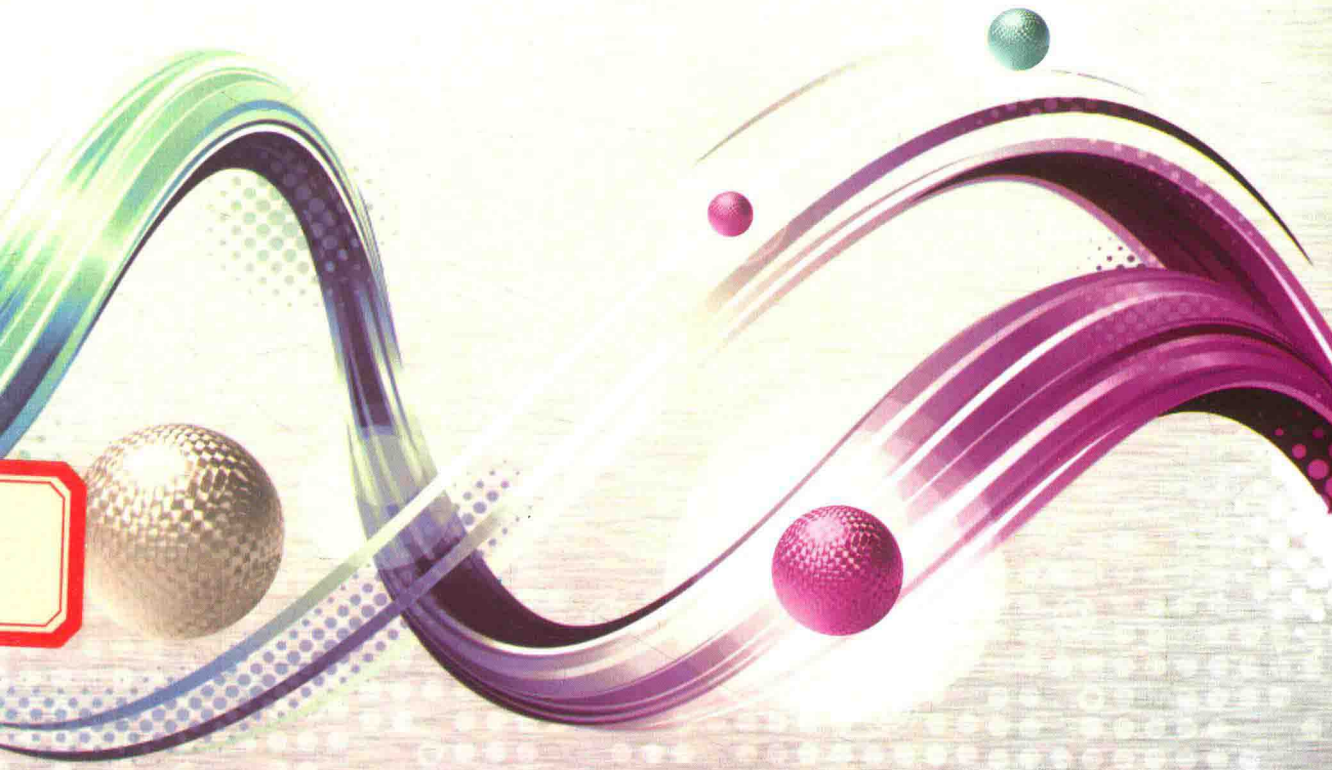
高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

网络攻击与防御

王敏　甘刚　吴震　杜之波　编著



西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类“十三五”规划教材
应用型网络与信息安全工程技术人才培养系列教材

网络攻击与防御

王 敏 甘 刚 吴 震 杜之波 编著

西安电子科技大学出版社

内 容 简 介

本教材涵盖了网络攻击原理、技术及实践三大部分内容，主要介绍网络攻击的一般流程、常用方法和常见攻击技术。全书内容包括网络攻击的基本知识、攻击流程、常见的主流攻击技术与防御技术、恶意代码攻击与防御技术、网络安全设备的攻击与防御技术，可为今后进一步学习和研究网络攻击与防御或者从事计算机网络安全管理工作奠定理论与技术基础。

全书共八章，第一章为网络安全概述，第二、三章为网络预攻击阶段所涉及的理论和技术，第四至七章为攻击阶段所涉及的常见攻击方式，包括基于系统的攻击与防御、脚本攻击与防御、恶意代码攻击与防御、网络安全设备的攻击与防御等，第八章介绍了四个真实的攻击实例。

本教材概念清晰、实例丰富，可作为信息安全专业、计算机应用专业或其他相近专业的教材，也可作为相关领域工作人员的参考书。

图书在版编目(CIP)数据

网络攻击与防御/王敏等编著. — 西安：西安电子科技大学出版社，2017.1
高等学校电子信息类“十三五”规划教材
ISBN 978-7-5606-4333-5

Ⅰ. ① 网… Ⅱ. ① 王… Ⅲ. ① 计算机网络—安全技术—高等学校—教材 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字(2016)第 277408 号

策划编辑　李惠萍
责任编辑　宁晓蓉
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　wmcuit@cuit.edu.cn
经　　销　新华书店
印刷单位　陕西天意印务有限责任公司
版　　次　2017 年 1 月第 1 版　　2017 年 1 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　16.5
字　　数　386 千字
印　　数　1～3000 册
定　　价　30.00 元
ISBN 978-7-5606-4333-5/TP
XDUP 4625001-1
***** 如有印装问题可调换 *****

前 言

“网络攻击与防御”是计算机科学技术、信息安全和信息对抗技术等专业本科生的专业基础必修课程，一般安排 2~3 学分，32～48 个学时。这门课程不仅要介绍信息安全学科相关的理论知识，还要介绍网络攻击与防御技术，同时涉及多个学科的基础知识。在通常的教学实践中，有的专业是在开设了“信息安全原理与技术”课程的基础之上再开设这门课程，让学生在了解原理的基础上，从攻防实践着手，更深刻地体会到信息安全的重要性。

目前国内大多数高校正在推行工程教育理念，加上学生还需要参加各种专业认证，这就要求学生不仅要掌握扎实的理论知识，还要具有较强的动手能力，以便满足社会需求。但目前许多高校培养的工科学生有一个通病，要么强调理论轻视技术，要么重视技术轻视理论，不同层次的高校学生犯相同的毛病。如何结合工程教育理念来教育学生，使他们明白，理论是基础，技术只是理论指导下的实现手段，没有理论作为指导，技术无法达到一定的高度，这是摆在教师面前的一个巨大问题。解决不了这个问题，就无法教育出优秀的学生，也无法成为一个优秀的教育工作者。

具体到“网络攻击与防御”这门课程来说，首先要使学生明白网络攻击所涉及的理论。它要求学生能将之前学习过的“Linux 实用操作系统”、“计算机网络”、“TCP/IP 协议”、“数据库原理与技术”、“Web 应用开发技术”、“防火墙与入侵检测技术”、“病毒原理与防范”等课程的理论与本课程有关知识贯穿起来，同时在讲解具体攻防技术时，使学生明白攻防技术是多种技术的结合，要有一个系统的概念。在信息安全相关理论指导下进行多种技术的继承，从攻的角度，才能实现进攻的有效性；从防的角度，才能构建一个安全的系统。没有系统的思维，单靠一门技术会给系统留下巨大的隐患。在讲解网络安全概述时，教师要注意对前期课程的复习，特别是常用协议的相关内容；在讲解具体的攻击技术时，教师要注意理论与实践相结合，可以预先布置，让学生预习，带着问题来听课；涉及实验内容时，教师应该指导并监督学生完成实验过程。这样，通过一门课程的教学，可以实现现代工程教育理念所要求的培养学生的目标。

本教材主要介绍网络安全基本概念、网络攻击的方法与技术，使学生掌握网络攻击与防御的基本知识、信息收集技术及工具的使用、网络扫描技术及工具的使用、基于系统的攻击与防御、SQL 注入攻击与防御、跨站脚本攻击与防御、基于 cookie 的攻击与防御、恶意代码攻击与防御、网络安全设备的攻击与防御等，为今后进一步学习与研究网络攻击与防御或从事计算机网络信息安全管理工作奠定理论与技术基础。

为了巩固理论知识，提高学生的动手实践能力，本教材提供了丰富的实验案例，并在最后一章详细叙述了笔者亲身尝试过的几个渗透案例，给学生提供了整体渗透的指导思路和方法，起到抛砖引玉的作用。

由于时间仓促，许多地方还不完善，敬请专家指正。

编 者

2016 年 8 月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第一章　网络安全概述

在世界成为“地球村”的同时，人们一方面享受着网络带来的便利和效益，另一方面也不得不“提心吊胆”地提防各种网络安全事件的发生。网络发展到今天的程度，网络安全也得到越来越多的关注。

本章主要介绍网络安全的发展历程，以及与网络安全息息相关的操作系统的发展历程，网络攻击与防御的一般流程和技术发展，最后介绍常见的网络协议。

1.1　网络安全发展过程

1.1.1　网络安全的意义

所谓“网络安全”，是指网络系统的硬件、软件及系统中的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续、可靠、正常地运行，网络服务不被中断。在计算机应用日益广泛和深入的同时，计算机网络的安全问题日益复杂和突出，网络的脆弱性和复杂性更增加了其受到威胁和攻击的可能性。

1.1.2　网络安全发展历史

1986 年初，在巴基斯坦的拉合尔(Lahore)，巴锡特(Basit)和阿姆杰德(Amjad)两兄弟编写的第一个病毒——Pakistan 病毒(即 Brain)问世，在此之后的一年时间内，Brain 病毒传播到了世界各地。

2002 年 10 月，Bugbear 病毒以新的感染手法让连续半年稳居毒王宝座的 Klez(求职信)病毒退位。Bugbear 病毒可以窃取高度敏感的资料，如密码、账号等，并将其传送到指定的电脑中，另外被感染的电脑还会被其远端控制。

2003 年可以说是互联网出现以来最不太平的一年。安全漏洞和病毒不断出现，造成了一次又一次轰动全球的安全事件。

2003 年 1 月 25 日，互联网遭遇到全球性的病毒攻击。这个病毒名叫 Win32.SQLExp.Worm(蠕虫王)，其破坏性堪称互联网的“9.11”，这个病毒体极其短小，但却具有极强的传播性，它利用 Microsoft SQL Server 的漏洞进行传播。由于 Microsoft SQL Server 在世界范围内都很普及，因此此次病毒攻击导致全球范围内的互联网瘫痪。在中国，80%以上网民受此次全球性病毒袭击影响而不能上网，很多企业的服务器被此病毒感染引起网络瘫痪。美国、泰国、日本、韩国、马来西亚、菲律宾和印度等国家的互联网也受到严重影响。直

到 1 月 26 日晚，蠕虫王才得到初步的控制。这是继红色代码、尼姆达、求职信病毒后又一起极速病毒传播案例。蠕虫王病毒的出现，可以称为一个传奇，它令全世界范围内因此损失高达 12 亿美元。

2003 年 3 月 20 日，美国对伊拉克发动战争。在炸弹持续向伊拉克倾泻之际，抗议者和拥护美英的黑客在互联网上的口水大战也随之升级，他们互相篡改对方公司与政府网站的内容，黑客入侵网站事件激增。有三类黑客参与对网站的攻击：以美国为基地的爱国主义黑客、伊斯兰极端主义组织和反战的和平主义人士。每分钟就会有 3～4 起黑客组织篡改美国和英国网站的事件发生，并且攻击的数量和速度都有大幅度的提高。本次黑客大战使用了两种攻击手段。第一种是基于 WebDAV 缓冲区溢出漏洞的攻击。Microsoft IIS 5.0 默认提供了对 WebDAV 的支持，通过 WebDAV 可以利用 HTTP 向用户提供远程文件存储的服务。IIS 5.0 包含的 WebDAV 组件不充分检查传递给部分系统组件的数据，远程攻击者利用这个漏洞对 WebDAV 进行缓冲区溢出攻击，可能以 Web 进程权限在系统上执行任意指令。拒绝服务(DoS)攻击也是本次黑客大战常见的攻击方法，由于 TCP/IP 协议本身的缺陷，DoS 攻击不可防御。

2003 年 8 月 11 日，一种名为“冲击波”(WORM_MSBlast.A)的新型蠕虫病毒开始在我国互联网和部分专用信息网络上传播。该病毒传播速度快、波及范围广，对计算机正常使用和网络运行造成严重影响。该病毒能够在短时间内造成大面积的泛滥，是因为病毒运行时会扫描网络，寻找操作系统为 Windows 2000/XP 的计算机，然后通过 RPC 漏洞进行感染，并且该病毒会操纵 135、4444、69 端口，危害系统。受到感染的计算机中 Word、Excel、Powerpoint 等文件无法正常运行，弹出找不到链接文件的对话框，“粘贴”等一些功能无法正常使用，计算机出现反复重新启动等现象。Windows 的 RPC 服务(RPCSS)存在漏洞，当发送一个畸形包的时候，会导致 RPC 服务无提示地崩溃。冲击波病毒正是借此进行传播的。RPC 服务是一个特殊的系统服务，许多应用和服务程序都依赖于此，因而可以造成这些程序与服务的拒绝服务。在 RPC 服务崩溃以后，攻击者就可以通过劫持 Epmapper 管道和 135 端口的方法来提升权限和获取敏感信息。

2004 年病毒和黑客的破坏仍然呈上升趋势，特别是随着 ADSL 等宽带的普及和越来越多的企事业单位搭建了局域网，病毒传播速度越来越快。2004 年 4 月 30 日震荡波(Sasser)病毒被首次发现，短短一个星期时间之内就感染了全球 1800 万台电脑，成为那一年当之无愧的“毒王”。它利用微软公布的 LSASS 漏洞进行传播，可感染 Windows NT/XP/2003 等操作系统，开启上百个线程去攻击其他网上用户，造成机器运行缓慢、网络堵塞。

2005 年，美国超过 300 万的信用卡用户资料外泄，导致用户财产损失，同时，中国工商银行、中国银行等金融机构的网站先后成为黑客们模仿的对象，设计了类似的网页，通过网络钓鱼的形式获取利益。这一现象在 2005 年以平均每个月 73%的数字增长，使很多用户对于网络交易的信心大减，导致年底各家银行对于网络交易的安全提高重视度。针对这些愈演愈烈的网上银行诈骗事件，中国人民银行于 10 月 30 日向社会公布《电子支付指引(第一号)》，对银行从事电子支付活动提出了指导性要求，对银行针对不同客户在电子支付类型、单笔支付金额和每日累计支付金额等方面作出合理限制。

2010 年间最受安全产业关注的议题是 Stuxnet 恶意软件的出现。赛门铁克公司表示，该病毒的设计者拥有强大的幕后财政支持，用以创造出模拟攻击环境。该病毒包含 4000

个功能，每个功能都有它隐含的理由。一位安全分析专家指出，Stuxnet 的攻击目标是伊朗的布什尔核电站。2010 年 11 月 30 日，伊朗总统内贾德证实了其国内的核电站被 Stuxnet 攻击，位于布什尔和纳坦兹的伊朗核设施浓缩铀离心机被病毒破坏。普遍猜测 Stuxnet 传染源集中在以色列。

2014 年 2 月 27 日，中央网络安全和信息化领导小组宣告成立，并在北京召开了第一次会议，习近平亲自担任组长，李克强、刘云山任副组长。中央网信小组将着眼于国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强网络及信息安全保障能力。5 月 16 日，中国政府采购网公布的《中央国家机关政府采购中心重要通知》称，所有计算机类产品不允许安装 Windows 8 操作系统。7 月，公安部科技信息化局下发通知，称赛门铁克的“数据防泄露”产品存在窃密后门和高危漏洞，要求各级公安机关今后禁止采购。9 月，银监会正式发布的《应用安全可控信息技术指导意见》中明确指出，从 2015 年起，各银行业金融机构对安全可控信息技术的应用以不低于 15%的比例逐年增加，直至 2019 年掌握银行业信息化的核心知识和关键技术，安全可控信息技术在银行业达到不低于 75%的总体占比。这一系列举措意味着我国政府和企业开始正视网络信息安全长期依赖国外技术的现象，国产信息安全软件及企业将迎来新的发展机遇。

2015 年，不法分子攻击网站、机构，并窃取其储存私密信息的事件愈加频繁。英国宽带服务提供商 TalkTalk 于 2015 年 10 月 23 日证实，约 400 多万用户的隐私数据被泄露。其中包括用户姓名、地址、出生日期、电话号码、电子邮箱、TalkTalk 账号信息，甚至信用卡或银行账号的详细信息等。事实上，这已经是 TalkTalk 今年第三次遭受黑客攻击，但即便是在早有预警的情况下，此次攻击依然造成了“可怕的损失”。国内著名漏洞平台乌云爆料称：网易的用户数据库疑似泄露，影响数据总共数亿条，泄露信息包括用户名、MD5 密码、密码提示问题/答案(hash)、注册 IP、生日等。网易邮箱绑定的其他账户也受到波及，如 iPhone 用户的 Apple ID 等。新闻显示，自 2015 年 10 月 17 日起已经有相当多的网易用户受到影响，Apple ID 被锁，微博、支付宝、百度云盘、游戏账号被盗等不一而足。

1.1.3　网络安全发展现状

2016 年，各国围绕互联网关键资源和网络空间国际规则的角逐更加激烈，工业控制系统、智能技术应用、云计算、移动支付领域面临的网络安全风险进一步加大，黑客组织和网络恐怖组织等非国家行为体发起的网络安全攻击持续增加，影响力和破坏性显著增强，我国网络安全形势更加严峻。

1. 传统互联网威胁向工控系统扩散

随着“互联网+”、智能制造等新兴业态的快速发展，互联网快速渗透到工业各领域各环节，客观上导致工业行业原有相对封闭的使用环境被逐渐打破，传统网络安全威胁加速向工业网络、系统、设备渗透，针对工业控制系统的病毒、木马日益猖獗。自 2010 年以来，相继爆发了针对伊朗核设施的震网病毒攻击事件、针对化工企业的 Nitro 攻击事件、

此为试读，需要完整PDF请访问：www.ertongbook.com

针对能源企业的 Shamoon 攻击事件。2016 年，病毒、木马等传统互联网威胁更大面积地向工控系统扩散，工控系统面临着前所未有的安全挑战。

2. 智能技术应用安全问题更加突出

近年来，智能技术应用面临的网络安全威胁日益严重。2012 年，美国著名黑客巴纳比·杰克称，他可以在距离目标 50 英尺(15.24 m)的范围内侵入心脏起搏器，让起搏器释放出足以致人死亡的 830 V 电压；2013 年的 DefCon 黑客大会上，美国两位网络安全人员演示了如何通过攻击软件使高速行驶的汽车突然刹车；2014 年乌云安全峰会上黑客指出，360 安全路由、百度小度路由、小米路由等智能路由器均存在安全漏洞；2015 年的 Geekpwn 大会上，黑客演示了破解智能家居的过程。我国智能设备安全问题同样非常严重，但与之形成鲜明对比的是，消费者的安全意识十分淡薄。调查发现，我国只有 44%的人知道智能设备可能泄露个人隐私。随着智能技术在医疗、汽车、家居等各大领域的深入应用，2016 年，智能设备的安全问题已更加突出。

3. 云端安全事件将大量增加

随着云端业务和数据的逐步累积，针对云端的基于漏洞、病毒、未知威胁的 APT 攻击、0Day 攻击日益增加，云端的安全事件频频发生。2009 年，Gmail 电子邮箱发生故障，导致业务中断 4 个小时；2010 年，Intuit 的基于云连接的服务发生长达 36 小时的断网事故；2011 年，亚马逊的云计算数据中心发生宕机事件，大量企业业务受损；2014 年，UCloud 公司国内云平台发生大规模云服务攻击事件；2015 年，“毒液”漏洞使全球数以百万计的虚拟机处于网络攻击风险之中，严重威胁各大云服务提供商的数据安全。随着云计算广泛应用于各个领域，2016 年，云端的安全事件进一步增加。

4. 泄露和窃密性攻击步入“高发期”

2015 年，全球发生多起以泄露和窃密为目的的网络安全攻击事件。5 月，美国超过 10 万名纳税人的信息被盗，造成 5000 万美元的损失；6 月，日本养老年金信息系统泄露约 125 万份个人信息，美国人事管理办公室 2000 多万前联邦政府雇员及在职员工的数据泄露；10 月，英国电信运营商 TalkTalk 的 400 万用户信息泄露，包括电子邮件、姓名和电话号码，以及数万银行账户信息；12 月，香港伟易达集团发生客户信息泄露事件，导致全球多达 500 万消费者的资料泄露。2016 年，全球更加频繁地发生规模大、后果严重的信息泄露事件。

5. 移动设备和支付安全问题凸显

猎豹移动安全实验室发布的《2015 年上半年移动安全报告》显示，截至 2015 年 6 月，安卓平台的恶意应用总量为 451 万，2014 年同期仅有 215 万。新增手机病毒是过去数年的总和，其中移动支付、资费消耗和隐私窃取是手机病毒排行前列的三大危害。中国银联发布的《2015 移动互联网支付安全调查报告》称，2015 年，1/8 的受访者遭遇过网络诈骗，比 2014 年上升 6 个百分点。2016 年，移动设备和移动支付用户继续“爆炸式”增长，安全问题更加严重。

6. 网络空间国际话语权角逐激烈

近年来，各国围绕互联网关键资源和网络空间国际规则展开博弈，纷纷提出各自的方

案或版本，争夺话语权。在互联网关键资源管理方面，美国提出确保“私营机构在资源管理中处于领导地位”的方案；巴西等国提出分离“ICANN 的网络治理政策制定功能和管理配置根服务器权限”的方案；美国东西方研究所提出“多利益相关方”方案；印度提出“ITU 管理资源”方案。在网络空间国际规则制定方面，中国、俄罗斯等国家起草制定《信息安全国际行为准则》，提出了网络空间各国相处的原则规范；美国等西方国家推出《塔林手册》，提出了网络空间武装冲突的规则。2016 年，各国围绕互联网关键资源和网络空间国际规则的角逐更加激烈。

7. 黑客和网络恐怖组织破坏力加大

2015 年，以匿名者为代表的黑客团体和以 ISIS 为代表的网络恐怖组织制造了多起网络安全事件，其影响力和破坏力巨大。3 月，匿名者发布视频称将对以色列发动“电子大屠杀”，进攻政府、军事、金融、公共机构网站，将以色列从网络世界抹去。5 月，匿名者入侵了 WTO 的数据库，攻击以色列武器经销商网站，并在#OpIsrael 计划中泄露大量在线客户端登录的数据。11 月，ISIS 利用互联网组织实施巴黎恐怖袭击。2016 年，出于政治原因，以匿名者和 ISIS 组织为代表的黑客团体和网络恐怖组织频繁地对部分国家的政府网站、国家关键基础设施发动攻击，其破坏力显著增加。

8. 全球网络空间军备竞赛风险加剧

2015 年，世界各国不断加大在网络空间的部署，继续建立或增设网络部队，研发网络武器和新型对抗技术，开展攻防演习，网络空间军备竞赛和国家级网络冲突的风险不断增加。美国国防部计划于 2016 年将网络司令部网络战部队人数增至 6000 人，到 2019 年将建立 133 支网络战部队。美陆军国民警卫队提出将在未来 3 年成立 10 个网络保护小组，美国海军网络司令部计划研发进攻性网络武器并组建 40 支网络任务部队。目前，美国拥有的震网、毒曲等网络武器多达 2000 种。据联合国裁军研究所报告显示，全球已有近 50 个国家建立了网络战部队。2016 年，大国继续开展网络军备竞赛，进行网络战和攻防演习，网络空间剑拔弩张。

9. 我国网络安全战略有望公开发布

2015 年，我国网络安全政策、立法工作取得重大进展，但国家网络安全战略尚未出台，顶层设计依然不够清晰，没有明确划定网络空间的核心利益。与此同时，全球已有近 60 个国家发布网络安全战略，其中美国出台了 15 份战略文件，日本发布了 5 份战略文件，爱沙尼亚颁布了 3 份战略文件，加拿大、英国、法国等国家也制定了 2 份战略文件。2016 年 12 月 27 日，我国第一份关于网络空间安全的战略文件《国家网络空间安全战略》公开发布。

10. 我国网络安全产业高速发展

随着“互联网+”行动持续发酵以及国家网络安全相关政策的不断出台，网络安全的重要性被提升至前所未有的高度，加之网络安全需求的持续推动，网络安全产业面临爆发式增长机遇，近两年呈高速发展趋势。据赛迪统计，2015 年网络安全产业规模突破 550 亿元，增幅达到 30%。2016 年，我国网络安全产业发展继续保持良好势头，产业增长率保持在 28%，产业规模达到 700 亿元。

1.1.4 黑客发展历史

“黑客”一词是英文 Hacker 的音译。这个词早在莎士比亚时代就已存在了，但是人们第一次真正理解它，却是在计算机问世之后。根据《牛津英语词典》解释，“Hack”一词最早的意思是劈砍，而这个词意很容易使人联想到计算机遭到别人的非法入侵。因此在《牛津英语词典》中“Hacker”还有“利用自己在计算机方面的技术，设法在未经授权的情况下访问计算机文件或网络的人”的释义。黑客是一个中文词语，在台湾地区对应的中文词语为骇客。Hacker 一词最初曾指热心于计算机技术、精通各种编程语言和各类操作系统、水平高超的电脑专家，尤其是程序设计人员，后逐渐区分为白帽、灰帽、黑帽等。其中黑帽(black hat)实际就是 cracker。到了今天，黑客一词已被用于泛指那些专门利用计算机病毒搞破坏的人。与黑客相对的是红客，当然，也有正义的黑客。

黑客最早被引进计算机领域可追溯自 20 世纪 60 年代。加州大学伯克利分校计算机教授 Brian Harvey 在考证此词时曾写到，当时麻省理工学院(MIT)中的学生分成两派，一派是 tool，意指乖乖牌学生，成绩都拿甲等；另一派则是所谓的骇客，也就是常逃课，上课爱睡觉，但晚上却又精力充沛喜欢搞课外活动的学生。著名的计算机程序员、开源软件运动的旗手埃里克·史蒂文·雷蒙德对 Hacker 的解释是：“黑客兵工厂”与“cracker”是分属两个不同世界的族群，基本差异在于，黑客是有建设性的，而骇客则专门搞破坏。黑客兵工厂所做的不是恶意破坏，他们是一群纵横于网络上的技术人员，热衷于科技探索、计算机科学研究。在黑客圈中，Hacker 一词无疑带有正面的意义，例如 system hacker 熟悉操作系统的设计与维护，password hacker 精于找出使用者的密码，computer hacker 则是通晓计算机、进入他人计算机操作系统的高手。

最早的计算机于 1946 年在宾夕法尼亚大学诞生，而最早的黑客出现于麻省理工学院。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。电脑安全黑客会使用密码破解(password cracking)或穷举法(brute force attack)。对一个黑客来说，学会编程是必须的，计算机可以说就是为了编程而设计的，运行程序是计算机的唯一功能。运行程序其实就是运算，要具备离散数学、线性代数、微积分等方面的相关知识，所以，真正的一流黑客并非整天不学无术，而是会热衷追求某种特殊嗜好，比如研究电话、无线电或计算机。黑客一词在圈外或媒体上通常被定义为：专门入侵他人电脑系统进行不法行为的计算机高手。现在网络上出现了越来越多的骇客，他们只会入侵，使用扫描器到处乱扫，进行毫无目的的破坏活动或恶作剧，他们无益于电脑技术的发展，反而有害于网络的安全甚至造成网络瘫痪，给人们带来巨大的经济甚至精神损失。

“蓝客”一词由蓝客联盟在 2001 年 9 月提出。蓝客联盟(LUC)简称蓝盟，组建于 2001 年 10 月 1 日。蓝客联盟是一个非商业性的民间网络技术机构，联盟进行有组织有计划的计算机与网络安全技术方面的研究、交流、整理与推广工作，提倡共享、自由、平等、互助的原则。

2001 年底至 2002 年 1 月，中日关系空前紧张，国内爱国网站、网民纷纷强烈抗议时任日本首相小泉纯一郎再次参拜靖国神社和日本新教科书事件。2002 年 1 月，蓝盟策划与中国黑客联盟、中国红客联盟在 2002 年 2 月春节期间，对日展开联合技术攻击行动。那

次对日行动代号“蓝色尊严”，三个组织及众多自发报名参加行动的网友于2002年春节准时展开了对日的技术打击。当时80%左右的日本IP段受到不同程度的影响，百余家日本商业网站被替换首页或被迫下线，几十家日本政府网站受到首页替换或DDoS攻击。

2010年6月9日，蓝客联盟与国内多个网络安全组织共同发起“69圣战”，对韩国网络进行大规模DDoS攻击。2011年5月，越南就南海主权问题挑衅中国引发争端并愈演愈烈，越南外交部宣布欢迎包括美国在内的国际社会“协助解决”南海主权争执，矛头直指中国。越南海军并于6月份在南海进行了实弹军演。2011年6月7日，蓝客联盟对越南发起代号为“华夏尊严”的技术行动，迅速击溃越南外交部官网并对数百家越南企业、集团网站采取技术性打击，间接性给予越南经济裁判。10日，网警介入调查并终止行动，行动仅历时三天。

红客(Honker)是指维护国家利益，不去利用网络技术入侵自己国家电脑，而是维护正义，为自己国家争光的黑客。HUC是红客联盟的字母简写。红客联盟成立于2000年底，是由黑客界传奇人物Lion牵头组建的，吸纳了全国众多黑客高手，其成员曾达到8万多人，成为世界排名第5的黑客组织。中国红客联盟主要反击国外一些黑客的攻击，其中2001年反攻美国白宫网站最为著名。红客联盟于2004年12月31日成立四周年之际在其网站上发表公开信，宣布解散，同时关闭网站。随后，数个红盟相继宣布成立。

2001年4月，中美撞机事件引发中美黑客大战，以至于美国太平洋司令部将其信息系统面临威胁状况的等级由一般提升至A级，这样有关人员会随时对网站的运营情况进行密切关注。同时，美国军方到5月2日左右还可能将上述威胁等级由A级提升至B甚至C级，一旦提升到B级，那么用户登录所有军方网站时就会受到限制，而C级则意味着军方网络系统不会保持时刻在线。威胁等级最高一级为D级，届时整个军方系统将全部关闭。4月29日美国劳工部及卫生部网站遭到中国黑客攻击，5月1日，中美黑客大战再升级，美国白宫官方网站遭攻击，5月2日，中美黑客大战升级两天之内700多家网站被黑，5月5日，白宫网站再遭黑客袭击，被迫关闭两个多小时。在历经七天的反攻之后，中国黑客组织宣布停止反攻。此次大战结束后大批黑客成员相继消失退隐，加之中国红客联盟的解散，更让此次震惊全球的战役成为世界第一次黑客大战。

目前，我国已成为世界上黑客攻击的主要受害国之一，针对网络犯罪行为，我国也制定了有关法律法规。2011年8月29日，最高人民法院和最高人民检察院联合发布《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》。该司法解释规定，黑客非法获取支付结算、证券交易、期货交易等网络金融服务的账号、口令、密码等信息10组以上，可处3年以下有期徒刑等刑罚，获取上述信息50组以上的，处3年以上7年以下有期徒刑。2013年3月11日，国家互联网应急中心(CNCERT)的最新数据显示，中国遭受境外网络攻击的情况日趋严重。CNCERT抽样监测发现，2013年1月1日至2月28日不足60天的时间里，境外6747台木马或僵尸网络控制服务器控制了中国境内190万余台主机；其中位于美国的2194台控制服务器控制了中国境内128.7万台主机，无论是按照控制服务器数量还是按照控制中国主机数量排名，美国都名列第一。

2014年8月2日至8月7日，一年一度的BlackHat(黑帽子大会)在美国拉斯维加斯召开，全球近万名黑客汇聚一堂。因为西方电影中的反派常戴着黑帽子，所以，1997年美国黑客杰夫·莫斯创办这一黑客盛会时，将它命名为“黑帽子大会”。如今，黑帽子大会已

成为一个世界级的信息安全会议，世界 500 强企业、国际网络安全产品和服务提供商，甚至美国联邦调查局(FBI)，都成了参会嘉宾。门票一张要 2000 多美金，参加会议的多是全球大型信息安全企业的高管及核心技术人员，或是黑客界的大腕。黑帽子大会结束后的三天，则是 DefCon(世界黑客大会)，DefCon 创办于 1993 年，比黑帽子大会还要早，创始人也是杰夫·莫斯，当时他才 18 岁。谁能掌控互联网，谁就能掌控未来。作为全球规模最大的黑客盛会，DefCon 就如同黑客世界的华山论剑。

就中国黑客而言，范渊是第一个登上 BlackHat 这一全球顶级黑客盛会舞台的中国人，早在 2006 年他就曾受邀在会议上向全球黑客分享自己的研究成果。目前，尽管国内仍然聚集着一大批顶尖的黑客人才，但相比国外而言，包括全球顶级的信息安全公司 Fire Eye 在内，很多行业内尖端企业的核心技术人员中，都有中国人的身影，他们大多供职于美国的信息安全企业。在中国的黑客界，由龚蔚在上海创立的“绿色兵团”被称为黑客界的“黄埔军校”，其中聚集了国内最早的一批顶尖黑客高手。其中安全焦点更是拥有冰河等一大批武林高手，稳保黑客江湖第一大门派的地位。很多最初的黑客高手如今都在信息安全行业身居要职。来自清华大学的蓝莲花战队是唯一一支参与 CTF 夺旗大赛的中国大陆战队，这项赛事也被视为世界黑客大会的压轴项目。蓝莲花最终在 20 支参赛队伍中排名第五。

1.2 操作系统的发展过程

1.2.1 Windows 早期版本及 Windows NT 的技术特点

Windows NT 之前的 Windows 操作系统依赖于 DOS 操作系统，具有友好、直观、高效的面向对象的图形用户界面，采用丰富但与设备无关的图形操作，支持多任务环境，在 32 位的方式下具有抢先多任务能力，实现了虚拟管理，突破了 640 KB 的限制。Windows 操作系统提供各种系统管理工具，方便用户对系统进行可视化管理，同时支持装入和运行 DOS 下开发的程序，提供数据库接口和网络通信接口，拥有丰富的软件开发工具，并具有面向对象的程序设计思想，支持 FAT32 文件系统。

Windows NT 操作系统与较早期的 Windows 操作系统具有显著的差异，首先 Windows NT 支持对称多处理和多线程，支持抢先的可重入多任务处理，采用 32 位页式授权虚拟存储管理，支持多种 API，提供源码级兼容性，支持多种可装卸文件系统，具有各种容错功能，达到 C2 安全级，可移植性好，采用集成网络计算，能与 Microsoft SQL Server 结合，提供 C/S 数据库应用系统的最好组合。

1.2.2 UNIX 操作系统

UNIX 系统是美国麻省理工学院(MIT)在 1965 年开发的分时操作系统 Multics (Multiplexed Information and Computing Service System)的基础上不断演变而来的，它原是 MIT 和贝尔实验室等为美国国防部研制的。贝尔实验室的系统程序设计人员汤普逊(Thompson)和里奇(Ritchie)于 1969 年在 PDP-7 计算机上成功地开发了 16 位微机操作系统。该系统继承了 Multics 系统的树形结构、Shell 命令语言和面向过程的结构化设计方法，以

及采用高级语言编写操作系统等特点，同时，又摈弃了它的许多不足之处。为了表示它与Multics既继承又背叛的关系，该系统被命名为UNIX，UNIX中的UNI正好与Multi相对照，表示UNIX系统不像Multics系统那样庞大和复杂，而X则是cs的谐音。

由于当时美国政府禁止AT&T经营计算机业务，所以在整个20世纪70年代，UNIX没能作为商品进入市场，而主要是提供给学校和科研机构等非盈利单位使用。

1972年，UNIX系统开始移植到PDP-11系列机上运行，1979年，贝尔实验室又将其移植到类似于IBM370的32位机上运行，并公布了得到西部电气公司正式承认的UNIX第七版。1980年又公布了为VAX-11/780计算机编写的操作系统UNIX 32V。在此基础上，加利福尼亚大学伯克利分校同年发表了VAX-l1型机用的BSD 4.0和BSD 4.1版本。1982年，贝尔实验室又相继公布了UNIX systems III的3.0、4.0和5.0等版本。它们是对UNIX 32V的改进，但却不同于BSD 4.0和BSD 4.1版本。从此，UNIX系统走上了以AT&T和伯克利分校二者为主的开发道路。例如，1983年AT&T推出了UNIX systems V和几种微处理机上的UNIX操作系统，而伯克利分校公布了BSD 4.2版本。1986年，UNIX systems V又发展为它的改进版Res 2.1和Res 3.0，而BSD 4.2又升级为BSD 4.3。

在这种背景下，美国IEEE组织成立了POSIX委员会，专门进行UNIX标准化方面的工作。此外，1988年，以AT&T和Sun Microsystems等公司为代表的UI(UNIX International)和以DEC、IBM等公司为代表的OSF(Open Software Foundation)组织也开始了这种标准化工作。它们对UNIX的开发工作虽不一样，但却定义了UNIX的统一标准，即可以运行UNIX应用软件的操作系统就是UNIX。从而统一UNIX系统的关键就变成是否能提供一个标准的用户界面，而不在于其系统内部是如何实现的了。

像使用文件那样使用任一设备，而不必了解该设备的内部特性，这既简化了系统设计，又方便了用户的使用。

1. UNIX系统的特点

UNIX系统具有很多特点，所以得到了广泛的应用。其主要特点表现在如下几个方面：

(1) 多用户的分时操作系统，即不同的用户分别在不同的终端上进行交互式的操作，就好像各自单独占用主机一样。

(2) 可移植性好。硬件的发展是极为迅速的，迫使依赖于硬件的基础软件特别是操作系统不断地进行相应的更新。由于UNIX几乎全部是用可移植性很好的C语言编写的，其内核极小，模块结构化，各模块可以单独编译。所以，一旦硬件环境发生变化，只要对内核中有关的模块进行修改，编译后与其他模块装配在一起，即可构成一个新的内核，而内核上层完全可以不动。

(3) 可靠性强。经过十几年的考验，UNIX系统已成为一个成熟而且比较可靠的系统。在应用软件出错的情况下，虽然性能会有所下降，但工作仍能可靠进行。

(4) 开放式系统，即UNIX具有统一的用户界面，使得UNIX用户的应用程序可在不同环境下运行。此外，其核心程序和系统的支持软件大多都用C语言编写。

(5) 它向用户提供了两种友好的用户界面。其一是程序级的界面，即系统调用，使用户能充分利用UNIX系统的功能，它是程序员的编程接口，编程人员可以直接使用这些标准的实用子程序。例如，对有关设备管理的系统调用read、write，便可对指定设备进行读

此为试读，需要完整PDF请访问：www.ertongbook.com