计算机网络安全实用技术

COMPUTER NETWORK SECURITY PRACTICAL TECHNOLOGY

徐超汉　柯宗贵　　编著

COMPUTER NETWORK SECURITY PRACTICAL TECHNOLOGY

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

计算机网络安全实用技术

徐超汉　柯宗贵　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书着重介绍当代计算机网络安全领域中最实用、最先进的技术，其中包括网络安全系统中最常用的防火墙技术、入侵检测技术、防病毒技术，以及网络安全加固、安全审计与敏感信息跟踪等。

计算机网络安全不仅是一个含金量较高的技术问题，更是一个管理问题。因此，本书除了适用于计算机系统管理员、网络管理员和信息工程系统集成工程师外，也适用于有关主管领导和计算机网络系统资源的使用者。

图书在版编目（CIP）数据

计算机网络安全实用技术 / 徐超汉，柯宗贵编著. —北京：电子工业出版社，2005.3
ISBN 7-121-00949-8

Ⅰ. 计… Ⅱ.①徐… ②柯… Ⅲ. 计算机网络—安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 011420 号

责任编辑：龚立堇
印　　刷：北京东光印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：16.5　字数：416 千字
印　　次：2005 年 3 月第 1 次印刷
印　　数：5 000 册　　定价：26.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

计算机网络无疑是当今世界最为激动人心的高新技术之一，尤其是因特网的迅速发展正在把一个世界连接成一个整体，“世界”的概念已变小。网络的迅速发展正在改变人们的传统生活方式，给人们带来了新的工作、学习和娱乐方式。

但是，在科学技术发展的同时，人类必然面临新的威胁，计算机及计算机网络的发展带来的计算机网络犯罪就是其中一个颇为典型的例子。因此，构建一个完整的计算机网络安全体系已刻不容缓。

本书的目的是帮助计算机网络系统管理员在这个千变万化的网络世界中如何去保护自己的网络，以及网络中的数据，也就是说保护“数据”财富不被毁坏和丢失。本书的内容较为广泛，凡与当今网络安全技术有关的课题基本上都已包含。其中包括鉴别、加密、防火墙、入侵检测、防病毒、安全扫描、安全审计、敏感信息的跟踪、网络的安全加固、防垃圾邮件和防病毒邮件等。

信息技术在我国正处于蓬勃发展的时期，21 世纪的中国必然是一个遍布信息网络的中国。本书如能为网络工作者和网络用户提供帮助的话，我们将感到万分的欣慰。

计算机网络安全是一个不断发展的全新课题，经验不足在情理之中，又由于作者的水平有限，时间仓促，在编写之中难免有不妥之处，衷心希望广大读者批评指正。

本书在出版的过程中，得到了广东天海威数码科技有限公司郑少荣高级工程师，张贺勋、蔡庆润、陈伟纯等工程师的大力支持，他们不仅提供并整理部分颇有价值的资料，还为本书的大部分内容进行了测试，在此特致以谢意！

作　者

2005 年 1 月于广州

目　录

第1章 概 述

“安全”一词在字典中被定义为“远离危险的状态或特性”和“为防范间谍活动、蓄意破坏、犯罪、攻击或逃跑而采取的措施”。随着经济信息化的迅速发展，计算机网络对安全的要求越来越高，尤其 Internet 和 Intranet 应用发展以来，网络的安全已经涉及到国家主权等许多重大问题。由于“黑客”工具技术的日益发展，使得使用它所需要具备的各种技巧和知识相对简单，从而造成全球范围内“黑客”行为的泛滥，导致了一个全新战争形式的出现，即网络安全技术的大战。

1.1 导致网络不安全的因素

网络不安全的因素来自两个方面，一方面是网络本身存在的安全缺陷；另一方面是人为因素和自然因素。自然因素是一些意外事故，如发生地震毁坏网络或服务器突然断电等，这种因素并不可怕，可怕的是人为因素，即人为的入侵和破坏。

由网络自身存在安全隐患而导致网络不安全的主要因素有：网络操作系统的脆弱性、TCP/IP 协议的安全性缺陷、数据库管理系统安全的脆弱性、网络资源共享、数据通信、计算机病毒等。

1.1.1 网络操作系统的脆弱性

网络操作系统是计算机网络最基本的软件。无论哪一种操作系统其体系结构本身就是一种不安全的因素。由于操作系统是可以动态连接的，包括 I/O 驱动程序与系统服务都可以用打补丁的办法进行升级和动态连接。这种打补丁的方法，生产该产品的厂商可以使用，“黑客”也可以使用，因而这种动态连接正是计算机病毒产生的温床。这种使用打补丁与渗透开发的操作系统是不可能从根本上解决安全问题的。由于操作系统支持的程序动态连接和数据动态交换是现代系统集成和系统扩展的必备功能，所以，操作系统的这种安全性弱点是无法避免的。

操作系统不安全的另一个原因在于它可以创建进程，即使在网络结点上同样也可以进行远程进程的创建与激活。更令人不安的是被创建的进程具有可以继续创建进程的权利，这一点加上操作系统支持网络上传输文件，在网络上能加载程序，二者结合起来就构成了可以在远端服务器上安装“间谍”软件的条件。如果把这种“间谍”软件以打补丁的方式“打”入合法用户，尤其是“打”入特权用户，那么，系统进程与作业监视程序根本监测不到“间谍”的存在。

在 UNIX 与 Windows NT 中的 Daemon 软件实际上是一些系统进程，它们通常总是在等

待一些条件的出现，一旦有满足要求的条件出现，程序便继续运行下去。这类软件正是被“黑客”们所看中利用的。更令人担忧的是 Daemon 软件具有与操作系统核心层软件同等的权力。

网络操作系统提供的远程过程调用（RPC）服务，以及它所安排的无口令入口也是“黑客”攻击网络的通道。

凡此种种，充分暴露了操作系统在安全方面的脆弱性对网络安全已构成了威胁。

1.1.2 TCP/IP 协议的安全性缺陷

因特网的基础是 TCP/IP 协议，该协议在实现上力求简单高效，而没有考虑安全因素。第一，TCP/IP 是以明文（未加密）数据包的方式发送数据的，电子邮件口令、文件传输很容易被监听和窃取，而且可以实现监听和窃取行为的工具很多，在网上又是免费提供的；第二，基于 TCP/IP 的应用服务都在不同程度上存在安全弱点；第三，TCP/IP 在流程设计上也存在安全缺陷，缺乏安全策略；第四，访问控制的配置十分复杂，易被错误配置，从而给“黑客”以可乘之机。

1.1.3 数据库管理系统安全的脆弱性

由于数据库管理系统（DBMS）对数据库的管理是建立在分级管理概念上的，因此，DBMS 的安全是可想而知的。另外，DBMS 与网络操作系统之间存在不少接口，它的安全必须与操作系统的安全配套，这无疑是一个先天性的不足之处。由于 DBMS 是在操作系统上运行的，所以，这种安全性弱点是无法克服的。

1.1.4 网络资源共享

计算机网络系统的最大优点是实现系统资源共享，包括硬件资源、软件资源、数据资源等的共享。各终端用户可以访问服务器的资源，各终端之间也可以相互共享资源。这种资源共享为异地用户提供了巨大的方便，同时，也为非法用户窃取信息、破坏信息创造了条件。非法用户可以通过终端或结点进行非法浏览、非法修改。此外，系统硬件或软件的故障也可能引起泄密。由于大多数共享的资源，往往同许多使用者之间有相当一段距离（如网络打印机），这样就给窃取信息在时间和空间上创造了许多便利条件。

1.1.5 数据通信

计算机网络系统需要通过数据通信来交换信息，这些信息是需要通过物理线路或无线电波，以及电子设备进行传播的。这样在通信中传输的信息极易遭到破坏，如网络侦听、搭线窃听、电磁窃听、网络线路的辐射泄密等。

1.1.6 计算机病毒

计算机网络可以从多个结点接收信息，因而极易感染计算机病毒。病毒一旦入侵网

络，再按指数增长进行复制和传染，很快就会遍及网络各结点，短时间内可以造成网络系统瘫痪。

1.2 网络安全技术的分类

计算机信息网络的安全技术可分为三大类，即

- 实体安全：包括机房、线路、主机、媒体和其他设备及物理环境等。
- 运行安全：包括网络的畅通、准确，以及网上信息的安全（授权、加密、身份鉴别等）。
- 信息安全：又称应用安全，其中包括电子邮件安全、浏览器安全、程序安全、I/O安全、数据库安全，以及审计与控制、数据备份等。

1.3 网络安全系统的解决方案

网络安全系统实际上是一组用于控制网络之间通信流的部件。这种网络安全系统根据本单位规定的安全策略，准许或拒绝网络通信。

由于网络安全范围的不断扩大，如今的网络安全不仅仅保护内部资源的安全，还必须提供其他大量的服务，例如，用户确认，加密，甚至安全管理传统的商务交易机制，如订货和记账等。

1.3.1 安全策略的制定依据

在设计一个网络安全系统时，首要任务是确认该单位的需要和目标，并制定安全策略。安全策略需要反映出该单位同公用网络连接的理由，并分别规定对内部用户和公众用户提供的服务。当制定安全策略时，需首先确定的最重要的原则是允许访问除明确拒绝以外的全部服务程序，还是拒绝访问除明确准许以外的全部服务程序。在建立安全策略时，这是关键性的，但往往又是容易被忽视的一步。准许访问除明确拒绝以外的全部服务程序，对大部分服务程序都很少干预。危及安全的服务程序可能被提供使用并已引发问题，直到管理人员明确加以禁止为止，安全问题颇为突出。当安全策略是拒绝访问除明确准许以外的全部服务程序时，可能在有新的有用的服务程序可供使用时，用户无法得到，此时，用户需要将该新服务程序通知管理人员，管理人员对该程序进行鉴定后决定是否允许被使用。

在做出基本的决策之后，决定哪些服务程序可供内部用户使用，哪些服务程序可供外部网络用户使用。

安全策略设计还需要有监视安全的方式和实施策略的方式。

在设计安全策略和选择网络安全系统时，还需要考虑成本与方便两者的平衡。这取决于所期望的安全程度和所选用的安全系统，可能需要的额外硬件，如路由器和专用主计算机，也可能需要特殊的软件，还可能需要安全专家进行系统编程和维护工作。其他需要考虑的因素是，安全系统对生产率和服务利用率的影响。有的网络安全系统会降低网络性能，有的会限制和拒绝网络上的一些有用的服务程序，如邮件和文件传输，有的则需要将

软件分配给内部网络中每一台主机，给用户带来了诸多的不便。因此，网络安全系统应该被设计成一个透明的安全系统，这样才能为网络提供安全保护而不会对网络性能有重大的影响，也不会迫使用户放弃一些服务程序或迫使用户去学习某些新的服务程序。

在网络安全策略设计时，需要考虑的另一个重要因素是，对安全程度和复杂程度两者的平衡。在网络安全设计中，安全系统越复杂，就容易遭到破坏，维护也越困难。网络安全系统的复杂程度由于下列因素而增加：增添和管理较多的网络，追加额外的硬件，增加筛选规则的数量。复杂的系统不容易进行正确的配置，因而可能发生安全问题。

总之，在制定网络安全策略时应当考虑如下因素：

- 对于内部用户和外部用户分别提供哪些服务程序；
- 初始投资额和后续投资额（新的硬件、软件及工作人员）；
- 方便程度和服务效率；
- 复杂程度和安全等级的平衡；
- 网络性能。

1.3.2 网络安全的解决方案

通常计算机信息网络安全的解决方案应从以下六个方面考虑。

1. 物理层安全解决方案

物理层安全是保护计算机网络设备、设施和其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误或错误、各种犯罪行为导致的破坏，主要包括：

- 环境安全；
- 设备安全（含主机）；
- 通信线路安全。

此外，对不同密级的网络必须隔离开。需采用隔离安全技术将不同密级要求的两个网络在物理上隔开，同时，又要保证在逻辑上两个网络能够连通。

2. 网络层安全解决方案

网络层的安全性提供了一种手段来保证对网络应用、数据和服务的访问安全性，即只有通过认证和授权的用户才能访问网络。通常为网络层提供安全性控制是通过访问限制设备，如防火墙设备等。

根据防火墙技术，建议在各中心网络边界，以及与因特网连接的边界安装防火墙，并需实施相互的安全策略控制。如果对外提供信息查询等服务，为控制对关键服务器的授权访问，建议把对外服务器集合起来划分为一个专门的服务器子网，并实施防火墙策略对之加以保护。

为了能实时地对网络入侵进行检测，建议在设置防火墙的同时配置入侵检测系统 IDS。

为了数据传输的安全，建议采用 VPN，对拨号用户采用强制身份认证。

其他可以有助于提高网络层安全性级别的工具有病毒扫描器和内容过滤器（Content filter）。

3. 系统层安全解决方案

系统层包括两部分，即操作系统和数据库系统。前者的安全性主要针对防病毒，后者

的安全性主要为敏感数据加密。

4. 应用层安全解决方案

对于应用层的安全，主要采用如下安全技术：

- 身份认证；
- 防火墙技术和入侵检测技术；
- 各种应用服务的安全性可增强配置服务来保障应用层的安全。

5. 安全管理解决方案

建议：

- 加强安全体系建设的规范化，建立整网统一的安全建设规范；
- 加强安全组织体系的建设；
- 加强安全管理制度的建设；
- 安全管理手段的多样性，对 OSI 的各层进行综合技术管理，包括备份与灾难性备份等。

6. MODEM 安全

防止对网络拨号设备的非授权访问。此外需要限制 MODEM 的速率，因为当 MODEM 速率能激活 SLIP 协议和 PPP 协议的时候，防火墙将形同虚设。

1.4 网络安全性措施

网络安全是一个涉及到多方面的问题，可以说是一个极其复杂的系统工程，它不仅仅局限于通信保密、对信息的加密等功能要求。通常，要实施一个完整的网络安全系统，至少应该包括三类措施：

- 社会的法律、法规，以及企业的规章制度和安全教育等外部软件环境。
- 技术方面的措施，如网络防毒、信息加密、存储通信、授权、认证及防火墙技术等。
- 审计和管理措施，这方面措施同时也包含了技术与社会措施，如实时监控系统的安全状态，提供实时改变安全策略的能力，对现有的安全系统实施漏洞检查等。

建议采用的可以为网络提供适当安全的常用方法有：修补系统漏洞，病毒检查，加密，执行身份鉴别，防火墙，捕捉闯入者，直接安全，空闲机器守则，废品处理守则，口令守则等。

上述这些方法中后四种是必须向网络管理人员及企业其他工作人员下达的守则，其余部分是能够在系统上实现的。

此外，可以采用的网络安全性措施有：

- 选择性能优良的服务器。服务器是网络的核心，它的故障意味着整个网络的瘫痪，因此，要求服务器应具有容错能力、带电热插拔技术、智能 I/O 技术，以及具有良好的扩展性。
- 采用服务器备份。服务器备份方式分冷备份与热备份两种，热备份方式由于实时性好，可以保证数据的完整性和连续性，是得到广泛采用的一种备份方式。
- 对重要网络设备、通信线路的备份。通信故障就意味着正常工作无法进行。所以，对于交换机、路由器及通信线路，最好都有相应的备份措施。