面向21世纪网络技术实用教程系列

网络安全技术教程

赵小林 主编　　彭祖林　王亚彬 编著

国防工业出版社

面向21世纪网络技术实用教程系列

网络安全技术教程

赵小林　主编
彭祖林　王亚彬　编著

国防工业出版社
·北京·

内 容 简 介

本书着重讲述了网络安全的基本概念以及实际问题的解决，很多资料均有可靠的实验为背景，为工程技术人员提供了一份可供参考的资料。

全书共分六章，每章的内容都是由简单到复杂，便于读者学习掌握。不仅讲述了网络安全的基础知识，还以实例分析的方式介绍了一些防病毒、防黑客软件的基本用法以及如何将结果显示出来。

本书实例贴近生活，实用性强，尤其取材于生活实践，激发读者的学习热情，通过学习，可以达到学以致用、立竿见影的效果。特别适用于从事网络安全的科研人员和高校的师生使用。

图书在版编目(CIP)数据

网络安全技术教程/赵小林主编 .—北京：国防工业出版社，2002(2004.2 重印)
(面向 21 世纪网络技术实用教程系列)
ISBN 7-118-02920-3

Ⅰ.网… Ⅱ.赵… Ⅲ.计算机网络－安全技术－高等学校－教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 055218 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号)
(邮政编码 100044)
腾飞胶印厂印刷
新华书店经售
*
开本 787×1092 1/16 印张 19¼ 443 千字
2002 年 10 月第 1 版 2004 年 2 月北京第 2 次印刷
印数：4001—6000 册 定价：26.00 元

前　言

以 Internet 为代表的全球性信息化浪潮日益高涨，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要问题，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在：

1. 开放性的网络，导致网络的技术是全开放的，任何一个人、一个团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的，可以对物理传输线路的攻击，也可以对网络通信协议和实现实施攻击；可以对软件实施攻击，也可以对硬件实施攻击。比如：通过在网络上监听获取网上用户的账号和密码，监听密钥分配过程，攻击密钥分配服务器；利用 UNIX 操作系统提供的 Daemon，利用 FTP 采用匿名用户访问进行攻击，等等。

2. 国际性的网络意味着网络受到攻击不仅仅来自本地网络的用户，它可以来自 Internet 上的任何一台机器，也就是说，网络安全所面临的是一个国际化的挑战。

3. 自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

4. 尽管开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得他们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力。通过 Internet，他们可以从异地取回重要数据，同时又要面对 Internet 开放带来的数据安全的新挑战和新危险。如何保护企业的机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要考虑的重要事情之一。

在我国，对网络安全的研究起步晚，网络安全技术还有待整体地提高和发展。面对日益严重的安全问题，我们应该如何去认识、去分析、去防范，是我们当前每一个投身于 Internet 的人所面临的一个迫切的问题，本书即是从这个目的出发，希望通过对安全问题的一些探讨，和对网络入侵（黑客）技术的分析，来提高广大读者朋友在网络及整个系统安全方面的意识。

由于网络安全技术和其中所涉及的黑客技术都要涉及很多很深的领域，加上作者水平有限，不当之处在所难免，敬请各位读者不吝指正。望集众人之才思，筑起中国坚强的防火长城。

目　录

第 1 章　网络安全概论

§1.1　网络安全的概念

随着 Internet 的发展，网络安全越来越成为一个敏感的话题。网络安全有很多基本的概念，我们先来简单地介绍一下。

1.1.1　网络安全威胁

目前，计算机互联网络面临的安全性威胁主要有以下几个方面：

1. 非授权访问和破坏("黑客"攻击)

非授权访问：没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。操作系统总不免存在这样那样的漏洞，一些人就利用系统的漏洞，进行网络攻击，其主要目标就是对系统数据的非法访问和破坏。"黑客"攻击已有十几年的历史，黑客活动几乎覆盖了所有的操作系统，包括 UNIX、Windows NT 、VM、VMS 以及 MVS。

我们后面会对这一节的内容进行详细讨论。

2. 拒绝服务攻击(Denial Of Service Attack)

一种破坏性攻击，最早的拒绝服务攻击是"电子邮件炸弹"，它能使用户在很短的时间内收到大量电子邮件，使用户系统不能处理正常业务，严重时会使系统崩溃、网络瘫痪。它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

3. 计算机病毒

计算机病毒程序很容易做出，有着巨大的破坏性，其危害已被人们所认识。单机病毒就已经让人们"谈毒色变"了，而通过网络传播的病毒，无论是在传播速度、破坏性，还是在传播范围等方面都是单机病毒不能比拟的。

4. 特洛伊木马(Trojan Horse)

特洛伊木马的名称来源于古希腊的历史故事。特洛伊木马程序一般是由编程人员编制，它提供了用户所不希望的功能，这些额外的功能往往是有害的。把预谋的有害的功能隐藏在公开的功能中，以掩盖其真实企图。

5. 破坏数据完整性

指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，可以修改

网络上传输的数据，以及销毁网络上传输的数据，替代网络上传输的数据，重复播放某个分组序列，改变网络上传输的数据包的先后次序，使攻击者获益，以干扰用户的正常使用。

6. 蠕虫(Worms)

蠕虫是一个或一组程序，它可以从一台机器向另一台机器传播。它同病毒不一样，它不需要修改宿主程序就能传播。

7. 活板门(Trap Doors)

为攻击者提供“后门”的一段非法的操作系统程序。这一般是指一些内部程序人员为了特殊的目的，在所编制的程序中潜伏代码或保留漏洞。

8. 隐蔽通道

是一种允许违背合法的安全策略的方式进行操作系统进程间通信(IPC)的通道，它分为隐蔽存储通道和隐蔽时间通道。隐蔽通道的重要参数是带宽。

9. 信息泄漏或丢失

指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括：信息在传输中丢失或泄漏(如“黑客”们利用电磁泄漏或搭线窃听等方式截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等)，信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息等。

在所有的操作系统中，由于 UNIX 系统的核心代码是公开的，这使其成为最易受攻击的目标。攻击者可能先设法登录到一台 UNIX 的主机上，通过操作系统的漏洞来取得特权，然后再以此为据点访问其余主机，这被称为“跳跃”(I stand-hopping)。攻击者在到达目的主机之前往往会先经过几次这种跳跃。这样，即使被攻击网络发现了攻击者从何处发起攻击，管理人员也很难顺次找到他们的最初据点，而且他们在窃取某台主机的系统特权后，退出时删掉系统日志。用户只要能登录到 UNIX 系统上，就能相对容易地成为超级用户。所以，如何检测系统自身的漏洞，保障网络的安全，已成为一个日益紧迫的问题。

1.1.2 网络安全策略

在网络安全中，加强网络的安全管理，制定有关规章制度，对于确保网络的安全、可靠地运行，将起到十分有效的作用。

安全策略是指在一个特定的环境里，为提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括了建立安全环境的三个重要组成部分，即：

威严的法律：安全的基石是社会法律、法规与手段，这是建立一套安全管理的标准和方法。即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

先进的技术：先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，根据安全服务的种类，选择相应的安全机制，然后集成先进的安全技术。

严格的管理：网络的安全管理策略包括有确定安全管理等级和安全管理范围；制定有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。各网络使用机构、企业和单位应建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

1.1.3 网络安全的五要素

安全包括五个基本要素：机密性、完整性、可用性、可控性与可审查性。

机密性：确保信息不暴露给未授权的实体或进程。

完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。

可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。

可控性：可以控制授权范围内的信息流向及行为方式。

可审查性：对出现的网络安全问题提供调查的依据和手段。

1.1.4 网络安全服务、机制与技术

安全服务：包括控制服务、数据机密性服务、数据完整性服务、对象认证服务、防抵赖服务。

安全机制：包括访问控制机制、加密机制、认证交换机制、数字签名机制、防业务流分析机制、路由控制机制。

安全技术：包括防火墙技术、加密技术、鉴别技术、数字签名技术、审计监控技术、病毒防治技术。

在安全的开放环境中，用户可以使用各种安全应用。安全应用由一些安全服务来实现；而安全服务又是由各种安全机制或安全技术来实现的。应当指出，同一安全机制有时也可以用于实现不同的安全服务。

1.1.5 网络安全工作目的

安全工作的目的就是为了在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，完成以下任务：

(1) 使用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。

(2) 使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

(3) 使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

(4) 使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而确保信息的完整性。

(5) 使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

§1.2 网络安全体系结构

关于网络安全的体系结构的划分有很多种。我们下面介绍一种比较有代表性的体系结构划分。

1.2.1 物理安全

物理安全是指用一些装置和应用程序来保护计算机硬件和存储介质的安全。比如在计算机下面安装将计算机固定在桌子上的安全托盘、硬盘震动保护器等。下面详细地谈一下物理安全。

物理安全非常重要，它负责保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误、错误和各种计算机犯罪行为导致的破坏过程。它主要包括三个方面：

(1) 环境安全：对系统所在环境的安全保护，如区域保护和灾难保护。参见国家标准GB50173－93《电子计算机机房设计规范》、国标 GB2887－89《计算站场地技术条件》、GB9361－88《计算站场地安全要求》。

(2) 设备安全：主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

(3) 媒体安全：包括媒体数据的安全及媒体本身的安全。

显然，为保证信息网络系统的物理安全，除在网络规划和场地、环境等要求之外，还要防止系统信息在空间的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多，在理论和技术支持下的验证工作也证实这种截取距离在几百甚至可达千米的复原显示，给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间上的扩散，通常在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。这是重要的政策、军队、金融机构在兴建信息中心时的首要设置条件。

正常的防范措施主要在三个方面：

(1) 对主机房及重要信息存储、收发部门进行屏蔽处理，即建设一个具有高效屏蔽效能的屏蔽室，用它来安装运行的主要设备，以防止磁鼓、磁带与高辐射设备等的信号外泄。为提高屏蔽室的效能，在屏蔽室与外界的各项联系、连接中均要采取相应的隔离措施和设计，如信号线、电话线、空调、消防控制线，以及通风管道、门的开关等。

(2) 对本地网、局域网传输线路传导辐射的抑制。由于电缆传输辐射信息的不可避免性，现均采用了光缆传输的方式，大多数均在 Modem 出来的设备用光电转换接口，用光缆接出屏蔽室外进行传输。

(3) 对终端设备辐射的措施。终端机，尤其是 CRT 显示器，由于上万伏高压电子流的作用，辐射有极强的信号外泄，但又因终端分散使用不宜集中采用屏蔽室的办法来防止，故现在的要求除在订购设备上尽量选取低辐射产品外，目前主要采取主动式的干扰设备如干扰机来破坏对应信息的窃取，个别重要的首脑或集中的终端也可考虑采用有窗子的装饰性屏蔽室，这样虽降低了部分屏蔽效能，但可大大改善工作环境，使人感到在普通机房内一样工作。

1.2.2 网络安全

网络安全主要包括系统(主机、服务器)安全、网络运行安全、局域网和子网安全。

1. 内外网隔离及访问控制系统

在内部网与外部网之间，设置防火墙(包括分组过滤与应用代理)实现内外网的隔离

与访问控制是保护内部网安全的最主要、最有效、最经济的措施之一。防火墙技术可根据防范的方式和侧重点的不同分为很多种类型，但总体来讲有两大类较为常用：分组过滤、应用代理。

(1) 分组过滤(Packet Filtering)：作用在网络层和传输层，它根据分组包的源地址、目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。

(2) 应用代理(Application Proxy)：也叫应用网关(Application Gateway)，它作用在应用层，其特点是完全"阻隔"了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。实际中的应用网关通常由专用工作站实现。

无论何种类型防火墙，从总体上看，都应具有以下五大基本功能：

① 过滤进、出网络的数据；

② 管理进、出网络的访问行为；

③ 封堵某些禁止的业务；

④ 记录通过防火墙的信息内容和活动；

⑤ 对网络攻击的检测和告警。

应该强调的是，防火墙是整体安全防护体系的一个重要组成部分，而不是全部。因此必须将防火墙的安全保护融合到系统的整体安全策略中，才能实现真正的安全。

2. 内部网不同网络安全域的隔离及访问控制

在这里，防火墙被用来隔离内部网络的一个网段与另一个网段。这样，就能防止影响因一个网段的问题而穿过整个网络传播。针对某些网络，在某些情况下，它的一些局域网的某个网段比另一个网段更受信任，或者某个网段比另一个更敏感。而在它们之间设置防火墙就可以限制局部网络安全问题对全局网络造成的影响。

3. 网络安全检测

网络系统的安全性是网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节，如何最大限度地保证网络系统的安全，最有效的方法是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。

网络安全检测工具通常是一个网络安全性评估分析软件，其功能是用实践性的方法扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议补救措施和安全策略，达到增强网络安全性的目的。

4. 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能指出系统正被怎样地使用。对于确定是否有网络攻击的情况，审计信息对于确定问题和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累，并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

5. 网络反病毒

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，因此计算机病毒的防范是网络安全性建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消毒三种技术：

(1) 预防病毒技术：它通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制(如防病毒卡等)。

(2) 检测病毒技术：它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

(3) 消毒技术：它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测；在工作站上使用防病毒芯片和对网络目录及文件设置访问权限等。

6. 网络备份系统

备份系统为一个目的而存在：尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场地内高速度、大容量自动的数据存储、备份与恢复；场地外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。

一般的数据备份操作有三种：一是全盘备份，即将所有文件写入备份介质；二是增量备份，只备份那些上次备份之后更改过的文件，它是最有效的备份方法；三是差分备份，备份上次全盘备份之后更改过的所有文件，其优点是只需两组磁带就可恢复最后一次全盘备份的磁带和最后一次差分备份的磁带。在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到令一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。热备份的优点是投资大，但调用快，使用方便，在系统恢复中需要反复调试时更显优势。热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。冷备份弥补了热备份的一些不足，二者优势互补，相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

在进行备份的过程中，常使用备份软件，它一般应具有以下功能：

① 保证备份数据的完整性，并具有对备份介质的管理能力；

② 支持多种备份方式，可以定时自动备份，还可设置备份自动启动和停止日期；

③ 支持多种校验手段(如字节校验、CRC 循环冗余校验、快速磁带扫描)，以保证备份的正确性；

④ 提供联机数据备份功能；

⑤ 支持 RAID 容错技术和图像备份功能。

1.2.3 信息安全

Internet是信息的革命。在方便地享用信息的同时，也带来了安全方面的问题。由于Internet从建立开始就缺乏安全的总体构想和设计，而TCP/IP协议也是在可信环境下为网络互联专门设计的，同样缺乏安全措施的考虑，加上黑客的攻击及病毒的干扰，使得网络存在很多不安全因素，如口令猜测、地址欺骗、TCP盗用、业务否决、对域名系统和基础设施破坏、利用Web破坏数据库、社会工程、邮件炸弹、病毒携带等。

诸多的不安全让我们措手不及，害怕自己的信息被他人利用及信息漏失；担心自己的计算机系统遭到外界的破坏(收到大批电子邮件垃圾)；最迫切需要使用时计算机却出现了系统故障，什么事也干不了，浪费时间；存在计算机上的有关个人钱财、健康状况、购物习惯等个人隐私也有被偷窥的可能。

所以采取必要的措施和手段，来保护网络与信息的安全是非常必要的。所谓信息安全就是要保证数据的机密性、完整性、抗否认性和可用性。主要涉及到信息传输的安全、信息存储的安全以及对网络传输信息内容的审计三方面。

安全级别有四等：绝对可信网络安全、完全可信网络安全、可信网络安全、不可信网络安全。

安全的层次有四层：企业级安全、应用级安全、系统级安全、网络级安全。安全访问控制就是属于系统级安全。

网络上系统信息的安全包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密等等。

1. 鉴别

鉴别是对网络中的主体进行验证的过程，通常有三种方法验证主体身份。一是只有该主体了解的秘密，如口令、密钥；二是主体携带的物品，如智能卡和令牌卡；三是只有该主体具有的独一无二的特征或能力，如指纹、声音、视网膜或签字等。

(1) 口令机制：口令是相互约定的代码，只有用户和系统知道。口令有时由用户选择，有时由系统分配。通常情况下，用户先输入某种标志信息，比如用户名和ID号，然后系统询问用户口令，若口令与用户文件中的相匹配，用户即可进入访问。口令有多种，如一次性口令，系统生成一次性口令的清单，第一次时必须使用X，第二次时必须使用Y，第三次时用Z，这样一直下去；还有基于时间的口令，即访问使用的正确口令随时间变化，变化基于时间和一个秘密的用户密钥。这样口令每分钟都在改变，使其更加难以猜测。

(2) 智能卡：访问不但需要口令，也需要使用物理智能卡。在允许进入系统之前检查是否允许其接触系统。智能卡大小形如信用卡，一般由微处理器、存储器及输入、输出设施构成。微处理器可计算该卡的一个唯一数(ID)和其他数据的加密形式。ID保证卡的真实性，持卡人就可访问系统。为防止智能卡遗失或被窃，许多系统需要卡和身份识别码(PIN)同时使用。若仅有卡而不知PIN码，则不能进入系统。智能卡比传统的口令方法进行鉴别更好，但其携带不方便，且开户费用较高。

(3) 主体特征鉴别：利用个人特征进行鉴别的方式具有很高的安全性。目前已有的设备包括：视网膜扫描仪、声音验证设备、手型识别器。

2. 数据传输安全系统

1) 数据传输加密技术

数据传输加密技术的目的是对传输中的数据流加密,以防止通信线路上的窃听、泄漏、篡改和破坏。如果以加密实现的通信层次来区分,加密可以在通信的三个不同层次来实现,即:链路加密(位于 OSI 网络层以下的加密),节点加密,端到端加密(传输前对文件加密,位于 OSI 网络层以上的加密)。

一般常用的是链路加密和端到端加密这两种方式。链路加密侧重与在通信链路上而不考虑信源和信宿,保密信息通过各链路时采用不同的加密密钥提供安全保护。链路加密是面向节点的,对于网络高层主体是透明的,它对高层的协议信息(地址、检错、帧头帧尾)都加密,因此数据在传输中是密文的,但在中央节点必须解密得到路由信息。端到端加密则指信息由发送端自动加密,并进入 TCP/IP 数据包回封,然后作为不可阅读和不可识别的数据穿过互联网,当这些信息一旦到达目的地,将自动重组、解密,成为可读数据。端到端加密是面向网络高层主体的,它不对下层协议进行信息加密,协议信息以明文形式传输,用户数据在中央节点不需解密。

在传统上,有几种方法来加密数据流。在所有的加密算法中最简单的一种就是"换表算法",这种算法也能很好地达到加密的需要。

还有一种更好的加密算法,只有计算机可以做,就是字/字节循环移位和 XOR 操作。

一个好的加密算法可以定一个密码或密钥,并用它来加密明文,不同的密码或密钥产生不同的密文。这又分为两种方式:对称密钥算法和非对称密钥算法。将在第 6 章对这些内容作详细讨论。

2) 数据完整性鉴别技术

目前,对于动态传输的信息,许多协议确保信息完整性的方法大多是收错重传、丢弃后续包的办法,但黑客的攻击可以改变信息包内部的内容,所以应采取有效的措施来进行完整性控制。

(1) 报文鉴别:与数据链路层的 CRC 控制类似,将报文名字段(或域)使用一定的操作组成一个约束值,称为该报文的完整性检测向量 ICV(Integrated Check Vector)。然后将它与数据封装在一起进行加密,传输过程中由于侵入者不能对报文解密,所以也就不能同时修改数据并计算新的 ICV,这样,接收方收到数据后解密并计算 ICV,若与明文中的 ICV 不同,则认为此报文无效。

(2) 校验和:一个最简单易行的完整性控制方法是使用校验和,计算出该文件的校验和值并与上次计算出的值比较。若相等,说明文件没有改变;若不等,则说明文件可能被未察觉的行为改变了。校验和方式可以查错,但不能保护数据。

(3) 加密校验和:将文件分成小快,对每一块计算 CRC 校验值,然后再将这些 CRC 值加起来作为校验和。只要运用恰当的算法,这种完整性控制机制几乎无法攻破。但这种机制运算量大,并且昂贵,只适用于那些完整性要求保护极高的情况。

(4) 消息完整性编码 MIC(Message Integrity Code):使用简单单向散列函数计算消息的摘要,连同信息发送给接收方,接收方重新计算摘要,并进行比较验证信息在传输过程中的完整性。这种散列函数的特点是任何两个不同的输入不可能产生两个相同的输出。因此,一个被修改的文件不可能有同样的散列值。单向散列函数能够在不同的系统中高

效实现。

(5) 防抵赖技术:它包括对源和目的地双方的证明,常用方法是数字签名,数字签名采用一定的数据交换协议,使得通信双方能够满足两个条件:接收方能够鉴别发送方所宣称的身份,发送方以后不能否认它发送过数据这一事实。比如,通信的双方采用公钥体制,发方使用收方的公钥和自己的私钥加密的信息,只有收方凭借自己的私钥和发方的公钥解密之后才能读懂,而对于收方的回执也是同样道理。另外实现防抵赖的途径还有:采用可信第三方的权标、使用时戳、采用一个在线的第三方、数字签名与时戳相结合等。

鉴于为保障数据传输的安全,需采用数据传输加密技术、数据完整性鉴别技术及防抵赖技术。因此为节省投资、简化系统配置、便于管理、使用方便,有必要选取集成的安全保密技术措施及设备。这种设备应能够为大型网络系统的主机或重点服务器提供加密服务,为应用系统提供安全性强的数字签名和自动密钥分发功能,支持多种单向散列函数和校验码算法,以实现对数据完整性的鉴别。

3. 数据存储安全系统

在计算机信息系统中存储的信息主要包括纯粹的数据信息和各种功能文件信息两大类。对纯粹数据信息的安全保护,以数据库信息的保护最为典型。而对各种功能文件的保护,终端安全很重要。

数据库安全:对数据库系统所管理的数据和资源提供安全保护,一般包括以下几点:

(1) 物理完整性,即数据能够免于物理方面破坏的问题,如掉电、火灾等;

(2) 逻辑完整性,能够保持数据库的结构,如对一个字段的修改不至于影响其他字段;

(3)元素完整性,包括在每个元素中的数据是准确的;

(4) 数据的加密;

(5) 用户鉴别,确保每个用户被正确识别,避免非法用户入侵;

(6) 可获得性,指用户一般可访问数据库和所有授权访问的数据;

(7) 可审计性,能够追踪到谁访问过数据库。

要实现对数据库的安全保护,一种选择是安全数据库系统,即从系统的设计、实现、使用和管理等各个阶段都要遵循一套完整的系统安全策略;二是以现有数据库系统所提供的功能为基础,构建安全模块,旨在增强现有数据库系统的安全性。

终端安全:主要解决微机信息的安全保护问题,一般的安全功能如下。基于口令或(和)密码算法的身份验证,防止非法使用机器;自主和强制存取控制,防止非法访问文件;多级权限管理,防止越权操作;存储设备安全管理,防止非法软盘拷贝和硬盘启动;数据和程序代码加密存储,防止信息被窃;预防病毒,防止病毒侵袭;严格的审计跟踪,便于追查责任事故。

4. 信息内容审计系统

实时对进出内部网络的信息进行内容审计,以防止或追查可能的泄密行为。因此,为了满足国家保密法的要求,在某些重要或涉密网络,应该安装使用此系统。

1.2.4 网络安全管理

安全管理主要是管理和监控计算机设备的安全运转。

面对网络安全的脆弱性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，还必须花大力气加强网络的安全管理，因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面，而这又是计算机网络安全所必须考虑的基本问题，所以应引起各计算机网络应用部门领导的重视。

1. 网络安全管理原则

网络信息系统的安全管理主要基于三个原则。

1) 多人负责原则

每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。

以下各项是与安全有关的活动：

(1) 访问控制使用证件的发放与回收；

(2) 信息处理系统使用的媒介发放与回收；

(3) 处理保密信息；

(4) 硬件和软件的维护；

(5) 系统软件的设计、实现和修改；

(6) 重要程序和数据的删除和销毁等。

2) 任期有限原则

一般地讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

3) 职责分离原则

在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。

出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

(1) 计算机操作与计算机编程；

(2) 机密资料的接收和传送；

(3) 安全管理和系统管理；

(4) 应用程序和系统程序的编制；

(5) 访问证件的管理与其他工作；

(6) 计算机操作与信息处理系统使用媒介的保管等。

2. 网络安全管理的实现

信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制订相应的管理制度或采用相应的规范。具体工作是：

(1) 根据工作的重要程度，确定该系统的安全等级。

(2) 根据确定的安全等级，确定安全管理的范围。

(3) 制订相应的机房出入管理制度。对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理可采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记管理。