普通高等教育“十三五”创新型规划教材
理论+实践+数字资源一体化规划教材

计算机网络安全技术

主编 王艳柏 侯晓磊 龚建锋

电子科技大学出版社
University of Electronic Science and Technology of China Press

计算机网络安全技术

主　编　王艳柏　侯晓磊　龚建锋
副主编　谭　璐　王秀丽　邓作杰
　　杨战武　朱德新　朱艳艳
　　李晓辉　刘　亮　齐鸣鸣

电子科技大学出版社
·成都·

图书在版编目(CIP)数据

计算机网络安全技术／王艳柏，侯晓磊，龚建锋主编
．—成都：电子科技大学出版社，2019.8
ISBN 978-7-5647-7143-0

Ⅰ．①计… Ⅱ．①王… ②侯… ③龚… Ⅲ．①计算机网络－安全技术 Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 122894 号

计算机网络安全技术

JISUANJI WANGLUO ANQUAN JISHU

王艳柏　侯晓磊　龚建锋　主编

策划编辑　高小红
责任编辑　刘　愚

出版发行　电子科技大学出版社
　　成都市一环路东一段 159 号电子信息产业大厦九楼　邮编　610051
主　　页　www.uestcp.com.cn
服务电话　028-83203399
邮购电话　028-83201495

印　　刷　湖北鄂南新华印刷包装股份有限公司
成品尺寸　185mm×260mm
印　　张　16
字　　数　379 千字
版　　次　2019 年 8 月第 1 版
印　　次　2019 年 8 月第 1 次印刷
书　　号　ISBN 978-7-5647-7143-0
定　　价　46.80 元

前 言

随着网络应用的普及和信息化建设的快速推进，网络基础设施与信息系统已经渗透到社会的政治、经济、文化、军事、意识形态和社会生活的各个方面。特别是随着近年来电子商务、电子政务、办公自动化和企事业单位信息化建设的飞速发展，黑客入侵、网络病毒肆虐，网络系统损害或瘫痪，重要数据被窃取或毁坏等，给政府、企业以及个人带来了巨大的经济损失，也为网络的健康发展造成巨大的障碍。网络信息安全问题已成为网络技术领域的重要研究课题，因此，计算机网络安全已成为当今世界各国共同关注的焦点。我国网络基础设施和信息系统安全保障建设远滞后于信息化发展，尽管安全意识不断增强，但缺乏信息安全防护措施。特别是国家强制实施信息安全等级保护工作以来，越来越多的相关专业技术人员需要学习和掌握信息安全技术与应用技能。

计算机网络安全是个涉及计算机科学、网络技术、软件工程、通信技术、密码技术、法律、法规、管理、教育等多个领域的复杂系统工程。计算机应用技术和网络技术的发展是非常迅速的，本书在内容组织上力图靠近新知识、新技术的前沿，以较好地反映新理论和新技术。本书按照信息安全基础理论、工作原理、技术应用和工程实践层次体系结构组织教学内容，对当前网络安全领域的核心技术进行了全面与系统的介绍，内容包括概述、网络安全法规与标准、计算机网络安全基础、密码学基础、身份认证与访问控制、攻击与防御技术分析、计算机病毒、操作系统与数据库安全技术、无线局域网安全技术和云计算安全。在撰写风格上力求做到深入浅出、概念清晰和通俗易懂。

在本书编写过程中，引用了一些成果和参考文献，在此，谨向被引用文献的著（作）者表示真挚的谢意。

由于作者水平有限，书中难免会有谬误或不足之处，敬请各位同仁、专家和使用者批评指正。

编 者

2019 年 4 月

目 录

第 1 章 绪　论

本章简介：在分析计算机网络面临的威胁和不安全因素与原因的基础之上，对计算机网络安全的概念、计算机网络安全的体系结构、计算机网络安全管理以及计算机网络安全技术发展趋势进行了系统的讨论，使读者对计算机网络安全建立起一个全面的认识。

1.1　计算机网络面临的主要威胁

计算机网络面临的主要威胁包括计算机网络实体(硬件)面临的威胁、计算机网络系统(软件和信息)面临的威胁和恶意程序的威胁三种，而到底什么人在威胁计算机网络的安全以及为什么要威胁计算机网络安全，这也是解决计算机网络所面临威胁的根本之道。

1.1.1　计算机网络实体面临威胁

计算机网络实体面临的威胁主要指计算机网络硬件及其所处环境所面临的威胁。具体包括计算机网络机器所面临的威胁、计算机网络互联设备面临的威胁、计算机网络通信介质面临的威胁以及计算机网络硬件所处环境面临的威胁。

计算机网络机器所面临的威胁包括客户机端和服务器端面临的威胁。比如变成靶机或者被当作“肉鸡”，服务器端计算机电源跳闸、被放置于高温环境，或者遭受各种黑客攻击导致宕机甚至崩溃。

计算机网络互联设备面临的威胁主要包括有线互联设备和无线互联设备所面临的威胁，前者主要有调制解调器、网卡、交换机、路由器、防火墙等面临的各种故意威胁(如窃取信号等)和无意威胁(如配置错误等)，后者主要有无线网卡、无线路由器、无线 AP 等面临的故意(如窃取账号密码等)或者无意威胁(如置于电磁干扰环境等)。

计算机网络通信介质面临的威胁也可以从有线通信介质和无线通信介质两方面考察，有线通信介质主要有电信号通信介质(主要是双绞线和同轴电缆)、光信号通信介质(主要是光纤)，无线通信介质主要包括无线电波(内含微波)、红外线。计算机网络通信介质面临的无意威胁主要有电磁辐射等，故意威胁主要有电磁干扰等。

计算机网络硬件所处环境面临的威胁中，主要有自然灾害、气候与天气、温度与湿度等。

1.1.2 计算机网络系统面临威胁

计算机网络系统面临的威胁主要可从计算机网络软件系统和计算机网络信息系统两方面进行考察。计算机网络软件系统包括计算机网络系统软件(包含网络操作系统软件、网络数据库管理软件、网络服务器软件和网络通信软件)和计算机网络应用软件(主要是各种网站程序和各种 APP)。计算机网络信息系统主要指文件和数据。

典型的网络系统安全威胁包括窃听(传输过程中的信息被盗取)、重传(事先获得部分或全部信息再重新发送信息)、伪造(制造虚假信息)、篡改(修改、删除或插入信息)、非授权访问(非法手段获得访问权后操作信息)、拒绝服务攻击(使系统变慢甚至瘫痪以阻止合法用户正常获取信息)、行为否认(不承认已经实行的操作)、旁路控制(从系统缺陷处操作系统以获取信息)、电磁/射频截获(通过无线射频或电磁辐射的方式获取信息)、人员疏忽(管理问题造成信息泄露)。

1. 操作系统所面临的威胁

(1) 操作系统的结构性缺陷。操作系统本身程序的设计存在缺陷，被黑客利用使得系统崩溃或者瘫痪。

(2) 操作系统的功能性缺陷。比如允许网络传送文件、同意加载或安装程序、批准创建进程、开放远程调用等，被恶意软件利用可能造成系统泄密甚至崩溃。

(3) 操作系统的人为因素。比如后门造成信息泄密和丢失。

2. 数据库管理系统所面临的威胁

数据库管理系统所面临的威胁主要包括系统本身面临的威胁和系统所管理的数据面临的威胁，以前者为主。前者比如账号被窃取，后者比如数据泄露。威胁数据库管理系统的途径主要包括数据的独立性(包括物理独立性和逻辑独立性两个方面)、数据的安全性(包括存储安全、操作安全)、数据的完整性(包括数据的正确性、有效性和一致性)、并发控制、故障恢复等方面。

3. 网络服务器软件所面临的威胁

目前网络服务器(此处主要讨论 Web 服务器)软件主要有 MS IIS、Apache、Tomcat、WebSphere、WebLogic、Nginx、Kangle、Jboss 等。Web 服务器软件比较常见的威胁主要有盗用账号、缓冲区溢出以及执行任意命令等，而制造威胁的手段主要有黑客攻击、蠕虫病毒以及木马等，其中黑客攻击比较常见的方式主要有口令攻击、拒绝服务攻击以及 IP 欺骗等。

4. 网络通信软件所面临的威胁

网络通信软件包括网络通信支撑平台软件、网络通信服务支撑平台软件、网络应用支撑平台软件、网络协议软件等。它们所面临的主要威胁有：

(1) 网络通信软件的漏洞及缺陷被利用，使网络遭到入侵和破坏；

(2) 网络通信软件安全功能不健全或被安装了“特洛伊木马”软件；

（3）应加安全措施的软件可能为未给予标识和保护，要害的程序可能没有安全措施，使软件被非法使用、被破坏或产生错误的结果；

（4）未对用户进行分类和标识，使数据的存取未受到限制或控制，而被非法用户窃取或非法处理；

（5）错误地进行路由选择，为一个用户与另一个用户之间的通信选择了不合适的路径；

（6）拒绝服务，中断或妨碍通信，延误对时间要求较高的操作；

（7）信息重播，即把信息收录下来准备过一段时间重播；

（8）对软件更改的要求没有充分理解，导致软件缺陷；

（9）没有正确的安全策略和安全机制，缺乏先进的安全工具和手段；

（10）不妥当的标定或资料，导致所改的程序出现版本错误。如程序员没有保存程序变更的记录；没有做拷贝；未建立保存记录的业务。

5. 计算机网络应用软件所面临的威胁

计算机网络应用软件所面临的威胁即计算机网站或者 APP 所面临的威胁，包括自身威胁即无意威胁和外在威胁即故意威胁。自身威胁主要是指网站程序自身存在的 bug、漏洞以及后门；外在威胁包括网络钓鱼和分布式拒绝服务（DDoS）攻击，前者被用来窃取网站访问者的个人信息，如银行支付账户、姓名和地址等，后者主要是使得网站响应变得缓慢，甚至停止服务。

1.1.3　恶意程序的威胁

恶意程序通常是指具有攻击意图的某些程序。它所带来的威胁可以分成需要宿主程序的威胁和彼此独立的威胁两种。前者基本上是不能独立于某个实际的应用程序、实用程序或系统程序的程序片段，后者是可以被操作系统调度和运行的自包含程序。也可以将这些软件威胁分成不进行复制工作和进行复制工作的两类。

恶意程序主要包括：陷门、逻辑炸弹、特洛伊木马、蠕虫、细菌、病毒等。

1. 陷门

计算机操作的陷门设置是指进入程序的秘密入口。它本来是为了方便程序员进行调试、一旦被用来做恶意攻击时，它就变成了威胁。对付陷门最好的方法就是程序交付时进行关闭。

2. 逻辑炸弹

逻辑炸弹是在病毒和蠕虫之前最古老的程序威胁之一，它是嵌入在程序里面的一段待机发作（满足激活条件）的代码，和病毒一样具有明显的潜伏性。一旦触发，它就可能改变或删除数据或文件、引起机器关机或完成某种特定的破坏工作。

3. 特洛伊木马

特洛伊木马是一个有用的，或表面上有用的程序或命令过程，包含了一段隐藏的、激活时进行某种不想要的或者有害的功能的代码。它会破坏数据直至破坏数据文件，是一种

非常常见的病毒攻击方式。

4. 蠕虫

网络蠕虫程序是一种使用网络连接从一个系统传播到另一个系统的感染病毒程序。它一旦被激活，就表现得像计算机病毒或细菌，或者可以注入特洛伊木马程序，或者进行任何次数的破坏或毁灭行动。

5. 细菌

计算机中的细菌是一些并不明显破坏文件但不停复制自身的程序，它通过耗尽计算机所有系统资源(如 CPU，RAM，硬盘等)的方式使计算机瘫痪。

6. 病毒

病毒是一种复制到其他文件并且一旦被调入内存就继续复制的攻击性程序，它通常都具有破坏性作用，有些是故意的，有些则不是。比如 CIH 病毒，它是迄今为止发现的首例不仅破坏硬盘的引导区和分区表还直接破坏计算机系统硬件的病毒。

1.1.4 计算机网络威胁的潜在对手和动机

计算机网络所面临的威胁主要来自外部的人为因素和自然环境因素，它们包括对网络软硬件的威胁和对网络中信息的威胁。这些威胁的具体表现主要包括非法授权访问、假冒合法用户、病毒破坏、线路窃听、黑客入侵、干扰系统正常运行、修改或删除数据等。这些威胁大致可分为无意威胁和故意威胁两大类。

1. 无意威胁

无意威胁是指不是故意的条件下破坏系统的安全性、可靠性或信息的完整性。无意威胁主要是由一些偶然因素引起，如软硬件的机能失常、人为误操作、电源故障和自然灾害等。

软硬件的机能失常包括长时间开机引起硬件过热导致死机甚至硬件烧毁、软件长时间工作引起的死机等。

人为误操作包括：管理不善而造成系统信息丢失、设备被盗、发生水灾或火灾，安全设置不当而留下的安全漏洞，用户口令不慎暴露，信息资源共享设置不当而被非法用户访问等。

自然灾害威胁如地震、风暴、泥石流、洪水、闪电雷击、虫鼠害及高温、各种污染等构成的威胁等。

2. 故意威胁

故意威胁是指有意进行攻击。攻击者利用各种漏洞或者 bug 进行攻击，以破坏系统软硬件或者信息。

故意威胁中的攻击按照攻击的破坏方式与程度又可分为被动攻击和主动攻击。

(1) 被动攻击：被动攻击是指攻击者只通过监听网络线路上的信息流而获得信息内容，或获得信息的长度、传输频率等特征，以便进行信息流量分析攻击。被动攻击不干扰信息的正常流动，如被动地搭线窃听或非授权地阅读信息。被动攻击破坏了信息的机密性。

(2) 主动攻击：主动攻击是指攻击者对传输中的信息或存储的信息进行各种非法处理，有选择地更改、插入、延迟、删除或复制这些信息。主动攻击常用的方法有：篡改程

序及数据、假冒合法用户入侵系统、破坏软件和数据、中断系统正常运行、传播计算机病毒、耗尽系统的服务资源而造成拒绝服务等。主动攻击的破坏力更大，它直接威胁网络系统的可靠性、信息的机密性、完整性和可用性。

被动攻击不容易被检测到，因为它没有影响信息的正常传输，发送和接收双方均不容易觉察。但被动攻击却容易防止，只要采用加密技术将传输的信息加密，即使该信息被窃取，非法接收者也不能识别信息的内容。

主动攻击较容易被检测到，但却难于防范。因为正常传输的信息被篡改或被伪造，接收方根据经验和规律能容易地觉察出来。除采用加密技术外，还要采用鉴别技术和其他保护机制和措施，才能有效地防止主动攻击。

被动攻击和主动攻击有以下四种具体类型：

（1）窃取：非法获取信息，这是对信息保密性的威胁，例如通过搭线捕获线路上传输的数据等。

（2）中断：非法停止信息的传输，这是对信息可用性的威胁，例如破坏存储介质、切断通信线路、侵犯文件管理系统等。

（3）篡改：非法改变信息，这是对信息完整性的威胁，例如修改文件中的数据、改变程序功能、修改传输的报文内容等。

（4）伪造：非法添加信息，这也是对信息完整性的威胁，如向网络用户发送虚假信息，在文件中插入伪造的记录等。

1.2　计算机网络不安全因素

一般来说，计算机网络本身的脆弱性和通信设施的脆弱性共同构成了计算机网络的潜在威胁。一方面，计算机网络的硬件和通信设施极易受自然环境和人为的物理破坏；另一方面，计算机网络的软件资源和数据信息易受到非法窃取、复制、篡改等。

1.2.1　不安全的主要因素

计算机网络不安全的主要因素包括：

（1）偶发因素：如电源故障、设备的功能失常及软件开发过程中留下的漏洞或逻辑错误等。

（2）自然灾害：各种自然灾害对计算机系统构成严重的威胁。

（3）人为因素：人为因素对计算机网络的破坏也称为人对计算机网络的攻击。它又可分为几个方面：被动攻击、主动攻击、邻近攻击、内部人员攻击、分发攻击等。

1.2.2　不安全的主要原因

1. 网络自身的不安全性

网络，特别是互联网，尤其是国际互联网也即因特网，因为其自身所具有的开放性、共享性、国际性的特点，既带来了无穷的便利，同时也给计算机网络安全提出了巨大的挑

战。互联网不安全性的原因主要有以下几点：

（1）网络的开放性：这主要指计算机网络硬件上的模块化、软件上的标准化，比如攻击网络通信介质、攻击网络通信协议、以及攻击计算机网络软件的漏洞。

（2）网络的国际性：计算机网络的开放性，带来了全球性的用户，这样，某一地方的网络，不仅攻击者可能是本地的，更多可能是外地以及外国的。

（3）网络的自由性：大多数的网络对用户的使用没有技术上的约束，用户可以自由的上网、发布和获取各类信息。

2. 操作系统存在的安全问题

操作系统自身的漏洞比如动态链接、创建进程、空口令和 RPC、超级用户等，使得操作系统并不如大众想象的那么安全。

3. 数据的安全问题

国际通用的数据库如 Oracle、SQL Server、MySQL、DB2 等本身存在的安全漏洞，数据库应用程序存在的漏洞以及 bug 等，都使得数据的安全始终存在隐患。

4. 传输的安全问题

各种存储器中存储大量的信息，这些存储介质很容易被盗窃或损坏，造成信息的丢失；存储器中的信息也很容易被复制而不留痕迹。

5. 网络安全管理的问题

网络安全管理不好、规章制度不健全、安全管理水平较低、操作失误、渎职行为等都会对计算机信息安全造成威胁。

另外，网络系统的脆弱性还表现为保密的困难性、介质的剩磁效应和信息的聚生性等。

1.3 计算机网络安全的概念

计算机网络安全的概念主要从计算机网络安全的定义、计算机网络安全的目标、计算机网络安全的层次三方面进行论述。计算机网络安全的定义即计算机网络安全概念的内涵，而计算机网络安全的目标以及计算机网络安全的层次均为计算机网络安全概念的外延，其中计算机网络安全的目标即计算机网络安全的存在意义，计算机网络安全的层次即计算机网络安全的具体内容。

1.3.1 计算机网络安全的定义

从不同的角度和层面，对计算机网络安全的认识也有不同的理解，但是基本上是大同小异的。

有人认为，计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。计算机网络安全包括两个方面，即物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻

辑安全包括信息的完整性、保密性和可用性。

与之稍有不同的认识是：计算机网络安全是指利用管理控制和技术措施，保证在一个网络环境里信息数据的机密性、完整性及可使用性得到保护。从广义上说，网络安全包括网络硬件资源和信息资源的安全性。硬件资源包括通信线路、通信设备(交换机、路由器等)、主机等，要实现信息快速、安全地交换，一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件，以及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性、真实性等是网络安全研究的重要课题。

也有人认为：计算机网络安全不仅包括组网的硬件、管理控制网络的软件，也包括共享的资源，快捷的网络服务，所以定义网络安全应考虑涵盖计算机网络所涉及的全部内容。参照 ISO 给出的计算机安全定义，认为计算机网络安全是指："保护计算机网络系统中的硬件，软件和数据资源，不因偶然或恶意的原因遭到破坏、更改、泄露，使网络系统连续可靠性地正常运行，网络服务正常有序。"

同样类似的说法是：计算机网络安全的定义包含物理安全和逻辑安全两方面的内容，其逻辑安全的内容可理解为通常所说的信息安全，是指对信息的保密性、完整性和可用性的保护，而网络安全性的含义是信息安全的引申，即网络安全是对网络信息保密性、完整性和可用性的保护。计算机网络安全是指"为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄漏"。

综上所述，计算机网络安全是指利用技术与非技术手段，使得计算机网络系统中的硬件、软件以及信息资源不被破坏、攻击、窃取的相关内容。而作为一门课程，计算机网络安全是一门涉及计算机科学、计算机网络技术、密码技术、信息安全技术、应用数学、数论和信息论、控制论、系统论等多种学科的综合性学科。从广义来说，凡是涉及计算机网络上硬件、软件以及信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是计算机网络安全的研究领域。

1.3.2　计算机网络安全的目标

由计算机网络安全的定义即计算机网络安全的内涵可知，计算机网络安全的目标即保证计算机网络上硬件、软件以及信息这三种主要资源的保密性、完整性、真实性、可用性和可控性。

具体阐述如下。

1. 机密性(confidentiality)

机密性是指计算机网络系统中的硬件、软件以及信息不泄漏给非授权用户、实体或过程，或供其利用的特性。机密性就是保证具有授权用户可以访问计算机网络系统中的硬件、软件以及信息，而限制其他人对硬件、软件以及信息的访问。机密性分为网络传输保密性和信息存储保密性。

机密性的主要实现技术包括：

(1) 保证计算机网络不被非授权者获取与使用、保证计算机网络系统不以电磁方式向外泄露信息的电磁屏蔽技术、加扰技术。