik})\, r_{his1}(x_{kj})}{\sum_{k\in P_{ij}} r_{his1}(x_{ik})} & P_{ij}\neq\varnothing\\ 1 & P_{ij}=\varnothing\end{cases} \tag{4}$$

1.4 频率风险值

在每一个访问周期$t_{d\text{-}p}$内,主体会发起多次访问,将申请访问的时长作为计算定量风险值的参考因素,请求的时间越长,风险值越大,本次访问请求的风险越高,记为访问频率风险r_{fre}。主体s_i对客体o_j的访问频率记为$p_{ij}=c_{ij}/t_{d\text{-}p}$,其中$c_{ij}$为当前主体对客体的访问次数。域 d 内所有节点的平均访问频率为 $p_d=\sum_{i=1}^{m} p_{ij}/m$,主体$s_i$的访问活跃对比度用$f_{ij}=p_{ij}/p_d$表示,在$t_{d\text{-}p}$范围内,数值越大则访问越频繁,相应的风险值也会越大。利用无理数的单调性,将频率风险限制在(0,1]范围内,此处定义与访问频率相关风险值:

$$r_{fre}=1-e^{-f_{ij}} \tag{5}$$

1.5 预支风险值

预支风险值是系统在每个访问周期为低风险节点预支的风险额度值,代表系统对其造成风险的容忍程度,也表示系统对低风险节点的信任。在本模型中,如果访问周期$t_{d\text{-}p}$内主体节点发起访问的次数已经超过c_{max}(c_{max}为域节点根据本域情况自主设定的周期内最大访问次数),并且节点在本周期内访问记录良好(即为低风险节点),且在本访问周期内访问优先级较高,那么可以向管理节点额外发出继续访问的申请,管理节点会在本周期内通过预支一定额度风险值的方式允许低风险节点的访问申请,以此提高整体访问的效率。

管理节点根据申请节点的历史访问信息为其分配风险机动额度φ_{s_i},此额度会随着访问的增加而减少,

$\varphi_{s_i}=\varphi_{s_i}-r_{s_i}$。参考历史访问记录,在周期$t_{\text{d-p}}$内,对于每一次访问($J_{\text{req}_i}(s_i,o_j,x)$ $(j=1,2,\cdots,n)$,根据直接访问风险值,基于信息熵的计算公式,得出s_i在o_j下的信息量为

$$H_{s_i}(o_j)=-\sum_{k=1}^{|c_{s_i}|}\frac{S_{ij}}{\sum_{j=1}^{n}(S_{ij}+F_{ij})}\ln\frac{S_{ij}}{\sum_{j=1}^{n}(S_{ij}+F_{ij})} \tag{6}$$

式中:c_{s_i}——访问次数计数器的值。

同样,也可以得到访问o_j的所有节点的访问记录,$c(o_j)$表示所有访问节点的个数,从而得到平均信息量$H_{\text{ave}}(o_j)=H_{\text{all}}(o_j)/c(o_j)$,即可以得到风险值 $R_{\text{lim}}(s_i,o_j)=\max(H_{\text{ave}}(o_j)-H_{s_i}(o_j),0)$,从而得到平均风险值为 $R_{\text{ave}}=\sum_{i=1}^{m}R_{\text{lim}}(s_i,o_j)/|c_{s_i}|$, 风险额度$\varphi_{s_i}=R_{\text{ave}}c_{\text{ave}}$,其表示周期$t_{\text{d-p}}$为节点$s_i$分配的风险额度。其中$c_{\text{ave}}=|c_{s_i}|t_{\text{d-p}}/T$代表在时间周期$t_{\text{d-p}}$内$s_i$的平均访问次数,$T$ 为总的时间。由此可以看出如果该主体本身历史记录良好,则当前访问几乎不受访问次数限制。

1.6　节点综合访问风险值

定义 1　C 为各风险分量权值的集合,$C=(\alpha,\beta_1,\beta_2,\gamma)$,其中 $\alpha+\beta_1+\beta_2+\gamma=1$,它们分别表示初始风险值、直接访问风险值、间接访问风险值和频率风险值的权值。节点综合访问风险值的计算式为

$$r=[\alpha,\beta_1,\beta_2,\gamma][r_{ini},r_{\text{his1}},r_{\text{his2}},r_{\text{fre}}]^{\text{T}}+\varphi_{s_i} \tag{7}$$

域整体风险值r_{d},可以通过域中所有节点风险值求平均值得到:

$$r_{\text{d}}=\frac{\sum_{i=1}^{m}r_{s_i}+\sum_{j=1}^{n}r_{o_j}}{m+n} \tag{8}$$

2　模 型 分 析

2.1　形式化描述

本模型是一个状态机模型,系统的状态是系统中元素的表示,它由主体、客体、访问属性、访问矩阵以及标识主体和客体的访问类属性的函数等组成。其相关定义如下:

定义 2　$S=\{s_1,s_2,\cdots,s_m\}$表示主体的集合。$O=\{o_1,o_2,\cdots,o_n\}$表示客体的集合。

定义 3　$D=\{d_1,d_2,\cdots,d_p\}$表示多自治域构成的域集合。

定义 4　函数 dom( ):$S\cup O\rightarrow D$,表示主体或客体所在的域。每个主体或客体都有唯一所在的域。

定义 5　集合 $A=\{r_{\text{d}},a,w,e\}$表示访问属性集,定义模型有以下 4 种访问方式:(a)Read(r_{d})读包含在客体中的信息;(b)Append(a)向客体中添加信息,且不允许读客体中的信息;(c)Write(w)向客体中写信息,且允许读客体中的信息;(d)Execute(e)执行另一个客体(程序)。

定义 6　当前访问集合 $B\subseteq(S\times O\times A)$:表示在某个特定的状态下哪些主体以何种访问属性访问哪些客体。

定义 7　访问请求集合J_{REQ},函数$J_{\text{req}}(s_i,o_j,x)$表示主体$s_i$对客体$o_j$的访问,其中 $x\in A$。

定义 8　访问矩阵集 M,表示系统中所有主体对系统中所有客体所拥有的访问权限,元素 $\boldsymbol{M}_{ij}\subseteq A$ 表示主体s_i对客体o_j具有的访问权限。

定义 9　模型中节点状态集表示为 $V=\{V_0,V_1,V_2,\cdots,V_k\}$,状态 $v\in V$,由(b,M,f,s_{M},R)表示,其中 $b\in B$,f 为访问周期内的访问频率,$s_{\text{M}}\in S$,R 为风险函数集合,表示主客体的风险状态。用v^*表示通过请求之后的状态。

定义 10　安全标记函数集合 F,主体、客体的当前安全标记用访问类函数f表示,$f=(f_{\text{SH}},f_{\text{SL}},f_{\text{IH}},f_{\text{IL}},f_{\text{SO}},f_{\text{IO}})$,$f\in F$,其中$f_{\text{SH}}$、$f_{\text{SL}}$和$f_{\text{SO}}$分别表示主体和客体的保密级区间和函数,$f_{\text{IH}}$、$f_{\text{IL}}$和$f_{\text{IO}}$分别表示主体和客体的完整级区间和函数。

约定 1　$H_{\text{IS}}(s)\in\{h_{\text{SH}}(s),h_{\text{IL}}(s)\}$为主体的访问历史函数。

2.2　机密性分析

本文模型建立在经典的多级安全模型基础之上,是一个有限状态机模型,系统是安全状态,当且仅当系

统的每一个状态$(v_0,v_1,v_2,\cdots,v_n)$均为安全状态,其中v_0是初始状态,$v_1,v_2,\cdots,v_n$是其他的输出状态。定义规则$\rho:J_{\mathrm{REQ}}\times V\to G\times V$,表示给定一个请求和一个状态,规则$\rho$决定系统产生的响应和下一个状态。$G$为判定集$\{y,n,e,u\}$,$y$表示请求被执行,$n$表示请求被拒绝,$e$表示多个规则适合于这一请求,$u$表示本规则不能处理此次请求。

约定2 系统的当前状态为$v=(b,M,f,s_{\mathrm{M}},R)$,请求通过后系统的状态转变为$v'=(b',M',f',s'_{\mathrm{M}},R')$。

定理1 若状态$v=(b,M,f,s_{\mathrm{M}},R)$是安全的,则经过规则1′得到的状态$v'=(b',M',f',s'_{\mathrm{M}},R')$满足BLP公理强制访问控制部分。

定理2 一个系统是机密性安全的,当且仅当它的每个状态都满足机密性强制规则。

公理1 (简单安全性)状态$v=(b,M,f,s_{\mathrm{M}},R)$满足简单安全特性,当且仅当所有的$s\in S\Rightarrow[o\in b(s:r)\Rightarrow f_{\mathrm{SH}}(s)\geqslant f_{\mathrm{SO}}(o)\geqslant f_{\mathrm{SL}}(s)]$。符号$\geqslant$表示前者支配后者。

公理2 (*安全特性)设s是S的一个子集,表示受*特性控制的主体。状态$v=(b,M,f,s_{\mathrm{M}},R)$满足*特性,当且仅当所有的$s\in S\Rightarrow[o\in b(s:a,w)\Rightarrow f_{\mathrm{SH}}(s)\geqslant f_{\mathrm{SO}}(o)\geqslant f_{\mathrm{SL}}(s)\wedge h_{\mathrm{SH}}(s)\geqslant f_{\mathrm{SO}}(o)]$

规则1′ 用于域d中主体s_i请求得到对域p中客体o_j的read访问权。

if $J_{\mathrm{req}}\notin\mathrm{dom}(J_{\mathrm{req}}(1))$

then $J'_{\mathrm{req}}(J_{\mathrm{req}},v)=(u,v)$

else if $[J_{\mathrm{req}}\in\mathrm{dom}(J_{\mathrm{req}}(1))]\wedge[f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_j)\geqslant f_{\mathrm{SL}}(s_i)]\wedge[J_{\mathrm{req}s_i}<R_{\mathrm{d}}]\wedge[J_{\mathrm{req}o_j}R_{\mathrm{d}}]$

then $J'_{\mathrm{req}}(J_{\mathrm{req}},v)=(y,(b(\cup(s_i,o_j,r),M,f,s_{\mathrm{M}},R)))$

else $J'_{\mathrm{req}}(J_{\mathrm{req}},v)=(n,v)$

R_{d}表示该域设置的风险阈值。

证明:

a. 证明规则1′满足简单安全性公理。设$o_t\in(b',r)$,若$o_t=o_j$,则$f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_j)=f_{\mathrm{SO}}(o_k)\geqslant f_{\mathrm{SL}}(s_i)$,若$o_t\neq o_j$则$o_t\in(b,r)$,由状态$v=(b,M,f,s_{\mathrm{M}},R)$满足的先验条件知$f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_t)\geqslant f_{\mathrm{SL}}(s_i)$。总之,若$o_t\in(b',r)$则$f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_t)\geqslant f_{\mathrm{SL}}(s_i)$,规则1′满足公理1。

b. 证明规则1′满足*特性公理。设$o_t\in(b',a)$,若$o_t=o_j$,由规则1′可知,无论请求是否拒绝,都不改变模型中的append状态,则由$o_t\in(b,a)$,以及状态$v=(b,M,f,s_{\mathrm{M}},R)$满足的先验条件知$f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_t)\geqslant f_{\mathrm{SL}}(s_i)\wedge h_{\mathrm{SH}}(s_i)\leqslant f_{\mathrm{SO}}(o_t)$。

若$o_t\neq o_j$,则$o_t\in(b,a)$,同上。

同理可证,$o_t\in(b',w)$时,$f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_k)\geqslant f_{\mathrm{SL}}(s_i)\wedge h_{\mathrm{SH}}(s_i)\leqslant f_{\mathrm{SO}}(o_t)$,总之,若$o_t\in(b',a\vee w)$,则$f_{\mathrm{SH}}(s_i)\geqslant f_{\mathrm{SO}}(o_k)\geqslant f_{\mathrm{SL}}(s_i)\wedge h_{\mathrm{SH}}(s_i)\leqslant f_{\mathrm{SO}}(o_t)$,则规则1′满足公理2。

其余规则可类似给出,此处省略。

2.3 完整性分析

公理3 (简单完整性)满足简单完整性当且仅当客体的完整级在主体可访问的完整级区间,主体可读客体,即状态$v=(b,M,f,s_{\mathrm{M}},R)$满足简单完整特性,当且仅当所有的$s\in S\Rightarrow[o\in b(s:r)\Rightarrow f_{\mathrm{IH}}(s)\geqslant f_{\mathrm{IO}}(o)\geqslant f_{\mathrm{IL}}(s)]$。

公理4 (*完整特性)满足*完整特性当且仅当客体的完整级在主体的可访问完整级区间,且主体读过所有客体的完整级都支配主体要写客体的完整级时,主体可写该客体。状态$v=(b,M,f,s_{\mathrm{M}},R)$满足简单完整特性,当且仅当所有的$s\in S\Rightarrow[o\in b(s:a,w)\Rightarrow f_{\mathrm{IH}}(s)\geqslant f_{\mathrm{IO}}(o)\geqslant f_{\mathrm{IL}}(s)\wedge h_{\mathrm{IH}}(s)\leqslant f_{\mathrm{IO}}(o)]$。

定理3 设任意初态v_0满足简单完整性,若模型满足简单完整性当且仅当对于每一个变换$(J_{\mathrm{req}},p,(b,M,f,s_{\mathrm{M}},R),(b^*,M^*,f^*,s^*_{\mathrm{M}},R^*))$下列条件成立:(a)每个$(s,o,x)\in b^*-b$,满足简单完整性;(b)每个属于$b$但不满足简单完整性的$(s,o,x)$,不属于$b^*$。

证明:

a. 证明其充分性。设J_{req}是J_{REQ}中的任意一个动作,T为系统的执行时间,对于$(J_{\mathrm{req}},v,p',v')$,当且仅当存在一个$\alpha=(v_0,\pi_1,v_1,\cdots)$和某个$t\in T$,使得$v_t=(p,v)$,$v_{t+1}=(p',v')$。

设$v_0=(b,M,f,s_{\mathrm{M}},R)$满足简单完整性,$\alpha=(v_0,\pi_1,v_1,\cdots)$是一个执行,对每个$t\in T$,令$v_t=(b_t,M_t,f_t,s_{\mathrm{M}_t},R_t)$。

证明v_1满足简单完整性:设$(J_{\mathrm{req}1},v_0,p_1,v_1)$为一个变换,根据定理3中的(a)可得$\forall(s,o,x)\in(b_1-b)$,

满足简单完整性;令$b_\partial=\{\forall(s,o,x)\in b\wedge(s,o,x)\}$不满足简单完整性,根据定理 3 中的(b)可得$b_\partial\wedge b_1=\varnothing$。所以可得到$\forall(s,o,x)\in b_1\cap b_0$满足简单完整。并且由于$\forall(s,o,x)\in(b_1\cap b_0\vee b_1-b_0)$,得$v_1$满足简单完整性。

证明若v_{t-1}满足简单完整性,则v_t满足简单完整性。

同理,可以证明v_{t-1}和v_t满足简单完整性。

综上所述,模型充分性得证。

b. 证明其必要性。采用反证法,假设模型满足简单完整性,则存在某个执行$(J_{\text{req}},v_{t-1},p_t,v_t)$使得下列条件其中之一成立:(a)某个$(s,o,x)\in b_t-b_{t-1}$不满足简单完整性;(b)某个不满足简单完整性的$(s,o,x)\in b_{t-1}\wedge(s,o,x)\in b_t$。

当(a)成立时,存在某个$(s,o,x)\in b_t-b_{t-1}$不满足简单完整性,所以v_t不满足简单完整性,推得模型不满足简单完整性。当(b)成立时,由于存在某个不满足简单完整性的$(s,o,x)\in b_{t-1}\wedge(s,o,x)\in b_t$,所以$v_t$不满足简单完整性,推得模型不满足简单完整性。

综上所述,必要性得证。

定理 4　假设任意初态v_0满足完整性 * 规则,则若模型满足 * 完整性规则当且仅当对每个变换$(J_{\text{REQ}},p,(b,M,f,s_{\text{M}},R),(b^*,M^*,f^*,s_{\text{M}}^*,R^*))$,下列条件成立:(a)对任意主体$s\in S,(s,o,x)\in b^*-b,\exists[(x=a)\vee(x=w)]\Rightarrow f_{\text{IH}}(s)\geqslant f_{\text{IO}}(o)\geqslant f_{\text{IL}}(s)\wedge h_{\text{IH}}(s)\geqslant f_{\text{IO}}(o)$。(b)对任意主体$s\in S,(s,o,x)\in b^*-b,\exists[(x=a)\vee(x=w)]\wedge!\ (f_{\text{IH}}(s)\geqslant f_{\text{IO}}(o)\geqslant f_{\text{IL}}(s)\wedge h_{\text{IH}}(s)\geqslant f_{\text{IO}}(o))\Rightarrow o\notin(s,x)$,这里可以采用反证的方法进行证明。

定理 5　一个系统是安全的,当且仅当它的每个状态都满足强制安全规则。

由于满足本模型机密性强制规则的系统是机密性安全的,同时满足完整性强制规则的系统是完整性安全的,由此可知定理 5 成立。

3　结　　语

本文提出了分布式环境下的面向多域访问的动态多级安全模型,给出了定性和定量相结合的风险量化标准。在模型的访问域和被访问域增加了风险敏感标记的动态调整机制,每次访问之前需要通过本域管理节点的验证,提高了跨域访问的安全性,增加了模型的动态适应性。给出风险机动额度,结合历史访问信息,灵活地调整了主体访问能力,提高了访问控制模型的灵活性,实现了对风险的自适应访问控制动态授权,提高了模型对异构网络环境的适应能力。但是本模型在处理过程中没有充分考虑到在访问周期内如果有节点恶意篡改访问记录、伪造低风险或者无风险访问的假象。管理节点可以记录本域节点进域或者离域,并在访问前后对记录进行比较,或者对访问记录进行加密以防恶意篡改,这是下一步主要研究的工作。

参考文献:

[1] 李昊,张敏,冯登国,等. 大数据访问控制研究[J]. 计算机学报, 2017,40(1):72-91. (LI Hao, ZHANG Min, FENG Dengguo, et al. Research on access control of big data[J]. Chinese Journal of Computers, 2017,40(1):72-91. (in Chinese))

[2] KUNAL S, SAHA A, AMIN R. An overview of cloud-fog computing: architectures, applications with security challenges[J]. Security and Privacy, 2019, 2(4):1-14.

[3] HAO Jialu, LIU Jian, WANG Huimei, et al. Efficient attribute-based access control with authorized search in cloud storage[J]. IEEE Access, 2019,7:72-83.

[4] TANG Hua, YANG Jiejun, WANG Xiaofang, et al. A research for cloud computing security risk assessment[J]. Open Cybernetics & Systemics Journal, 2016, 10(1):210-217.

[5] SERVOS D, OSBORN S L. Current research and open problems in attribute-based access control[J]. ACM Computing Surveys (CSUR), 2017, 49(4): 1-45.

[6] NAZERIAN F, MOTAMENI H, NEMATZADEH H. Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy[J]. Journal of Information Security and Applications, 2019, 45: 131-142.

[7] GHAFOORIAN M, ABBASINEZHAD M D, SHAKERI H. A thorough trust and reputation based RBAC model for secure data storage in the cloud [J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(4): 778-788.

[8] 冯登国,张敏,李昊. 大数据安全与隐私保护[J]. 计算机学报, 2014,37(1):246-258. (FENG Dengguo, ZHANG Min, LI

Hao. Big data security and privacy protection[J]. Chinese Journal of Computers,2014,37(1):246-258. (in Chinese))
[9] 王于丁,杨家海, 徐聪,等. 云计算访问控制技术研究综述[J]. 软件学报, 2015,26(5):1129-1150. (WANG Yuding, YANG Jiahai, XU Cong, et al. Review of cloud computing access control technology research [J]. Chinese Journal of Computers, 2015,26(5):1129-1150. (in Chinese))
[10] DÍAZ-LÓPEZ D, DÓLERA-TORMO G, GÓMEZ-MÁRMOL F, et al. Dynamic counter-measures for risk-based access control systems: an evolutive approach[J]. Future Generation Computer Systems, 2016,55(C):321-335.
[11] LYU Junjie, RONG Juling. Virtualisation security risk assessment for enterprise cloud services based on stochastic game nets model[J]. IET Information Security, 2018, 12(1): 7-14.
[12] ZHENG Yaoyu, FANG Yangwang,WEI Xianzhi, et al. Evaluation method for simulation credibility based on cloud model[J]. Journal of Computer Applications, 2018, 38(6): 1535-1541.
[13] UIKEY C, BHILARE D S. RBACA: role-based access control architecture for multi-domain cloud environment [J]. International Journal of Business Information Systems, 2018, 28(1): 1-17.
[14] DOS-SANTOS D R, MARINHO R, SCHMITT G R, et al. A framework and risk assessment approaches for risk-based access control in the cloud[J]. Journal of Network & Computer Applications, 2016, 74:86-97.
[15] LALEH N, CARNINATI B, FERRARI E . Risk assessment in social networks based on user anomalous behaviors[J]. IEEE Transactions on Dependable & Secure Computing, 2018, 15(2):295-308.

(收稿日期:2019-03-14 编辑:高建群)

·简讯·

水利部召开水利网信工作视频会议

中国水利网站2020年5月13日讯,2020年5月12日,水利部召开水利网信工作视频会议。会议按照2020年全国水利工作会议部署,践行“安全、实用”水利网信发展总要求,总结2019年水利网信工作,分析当前水利网信工作形势,部署近期水利网信工作重点任务。水利部副部长、部网信领导小组副组长叶建春在主会场出席会议并讲话,强调要贯彻落实水利改革发展总基调,大力推进智慧水利,全力驱动水利治理体系和治理能力现代化。水利部总工程师刘伟平主持会议并作总结讲话。部网信办负责人作工作报告,浙江省水利厅、福建省水利厅、宁夏回族自治区水利厅、深圳市水务局、长江水利委员会、监督司等6家单位代表作了交流发言。

叶建春指出,2019年,水利网信部门深入贯彻党中央、国务院决策部署,紧密围绕水利中心工作,努力补水利网信之短板,全力支撑总基调各项工作取得显著成效。一是以需求为引领,完善了水利网信顶层设计;二是以问题为导向,强化了网络安全防护能力建设;三是以实用为目标,水利网信补短板取得了明显成效;四是以创新为动力,持续提升了水利信息化水平。当前和今后一个时期,水利网信部门要牢牢抓住信息技术加快发展以及水利工作转型升级的重大战略机遇,深化信息技术与水利业务的融合发展,准确把握网络安全面临的严峻形势,切实做好水利关键信息基础设施网络安全保护,努力践行水利改革发展总基调,为水利治理体系和治理能力现代化提供强劲动力。

叶建春强调,2020年是“十三五”的收官之年,是全面建成小康社会、实现第一个百年奋斗目标的决胜之年,要扎实做好各项水利网信工作。一要大力推进智慧水利,继续创新机制、重点推进、先行先试,加快智慧水利尽快落地见效;二要强力支撑行业监管,开发完善水利监督信息平台各项功能,扩大使用覆盖面,全面支撑综合监管、专职监管、专业监管、日常监管;三要严守网络安全底线,重点做好水利信息系统等保达标、应用系统安全防护、关键信息基础设施保护等工作;四要提升水利网信工作水平,做好水利网信建设、信息共享、网络安全等领域监管。

部机关有关司局、部直属有关单位负责同志在主会场参加会议。各流域管理机构、各省(自治区、直辖市)水利(水务)厅(局)及计划单列市水利(水务)局、新疆生产建设兵团水利局有关负责同志,各智慧水利先行先试单位负责同志在分会场参加会议。

(本刊编辑部供稿)