网络安全实用丛书

网络安全技术实践与代码详解

牛冠杰　笋大伟　李晨旸　徐颖娜　王　倩　魏小康　编著

人 民 邮 电 出 版 社

北　京

图书在版编目（CIP）数据

网络安全技术实践与代码详解/牛冠杰等编著．—北京：人民邮电出版社，2007.8
（网络安全实用丛书）
ISBN 978-7-115-16287-8

Ⅰ．网… Ⅱ．牛… 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（2007）第 074688 号

内 容 提 要

本书的特色是网络安全理论知识与实例代码完美的结合，使读者不仅可以从理论深度上对网络安全有宏观的认识，而且可以根据实例代码对网络安全措施有更直观的把握。

本书主要分为 3 个部分，包括网络安全基础；网络攻击与防范；Web 安全及 Web 安全评估。网络安全基础部分讲解了网络安全的基础理论、TCP/IP 协议以及代码的实现，使读者初步了解网络安全并掌握网络安全编程技术。网络攻击与防范部分从攻与防两个角度讲解网络安全技术，包括加密与解密、木马、DoS 攻击、缓冲区溢出攻击、网络嗅探、网络扫描、防火墙、入侵检测等技术的原理与代码讲解。Web 安全与 Web 安全评估部分讲解了 Web 领域的攻防技术和 Web 安全性评估技术，提高读者对 Web 领域的安全意识。

本书可作为网络安全工程师、网络管理员等信息与网络安全领域从业人员学习、研究及探讨安全理论知识与实例代码的阅读参考用书。同时本书也可作为大专院校计算机类、网络类、通信类、信息安全类等专业高年级本科生和研究生学习网络安全的参考书。

网络安全实用丛书

网络安全技术实践与代码详解

- 编　　著　牛冠杰　笋大伟　李晨旸　徐颖娜　王　倩　魏小康
  责任编辑　刘　洋
- 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
  邮编　100061　　电子函件　315@ptpress.com.cn
  网址　http://www.ptpress.com.cn
  北京隆昌伟业印刷有限公司印刷
  新华书店总店北京发行所经销
- 开本：787×1092　1/16
  印张：22.5
  字数：549 千字　　2007 年 8 月第 1 版
  印数：1 – 4 000 册　　2007 年 8 月北京第 1 次印刷

ISBN 978-7-115-16287-8/TN

定价：41.00 元

读者服务热线：(010)67129258　印装质量热线：(010)67129223

前　言

n Foreword

国际数据公司（IDC）在一项研究中透露，预计到 2007 年，计算机安全软件市场规模将增长到数百亿美元，从事防范计算机网络入侵和检测企业网络薄弱环节的专业公司数量将迅速增加。2006 年，网络蠕虫和病毒已导致全球经济损失超过 120 亿美元。从目前来看，最需要网络安全支持的是中小企业。由于缺乏资源和专业知识，它们最容易受到黑客与病毒的攻击。在网络安全防护相对发达的美国，仅有 35%的中小企业拥有防火墙，而在中国这个比例就更不容乐观。但是 IT 网络安全市场发展前景广阔，尤以亚洲市场增长最为迅猛，而引领亚洲 IT 网络安全市场高速发展的无疑将是中国。

本书编写的目的

网络安全工程师是前景普遍看好的一个新兴职业，当前社会缺口很大，但针对网络安全工程师的图书暂时不多。本书是从专业学习和职业需求的角度出发来进行内容组织和安排的，非常具有针对性。如果想做好网络安全相关工作，必先了解网络上存在哪些威胁和攻击，以及这些攻击的原理和特点，从而才能针对攻击的特性做好防御工作。

对于很多希望学习网络安全技术的人已经具备了一定的网络安全知识基础，对计算机网络与信息安全的概念和整体架构有了比较全面的了解，但在具体工程实现上又是零起点。而目前市面上大部分书是从宏观概念上讲述网络安全，使读者在整体上了解了网络安全工作，但更多的读者是想根据实例代码从具体细节上掌握网络安全技术。

本书的特点是不仅讲述了网络安全技术的原理和特点，而且针对典型的网络安全应用实例代码进行详细讲解与分析，可以使读者从项目工程角度理解掌握网络安全技术。并根据不同的网络攻击提出对应的防御措施，从而使网络安全工程师和相关研究人员可以有的放矢，做到知己知彼。

本书的主要内容

本书共分为 3 个部分。第 1 部分主要讲解了网络安全的基础理论和编程知识。从网络安全概述讲起，全面介绍网络安全概念和目标、网络安全措施、网络安全策略、网络安全技术的发展。然后讲解了 TCP/IP 协议及代码实现。TCP/IP 协议是 Internet 上使用最广泛的协议，

众多网络安全技术是基于 TCP/IP 协议上产生的。本部分包括 TCP/IP 协议简介、Windows 网络编程基础，并具体分析了 Ping、Traceroute、TCP 通信、UDP 通信的原理及代码实现。

第 2 部分主要讲解了网络攻击与防范技术。包括加密与解密、网络攻击、网络嗅探、网络扫描、网络防御等。其中加密与解密具体分析了 DES 算法、RSA 算法、MD5 算法。网络攻击具体分析了木马、DoS 攻击、缓冲区溢出攻击的原理与代码实现。网络嗅探具体分析了基于原始套接字嗅探实例和基于 Winpcap 嗅探实例的原理与代码实现，并介绍了专业级嗅探工具 Sniffer Pro 的使用方法。网络扫描具体分析了端口扫描、操作系统探测、活动主机探测、远程主机 NetBIOS 探测、伪 IP 干扰的原理与代码实现，并介绍了专业级扫描器 X-Scan 的使用方法。网络防御则具体分析了网络防火墙与入侵检测的原理及代码实现。

第 3 部分主要讲解了 Web 安全与 Web 安全评估技术。Web 安全包括认证的威胁、授权的威胁、客户端攻击的威胁、命令执行的威胁、信息暴露的威胁、逻辑攻击等。Web 安全性评估包括 Nikto 代码解析、Paros Proxy 工具以及其他评估工具的简介。

本书的阅读建议

本书以实例代码为特色，若读者能结合网络安全理论动手操作书中安排的每一个实例，必定能获得很快的提高。

网络安全的编程与具体的操作系统密切相关，作者主要讲解了 Windows 平台上的安全编程技术，开发环境为 VC6 和 VC7。另外，一些使用原始套接字技术的程序必须运行在 Windows XP SP2 版本以下。读者可以结合实例学习 Linux 系统下的安全编程技术，这样就会对网络安全技术有一个整体的把握。

说明：书中所有实例的完整代码均可到人民邮电出版社的网站上下载。下载网址为：www.ptpress.com.cn。

本书声明

需要（声明）的是，作者编写本书的目的是希望帮助读者全面了解网络安全方面的基本技术，以建立起安全方面的防范意识，绝不是为怀有不良动机的人提供支持，也不承担因技术被滥用而产生的连带责任。

本书在编写过程中参考了互联网上公布的一些相关资料，由于互联网上的资料很多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。

本书的第 1、2、3、4、5、6 章由牛冠杰编写，第 7 章由李晨旸编写，第 8、9 章由笪大伟编写。校验工作由徐颖娜、王倩完成。

由于作者水平有限，书中难免有疏漏和错误之处，希望读者批评指正，以期再版时修订。

欢迎读者对人民邮电出版社的图书出版工作提出宝贵的意见与建议。

编辑信箱：liuyang@ptpress.com.cn。

目 录

nCONTENTS

第 1 章
网络安全概述

CHAPTER 1

在进行网络安全应用实例分析之前，本章将使读者对网络安全有宏观上的认识，这样才能更加深刻理解网络安全的精髓。在学习了本章后，读者能够掌握以下几点内容。

- 熟悉网络安全基础理论及重要性；
- 熟悉网络安全的目标及基础架构；
- 熟悉网络安全的防御措施和策略；
- 熟悉网络安全的历史及发展趋势。

1.1 网络安全简介

1.1.1 网络安全概念

什么是网络安全？狭义上的网络安全是指计算机及其网络系统资源和信息资源不受网络上人为有害因素的威胁和侵害，即网络防御措施。其表现形式有杀毒软件、网络防火墙、VPN、IDS 等安全措施。但网络攻击技术不应该是网络安全的对立面，而应包括在网络安全之中，而且是最重要的环节。知己知彼，百战不殆。首先必须对网络攻击技术有深刻的了解，才能做好网络安全工作。因此，广义地讲，凡是涉及计算机网络上信息的保密性、完整性、可用性、真实性的理论和技术都属于网络安全的领域。如图 1-1 所示为广义上的网络安全体系的架构。

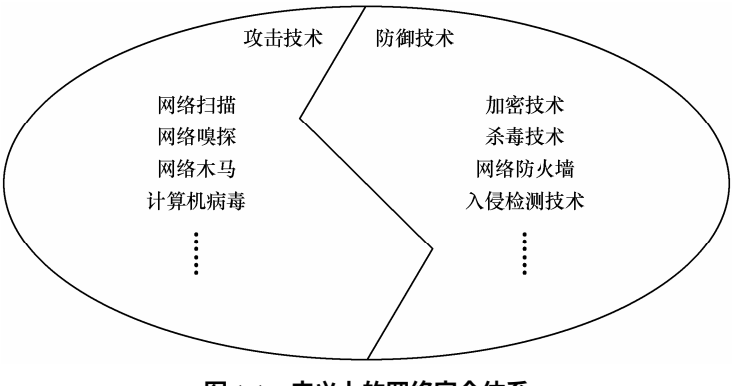

图 1-1　广义上的网络安全体系

1.1.2 网络安全脆弱性与重要性

随着计算机和网络广泛应用，网络安全的重要性突显出来。军事上，现代战争是高科技与信息化的战争，计算机和网络经常成为敌对势力与不法分子的攻击目标。随着计算机网络由最初军事上的应用扩展到民用上以后，越来越多的人开始接触计算机网络，与此同时，由于操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全方面的不足。日益增多的计算机犯罪使得网络安全成为各种网络应用开展应该考虑的首要问题。随着网络的进一步普及和网络技术的发展，计算机黑客的网络攻击技术和手段也在不断提高和发展。每年由于计算机网络犯罪造成了巨大的损失，所以在网络应用中不可能不对数据安全问题加以特殊的重视。

网络安全问题与计算机和网络的脆弱性密切相关，其脆弱性主要体现在以下几点。

（1）人为操作失误。

如由于操作员对其安全配置不当造成的安全漏洞；用户安全意识不强；用户口令选择不慎；用户将自己的账号随意转借他人或与别人共享等都会给网络安全带来威胁。

（2）操作系统。

操作系统结构体制本身不可避免地有其漏洞。例如，可以远程创建和激活进程；一般操作系统都提供远程过程调用（RPC）服务，而提供的安全验证功能却很有限；对于操作系统安排的无口令入口，是为系统开发人员提供的边界入口，但这些入口也可能被黑客利用；操作系统还有隐藏的信道，也存在着潜在的危险；尽管操作系统的缺陷可以通过版本的不断升级来克服，但系统的某一个安全漏洞就会使系统的所有安全控制变得毫无价值。

（3）网络。

使用 TCP/IP 协议的网络所提供的 FTP、E-mail、RPC 和 NFS 都包含许多不安全因素，存在着许多漏洞。同时，网络的普及，使信息共享达到了一个新的层次，也使信息被泄露的机会大大增多。特别是 Internet 网络就是一个不设防的开放大系统。另外，数据处理的可访问性和资源共享的目的性是一对矛盾体，它造成计算机系统保密性难以保证。

（4）数据库。

当前，大量的信息存储在各种各样的数据库中。然而，这些数据库系统在安全方面的考虑却很少。而且，数据库管理系统安全必须与操作系统的安全相配套，但实际上有时却不是这样，这就造成了数据库不安全因素的存在。

（5）防火墙。

尽管利用防火墙可以保护网络免受外部黑客的攻击，但它只是能够提高网络的安全性，不可能保证网络绝对安全。事实上仍然存在着一些防火墙不能防范的安全威胁，例如防火墙不能防范不经过防火墙的攻击。另外，防火墙很难防范来自于网络内部的攻击以及病毒的威胁。

1.1.3 网络安全目标

网络安全目标主要表现在系统的保密性、完整性、可靠性、可用性、不可抵赖性和可控性等方面。

（1）保密性。

保密性是指网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即防

止信息泄露给非授权个人或实体，信息只为授权用户所使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。常用的保密技术包括：防侦收（使对手侦收不到有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息，也会因为没有密钥而无法读懂有效信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）。

（2）完整性。

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。其影响网络信息完整性的主要因素包括：设备故障、误码（传输、处理和存储过程中产生的误码；定时的稳定度和精度降低造成的误码；各种干扰源造成的误码）、人为攻击、计算机病毒等。

（3）可靠性。

可靠性是网络信息系统能够在规定条件下和规定时间内完成规定功能的特性。可靠性是系统安全的最基本要求之一，也是所有网络信息系统的建设和运行目标。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演着重要的角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理、技术熟练程度、责任心和品德等方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

（4）可用性。

可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。同时，可用性还应该满足以下要求：身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪。

（5）不可抵赖性。

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确保参与者的真实同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

（6）可控性。

可控性是对网络信息的传播及内容具有可控制能力的特性。

概括地说，网络安全目标是通过计算机、网络、密码技术和安全技术，保护在公用网络系

统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

1.2 网络安全措施

网络安全问题是极其庞杂的，现在没有任何一种单一的网络安全技术和网络安全产品能解决所有的问题。所以，网络安全建设要从体系结构的角度，用系统工程的方法，根据具体的互联网环境及其应用需求提出综合处理的安全解决方案和措施。下面简要地分析一些常见的网络安全措施。

1.2.1 加密与解密

加密与解密是通信安全最重要的机制，它能保护传输中的信息不被恶意获取。重要文件加密后，则可以保证存储信息的安全性。然而，密码系统并不区分合法用户和非法用户，无论哪种用户访问加密文件都必须出示正确的密码。因此，加密解密本身并不提供安全措施，它们必须由密钥控制并将系统作为整体来管理。

1.2.2 防杀病毒软件

防杀病毒软件是网络安全程序的必备部分。如果能正确地配置和执行，可减少恶意程序对计算机网络的危害。然而，防杀病毒软件并不是对所有的恶意程序的防护都有效，尤其对新出现的病毒就更无能为力了。而且，它既不能防止入侵者利用合法程序得到系统的访问，也不能防止合法用户企图得到超出其权限的访问。

1.2.3 网络防火墙

网络防火墙是用于网络的访问控制设备，有助于帮助保护组织内部的网络，以防外部攻击。本质上讲网络防火墙是边界安全产品，存在于内部网和外部网的边界。因此，只要配置合理，网络防火墙是必需的安全设备。然而，网络防火墙不能防止攻击者使用合理的连接来攻击系统。例如，一个 Web 服务器允许来自外部的访问，攻击者可以利用 Web 服务器软件的漏洞，这时网络防火墙将允许这个攻击进入，因为 Web 服务器是应该接收这个 Web 连接的。对于内部用户，网络防火墙也没有防备作用，因为内部用户已经在内部网中了。

1.2.4 访问权限控制

网络内的每一个计算机系统具有基于用户身份的访问权限的控制。假如系统配置正确，文件的访问许可权配置合理，则文件访问控制能限制合法用户进行超出其权限的访问，但是不能阻止一些人利用系统的漏洞，得到像管理员一样的权限来访问系统及读写系统的文件。访问控制系统甚至允许跨域进行系统访问控制的配置，对访问控制系统而言，这样的攻击看起来类似于一个合法的管理员试图访问账户或允许访问的文件。

1.2.5 入侵检测

入侵检测系统（Intrusion Detection System，IDS）是一种用于分析系统和网络上未经授

权的进入和（或）有不良企图的活动的积极进程或设备。IDS 检测异常情况的方法可能会大相径庭，但是它们的最终目的都是在攻击者尚未对系统造成损害前当场捕捉他们，通过对行为、安全日志、审计数据或其他网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图。入侵检测是检测和响应计算机误用的学科，其作用包括威慑、检测、响应、损失情况评估、攻击预测和起诉支持等。入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。进行入侵检测的软件与硬件的组合便是入侵检测系统（IDS）。它是一种不同于网络防火墙的、主动保护网络资源的网络安全系统，是网络防火墙合理和必要的补充。它完全改变了传统网络安全防护体系被动防守的局面，使网络安全防护变得更积极、更主动，特别是 IDS 的可视化安全管理功能给网络安全防护工作带来了革命性的变化。

综上所述，网络安全是一个系统的工程，如果想较好地解决网络安全问题，必须从多方面、多角度来考虑。只有采用多样化的安全措施，从整体上对网络进行联动保护，才能使网络处于最大限度的安全之中。

1.3　网络安全策略

当考虑网络信息系统的安全问题时，必须依据信息系统安全工程学的理论和方法，构造一个全方位的防御机制。下面具体介绍几种安全策略的类型和内容。

1.3.1　物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。抑制和防止电磁泄露（即 TEMPEST 技术）是物理安全策略的一个主要问题。目前主要防护措施有两类：一类是对传导发射的保护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；另一类是对辐射的防护。

1.3.2　访问控制策略

访问控制是网络安全防范和保护的主要策略，其主要任务是保证网络资源不被非法使用和非法访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，可以说访问控制是保证网络安全的核心策略之一。下面分述几种访问控制策略。

（1）入网访问控制。

入网访问控制为网络访问提供了第一层访问控制。它用来控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许在哪个工作站入网。用户的入网访问控制可分为 3 个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的默认限制检查。只要 3 道关卡中有任何一关未过，该用户便不能进入该网络。

（2）网络权限控制。

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络权限控制着用户和用户组可以访问哪些目录、子目录、文件和其他资源，指定用户对这些文件、目录、设备执行哪些操作。根据访问权限可以将用户分为特殊用户（即系统管理员）、一般用户（系统管理员根据实际需要为他们分配操作）、审计用户（负责网络的安全控制与资源使用情况的审计）3 类。用户对网络资源的访问权限可以用一个访问控制表来描述。

（3）网络服务器安全控制。

网络允许在服务器控制台上执行一系列操作，如进行装载和卸载模块、安装和删除软件等操作。网络服务器的安全控制包括：可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

（4）网络监测和锁定控制。

网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问。对非法的网络访问，服务器应以图形、文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应能自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

1.3.3 数据加密策略

数据加密作为主动网络安全技术，是提高网络系统数据的保密性、防止秘密数据被外部破译所采用的主要技术手段，是许多安全措施的基本保证。加密后的数据能保证在传输、使用和转换时不被第三方获取。加密算法主要有以下几类。

（1）对称性加密算法。

使用单个密钥对数据进行加密或解密，其特点是计算量小、加密效率高。但是此类算法在分布式系统上使用较为困难，主要是密钥管理困难，使用成本较高，保密性能也不易保证。这类算法的代表是在计算机专网系统中广泛使用的 DES（数字加密标准）算法。

（2）不对称加密算法。

不对称加密算法也称公用密钥算法，其特点是有两个密钥（即公用密钥和私有密钥），只有二者搭配使用才能完成加密和解密的全过程。由于不对称算法拥有两个密钥，它特别适用于分布式系统中的数据加密，在 Internet 中得到了广泛应用。其中公用密钥在网上公布，为数据源对数据加密使用，而用于解密的相应私有密钥则由数据的接收方妥善保管。在网络系统中得到应用的不对称加密算法有 RSA 算法和美国国家标准局提出的 DSA（数字签名算法）。不对称加密法在分布式系统中应用时，需注意的问题是如何管理和确认公用密钥的合法性。

（3）不可逆加密算法。

不可逆加密算法的特征是加密过程不需要密钥，并且经过加密的数据无法被解密，只有同样的输入数据经过同样的不可逆加密算法才能得到相同的加密数据。不可逆加密算法不存在密钥保管和分发问题，适合在分布式网络系统上使用，但是其加密计算工作量相当大，所以通常用于数据量有限的情形下的加密，如计算机系统中的口令就是利用不可逆算法加密的。近来随着计算机系统性能的不断改善，不可逆加密的应用逐渐增多。

1.3.4　网络安全管理策略

在网络安全中，除了采用上述技术措施之外，加强网络的安全管理、制定有效的规章制度，对于确保网络的安全、可靠运行，将起到十分有效的作用。网络的安全管理策略包括：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。一个完整的网络安全解决方案所考虑的问题应是非常全面的。保证网络安全需要靠一些安全技术，但是，最重要的是要有详细的安全策略和良好的内部管理。在确立网络安全的目标和策略后，还要确定实施网络安全应付出的代价，然后选择切实可行的技术方案，方案实施完成之后最重要的是要加强管理，制定培训计划和网络安全管理措施。完整的安全解决方案应该覆盖网络的各个层次，并且与安全管理相结合。

1.4　网络安全技术的发展

1.4.1　第一代网络安全技术

当设计和研究信息安全措施时，人们最先想到的是“保护”，这样的技术称为第一代网络安全技术。它假设能够划分明确的网络边界并能够在边界上阻止非法入侵。比如，通过口令阻止非法用户的访问；通过存取控制和权限管理让某些人看不到敏感信息；通过加密使别人无法读懂信息的内容；通过等级划分使保密性得到完善等。其技术基本原理是保护和隔离，通过保护和隔离达到真实、保密、完整和不可否认等安全目的。如图 1-2 所示为第一代网络安全技术的示意图。

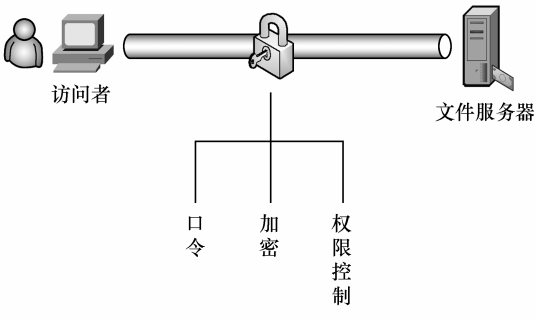

图 1-2　第一代网络安全技术

第一代网络安全技术解决了很多安全问题，但是，并不是在所有情况下都能够清楚地划分并控制边界，保护措施也并不是在所有情况下都有效。当 Internet 逐步扩展的时候，人们发现这些保护技术在某些情况下无法起作用。比如，在正常的数据中夹杂着可能使接收系统崩溃的参数；在合法的升级程序中夹杂着致命的病毒；黑客冒充合法用户进行信息偷窃；利用系统漏洞进行攻击等。随着信息空间的增大，边界保护的范围必须迅速扩大，正如长城虽然修得高，但空间边界的保护乃至太空边界的保护无法通过修建长城来解决一样，保护技术在现代网络环境下已经没有能力全面保护网络的信息安全了。

1.4.2　第二代网络安全技术

在以第一代安全技术为主的年代，为了保护网络，人们尽量多修一些不同类型的“墙”。比如，在系统存取控制的基础上，发明了各种类型的防火墙，希望这些“高墙”能够堵住原来系统中的缺口。然而，实际情况往往比设计者和评估者想象的还要复杂得多，许多著名的