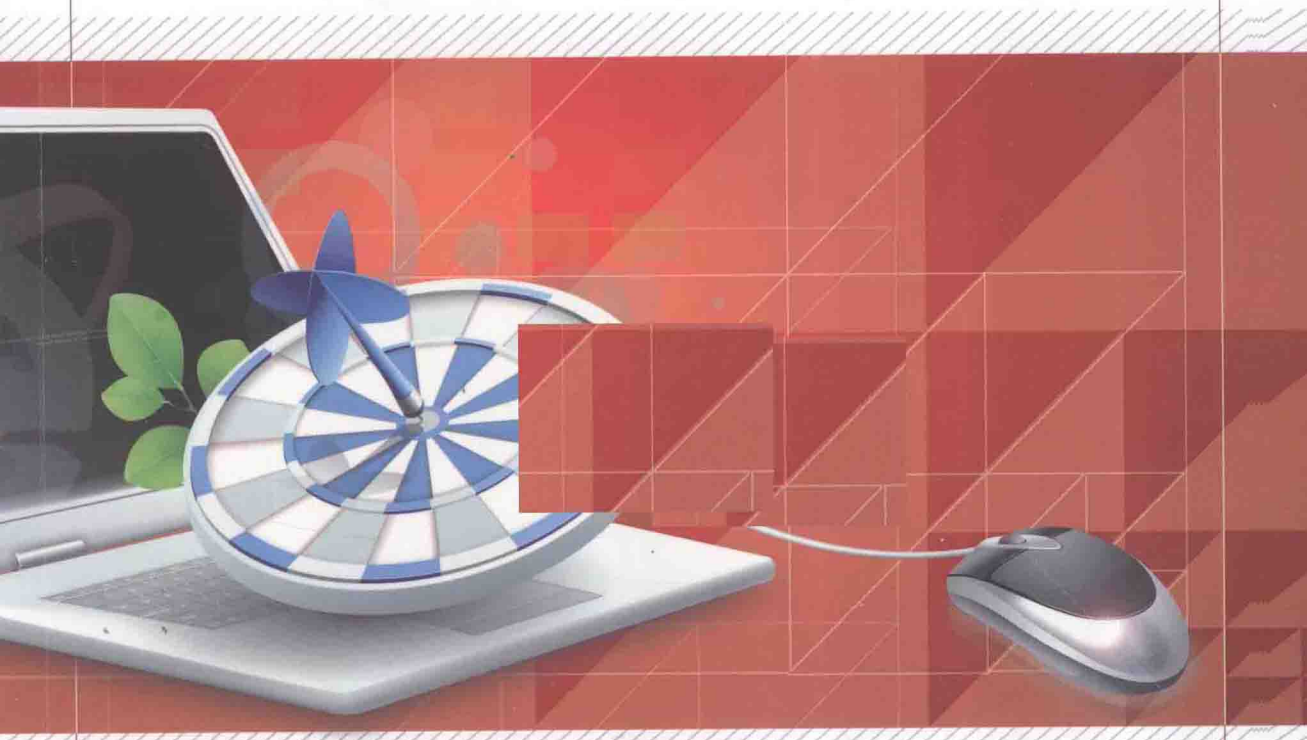
职业教育教学用书

计算机网络安全技术

◆ 汪双顶　杨剑涛　余 波　主编



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

职业教育教学用书

计算机网络安全技术

主　编　汪双顶　杨剑涛　余　波
副主编　龚正江　杨　霞　康世瑜
郑　娟

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

内 容 简 介

本书全面地介绍计算机网络安全领域的安全实施和安全防范技术。全书共分为 11 个项目，项目一介绍计算机网络安全的基本概念、内容和方法，随后的十个项目分别从网络安全技术在日常生活中实施的过程角度，针对日常使用网络过程的不同层面，对计算机网络安全的相关理论与方法进行了详细介绍；主要内容包括：排除常见网络故障，使用 360 软件保护客户端安全，保护 Windows 主机安全访问，保护 Windows 文件系统安全，保护网络设备控制台安全，保护交换机端口安全，实施虚拟局域网安全，实施网络广播风暴控制安全，实施访问控制列表安全，实施防火墙安全。

本书适用于职业类学校的学生、教师，可在实验室实施网络安全和防范技术；强化职业学校的学生锻炼安全技能，增强安全防范技术。

图书在版编目（CIP）数据

计算机网络安全技术 / 汪双顶，杨剑涛，余波主编. —北京：电子工业出版社，2015.3
职业教育教学用书

ISBN 978-7-121-20867-6

Ⅰ. ①计… Ⅱ. ①汪… ②杨… ③余… Ⅲ. ①计算机网络—安全技术—高等学校—教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 145184 号

策划编辑：施玉新
责任编辑：郝黎明
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
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
开　　本：787×1092　1/16　印张：9　字数：230.4 千字
版　　次：2015 年 3 月第 1 版
印　　次：2015 年 3 月第 1 次印刷
定　　价：26.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

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。
服务热线：（010）88258888。

前　言

随着网络新技术的不断发展，社会经济建设与发展越来越依赖于计算机网络，与此同时，网络安全对国民经济的威胁、甚至对地区和国家的威胁也日益严重。计算机网络给人们带来便利的同时，也带来了保证信息安全的巨大挑战。如何使人们在日常生活和工作过程中，信息不受病毒的感染，保持数据的完整、安全；计算机不被黑客侵入，保障网络的安全；如何保证计算机网络不间断地工作，并提供正常的服务……这些都是各个组织信息化建设必须考虑的重要问题。因此，加快培养网络安全方面的应用型人才，广泛普及网络安全知识和掌握网络安全技术突显重要和迫在眉睫。

1．关于本教材开发思想

本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范，并通过研究实践而形成的适合职业教育改革和发展特点的教程。与国内已出版的同类书籍相比，本书更注重以能力为中心，以培养应用型和技能型人才为根本。通过认识、实践、总结和提高这样一个认知过程，精心组织学习内容，图文并茂，深入浅出，全面适应社会发展需要，符合职业教育教学改革规律及发展趋势，具有独创性、层次性、先进性和实用性。

2．关于本教材内容

全书以生活中各种网络安全需求和实际网络安全事件为主线，以生活和工作中遇到的网络安全问题的解决能力为目标，加强网络安全技术，强化网络安全工作技能锻炼，满足职业学校学生网络安全实践技能的教学需要。

区别于传统的网络安全技术的教材，本课程针对职业学校的学生学习习惯和学习要求，本着“理论知识以够用为度，重在实践应用”的原则，以“理论+工具+分析+实施”为主要形式编写，依托终端设备安全、用户账户安全、攻击和防御等网络安全的技术，分别从网络安全技术在日常生活中实施的角度，针对日常使用网络过程不同层面，对计算机网络安全的相关理论与方法进行了详细介绍。主要内容包括：使用 360 软件保护客户端安全、保护 Windows 主机安全访问，保护 Windows 文件系统安全，保护网络设备控制台安全，保护交换机端口安全，实施虚拟局域网安全，实施网络广播风暴控制安全，实施访问控制列表安全，实施防火墙安全以及网络故障排除技术。

全书旨在加深学生对未来工作中遇到网络安全事件和面对网络安全故障时，增强经验的积累，培养学生对网络安全的兴趣，帮助学生在学校期间就建立全面的网络安全观，培养使用网络的安全习惯，加深对所涉及的网络安全技术、理论的理解，提高学生网络安全事件处理的动手能力、分析网络安全问题和解决网络安全问题的能力。

3．关于课程资源、课程环境

本书作为计算机网络及其相关专业的核心课程，纳入课程的教学体系中。全书在使用的过程中，根据各所学校教学计划安排要求，以 96 学时左右（6 节×16 周）作为建议教学比重和学时。

所有网络安全实训操作，都以日常生活中网络安全应用需求为主线，串接网络安全技术和网络安全知识；以解决网络安全过程作为核心，帮助学生加强对抽象计算机网络安全理论的理解。

为顺利实施本教程，每个课程学习者除需要对网络技术有学习的热情之外，还需要具备基本的计算机、网络基础知识。这些基础知识为学习者提供一个良好的脚手架，帮助理解本书中网络安全技术的原理，为网络安全技术的进阶提供良好帮助。

为有效保证本课程有效实施，课程教学资源长期提供，研发队伍为本课程专门建设一个百度云空间，集中存放本书涉及课件、网络安全工具、小程序等资源，访问百度云地址为：http://pan.baidu.com/s/1jGzGTM2（区分大小写）。

此外，为更好地实施课程中部分单元内容，还需要为本课程提供一个可实施交换、路由技术的网络安全环境，包括二层交换机设备、三层交换机设备、模块化路由器设备、防火墙设备、测试计算机和若干双绞线（或制作工具）。

4．关于教材开发队伍

本书第一作者汪双顶先生，为北京师范大学信息科学学院硕士。汪双顶先生先后有在院校、网络公司，以及产品生产厂商等不同环境的工作经历，这为本书把网络安全项目和课堂中网络安全知识，以及工作中岗位技能有机融合在一起，提供了良好的根基，有效地保证了本书所倡导的“基于工作过程”的计算机网络专业课程教学思想的实施。

此外，在本书的编写过程中，汪双顶、杨剑涛、余波担任主编，龚正江、杨霞、康世瑜、郑娟担任副主编，冯理明、黄剑文、王志平、沈海亮、姚正刚、熊玉金等参与编写，以及来自企业的技术工程师、产品经理等给予大力支持。他们积累了多年来自教学和工程一线的工作经验，都为本书的真实性、专业性以及方便在学校教学、实施给予了有力的支持。本书规划、编辑过程历经近两年多的时间，前后经过多轮的修订，其改革力度较大，远远超过前期策划者原先的估计，加之课程组文字水平有限，错漏之处敬请广大读者指正。

编　者

目　录

项目一　计算机网络安全概述

核心技术

- 解决安全隐患的方案

任务目标

- 了解网络安全威胁
- 熟悉网络安全隐患
- 掌握网络安全需求

随着科技的不断发展，网络已走进千家万户，到目前为止，互联网已经覆盖了 175 个国家和地区的数千万台计算机，用户数量超过一亿。网络给人们带来前所未有的便捷，人们利用网络可以开展工作，基于互联网的娱乐，购物，互联网的应用也变得越来越广泛。

今天人们对网络的需求，已经不再是单一的联网需求，而更希望在实现互联互通的网络的基础上实现多业务的融合，如语音、视频等。互联网以其开放性和包容性，融合了传统行业的所有服务。但网络的开放性和自由性，也产生了私有信息和保密数据被破坏或侵犯的可能性，这样就对网络提出了更高的要求，安全问题从而显现出来。

针对重要信息资源和网络基础设施的入侵行为和企图入侵行为的数量仍在持续不断增加，网络攻击与入侵行为对国家安全、经济和社会生活造成了极大的威胁。计算机病毒不断地通过网络产生和传播，计算机网络被不断地非法入侵，重要情报、资料被窃取，甚至造成网络系统的瘫痪等，诸如此类的事件已给政府及企业造成了巨大的损失，甚至危害到国家的安全。网络安全已成为世界各国当今共同关注的焦点，由此可见，网络安全的重要性不言而喻。

1.1 网络安全的概念

网络安全可以用一个通俗易懂的例子来说明，问问自己为何要给家里的门上锁？那是因为不愿意有人随意到家里偷东西。网络安全就是为了阻止未授权者的入侵、偷窃或对资产的破坏，这里的“资产”在网络中指数据，保护网络中数据的安全是实施网络安全最为重要的安全措施之一，从本质上来讲，网络安全就是保护网络上的信息安全，如图 1-1 所示。

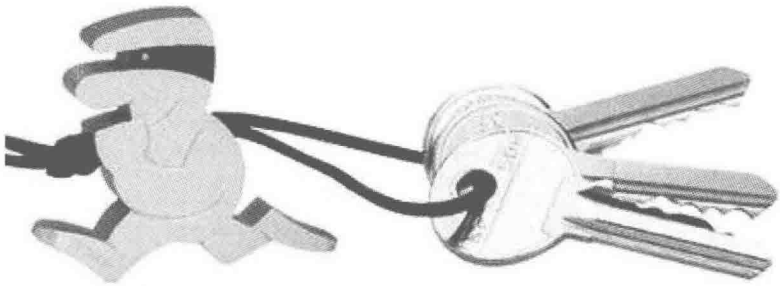


图 1-1 网络安全

针对网络安全的定义，业界给出的普遍答案是：网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。通过实施网络安全技术，保护网络系统的硬件、软件及其系统中的数据不受偶然或者恶意的原因而遭到破坏、更改、泄露，保证系统连续可靠、正常地运行，保障网络服务不中断。网络安全是对安全设施、策略和处理方法的实现，用以阻止对网络资源的未授权访问、更改或者是对资源、数据的破坏。

广义来说，凡是涉及网络上信息的保密性、完整性、真实性和可控性的相关技术和理论，都是网络安全研究的领域。除此之外，网络安全还是围绕安全策略进行完善的一个持续不断的过程，通过实施保护、监视、测试和提高过程，不断循环过程，如图 1-2 所示。

（1）保护：具体实施网络设备的部署与配置，如防火墙、IDS 等设备的配置。

（2）监视：在网络设备部署与配置之后，最重要的工作是监控网络设备的运行情况。

（3）测试：整体网络环境，包括设备的测试，测试网络设备部署和配置的效果。

（4）提高：检测到网络中有哪些问题，及时调整，使其在网络环境中发挥更好的性能。

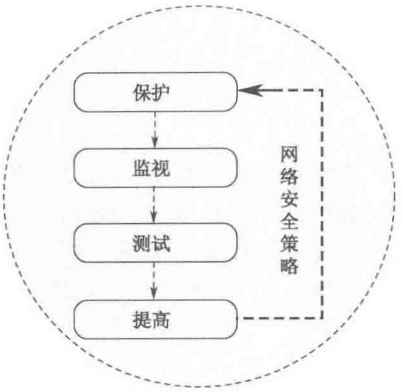


图 1-2　网络安全是一个持续不断的过程

1.2　网络安全现状

据美国联邦调查局统计，美国每年因网络安全造成的损失高达 75 亿美元。据美国金融时报报道，世界上平均每 20 分钟就发生一起入侵互联网的计算机网络安全事件发生，遍布世界的 1/3 的防火墙都被黑客攻破过。

近年来，计算机犯罪案件也急剧上升，计算机犯罪已经成为普遍的国际性问题。据美国联邦调查局的报告显示，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额为 45000 美元，每年计算机犯罪造成的经济损失高达 50 亿美元。

而我国的情况也不容乐观，政府、证券，特别是金融机构的计算机网络相继遭到多次攻击。公安机关受理各类信息网络违法犯罪案件也逐年增加，尤其以电子邮件、特洛伊木马、文件共享，盗取银行账号等一系列的黑客与病毒问题愈演愈烈。

常见的计算机网络安全主要面临了哪些问题？如图 1-3 所示的图形，分别从时间的发展维度，由低到高列举了常见的计算机网络安全时间，分别是口令猜测、自我复制代码、口令破解、后门、关闭审计、会话劫持、清除痕迹、嗅探器等。

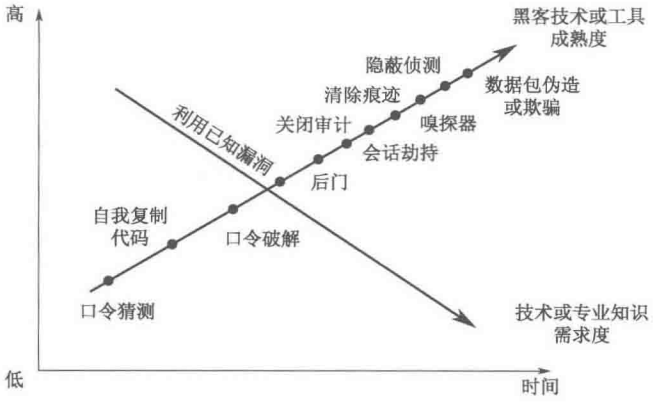


图 1-3　网络安全面临的问题

网络安全的已经越来越发展成为社会关注的焦点问题：如何保护账户的安全？如何保护网银的安全？如何保护网络免受攻击？如何防范等安全事件，这些都是摆在网络工程师面前的一个难题。

1.3 网络安全威胁

早期的网络安全大多是局限于各种病毒的防护。随着计算机网络的发展，除了病毒，人们更多的是防护木马入侵、漏洞扫描、DDoS 等新型攻击手段层出不穷。威胁网络安全的因素是多方面，目前还没有一个统一的方法，对所有的网络安全行为进行区分和有效的防护。

针对网络安全威胁，常见的产生网络攻击的事件主要分为以下几类。

1．中断威胁

中断威胁破坏安全事件，主要是网络攻击者阻断发送端到接收端之间的通路，使数据无法从发送端发往接收端，工作流程如图 1-4 和图 1-5 所示。

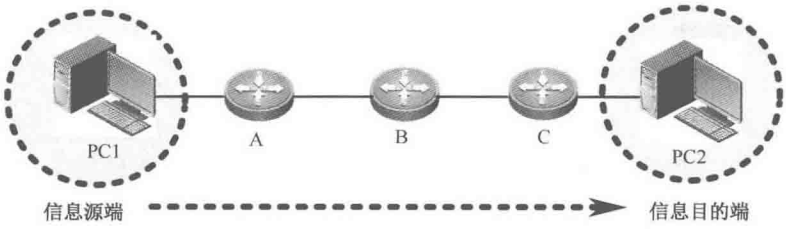


图 1-4 正常的信息流

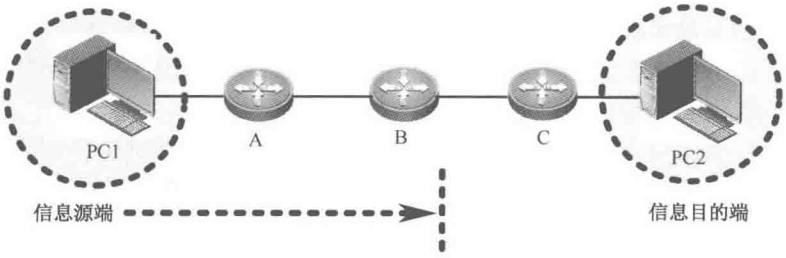


图 1-5 中断威胁

造成中断威胁的原因主要有以下几个方面。

（1）攻击者攻击破坏信息源端与信息目的端之间的连通性，造成网络链路中断。

（2）信息目的端无法处理来自信息源端的数据，造成服务无法响应。

（3）系统崩溃：物理上破坏网络系统或者设备组件，如破坏磁盘系统，造成整个磁盘的损坏及文件系统的瘫痪等。

在目前网络当中，最典型的中断威胁是拒绝服务攻击（DoS）。

2．截获威胁

截获威胁是指非授权者通过网络攻击手段侵入系统，使信息在传输过程中丢失或者泄露的一种威胁，称为截获威胁，截获威胁破坏了数据保密性原则，如图 1-6 所示。

常见的使用截获威胁的原理，产生攻击的包括利用电磁泄漏或者窃听等方式，截获保密信息；通过对数据的各种分析，得到有用的信息，如用户口令、账号信息。

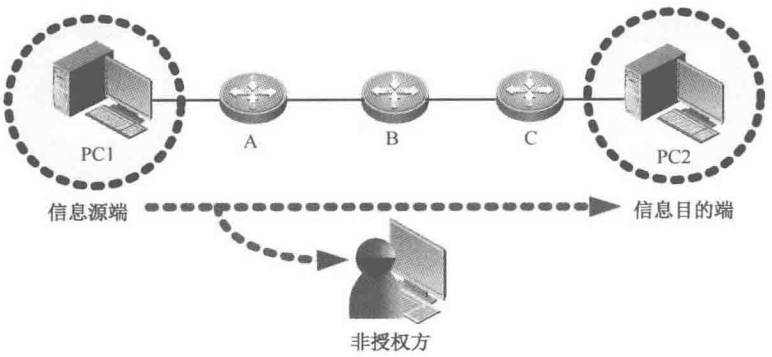


图 1-6　截获威胁

3．篡改威胁

所谓篡改威胁，是指以非法手段获得信息的管理权，通过以未授权的方式，对目标计算机进行数据的创建、修改、删除和重放等操作，使数据的完整性遭到破坏，篡改威胁工作原理如图 1-7 所示。

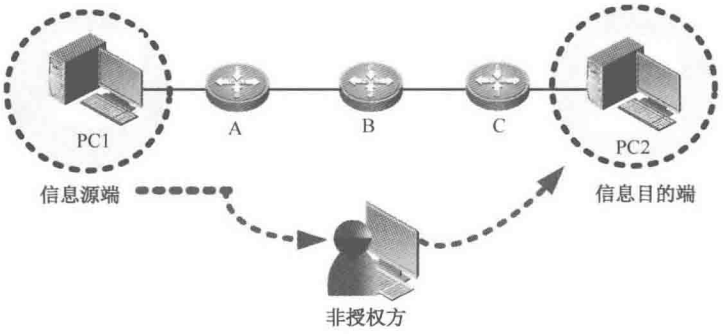


图 1-7　篡改威胁

篡改威胁攻击的手段主要包括以下两个方面。

（1）改变数据文件，如修改信件内容。

（2）改变数据的程序代码，使程序不能正确的执行。

4．伪造威胁

伪造威胁是指一个非授权者将伪造的数据信息插入数据中，破坏数据的真实性与完整性，从而盗取目的端信息的行为，伪造威胁如图 1-8 所示。为了避免数据被非授权者篡改，业界开发了一种解决方案：数字签名。

所谓数字签名，就是附加在数据单元上的一些数据或对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者，用以确认数据单元的来源和数据单元的完整性，并保护数据，防止进行数据伪造。

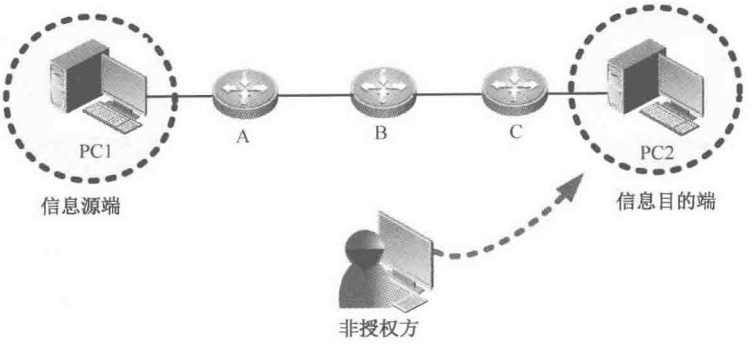


图 1-8 伪造威胁

1.4 网络安全隐患的范围

网络安全的隐患是指计算机或其他通信设备利用网络进行交互时可能会受到的窃听、攻击或破坏，它是指具有侵犯系统安全或危害系统资源的潜在的环境、条件或事件。计算机网络和分布式系统很容易受到来自非法入侵者和合法用户的威胁。

网络安全隐患包括的范围比较广，如自然火灾、意外事故、人为行为（如使用不当、安全意识差等）、黑客行为、内部泄密、外部泄密、信息丢失、电子监听（信息流量分析、信息窃取等）和信息战等。所以，对网络安全隐患的分类方法也比较多，如根据威胁对象可分为对网络数据的威胁和对网络设备的威胁；根据来源可分为内部威胁和外部威胁。

网络安全隐患的来源一般可分为以下几类。

（1）非人为或自然力造成的硬件故障、电源故障、软件错误、火灾、水灾、风暴和工业事故等。

（2）人为但属于操作人员无意的失误造成的数据丢失或损坏。

（3）来自企业网络外部和内部人员的恶意攻击和破坏。

其中安全隐患最大的是第三类。

网络安全外部威胁主要来自一些有意或无意的对网络的非法访问，并造成了网络有形或无形的损失，其中的黑客就是最典型的代表。

还有一种网络威胁来自企业的网络系统内部，这类人熟悉网络的结构和系统的操作步骤，并拥有合法的操作权限。中国首例“黑客”操纵股价案例便是网络安全隐患中策略失误和内部威胁的典型实例。

1.5 网络安全隐患的原因

影响计算机网络安全的因素很多，有些是人为蓄意的，有些是无意造成的。归纳一下，产生网络安全的原因主要有以下几个方面。

（1）网络设计问题。

由于网络设计的问题导致网络流量据增，造成终端执行各种服务缓慢。典型的案例是由于公司内二层设备设计导致广播风暴的问题。

（2）网络设备问题。

在构建互联网络中，每台设备都有其特有的功能。例如，路由器和防火墙在某些功能上起到的作用一样，如访问控制列表技术（Access Control List，ACL）。但路由器通过 ACL 来实现对网络的访问控制，安全效果及性能不如防火墙；对于一个安全性需求很高的网络来说，采用路由器 ACL 来过滤流量，性能上得不到保证，更重要的是网络黑客利用各种手段来攻击路由器，使路由器瘫痪，不但起不到过滤 IP 的功能，更影响了网络的互通。

（3）人为无意失误。

此类失误多体现在管理员安全配置不当，终端用户安全意识不强，用户口令过于简单等因素带来的安全隐患。

（4）人为恶意攻击。

人为恶意攻击是网络安全最大的威胁。此类攻击指攻击者通过黑客工具，对目标网络进行扫描、侵入、破坏的一种举动，恶意攻击对网络性能，数据的保密性、完整性均都受到影响，并导致机密数据的泄露，给企业造成损失。

（5）软件漏洞。

由于软件程序开发的复杂性和编程的多样性，应用在网络系统中的软件，都有意无意会留下一些安全漏洞，黑客利用这些漏洞的缺陷，侵入网络中计算机，危害被攻击者的网络及数据。如 Microsoft 公司每月都在对 Windows 系列操作系统进行补丁的更新、升级，目的是修补其漏洞，避免黑客利用漏洞进行攻击。

（6）病毒威胁。

计算机病毒是一种小程序，能够自我复制，会将病毒代码依附在程序上，通过执行，伺机传播病毒程序，会进行各种破坏活动，影响计算机的使用。

1.6　网络安全需求

目前企事业单位内部网络可能所受到的攻击包括黑客入侵，内部信息泄露，不良信息的进入内网等方式。计算机网络安全的需求，大体上可分为保密性、完整性、可控行、不可否认性、可存活性、真实性、实用性、占有性。

（1）机密性（Confidentiality）。

对数据进行加密，防止非授权者接触秘密信息，破译信息。一般采用对信息的加密、对信息划分等级、分配访问数据的权限等方式，实现数据的保密性。

（2）完整性（Integrity）。

完整性是指数据在传输过程中不被篡改或者即使被篡改，接收端能通过数字签名的方式发现数据的变化，从而避免接收到错误或者是有危害的信息。

（3）可用性（Availability）。

可用性是指对信息可被合法的用户访问。可用性与保密性不但有一定的关联，还存在着矛盾性，这就是人们常说的平衡业务需求与安全性需求规则。

（4）可控性（Controllability）。

可控性是指对信息的内容及传播具有控制能力与控制权限。

（5）不可否认性（Non-repudiation）。

不可否认性是指发送数据者无法否认其发出的数据与信息，接收数据者无法否认已经接收的信息。不可否认性的举措主要是通过数字签名、第三方认证等技术实现。

（6）可存活性（Survivability）。

可存活性是指计算机系统在面对各种攻击或者错误情况下，继续提供核心任务的能力。

（7）真实性（Authenticity）。

数据信息的真实性是指信息的可信程度，主要是指信息的完整性、准确性和发送者与接受者身份的确认。

（8）实用性（Utility）。

信息的实用性是指数据加密用的密钥，不可被攻击者盗用或者泄密，否则就失去了信息的实用性。

（9）占有性（Possession）。

占有性是指磁盘、存储介质等信息载体被盗用，从而导致对信息占有的丧失。

1.7 常见解决安全隐患的方案

计算机网络最早出现在军事网，在它诞生之后的几十年间，主要用于在各科研机构的研究人员之间传送电子邮件，以及共同合作的职员间共享打印机。早期的计算机网络应用得非常简单，在当时的环境下，网络的安全性未能引起人们足够的关注。

随着信息技术的迅猛发展，特别是进入 21 世纪，网络正在以惊人的速度改变着人们的工作效率和生活方式，从各类机构到个人用户都将越来越多地通过各种网络处理工作、学习、生活方方面面的事情，网络也将以它快速、便利的特点给社会、个人带来了前所未有的高效速度，所有这一切正是得益于互联网络的开放性和匿名性的特征。

在此背景下发展起来的园区网络，由于其开放性和匿名性的特征，不可避免地存在着各种各样的安全隐患，若不解决这一系列的安全隐患，势必对园区网络的应用和发展，以及网络用户的利益造成很大的影响。为了防止来自各方面的园区网络安全威胁的发生，除进行宣传教育外，最主要的就是制定一个严格的安全策略，这也是网络安全中的核心和关键。

但是由于我国的信息安全技术起步晚，整体基础薄弱，特别是信息安全的基础设施和基础部件几乎全部依赖国外技术。所以，我国的网络安全产品，总的来说是自主开发少，软硬件技术受制于人。

近几年来，我国的信息技术得到了迅猛的发展，国家性的一些关键部门，如银行和电信等，很多都采用了国外的信息产品，特别是操作系统、数据库和骨干网络设备。这些部门要么采用国外的安全产品，要么就根本不采用任何安全措施，这些都给国家安全和人们的日常生活留下了严重的安全隐患。

可喜的是，近一两年来，我国网络信息安全领域也得到了迅猛的发展，除了专注于安全产品研发的公司外，国产化的网络设备供应商也越来越重视新产品安全功能的应用。锐捷网络公司也紧跟应用趋势，在新产品系列中都注重了网络安全的应用，可以通过交换机端口安全、配置访问控制列表 ACL、在防火墙实现包过滤等技术来实现一套可行的园区网安全解决方案。

1.8 常见网络包分析工具软件介绍

1. 网络包分析工具软件的概念

当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口

设置在监听模式，便可以将网上传输的、源源不断的信息截获。网络包分析工具软件的主要作用是尝试捕获网络包，并尝试显示包的尽可能详细的情况。可以认为网络包分析工具软件是一个用户检查网络数据报文的设备，就像用电压表测量电路电压。

该项技术被广泛地应用于网络故障诊断、协议分析、应用性能分析和网络安全保障等各个领域。

2．Sniffer 网络包分析工具软件介绍

Sniffer，中文可以翻译为嗅探器，是一种基于被动监听原理的网络分析方式。使用这种技术方式，可以监视网络的状态、数据流动情况以及网络上传输的信息，如图 1-9 所示。

Sniffer 网络包分析工具软件是一个网络故障、性能和安全管理的有力工具，它能够自动地帮助网络专业人员维护网络，查找故障，极大地简化了发现和解决网络问题的过程，广泛适用于 Ethernet、Fast Ethernet、Token Ring、Switched LANs、FDDI、X.25、DDN、Frame Relay、ISDN、ATM 和 Gigabits 等网络。

图 1-9　Sniffer 网络包分析工具软件

3．Ethereal 网络包分析工具软件介绍

网络包分析工具软件 Ethereal 是一款开源网络数据包分析软件。数据包分析软件会抓取网络中的数据包，并试图逐条详细地显示数据包数据。用户通过 Ethereal，同时将网卡插入混合模式，可以查看到网络中发送的所有通信流量。

Ethereal 是一款抓包软件，比较易用，在平常可以利用它抓包，分析协议或者监控网络，是一个比较好的工具，应用于故障修复、分析、软件和协议开发以及教育领域，如图 1-10 所示。

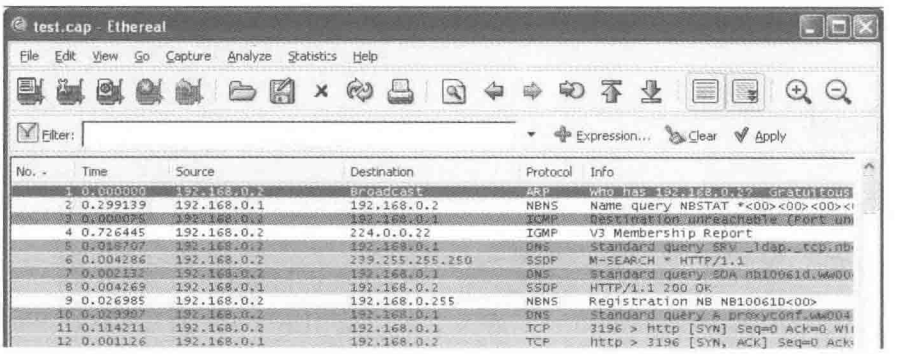


图 1-10　Ethereal 网络包分析工具软件