

基于角色的透明计算应用权限控制模型

赵晓参¹, 王国军²

(1 中南大学 信息科学与工程学院, 湖南 长沙 410083;

2 广州大学 计算机科学与教育软件学院, 广东 广州 510000)

摘 要: 提出一种基于角色的透明计算应用权限控制模型 TCACM(Transparent computing access control model). 该模型能够较好地解决透明计算中的系统安全性问题. 该模型由客户端和服务端两部分组成. 客户端启动应用程序, 计算出应用程序的数据指纹, 将其与服务端“安全应用程序”数据库匹配, 进行完整性验证; 根据授权角色权限集进行授权验证, 由验证结果动态地管理用户可运行应用程序集. 实验结果验证了该模型的可行性.

关键词: 应用权限; 安全应用; 透明计算; 基于角色的访问控制

中图分类号: TP309.2

文献标识码: A

文章编号: 1000-7180(2017)11-0080-05

Applications Access Control Model Based on Role in Transparent Computing Environment

ZHAO Xiao-can¹, WANG Guo-jun²

(1 College of Information Science and Engineering, Central South University, Changsha 410083, China;

2 College of Computer Science and Educational Software, Guangzhou University, Guangzhou 510000, China)

Abstract: A TCACM (Transparent computing access control model) based on role in transparent computing environment is proposed. The model can solve the problem of system security in transparent computing. The model consists of two parts: the client and the server. The client initiates the application, calculates the application's data fingerprint, matches it with the server-side "security application" database for integrity verification. According to the authorization role permission set for authorization verification, by the verification results dynamically manage the user can run the application set. The experimental results verify the feasibility of the model.

Key words: application right; integrity; transparent computing; role-based access control

1 引言

透明计算^[1-5]是一种新的计算模式. 在该模式中, 用户无需感知计算机操作系统、中间件、应用程序和通信网络的具体所在, 只根据自己的需求, 通过网络从所使用的各种终端设备中选择并使用相应服务.

透明计算给用户提供了极大的自主服务权限, 但因此也带来了相应的安全性问题, 例如用户操作的随机性问题, 用户随机安装或运行危险软件会导致数据泄露或平台崩溃. 目前, 许多研究者提出了多

种访问控制模型, 例如自主访问控制(Discretionary Access Control, DAC)^[6], 强制访问控制(Mandatory Access Control, MAC)^[7-9]和基于角色的访问控制(Role-Based Access Control, RBAC)^[10-14]等. 本文将结合 RBAC 模型理论, 与透明计算进行融合, 实现 TCACM.

2 TCACM 理论分析

TCACM 分为两个部分: 服务器端和客户端.

服务器端有两个功能: 其一维护“安全应用程序”数据库, 在该数据库中存放通过安全测试的应用

程序的数据指纹,其中数据指纹唯一映射一个应用程序;其二借鉴 RBAC 思想,引入角色的概念,以最小权限原则为角色分配应用程序集,并根据实际动态变化,实时地调整用户与角色的绑定关系,角色的授权应用程序集。

客户端的主要功能有:当检测到应用程序启动请求后,分析请求参数,计算应用程序数据指纹,通过网络在服务器端进行完整性和授权检测,根据检测结果决定转入正常启动逻辑或停止启动过程。

关于 TCACM 首先建立以下定义:

定义 1 用户集 $U: \{u_1, u_2, u_3, \dots, u_m\}$, 角色集 $R: \{r_1, r_2, r_3, \dots, r_n\}$, 安全应用程序集 $P: \{p_1, p_2, p_3, \dots, p_k\}$, 安全应用程序唯一一对数据指纹集 $F: \{f_1, f_2, f_3, \dots, f_k\}$ 。

定义 2 客户端: $GF: (p_i) = f_i$, 其中 $p_i \in P$, $f_i \in F$, $GF(p_i)$ 根据应用程序 p_i 文件信息计算其唯一数据指纹 f_i 。

定义 3 服务器端: $GR: (u_j) = R_j$, 其中 $R_j \subset R$, 表示用户 u_j 绑定的角色集; $GL: (R_j) = P_j$, 其中 $P_j = \{P_{j1} \cup P_{j2} \cup \dots \cup P_{jt} \mid GL(r_{jk}) = P_{jk}, r_{jk} \in R_j\}$, $P_j \subset P$, $GL(R_j)$ 表示角色集 R_j 被授权使用的应用程序集; $GP: (p_i) = f_i$, 其中 $p_i \in P$, $f_i \in F$, $GP(p_i)$ 表示根据应用程序信息 p_i 在服务器端“安全应用程序”集 P 中查找其数据指纹 f_i 。

定义 4 服务器端: $BR: (u_j) = R_j$, 为用户 u_i 绑定角色集 R_i ; $RBR: (u_j) = R_k$, 调整用户 u_i 的绑定角色集为 R_k ; $GPR: (r_j) = P_j$, 为角色 r_j 授权应用程序集 P_j ; $MPR: (r_j) = P_k$, 修改角色 r_j 授权应用程序集为 P_k 。

定义 5 完整性检测: 判断启动应用程序的完整性 $IN: (p_i) = \{\text{true}, \text{false} \mid f_{i1} = GF(p_i), f_{i2} = GP(p_i), \text{if } f_{i1} = f_{i2}, IN(p_i) = \text{true}; \text{else } IN(p_i) = \text{false}\}$ 。其中 f_{i1} 是客户端应用程序数据指纹, f_{i2} 是“安全应用程序”数据库中对应数据指纹。

定义 6 授权检测: 判断用户是否被授权使用某应用程序 $O: (u_i, p_j) = \{\text{true}, \text{false} \mid R_i = GR(u_i), P_j = GL(R_i), \text{如果 } p_j \in P_j, O(u_i, p_j) = \text{true}; \text{否则 } O(u_i, p_j) = \text{false}\}$ 其中 R_i 是用户 u_i 所属角色集, P_j 是角色集被授权使用的应用程序集合。

根据以上相关定义,给出 TCACM 理论分析步骤: 用 $M = \langle GF, GP, GR, GL, BR, RBR, GPR, MPR, IN, O \rangle$ 表示 TCACM, 模型的输入是 GF, GP , 输出是 IN, O 。当客户端用户 u_i 启动应用程序

p_j 时, 计算其数据指纹 $f_j = GF(p_j)$, 服务器端检测应用程序 p_j 的完整性 $IN(p_j)$, 用户授权验证 $O(u_i, p_j)$, 客户端根据完整性检测结果 $IN(p_j)$ 和授权验证结果 $O(u_i, p_j)$ 决定应用程序 p_j 的启动逻辑。服务器端管理员可以根据实际情况高效地为用户绑定角色 $BR(u_i)$, 为角色授权应用权限 $GPR(u_i)$; 根据动态变化实时地修改用户绑定角色 $RBR(r_i)$, 角色的授权应用权限 $MPR(r_i)$ 。

3 TCACM 实现过程

3.1 透明计算核心组成

透明计算由透明服务器和透明终端组成, 两部分通过网络进行及时通信。刚启动时, 透明终端不具有操作系统, 而是由超级操作系统 (Meta OS) 进行操作和管理, 用户可按需从透明服务器端获取操作系统和应用程序。透明计算组成结构由图 1 所示。

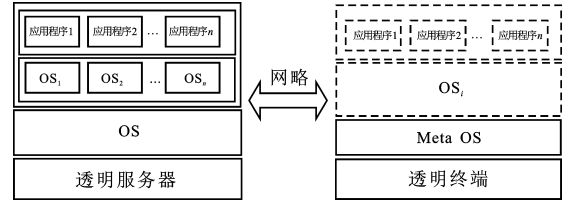


图 1 透明计算组成结构图

透明服务器根据具体应用环境和执行环境的不同, 将基于用户的安全需求及应用按需组合, 同时根据用户之间数据保护相互依赖的多样性, 在实际应用中将操作系统和应用程序加载到透明终端。

透明服务器管理操作系统和应用服务等软件资源, 与透明终端之间由软件流和数据流进行信息交互, 透明服务器按照不同的安全服务策略组合不同的实际应用, 减轻自身的服务性能瓶颈并起到安全隔离的作用, 降低服务的安全风险, 提高系统的可信性。透明终端根据需求加载软件流执行, 减少非相关应用的执行, 有效提高计算服务效率的同时, 减少计算开销和安全风险。

3.2 TCACM 核心模块

TCACM 包括服务器端和客户端, 服务器端的主要模块为应用权限管理模块, 客户端的主要模块为监控模块。其模型系统架构如图 2 所示。

3.2.1 服务器端应用权限管理模块

服务器端的应用权限管理模块是 TCACM 重点部分, 其又细分为三个部分, 分别是“安全应用程序”数据库维护模块、应用权限管理模块和客户端监控请求处理模块。

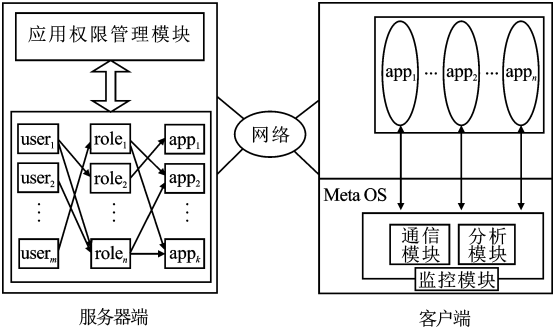


图 2 TCACM 系统框架图

“安全应用程序”数据库维护模块:根据实际需要选择应用程序集,筛选出经过检测并确认安全的应用程序版本,使用安全哈希算法^[15](Secure Hash Algorithm)计算应用程序数据指纹,并将其存储在“安全应用程序”数据库中.系统管理员可根据需求变化修改、增加和删除数据库中数据指纹.

应用权限管理模块:这个模块引用了基于角色的应用权限控制模型思想.引入了角色概念,用户通过与角色的绑定获取应用权限,如图 3 所示,服务器端管理员将“安全应用程序”以集合的形式关联到不同的角色,同时根据用户需求灵活地绑定角色.根据动态变化实时地调整用户的绑定角色和角色的授权应用程序集.

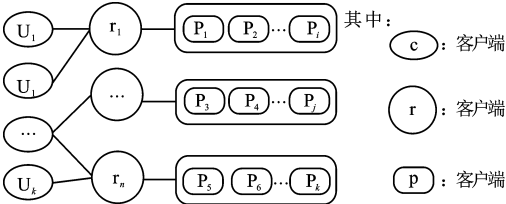


图 3 基于角色的应用权限逻辑图

该模块其核心思想伪代码如下:

GetUserApplication(Username)

Input: username-用户名

Output: BUP 用户应用权限集

- (1) Initialize BUP = $\emptyset$
- (2) Initialize UR = $\emptyset$ // 用户和角色映射关系
- (3) Initialize RP = $\emptyset$ // 角色和应用权限映射关系
- (4) Initialize ROLE_U = $\emptyset$ // 用户的授权角色集
- (5) GetURFromDB(UR)
- (6) GetRPFFromDB(RP)
- (7) Foreach (username_i, rname_j) ∈ UR Do // 遍历 UR, 获取用户授权角色集
- (8) If (username_i = Username) then
- (9) ROLE_U = ROLE_U ∪ {rname_j}

- (10) Foreach rname_i ∈ ROLE_U Do // 遍历 RP, 获取基本应用权限集
- (11) Foreach (rname_j, aname_k) ∈ RP Do
- (12) If (rname_i = rname_j) then
- (13) BUP = BUP ∪ {(Username, aname_k)}
- (14) return BUP

客户端监控请求处理模块:当服务器端接收到客户端监控请求后,查找“安全应用程序”数据库中客户端启动应用程序对应数据指纹,与监控请求中软件数据指纹进行一致性计算;查找用户绑定角色集对应的应用程序集,查看客户端启动应用程序是否包含在该授权应用程序集中 BUP.把检测结果返回客户端.服务器端的总流程图如图 4 所示.

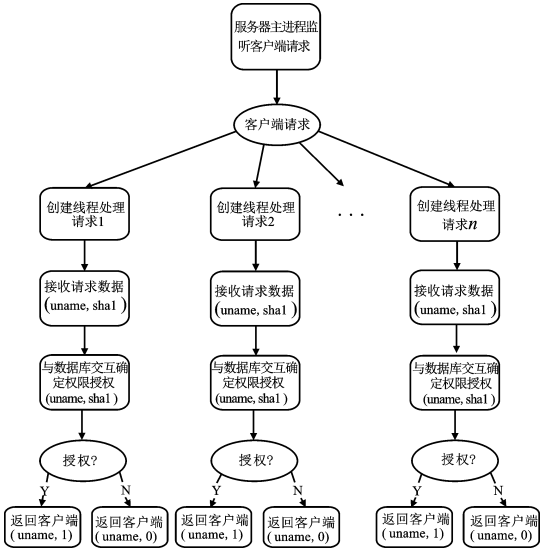


图 4 TCACM 服务器端总流程示意图

3.2.2 客户端监控模块

客户端监控模块实现对应用程序运行的实时监控、分析和处理,根据功能不同,监控模块又划分为分析模块和通信模块.

分析模块:客户端中的分析模块需要对从透明服务器接收过来的应用程序进行数字指纹计算分析.根据透明计算 Meta OS 中用户登录信息获取用户唯一标识符.把应用程序数字指纹和用户标识符通过通信模块在服务器端进行完整性和授权验证.如果验证成功,用户被授权使用该应用程序,则应用程序转入正常启动逻辑,否则返回错误.

通信模块:通信模块提供面向连接的、可靠的数据传输服务,保证数据能够无差错、无重复和顺序接收.为分析模块提供远程通信服务支持.

4 TCACM 在透明计算环境的实际应用

本文在透明计算实验室搭建起一个实验平台,在此平台上实际应用 TCACM,实验将 TCACM 的客户端部分运用到透明计算环境中的透明终端 Meta OS 中,将 TCACM 的服务器端运用到透明计算环境中透明服务器 OS 中.将 TCACM 与透明计算进行融合.以下做具体介绍时,已默认将模型导入了透明计算中.具体实际应用步骤如下所示.

Step1:透明服务器端启动,预先为角色分配应用权限,并给相应的用户授权角色.

Step2:透明终端启动,用户登录透明计算实验系统.

Step3:用户按需选择操作系统.

Step4:用户启动需要的应用程序.

Step5:由于透明计算中应用程序存放在透明服务器中,当用户开始选择应用程序时,操作系统发生缺页中断.透明终端 Meta OS 接收到缺页中断后,通过网络从透明服务器获取相关应用程序代码,并存放至透明终端 Meta Os 的内存中.

Step6:客户端分析模块根据应用程序执行代码计算出数据指纹,并从透明终端 Meta OS 中获取用户信息.

Step7:透明终端用户信息和应用程序信息通过网络模块发送到透明服务器端进行完整性和授权验证.

Step8:服务器端权限管理模块获取用户信息和应用程序信息.

Step9:将应用程序数据指纹与服务器端指纹数据库中的数据指纹进行匹配.如果匹配成功,进入下一步骤.匹配失败,给客户端发送验证失败消息(此步骤为模型完整性验证过程).

Step10:服务器端根据用户信息确定其授权角色,然后确定角色的应用权限集,如果启动应用程序属于应用权限集,给客户端发送验证成功消息.如果不属于,则发送验证失败消息(此步骤为模型一致性验证过程).

Step11:客户端接收由服务器端发来的验证消息.

当客户端收到验证成功的消息时,客户端将应用程序代码和相关文件上传给上层操作系统.否则,上传错误指令.

Step12:当该模型完成验证后,清空透明终端 Meta OS 中内缓存.

5 实验测试

5.1 测试环境

实验室搭建起透明计算环境,配置好网络、透明服务器与各个透明终端.在进行此次测试实验中,透明终端均为个人电脑,透明计算实验室系统结构如图 5 所示.

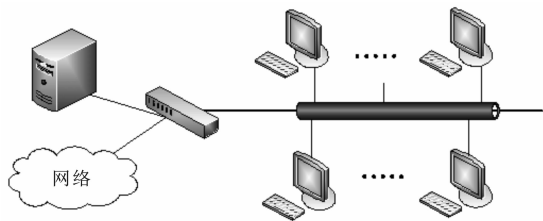


图 5 透明计算实验机房系统结构图

5.2 功能验证

系统管理员把安全应用程序的数据指纹录入到根据课程、职位等设置不同角色;根据学号(教工号)作为用户唯一标示录入数据库;管理员根据课程需求为角色分配应用程序集;管理员为用户绑定角色.初始数据如表 1~3 所示.

学生信息表			
uid	name	grade	rid
2016100430	Lily	14 级	01
2016100501	Stone	15 级	02
...	...	...	...
2016100615	Mary	16 级	25

表 2 角色信息表		
rid	role	sid
01	C Language	0001/0004/.../0100
01	DataStruction	0001/0002/.../0090
...	...	...
25	Linux	0002/0015/.../0100

表 3 “安全应用软件”表		
sid	software	software_finger
0001	eclipse	“f85c1f59cfd8a22a14eb74af77066af714e0eb39”
0002	firefox	“43443846aeada35dd33b3917874706a27f4aaf56”
...	...	...
0100	mysql	“ec7a0241e1048466d8c42af3e9c0c368bfc13a69”

分别使用 Lily 和 Mary 两人在终端登录,启动操作系统后分别运行 eclipse、firefox 和 mysql 时.如表 4 所示,Lily 可以正常使用 eclipse 和 mysql,没有权限使用 firefox,当管理员把 Lily 的绑定角色修改为 Data Structions 时,Lily 立刻可以使用 firefox,但无法再使用 mysql;如表 5 所示,Mary 可以

正常使用 firefox 和 mysql,不被允许使用 eclipse,管理员为角色 Linux 的应用程序集中添加 eclipse 后,Mary 立刻可以运行 eclipse.

表 4 切换 Lily 的角色时应用权限变化

学生	角色切换	安全应用软件		
		eclipse	firefox	mysql
Lily	C Language	是	否	是
	DataStructions	是	是	否

表 5 修改角色应用权限集

学生	角色	操作	安全应用软件		
			elipse	firefox	mysql
Mary	Linux	无	否	是	是
		授权 eclipse	是	是	是

由上述测试结果可知基于角色的应用权限控制模型是合理的、可行的,它能根据实际需求高效实时地管理用户与角色的绑定管理,并动态地调整角色的应用权限集.该模型中服务器端灵活且强制地控制客户端用户的可运行应用程序集,有效地提高了系统管理员更新客户端应用权限的灵活性和便利性,同时提高了客户端平台的安全性和稳定性.

6 结束语

针对透明计算系统中用户操作随机性导致运行危险程序带来的安全隐患,本文提出一种基于角色的透明计算应用权限控制模型 TCACM(Transparent computing access control model),利用该模型结合透明计算环境,能够较好地保证用户运行应用程序的完整性和安全性.

参考文献:

[1] ZHANG Y, ZHOU Y. 4VP+: A novel Meta OS approach for streaming programs in ubiquitous computing [C]// Proc. of the IEEE 21st International Conference on Advanced Information Networking and Applications (AINA 2007). Niagara Falls, Canada, 2007:394-403.

[2] 张尧学,周悦芝. 一种云计算操作系统 TransOS:基于透明计算的设计与实现[J]. 电子学报, 2011, 39(5): 985-990.

[3] Zhang Yaoxue, Zhou Yuezhi. Transparent computing: spatio-temporal extension on von neumann architecture for cloud services[J]. Tsinghua Science and Technology, 2013, 18(1):10-21.

[4] Yaoxue Zhang, Yuezhi Zhou. Separating computation and storage with virtualization[J]. Computer Commu-

nications, 2011, 34(13):1539-1548.

[5] 匡文渊,张尧学,周悦芝,等. NSAP-支持透明计算的网路存储访问协议[J]. 清华大学学报(自然科学版), 2009, 49(1): 106-109.

[6] Zhang Hong, He Ye-Ping, Shi Zhi-Guo. A delegation model for periodicity constraints-based DAC[J]. Chinese Journal of Computer,2006, 29(8):1427-1437.

[7] LIU G, ZHANG J, LIU J, et al. Improved Biba model based on trusted computing [J]. Security and Communication Networks, 2015,8(16)2793-2797.

[8] SASSU R, RAMUNNO G, LIOY A. Practical assessment of biba integrity for TCG-Enabled platforms[C] //2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2014: 495-504.

[9] ZHAO H, WANG H, LI H. Analysis and improvement of the BLP security model [C]//Advanced Materials Research. Trans Tech Publications, 2014, 998: 578-581.

[10] ANSI. American national standard for information technology: role based access control[S]. New York: American National Standard Institute, 2004.

[11] Ferrara A L, Madhusudan P, Parlato G. Security analysis of role-based access control through program verification [C]// Proc of the 25th IEEE Computer Security Foundations Symposium. Cambridge: IEEE Press,2012:113-125.

[12] LU J, JAMES B D JOSHI, JIN L, et al. Towards complexity analysis of User Authorization Query problem in RBAC [J]. COMPUTERS & SECURITY, 2015,48:116-130.

[13] KIVIHARJU M. RBAC with ABS: Implementation practicalities for RBAC integrity policies[C] // 2014 11th International Conference on Security and Cryptography (SECRYPT). IEEE, 2014: 1-10.

[14] 李风华,苏铨,史国振,等. 访问控制模型研究进展及发展趋势[J]. 电子学报, 2012, 40(4): 805-813.

[15] LI Y, ZHAO D, LI H, et al. HMAC-SHA1 Applied in the diagnosis service for security access[C] //Proceedings of SAE-China Congress 2014: Selected Papers. Springer Berlin Heidelberg, 2015: 507-512.

作者简介:

赵晓参 男,(1990-),硕士研究生.研究方向为透明计算、访问控制. E-mail:992536614@qq.com.

王国军 男,(1970-),博士,教授.研究方向为可信计算、透明计算、隐私保护.