

计算机网络访问隔离控制方法研究

陈滢生

(重庆人文科技学院 计算机工程学院, 重庆 401524)

摘 要: 提出基于可信计算的计算机网络访问隔离控制方法, 首先利用小波分析方法完成计算机网络访问分析, 然后利用基于频繁 IP 地址距离算法对危险访问进行识别, 分析危险访问特点. 在此基础上, 根据危险访问特点, 利用可信计算技术, 建立网络访问隔离控制模型, 从而完成计算机网络访问隔离控制系统的总体结构设计, 并分析结构中各模块内容. 通过分析网络访问隔离控制的安全属性, 得到计算机网络访问隔离控制流程, 从而实现计算机网络访问隔离控制. 实验证明, 所提方法能够有效对计算机网络访问进行隔离控制, 提高隔离控制的准确度, 降低计算机网络访问隔离控制难度, 具有良好的使用价值.

关键词: 计算机网络; 访问隔离; 控制方法

中图分类号: TP391

文献标识码: A

文章编号: 1000-7180(2017)06-0141-04

Research on Computer Network Access Isolation Control Method

CHEN Ying-sheng

(Institute of Computer Engineering, Chongqing College of Humanities, Science & Technology, Chongqing 401524, China)

Abstract: This access isolation control method of trusted computing based on computer network, using wavelet analysis method to complete the analysis of computer network access, and then use the IP algorithm to address frequent distance access risk identification based on the analysis of risk characteristics, access. Based on this, according to the risk characteristics of access, using trusted computing technology, establishing network access quarantine control model, thus completing the computer network access quarantine overall structure design of the control system, and analyze the content of each module structure. Based on the analysis of the security attributes of network access control, the process of computer network access control is obtained. The experimental results show that the proposed method can effectively control the access of computer network, improve the accuracy of isolation control and reduce the difficulty of computer network access control.

Key words: computer network; access isolation; control method

1 引言

计算机网络技术的发展在推动物联网事业发展的同时, 也给计算机网络安全带来严重威胁^[1]. 控制客户端对网络资源的访问能有效减少危害计算机网络行为的手段, 越来越受到人们重视^[2]. 根据计算机网络访问隔离控制的实时性和持续性^[3], 提出一种基于 RBAC 策略的网络访问控制方法^[4], 通过静态策略合并和动态授权搜索相结合方法, 制定安全策

略. 通过基于 RBAC 的授权搜索方法, 利用访问请求权限驱动域间访问授权过程, 动态地建立域间安全互操作, 然后对安全策略进行管理, 通过基于有向图的策略冲突检测方法, 将安全域角色系统抽象成有向图, 并利用该策略冲突检测方法对策略冲突进行分类处理, 针对不同策略类型对策略进行检测, 最后通过基于安全标签和层次 RBAC 策略的网络访问控制系统及其策略配置管理平台的原型实现, 完成计算机网络访问隔离控制, 该方法存在应用范围

较小,隔离控制过程复杂等缺点,难以保证隔离控制的准确性^[5]. 这个问题在相关专家学者之间引起了较大反响,对该问题的研究也逐渐成为研究热点,随着研究内容的深入,产生了丰硕的研究成果^[6-7].

文献[8]提出了基于流量分析的网络访问控制方法,但这种方法需要设计访问控制系统,通过控制系统进行网络访问隔离控制,存在运行占用内存较大的问题. 文献[9]提出基于 Portal 协议的网络访问控制方法,但这种方法存在安全保密性低的问题. 文献[10]提出一种基于安全域隔离的访问控制方法,该方法由于过于注重安全保密性,所以访问隔离控制的效率不高.

针对上述问题,提出一种基于可信计算的计算机网络访问隔离控制方法,实验证明,所提方法能够有效对计算机网络访问进行隔离控制,提高了隔离控制的准确度,降低了计算机网络访问隔离控制难度,具有良好的使用价值.

2 计算机网络访问控制方法研究

2.1 计算机网络危险访问识别

小波分析方法是一种常用的网络危险访问分析方法,本文通过小波分析的方法,完成危险访问的检测,具体检测流程如下所述.

设定 $\phi(t) \in L^2(R)$, 其中 L 表示小波变换的迭代次数, R 表示访问的次数, 其傅里叶变换为 $\Psi(\omega)$. 当 $\Psi(\omega)$ 满足式(1)时, 则可以将 $\phi(t)$ 称为危险访问的基本小波或母小波.

$$C_{\Psi} = \int_R \frac{|\Psi(\omega)|^2}{|\omega|} d\omega < \infty \quad (1)$$

式中, d 表示访问控制的参数; ω 表示访问控制的权值. 将母函数 $\phi(t)$ 经伸缩和平移变换后, 则得到小波序列.

在连续访问中, 小波序列为

$$\phi_{a,b}(t) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{t-b}{a}\right) \quad (2)$$

式中, $a, b \in R, a \neq 0, a, b$ 分别表示母函数的伸缩因子和平移因子, t 表示小波变换参数.

对网络访问控制函数 $f(t) \in L^2(R)$ 的连续小波变换为

$$W_f(a, b) = |a| - \frac{1}{2} \int_R f(t) \bar{\psi}\left(\frac{t-b}{a}\right) dt \quad (3)$$

为了提高访问隔离的准确性, 在利用小波变换进行网络异常访问分析的同时通过基于频繁 IP 地址距离算法对危险访问进行识别, 为保证危险访问

识别的准确率, 提高识别效率, 在过程中引入期望值, 均值以及无偏估计值.

无偏估计值表示一组统计数的期望值与这组统计数的平均值的偏差, 其可以表示为

$$\eta = \frac{Ei}{Ai} \quad (4)$$

式中, 偏差 η 范围应与实际网络环境相协调; Ei 表示访问地址 $IP[i]$ 的期望值; Ai 表示访问地址 $IP[i]$ 的均值; 其计算公式如下所示, 其中 $0 \leq j < 255, 0 \leq i \leq 3$.

$$Ei = \frac{\sum_{j=0}^{255} j IP[i][j]}{\sum_{j=0}^{255} n} \quad (5)$$

$$Ei = \frac{\sum_{j=0}^{255} IP[i][j]}{256} \quad (6)$$

式中, $IP[i][j]$ 表示访问数组的数据. 当 η 接近 1 时, 说明这组访问数据的离散度很小, 溢出的可能较小, 这组访问数据较安全; 当 η 与 1 差距逐渐增大, 表明这组访问数据的离散度越来越大, 这组访问数据的危险概率逐渐提高. 设定 IP 地址的 4 个字节分别对应 A、B、C、D, 则结果会出现 A、B、C、D 组合的几种溢出情况.

利用可能发生溢出的字节组合可疑 IP 地址, 当 $IP[i][j] > \text{temp}$ 时, 则可以初步判定其为危险 $IP[i]$, 其中, 阈值 temp 可以表示为

$$\text{temp} = \lambda \min\{E_0, E_1, E_2, E_3\} \quad (7)$$

式中, λ 表示可以 IP 地址的支持度, 其取值需根据实际情况确定.

定期更新访问数组的信息, 如果攻击发生在上一个周期的末期和下一个周期的初期, 当访问数组的数据设为 0 时, 可能遗漏一些危险访问数据, 导致访问数据隔离的准确度下降. 所以在设置访问数组的数据时, 将其设置为

$$IP[i][j] = \frac{1}{2} IP[i][j] \quad (8)$$

2.2 计算机网络访问隔离控制方法

在对计算机网络访问隔离控制时, 采用可信计算的方法. 通过可信计算, 将 2.1 节识别出来的危险访问进行隔离控制, 保证计算机网络安全.

本文中, 通过将可信平台技术、网络连接技术和网络访问隔离控制技术相结合, 建立网络访问隔离控制模型(如图 1 所示).

通过图 1 可以看出, 在用户连接网络时, 首先经过可信平台通过可信平台, 对网络终端以及网络连

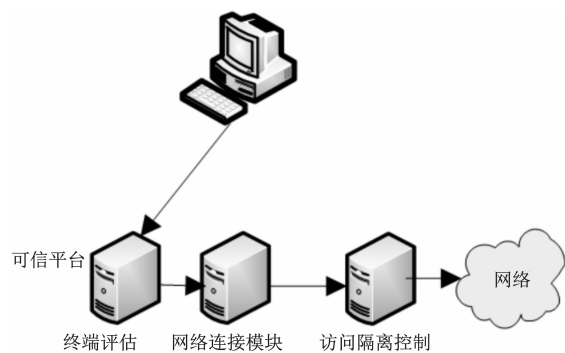


图 1 网络访问隔离控制模型

接模块进行评估,然后对危险网络访问进行控制隔离,之后连接网络。

根据可信平台的特点,完成计算机网络访问隔离控制的总体结构图,如图 2 所示。

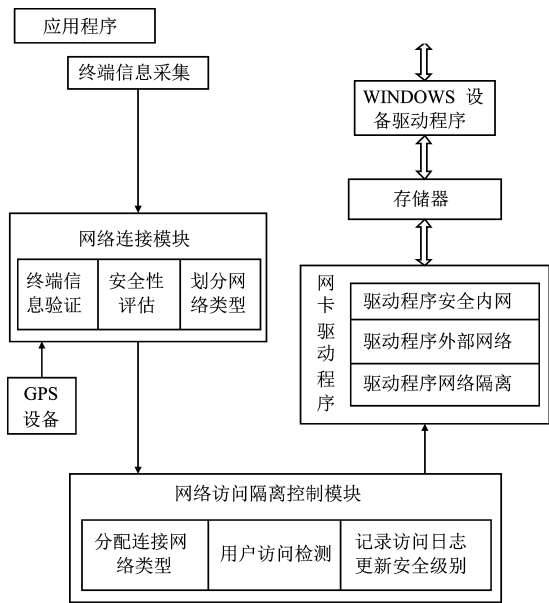


图 2 计算机网络访问隔离控制的总体结构

图 2 中,信息采集模块主要是采集用户的登陆信息以及 WINDOES 终端的硬件信息,并将采集到的信息传送到可信平台。WINDOES 设备驱动程序主要目的是收发所有的网络数据包。存储器主要是作为 WINDOWS 端驱动程序和可信平台数据交换的桥梁。网卡驱动程序负责驱动芯片进行数据包的收发工作,并分析网络数据包。网络连接模块实现可信网络的接入,并对网络终端的可信度进行评估。访问控制模块则是根据预先制定的网络安全策略进行访问控制,保证网络正常访问。

根据上文,计算机网络访问隔离控制评估终端的安全属性主要有用户登陆身份信息安全、终端平台的硬件信息安全、终端位置信息安全,以及终端历

史访问记录安全。

网络访问隔离控制中,用户登陆身份信息是根据用户级别,获取对应的网络访问权限。用户通过设定的用户名和密码验证自己身份,可信平台利用 WINDOWS 端应用程序,获取用户在登录时输入的身份信息。

在网络访问评估终端中,其硬件信息需要满足所有硬件必须有唯一标识,且硬件质量较好,不容易损坏。

网络访问隔离控制评估终端位置信息是一个非常重要的评估内容,一旦终端离开其常在位置,便会脱离安全管辖范围,造成评估终端的可信度降低,甚至评估终端不可信情况。

3 实验结果与分析

为了证明本文提出的基于可信计算的计算机网络访问隔离控制方法的有效性和可行性,进行了一次仿真实验,实验是在 Windows 7 Ultimate 的操作系统下进行的,CPU 型号是 3.2 GHz 的 Intel Core I3,运行平台为 Microsoft Visual Studio. NET 2010。将本文提出的计算机网络访问隔离控制方法与文献[7-8]所提的网络访问隔离控制方法进行对比,从而完成本次实验。

首先,分别利用本文提出的网络访问隔离控制方法与文献[7]和文献[8]所提网络访问隔离控制方法进行访问隔离控制响应时间对比,隔离响应时间(s)的计算方法如下所示。

$$T = \frac{\sum IP[i][j]}{\sqrt{a^2 + b^2}} \cdot \delta \tag{9}$$

式中, δ 表示三种方法的调节参数, $\delta = \eta \cdot \text{temp} + 1$ 。通过上式,为保证实验的准确性,以 50 次实验数据为一组,计算平均 T 值,得到三种网络访问隔离控制的平均响应时间对比,对比结果如图 3 所示。

根据图 3 可以看出,本文所提方法进行访问隔离控制,响应时间较短,说明本文所提方法在进行隔离控制时延迟较小,能较好地保证计算机网络访问隔离控制的实时性。且由于本文所提方法的响应时间折线波动较小,说明本文所提方法的响应时间较为稳定。

然后对网络访问隔离控制的准确性进行对比,其准确性(个)可用式(10)进行计算。

$$\sigma = \frac{\theta IP[i]}{Ei - Ai} \tag{10}$$

式中, θ 表示三种方法进行隔离控制的系数。根据上

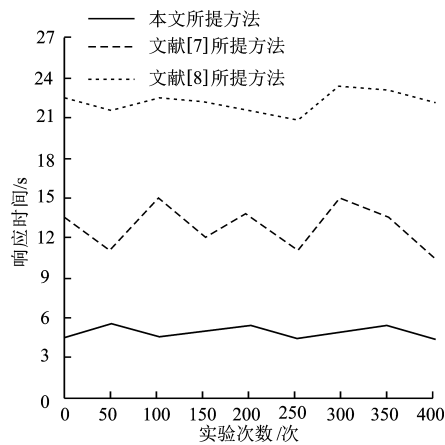


图3 三种方法平均响应时间对比

式,得到三种方法隔离控制的准确性对比,对比结果如表1所示。

表1 三种方法进行隔离控制准确性对比 个

隔离控制总数量	本文方法隔离控制数量	文献[7]方法隔离控制数量	文献[8]方法隔离控制数量
57	54	48	49
102	97	89	92
156	143	131	134
189	176	167	171
203	186	171	173
279	263	242	246
338	321	302	306
423	402	381	385

通过表1可以看出,本文所提方法能够提高隔离控制的准确性较高,说明本文所提方法进行网络访问隔离控制的效率较高。

最后,对三种方法的能耗进行对比,定义能耗(N)的计算方式如下所示。

$$N = \frac{\sum IP[i][j]}{Ei \cdot Ai} \cdot \lambda \tag{11}$$

根据上式,得到三种网络访问隔离控制方法进行访问隔离控制的能耗对比,对比如图4所示。

通过图4可以看出,本文所提方法的能耗与文献[7-8]所提方法的能耗相比,本文所提方法的能耗较少,且本文所提方法的能耗曲线较平稳,说明本文所提方法的能耗较为稳定。综上所述,采用本文所提方法进行网络访问隔离控制,结果较为稳定,且本文所提方法的响应时间较短,进行访问隔离控制实时性较好。

4 结束语

计算机网络访问隔离控制是一种有效的保证计算机安全的手段,随着计算机网络的发展,对其的重

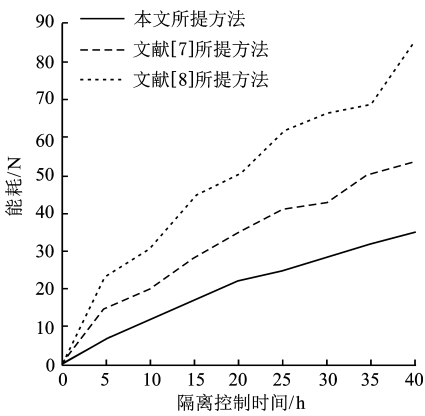


图4 三种方法进行访问隔离控制能耗对比

视程度越来越高. 本文提出的基于可信计算的计算机网络访问隔离控制方法能够有效提高访问隔离控制的准确性和实用性,对计算机网络访问隔离控制方法的研究有借鉴价值。

参考文献:

[1] 胡小龙,蒋光庆,郭玉东,等. 基于协作型 VMM 的虚拟
机网络访问控制技术研究[J]. 小型微型计算机系统,
2014,35(4):883-888.

[2] 卢志刚,姜政伟,刘宝旭. 一种基于 VXLAN 的虚拟网
络访问控制方法[J]. 计算机工程,2014,40(8):86-90.

[3] 周自飞,谭小彬,牛玉坤,等. 信息中心网络中授权视频
访问控制[J]. 电信科学,2014,30(9):53-60.

[4] 李凤华,王彦超,殷丽华,等. 面向网络空间的访问控制
模型[J]. 通信学报,2016,37(5):9-20.

[5] 陈婷,卢建朱,江俊晖. 一种具有强匿名性的无线传感
器网络访问控制方案[J]. 计算机工程,2015,41(1):
126-129.

[6] 刘浩. 多域环境下基于信任的 P2P 访问控制模型[J].
计算机工程与应用,2014,50(21):116-120.

[7] 于烨,郭治成,王连忠,等. 基于信任的云访问控制
系统的设计与实现[J]. 现代电子技术,2017,40(3):
62-64.

[8] 刘艺,张红旗,代向东,等. 面向 OpenFlow 网络的访问
控制规则自动实施方案[J]. 计算机应用,2015, 35
(11):3270-3274.

[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.

[10] 马勇. 基于 IBC 机制的内容中心网络安全认证方案
[J]. 电子设计工程,2016,24(13):88-91.

作者简介:

陈滢生 女,(1982-),硕士,讲师. 研究方向为数据库技术、
软件与理论. E-mail:yinger0142@163. com.