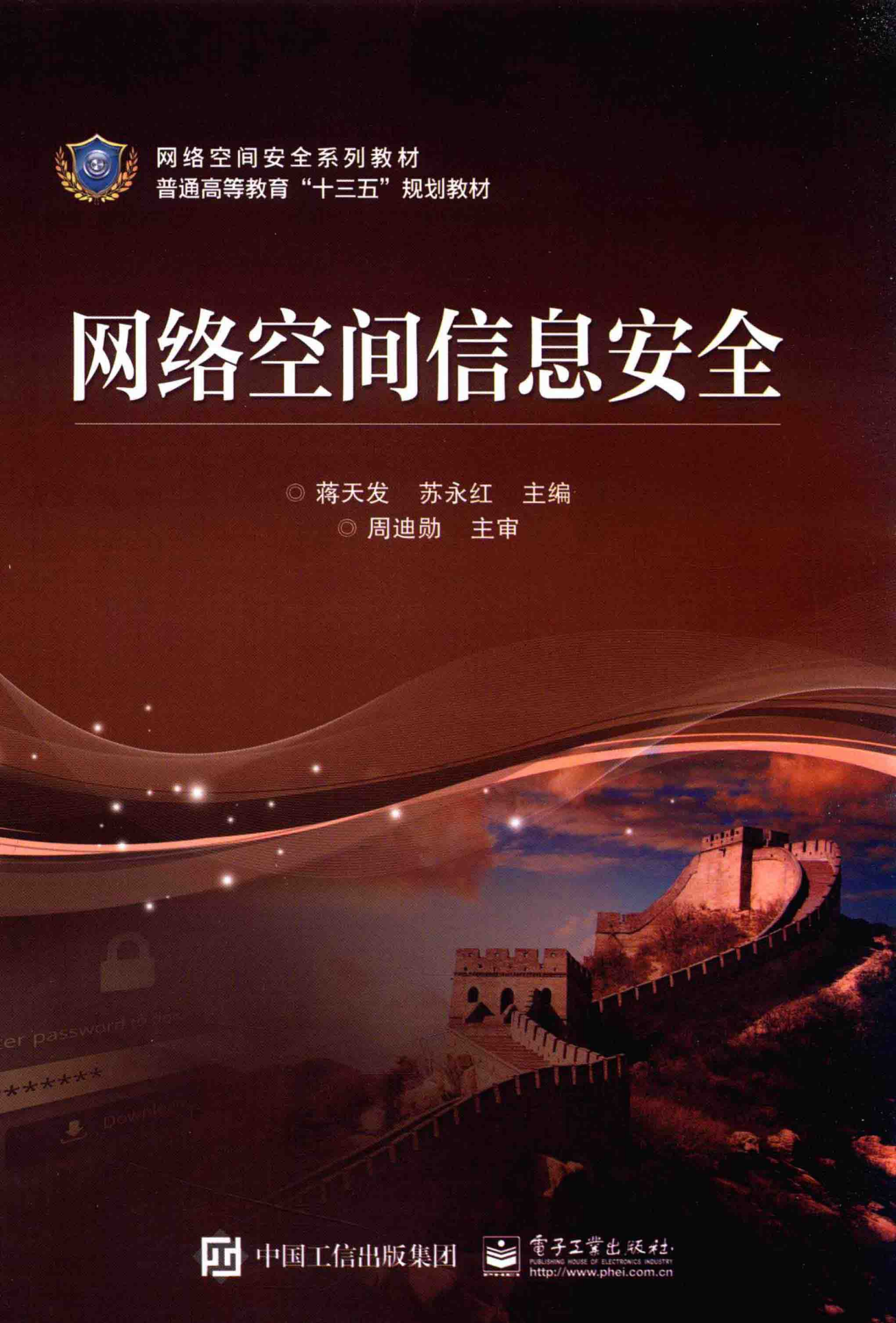
网络空间安全系列教材
普通高等教育“十三五”规划教材

网络空间信息安全

◎ 蒋天发　苏永红　主编
◎ 周迪勋　主审



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

网络空间安全系列教材
普通高等教育“十三五”规划教材

网络空间信息安全

蒋天发　苏永红　主　编
毋世晓　柳　晶　牟群刚　副主编
周迪勋　主审

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

内 容 简 介

本书重点阐述网络空间信息安全的基础理论和基础知识，侧重论述网络空间安全技术的选择策略，安全保密的构建方法和实现技能。本书共分 13 章，主要内容包括网络空间信息安全概论、病毒防范技术、远程控制与黑客入侵、网络空间信息密码技术、数字签名与验证技术、网络安全协议、无线网络安全机制、访问控制与防火墙技术、入侵防御系统、网络数据库安全与备份技术、信息隐藏与数字水印技术、网络安全测试工具及其应用、网络信息安全实验及实训指导等。本书配有免费电子教学课件。

本书内容丰富，结构合理，可作为普通高等院校和高等职业技术学校网络空间信息安全、计算机及相关专业课程的教材，也可供从事网络空间信息安全方面工作的工程技术人员参考使用。

图书在版编目（CIP）数据

网络空间信息安全 / 蒋天发，苏永红主编. —北京：电子工业出版社，2017.2

ISBN 978-7-121-29958-2

Ⅰ. ①网… Ⅱ. ①蒋… ②苏… Ⅲ. ①计算机网络—信息安全 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2016）第 229078 号

策划编辑：王晓庆
责任编辑：郝黎明
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：24　字数：706 千字
版　　次：2017 年 2 月第 1 版
印　　次：2017 年 2 月第 1 次印刷
定　　价：55.00 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：（010）88254113，wangxq@phei.com.cn。

前　言

现在人们享受互联网（Internet）以及互联网+带来的便利的同时，也面临着种种网络空间安全危机。然而，或许是互联网以及互联网知识欠缺，或许是过于信任开发厂商，大多数人只是将互联网以及互联网+作为一种学习、娱乐、办公、社交的便捷方式，而忽略了与互联网+如影随形的网络空间安全风险，使个人隐私与利益面临着种种威胁。目前，互联网以及互联网+逐渐暴露出越来越多的安全问题，各种网络空间安全现象日益突出，很多研究机构都在针对网络空间信息安全问题积极展开教研工作。

在计算机系统和互联网以及互联网+这个平台上，许许多多的革新正在不知不觉中上演，人们需要及时更新自己的思维与视角，才能跟上时代的步伐。网络空间信息安全是一个交叉学科，和众多学科一样，在解决问题时有两个经典思路：其一，碰到一个问题，解决一个问题，即可以自下而上一点儿一点儿拼成系统；其二，构想系统应该是什么样子的，自上而下宏观思考构建系统。本书有针对性地介绍了网络空间信息安全问题的产生，以及网络安全威胁的攻击与防范等读者关心的具体问题，并针对这些问题提出了具体的解决方案。

本书是在 2009 年出版的《网络信息安全》的基础上，针对普通高等院校和高等职业技术学校网络空间信息安全、计算机及相关专业课程的教学现有特点，将相关理论、专业知识与工程技术相结合编写而成的。本书力求紧跟国内网络空间信息安全技术的前沿领域，全面、通俗、系统地反映了网络空间信息安全的理论和实践。全书共分 13 章，主要包括网络空间信息安全概论、病毒防范技术、远程控制与黑客入侵、网络空间信息密码技术、数字签名与验证技术、网络安全协议、无线网络安全机制、访问控制与防火墙技术、入侵防御系统、网络数据库安全与备份技术、信息隐藏与数字水印技术、网络安全测试工具及其应用、网络信息安全实验及实训指导。全书由蒋天发教授统稿，蒋天发和苏永红担任主编。其中，苏永红编写第 1、5、9 章，柳晶编写第 2、10 章，蒋天发编写第 3、4、8、13 章，毋世晓编写第 6、7 章，牟群刚编写第 11、12 章。

本书在出版之际，新加坡南洋理工大学马懋德（Maode Ma）教授为本书体系结构调整进行了指导；本书主审武汉理工大学（原网络中心主任、博导）周迪勋教授、中南民族大学计算机科学学院硕士研究生张颖同学对全书进行了整理；电子工业出版社王晓庆（策划编辑）、中国软件评测中心蒋巍和张博（新华保险公司）夫妇对本书出版给予了大力支持和帮助，在此表示衷心感谢！

本书配有免费电子教学课件，请登录华信教育资源网（http://www.hxedu.com.cn）注册下载，也可联系本书编辑（wangxq@phei.com.cn）索取。

在本书的策划与编写过程中，编者参阅了国内外有关的大量文献和资料（包括网站），从中得到有益启示；也得到了国家自然科学基金项目（40571128）和武汉华夏理工学院科研项目（16038）与精品共享课程项目（2014105）的全体成员，以及武汉华夏理工学院和中南民族大学的有关领导、同事、朋友及学生的大力支持和帮助，在此表示衷心感谢！

由于网络空间信息安全的技术发展非常快，本书的选材和编写还有一些不尽如人意的地方，加上编者学识水平和时间所限，书中难免存在缺点和谬误，恳请同行专家及读者指正，以便进一步完善提高。编者联系方式：jiangtianta@163.com。

编　者

目　录

第1章 网络空间信息安全概论

本 章 提 要

本章首先阐述网络空间信息安全的重要意义，指出信息安全是国家安全的重要基础，然后列出一些网络空间面临的安全问题，如电子邮件的安全问题、域名系统的安全威胁、IP 地址的安全问题、Web 站点的安全问题等，简要介绍了本课程的主要内容，即病毒防范技术、远程控制与黑客入侵、网络信息密码技术、数字签名与验证技术、网络安全协议、无线网络安全机制、访问控制与防火墙技术、入侵检测技术、网络数据库安全与备份技术、信息隐藏与数字水印技术、网络安全测试工具及其应用，又介绍了网络空间信息安全与网络信息安全的区别，最后介绍了网络空间信息安全的七大趋势。

1.1 网络空间信息安全的重要意义

进入信息社会，信息已经成为一种非常重要的资源，它的安全与否已经影响到个人、企业甚至国家的根本利益。网络空间信息安全是一个涉及网络技术、通信技术、密码技术、信息安全技术、计算机科学、应用数学、信息论等多种学科的边缘性综合学科。网络空间信息安全是国家安全的重要基础，网络信息在国民经济建设、社会发展、国防和科学研究等领域的作用日益重要。实际上，网络的快速普及与发展、客户端软件多媒体化、协同计算、资源共享、开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。确保网络空间信息安全至关重要，没有网络空间信息的安全就谈不上网络信息的应用。当今，由于计算机互联网的迅速发展和广泛应用，它打破了传统的时间和空间的局限性，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。计算机网络和通信是促进信息化社会发展的最活跃的因素。然而，任何事物的发展都具有两重性。由于计算机互联网的国际化、社会化、开放化、个性化的特点，使它在向人们提供网络信息共享、资源共享和技术共享的同时，也带来了不安全的隐患。网络空间信息安全问题已威胁到国家的政治、经济和国防等领域。这是因为对互联网的非法侵入或人为的故意破坏，将会轻而易举地改变互联网上的应用系统或导致网络瘫痪，从而使网络用户在军事、经济、政治上造成无法弥补的巨大损失。因此，很早就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器和化学武器之后的第四大武器。网络信息的泄露、篡改、假冒和重传，黑客入侵，非法访问，计算机犯罪，计算机病毒传播等对网络信息安全已构成重大威胁。如果这些问题不解决，国家安全会受到威胁，电子政务、电子商务、网络银行、网络科研、远程教育、远程医疗等都将无法正常开展，个人的隐私信息也得不到保障。

网络空间是一个虚拟的空间，用规则管理起来，我们称之为“网络空间”。虚拟空间包含了三个基本要素：第一个是载体，也就是通信信息系统；第二个是主体，也就是网民、用户；第三个是构造一个集合，用规则管理起来，我们称之为“网络空间”。网络空间是人运用信息通信系统进行交互的空间，其中信息技术通信系统包括各类互联网、电信网、广电网、物联网、在线社交网络、计算系统、通信系统、控制系统、电子或数字信息处理设施等。人间交互指信息通信技术活动。网

络空间安全涉及网络空间中的电子设备、电子信息系统、运行数据、系统应用中存在的安全问题，分别对应这四个层面：设备、系统、数据、应用。

网络空间信息安全包括两个部分：防治、保护、处置包括互联网、电信网、广电网、物联网、工控网、在线社交网络、计算系统、通信系统、控制系统在内的各种通信系统及其承载的数据不受损害；防止对这些信息通信技术系统的滥用所引发的政治安全、经济安全、文化安全、国防安全。一个是保护系统本身，另一个是防止利用信息系统带来其他的安全问题。所以针对这些风险，要采取法律、管理、技术、自律等综合手段来应对，而不能像过去一样信息安全主要依靠技术手段。

1.2 网络空间面临的安全问题

网络空间面临的安全问题包括 Internet 安全问题、电子邮件的安全、域名系统的安全问题、IP 地址的安全问题、Web 站点的安全问题、文件传输的安全问题、社会工程学的安全问题。

1.2.1 Internet 安全问题

Internet 是全球最大的信息网络，它的发展促进了国家的政治、军事、文化和人们生活水平的提升，甚至改变了人们的生活、学习和工作方式。Internet 是一个开放系统。窃密与破坏已经从个人、集团的行为上升到国家的信息战行为。其不安全的问题日显突出。据 CERT/CC 统计，在历年的 Internet 网络安全案件中，其安全威胁来自黑客攻击和计算机病毒。Internet 的安全来自内因和外因的各种因源。

（1）站点主机数量的增加，无法估计其安全性能。网络系统很难动态适应站点主机数量的突增，系统网管功能升级困难也难以保证主机的安全性。

（2）主机系统的访问控制配置复杂、软件的复杂等，没有能力在各种环境下进行测试，UNIX 系统从 BSD 获得网络部分代码。而 BSD 源代码可轻易获取，导致攻击者易侵入网络系统。

（3）分布式管理难于预防侵袭，一些数据库用口令文件进行分布式管理，又允许系统共享数据和共享文件，这就带来不安全因素。

（4）验证环节虚弱。Internet 中的许多事故源于虚弱的静态口令，易被破译，且易于解密或通过监视信道窃取口令。TCP/IP 和 UDP 服务也只能对主机地址进行验证，而不能对指定的用户进行验证。

（5）Internet 和 FTP 的用户名及口令的 IP 包易被监视与窃取。使用 Internet 或 FTP 连接到远程主机上的账户时，在 Internet 上传输的口令是没有加密的，攻击者通过获取的用户名和口令的 IP 包登录到系统。

（6）攻击者的主机易冒充成被信任的主机。这种主机的 IP 地址是被 TCP 和 UDP 信任的，导致主机失去安全性。攻击者用客户 IP 地址取代自己的 IP 地址或构造一条攻击的服务器与其主机的直接路径，客户误将数据包传送给攻击者的主机。

一般 Internet 服务安全内容包括 E-mail 安全、文件传输（FTP）服务安全、远程登录（Telnet）安全、Web 浏览服务安全和 DNS 域名安全、设备的物理安全以及社会工程学的安全问题。

1.2.2 电子邮件（E-mail）的安全问题

E-mail 即电子邮件，是一种用电子手段提供信息交换的通信方式，也是全球网上最普及的服务方式，数秒内通过 E-mail 传遍全球，它加速了信息交流。E-mail 除传递信件之外，还可以传送文件（当作附件）、声音、图形等信息。

E-mail 不是“终端到终端”的实时服务，而是“存储转发式”服务，它非实时通信，而发送者可随时随地发送邮件，将邮件存入对方电子邮箱，并不要求对方接收者实时在场收发邮件，其优点是不受时间、空间约束。

E-mail 邮件系统的传输过程包括邮件用户代理（Mail User Agent，MUA）、邮件传输代理（Mail Transfer Agent，MTA）和邮件接收代理（Mail Delivery Agent，MDA）三部分。用户代理是一个用户端发信和收发的程序，负责将信件按一定的标准进行包头，然后送到邮件服务器。传输代理负责信件的交换和传输，将信件传送到邮件主机，再交给接收代理。接收代理按收信人的地址，根据简单邮件传输协议将信件传递到目的地。一般采用 Sendmail 程序来完成此工作。接收代理的 POP（Post Office Protocol）网络邮局协议或网络中转协议能使用户在自己的主机上读取这份邮件。E-mail 服务器是向全体开放的，故有一个“路由表”，列出了其他 E-mail 服务器的目的地地址。当服务器读取信头时，如果不是发给自己的，会自动转发到目的地的服务器。

E-mail 的正常服务靠的是 E-mail 服务协议。有以下几种 E-mail 相关协议。

（1）SMTP。

简单邮件传输（Simple Mail Transfer Protocol，SMTP）是邮件传输协议。经过它传递的电子邮件都是以明文形式进行的，但这种明文传输很容易被中途窃取、复制或篡改。

（2）ESMTP。

ESMTP（Extended SMTP）指扩展型 SMTP。其主要有不易被中途截取、复制或篡改的功能。

（3）POP。

POP3 是邮局协议，其在线工作，有邮件保留在邮件服务器上允许用户从邮件服务器收发邮件的功能。POP3 是以用户当前存在邮件服务器上的全部邮件为对象进行操作的，并一次性将它们下载到用户端计算机中。但用户不需要的邮件也下载了。

（4）IMAP4。

Internet 消息访问协议版本 4（Internet Message Access Protocol，IMAP4）为用户提供了有选择地从邮件服务器接收邮件的功能。IMAP4 在用户登录到邮件服务器之后，允许采取多段处理方式，查询邮件，用户只读取电子信箱中的邮件信头，然后下载指定的邮件。

（5）MIME。

MIME（Multipurpose Internet Mail Extensions）协议的功能是将计算机程序、声音和视频等二进制格式信息先转换成 ASCII 文本，然后利用 SMTP 传输这些非文本的电子邮件，也可随同文本电子邮件发出。

E-mail 的安全漏洞有以下几种。

（1）窃取 E-mail。从浏览器向 Internet 上另一方发送 E-mail 时，要经过许多路径上的网络设备，故入侵者可在路径上窃取 E-mail 或伪造 E-mail。

（2）Morris 内有一种会破坏 Sentmail 的指令。这种指令可使其执行黑客发出的命令，故 Web 提供的浏览器更容易受到侵袭。

（3）E-mail 轰炸，E-mail Spamming 和 E-mail 炸弹。E-mail 炸弹（End Bomb 和 KaBoom）能把攻击目标加到近百个 E-mail 列表中。Up Yours 是最流行的炸弹程序，它使用最少的资源，又隐藏自身攻击者的源头而进行攻击。E-mail 轰炸使同一收件人会不停地接到大量同一内容的 E-mail，使电子信箱挤满而不能工作。E-mail Spamming 是同一条信息被传给成千上万的不断扩大的用户，如果一个人用久了 E-mail Spamming，那么所有用户都会收到这封信。E-mail 服务器如果收到很多 E-mail，服务器会脱网，导致系统崩溃，不能服务。

（4）E-mail 欺骗。E-mail 伪称来自网络系统管理员，要求用户将口令改变为攻击者的特定字符串，并威胁用户，如果不按此处理，将关闭用户的账户。

（5）虚构某人名义发出 E-mail。由于任何人都可以与 SMTP 协议的端口连接，故攻击者可以虚构某人名义利用与 SMTP 协议连接的端口发出 E-mail。

（6）电子邮件病毒。由于 Outlook 存在安全隐患，可让攻击者编制一定的代码使病毒自动执行，病毒多以 E-mail 附件形式传给用户，一旦用户点击该附件，计算机就会中毒。故不要打开不明的邮件，如果要打开附件，应先用防毒软件扫描一下，确保附件无病毒。E-mail 为计算机病毒最主要的传播媒介。

E-mail 的安全措施包括以下几种。

（1）在邮件系统中安装过滤器，在接收任何 E-mail 之前，先检查（过滤）发件人的资料，删去可疑邮件，不让它进入邮件系统。

（2）防止 E-mail 服务器超载，超载会降低传递速度或不能收发 E-mail。

（3）如有 E-mail 轰炸或遇上 E-mail Spamming，就要通过防火墙或路由器过滤来自这个地址的 E-mail 炸弹邮包。

（4）防止 E-mail 炸弹指删除文件或在路由的层次上限制网络的传输。另一种方法是写一个 Script 程序，当 E-mail 连接到自己的邮件服务器时，它就会捕捉到 E-mail 炸弹的地址，对邮件炸弹的每一次连接，它都会自动终止其连接，并回复一个声明指出触犯法律。

（5）严禁打开 E-mail 附件中的可执行文件（.EXE、.COM）及 Word/Excel 文档，因为这些多是病毒“特洛伊木马”的有毒文件。

1.2.3 域名系统的安全问题

域名系统（Domain Name System，DNS）是一种用于 TCP/IP 应用程序的分布式数据库，它的作用是提供主机名称和地址的转换信息。网络用户通过 UDP 协议与 DNS 域名服务器进行通信，而服务器在特定的 53 端口监听，并返回用户所需要的相关信息，这是正向域名解析的过程，而反向域名解析是一个查询 DNS 的过程。当用户向一台服务器请求服务时，服务器会根据用户的 IP 地址反向解析出其对应的域名。

域名系统的安全威胁有以下几种。

（1）DNS 会查漏内部的网络拓扑结构，故 DNS 存在安全隐患。整个网络架构中的主机名、主机 IP 列表、路由器名、路由器 IP 列表、计算机所在位置等可以被轻易窃取。

（2）攻击者控制了 DNS 服务器后，就会篡改 DNS 的记录信息，利用被篡改的记录信息达到入侵整个网络的目的，使到达原目的地的数据包落入攻击者控制的主机。

（3）DNS 服务器有其特殊性，在 UNIX 中，DNS 需要 UDP 53 和 TCP 53 的端口，它们需要使用 root 执行权限，这样防火墙很难控制对这些端口的访问，导致入侵者可窃取 DNS 服务器的管理员权限。

（4）DNS ID 欺骗行为：黑客伪装的 DNS 服务器提前向客户端发送响应数据包，使客户端的 DNS 缓存里域名所对应的 IP 变成黑客自定义的 IP，于是客户端被带到黑客设定的网站。

域名系统的威胁解除办法：遇到 DNS 欺骗，先禁止本地连接，然后启用本地连接即可消除 DNS 缓存。如果在 IE 中使用代理服务器，DNS 欺骗就不能进行，因为这时客户端并不会在本地进行域名请求。如果访问的不是网站主页，而是相关子目录的文件，则在自定义的网站上不会找到相关的文件。所以，禁用本地连接，再启用本地连接就可以清除 DNS 欺骗。

1.2.4 IP 地址的安全问题

IP 地址的安全威胁有以下几种。

（1）盗用本网段的 IP 地址，但会记录下物理地址。在路由器上设置静态 ARP 表，可以防止在

本网段盗用 IP。路由器会根据静态 ARP 表检查数据，如果不能对应，则不进行处理。

（2）IP 电子欺骗：IP 欺骗者通过 RAW Socket 编程，发送带有伪造的源 IP 地址的 IP 数据包，让一台机器来扮演另一台机器达到的目的，获得对主机未授权的访问。即使设置了防火墙，如果没有配置对本地区域中资源 IP 包地址的过滤，这种 IP 欺骗仍然奏效。当黑客进入系统后，黑客绕过口令及身份验证，专门等候合法用户连接登录到远程站点，一旦合法用户完成其身份验证，黑客就可控制该连接。这样，远程站点的安全就被破坏了。

IP 欺骗攻击的防备有以下几种办法。

（1）通过对包的监控来检查 IP 欺骗。可用 netlog 或类似的包监控工具来检查外接口上包的情况，如发现包的两个地址——源地址和目的地址都是本地域地址，就意味着有人试图攻击系统。

（2）安装一个过滤路由器，来限制对外部接口的访问，禁止带有内部网资源地址包的通过。当然也应禁止（过滤）带有不同的内部资源地址内部包通过路由器到其他网络中，这就防止内部的用户对其他站点进行 IP 欺骗。

（3）将 Web 服务器放在防火墙外面有时更安全。如果路由器支持内部子网的两个接口，则易引发 IP 欺骗。

（4）在局部网络的对外路由器上加一个限制条件，不允许声称来自内部网络包通过，也能防止 IP 欺骗。

1.2.5 Web 站点的安全问题

Web 服务器有以下安全漏洞。

（1）安全威胁类来源有以下几种。

①外部接口。

②网络外部非授权访问。

③网络内部的非授权访问。

④商业或工业间谍。

⑤移动数据。

（2）入侵者会重点针对访问攻击某个数据库、表、目录，达到破坏数据或攻击数据的目的。

（3）进行地址欺骗、IP 欺骗或协议欺骗。

（4）非法偷袭 Web 数据，如电子商务或金融信息数据。

（5）伪装成 Web 站点管理员，攻击 Web 站点或控制 Web 站点主机。

（6）服务器误认闯入者是合法用户，而允许其访问。

（7）伪装域名，使 Web 服务器向入侵者发送信息，而客户无法获得授权访问的信息。

常用的 Web 站点安全措施有以下几种。

（1）将 Web 服务器当作无权限的用户运行，很不安全，故要设置权限管理。

（2）将敏感文件放在基本系统中，再设置二级系统，所有敏感文件数据都不向 Internet 开放。

（3）要检查 HTTP 服务器使用的 Applet 和脚本，尤其是与客户交互作用的 CGI 脚本，以防止外部用户执行内部指令。

（4）建议在 Windows NT 上运行 Web 服务器，并检查驱动器和共享的权限，将系统设为只读状态。

（5）采用 Macintosh Web 服务器更为安全，但又缺少 Windows NT 的一些设置特性。

（6）要克制 daemons 系统的软件安全漏洞。daemons 会执行不要执行的功能，如控制服务、网络服务、与时间有关的活动及打印服务。

（7）为防止入侵者用电话号码作为口令进入 Web 站点，要配备能阻止和覆盖口令的收取机制

及安全策略。

（8）不断更新、重建和改变 Web 站点的连接信息，一般 Web 站点只允许单一种类的文本作为连接资源。

（9）假设 Web 服务器放置在防火墙的后面，就可将“Wusage”统计软件安装在 Web 服务器内，以控制通过代理服务器的信息状况，这种统计工具能列出站点上往返最频繁的用户名单。

（10）安装在公共场所的浏览器，以防被入侵者改变浏览器的配置，并获得站点机要信息、IP 地址、DNS 入口号等，故要做防御措施。

1.2.6 文件传输的安全问题

文件传输协议（File Transfer Protocol，FTP）是为用户在 Internet 上主机之间进行收发文件提供的协议。FTP 使用客户机/服务器模式。当使用客户端程序时，用户的命令要求 FTP 服务器传送一个指定文件，服务器会响应发送命令，并传送这个文件，存入用户机的目录中。FTP 传送条件是用户拥有 FTP 服务器的权限。FTP 可通过 CERN 代理服务器访问该服务器或直接访问该服务器。

目前，FTP 的安全问题是 FTP 自身的安全问题及协议的安全功能如何扩展。即便使用安全防火墙，黑客仍有可能访问 FTP 服务器，故 FTP 存在安全问题。

FTP 的安全漏洞有以下几种。

（1）代理 FTP 中的跳转攻击。代理 FTP 是 FTP 规范 PR85 提供的一种允许客户端建立的控制连接，是在两台 FTP 服务器间传输文件的机制。可以不经过中间设备传给客户端，再由客户端转给另一个服务器，这就减少了网络流量，但攻击者可以发出一个 FTP“PORT”命令给目标 FTP 服务器，其中包括该被攻击主机的网络地址和与命令及服务相对应的端口号。这样，客户端就能命令 FTP 服务器发送数据给被攻击的服务器。由于通过第三方连接的，使跟踪攻击者出现难度。其防范措施有：①禁止使用 PORT 命令，而通过 PASV 命令来实现传输，缺点是损失了使用代理 FTP 的能力；②服务器不打开数据连接到小于 1024 的 TCP 端口号，因为 PR85 规定 TCP 端口从 0～1023 是留给用户服务器的端口号，而 1024 以上的服务才是由用户自定义的服务。

（2）FTP 软件允许用户访问所有系统中的文件，且 FTP 文件系统存在可写区域可供攻击者删改文件。

（3）地址被盗用。基于网络地址的访问，会使 FTP 服务器的地址易被盗用，攻击者冒用组织内的机器地址，从而将文件下载到组织外未授权的机器上，防范措施是加上安全鉴别机制。

（4）用户名和密码被猜测。为了防止用户名和密码被猜测，FTP 服务器要限制大于 5 次的查询尝试，停止设备的 5 次以上尝试的控制连接。此时，应给用户一个响应返回码 421，表示服务器不可用，即将关闭控制连接。

（5）端口盗用。

因为用户要获得一个 TCP 端口号，才能连接上一个 FTP 服务器，故端口号易被盗用。从而使黑客盗取合法用户的文件或从授权用户发出的数据流中伪造文件。为防止端口盗用，可以采取随机性分配端口号。

FTP 的安全措施有以下几种。

（1）未经授权的用户禁止进行 FTP 操作，FTP 使用的账号必须在 password 文件中有记载，并且它的口令不能为空。凡是被 FTP 服务器拒绝访问的账号和口令都记录在 FTP 的保护进程 FTP 的 /ete/FTPuser 文件中，凡在此文件出现的用户将拒绝访问。

（2）保护 FTP 使用的文件和目录。

① FTP\bin 目录的所有者设为 root，此目录主要放置系统文件，设为用户不可访问的文件。

② FTP\exe 目录的所有者设为 root，此目录存放 group 文件和 password 文件，设为只读属性，