文章编号:1005-0523(2004)03-0158-04

构建高校网络安全系统

杨学富

(九江学院 主校区,江西 九江 332005)

摘要:先就高校网络安全系统的必要性做了一个简单的阐述,然后指出当前的一些网络系统安全模型,最后提出一个基于高校网络的新型系统安全模型.

关 键 词:网络安全;高校;系统;防火墙;模型
中图分类号:TU201 **文献标识码**:A

0 引 言

在人类步入全球信息化的今天,网络的潜力才刚刚开始发掘出来,由此而降临的机遇是无穷无尽的,社会上的各种组织机构都已经或者正在体验着国际互联网带来的诸多便利,然而,随着网络的发展,个人信息和关键性的机构信息也面临着前所未有的安全问题.事实上,信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分,是世纪之交世界各国在奋力攀登的制高点.高校作为社会主义建设的排头兵,前瞻性的建立起一整套有中国特色的高校网络安全系统已经成为一个迫在眉睫的重要课题.

1 建立高校网络安全系统的迫切性

目前影响网络安全的方式主要有两种:网络黑客和网络病毒.

1.1 从全球的角度看

世界500强企业,面临越来越多的黑客袭击、病毒事件,这已经影响到企业的信息安全.

美国国防部已经花费了数十亿美元用以整治网络安全,但是黑客们总是能突破防线.

2003年,黑客袭击了全球13台最重要的母服务器中的9台,充分显示了当前互联网体系的脆弱.

1.2 从全国的角度看

我国计算机病毒疫情调查报告显示:信息安全面临严峻形势主要表现在:

1)信息与网络安全的防护能力很弱.

2)对引进的信息技术和设备缺乏保护信息安全所必不可少的有效管理和技术改造.

3)基础信息产业薄弱,严重依赖国外.

4)国家信息安全管理机构缺乏权威,协调不够.

5)信息犯罪在我国有发展蔓延的趋势.

6)全社会的信息安全意识急需提高.

此外,在意识形态领域,电子媒介成为国际意识形态斗争的主导工具;在军事领域,网络泄密是军事信息安全问题的重要表现;黑客攻击对军事信息安全危害极大;信息战是影响军事信息安全的极端表现形式.

1.3 从全国高校的角度看

首先,高校的用户基数较大,校园网节点众多,网络拓扑相当复杂,资源共享、信息交互成为病毒传播的一个很重要的途径,病毒泛滥屡见不鲜;其次,安全管理刻不容缓,据相关数字显示,80%以上的网络攻击是来自于校园网内部,部分学生受好奇

收稿日期:2004-01-10

作者简介:杨学富(1956-),男,吉林省长春市人,副教授.

中国知网 http://www.cnki.net

心等动机驱使,窃听他人密码等重要信息,蓄意进行 DoS 等攻击,甚至进攻校园试卷、成绩系统.最后,由于互联网的每个网关都是进入网络的门户,因此黑客能利用这个弱点通过校园的互联网连接侵入学校网络,并给系统和数据造成严重破坏.这些已经成为校园网络的重大安全隐患.

2　当前网络系统安全模型

根据国际上的标准划分,将信息安全威胁分为三大类:

Ⅰ、C 级威胁

信息攻击者是个体,单点攻击,攻击的范围、深度和能够完成的攻击任务不太复杂,往往是黑客行为.

Ⅱ、B 级威胁

有组织分布式协同攻击.多点、多技术和协同攻击,相互掩护,危害大,难于对付.

Ⅲ、A 级威胁

信息战威胁(IT War).是比 B 级威胁更大范围的攻击,使用的攻击技术更全面,危害更大.可以采用一切目前已知攻击手段,包括可控计算机病毒、信息炸弹、信息炮弹、网络远程安装攻击软件、使用网络攻击平台.使用多技术体制的网络,包括卫星通信在内的一切可利用的通信网络.

基于这三个层面的安全系统模型主要有以下三种:

2.1　纵深防御模型

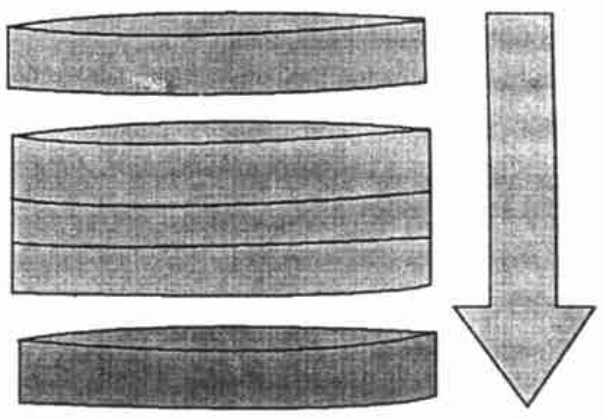
基本思想:安全不论攻击和防守总体来说都是过程.安全的成功与否关键在于对过程的把握.在这个过程中防御层数越多,对网络资源进行未授权访问的难度就越大.这一战略通过提供冗余防御层来确保安全性,在某一层或者在某些情况下多个层被攻破时,冗余的防御层能够对资源进行保护.

这种模型防御如图 1 所示,其中:边界安全保护的是系统和外界接口部分;平台安全保护的是网络和系统平台;业务安全包含业务系统和业务系统开发安全两个部分.

2.2　多层次防护模型

"多层次防护"提供了这样一种思路:结合不同的安全保护因素,例如防病毒软件、防火墙和安全漏洞检测工具,来创建一个比单一防护有效得的多的综合的保护屏障.分层的安全防护成倍地增加了黑客攻击的成本和难度,从而大大减少了他们对企业的攻击.

分层的安全防护技术具体来说包括攻击检测,攻击防范,攻击后的恢复这三个大方向,每一个方向上有代表性的产品:入侵检测系统负责进行攻击检测,防火墙和强制访问控制系统负责攻击防范,攻击后的恢复则由自动恢复系统来解决.这三大方向就说明了在网络安全防护上的多层安全防护措施.



图(1)　纵深防御模型

2.3　通道安全模型

所谓网络安全传输通道,就是利用安全通道技术(Secure Tunneling Technology),通过将待传输的原始信息进行加密和协议封装处理后再嵌套装入另一种协议的数据包送入网络中,像普通数据包一样进行传输.经过这样的处理,只有源端和目的端的用户对通道中的嵌套信息能够进行解释和处理,而对于其他用户而言只是无意义的信息.网络安全传输通道应该提供以下功能和特性:

1) 机密性:通过对信息加密保证只有预期的接收者才能读出数据.

2) 完整性:保护信息在传输过程中免遭未经授权的修改,从而保证接收到的信息与发送的信息完全相同.

3) 对数据源的身份验证:通过保证每个计算机的真实身份来检查信息的来源以及完整性.

4) 反重发攻击:通过保证每个数据包的唯一性来确保攻击者捕获的数据包不能重发或重用.

3　多维高校网络系统安全模型

经过实践探索,结合我校实际情况,笔者提出一种理论模型:多维高校网络系统安全模型.

该模型由:密码理论与技术, 信息安全、对抗、

中国知网 https://www.cnki.net

分析和监控理论与技术，安全协议理论与技术，安全体系结构理论与技术，主机网络安全理论与技术五个要素组成一个立体的、多维的高校网络系统安全模型.

3.1 密码理论与技术

密码理论与技术主要包括两部分，即基于数学的密码理论与技术(包括公钥密码、分组密码、序列密码、认证码、数字签名、Hash 函数、身份识别、密钥管理、PKI 技术等)和非数学的密码理论与技术(包括信息隐形，量子密码，基于生物特征的识别理论与技术).本文主要涉及是前者，应用基于数学的密码理论的加密技术又可分为对称加密和非对称加密两大类.

3.1.1 对称加密技术

在对称加密技术中，对信息的加密和解密都使用相同的钥，也就是说一把钥匙开一把锁.这种加密方法可简化加密处理过程，信息交换双方都不必彼此研究和交换专用的加密算法.如果在交换阶段私有密钥未曾泄露，那么机密性和报文完整性就可以得以保证.

3.1.2 非对称加密/公开密钥加密

在非对称加密体系中，密钥被分解为一对(即公开密钥和私有密钥).这对密钥中任何一把都可以作为公开密钥(加密密钥)通过非保密方式向他人公开，而另一把作为私有密钥(解密密钥)加以保存.公开密钥用于加密，私有密钥用于解密.非对称加密方式可以使通信双方无须事先交换密钥就可以建立安全通信.

3.2 信息安全、对抗、分析和监控理论与技术

网络信息安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断.

消除这种危险的最有效策略是使用防火墙.网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，保护内部网络操作环境的特殊网络互联设备.它对两个或多个网络之间传输的数据包如链接方式按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态.

如果在连接外部世界的每个网络部署防火墙，它们就会在网络的周围竖起一道"围墙".此举有利于确保只有经过授权的用户才能进入网络.

随着网络安全技术的整体发展和网络应用的不断变化，现代防火墙技术已经逐步走向网络层之外的其他安全层次，不仅要完成传统防火墙的过滤任务，同时还能为各种网络应用提供相应的安全服务.另外还有多种防火墙产品正朝着数据安全与用户认证、防止病毒与黑客侵入等方向发展.

3.3 安全协议理论与技术

在因特网上普遍采用的是TCP/IP 协议，TCP/IP 协议的体系结构相对于 OSI/ISO 体系结构的 7 层模型是比较简单而实用的，其模型如下：

应用层
传输层
网络层
主机到网络层

此体系结构中，最下面的主机到网络层实际上包括了 OSI 模型中的 2 层：数据链路层和物理层.本文将从 TCP/IP 的各个层次介绍相关的安全协议理论与技术.

数据链路层技术涉及到软件和硬件两个方面，硬件方面不在本文中讨论.当前能在此层提供安全通道技术的安全协议主要有：PPTP 和 L^2TP.它们主要是为了组建远程访问 VPN 而提出的.

在网络层的协议是 Internet 工程任务组(IETF)于 1998 年公布了因特网安全体系结构—IPSec 规范.

在传输层能够实现安全传输通道的协议是 Netscape 通信公司制定的安全套接层协议(Secure Socket Layer，简称 SSL)，它建立在可靠的传输服务(如 TCP/IP 所提供)基础之上.

网络层(或传输层)的安全协议允许为主机(进程)之间的数据通道增加安全属性.

3.4 安全体系结构理论与技术

对于网络安全这个新兴的课题，由于其本身涉及的层面较为广泛，其复杂程度超出一般人的想象.网络安全作为支撑网络经济的一个独特而重要的基石，需要强有力的技术支持.要求每一位网络管理教师或网络技术教师在精通网络技术的同时又是一位合格的、全面的安全专家是不现实的.在此，给出一种由网络安全专家、专业的网络安全工具和安全管理策略组成的多维技术支持体系模型：

Ⅰ.定期安全评估

由数名网络安全专家结合高校实际情况及目前国际先进安全标准体系，从整体上帮助网络管理者及时发现网络中的安全隐患，并提出切实可行的

中国知网 https://www.cnki.net

防范措施.

Ⅱ.常规与紧急响应

当有非法入侵、恶意攻击、网络病毒等网络犯罪行为发生时,专家可以根据事件的紧急情况,提供常规或紧急响应的技术支持.

Ⅲ.安全日志分析

Ⅳ.漏洞修补与安全配置

Ⅴ.网络安全培训

3.5　主机网络安全理论与技术

由于主机安全和网络安全的技术手段难以有机地结合,因此容易被入侵者各个击破.并且,由于它们在保护计算机和信息的安全上各自为政,因此很难解决系统安全性和使用方便性之间的矛盾.举一个简单的例子,从严密保护主机安全来说应该禁止用户的远程登录,但是这给用户的使用将带来极大的不便,对 Internet 上绝大多数 Unix 主机来说是不可以接受的.而一旦允许用户远程登录,却无法区分用户的远程登录是合法的还是非法的,也就控制不了非法用户的入侵,并且系统一旦被入侵,入侵者就拥有该用户的全部权力,危害极大.对于防火墙系统来说也有同样的问题,防火墙可以禁止外部主机对于内部主机的访问(安全而不方便),但是一旦允许用户经防火墙授权验证后进入内部主机,就无法控制其在内部主机上的行为(方便就不安全了).

为了解决这些问题,可采取主机网络安全技术.主机网络安全技术是一种主动防御新兴的边缘安全技术.它结合网络访问的网络特性和操作系统特性来设置安全策略,可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行,实现对于同一用户在不同的场所拥有不同的权限,从而保证合法用户的权限不被非法侵占.主机网络安全技术考虑的元素有 IP 地址、端口号、协议、甚至 MAC 地址等网络特性和用户、资源权限以及访问时间等操作系统特性,并通过对这些特性的综合考虑,来达到用户网络访问的细粒度控制.

4　结束语

网络信息安全是国内外都十分重视的研究课题,高校网络安全系统的研究是一门新兴的计算机网络安全边缘学科,它的理论尚未成熟,其功能、需求、体系结构、实现技术都有待进一步的研究.但是,高校网络安全系统在全国网络安全系统中的示范作用、前导作用、预警作用会越来越明显,因此,它值得我们重视,并更加深入地研究.

参考文献:

[1]葛秀慧、田浩、王凌云、盖俊飞.计算机网络安全管理[M].北京:清华大学出版社,2003

[2]李志、徐时新、蒋东兴.构建主机安全系统[M].计算机工程与应用,2000,(8)

[3]李海泉、李健.计算机网络安全与加密技术[M].北京:科学出版社,2003

[4]张越今.网络安全与计算机犯罪勘查技术学[M].北京:清华大学出版社,2003

[5]蒋东兴、徐时新、李志.主机网络安全初探,小型微型计算机系统[J].北京:2000,(7)

[6]汤惟.密码学与网络安全技术基础[M].北京:机械工业出版社,2004

[7]张世永.网络安全原理与应用[M].北京:科学出版社,2003

[8]钟乐海.网络安全技术[M].北京:电子工业出版社,2003

[9]Chris Hare 等.Internet 防火墙与网络安全[M].北京:机械工业出版社,1998

[10]刘玉珍等译.密码编码学与网络安全:原理与实践[M].北京:电子工业出版社,2004

Structuring College Network Security System

YANG Xue-fu

(Jiujiang University, Jiujiang 332005, China)

Abstract: This text first gives a simple exposition on the necessity of building university network security system, then points out the safe models of some present network systems, finally put forwards a new-type safe model of system used in university network finally.

中国知网 https://www.cnki.net

Key words: network security; university; system; fire wall; model