



普通高等教育“十三五”计算机类规划教材

网络安全技术

◎ 刘化君 等编著

Wangluo
Anquan Jishu

第2版



机械工业出版社
CHINA MACHINE PRESS

普通高等教育“十三五”计算机类规划教材

20882 协同软件技术及应用	汤 庸 冀高峰 朱 君
20998 形式语言与自动机理论 (免费电子课件)	吴哲辉 吴振寰
22780 数据库原理及应用 (免费电子课件)	胡孔法
29294 数据库原理及应用学习与实验指导教程	胡孔法 汤克明 纪兆辉
49704 计算机专业英语 (第2版)	霍宏涛
48888 微机原理与接口技术 (第2版) (免费电子课件)	吉海彦
22750 IBM-PC汇编语言程序设计 (免费电子课件)	余朝琨
22779 C#.NET程序设计 (免费电子课件)	李 旗
22781 ATmega系列单片机原理及应用——C语言教程 (免费电子课件)	海 涛
30707 数字电子技术基础 (免费电子课件)	王友仁 陈则王 洪春梅
30716 数字电子技术基础学习指导与习题解析	王友仁 陈则王 林 华
23185 计算机网络技术与应用 (免费电子课件)	刘 冰
23200 多媒体技术基础及应用 (免费电子课件)	刘 建
23201 数据结构 (免费电子课件)	戴 敏
10423 计算机文化基础教程 (第2版) (免费电子课件)	吕昌玲
23298 电路与电子技术基础 (第2版) (免费电子课件)	李心广 王金矿 张 晶
48218 电路与电子技术基础学习指导与实验教程 (第2版)	李心广 等
25355 信号与系统 (免费电子课件)	王玲花
23502 Visual Basic程序设计 (免费电子课件)	王怀彬
23535 离散数学及其应用 (免费电子课件)	魏雪丽
23846 C++程序设计 (免费电子课件)	张 桦
24309 数字化摄影技术 (免费电子课件)	穆 强
24707 算法设计方法 (免费电子课件)	吴哲辉 崔焕庆 马炳先
24919 计算机网络与Internet实验教程 (免费电子课件)	吴振寰
44703 Access数据库基础及应用教程 (第3版) (免费电子课件)	郭银章
45056 Access数据库基础及应用教程学习指导	米红娟
46506 C++程序设计基础教程 (免费电子课件)	刘厚泉 李政伟
32663 C++程序设计与应用实验指导及习题解答	周仲宁
26109 实用软件工程教程 (免费电子课件)	陈雄峰
26371 信号与系统 (免费电子课件)	郭银景
26761 网络编程与计算技术 (免费电子课件)	刘化君
49936 网络安全技术 (第2版) (免费电子课件)	刘化君
26868 汇编语言与计算机系统组成 (免费电子课件)	李心广 张建民 潘智刚等
29458 现代科技信息检索 (第2版) (免费电子课件)	林 燕
30130 C程序设计教程 (免费电子课件)	戴水贵 敖志刚 俞海英
30212 Java 2 程序设计 (免费电子课件)	刘英华
30824 计算机网络 (免费电子课件)	高殿武
31122 软件工程基础与实例分析 (免费电子课件)	王阿川
31261 编译原理及实现技术 (第2版) (免费电子课件)	刘 磊
31698 计算机图形学 (第2版) (免费电子课件)	徐长青 许志闻 郭晓新等
32552 计算机软件技术实训教程	冯元椿
39125 C#程序设计基础 (免费电子课件)	伍 星 熊 壮
40228 微机原理、汇编语言与接口技术 (免费电子课件)	韩晓茹
40667 网页设计与制作应用教程 (第2版) (免费电子课件)	王任华
43444 网络基础与信息安全 (免费电子课件)	王建刚 钱宗峰
44898 Linux系统应用基础教程 (第2版) (免费电子课件)	张小进
47287 计算机应用基础 (第2版) (免费电子课件)	钱宗峰 李晓辉
48543 单片机原理与项目实践——基于C语言	钱宗峰 刘培国 于 飞

地址：北京市百万庄大街22号
 邮政编码：100037

电话服务
 服务咨询热线：010-88379833
 读者购书热线：010-88379649

网络服务
 机工官网：www.cmpbook.com
 机工官博：weibo.com/cmp1952
 教育服务网：www.cmpedu.com
 金书网：www.golden-book.com
 封面防伪标均为盗版

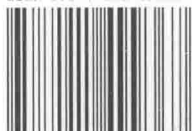


机工教育微信服务号

ISBN 978-7-111-49936-7

策划编辑◎刘丽敏 / 封面设计◎张静

ISBN 978-7-111-49936-7



9 787111 499367 >

定价：55.00元

普通高等教育“十三五”计算机类规划教材

网络安全技术

第2版

刘化君 等编著



机械工业出版社

本书内容共9章,包含网络安全理论、网络攻击与防护、网络安全应用及网络安全实验4个部分。网络安全理论部分介绍网络安全的基础知识、网络安全体系、TCP/IP的安全性以及系统平台安全等。网络攻击与防护部分从攻与防两个角度讨论网络安全技术,包括网络侦察、DoS/DDoS攻击、缓冲区溢出、欺骗攻击、防火墙、入侵检测、恶意代码防范与应急响应,以及网络攻击取证与安全审计等。网络安全应用部分讨论密码技术在网络安全中的应用、IP安全、VPN、安全电子邮件、Web安全技术和云计算安全。网络安全实验部分从搭建网络安全实验环境开始,分11个实验项目比较全面地呈现攻与防技术,使课程理论与实践紧密地结合起来。

本书内容丰富,技术性强,实现了网络安全理论与应用的完美结合,给读者以实用和最新的网络安全技术。

本书适用范围广,既可作为高等院校网络安全课程的教材和教学参考书,又可作为政府、企事业单位网络安全培训教材或参考书;对于具有一定网络管理、网络安全基础,并希望进一步提高网络安全技术水平的读者,也是一本理想的技术参考书。

图书在版编目(CIP)数据

网络安全技术/刘化君等编著.—2版.—北京:机械工业出版社,2015.4
普通高等教育“十三五”计算机类规划教材
ISBN 978-7-111-49936-7

I. ①网… II. ①刘… 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(2015)第074369号

机械工业出版社(北京市百万庄大街22号 邮政编码100037)
策划编辑:刘丽敏 责任编辑:刘丽敏 吴晋瑜 吴超莉
版式设计:赵颖喆 责任校对:聂美琴
封面设计:张静 责任印制:刘岚
北京圣夫亚美印刷有限公司印刷
2015年6月第2版第1次印刷
184mm×260mm·27印张·735千字
0001—2000册
标准书号:ISBN 978-7-111-49936-7
定价:55.00元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

电话服务

网络服务

服务咨询热线:010-88379833

机工官网:www.cmpbook.com

读者购书热线:010-88379649

机工官博:weibo.com/cmp1952

教育服务网:www.cmpedu.com

封面无防伪标均为盗版

金书网:www.golden-book.com

前言

网络安全正面临着严峻的挑战,一方面是互联网规模扩大和关键应用的剧增,如电子政务、电子商务、电子支付与网络银行等网络应用业务的飞速发展,对网络安全的需求提高;另一方面是网络安全攻击的持续不断,安全威胁形式变化多样,给网络应用的健康发展带来巨大障碍。因此,网络安全问题已成为人们普遍关注的问题,网络安全技术也成为信息技术领域的重要研究课题。为适应网络安全技术发展及其课程教学需要,决定对《网络安全技术》第1版进行全面修订。

考虑到网络安全技术的新发展,结合一线教师和学生的反馈意见,本书第2版对上一版教材的内容进行了适当的调整和补充,主要包括:对内容的系统性进行了修订,如调整了网络安全体系结构,使之在体系上更科学,在逻辑上更合理;针对网络安全对内容实效性要求高的特点,对网络安全技术的实效性进行检查和更新,删除了一些陈旧的知识,增加了当前最新的技术和发展动态,包括网络访问控制、网络存储备份、云计算安全,以及软件定义网络(SDN)的安全、物联网安全保障等,保持了网络安全技术的先进性;更加突出实验、实践能力的培养,将原第3章网络协议的安全性改写为网络协议安全性分析,更新了网络安全实验题目和方法,进一步凸显了理论与实践的紧密结合,使读者能够更好地结合实际应用进行学习。

本书仍然保持了第1版的内容体系结构,内容共9章,分为网络安全理论、网络攻击与防护、网络安全应用、网络安全实验4个大部分,涵盖了攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)等多方面的基本理论和技术。网络安全理论部分介绍网络安全的基础知识、网络安全体系结构、网络协议安全性分析、网络系统平台安全等。网络攻击与防护部分从攻与防两个角度讨论网络安全技术,包括网络信息收集技术、欺骗攻击及防范、DoS/DDoS攻击、缓冲区溢出攻击、网络资源访问控制、防火墙技术、入侵检测技术、恶意代码防范与应急响应,以及网络攻击取证与安全审计等内容。网络安全应用部分首先介绍密码技术在网络安全中的应用,然后重点讨论IP安全、虚拟专用网技术(VPN)、Web安全技术、云计算安全。网络安全实验部分从搭建网络安全实验环境开始,分11个实验项目介绍网络攻与防实验技术,使课程理论与实践紧密地结合起来。

本书这次修订在保持第1版体例结构、编著特色的基础上,进一步彰显了理论与实践紧密结合的工程应用性特色,主要特点如下。

1) 内容丰富,科学合理,搭建了一个有机的知识体系。在教学内容选取方面进行了深入的考虑,遵照循序渐进的基本原则构建了一条知识链;在协调内容的深度、广度、难度的关系时,充分考虑学生的基础和能力的,使之能够适应普通高等教育专业教学需要;在理论与应用知识的比例方面,在保持科学性和实用性的同时,使理论与技术相得益彰。

2) 理论与实践密切结合,侧重实践能力的培养。网络安全课程的宗旨是培养学生在信息存储、传输和处理过程中所应具备的解决安全问题的能力,是一门实践性很强的课程。本书将大量网络安全实例融合到理论阐释之中,实现了理论指导下的实践,实践基础上的理论提升。更为重要的是精选了11个实验项目并单列一章,从实验环境搭建到网络安全攻防多个层面,将网络安全实践能力培养提高到了一个新的水平。



3) 言简意赅, 清楚易懂, 理论阐述严谨、透彻, 技术讨论翔实、细致。在编写过程中, 融入学科方法论, 倡导科学的思维方法, 通过大量的图表, 形象直观地讲解了知识概念。

本书可作为高等院校信息安全、计算机类、电子信息类各专业本科生和研究生的教材或教学参考书, 也可作为政府、企事业单位网络安全培训教材或参考书; 对于具有一定网络管理、网络安全基础, 并希望进一步提高网络安全技术水平的读者, 仍是一本理想的技术参考书。

本书由杨洁(南京工程学院)执笔编写第4章、第9章, 并对本书提出了许多具体的修订意见, 钱骁执笔撰写第6章中的网络访问控制部分的初稿, 顾礼峰执笔改写了第9章中的9.1节和实验11基于路由器VPN安全配置等内容, 其余各章节由刘化君执笔编撰。全书由刘化君统编定稿。在编写过程中, 许多研究生如邓大为等同学也参与了相关工作。在本书编写过程中参阅了大量中外文献及安全网站, 从中获得了许多启示和帮助, 在此一并表示衷心感谢!

网络安全是一个内容广博、不断发展的技术领域。在本书的编撰过程中, 尽管编者力求精益求精, 及时吸纳最新的网络安全研究成果及技术, 但由于编者理论水平和实践经验所限, 书中的疏漏和不足之处在所难免, 敬请广大读者批评指正。

编者

目 录

前言

第 1 章 绪论 1

1.1 何谓网络安全 1

1.2 网络安全风险分析与评估 6

1.3 网络安全策略 12

1.4 网络安全的关键技术 15

1.5 网络安全技术研究与发展 20

小结与进一步学习建议 23

思考与练习 24

第 2 章 网络安全体系结构 25

2.1 OSI 安全体系结构 25

2.2 网络安全模型 31

2.3 可信计算 34

2.4 网络安全标准及管理 39

小结与进一步学习建议 45

思考与练习 46

第 3 章 网络协议安全性分析 47

3.1 网络协议分析 47

3.2 网络接口层的安全性 59

3.3 网络层协议的安全性 61

3.4 传输层协议的安全性 67

3.5 应用层协议的安全性 76

3.6 TCP/IP 体系安全性能的改进 81

小结与进一步学习建议 84

思考与练习 85

第 4 章 网络系统平台安全 86

4.1 网络的物理与环境安全 86

4.2 操作系统的安全 92

4.3 数据备份与恢复 115

小结与进一步学习建议 128

思考与练习 129

第 5 章 网络攻击原理及技术 130

5.1 网络攻击 130

5.2 网络信息收集技术 137

5.3 网络监听 154

5.4 欺骗攻击及防范 168

5.5 DoS/DDoS 攻击 177

5.6 缓冲区溢出攻击 182

5.7 Web 服务欺骗攻击及防范 192

小结与进一步学习建议 197

思考与练习 198

第 6 章 网络安全防护技术 199

6.1 网络资源访问控制 199

6.2 防火墙技术 209

6.3 入侵检测技术 231

6.4 恶意代码防范与应急响应 243

6.5 网络攻击取证与安全审计 262

小结与进一步学习建议 268

思考与练习 269

第 7 章 密码技术应用 270

7.1 密码技术概要 270

7.2 典型密码算法简介 276

7.3 认证技术 283

7.4 公开密钥基础设施 293

小结与进一步学习建议 301

思考与练习 302

第 8 章 网络安全应用 303

8.1 IP 安全 303

8.2 虚拟专用网技术 311

8.3 安全电子邮件 327

8.4 Web 安全技术 336

8.5 云计算安全 343

小结与进一步学习建议 349

思考与练习 350

第 9 章 网络安全实验 351

9.1 网络安全实验环境搭建 351

9.2 操作系统安全配置实验 358

9.3 网络安全攻击技术实验 371

9.4 网络安全防护技术实验 385

参考文献 424

第1章 绪论

信息网络的迅速发展普及应用,在给人们的工作、生活带来巨大便利的同时,也带来了许多安全隐患,出于政治、经济、文化等利益的需要或者好奇心的驱动,网络攻击事件层出不穷、屡见不鲜,且有愈演愈烈之势;轻者会给个人或机构带来信息损害和经济利益损失,重者将会影响国家的政治、经济和文化安全。因此,信息网络安全问题已成为国内外重大的研究课题之一。

信息网络安全是一个非常复杂的综合性问题,涉及包括技术、产品和管理在内的诸多因素。网络安全主要研究信息网络安全理论、安全应用和安全管理技术,确保网络免受各种威胁和攻击,以便能够正常工作。本章主要介绍网络安全的基本概念、网络安全风险及其评估、网络安全策略;并讨论信息网络安全研究的主要内容、关键技术以及发展趋势。

1.1 何谓网络安全

互联网技术的普及应用,使得信息突破了时间和空间上的障碍,信息的价值在不断提高。然而,计算机技术、网络技术及信息技术也与其他科学技术一样是一把双刃剑。在大部分人使用信息技术提高工作效率,为社会创造更多财富的同时,也有一些人在利用信息技术做着相反的事情。他们非法侵入他人的计算机系统窃取机密信息、篡改和破坏数据,给社会造成了难以估量的巨大损失。网络安全日渐成为关系国计民生的大事,已经引起了全社会的高度重视。网络安全涉及网络和通信,并不像初次接触这个领域的人想象的那样简单。网络安全所涉及的内容很多,下面先介绍一些有关信息安全、网络安全的基本概念。

1.1.1 安全的历史回顾

“安全”一词通常被理解为“远离危险的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击或逃跑而采取的措施”。这是在广泛意义上对安全的表述。对信息技术而言,纵观其快速发展与广泛的应用,信息安全的含义也有一个不断丰富和发展的过程。根据社会对信息安全的需求,它经历了三个重要的发展阶段。

第一个阶段是通信安全阶段,这一历史时期比较长。早在远古时代,就有了信息安全的概念。那时,所有资产都是物理的,重要的信息也是物理的,如将文字刻在石头上、竹片上,到后来写在纸张上。保护这种信息,也是采取一些物理性的手段,如深藏密窖、护卫把守等。这时信息传递通常也只能用信使完成,飞鸽传书也算是一种信息传递方式。物理安全存在许多安全缺陷,如果报文在传递过程中被截获,报文的信息就会被敌人知悉,因此产生了通信安全问题。早在公元前600年,Julius Caesar发明了凯撒密码(Caesar Cipher),从此,敌方即使截获了报文,也无法读懂。此后,加密报文这个概念得到了迅速发展与应用,一直到目前的量子密码。与此同时,军事通信也开始使用密码技术,即将每个字符编码后放入报文传输。敌人即使通过无线电通信手段窃听、截获到报文,也无法识别其含义。在这一时期,通信安全的主要任务是解决数据传输的安全问题,所采取的主要措施是密码技术。

到了20世纪中期,在广泛使用计算机等数据处理设备之前,主要依靠物理和行政手段来保障重要信息的安全。所采用的物理手段主要是将重要的文件资料存放在带有密码锁的文件柜或保

密室里；行政手段则是通过制订强有力的管理措施，对工作人员加强检查和限制。这时的信息安全技术尚处于原始工具阶段。

第二个阶段是计算机系统信息安全时期。当计算机技术普及之后，信息被以电子形式移植到计算机系统中，而计算机系统里的信息对任何访问者都是开放的。显然，存放在计算机系统里的文件和其他一些信息，需要一种自动工具来保护。这些自动工具（诸如分时共享系统、通过公共电话网或互联网可访问的系统等）可作为保护数据信息和阻止攻击者实施破坏行为的工具，因此便产生了计算机系统信息安全，简称计算机安全或信息安全。计算机安全的主要任务是解决计算机信息载体及其运行的安全问题；采取的主要措施是根据主、客体的安全级别，正确实施主体对客体的访问控制。

第三个发展阶段是信息安全保障，即网络系统安全阶段。当通过网络把分布在不同地理位置的计算机系统连接起来后，网络用户也来自社会各个阶层与部门，如何保护在网络中大量存储和传输的数据就越来越重要了，因此网络安全应运而生，并迅速发展起来。网络安全的主要任务是解决计算机信息载体及其运行的安全问题；采取的主要措施是提供完整的信息安全保障体系，包括防护、检测、响应和恢复。

实际上，对于计算机安全和网络安全并没有明确的界限，例如，对信息系统最常见的攻击是计算机病毒，它可能已经感染移动存储介质（如磁盘、U 盘），然后再加载到计算机上，从而进入系统；也可能是通过互联网进入系统。无论哪一种情况，一旦病毒驻留在计算机系统中，就需要内部计算机安全工具来查杀病毒并恢复数据。

信息安全的继续发展是物联网的安全保障，即物联网安全阶段，也就是第四个阶段。物联网被称为继计算机、互联网与移动通信网之后的又一次信息产业浪潮。在物联网时代，人类会将基本的日常管理交给人工智能去处理，继而从烦琐的低层次管理中解脱出来，将更多的人力、物力投入到新技术的研发中。因此，物联网的信息安全也将更为重要。

1.1.2 信息安全

进入 21 世纪，信息技术给人们的生活、工作带来了数不尽的便捷和好处。与此同时，网页篡改、计算机病毒、系统非法入侵、信息泄漏、网站欺骗、拒绝服务、非法利用漏洞等信息安全事件时有发生，从而不断突显出信息安全的重要性。信息与信息系统安全现在已经成为一门新兴学科，而且是一门边缘交叉性学科，涉及通信技术、计算机科学、计算机网络、信息论、数论、密码学、人工智能及社会工程学等。

1. 信息安全的定义

由信息安全技术的发展过程可以知道，信息安全的内涵是在不断丰富和发展的。国际标准化组织（ISO）将计算机系统信息安全（Computer System Security）定义为“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、更改和泄露”，这一定义偏重于静态信息保护。因此，可将计算机系统信息安全进一步定义为“计算机的硬件、软件和数据得到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行”，这一定义侧重了动态意义的描述。显然，“安全”一词是指将服务与资源的脆弱性降到最低限度，其中脆弱性是指计算机信息系统的任何弱点。

信息安全涵盖的内容比较丰富，包括操作系统安全、网络安全、病毒查杀、访问控制、加密与认证以及数据库安全等多个方面。

2. 信息安全的属性

美国国家信息基础设施（NII）的文献给出了信息安全的 5 个属性：可用性、可靠性、完整

性、机密性和不可抵赖性。这5个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛领域。

1.1.3 网络安全

20世纪90年代以来,计算机网络技术得到了飞速发展,信息的处理和传输突破了时间和地域的限制,网络化与全球化成为不可抗拒的世界潮流,互联网进入了社会生活的各个领域和环节。随着计算机的网络化和全球化,人们日常生活中的许多活动已逐步转移到网络中,然而,安全却是计算机网络尤其是互联网技术中的一个薄弱环节。

1. 网络安全的定义

假若A和B要应用网络进行通信,并希望该网络及其通信过程是“安全”的。在这里,A和B可以是两台需要安全交换路由表的路由器,也可以是希望建立一个安全传输连接的客户端和服务端,或者是交换安全电子邮件的应用程序,因此,可把A和B看作两个网络通信实体,即应用进程。A和B要进行网络通信并希望做到“安全”,那么,此处的安全意味着什么呢?显然,这个“安全”的内涵是丰富多彩的,且涉及多个方面。譬如,A和B希望存储在客户端或服务端中的数据不被破坏、篡改、泄露;它们之间的通信内容对于窃听者是保密的,而且在通信时,的确是在与真实的对方在进行;它们还希望所传输的内容即使被窃听者窃取了也不能理解其报文的含义;还要确保它们的通信内容在传输过程中没有被篡改;即使被篡改了,也应该能够检测到该信息已经被篡改、破坏。由此归纳起来,可以给出网络安全(Network Security)的定义:网络安全就是在分布式网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护,以防数据、信息内容遭到破坏、更改、泄露,或网络服务中断或拒绝服务或被非授权使用和篡改。

对网络安全内涵的理解会随着“角色”的变化而有所不同,而且在不断地延伸和丰富,比如,从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免被他人利用窃听、冒充、篡改、抵赖等手段侵犯自身利益。

从网络运行和管理者角度说,他们希望对本地网络信息的访问、读写等操作受到保护和控制,避免出现陷门(后门)、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。

对安全保密部门来说,他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄露,避免对社会产生危害,对国家造成巨大损失。

从社会教育和意识形态角度来讲,网络上不健康的内容,会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

可见,网络安全的内涵与其保护的信息对象有关,但本质都是在信息的安全期内保证在网络上传输或静态存放时允许授权用户访问,而不被未授权用户非法访问。因此,网络安全与信息安全的研究领域是交错与关联的。

网络安全涉及的内容既有安全理论、安全应用技术等方面的问题,还有社会、教育、法律等管理问题,这几个方面相互补充,缺一不可。技术方面主要侧重于防范非法用户的攻击,管理方面则侧重于防范人为因素的破坏。如何更有效地保护重要的数据信息、提高网络系统的安全意识,已经成为网络安全必须考虑和解决的重要问题之一。

2. 网络安全的特性

网络安全具有信息安全的基本属性。从其本质上来讲,网络安全就是要保证网络上信息存储

和传输的安全性。根据网络安全的定义,网络的安全具有下述几个特性。

(1) 机密性

机密性 (Confidentiality) 是指网络通信中的信息,仅能由发送者和预定的接收者所理解。即便窃听者截获了报文,也会因为报文在一定程度上进行了加密处理(即进行了数据伪装)而不能解密(即理解)所截获报文的含义。这里所指的报文不但包括国家秘密,而且也包括各种社会团体、企业组织的工作秘密、商业秘密和个人私密(如浏览习惯、购物习惯)。防止信息失窃和泄露的保障技术称为保密技术。在网络的不同层次上,有不同的机制来保障机密性;在物理层上,主要是采取电磁屏蔽技术、干扰及跳频技术来防止电磁辐射造成的信息外泄;在网络层、传输层及应用层,主要采取加密、访问控制、审计等方法来保障信息的机密性。

(2) 认证

认证 (Authentication) 是指发送者和接收者都应该能证实网络通信过程中所涉及的另一方,确信通信的另一方确实具有它们自己所声称的身份。人类面对面通信可以通过视觉很轻松地解决这个问题,但当通信实体在不能看到对方的媒体上交换信息时,认证就比较复杂了。认证是网络通信系统安全的基础。

(3) 完整性

完整性 (Integrity) 是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程,并且能够判别出实体或进程是否已被篡改,即信息的内容不能被未授权的第三方修改;数据在存储或传输的过程中不被修改、破坏,不出现数据包的丢失、乱序等。

(4) 不可否认性

不可否认性 (Non-Repudiation) 也称为不可抵赖性。不可否认性是面向通信双方(人、实体或进程)信息真实统一的安全要求,它包括收、发双方均不可抵赖。一是源节点发送证明,它是提供给信息接收者的证据,使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞;二是交付证明,它是提供给信息发送者的证据,使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

(5) 可用性

可用性 (Availability) 是指可被授权实体访问并按需求使用的特性。安全通信的一个关键要求就是首先能够进行通信,无论在何时,只要用户需要,网络通信系统必须是可用的,也就是说,网络通信系统不能拒绝服务。然而,用户的通信需求是随机的、多方面的(语音、数据、文字和图像等),有时还要求时效性,网络必须随时满足用户通信的要求。攻击者通常采用占用资源的手段阻碍授权者的工作,例如,网络环境下的拒绝服务、破坏网络系统的正常运行等都属于对可用性的攻击。可以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。增强可用性还包括如何有效地避免因各种灾害(战争、地震等)造成的系统失效。

(6) 可靠性

可靠性 (Reliability) 是指系统在规定条件下和规定时间内完成规定任务的概率。可靠性是网络安全最基本的要求之一,网络不可靠,故障不断,就谈不上网络的安全。目前,对于网络可靠性的研究基本上偏重于硬件的可靠性。除了研制高可靠性的元器件设备以外,采取合理的冗余备份措施仍是最基本的可靠性对策。另外,许多网络故障与软件可靠性、人员可靠性和环境可靠性也有直接关系。

(7) 可控性

可控性 (Controllability) 是指网络对信息的传播应具有控制能力,确保仅允许拥有适当访问

权限的实体以定义明确的方式,对访问权限内的资源进行访问。

机密性、完整性、认证和不可否认性将在相当长的时期内仍是安全通信的关键特性。可用性、可靠性和可控性则是对安全通信概念的最新扩展,是为保证网络基础设施安全免受攻击而提出的。

3. 网络安全是一个系统

由上述对网络安全定义及其特性的讨论可知,网络安全的内涵主要集中在对通信和网络资源的保护方面。实际上,网络安全不仅涉及安全防护,还涉及入侵检测、应急响应以及数据灾难备份与恢复等内容。在许多情况下,作为对攻击的响应,网络管理员需要设置附加的保护机制和措施。同时,网络攻击技术也应包含在网络安全研究的范畴之中。只有对网络攻击技术有比较深刻的了解,才能做好网络安全工作。因此,ITU-T X.800 标准认为:网络安全包括安全攻击 (Security Attack)、安全服务 (Security Service) 和安全机制 (Security Mechanism) 等方面,并在逻辑上分别进行了定义。安全攻击是指损害机构所拥有信息安全的任何行为;安全服务是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全性的服务;安全机制是指用于检测、预防安全攻击或者恢复系统的机制。在这种意义上,网络安全是通过循环往复的保护、攻击、检测和响应而实现的。

由此看来,网络安全不仅研究安全防护技术,还研究网络攻击技术以及用于防御这些攻击的对策。从网络系统安全的角度考虑,网络安全攻防技术包括防护技术和攻击技术两大类,如图 1-1 所示。

对于不同环境和应用中的网络安全,还可以将其划分为以下几个方面。

1) 运行系统安全,即保证数据处理和传输系统的安全。它侧重于保证系统的正常运行,避免因为系统的崩溃和损坏而对系统存储、处理和传输的数据造成破坏和损失;避免由于电磁泄漏,产生信息泄露,干扰他人或受他人干扰。

2) 网络系统信息的安全,包括用户口令认证、用户存取权限控制、数据存取权限、访问方式控制、安全审计、安全问题跟踪、计算机病毒防治和数据加密等。

3) 网络信息的健康性,包括信息过滤等,主要指防止和控制非法、不健康的信息自由传输,抑制公用网络信息传输失控。

4) 网络上信息内容的安全,主要侧重于保护信息的机密性、真实性(认证)和完整性。避免攻击者利用系统漏洞实施篡改、泄露、窃听、冒充、欺骗等破坏行为。

根据以上对网络安全定义的讨论可知,网络安全是一个系统。它不是防火墙、不是入侵检测、不是虚拟专用网,也不是加密、认证、授权以及审计。安全也不是网络设备公司及其任何合作伙伴或竞争对手能够为用户提供的任何东西。尽管这些产品、技术在其中扮演着十分重要的角色,但网络安全的概念更为宽泛。网络安全始于安全策略,还涵盖了必须遵守这些安全策略的人以及实施这些策略的人。那么,对于网络安全来说什么是系统呢?网络安全系统是指通过相互协作的方式为信息资产提供安全保障的全体网络产品、技术、策略以及最优做法的集合。因此,从狭义的角度看,网络安全是指防护网络系统和信息资源不受自然和人为有害因素的威胁和危害。若从广义的角度讲,凡是与网络上信息的机密性、完整性、认证、可用性、可控性、不可否认性

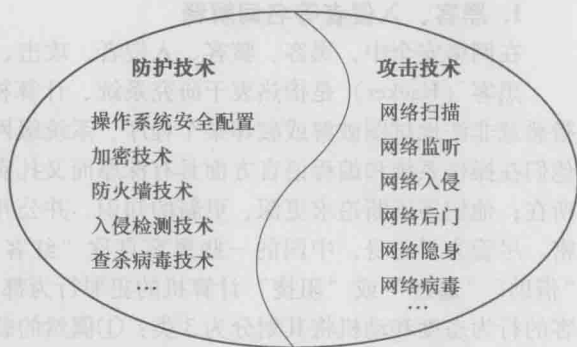


图 1-1 网络安全攻防技术