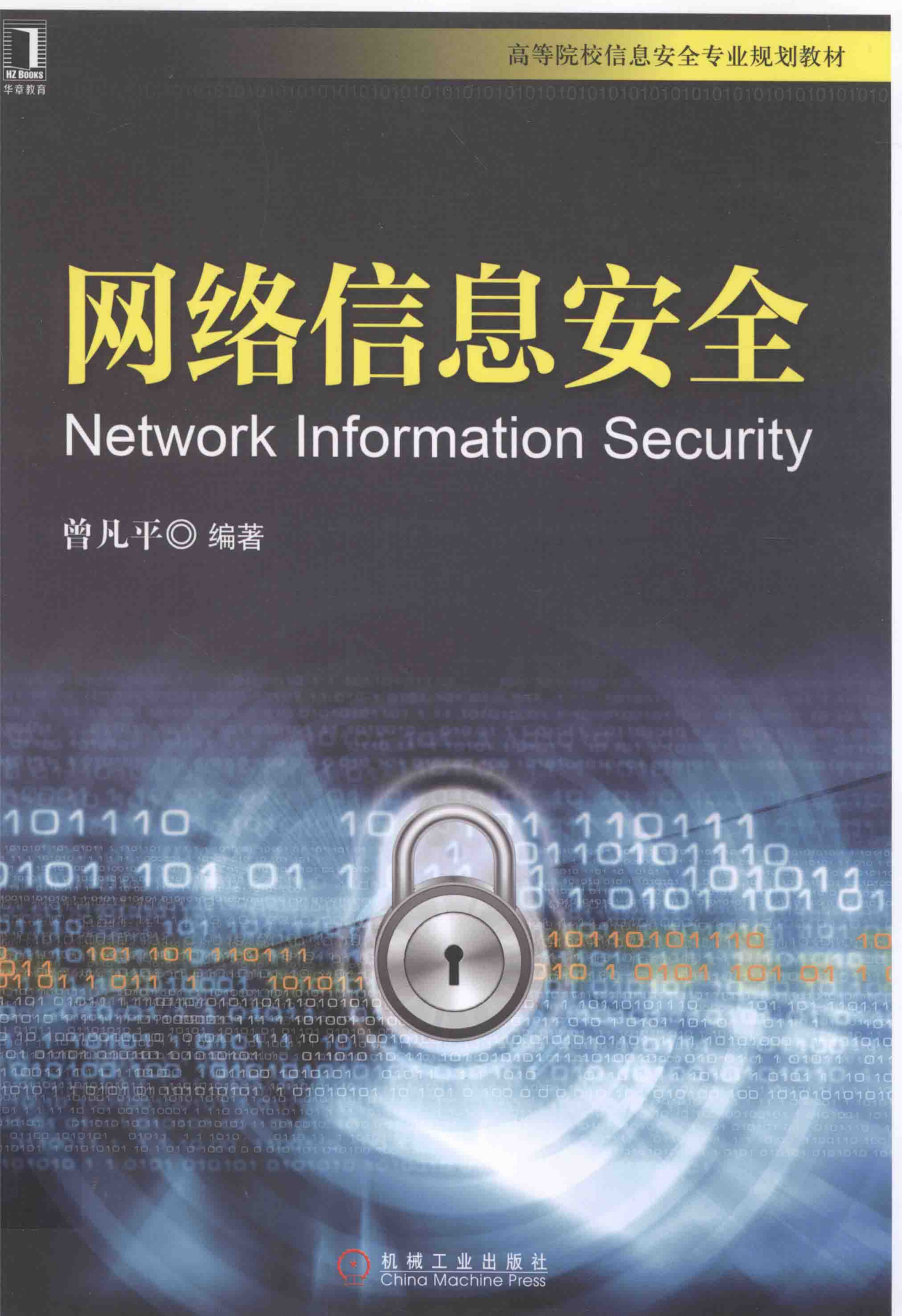
HZ BOOKS
华章教育

高等院校信息安全专业规划教材

网络信息安全

Network Information Security

曾凡平◎ 编著



机械工业出版社
China Machine Press

高等院校信息安全专业规划教材

网络信息安全

Network Information Security

曾凡平◎编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

网络信息安全 / 曾凡平编著 . —北京：机械工业出版社，2015.11
（高等院校信息安全专业规划教材）

ISBN 978-7-111-52008-5

I. 网… II. 曾… III. 计算机网络 - 信息安全 - 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（2015）第 261484 号

本书从网络攻击与防护的角度讨论网络安全原理与技术。在网络防护方面，介绍了密码学、虚拟专用网络、防火墙、入侵检测和操作系统的安全防护；在网络攻击方面，详细讨论了缓冲区溢出攻击、格式化字符串攻击、拒绝服务攻击和恶意代码攻击。本书的最大特点是理论结合实践，书中的实例代码只需经过少量修改即可用于设计实践。

本书可作为信息安全、信息对抗、计算机、信息工程或相近专业的本科生和研究生教材，也可作为网络安全从业人员的参考书。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：王　彬　　责任校对：殷　虹
印　　刷：三河市宏图印务有限公司　　版　　次：2016 年 1 月第 1 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：16.75
书　　号：ISBN 978-7-111-52008-5　　定　　价：45.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前言

笔者从2004年起承担“网络安全”研究生课程的主讲工作，最初的课程参考了《黑客大曝光》[㊀]系列书籍，主要讲解计算机及网络攻击技术，后来逐步增加网络安全防护方面的理论和技术等相关内容；在教学过程中参考了众多计算机与网络安全方面的教材，并将其中最有价值的内容引入课堂教学。

笔者认为，计算机类课程的教学应注重理论与实践相结合。如果只强调理论，难免枯燥无味，很难让读者坚持学习下去，甚至会产生“读书无用”的感觉。如果只强调实践，一味讲解案例，会让读者觉得“网络安全就是黑客攻防大全”。

本书面向高年级本科生和硕士研究生，从网络攻击和防护的角度阐述网络安全原理与实践。在网络防护部分，主要介绍原理和方法，并简要介绍原理与技术的具体应用。在网络攻击部分，主要介绍方法和实践，披露一些所谓的“黑客秘技”，并给出大量的实例代码供读者参考。

本书的网络攻击技术是从公开的出版物或网络资料总结而来的，目的是让读者了解网络攻击技术，更好地进行网络安全防护。读者只能在虚拟的实验环境下验证相关技术，不得在真实环境下使用攻击技术。

本书的最大特点是实用。书中的实例代码均通过验证，略作修改就可用于设计实践。为了便于教学，笔者制作了16次课（每次课3学时）的课件，适合国内高校一个学期每周3学时的教学任务。其中的“网络信息侦察技术”是从《黑客大曝光》系列书籍中总结而来的，仅用于保持教学内容的完整，不是本书的内容；另外，本书对“数字证书”介绍得不多，课件的部分内容扩充自其他教材。读者可登录华章网站（www.hzbook.com）下载随书课件及所有的实例代码。书中用到的工具和虚拟机可通过链接http://staff.ustc.edu.cn/~billzeng/books/books.htm获取。

由于笔者水平及精力有限，不足之处在所难免，恳请读者提出宝贵的意见和建议，以便进一步完善教材内容。笔者电子邮件地址为billzeng@ustc.edu.cn。

㊀《黑客大曝光》系列书籍已由机械工业出版社引进并出版，详情参见华章网站（www.hzbook.com）。——编辑注

目录

Chapter 1

第1章 网络安全综述

计算机网络已经成为了信息社会的基础，围绕计算机网络的攻击与防护漏洞也层出不穷。如何认识网络安全的内涵，从而保障网络信息系统的安全，这是需要研究的重要课题。

本章首先给出网络安全的基本概念，然后分析网络及信息系统面临的威胁，接着阐述网络攻防的核心技术，最后介绍网络攻防的发展历史。

1.1 网络安全概述

1.1.1 网络安全概念

网络安全（network security）是指网络系统的硬件、软件及其系统中的数据受保护，不因偶然的或者恶意的原因而遭受破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。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。

网络安全大体上可以分为信息系统安全、网络边界安全及网络通信安全。信息系统安全主要指计算机安全（智能手机及终端也是一种计算机），包括操作系统安全和数据库安全等；网络边界安全是指不同网络域之间的安全，包括网络上的访问控制、流量监控等，以保护内部网络不被外界非法入侵；网络通信安全是对通信过程中所传输的信息加以保护。

网络安全的目标是保护网络系统中信息的保密性、完整性、可用性、不可抵赖性、真实性、可控性和可审查性，其中，保密性、完整性、可用性也称为信息安全的三要素。

（1）保密性

保密性（confidentiality）也被称为机密性，是指保证信息不被非授权访问，即使非授权用户得到信息也无法理解信息的内容。它的任务是确保信息不会被未授权的用户访问，一般使用访问控制技术阻止非授权用户获得机密信息，通过密码技术阻止非授权用户获知信息内容。

（2）完整性

完整性（integrity）是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不发生人为或非人为的非授权篡改。一般通过访问控制阻止篡改行为，同时通过消息摘要算法来检验信息是否被篡改。要保护信息的完整性，需要保证数据及系统的完整性。

1）数据的完整性：数据没有被非授权篡改或者损坏。

2）系统的完整性：系统未被非法操纵，按既定的目标运行。

一般而言，如果系统的完整性被破坏，则很难保护其中数据的完整性。

（3）可用性

可用性（availability）是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息。可用性是信息资源服务功能和性能可靠性的度量，涉及物理、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的要求。

（4）不可抵赖性

不可抵赖性是信息交互过程中，所有参与者不能否认曾经完成的操作或承诺的特性，这种特性体现在两个方面，一是参与者开始参与信息交互时，必须对其真实性进行鉴别；二是信息交互过程中必须能够保留下使其无法否认曾经完成的操作或许下的承诺的证据。

（5）真实性

信息的真实性要求信息中所涉及的事务是客观存在的，信息的各个要素都真实且齐全，信息的来源是真实可靠的。

（6）可控性

信息的可控性是指对信息的传播及内容具有控制能力，也就是可以控制用户的信息流向，对信息内容进行审查，对出现的安全问题提供调查和追踪手段。

（7）可审查性

出现安全问题时提供依据与手段，以可控性为基础。

网络安全是信息安全学科的重要组成部分。网络安全的研究内容相当宽泛，涉及网络、通信和计算机等方面的安全。网络安全、通信安全和计算机安全措施需要与其他类型的安全措施（如物理安全和人员安全措施）配合使用，才能更有效地发挥其作用。

1.1.2 网络安全体系结构

网络安全体系结构是安全服务、安全机制、安全策略及相关技术的集合。国际标准化组织（ISO）于 1988 年发布了 ISO 7498-2 标准，即开放系统互联（Open System Interconnection，OSI）安全体系结构标准，该标准等同于中华人民共和国国家标准 GB/T 9387.2—1995。1990 年，国际电信联盟（International Telecommunication Union，ITU）决定采用 ISO7498-2 作为其 X.800 推荐标准。因此，X.800 和 ISO7498-2 标准基本相同。1998 年，RFC 2401 给出了 Internet 协议的安全结构，定义了 IPSec 适应系统的基本结构，这一结构的目的是为 IP 层传输提供多种安全服务。

下面列出一些与安全体系结构相关的术语。

（1）安全服务

X.800 对安全服务做出定义：为了保证系统或数据传输有足够的安全性，开放系统通信协议所提供的服务。

RFC 2828 对安全服务做出了更加明确的定义：安全服务是一种由系统提供的对资源进行特殊保护的进程或通信服务。

（2）安全机制

安全机制是一种措施或技术，一些软件或实施一个或更多安全服务的过程。常用的安全机制有认证机制、访问控制机制、加密机制、数据完整性机制、审计机制等。

（3）安全策略

所谓安全策略，是指在某个安全域内，施加给所有与安全相关活动的一套规则。所谓安全域，通常是指属于某个组织机构的一系列处理进程和通信资源。这些规则由该安全域中所设立的安全权威机构制定，并由安全控制机构来描述、实施或实现。

（4）安全技术

安全技术是与安全服务和安全机制对应的一系列算法、方法或方案，体现在相应的软件或管理规范之中。比如密码技术、数字签名技术、防火墙技术、入侵检测技术、防病毒技术和访问控制技术等。

众所周知，计算机网络具有分层的体系结构。**信息安全技术可以应用到网络体系结构的任何一层**，每一层均可以增加安全功能，安全功能相互协调、相互作用，共同保障网络信息系统的安全。正因为网络的每一层次均可施加安全功能，所以可以将网络安全体系结构看作网络协议层次、安全功能和安全技术的集合。对于目前广泛使用的 TCP/IP 协议，其分层的网络安全体系结构如图 1-1 所示。

应用层	应用层安全协议，如HTTPS、SSH、FTPS
传输层	传输层安全协议，如SSL、TLS
网络层	网络层安全协议，如IPSec
网络接口层	网络接口层安全技术，如PPTP、L2TP

图 1-1　分层的网络安全体系结构

1）应用层：对各种应用层软件施加安全功能，如 Web 安全、电子邮件安全、数据库安全、电子交易安全等。该层涉及众多的安全协议及软件，如 HTTPS、SSH、SET、PGP。此外，计算机上的所有软件都与应用层的安全相关。

2）传输层：提供端到端的安全通信，如安全套接字等。

3）网络层：保证网络传输中的安全，包括安全接入、安全路由、传输加密等。IPSec 是最常用的网络层安全协议。

4）网络接口层：如 PPTP、L2TP 及链路层加密等技术。

除了各层的安全协议外，还有一些通用的安全技术，如密码技术、访问控制技术、数字签名及身份认证技术等。

1.1.3　网络安全的攻防体系

从系统安全的角度，可以把网络安全的研究内容分成两大体系：攻击和防护。

网络攻击是指采用技术手段，利用目标信息系统的安全缺陷，破坏网络信息系统的保密性、完整性、真实性、可用性、可控性与可审查性等的措施和行为。其目的是窃取、修改、伪造或破坏信息，以及降低、破坏网络使用效能。

网络防护是指为保护己方网络和设备正常工作、信息数据安全而采取的措施和行动。其目的是保证己方网络数据的保密性、完整性、真实性、可用性、可控性与可审查性等。

本教材从网络攻防（也称网络对抗）角度讨论网络安全，介绍网络攻击与防护的相关原理和技术。

1.2　计算机网络面临的安全威胁

由于网络分布的广域性、网络体系结构的开放性、信息资源的共享性和通信信道的共用性，使得网络存在严重的脆弱性。如果这些脆弱性被恶意利用，将导致网络遭受来自各方面的威胁和攻击，从而在根本上威胁网络系统的安全性。

1.2.1　TCP/IP 网络体系结构及计算机网络的脆弱性

层和协议的集合称为**网络体系结构**（network architecture）。目前，互联网络事实上的标准是 TCP/IP 网络体系结构，如图 1-2 所示。

图 1-2　TCP/IP 网络体系结构

该网络体系结构的协议及每一层均存在安全隐患。此外，网络协议依托于计算机软件和硬件，而计算机软件和硬件也存在大量的安全问题。

（1）网络基础协议存在安全漏洞

TCP/IP 协议在设计初期并没有考虑安全性，从而导致存在大量的安全问题。例如，在 IP 层协议中，IP 地址可以由软件设置，这就造成了地址欺骗安全隐患；IP 协议支持源路由方式，即源点可以指定信息包传送到目的节点的中间路由，这就为源路由攻击提供了条件。再如，应用层协议 Telnet、FTP、SMTP 等缺乏认证和保密措施，这就有可能导致发生抵赖和信息泄露等行为。

（2）网络硬件存在着安全隐患

计算机硬件在制造和使用的过程中会存在一些安全隐患。

1）制造计算机硬件的国家故意在计算机硬件及其外围设备的生产或运输过程中在硬件芯片中固化病毒或其他程序，在战时通过遥控手段激活，从而让计算机病毒在敌方计算机网络中迅速传播，导致敌方的计算机网络瘫痪，或者为入侵敌方计算机网络提供后门。在 1991 年的海湾战争中，美国就是通过在伊拉克购买的打印机芯片中植入病毒，在战时遥控激活病毒，从而在很短的时间内赢得了胜利。

2）由于技术上的原因，硬件有可能存在漏洞。恶意软件利用硬件的漏洞也可以直接破坏计算机硬件。比如，CIH 病毒就是利用计算机硬件的漏洞，攻击和破坏硬件系统的。

3）计算机硬件系统本身是电子产品，其抵抗外部环境影响的能力还比较弱，特别是在强磁场和强电场环境下有可能导致比特翻转，从而使系统失效。计算机硬件会向外辐射电磁信

号，采用适当的手段可以接收其辐射的电磁信号，经过适当处理和分析能够获取需要的信息。连接计算机系统的通信网络在许多方面也存在薄弱环节，使得搭线窃听、远程监控、攻击破坏等成为可能。

（3）软件缺陷

软件是网络信息系统的核心。然而由于技术或人为因素，软件不可避免地存在缺陷，这就可能导致出现安全漏洞。事实上，软件漏洞是威胁网络及信息系统安全的最根本原因。软件缺陷主要表现在以下几个方面：

1）对程序输入的处理不当。保证程序安全的最重要原则是对输入做严格的检查，特别是从用户获得输入时更是如此。对于应用程序来说，如果用户只能通过这个应用程序所允许的方式访问系统，则用户滥用这一应用程序的可能性便小了一些。如果应用程序允许用户输入自己的信息，一个恶意用户就可能输入一些特殊的信息来达到自己的目的。比如缓冲区溢出漏洞，主要是因为对输入的数据未做边界检查导致的。又比如格式化字符串漏洞，是因为没有检查格式串导致的。SQL 注入攻击也是因为没有对用户的输入进行过滤而发生的。

2）程序所提供的功能缺乏适当的用户身份认证。有些软件功能非常强大，但在一个操作系统上对所有登录用户都开放，缺少应有的分级审查制度和身份认证机制。特别是对一些敏感的、要访问系统内核的程序，这种缺陷会造成更大的危害。有可能一般用户会利用这种缺陷来提升自己的权限，从而控制整个系统。

3）对程序功能的配置处理不当。这表现在一些病毒防火墙和网络防火墙的配置上。比如基于状态检测的防火墙，虽然其提供了非常好的防火墙功能，然而有些管理员只按默认方式使用该防火墙，即只使用了动态包过滤的功能，其后果就是防护能力下降。

（4）操作系统存在安全隐患

1）操作系统也是软件系统，而且是巨型复杂高纬度的软件，其代码量非常庞大，由成百上千位工程师协作完成，很难避免产生安全漏洞。

2）操作系统的功能越来越多，配置起来越来越复杂，从而会造成配置上的失误，产生安全问题。

3）操作系统的安全级别不高。目前大规模使用的 Windows 和 Linux 系统的安全级别为 TCSEC 的 C2 级，而 C2 级难以保证信息系统的安全。

此外，**我国目前特别严重的问题是操作系统基本上自国外引进**，不能排除某些国家出于不可告人的目的而在其中设置了后门。因此，软件（特别是操作系统）国产化是一个迫切需要解决的根本问题。

1.2.2　计算机网络面临的主要威胁

由于网络信息系统存在脆弱性，使其面临各种各样的安全威胁。安全威胁主要有以下几类：

（1）各种自然因素

包括各种自然灾害，如水、火、雷、电、风暴、烟尘、虫害、鼠害、海啸和地震等；网络的环境和场地条件，如温度、湿度、电源、地线和其他防护设施不良造成的威胁；电磁辐射和电磁干扰的威胁；网络硬件设备自然老化、可靠性下降等。

（2）内部窃密和破坏

内部人员可能对网络系统形成下列威胁：内部涉密人员有意或无意泄密、更改记录信息；内部非授权人员有意或无意偷窃机密信息、更改网络配置和记录信息；内部人员恶意破坏网

络系统。

（3）信息的截获和重演

攻击者可能通过搭线或在电磁波辐射的范围内安装截收装置等方式，截获机密信息，或通过对信息流和流向、通信频度和长度等参数的分析，推出有用信息。它不破坏传输信息的内容，不易被察觉。截获并录制信息后，可以在必要的时候重发或反复发送这些信息。

（4）非法访问

非法访问指的是未经授权使用网络资源或以未授权的方式使用网络资源，包括：非法用户（如黑客）进入网络或系统，进行违法操作；合法用户以未授权的方式进行操作。

（5）破坏信息的完整性

攻击可能从3个方面破坏信息的完整性：改变信息流的时序，更改信息的内容；删除某个消息或消息的某些部分；在消息中插入一些信息，让接收方读不懂或接收错误的信息。

（6）欺骗

攻击者可能冒充合法地址或身份欺骗网络中的其他主机及用户；冒充网络控制程序套取或修改权限、口令、密钥等信息，越权使用网络设备和资源；接管合法用户，欺骗系统，占用合法用户的资源。

（7）抵赖

可能出现下列抵赖行为：发信者事后否认曾经发送过某条消息；发信者事后否认曾经发送过某条消息的内容；发信者事后否认曾经接收过某条消息；发信者事后否认曾经接收过某条消息的内容。

（8）破坏系统的可用性

攻击者可能从下列几个方面破坏网络系统的可用性：使合法用户不能正常访问网络资源；使有严格时间要求的服务不能及时得到响应；摧毁系统。

1.3 计算机网络安全的主要技术与分类

从系统的角度可以把网络安全的研究内容分成3类：网络侦察（信息探测）、网络攻击和网络防护。因此其主要技术也可以相应地分为3类，即网络侦察技术、网络攻击技术和网络防护技术。

1.3.1 网络侦察

网络侦察也称网络信息探测，是指运用各种技术手段，采用适当的策略对目标网络进行探测扫描，获得有关目标计算机网络系统的拓扑结构、通信体制、加密方式、网络协议与操作系统、系统功能，以及目标地理位置等各方面的有用信息，并进一步判别其主控节点和脆弱节点，为实施网络攻击提供可靠的情报。所涉及的关键技术如下。

（1）端口探测技术

主要利用端口扫描技术，以发现网络上的活跃主机及其上开放的协议端口。网络信息系统的目标是资源共享和提供连通服务，二者均离不开网络协议端口。比如，Web服务的默认端口是TCP 80，FTP服务的默认端口是TCP 21。通过端口探测，就可以初步判断哪些主机提供了哪些服务，为进一步的信息探测提供依据。一般利用端口扫描软件进行端口探测，如开源软件Nmap就提供了丰富的端口探测功能。

（2）漏洞探测技术

在硬件、软件、协议的具体实现或系统安全策略上不可避免会存在缺陷，如果这些缺陷能被攻击者利用，则这样的缺陷就成为漏洞。

漏洞探测也称为漏洞扫描，是指利用技术手段，以获得目标系统中漏洞的详细信息。目前有两种常用的漏洞探测方法。其一是对目标系统进行模拟攻击，若攻击成功则说明存在相应的漏洞；其二是根据目标系统所提供的服务和其他相关信息，判断目标系统是否存在漏洞，这是因为特定的漏洞是与服务、版本号等密切相关的，也称为信息型漏洞探测。目前的反病毒软件（如 360、金山毒霸等）附带的漏洞修补软件就采用了信息型漏洞探测方法。

（3）隐蔽侦察技术

一般来说，重要的信息系统都具有很强的安全防护能力和反侦察措施，常规侦察技术很容易被目标主机觉察或被目标网络中的入侵检测系统发现，因而要采用一些手段进行隐蔽侦察。隐蔽侦察采用的主要手段有：秘密端口探测、随机端口探测、慢速探测等。

1）**秘密端口探测**：因为常规的端口探测首先必须要与目标主机的端口建立连接，目标主机对这种完整的连接会做记录，而秘密端口探测并不包含连接建立的任何一个过程，因此很难被发现。

2）**随机端口探测**：许多入侵检测系统和防火墙会检测到连续端口连接尝试。采用随机端口号跳跃扫描能减少被检测到的可能性。

3）**慢速探测**：入侵检测系统能够通过在一段时间内对网络流量进行分析，检测到是否有一个固定的 IP 地址对被防护的主机进行端口扫描。这段时间称为检测门限。因此可将对同一目标的探测时间间隔延长，使其超过检测门限，以达到不被发现的目的。

（4）渗透侦察技术

渗透侦察指的是在目标系统中植入特定的软件，从而完成情报的收集。渗透侦察技术主要采用反弹端口型木马技术。

为了将木马植入目标系统中，一般采用诱骗方法使目标用户主动下载木马软件。比如可以设置一些免费共享软件网站，引诱用户单击相关链接，而一旦单击该链接，则下载了木马。

1.3.2　网络攻击

网络攻击的目的是破坏目标系统的安全性，即破坏或降低目标系统的机密性、完整性和可用性等，因此凡是可以达成这个目标的行为和措施都可认为是网络攻击。由于计算机硬件和软件、网络协议和结构，以及网络管理等方面不可避免地存在安全漏洞，使得网络攻击成为了可能。网络攻击所涉及的技术和手段很多，下面列举几种常见的网络攻击技术。

（1）拒绝服务

拒绝服务（Denial of Service，DoS）攻击的主要目的是降低或剥夺目标系统的可用性，使合法用户得不到服务或不能及时得到服务，一般通过耗尽网络带宽或耗尽目标主机资源的方式进行。比如：攻击者通过向目标建立大量的连接请求，阻塞通信信道、延缓网络传输、挤占目标机器的服务缓冲区，以致目标计算机疲于应付、响应迟钝，直至网络瘫痪、系统关闭。为了增加攻击的成功率，实际攻击中多采用分布式拒绝服务攻击，也就是协调多台计算机同时对目标实施拒绝服务攻击。

（2）入侵攻击

入侵攻击是指攻击者利用目标系统的漏洞非法进入系统，以获得一定的权限，进而可以

窃取信息、删除文件、埋设后门，甚至瘫痪目标系统等行为。入侵攻击是最有效也是最难的攻击方式。

入侵攻击最常用的技术手段是攻击目标系统中存在缓冲区溢出漏洞的进程，在目标进程中执行具有特定功能的代码（称为 Shellcode），从而获得目标系统的控制权。

（3）病毒攻击

计算机病毒一般指同时具有感染性和寄身性的代码。它隐藏在目标系统中，能够自我复制、传播，并侵入到其他程序中，并篡改正常运行的程序，损害这些程序的有效功能。

（4）恶意代码攻击

恶意代码是指任何可以在计算机之间和网络之间传播的程序或可执行代码，其目的是在未授权的情况下有目的地更改或控制计算机及网络系统。计算机病毒就是一种典型的恶意代码，此外，还包括木马、后门、逻辑炸弹、蠕虫等。

木马是一种隐藏在目标系统中的特殊程序，主要目的是绕过系统的访问控制机制。木马可通过电子邮件或捆绑在一些下载的可执行文件中进行传播。

后门有时也叫作陷阱，是程序员故意在正常程序中设置的额外功能，它允许非法用户以未授权的方式访问系统。

逻辑炸弹也是程序员故意设置的额外功能，当某些条件满足时程序将会做与原来功能不一样的事，以达到破坏数据、瘫痪机器等目的。

蠕虫是一种可以在网络上不同主机间传播，而不修改目标主机上其他程序的一类程序。蠕虫其实是一种自治的攻击代理程序，可以自动完成网络侦察、网络入侵的功能。

（5）电子邮件攻击

利用电子邮件缺陷进行的攻击称为电子邮件攻击。

传统的邮件攻击主要是向目标邮件服务器发送大量的垃圾邮件，从而塞满邮箱，大量占用邮件服务器的可用空间和资源，使邮件服务器暂时无法正常工作，甚至使目标系统瘫痪。

由于反垃圾邮件技术的广泛使用，现在的邮件攻击更多是发送伪造或诱骗的电子邮件，诱骗用户去执行一些危害网络安全的操作。比如，在电子邮件的附件中捆绑病毒和木马，用户一旦打开附件就可能运行病毒或植入木马。

（6）诱饵攻击

诱饵攻击指通过建立诱饵网站，诱骗用户去浏览恶意网页，从而实现攻击。

有些网站提供免费共享的实用软件，然而某些软件被嵌入了木马或后门，当浏览者下载并运行这些貌似正常的软件时，木马会不知不觉地植入浏览者的计算机中。

有些网站提供免费共享的小说供用户阅读，然而却在页面上嵌套了恶意脚本（如 JavaScript 和 VBScript），可以使浏览者在浏览时执行特定的命令，比如删除系统文件等。特别是一些激情网站，几乎都挂了木马，一旦浏览其中的图片或视频则会被植入木马或病毒。

诱饵攻击是一种被动攻击，只要用户保持足够的警觉就可以避免。

1.3.3 网络防护

网络防护是指保证己方网络信息系统的保密性、完整性、真实性、可用性、可控性与可审查性而采取的措施和行为。

有人将网络防护的主要目标归结为“五不”，即进不来、拿不走、看不懂、改不了、走不脱。

- **进不来**：使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。

- **拿不走**：使用授权机制，实现对用户的权限控制，同时结合内容审计机制，实现对网络资源及信息的可控性。
- **看不懂**：使用加密机制，确保信息不暴露给未授权的实体或进程，从而实现信息的保密性。
- **改不了**：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，从而确保信息的完整性和真实性。
- **走不脱**：使用审计、监控、防抵赖等安全机制，使得破坏者走不脱，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。

网络防护涉及的面很宽，从技术层面上讲主要包括防火墙技术、入侵检测技术、病毒防护技术、数据加密技术和认证技术等。

（1）防火墙技术

防火墙是最基本的网络防护措施，也是目前使用最广泛的一种网络安全防护技术。防火墙通常安置在内部网络和外部网络之间，以抵挡外部入侵和防止内部信息泄密。防火墙是一种综合性的技术，涉及计算机网络技术、密码技术、安全协议、安全操作系统等多方面。防火墙的主要作用为过滤进出网络的数据包、管理进出网络的访问行为、封堵某些禁止的访问行为、记录通过防火墙的信息内容和活动、对网络攻击进行检测和告警等。

简单的防火墙可以用路由器实现，复杂的可以用主机甚至一个子网来实现。防火墙技术主要有两种：数据包过滤技术和代理服务技术。

数据包过滤是在 IP 层实现的，主要根据 IP 数据报头部的 IP 地址、协议、端口号等信息进行过滤。网络管理员先根据访问控制策略建立访问控制规则，然后防火墙的过滤模块根据规则决定数据包是否允许通过。数据包过滤技术的优点是速度快和易于实现，缺点是只能提供较低水平的安全防护，无法对高层的网络入侵行为进行控制。

所谓代理服务，实际上就是运行在防火墙主机上的一些特殊的应用程序或者服务器程序。这些代理程序工作在应用层，可以对 HTTP、FTP、TELNET 等数据流进行控制。外部计算机在访问内部网络时，是将请求发给防火墙主机上的代理程序，由其验证请求的合法性后，再转发给内部网络的计算机。代理服务程序可以对应用层的数据进行分析、注册登记、形成报告，同时当发现被攻击迹象时会向网络管理员发出报警，并保留攻击痕迹。与数据包过滤技术相比，代理服务技术能够在更大程度上提高安全性。

（2）入侵检测技术

入侵检测是一种动态安全技术，通过对入侵行为的过程与特征的研究，从而对入侵事件和入侵过程做出实时响应。由于入侵特征往往要到应用层才能体现出来，所以要在应用层以下判定入侵行为有一定的困难。

有两种主要的入侵检测技术：基于特征的检测和基于行为的检测，也称为误用检测和异常检测。基于特征的检测假定所有的入侵模式均可提取出唯一的模式特征，从而建立入侵模式特征库，在此基础上用特征匹配的方法进行检测。基于行为的检测假定所有的正常行为和入侵行为有统计意义上的差异，从而可以利用统计学的原理进行检测。

入侵检测系统从实现方式上一般分为两种，即基于主机的入侵检测系统和基于网络的入侵检测系统。基于主机的入侵检测系统用于保护关键应用的服务器，并且提供对典型应用的监视。基于网络的入侵检测系统保护的是整个网络，对本网段提供实时网络监视。入侵监测系统通常配置为分布式模式，在需要监视的服务器上安装代理模块，在需要监视的网络路径