信息网络的安全控制模式*

王　宇, 卢　昱
(装备指挥技术学院 网络安全实验室, 北京 101400)

摘　要: 信息网络的安全控制是一项复杂的系统工程。为了方便其安全分析与设计, 必须采用一定的安全控制方式。介绍了信息网络安全控制论系统的概念和控制结构, 归纳总结了安全控制的几种常用模式, 并对每种模式的特点、用途和使用方法进行了介绍。采用这些安全控制模式能增强系统安全控制的灵活性和可扩展性。

关键词: 信息网络; 安全控制; 控制模式
中图法分类号: TP393.08　　**文献标识码**: A　　**文章编号**: 1001-3695(2006)03-0133-03

Security Control Patterns for Info-Net

WANG Yu, LU Yu
(Lab. of Network Security, Academy of Equipment & Command & Technology, Beijing 101400, China)

Abstract: Security control for info-net is a complex system engineering. In order to give facilities to security analysis and design, it is necessary to adopt some security control patterns. The concept and control structure of secure info-net cybernetic system is proposed, several general control patterns are summarized, and their characteristics, efficiencies and utilizations are introduced. Using these control patterns can enhance system's controlling flexibility and extensibility.

Key words: Info-Net; Security Control; Control Pattern

信息网络[1](Info-Net)系统是一个实体系统, 它主要是由计算机网络和网络中无处不在的信息构成的。对它的安全控制构成了信息网络的安全控制系统(属于概念系统)。信息网络系统是信息网络安全控制系统的控制对象和运行基础, 而信息网络安全控制系统为信息网络系统提供安全指导和安全服务, 它们是相互关联, 相辅相成的, 共同构成信息网络安全控制论系统[2~5], 如图 1 所示。

不仅施控者可以作用于受控者, 而且受控者也可以反作用于施控者。前种作用是控制作用(前馈), 后种作用是反馈作用。信息网络的安全控制结构描述的就是信息网络安全控制论系统的控制结构, 如图 2 所示。

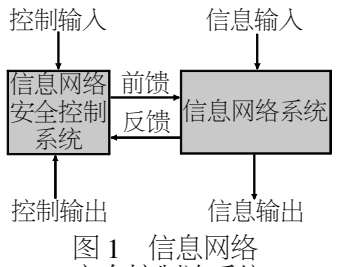

图 1　信息网络安全控制论系统

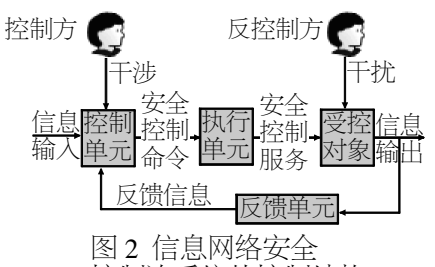

图 2 信息网络安全控制论系统的控制结构

和一般的控制系统类似, 信息网络安全控制论系统主要是由控制单元、执行单元、受控对象和反馈单元组成。控制单元根据输入网络系统的信息和反馈信息, 进行决策分析, 由控制方(可以是控制系统本身, 也可以是网络安全管理人员)下达安全控制命令给执行单元。执行单元按照下达的安全控制指令和安全策略, 对信息网络系统实施安全控制服务。安全控制服务是由必要的安全控制机制组成的。受控对象一般为网络系统和网络系统中的信息资源。反馈单元负责采集受控对象的状态信息和输出信息, 并进行安全效能评估和控制效能评估, 为控制方和控制单元提供改进控制策略、控制方式的决策支持。反控制方是来自网络系统外部的攻击者, 它会对网络系统实施被动和主动方式的各种攻击, 目的是干扰、破坏网络系统的正常运行, 降低信息价值。

在这种控制结构中, 控制单元、执行单元以及反馈单元组成的控制模式成为决定系统控制效能和系统稳定性的关键因素。简要地说, 模式是人们根据以往的经验总结出来的, 可以重复使用的设计方案。模式的定义包括以下四部分内容: 模式的名称; 特点和用途; 解决方案; 使用该模式后的后果(即优缺点)。

信息网络的安全控制模式是实施信息网络安全控制时能够利用的常用控制方式。通过将这些模式灵活运用到适合的控制环节中, 不但能够提高安全控制的效率, 增强系统的安全性, 还能降低系统分析与设计的复杂度。下面给出分析与设计信息网络安全控制系统时常用的几种安全控制模式。

1　管道过滤模式

模式名称: 管道过滤(Pipes and Filters)。

特点和用途: 管道过滤模式是指在受控对象的信息传输通路(即管道)上安插若干过滤控制部件(或控制单元), 每个控制部件完成一项相对独立的安全控制任务, 如数据加/解密、内容过滤、病毒检测与防护等, 它们相互配合, 当信息流通过所有控制部件后, 即实现了最终的控制服务。管道过滤模式特别适合于对指定信息流的安全控制, 如图 3 所示。

收稿日期: 2005-01-29; 修返日期: 2005-04-18
基金项目: 总装备部武器装备预研基金资助项目(51420010501-kg0202)

解决方案:实施管道过滤控制要确保每个控制单元的输入/输出接口与信息流的特征相匹配,能够鉴别并遵循信息流所采用的通信协议,每个控制单元还要提供相应参数配置和状态反馈接口,以便于高层控制单元收集信息和实施调度。在某些情况下,过滤控制部件之间要保持一定的顺序,例如,如果同时采用数据压缩控制与数据加密控制,在收发两端的控制顺序必须正好相反。管道过滤模式的控制部件一般安装在端实体或通信的中间节点上。

优缺点:管道过滤模式易于扩展,其控制单元组装灵活,不足之处是有可能会严重降低受控对象的工作性能,如数据通信的效率。

2 公告栏模式

模式名称:公告栏(Bulletin) 。

特点和用途:公告栏模式是一种数据驱动的安全控制模式,它由一个数据中心和若干分布的安全控制部件(或控制单元) 组成,如图 4 所示。每个控制部件同时具有控制和采集的功能,它们均向数据中心登记并报告自己所监控对象的当前状态,并不断查询数据中心以获得自己所需的系统状态信息,通过这些信息调整自身的控制策略和参数。高层控制单元可以通过监控和调整数据中心的相关数据,向分布在各处的控制部件间接下达控制指令,达到安全控制整个系统的目的。

解决方案:实现公告栏控制模式的关键在于制定统一的系统状态数据交换标准,正确选择与系统控制需求紧密相关的状态参量,并对这些状态数据的存取和利用实施安全保护,如进行访问控制、加密和完整性保护。它的典型应用包括:公钥基础设施(Public Key Infrastructure, PKI) 通过存储在 LDAP (Lightweight Directory Access Protocol) 证书服务器上的公钥证书和证书撤销列表对证书的分发与授权进行控制;国家网络安全应急响应中心通过其安全网站公布最新发现的系统漏洞和相应补丁,敦促相关部门对存在安全缺陷的网络系统采取补救措施;病毒控制中心通过其服务器接收病毒警报,并及时发布最新的病毒特征库,帮助分布在系统各处的病毒防火墙对病毒进行检测与防御。

优缺点:公告栏模式采用数据驱动的安全控制方式,各控制单元可以根据自身的需要灵活查询和公告相关的系统状态数据,有利于将分布在各处的、不同种类的控制模型粘合起来,共同实现系统信息的安全控制。由于采用以数据为中心的间接控制方式,控制反馈的时延和实时性不易确定。

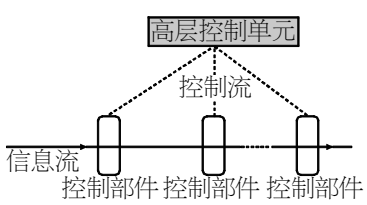

图 3 管道过滤控制模式

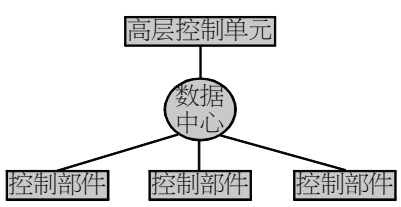

图 4 公告栏控制模式

3 分层模式

模式名称:分层(Layer) 。

特点和用途:分层模式是从不同的层次控制系统,每一层只处理与该层相关的安全问题,层与层之间通过相对独立,具有一致的通信接口。复杂的网络系统一般采用分层的方法实施安全控制。例如对网络协议堆栈中不同协议层的安全通信控制,每一层的安全需求和采用的安全控制策略均不相同,但是各层之间配合起来,就能保障整个系统网络通信的安全性,如图 5 所示。

解决方案:分层控制的关键在于正确划分系统的层次,并采用与该层安全需求相符合的控制技术和控制部件。分层控制的层数不宜太多,否则层与层之间的协调和管理会变得相当复杂,并可能降低网络系统的效率。

优缺点:分层控制模式有利于实现复杂网络系统的安全控制,更改某层的控制部件,不会对其他层造成太大的影响,增加了安全控制的灵活性,同时降低了控制的复杂度。但是,如果层与层之间控制策略不一致,容易造成控制资源浪费或产生安全控制冲突,甚至降低整个系统的安全性。

4 代理模式

模式名称:代理(Proxy) 。

特点和用途:代理模式能够代表系统中的某个组件,甚至是整个系统,与其他系统进行安全通信,传递请求与响应,并在这个过程中实施相应的安全控制。代理控制部件可以充当系统的安全适配器,它能在有效增强系统安全的同时,不影响系统本身的功能,如图 6 所示。基于代理的安全网关和防火墙采用的就是代理控制模式。

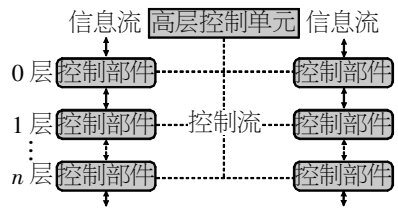

图 5 分层控制模式

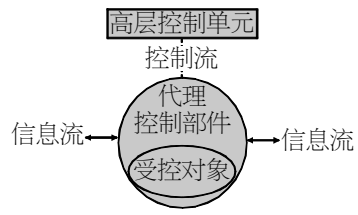

图 6 代理控制模式

解决方案:代理模式主要采用安全控制中间件实现,它们必须与被代理的系统紧密结合,相互信任。因此,安全控制部件一般安装在安全的计算环境中(如智能卡) 。

优缺点:通过安装安全代理控制部件能迅速提高系统的安全性,而不需对现有系统进行任何修改,但是它的通用性受到限制,还会降低系统的通信效率。

5 客户/服务器模式

模式名称:客户/服务器(Client/Server) 。

特点和用途:客户/服务器模式主要应用于分布式网络环境下的安全控制。它是由若干分布在各处的安全控制部件作为客户端,与作为服务器的中心安全控制部件建立通信关系,由客户直接向服务器提交受控对象的当前状态和控制请求,由服务器统一下达控制指令调度各客户端实施安全控制,各客户端之间彼此互不交换控制信息,如图 7 所示。分布式的网络病毒检测系统、分布式的入侵检测系统等采用了这种控制模式。

解决方案:与建立通用的客户/服务器系统一致,但必须保障各控制部件之间控制信息流的安全。

优缺点:客户端控制部件的实现相对简单,而服务器承担了大量的处理工作,往往成为被攻击的焦点和控制系统的性能瓶颈。

6　对等模式

模式名称: 对等(Peer to Peer) 。

特点和用途: 对等模式是一种很有前途的安全控制模式, 它主要用于分布式、大规模网络系统的安全控制, 每个安全控制部件都处于平等的地位, 它们具有自主性、移动性、可配置性和通用的配置管理接口, 它们能够自动监测受控对象的安全状态, 自动确定安全控制需求。当需要实施安全控制时, 每个控制部件均可采用查找与匹配算法, 通过中心调度服务器发现其他控制部件, 并向其他控制部件提出自己的协调控制请求, 或接收来自其他控制部件的控制请求, 相互配合完成各自的安全控制任务, 如图 8 所示。

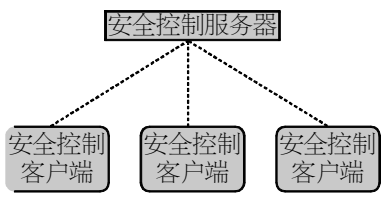

图 7　客户/服务器控制模式

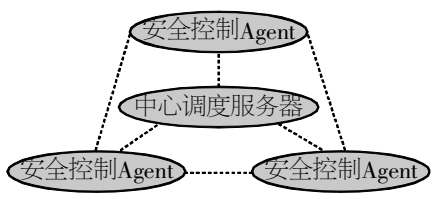

图 8　对等控制模式

解决方案: 对等控制往往采用移动 Agent 技术建立各安全控制部件, 并需要计算机操作系统或虚拟计算环境(如 Java 虚拟机) 的支持, 它们能在网络系统中自由移动, 充分利用网络系统本身的资源。它们自身的安全, 包括完整性和可靠性必须得到保证, 并接受中心调度服务器的生命周期管理。

优缺点: 对等模式是一种崭新的安全控制模式, 它具有可配置、动态灵活的特点, 特别适合于网络结构不固定、安全需求多变的分布式网络系统的安全控制。

7　结论

信息网络是一个复杂的巨系统, 对其进行安全控制是一项系统工程, 为了降低系统分析与设计的难度, 增强安全控制的灵活性、可扩展性和可复用性, 有必要使用一些常用的安全控制模式, 它们与自动控制理论中提出的控制方式[6] 有所不同, 而是融合了信息网络的特点和安全控制需求。对等控制模式应该是未来复杂网络, 特别是网格系统安全控制的潜在方式。

参考文献:

[1]　ndrew S Tanenbaum. Computer Networks(4th Edition) [M]. Prentice Hall, 2003.

[2]　卢昱. 网络控制论浅叙[J]. 装备指挥技术学院学报, 2002, 13(6): 60-64.

[3]　卢昱. 网络控制与控制方式[J]. 装备指挥技术学院学报, 2003, 14(1): 62-65.

[4]　卢昱, 王宇, 吴忠望. 网络控制论系统概念、特性及数学描述[J]. 计算机工程, 2003, 29(21): 128-130.

[5]　卢昱, 王宇, 吴忠望. 基于网络控制论概念的网络控制论系统与分析[J]. 计算机工程与科学, 2004, 26(3): 14-17.

[6]　王雨田. 控制论、信息论、系统科学与哲学[M]. 北京: 中国人民大学出版社, 1986.

作者简介:

王宇(1971-) , 男, 四川简阳人, 副教授, 博士研究生, 主要研究方向为信息网络安全、网络控制; 卢昱(1960-) , 河南洛阳人, 教授, 博士生导师, 国家有突出贡献的中青年专家, 主要研究方向为网络控制论, 信息对抗与网络安全。

(上接第 132 页)

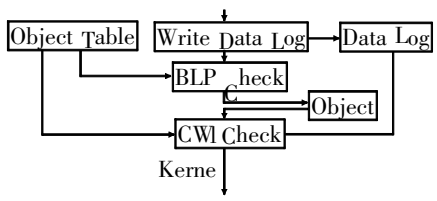

图 3　安全内核的结构和安全检查流程示意图

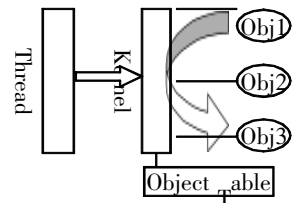

图 4　安全内核安全监控示意图

1.5　系统效率分析

假如系统中产生的对象数为 m, 每个对象的属性平均数为 n 个, 每个属性对应的 TP 为 2 个(读、写) 。假设每个属性仅访问一次, 基于两种方式进行分析。

(1) 如果不把一个完整的访问分离为多个独立的行为, 查找为顺序查找, 发出一个访问消息, 则, 查找对象的平均次数为 $(m+1)/2$, 查找对象属性的平均查找次数为 $(n+1)\times n/2$, 查找属性方法的平均查找次数为 $(2+1)/2$。整个访问所需的平均查找次数为 $((m+1)/2)\times((n+1)\times n/2)\times(2+1)/2$。

(2) 如果把一个完整的访问分离为单个独立的行为, 查找为顺序查找, 发出 n 个访问消息, 则, 查找对象的平均次数为 $n\times(m+1)/2$, 查找对象属性的平均查找次数为 $(n+1)\times n/2$, 查找属性方法的平均查找次数为 $(2+1)/2$。整个访问所需的平均查找次数为 $(n\times(m+1)/2)\times((n+1)\times n/2)\times(2+1)/2$。

第(2) 种方式要完成的平均查找次数为第(1) 种方式的 n 倍。如果 n 较小, 对系统效率的影响是可以接受的。第(1) 种方式虽然效率高, 但是不利于设计完整性检查机制。

2　结束语

基于前述, 通过 BLP 和 CW 两种安全策略结合使用, 可以有效地保证信息的机密性和完整性, 防止非法用户对基于安全开发平台的在线证书服务器的攻击。混合使用该两种策略时, 要注意系统的规模, 对于大的信息系统, 会增加构建系统的复杂度, 降低系统的效率[3] 。由于安全开发平台的规模较小, 因此, 使用 BLP 和 CW 构建安全内核时, 不会对系统效率有太大影响。

参考文献:

[1]　ell, D E L J LaPadulat. Secure Computer Systems[M]. ESD-TR-73-278 (Vol Ⅰ ～Ⅲ) (also Mitre TR-2547) , Mitre Corporation, Bedford, MA, 1974.

[2]　David D Clark, David Il Wilson. The Clark-Wilson Security Model [EB/OL]. URL: www. intel. com/ technology/itj/2003/volume07issue01/art_security/ p05_clr. htm.

[3]　王建军, 宁洪, 陈怀义, 等. 两种模型结合使用的研究与性能分析[J]. 计算机应用研究, 2004, 21(11): 95-96.

作者简介:

王建军(1969-) , 男, 副教授, 硕士, 主要研究方向为信息安全、软件体系结构; 宁洪, 教授, 主要研究方向为数据挖掘、信息安全; 彭代文, 硕士研究生, 主要研究方向为网络信息安全。