办公网的信息安全模型研究

朱斌红[1]，　胡　明[2]
(1. 广州军区空军司令部 自动化站，广东 广州　510071；2. 空军工程大学 电讯工程学院，陕西 西安　710077)

摘　要：介绍信息安全模型的作用和特征以及几种目前比较实用的安全模型。探讨机关办公网络的数据流特点，并提出一种适合部队和政府机关办公网络的树状安全状态机模型。

关键词：办公网；安全模型；安全状态机；安全策略
中图分类号：TP393.08　　**文献标识码**：A　　**文章编号**：1009-3516(2000)04-0048-04

根据美国FBI的调查，美国每年因为网络安全造成的经济损失超过1.70亿美元。75%的公司报告财政损失是由于计算机系统的安全问题造成的。平均每个组织损失US$402 000。国内的网络安全状况则更加严峻，仅在网络安全产品方面，中国同国外的差距至少有5－10年。97年中国国际互联网络信息中心CNNIC曾遭到美国南加州黑客的攻击，CNNIC的主页被黑客换成了一副骷髅头。这一方面源于我国总体上应用技术开发落后；另一方面是因为我国的网络在工商业中应用的范围和水平都还比较低，因而善良地希望黑客不光顾也是难以办到的。也许有些单位或个人以为只要不把办公网接入Internet就可以安枕无忧了，根据调查统计大约有70%的安全威胁来自内部。98年江西的邮电169公众服务网遭到一名中学生的攻击。99年发生在某银行的内部员工盗用他人帐号炒股等案例都说明加强网络安全已迫在眉睫。

1　几种常用安全模型

构造网络安全体系的初期首先需要建立安全模型。建立安全模型的目的是为了精确描述系统的安全需要。安全模型可以帮助我们尽可能精确地描述系统功能，同时遵守安全策略，并使得基于这种安全模型而实现的系统将不会有安全方面的漏洞。安全模型还将指导与安全有关的系统功能的实现。

安全模型有如下几个特点：

- 它是精确、无二义性的。
- 它是简单、抽象的，因而也是容易理解的。
- 它具有一般性，仅涉及安全性质，不过分限制系统的功能及其实现。
- 它是安全策略的一个清晰的表达方式。

目前实用的几种安全模型有：

1.1　状态机模型(State Machine Model)

状态机模型是将系统描述成一个抽象的数学状态机，它包括以下几个元素：

——初始状态S_0。

——状态变量，包括主体、客体、各自的安全属性及主体对客体的访问权。

——状态转移函数，它是对系统调用的抽象表示，它描述了状态变量可能发生的变化。

状态机模型是基于两个原则构造并实施的。第一，安全保持原则，即只要能够证明初始状态是安全的，并且所有的转移函数也是安全的，那么只要系统从某个安全状态出发，系统总是保持在安全状态。第二，递增原则，即若子系统被证明是安全的，且以安全的方式组合，那么整个系统也是安全的。这条原则允许我们把一个复杂的安全系统分解为小块，或者构造一些安全的构件库以组建安全系统。

1.2　访问矩阵模型(Access Matrix Model)

它是状态机模型的一种。它将系统的安全状态表示成一个大的矩形阵列。系统中的每一个主体都拥有

收稿日期：1999-12-07
作者简介：朱斌红(1972-)，女，广东湛江人，助理工程师，主要从事网络安全研究.

一行,每一个客体都拥有一列。矩阵中的交叉项表示某主体对某客体的访问模式。这个访问矩阵是状态机模型中的状态变量之一。模型的转移函数描述了访问矩阵是如何变化的以及变量所发生的相应变化。

1.3 BLP 模型(Bell & Lapadula Model)

这是一种信息流模型。由于信息流的有序性,信息只能由低向高流,因此必须制定能够区别信息流安全状态的安全等级尺度。BLP 模型就是描述这种多级安全策略最著名的形式。它不是校验主体对客体的访问模式,而是试图控制从一个客体流向另一个客体的信息流。这种控制是根据两个客体的安全属性强制实行的。

1.4 take grant 模型

这种模型是通过系统中权力和信息转移的有向图来研究系统的安全。该模型不仅指定操作而且指定操作能够发生的条件,它有助于查找系统的安全漏洞。

1.5 基于角色的模型(Role _ Based Access Control Model)

比起传统的访问控制模型来它能更确切地描述用户的访问权限,因为通过为某一个用户分配角色而授予给这个用户的权限实际是一种功能操作而不是简单的读、写权限。现在已经有些商业产品陆续推出基于角色的访问控制。

2 树状安全状态机模型

树状安全状态机模型是我们通过对传统的状态机模型进行改进和扩充,以使其适用于网络环境并且能够更全面和确切地描述机关办公网的安全需求和安全策略的安全模型。它包括通信访问控制部分以及读/写访问控制部分。

2.1 办公网络通信特点描述

由于部队或政府机关的组织结构呈现出一种类似树状的特点,因此其内部通信数据流向也具有树状特征。首长节点位于整个结构的根部,以各个处室为单位向外延伸,参谋节点则位于整个结构的末梢成为叶子节点。如图 1 所示:

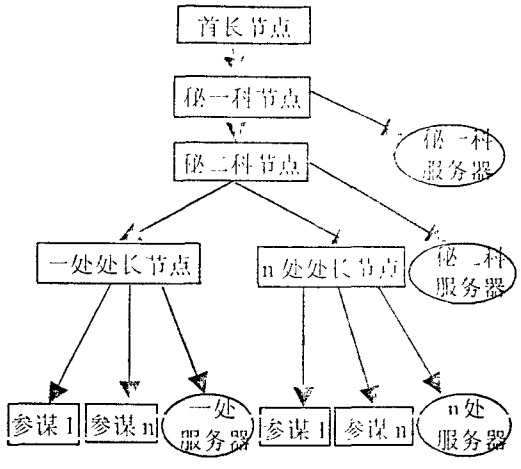

图 1　机关组织结构图

对其网络通信约束表达如下:

parent(n):节点 n 的上一级节点(即父节点而非祖先节点)

com(n,m):表示 n 和 m 节点间可以相互通信

type(n):表示 n 的类型(可为 w:客户机类型或 s:服务器类型)

必须满足:

if com(n,m) then

——若 n、m 可通信

(((type(n)=w) and (type(m)=w)) and ((parent(n)=m) or (parent(m)=n)))

——n 和 m 节点类型都是客户机型且 n、m 节点为父、子节点关系

or (((type(n)=w) and type(m)=s)) and ((parent(m)=n) or parent(m)=parent(n)))

or (((type(m)=w) and type(n)=s)) and ((parent(n)=m) or (parent(m)=parent(n)))

——m、n 节点类型一个是客户机型,一个是服务器型,且满足 m、n 节点在同一层上或是服务器节点是客户机节点的子节点的条件

2.2 网络描述

一个办公网络可以看作是若干网络节点的集合,其描述为:

N:网络内所有节点集合

parent(n):节点 n 的父节点

type(n):节点 n 的类型(取 w:客户机类型或 s:服务器类型)

level(n):节点 n 的安全等级(取下列值之一:A—首长节点等级,B—秘书节点等级,C—处长节点等级,D—参谋节点等级)。

拓朴约束:

1)if level(n)=A then parent(n)=n

——A 级节点的父节点即是它自己

2)if level(n)=D then ∉ m(m∈N and parent(m)=n)

——D 级节点无子节点

——服务器节点无子节点

3)if type(n)=S then ∉ m(m∈N and parent(m)=n)

说明:网络安全状态机模型是将若干独立的安全状态机纳入一个系统。因此它是由若干网络节点安全状态机根据一定规则构成的集合。

2.3 网络节点 n 的状态机描述

2.3.1 状态变量定义

S:当前主体集合

O:当前客体集合

sclass(s):主体 S 的安全访问类

oclass(o):客体 O 的安全访问类

A(S,O):访问模式集合,取下列集合之一.

{r}:若主体 S 能够读客体 O

{w}:若主体 S 能够写客体 O

{φ}:若主体 S 既不能读客体 O,又不能写客体 O

{r,w}:若主体 S 既能读客体 O,又能写客体 O

subj:当前活动主体

receiver:当前接收节点(假设每一时刻,每个通信节点只与一个节点通信。)

sender:当前发送节点

message:当前发送/接收客体

check:message 是否经过安全过滤器安全检查的标志

contents(O):客体 O 的内容

所以:State(n)={S,O,sclass,oclass,contents,A,subj,receiver,sender,message,check}。

说明:①S 表示当前主体集合。主体表示网络用户

②O 表示当前客体集合。客体表示网络中的信息资源

③sclass(S)/oclass(O)表示主/客体安全访问类。安全访问类用来表示主(客)体访问安全级。这里将访问安全级分为 A、B、C、D 四级,且 A>B>C>D。定义访问安全级目的是为了进行访问控制。

④安全过滤器:实质是某种安全机制的抽象。它往往是几种安全策略,如:密码策略、审计策略的综合运用,或者是一种防火墙产品。设置安全过滤器的目的是为了描述用户对信息安全级进行合法降级的需求。

2.3.2 定义安全状态

定义安全状态就是将安全策略用数学语言描述成一个不变式。访问控制安全策略可以根据不同办公网的安全需求有所不同。下面侧重对访问控制策略进行描述:

(1)仅当用户的安全级高于或等于信息的安全级时,该用户才可以读该信息。

(2)仅当用户的安全级低于或等于信息的安全级时,该用户才可以写该信息。

(3)从高安全级用户接收消息时,仅当消息的安全级低于或等于接收方的安全级,该接收方才可接收该消息。

(4)向低安全级用户发送消息时,仅当消息的安全级低于发送方的安全级,该发送方才可发送该消息。

(5)发送与接收方同时存在或同时不存在。

以下是对上述安全策略的不变式描述:

系统是安全的 当且仅当所有 s∈S,o∈O,有

①if r∈A(S,O)then sclass(S)≥oclass(O)

②if w∈A(S,O)then sclass(S)≤oclass(O)

③if receiver≠φ then(parent(n)=receiver)or((parent(receiver)=n)and(oclass(message)≤level(receiver)))

④sender≠φ then(parent(sender)=n)or((parent(n)=sender)and(oclass(message)≤level(n))

⑤Not(sender XOR receiver)

——收、发方为同或关系

说明:①当信息被发送、接收时,称这部分信息为消息(message).

②发方若将本级节点上的某些信息发送给下级节点,需要经过安全过滤器检查。这里认为经过安全过滤器检查过的信息是经过降低访问安全级后的消息。

③收、发方通信都是在客户机类型间进行。

2.3.3　转移函数

转移函数可以看成是主体对系统服务子例程的过程调用。服务完成后,状态变量就会产生相应的变化。状态转移函数是微不可分的。

Func(n):节点 n 的转移函数集

Func(n)包括:

访问状态转移函数(存贮子状态机函数)

①creat _ object(o,c):创建一个访问类为 c 的客体 o。

②set _ access(s,o,modes):使主体 s 对目标 o 具有 modes 访问模式。

③creat/change _ object(o,c):将 o 的访问类设为 c 并且生成它。

④write _ object(o,d):将数据 d 写入客体 o 中。

⑤copy _ object(from,to):将 from 客体内容复制到 to 客体中。

通信状态转移函数(通信子状态机函数)

⑥set _ receiver(r,m):设置消息 m 的接收者为 r。

(m∈O,r∈N)

⑦send( ):将消息发向接收方。

⑧receive(s,m):接收方接收从 s 方发来的消息 m。

限于篇幅这里只介绍了部分转移函数的作用,对函数的具体定义从略。

3　结束语

本文中的网络安全状态机模型中没有描述完整性安全控制策略。完整性安全控制在实际应用中也是非常重要和必需的,设置完整性控制可以再在该模型基础上增加两个完整性访问控制类型,即:S _ integclass/O _ integclass(O)表示主/客体完整性访问类。完整性访问类表示主(客)体的完整性控制级别,其对应关系与访问安全级类似。完整性控制级主要是用来防止信息内容被篡改。一种常用的保证信息完整性的方法是对信息进行签名。

参考文献:

[1] 江　水.基于角色的存取控制-RBAC[J]. 计算机工程,1998,18(10):45-47.

[2] 冯运波. 网络访问控制策略[J]. 通信保密,1998,13(2):30-35.

[3] Matt Bishop. Conspiracy and information flow in the Take-Grant Protection Model[J]. Journal of Computer Security, 1996,4(2):331-359.

Study on Information Security of Office Network

ZHU Bing-hong[1], HU Ming[2]

(1. The Automatic station of AFHQ, Guangzhou Military Command, Guangzhou 510071,China;

2. The Telecommunication Engineering Institute,AFEU. ,Xi'an 710077,China)

Abstract: This paper introduces some practical security models and their actions and characteristics. Based on the analysis of office network data flow we lay stress on the arboreous security state machine model which befits the office network of army or government.

Key words: office network;security model;security state machine;security policy