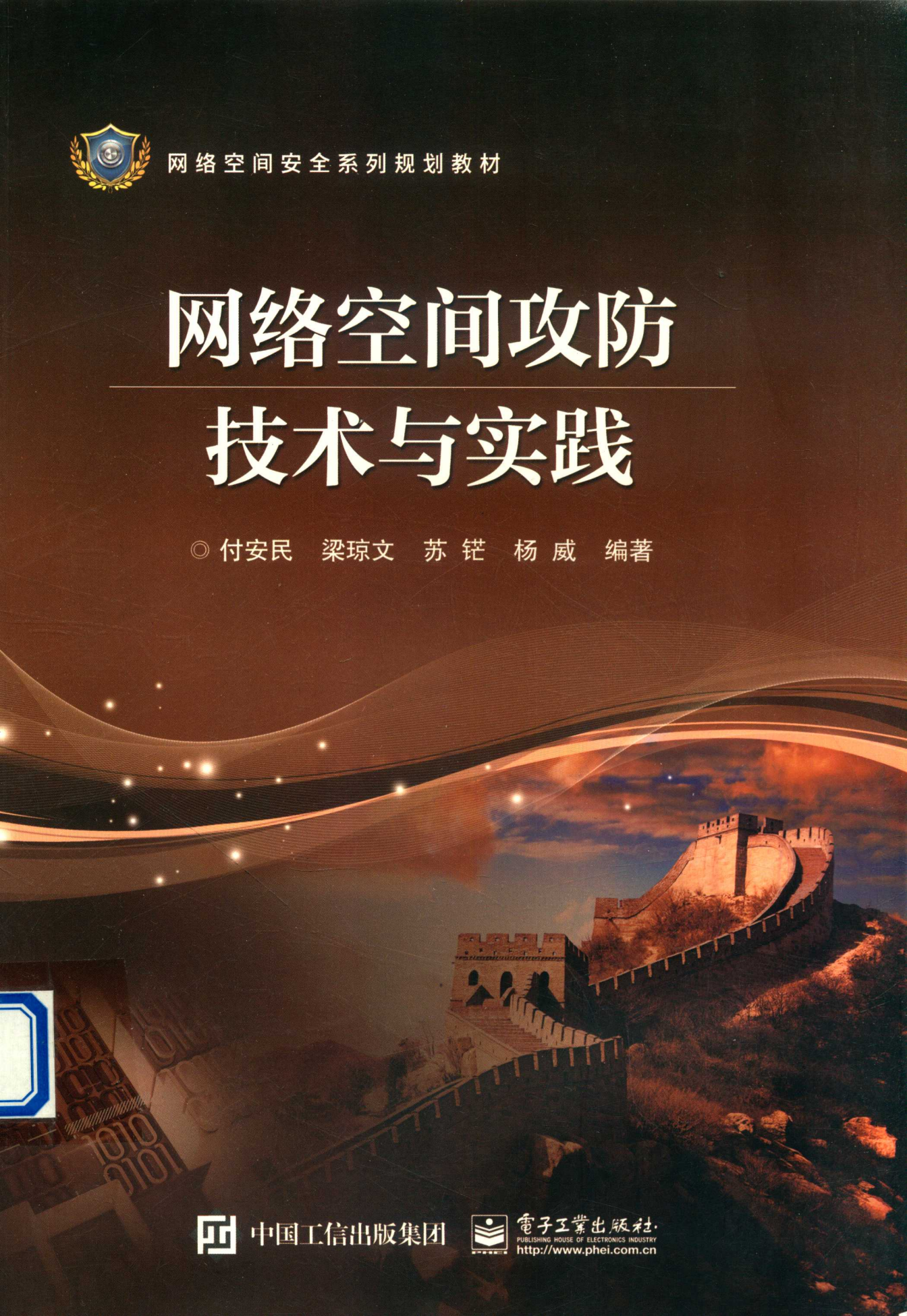
网络空间安全系列规划教材

网络空间攻防技术与实践

◎ 付安民　梁琼文　苏铓　杨威　编著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列规划教材

网络空间攻防技术与实践

付安民　梁琼文　苏　铠　杨　威　编著

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

内 容 简 介

本书从网络空间攻防基础知识入手，由浅入深地系统介绍了网络扫描与网络嗅探、口令破解、网络欺骗、拒绝服务、恶意代码、缓冲区溢出、Web 应用等的典型网络空间攻防技术原理和方法，并阐述了侧信道攻防、物联网智能设备攻防和人工智能攻防等当前热门技术。此外，本书通过真实网络空间攻防案例阐述、知名安全工具展示、网络空间攻防活动与 CTF 竞赛分析等多种形式的介绍，引导读者在掌握网络空间攻防技术原理的基础上，通过动手实战，强化网络空间攻防实践能力。本书内容系统全面，贯穿了网络空间攻防所涉及的主要理论知识和应用技术，并涵盖了网络空间攻防技术发展的新研究成果，力求使读者通过本书的学习既可以掌握网络空间攻防技术，又能够了解本学科新的发展方向。

本书既可作为高等学校网络空间安全和信息安全等相关专业本科生及研究生的教材，也可作为从事网络与信息安全工作的工程技术人员和网络攻防技术爱好者的学习参考读物。

图书在版编目（CIP）数据

网络空间攻防技术与实践 / 付安民等编著. —北京：电子工业出版社，2019.12
ISBN 978-7-121-37952-9

Ⅰ. ①网… Ⅱ. ①付… Ⅲ. ①网络安全－高等学校－教材 Ⅳ. ①TN915.08

中国版本图书馆 CIP 数据核字（2019）第 255656 号

责任编辑：戴晨辰
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：787×1 092　1/16　印张：21.25　字数：561 千字
版　　次：2019 年 12 月第 1 版
印　　次：2019 年 12 月第 1 次印刷
定　　价：59.80 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）88254888，88258888。

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。

本书咨询联系方式：dcc@phei.com.cn。

前言 Preface

随着信息技术的高速发展，互联网已经成为人们生活中不可或缺的一部分。网络空间信息在存储、转发过程中涉及大量用户隐私数据及信息，这使网络空间安全变得尤为重要。因此，网络空间安全工作者要为用户提供强大的安全保障。然而，在保护网络空间安全的同时，黑客技术也在不断发展，各类攻击工具简便易用，造成网络空间攻击行为泛滥，对用户的隐私数据和信息产生了极大威胁。特别是，近年来计算机病毒、网络攻击、垃圾电子邮件、网络窃密、网络诈骗、虚假信息传播、知识侵权、隐私侵权，以及网络色情等网络违法犯罪问题日渐突出，严重威胁到我国的经济、文化发展和国家安全。

编写本书的目的是，帮助网络安全人员掌握网络空间安全的基础知识，熟悉网络空间攻防的方法和步骤，理解典型的网络空间攻防原理和方法，树立良好的网络空间安全法律意识。本书系统介绍了网络扫描与网络嗅探、口令破解、网络欺骗、拒绝服务、恶意代码、缓冲区溢出、Web 应用、侧信道等的典型网络空间攻防技术原理和方法，并阐述了物联网智能设备攻防和人工智能攻防等热门攻防技术。同时，本书还通过真实网络空间攻防案例阐述、知名安全工具展示、网络空间攻防活动与 CTF 竞赛分析等多种形式的介绍，引导读者在掌握网络空间攻防技术原理的基础上，通过动手实战，强化网络空间攻防实践能力。本书内容系统全面，贯穿了网络空间攻防所涉及的主要理论知识和应用技术，并涵盖了网络空间攻防技术发展的最新研究成果，力求使读者通过本书的学习既可以掌握网络空间攻防技术，又能够了解本学科新的发展方向。

本书共分 13 章，内容由浅入深。第 1 章主要介绍了网络空间安全基础知识，分析了网络空间安全的主要威胁，阐述了网络空间攻击过程，以使读者对网络空间攻防有一个初步认识。第 2 章对国内外网络空间安全的法律法规和一些网络空间安全违法典型案例进行了介绍和分析，目的是使读者树立正确的网络空间安全观。第 3 章至第 10 章分别对网络扫描与网络嗅探、口令破解、欺骗、拒绝服务、恶意代码、缓冲区溢出、Web 应用、侧信道等的典型网络空间攻防手段和技术进行了深入细致的阐述和分析，并结合具体真实的网络空间攻防案例或利用知名安全工具演绎的攻击过程，以加深和强化读者对各类攻击方法与原理的理解。第 11 章主要围绕物联网智能设备这个热门领域，分别从其面临的安全威胁和相应的攻防与检测手段两方面进行了介绍和分析。第 12 章则重点讨论和分析了近年来兴起的人工智能攻防技术，以常见的验证码破解为例，引出了传统的信息保护技术可能已经无法满足人们保护自身信息安全的需求，然后详细介绍了最近出现的攻击方式及相应的防御策略，并给出了具体的攻击技术及防御策略实例，了解这些攻击模式能够帮助读者更好地解决常见的安全漏洞。最后，讨论

和分析了使用人工智能技术设计滥用检测防御系统时可能遇到的问题及解决方案。第 13 章详细地介绍了世界顶级的网络空间安全攻防活动 Black Hat Conference、DEFCON、Pwn2Own 和 GeekPwn，以及国内流行的网络攻防赛事 CTF，并对一些经典的 CTF 赛题进行了深入的解析，以期引导读者在掌握网络空间攻防技术与原理的基础上，通过动手实战，强化网络空间攻防实践能力。

本书既可作为高等学校网络空间安全和信息安全等相关专业本科生及研究生的教材，也可作为从事网络与信息安全工作的工程技术人员和网络攻防技术爱好者的学习参考读物。

本书包含配套教学资源，读者可登录华信教育资源网（www.hxedu.com.cn）免费下载。

本书由付安民、梁琼文、苏铠和杨威在长期从事网络与信息安全教学与科研工作的基础上编写而成。在编写过程中，南京理工大学的张功萱教授、王永利教授、俞研副教授等提供了宝贵的建议和有益的帮助，608 教研室的骆志成、丁纬佳、曾凡健、朱一明、李雨含、吴介、况博裕等研究生为本书的资料收集和整理做了大量工作，电子工业出版社的戴晨辰编辑也为本书的出版做了大量的工作，在此对他们表示由衷的感谢。本书在编写过程中参考了国内外的有关文献，在此向相关作者致以真诚的敬意和衷心的感谢。

由于编者水平所限，书中难免存在缺点和错误，殷切希望广大读者批评指正。

编著者

目录

Contents

第 1 章　网络空间攻防技术概述

随着信息技术的高速发展，互联网已经成为人类生活不可或缺的一部分。网络空间信息在存储、转发过程中涉及大量用户隐私数据，这使网络空间安全变得尤为重要，因此网络空间安全工作者必须为用户提供强大的安全保障。然而，在保护网络空间安全的同时，黑客技术也在不断发展，各类攻击工具简便易用，造成网络空间攻击行为泛滥，对用户的隐私信息产生了极大威胁。因此，学习网络空间攻防技术、保护网络空间安全是保障现代社会稳步发展的重要内容。

1.1　网络空间安全基础知识

网络空间安全关系到国家重要基础设施、国防工业等的正常运转。近年来，为了确保国家网络空间安全，我国及美、英、德等国家不断加强在网络空间的战略部署，纷纷将网络空间安全提升为国家战略。

网络空间是继陆、海、空、太空之后的第五作战空间和“军事高地”，是人类活动的新领域，也是世界各国争相控制的重要领地，已经成为与经济、社会、政治、文化联系的纽带。目前，人们在网络空间领域对很多规律性和基础性问题缺乏足够的重视和清醒的认识。网络空间安全的研发缺乏科学方法和理论支撑。

1.1.1　网络空间的概念

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息时代。在信息时代，信息产业成为第一大产业。信息就像水、电、石油一样，与所有行业和所有人都相关，成为一种基础资源。信息和信息技术改变着人们的生活和工作方式。离开计算机、网络设备、电视机和手机等电子信息设备，人们将无法正常生活和工作。可以说在信息时代，人们生存在物理世界、人类社会和信息空间组成的三维世界中。

20 世纪 80 年代初，作家威廉·吉布森创造了“网络空间”这个术语，用它来描述包含大量可带来财富和权力信息的计算机网络。所谓的网络空间，是指将客观世界和数字世界交融在一起，让使用它的人感知一个由计算机产生的、现实中并不存在的虚拟世界，并且，这个充满情感的虚拟数字世界也影响着人类现实物质世界。尽管威廉·吉布森关于计算机模拟现实世界、可控制的人类和人工智能体的描述还停留在科幻小说中，但人们利用大数据技术和访问远程计算机技术的想法却没停止前进。作为这些技术前提条件的计算机网络，包含着大量可为人们利用的信息。

网络是一个用户无法触摸到的、抽象的东西，空间又是一个抽象的概念，所以网络空间的概念更是抽象的。仁者见仁，智者见智，对于网络空间的概念有多种，但根据联合国国际电信联盟（ITU）的定义，网络空间是指由以下所有或部分要素创建或组成的物理或非物理的领域，这些要素包括计算机、计算机系统、网络及其软件支持、计算机数据、内容数据、流

量数据及用户。英国、美国和德国等对网络空间概念的定义都不尽相同，但本质都是一样的，都着重强调提供网络应用的整个系统。

1.1.2 网络空间安全的概念

基于对全球五大空间的新认知，网络领域与现实空间中的陆域、海域、空域、太空一起，共同形成了人类自然与社会及国家的公共领域空间，使网络空间安全具有全球空间的性质。有学者提出“网络空间安全”是指能够容纳信息处理的网络空间构建与管理的安全，是远比“信息安全”更为重要和根本的安全。网络空间安全保护是否得当不仅会影响用户的上网体验，还会对国家的安全和利益造成威胁。

网络空间安全依赖于信息安全（Information security）、应用安全（Application security）、网络安全（Network security）和因特网安全（Internet security），这些都是网络空间安全的基础构建模块。网络空间安全是关键信息基础设施保护（Critical Information Infrastructure Protection，CIIP）的必要组成部分，同时，对关键基础设施服务的充分保护也有助于满足基础安全需求（关键基础设施的安全性、可靠性和可用性），进一步实现网络空间安全的目标。

从信息论角度来看，系统是载体，信息是内涵。网络空间是所有信息系统的集合，是人类生存的信息环境，人在其中与信息相互作用、相互影响。因此，网络空间存在更加突出的信息安全问题，其核心内涵仍是网络安全。

网络安全的一个通用定义是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的原因而遭到破坏、更改或泄露，并且网络系统能够连续、可靠、正常地运行。

从用户（个人、企业等）的角度来说，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，避免其他人利用窃听、冒充、篡改和抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望当用户的信息保存在某个计算机系统上时，不受其他非法用户的非授权访问和破坏。

从网络运行和管理者的角度来说，对本地网络信息的访问、读/写等操作应受到保护和控制，避免出现病毒、非法存取、拒绝服务和网络资源造成的非法占用及非法控制等威胁，制止和防御网络“黑客”的攻击。

对安全保密部门来说，应对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免其通过网络被泄露，避免由于这类信息的泄露对社会产生危害，对国家造成巨大的经济损失，甚至威胁到国家安全。

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

因此，网络安全在不同的环境和应用中会得到不同的解释。

（1）网络运行系统的安全，即保证信息处理和传输系统的安全，包括计算机系统机房环境的保护、计算机结构设计上的安全性考虑、硬件系统的可靠安全运行、计算机操作系统和应用软件的安全、数据库系统的安全、电磁信息泄露的防护等。它侧重于保证系统正常的运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁信息泄露而产生信息泄露，干扰他人（或受他人干扰）。本质上，网络运行系统的安全就是保护系统的合法操作和正常运行。

（2）网络系统信息的安全，包括用户口令鉴别、用户存取权限控制、数据存取权限、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）网络信息传播的安全，即信息传播后的安全，包括信息过滤等。它侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充和诈骗等有损合法用户利益的行为，其本质是保护用户的利益和隐私。

显而易见，网络安全与其所保护的信息对象有关。网络安全的本质是在信息的安全期内，保证信息在网络流动或静态存放时不被非授权用户非法访问，但授权用户是可以访问的。网络安全、信息安全和系统安全的研究领域是相互交叉和紧密相连的。

1.1.3 网络空间安全的重要性

在现代化社会中，网络以其开放、便捷等特性对社会发展起到了巨大的促进作用。网络空间涉及国家的军事、政治等多个领域信息，在其中存储、转发的信息多为涉及政府重要文件、金融商业信息、科研数据等重要信息，而且大都为敏感信息，多为国家机密。因此，这些信息往往会成为各种网络攻击的目标。

虽然网络空间安全已经得到普遍重视，但近年来一些新的焦点问题相继显露。例如，“伪基站”导致的诈骗事件频频发生，暴露了通信领域对物理接入安全的忽视；云计算、大数据相关新概念、新应用的不断出现，使个人数据隐私泄露问题日益凸显；计算和存储能力日益强大的移动智能终端承载了大量与人们工作、生活相关的应用和数据，急需切实可用的安全防护机制，而互联网上匿名通信技术的滥用更是对网络监管、网络犯罪取证提出了严峻的挑战。在国家层面，危害网络空间安全的国际重大事件也是屡屡发生。例如，2010 年伊朗核电站的工业控制计算机系统受到震网病毒（Stuxnet）攻击，导致核电站推迟发电；2013 年美国棱镜计划被曝光，表明自 2007 年起美国国家安全局（NSA）即开始实施绝密的电子监听计划，通过直接进入美国网际网络公司的中心服务器挖掘数据、收集情报，涉及海量的个人聊天日志，存储的数据，语音通信、文件传输、个人社交网络数据。

上述种种安全事件的发生，凸显了网络空间仍然面临着从物理安全、系统安全、网络安全到数据安全等各个层面的挑战，迫切要进行全面而系统的安全基础理论和技术研究。安全是发展的前提，发展是安全的保障。当前，我国正在加速从网络大国向网络强国迈进，因此网络空间安全技术的研究起着越来越重要的支撑作用。

1.2 网络空间安全的主要威胁

随着计算机网络的不断发展，出现了各式各样网络空间安全的威胁因素，如图 1.1 所示。这些网络安全的威胁因素可能来自内部，也可能来自外部。

内部威胁包括设备缺陷及故障、系统漏洞、技术人员的不安全行为等。日常软件系统并非百分之百完美，都会存在一些缺陷或漏洞，而一些不法分子正是利用这些缺陷或漏洞对网络进行攻击，威胁网络空间安全的。同时，在研发过程中，有些技术人员为了自己方便而设置了软件的“后门”，这些不为人知的后门一旦被不法分子发现和利用，将造成极其严重的后果。

外部威胁则是指一些恶意软件、木马、病毒等。随着各种威胁因素的不断扩张，越来越多的用户开始意识到网络空间安全的重要性。目前，市场上的防病毒软件种类繁多，用户很

难进行判断并选购，而且国内权威的防病毒软件厂商不多，这些都限制了网络空间安全工作的加强。

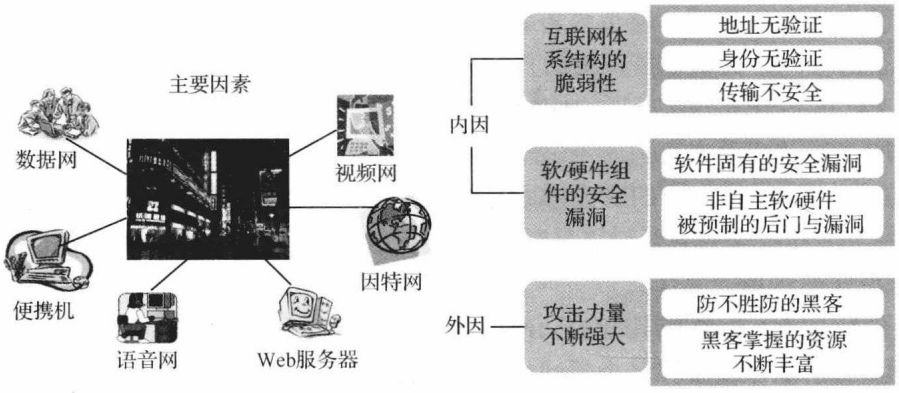


图 1.1　网络空间安全的威胁因素

1.2.1　安全漏洞

安全漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。安全漏洞的通俗描述性定义是存在于计算机网络系统中的、可能对系统中的组成和数据等造成损害的一切因素。比如，在 IntelPentium 芯片中存在的逻辑错误、在 Sendmail 早期版本中的编程错误、在 NFS 协议中认证方式上的弱点、在 UNIX 系统管理员设置匿名 FTP 服务时配置不当的问题都可能被攻击者使用，威胁到系统的安全。这些都可以认为是安全漏洞。

安全漏洞可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处，主要表现在软件编写 bug、系统配置不当、设计缺陷等方面。

1．软件编写 bug

无论是服务器程序、客户端软件，还是操作系统，只要是用代码编写的，都会存在不同程度的 bug，攻击者可以利用 bug 进行攻击。

（1）缓冲区溢出：攻击者只要发送超出缓冲区所能处理长度的指令，系统便进入不稳定状态。攻击者通过特别设置一串准备用作攻击的字符，甚至能访问根目录，从而拥有对整个网络的绝对控制权。

（2）联合使用问题：一个程序经常由功能不同的多层代码组成，甚至会涉及最底层的操作系统。入侵者通常会利用这个特点为不同代码层输入不同的内容，以达到窃取信息的目的。

（3）资源竞争：若不能妥善处理多任务多进程的资源竞争问题，入侵者就可能利用这个处理顺序上的漏洞改写某些重要文件，从而达到闯入系统的目的。

2．系统配置不当

系统配置通常由管理员进行，若管理员配置时不规范，则为攻击者提供了极大的便利。

（1）使用默认配置：许多系统安装后都有默认的安全配置信息，通常被称为“easy to use”，也就意味着“easy to break in”。

（2）空口令：系统安装后保持管理员口令的空值，不进行修改。入侵者第一步做的事情就是搜索网络上是否有这样的管理员口令为空的机器。

（3）临时端口：有时候为了测试，管理员会在机器上打开一个临时端口，但测试完成后却忘记了禁止它，这样就会使入侵者有“漏”可寻、有“洞”可钻。

3．设计缺陷

网络层、传输层、应用层的协议在设计上都存在一定的缺陷，可被攻击者利用。

（1）IP：IP 非常容易“轻信”，使入侵者可以随意地伪造及修改 IP 数据包而不被发现。

（2）TCP/IP：TCP 序列号预计是网络安全领域中最有名的缺陷之一，即受害主机不能接到信任主机应答确认时，入侵者通过预计序列号来建立连接，从而可以伪装成信任主机与目标主机通话。

（3）FTP：FTP 用户的口令一般与系统登录口令相同，而且采用明文传输，这就增加了系统被攻破的危险。只要在局域网内或路由器上进行监听，就可以获得大量的口令，利用这些口令就可以尝试登录系统。

1.2.2 恶意软件

恶意软件（流氓软件）在网上横行，威胁网络空间安全的趋势愈演愈烈，通过 Google 搜索“流氓软件”条目竟达 3 240 000 项。

针对流氓软件在网络上泛滥成灾的现象，中国互联网协会联合国内 30 多家厂商对恶意软件的官方定义如下。

（1）强制安装：是指未明确提示用户或未经用户许可，在用户计算机或其他终端上安装软件的行为。

① 在安装过程中未提示用户。

② 在安装过程中未提供明确的选项供用户选择。

③ 在安装过程中未给用户提供退出安装的功能。

④ 在安装过程中提示用户的信息不充分、不明确（明确充分的提示信息，包括但不限于软件作者、软件名称、软件版本、软件功能等）。

（2）难以卸载：是指未提供通用的卸载方式，或者在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。

① 未提供明确的、通用的卸载接口（如 Windows 系统下的“程序组”中“控制面板”的“添加或删除程序”）。

② 软件卸载时附有额外的强制条件，如卸载时要联网、输入验证码、回答问题等。

③ 在不受其他软件影响或人为破坏的情况下，不能完全卸载，仍有子程序或模块在运行（如以进程方式）。

（3）浏览器劫持：是指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。

① 限制用户对浏览器设置的修改。

② 对用户所访问网站的内容擅自进行添加、删除、修改。

③ 迫使用户访问特定网站或不能正常上网。

④ 修改用户浏览器或操作系统的相关设置导致以上 3 种现象的行为。

（4）广告弹出：是指未明确提示用户或未经用户许可，利用安装在用户计算机或其他终端上的软件弹出广告的行为。

① 安装时未告知用户该软件的弹出广告行为。

② 弹出的广告无法关闭。

③ 广告弹出时未告知用户该弹出广告的软件信息。

（5）恶意收集用户信息：是指未明确提示用户或未经用户许可，恶意收集用户信息的行为。

① 收集用户信息时，未提示用户有收集信息的行为。

② 未提供用户选择是否允许收集信息的选项。

③ 用户无法查看自己被收集的信息。

（6）恶意卸载：是指未明确提示用户、未经用户许可，或误导、欺骗用户卸载其他软件的行为。

① 对其他软件进行虚假说明。

② 对其他软件进行错误提示。

③ 对其他软件进行直接删除。

（7）恶意捆绑：是指在软件中捆绑已被认定为恶意软件的行为。

① 安装时，附带安装已被认定的恶意软件。

② 安装后，通过各种方式运行其他已被认定的恶意软件。

（8）其他侵犯用户知情权、选择权的恶意行为。

1.2.3 网络攻击

网络攻击可分为主动攻击和被动攻击。主动攻击会导致某些数据流的篡改和虚假数据流的产生。这类攻击包括篡改、伪造消息数据、拒绝服务攻击等。被动攻击中的攻击者不对数据信息做任何修改，截取/窃听是指在未经用户同意和认可的情况下，攻击者获得了信息或相关数据，通常包括窃听、流量分析、破解弱加密的数据流等攻击方式。如图 1.2 所示，从最早的密码猜测到嗅探、拒绝服务等，随着攻击手段的不断发展，入侵者的水平却变得越来越低。

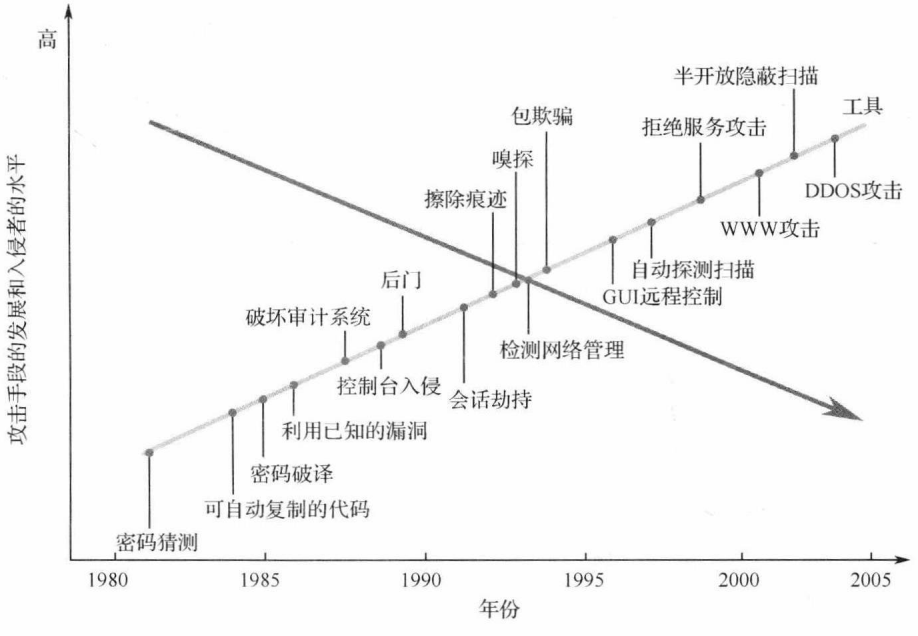


图 1.2 常见的攻击手段的发展和入侵者的水平

1．篡改

篡改是指一个合法消息的某些部分被改变、删除，消息被延迟或改变顺序，通常用以产生一个未授权的效果。例如，修改传输消息中的数据，将“允许甲执行操作”改为“允许乙执行操作”。

2．伪造消息数据

伪造指的是某个实体（人或系统）发出含有其他实体身份信息的数据信息，假扮成其他实体，从而以欺骗方式获取一些合法用户的权利。

3．拒绝服务攻击

拒绝服务攻击会导致通信设备的正常使用或管理被无条件地中断。拒绝服务攻击通常是对整个网络实施破坏。这种攻击也可能有一个特定的目标，如到达某特定目的地（如安全审计服务）的所有数据包都被阻止。

4．流量分析攻击

流量分析攻击方式适用于一些特殊场合。例如，敏感信息都是保密的，攻击者虽然从截获的消息中无法得到消息的真实内容，但攻击者还能通过观察这些数据包的模式，分析确定通信双方的位置、通信的次数及消息的长度，获知相关的敏感信息。

5．窃听

窃听是最常用的手段。目前应用最广泛的局域网上的数据传送是基于广播方式进行的，这就使一台主机有可能收到本子网上传送的所有信息。而计算机的网卡工作在杂收模式时，就可以将网络上传送的所有信息传送到上层，以供进一步分析。如果没有采取加密措施，通过协议分析，可以完全掌握通信的全部内容。窃听还可以用无限截获方式得到信息，通过高灵敏接收装置接收网络站点辐射的电磁波或网络连接设备辐射的电磁波，通过对电磁信号的分析恢复原数据信号从而获得网络信息。尽管有时数据信息不能通过电磁信号全部恢复，但可能得到极有价值的情报。

1.2.4 网络犯罪

随着网络的广泛使用，网络人口的比例越来越高，素质又参差不齐，网络成为一种新型的犯罪工具、犯罪场所和犯罪对象。网络犯罪向整个社会施加着压力，其中最突出的问题是，网络色情泛滥成灾，严重危害未成年人的身心健康；软件、影视、唱片的著作权受到盗版行为的严重侵犯，商家损失之大无可估计；电子商务受欺诈的困扰，例如，有的信用卡被盗刷，有的购买商品石沉大海，有的发出商品却收不回货款。这些现象表明，与网络相关的犯罪丛生，防治网络犯罪已经成为犯罪学、刑法学必须面对的新型课题之一。

1．网络色情和性骚扰

各国公众和立法更多地关注互联网的内容，特别是性展示材料、淫秽物品的传播。然而由于淫秽网页具有高点击率，又吸引了部分广告商开发这些网页。

目前，色情网站大部分在互联网上提供各种色情信息的网页，向各种搜索引擎注册关键字，或者在 BBS 和论坛上放置广告，或者向电子邮箱用户群发电子邮件，以达到吸引用户访问网站、浏览网页，从而接受其所提供服务的目的。这些色情网站的内容主要包括张贴淫秽图片，贩卖淫秽图片、光盘、录像带，提供超链接色情网站，散布性交易信息。

2．贩卖盗版光盘

由于计算机可以轻易地复制信息，包括软件、图片和书籍等，而且复制的信息又可以极快地传送到世界各地，使著作权的保护工作更为困难。在网络上贩卖的盗版光盘，其内容可能是各类计算机软件、图片、MP3、音乐 CD、影视 VCD 和 DVD 等。

3．欺诈

和传统犯罪一样，网络犯罪中欺诈也是造成损失较多、表现形式最为丰富的一种犯罪类型。美国消费者联盟早在 2000 年 11 月公布的报告中就指出，美国消费者因为网络欺诈而损失的金额在 1999 年每人平均为 310 美元，而到 2000 年就增加到了 412 美元。

4．妨害名誉

妨害名誉是指在网络上发表不实言论，辱骂他人，侵犯他人权益，妨害他人名誉等行为，以在网络上假冒他人名义征求性伴侣、一夜情人及公布他人电话号码的案例最多，还有将他人头像移花接木到裸体照片上，成为不堪入目的假照片。

5．侵入他人网站、电子邮箱、系统

近几年来，入侵他人网站并篡改网站事件已经成为各类安全事件之首。在国家计算机网络应急技术处理协调中心发布的 2007 年 11 月《我国网站被篡改情况月度报告》中指出，2007 年 11 月 1 日至 30 日，我国大陆地区被篡改网站的数量为 5 499 个，较上月增加了 537 个。还有许多恶意攻击者入侵后窃取他人档案或偷阅、删除电子邮件；将入侵获得的档案内容泄露给他人；入侵后将一些档案破坏，致使系统无法正常运行，甚至无法使用；盗用他人上网账号并使用，而上网所发生的费用则由被盗用者承担等。

6．制造、传播计算机病毒

在网络上散布计算机病毒的活动如今已经十分猖獗。有些病毒具有攻击性和破坏性，可能破坏他人的计算机设备、档案。计算机病毒不但本身具有破坏性，还具有传染性，一旦病毒被复制或产生变种，其传播速度之快令人难以预防。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可被大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下可造成被感染的计算机工作失常甚至瘫痪。

7．网络赌博

很多国家允许赌博行为或开设赌场。因此有人认为在赌博合法化的国家开设网站，只要该国不禁止，就不犯有赌博罪。其实，各国刑法都规定了管辖权制度，一般都能在其本国主权范围内处理这种犯罪。例如，对人的管辖权，特别是对行为的管辖权，只要犯罪的行为或结果有任意一项在一国领域中，该国即可管辖。

8．教唆、煽动各种犯罪，传授各种犯罪方法

除了教唆、引诱接触暴力信息、淫秽信息的网站，还有形形色色的专业犯罪网站。有的本身就是犯罪组织开设的，如各种邪教组织、暴力犯罪组织、恐怖主义组织等。普通人开设的专业性犯罪网站则更多，例如，有些专门煽动自杀的网站，就曾引发网友相约自杀的事件。此外，在网络上煽动危害国家安全行为的情况也值得被关注。