B/S模式信息安全系统的一种形式化描述*)

刘益和[1,2]

(四川大学信息安全研究所 成都610064)[1] (内江师范学院计算机与信息科学系 内江641112)[2]

摘 要 本文利用有限状态机、RABC模型和BLP模型原理,对B/S模式下的信息系统给出了一种形式化描述,该描述在操作平台、密码系统、传输环节是安全的前提下是安全的。

关键词 B/S模式,有限状态机,RABC模型,BLP模型,机密性

A Formal Description of the System of Information Security of B/S Mode

LIU Yi-He[1,2]

(School of Information Security Graduate,Sichuan University,Chengdu 610064)[1]

(Department of Computer and Information Neijiang Teachers College,Neijiang 641112)[2]

Abstract It was described about a information system of B/S(Browser/Server)Mode by formally,with finite-state machine and the ideals of the RABC and BLP model,the description which based on the system desk,the cryptosystem and the transmission procession were secure is secure.

Keywords B/S mode,Finite-state machine,RABC model,BLP model,Confidentiality

1 引言

随着网络的广泛应用和不断发展,利用计算机对信息进行收集、加工、存储、分析以及交换等各种处理,越来越成为必不可少的手段,Browser/Server(B/S)模式由于比Client/Server(C/S)模式更具有优越性,所以目前它的应用最为广泛。

本文利用有限状态机[1]、BLP模型[2]的不上读,不下写的思想和基于角色的访问控制(Role-Based Access Control RABC)[3]的基本思想,对B/S模式下的信息安全系统进行了形式化描述和验证,这有助于信息安全保障体系中的应用环境的安全体系框架的研究[4]。

2 基本概念

首先给出大家熟知的一些概念。

主体和客体:计算机中存在大量涉及安全的操作。凡实施操作的称为主体,用$s_1,s_2,\cdots,s_i,\cdots$或s表示,其集合用S表示,为了便于讨论本文把用户列为主体,不再细分;被操作的对象称为客体,用$o_1,o_2,\cdots,o_j,\cdots$,或o表示,其集合用O表示。

系统中可信主体集合记为S^T,不可信主体集合记为S',显然$S=S^T\cup S',S^T\cap S'=\Phi$。

安全等级:主体s_i的安全等级用$T(s_i)$表示;客体o_j的安全等级用$T(o_j)$表示,Web服务器的安全等级用T(w)表示。

为了简化讨论,本文以最基本RABC模型的概念和原理为准,如图1所示。

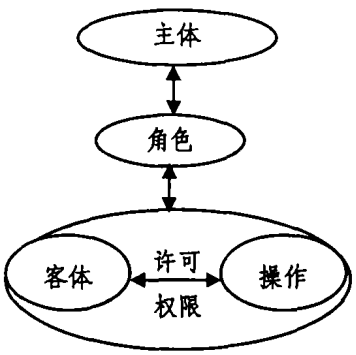

图1 RABC基本模型

系统拥有的角色集合记为R,令$R=\{r_1,r_2,\cdots,r_n\}$;所有角色对应的权限集集合记为P,令$P=\{p_1,p_2,\cdots,p_m\}$;主体s拥有的角色集合记为:SR(s);角色r对应的主体集合记为:RS(r);客体o拥有的角色集合记为:OR(o);角色r对应的客体o集合记为:RO(r);角色r对应的权限集合记为:RP(r);主体s基于角色拥的权限集合记为SP(s);客体o基

*)该课题得到国家973资助项目(编号:1999035801)、四川省教育厅自然科学重点项目(编号:2003A161)资助.刘益和 副教授,博士生,主要研究方向:信息安全.

于角色允许被使用的权限集合记为:OP(o)。

主体 s 从安全角度考虑对客体 o 的访问模式 access_model(s,o):其值域就是 s 作为一个用户,当它扮演一个角色,同时考虑 BLP 模型对应的安全限制,对 o 进行操作的所有权限集合,这个集合实际上是 P 的子集,其中应含 re:read,w:write,c:create;d:delete 等权限。

主体 s 从安全角度考虑对主体 s' 的访问模式 access_model(s,s'):在本文其值取 c:create;d:delete 两个。

主体 s 的出入网证:用 t(s)表示,在不混淆时,简记 t,内含用户信息 u_t(s),包括:用户名,用户代码,密码,客户机的地址等;服务器信息 s_t(s),包括:服务器名,服务器代码,服务器密码,是否允许 s 入网信息等;这里 t(s)= u_t(s)∪ s_t(s)。

系统中所有出入网证集合记为:$T=\{t_1,t_2,\cdots\}$。

为了简化起见,我们假设:用户与服务器端的信息传输是安全的,包括操作平台、加密系统和传输渠道是安全的,能抵御外来的攻击。

3 系统描述

3.1 一般策略假设

根据 BLP 模型中的最主要思想,系统是处于安全状态(机密性),需要满足:不上读,不下写原则,即有:

如果 T(s)>T(o),则主体可以读客体;如果 T(s)<T(o),主体可以写客体;如果 T(s)=T(o),则主体可以读写客体。

3.2 系统转移函数假设

下面我们给出 B/S 模式下的信息系统所涉及到的最主要状态转移函数,它们分别为:申请出入网证、创建客体、创建主体和删除主体、删除客体、创建角色和删除角色等,其创建基本思路是:首先满足 RABC 模型的要求,再从 BLP 模型安全的角度进行限制。

3.2.1 *申请出入网证* Request_in_out_certificate(s,u_t(s))//主体 s 申请出入网证 t(s)

If s∉S' then T=T∪t(s),t(s)=u_ t(s)∪s_t(s)

3.2.2 *创建客体* Creat_object(s',o,o_tlev,OR(o))//主体 s' 创建客体 o,这里 o_tlev 表示客体 o 的安全级,OR(o)是客体 o 允许被使用的角色集。

If t(s')⊄T or c∉ SP(s')then go_end//s 出入网证不正确或 s' 对 o 无创建权,结束

If o∉ O then O=O∪{o}and T(o)=o_tlev

∀ r ∈OR(o),OP(o)=∪RP(r)//构造客体的权限集合,所有 RP(r)的并集。

∀ s ∈ S, access_model(s,o) = SP(s) ∩ OP(o)//从角色的角度考虑,只有 s 拥有某项权限,而这一权限,允许对客体 o 使用时,主体 s 才能访问客体 o,后面的函数类似。

DO CASE//对 T(s),T(w),T(o)分情况讨论 access_model(s,o)

CASE (T(s)≥T(w)and T(w)>T(o))or(T(s)>T(w)and T(w)=T(o))

If{w}∈access_model(s,o)then access_model(s,o)=access_model(s,o)-{w}

// 去掉 w 权利,转结束。

CASE (T(s)≤T(w)and T(w)<T(o))or (T(s)< T(w)and T(w)=T(o))

If {re}∈access_model(s,o)then access_model(s,o)=access_model(s,o)-{re}

//去掉 re 权利,转结束。

CASE (T(s)>T(w)and T(w)<T(o))or (T(s)<T(w)and T(w)> T(o))

If {re,w}∈access_model(s,o)then access_model(s,o)=access_model(s,o)-{re,w}//去掉 re,w 权利,转结束。

ENDCASE

3.2.3 *删除客体* Delete_object(s,o)//主体 s 删除客体 o

If d∉access_model(s,o)then go_end//结束

∀ s' ∈S,access_model(s',o)= Φ

∀ r ∈R,if o∈RO(r)then RO(r)=RO(r)-{o}

OP(o)=Φ,OR(r)= Φ,O=O-{o}

3.2.4 *增加角色* Creat_role(s,r,RS(r),RP(r),RO(r))// 主体 s 为整个系统新增加角色 r,已知 r 对应的主体集合 RS(r)、权限集合 RP(r)和客体集合 RO(r)

If t(s)⊄T or c ∉SP(s)then go_end//s 出入网证不正确或 s 无创建权,结束

R=R∪{r},

∀ s' ∈RS(r),SR(s')=SR(s')∪{r}//修改主体拥有的角色集合

∀ s'∈RS(r),SP(s')=SP(s')∪RP(r)// 修改主体拥有角色 r 的权限集

∀ o' ∈RO(r),OR(o')=OR(o')∪{r}//修改客体拥有的角色集合

∀ o' ∈RO(r),OP(s')=OP(s')∪RP(r)// 修改客体拥有角色 r 的权限集

∀ s ∈S,∀ o∈O,access_model(s,o)=SP(s)∩OP(o)//根据新角色进行相应调整

//以下根据 T(s),T(w),T(o)的不同情况,对

access_model(s,o)进行讨论,讨论描述与创建客体的相应讨论描述类似,故从略。

另外,创建主体、删除主体和删除角色以及角色的部分权限调整、角色对应的主体和客体的调整可以仿照上面的函数进行描述,这里不再赘述。

3.3 浏览器/服务器(B/S)模式下的信息安全系统的形式化描述

根据上面的各种假设,我们将该系统的状态转移图描述如图2所示,系统初始状态定义为:S=Φ,O=Φ,显然是安全状态,不难证明,当在我们的操作平台、加密系统和传输环节是安全的前提条件下,系统由一个安全状态执行了上面的状态转移函数之后,新状态仍是安全的,反复做这些操作后,整个信息系统的安全性仍然得以保障,于是我们认为这个关于浏览器/服务器(B/S)模式下的信息系统的描述是安全的。

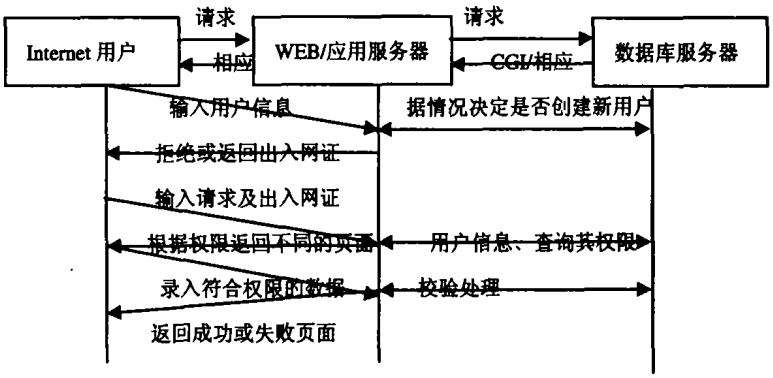

图2 浏览器/服务器体系状态转移图

结束语 本文利用有限自动机的思想、RABC模型和BLP模型,具体创建了若干个状态转移函数,在一定假设条件下,系统在这些状态间相互转换,能确保系统的安全性,从而给出了一个B/S模式下的信息系统的安全描述,这对构建信息安全保障体系将具有积极的意义。

参 考 文 献

1 李军,孙玉方.计算机安全和安全模型.计算机研究与发展,1996,33(2):312~320

2 Bell D E, Lapadula LJ. Secure compter system: mathematical foundation. MTR-2527, Mitre corp, Bedford, MA, 1973 (NTIS AD-771543)

3 Sandhu RS, Samarati P. Access control: principles and practice. IEEE communications, 1994, 32(9): 40~48

4 沈昌祥.构造积极防御的安全保障框架.计算机安全,2003,10:1~2

5 居梯,张小英,张伟民.B/S模式电信计费管理系统的安全策略研究.微机发展,2001,5:57~59

(上接第200页)

略,并在此基础上开发出了一套通用的验证平台,更为重要的是,该验证平台具有很高的可重用性,从而大大减轻了设计者的工作量,加快了系统设计的进程。

参 考 文 献

1 Anderson T. Your Core-My Problem? Integration and Verification of IP[J]. IEEE Design & Test, 2001, 18(5): 170~171

2 Hawana M, Schutten R. Testbench Design, A Systematic Approach. http://www.synopsys.com/sps/pdf/paper2.pdf, 2003.12

3 Semiconductor Reuse Standards, Motorola Inc. http://www.motorola.com/semiconductor/srs, 2003.12

4 VSIA: soft and hard VC structural, performance and physical modeling specification, implementation/verification development working group, Specification 1 Version 2.0 [Z]. 1999

5 Alliance VSI. On-chip bus development working group specification 1 Version 1.0 (OCE 1 1.0)[Z]. 1998

6 张宇弘,等.基于SOC典型结构的系统验证环境.微电子学[J].2003,33(2):98~101

7 Keating M, Bricaud P. Reuse Methodology Manual for System-on-a-Chip Desig ns[M]. London: Kluwer Academic Publishers, 1999. 110~116

8 Sabbatini N Jr, et al. Reuse issues on the verification of embedded MCU cores[A], Circuits and Systems. In: 4th IEEE Intl. Caracas Conf. on Devices [C]. Aruba: IEEE Computer Society, 2002. C012-1-C012-6