21世纪高等院校网络工程规划教材

21st Century University Planned Textbooks of Network Engineering

网络安全基础教程

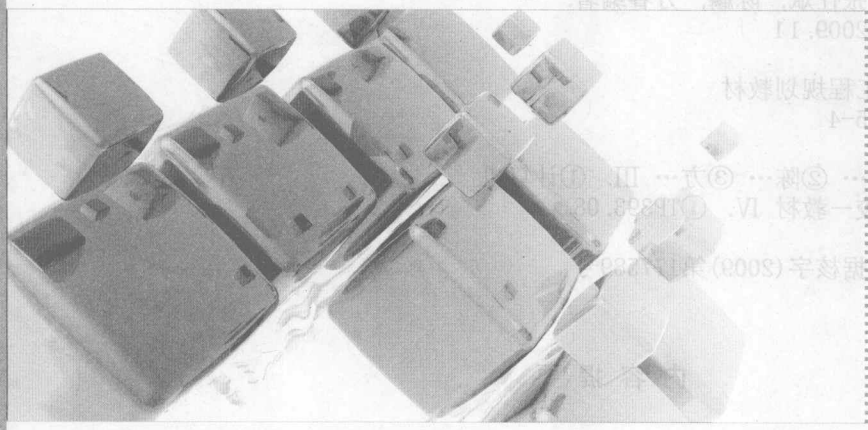
Network Security

张仕斌 陈麟 方睿 编著

- 内容全面，结合现实平台和网络安全规范
- 结构严谨，强调理论知识与实践操作结合
- 实用系统，通俗阐述最新的网络安全技术

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等院校网络工程规划教材
21st Century University Planned Textbooks of Network Engineering



网络安全基础教程

Network Security

张仕斌 陈麟 方睿 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全基础教程 / 张仕斌，陈麟，方睿编著. -- 北京 : 人民邮电出版社，2009.11

21世纪高等院校网络工程规划教材
ISBN 978-7-115-20215-4

Ⅰ. ①网… Ⅱ. ①张… ②陈… ③方… 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(2009)第177589号

内 容 提 要

网络安全理论与技术是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全理论与技术等多学科的综合性学科。本书用通俗的语言全面阐述了网络安全理论与技术。全书内容包括网络安全基础知识、密码技术、信息隐藏技术、数字签名技术、认证技术、网络入侵与攻击技术、网络安全防范技术、操作系统安全技术、数据与数据库安全技术、软件安全技术、Web 安全技术、网络互连安全技术等。

本书内容全面，深入浅出，构思新颖，突出实用，系统性强，可作为普通高等院校计算机、通信、网络工程、信息安全等相关专业的教材，也可供计算机、通信、信息等领域研究人员和专业技术人员参考。

21 世纪高等院校网络工程规划教材

网络安全基础教程

◆ 编　　著　张仕斌　陈　麟　方　睿
责任编辑　蒋　亮

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：21.5
字数：538 千字　　2009 年 11 月第 1 版
印数：1－3 000 册　　2009 年 11 月河北第 1 次印刷

ISBN 978-7-115-20215-4

定价：36.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

随着 Internet 的普及和 Internet 技术的不断发展，网络已经影响到政治、经济、文化、军事和社会生活的各个方面，已成为全球信息基础设施的主要组成部分。网络作为一把双刃剑，在加快人类社会信息化进程的同时，也给保障信息安全带来了极大的挑战。一方面，私人数据、重要的企业资源、政府机密信息等被暴露在公共网络空间中，而 Internet 的开放性使得这些重要信息很容易被获取；另一方面，计算机病毒的种类和数量也在迅猛增长，并且其借助网络传播的速度越来越快，危害面越来越广，破坏程度也越来越大。在人类社会进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求越来越迫切，而且显得尤为重要，它不仅关系到每个人的切身利益，甚至也关系到国家的安危、科技的进步、经济的发展。因此，网络安全已成为社会各界关注的热点问题。

当前，我国网络安全正面临着严峻的考验：一方面，随着电子政务、电子商务、电子现金、数字货币、网络银行、网络证券等的广泛应用，网络安全的需求更加严格和迫切；另一方面，黑客攻击、病毒传播以及形形色色的网络攻击日益增加，网络安全防线十分脆弱。因此，加快培养网络安全应用型人才、普及网络安全知识和掌握网络安全技术迫在眉睫。

本书是在广泛调研和充分论证的基础上，结合当前应用最为广泛的操作平台和网络安全规范，并通过研究实践编写而成的。在写作中，作者始终遵循这样一个原则：为网络安全领域提供一本既可以作为教学用书，也可以作为专业技术人员的参考书。

本书特别强调理论与实践相结合，具有科学严谨的体系结构，内容全面，深入浅出，构思新颖，突出实用，系统性强，并利用通俗的语言全面阐述了网络安全理论与实践技术。每章在授课中融合了实践内容，使理论联系实际，并配有相应的习题。全书内容包括网络安全基础知识、密码技术、信息隐藏技术、数字签名技术、认证技术、网络入侵与攻击技术、网络安全防范技术、操作系统安全技术、数据与数据库安全技术、软件安全技术、Web 安全技术、网络互连安全技术等。为了便于多媒体教学，本书配有相应的电子教案。

本书由张仕斌组织编写及统稿工作，其中第 1～6 章由张仕斌编写，第 7 章由陈麟和谭三编写，第 8 章由陈敏和彭城编写，第 9 章由方睿编写，第 10 章由安宇俊编写，第 11 章由付林编写，第 12 章由黄南铨编写。

为了便于多媒体教学，本书配有电子教案，订购本教材的教师可到人民邮电出版社教学服务与资源网（www.ptpedu.com.cn）上下载。

由于作者水平有限，加上时间仓促，书中难免有不足和错误之处，欢迎广大读者批评指正。

作　者

2009 年 9 月于成都

目　录

第1章 绪 论

随着网络及其应用技术的飞速发展，人们对互联网的依赖越来越强，网络已经成为人们生活中不可缺少的一部分。但是，网络作为一把双刃剑，在加快人类社会信息化进程的同时，也给保障网络及信息安全带来了极大的挑战。网络犯罪事件屡见不鲜，且呈逐年上升趋势。在人类社会进入信息化时代的今天，人们对信息的安全传输、安全存储、安全处理的要求越来越迫切,而且显得尤为重要，它不仅关系到每个人的切身利益，而且也关系到战争的胜负、国家的安危、科技的进步、经济的发展。本章主要介绍网络安全基础知识、网络安全的规划与管理、网络安全策略与风险和网络安全标准与法律法规等当前网络安全领域的有关基础知识。通过对本章的学习，使读者对网络安全及相关知识有一个粗略的了解，这对于按计划学好本书后续知识具有重要的指导作用。

1.1 网络安全基础知识

随着科学技术的飞速发展，人们对 Internet 的依赖性越来越强，网络已经成为人们生活中不可缺少的一部分。但是，互联网是一个开放、自由的系统，对信息系统的安全考虑并不完善。近年来，随着计算机和网络技术的广泛应用，计算机及网络系统被攻击与破坏的事件不胜枚举。网络犯罪已经渗入到各行各业，已成为现代社会的隐患，轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家的安全。目前，计算机及网络系统安全问题已经引起了世界各国的高度重视，各国不惜投入大量的人力、物力和财力来保障计算机及网络系统的安全。

1.1.1 计算机及网络系统所面临的安全威胁

现在讲安全已经不再像以前那样仅简单地谈计算机病毒，安全的防御也不再仅是安装了病毒软件和防火墙就能达到目的，这是因为计算机及网络系统所面临的威胁正随着计算机和网络技术的广泛应用不断增加。

1. 计算机所面临的主要安全威胁

随着个人计算机的普及，个人计算机也已成为黑客攻击的目标之一，计算机目前所面临的安全威胁主要涉及以下几个方面。

（1）计算机病毒

计算机病毒是当前计算机系统中最常见、最主要的威胁，几乎每天都有新的计算机病毒

产生。当然计算机病毒也有很多种，具体将在后面章节介绍。

计算机病毒的主要危害体现在：破坏计算机文件和数据，导致文件无法使用，系统无法启动；消耗计算机 CPU、内存和磁盘资源，导致一些正常服务无法进行，出现死机、占用大量磁盘空间的现象；有的还会破坏计算机硬件，导致计算机彻底瘫痪。

关于计算机病毒的防护，对于用户来说首先是安装计算机病毒防护软件（包括个人版或网络版），自动监测并查杀已感染的病毒的文件或数据；当然，对于高级用户来说也可以进行一些手工清除，但相对来说比较困难。后续章节将介绍一些典型的计算机病毒。

（2）木马

木马是一种基于远程控制的黑客工具，也称为“后门程序”。以前，我们一直说木马不是病毒，而现在一些专家把木马也归属于病毒。但是木马和病毒确实存在许多本质上的区别，具体将在后面的章节介绍。

目前，木马作为一种远程控制的黑客工具，主要危害包括窃取用户信息（比如计算机或网络账户和密码、网络银行账户和密码、QQ 账户和密码、E-mail 账户和密码等）、携带计算机病毒（造成计算机或网络不能正常运行，甚至完全瘫痪）或被黑客控制，攻击用户计算机或网络。关于木马的详细介绍也将在后面的章节进行。

（3）恶意软件

恶意软件是指一类特殊的程序，是介于计算机病毒与黑客软件之间的软件的统称。它通常在用户不知晓、也未授权的情况下潜入系统，具有用户不知道（一般也不许可）的特性，激活后将影响系统或应用的正常功能，甚至危害或破坏系统。其主要危害体现在非授权安装（也被称为“流氓软件”）、自动拨号、自动弹出各种广告界面、恶意共享和浏览器劫持等。当前，恶意软件的出现、发展和变化给计算机系统和网络信息系统带来了巨大的危害。尽管已经出现了很多防范措施，但恶意软件一般都很难甚至无法删除。有关恶意软件的详细内容将在后面的章节介绍。

2. 网络系统所面临的主要安全威胁

相对于个人计算机而言，网络系统所面临的安全威胁除包括计算机所面临的 3 种常见的威胁之外，主要就是网络黑客的入侵与攻击。由于互联网固有的缺陷，每个网络都有一定程度的漏洞和风险。网络系统所面临的安全威胁有多种形式，可以是对网络系统直接或间接的攻击，例如非授权的泄露、篡改或删除等，在机密性、完整性或可用性等方面造成危害，也可能是偶发或蓄意的事件。

（1）系统漏洞的威胁

系统漏洞是网络安全领域首要关注的问题，发现系统漏洞也是黑客进行入侵和攻击的主要步骤。据调查，国内 80%以上的网站存在明显的漏洞。漏洞的存在给网络上不法分子的非法入侵提供了可乘之机，也给网络安全带来了巨大的风险。据美国 CERT/CC 统计，2006 年总共收到系统漏洞报告 8 064 个，平均每天超过 22 个（自 1995 年以来，漏洞报告总数已经达到 30 780 个）。这些漏洞的存在给广大互联网用户的系统造成了严重的威胁。

当前，操作系统的漏洞是我们面临的最大风险。比如，Windows 操作系统是目前使用最为广泛的系统，但其经常被发现存在漏洞。过去 Windows 操作系统的漏洞主要被黑客用来攻击网站，对普通用户没有多大影响，但近年来一些新出现的网络病毒利用 Windows 操作系统的漏洞能够自动运行、繁衍、无休止地扫描网络和个人计算机，然后进行有目的的破坏，比

如“红色代码”、“尼姆达”、“蠕虫王”以及“冲击波”等。随着 Windows 操作系统越来越复杂和庞大，其出现的漏洞也越来越多，病毒利用 Windows 操作系统漏洞进行攻击造成的危害越来越大，甚至有可能给整个互联网带来不可估量的损失。

（2）人为因素的威胁

虽然人为因素和非人为因素都对计算机及网络系统构成威胁，但精心设计的人为攻击（因素）威胁更大。人为因素的威胁是指人为造成的威胁，包括偶发性和故意性威胁，具体来说主要包括网络攻击、蓄意入侵和计算机病毒等。一般来说，人为因素的威胁可以分为人为失误和恶意攻击。

① 人为失误。一是配置和使用中的失误，比如系统操作人员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不恰当，用户将自己的账号随意转借给他人或信息共享等都会对网络安全带来威胁。二是管理中的失误，比如用户安全意识薄弱，对网络安全不重视，安全措施不落实，导致安全事故发生。据调查表明，在发生安全事故的原因中，居前两位的分别是“未修补软件安全漏洞”和“登录密码过于简单或未修改”，这表明大多数用户缺乏基本的安全防范意识和防范常识。

② 恶意攻击。恶意攻击是当前计算机及网络面临的最大威胁，主要分为两大类：一是主动攻击，它使用各种攻击方式有选择地破坏信息的完整性、有效性和可用性等；二是被动攻击，它是在不影响计算机及网络系统正常工作的情况下，进行信息的窃取、截获、破译等，以获取重要的机密信息。这两类攻击均能对计算机及网络系统造成极大地破坏，并导致机密信息泄露。

3. 网络系统的主要安全隐患

隐患不等于威胁，但隐患来源于各种安全威胁。隐患所涉及的面要比威胁本身广得多，因为同一种威胁可能在不同方面造成安全隐患。

一般来说，个人网络安全问题仅限于与互联网连接时的网络安全，因此它唯一的安全隐患就是互联网。但对于企业网来说，其安全隐患不仅来自于互联网，内部网的安全隐患也非常值得重视，因为外网中的安全隐患同样也可以在内网中出现。即是说企业网的安全隐患有内、外网安全隐患之分。正因为如此，在企业网的安全策略设计中所考虑的不仅仅是病毒入侵、外网攻击，而是要充分考虑内、外网的安全隐患，而且内、外网的安全隐患不是完全孤立的，在大多数情况下，外网的安全问题最终来源于内网。

在当今开放式的网络环境中，网络安全隐患可以划分为以下几个大类：病毒、木马和恶意软件的入侵和感染，外部用户的攻击和入侵，内部网络用户的非法操作，数据备份与恢复等。这些安全隐患主要表现为以下几个方面：

（1）由于黑客攻击所带来的机密信息泄露或网络服务器瘫痪。

（2）由于病毒、木马或恶意软件所带来的文件损坏或丢失，甚至计算机系统破坏。

（3）重要邮件或文件的非法访问、窃取或截获与操作等。

（4）未经关键部门授权的非法访问和敏感信息的泄露等。

（5）备份数据和存储媒介的损坏和丢失等。

针对以上的主要几类安全隐患，作为网络用户来说，采取的安全策略就是一定要安装专业的网络病毒防护系统（目前包括木马、恶意软件的检测和清除功能），加强内部网络的安全管理（因为木马、恶意软件也可以通过内部网络进行传播）；配置好防火墙过滤策略和系统本

身的各项安全措施（如针对各类攻击所进行的通信协议安全配置），及时安装系统补丁（尽可能堵住系统本身所带来的安全隐患）；有条件的用户还可以在内、外网之间安装网络扫描检测、网络嗅探器（Sniffer）、入侵检测（IDS）和入侵防御（IPS）系统，甚至配置网络安全隔离系统，对内、外网进行安全隔离；加强内部网络的安全管理，严格执行“最小权限”原则，为各用户配置好恰当的用户权利和权限；同时对一些敏感数据进行加密保护，对发送的数据进行数字签名；根据网络系统的实际需要配置好相应的数据策略，并按策略认真执行。

1.1.2 网络安全的基本概念

计算机及网络所面临的安全威胁一直伴随着计算机和网络技术的发展而普遍存在。从20世纪70年代开始，计算机及网络安全问题就日益突出；到20世纪90年代，网络安全已经威胁到世界各国的利益，甚至威胁到世界各国的安全和主权问题。比如，1991年巴格达军方的指挥系统遭到攻击，1994年南非全民大选工作遭到干扰，1999年4月我国大规模爆发CIN病毒（造成巨大损失），2001年我国南部边境发生撞机事件等。由此可以看出，计算机及网络安全问题涉及方方面面，包括技术问题、法律问题和社会问题等。

1. 什么是网络安全

一般意义上讲，安全就是指客观上不存在威胁，主观上不存在恐惧，或者说没有危险和不出事故，不受威胁。对计算机及网络系统来说，其安全问题也是如此，就是要保证整个计算机及网络系统的正常运行和不受威胁。网络安全既要保证网络系统物理硬件与设施的安全，又要保证软件系统与数据信息存储、传输和处理等全部过程的安全，即通常所说的保证网络系统运行的可靠性，信息的保密性、完整性和可用性等，而且还要保证网络服务不中断（连续、可靠、安全地运行）。

由于现代的信息系统都是建立在网络基础之上的，因此网络的安全也就是信息系统的安全；而当今大家重点强调网络安全，是由于网络的广泛应用使得安全问题变得尤为突出的缘故。因此，网络安全包括系统运行的安全、系统信息的安全保护、系统信息传播后的安全和系统信息内容的安全四个方面的内容，即网络安全是对信息系统的安全运行、运行在信息系统中的信息的安全保护（包括信息的保密性、完整性和可用性保护等）、系统信息传播后的安全和系统信息内容的安全的统称。

（1）系统运行的安全是信息系统提供有效服务（即可用性）的前提，主要是保证信息处理和传输系统的安全，本质上是保护系统的合法操作和正常运行。其主要涉及计算机系统机房环境的保护，法律、政策的保护，计算机结构设计上的可靠安全的运行，计算机操作系统和应用软件的安全，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，避免因电磁泄露产生信息泄露，干扰他人（或受他人干扰）。

（2）系统信息的安全保护主要是确保数据信息的保密性和完整性等，包括用口令鉴别、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、数据加密等。

（3）系统信息传播后的安全包括信息过滤技术，它侧重于防止非法、有害信息的传播和控制传播后的后果；避免公用通信网络上大量自由传输信息的失控，本质上是维护道德、法

律或国家利益。

（4）系统信息内容的安全侧重于网络信息的保密性、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、冒充和诈骗等有损用户的行为，本质上是保护用户的利益和隐私。

2. 网络安全的主要特征

由前可知，网络安全主要涉及系统的可靠性、可用性和保密性以及软件及数据的保密性、完整性、可用性和可靠性等。

（1）保密性（Confidentiality）：主要是利用密码技术对软件和数据进行加密处理，保证在系统中存储和在网络上传输的软件和数据不被无关人员使用和识别。

（2）完整性（Integrity）：是指保护网络系统中存储和传输的软件及数据不被非法操作，即保证数据不被插入、替换和删除，数据分组不丢失、乱序，数据库中的数据或系统中的程序或数据不被破坏等。

（3）可用性（Availability）：是指在保证软件和数据完整性的同时，还要确保其能被正常使用和操作等。

（4）可靠性（Reliability）：是指保证网络系统不因各种因素的影响而中断正常工作。

1.1.3 网络安全体系结构

网络安全体系结构是网络安全层次的抽象描述，是从系统的角度理解网络安全问题的解决方案，对于网络安全解决方案的设计、实现与管理具有全局的指导作用。比如，在大型网络安全系统的设计及开发过程中，需要从全局出发考虑安全问题的整体解决方案，这样才能保证网络功能的完备性和一致性，降低安全代价和管理开销。

1. 网络安全模型

一般说来，安全模型是基于安全策略建立起来的。安全策略是指为达到预期的安全目标而制定的一套安全服务准则。目前，大多数网络安全策略都是建立在认证、授权、数据加密和访问控制等概念之上的。图 1-1 所示为网络安全的基本模型。通常，通信双方在网络上传输信息需要先在收发双方之间建立一条逻辑通道，这就要求先确定发送端到接受端的路由，再选择该路由上执行通信的协议（如 TCP/IP）。

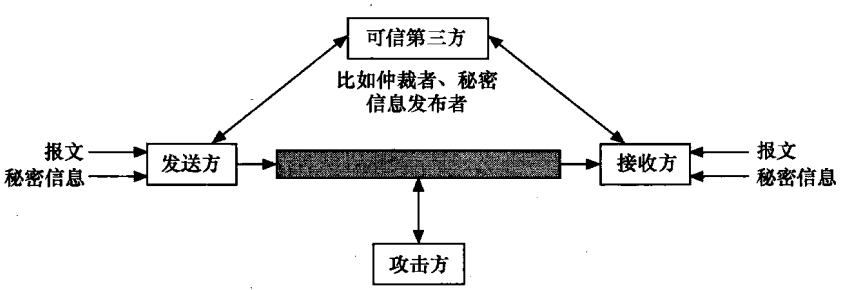


图 1-1 网络安全的基本模型

在图 1-1 中，为了在开放的网络环境中安全地传输信息，需要对信息提供安全机制和安全服务。信息的安全传输包括两个最基本的部分：①对发送的信息进行安全转换，如信息加

密，以实现信息的保密性，或附加一些特征码，以进行发送方身份的验证等；②收发双方共享的某些秘密信息，如加密密钥，除了对可信的第三方外，对其他用户都保密。

在图 1-1 中，为了进行信息的安全传输，通常还需要一个可信的第三方，其作用是负责向通信双方分发秘密信息以及在双方发生争议时进行仲裁。

由此可以看出，一个安全的网络通信模型（方案）必须考虑以下基本内容：

（1）实现与信息安全相关的信息转换的规则或算法。

（2）用于信息转换算法的秘密信息（如密钥）。

（3）实现秘密信息的分发和共享。

（4）信息转换算法和秘密信息获取安全服务所需要的协议。

2. P2DR 模型

当前，网络安全面临的现实是：基于静态密码体系的安全理论无法完整地描述动态的安全模型；现有的安全标准未能涵盖可能的风险；基于经典的、传统的计算机安全防护手段已不足以保障网络安全，信息网络安全防卫体系发生了动摇。20 世纪 90 年代末，美国国际互联网安全系统公司（ISS）提出了自适应网络安全模型（Adaptive Network Security Model，ANSM），并联合其他厂商组成 ANS 联盟，试图在此基础上建立网络安全的标准。该模型可量化，也可由数学家证明，是基于时间的安全模型，亦称为 P2DR（Policy（安全策略） Protection （防护） Detection（检测） Response（响应），如图 1-2 所示）。P2DR 模型是 TCSEC 模型（美国国防部 NCSC 国家计算机安全中心于 1985 年推出的 TCSEC 模型是静态计算机安全模型的代表，也是目前被普遍采用的安全模型）的发展，是一种常用的网络安全模型，也是一种动态的自适应网络安全模型。模型的基本描述为：

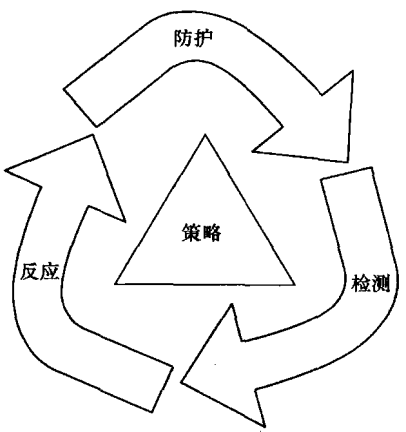


图 1-2 P2DR 安全模型

安全=风险分析＋执行策略＋系统实施＋漏洞监测＋实时响应

该模型强调系统安全的动态性，以安全检测、漏洞监测和自适应填充“安全间隙”为循环来提高网络的安全性，特别考虑人为管理的因素。其特点主要体现在如下几个方面：

（1）安全管理的持续性、安全策略的动态性，以实时监视网络活动、发现威胁和弱点来调整和填补系统缺陷。

（2）可测性（即可控性），通过经常性对网络系统的评估把握系统风险点，及时弱化甚至堵塞安全漏洞。

（3）利用专家系统、统计分析、神经网络方法对现有网络行为实时监控，报告并分析风险。

该模型已成为目前国际上较实用并可指导信息系统安全建设和安全运营的安全模型框架，它表征了这个时代的信息安全是面向网管、面向规约的。

3. 信息安全保证技术框架

信息安全保证技术框架（Information Assurance Technical Framework，IATF）是美国国家

安全局（NSA）于1998年制定，它提出了“深度防御策略”，确定了包括网络与基础设施、区域边界、计算环境和支撑性基础设施的深度防御及目标。IATF把信息保证技术划分为本地计算机环境（Local Computing Environment，LCE）、区域边界（Enclave Boundaries，EB）、网络和基础设施（Network & Infrastructures，NI）和支撑基础设施（Supporting Infrastructures，SI）4个领域。

（1）本地计算机环境

本地计算机环境一般包括服务器、客户端及其上面的应用（如打印服务、目录服务等）、操作系统、数据库和基于主机的监控组件（如病毒检测和入侵检测）。

（2）区域边界

区域边界是指在单一的安全策略的管理下，通过网络连接起来的计算机及网络设备的集合。区域边界是区域与外部网络发生信息交换的部分，它应确保进入的信息不会影响区域内资源的安全，而离开的信息是经过合法授权的。

在区域边界上有效的控制措施包括防火墙、门卫系统、虚拟专用网络（VPN）、标识和鉴别、访问控制等；区域边界上有效的监控措施包括基于网络的入侵检测系统（IDS）、脆弱性扫描器、局域网上的病毒检测器等。

区域边界的主要作用是防止外来攻击，它也可以用来对付某些恶意的内部攻击者，这些内部攻击者有可能利用边界来发起攻击，并通过开放后门/隐藏通道等来为外部攻击者提供便利。

（3）网络和基础设施

网络和基础设施在区域之间提供连接，包括局域网（LAN）、校园网（CAN）、城域网（MAN）和广域网（WAN）的连接等。它包括网络节点（如路由器和交换机等）、传递信息的传输部件（如卫星、微波、光纤等）以及其他重要的网络基础设施组件（如网络管理组件、域名服务和目录服务组件等）。对网络和基础设施的安全要求主要是鉴别、访问控制、机密性、完整性、抗抵赖性和可用性。

（4）支撑基础设施

支撑基础设施提供了一个IA（Information Assurance，信息保障）机制，它是网络、区域及计算环境内进行安全管理、提供安全服务的基础，主要为终端用户工作站、Web服务、应用、文件、域名系统（DNS）服务、目录服务等提供安全服务。

在IATF中涉及两个方面的支撑基础设施：一个是（Key Management Infrastructure /Public Key Infrastructure，密钥管理基础设施 / 公钥基础设施），提供了一个公钥证书及传统对称密钥的产生、分发及管理的统一过程；另一个是检测及响应基础设施，提供了对入侵的快速检测和响应。

在IATF中，信息安全分为4个主要环节：保护（Protection）、检测（Detection）、响应（Response）和恢复（Restore），如图1-3所示，简称为PDRR模型，其重要思想包括以下几个方面：

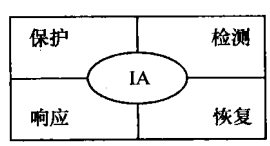


图1-3 信息安全保证技术框架

① 信息安全的3大要素是人、政策和技术其中，政策包括法律、法规、制度等，人是核心，是最为关键的要素。

② 信息安全的内涵包括鉴别性、保密性、完整性、可用性、不可抵赖性、可检查性和可恢复性等。

③ 信息安全的主要领域包括网络和基础设施安全、支撑基础设施安全、信息系统安全以

及电子商务安全等。

④ 信息安全的核心是密码理论和技术，安全协议是纽带，安全体系结构是基础，监控管理是保障，安全芯片的设计和使用是关键。

⑤ 网络安全的 4 个环节包括保护、检测、响应和恢复。

网络安全与这 4 个环节的处理时间直接相关。在 PDRR 模型中，网络安全是与被攻破保护时间（t_P）、检测到攻击的时间（t_D）、响应并反击的时间（t_R）和系统被暴露的时间（t_E）直接联系在一起的。

根据这些时间描述，可将网络安全划分为两个阶段：一是检测—保护阶段；二是检测—恢复阶段。

在检测—保护阶段，网络安全的含义就是及时检测和立即响应，用数学形式描述如下。

① 当 $t_P > t_D + t_R$ 时，说明网络处于安全状态。

② 当 $t_P < t_D + t_R$ 时，说明网络已受到危险，处于不安全状态。

③ 当 $t_P = t_D + t_R$ 时，说明网络处于临界安全状态。

从数学角度来分析，t_P 越大说明系统的保护能力越强，安全性也越高；反之，安全性能越低。t_D 和 t_R 的值越大说明系统安全性能越差，保护能力降低；反之，保护能力增强。

在检测—响应阶段，网络安全的含义是及时检测和立即恢复。

4. WPDRRC 安全模型

WPDRRC 安全模型是我国“863”信息安全专家组推出的适合我国国情的信息安全保障体系建设模型。WPDRRC 安全模型是在 PDRR 模型基础上改进的，它在 PDRR 模型前后增加了预警（Warning）和反击（Counterattack）功能。PDRR 模型把信息安全保障分为 4 个环节，即保护、检测、响应和恢复，并认为要保障信息安全就必须保护本地计算环境、保护网络边界和基础设施以及保护对外部网络的连接和支撑基础设施。而 WPDRRC 安全模型则把信息安全保障划分为 6 个环节：预警、保护、检测、响应、恢复和反击。这 6 个环节能较好地反映信息安全保障体系的预警能力、保护能力、检测能力、响应能力、恢复能力和反击能力。

预警能力包括攻击前的预测能力和攻击后的告警能力两个方面。预测能力是指根据所掌握的系统脆弱性和当前犯罪趋势来预测未来可能受到何种攻击和危害的能力；告警能力是指当威胁系统的攻击发生时能及时发现并发布警报的能力。

反击能力是指取证和打击攻击者的能力，这些能力要求整个系统能快速提供被攻击的线索和依据，及时审查和处理攻击事件，及时获取被攻击的证据，并制定有效的反击策略和进行强有力的反击。然而，在当前的网络系统中取证是比较困难的，要实现快速取证就必须发展相应的技术和开发相应的工具。近年来，国际上已经开始形成类似法医学的计算机取证学科，该学科不仅涉及取证、证据保全、举证、起诉和反击等技术的研究，还涉及媒体修复、媒体恢复、数据检查、完整性分析、系统分析、密码分析与破译和追踪等技术的研究。

WPDRRC 安全模型的 6 个环节具有较强的时序性和动态性，它是典型的信息安全保障框架。事实已表明，信息安全保障不单单是一个技术问题，它是涉及人、政策和技术在内的复杂系统。实际上，人、政策和技术是信息安全的三要素，这三要素具有较强的层次性，人是核心，属于最底层，技术是最高层，而政策属于中间层。但是技术必须通过人和相应的政策去操纵才能发挥作用。当然，这里所说的技术不是指单一的技术，而是指整个支撑信息安全应用的安全技术体系，该体系包括密码技术、安全体系结构、安全芯片、安全协议、监控管

理、攻击和评测技术等。其中，密码技术是整个安全技术体系的核心，安全体系结构是基础，安全协议是纽带，安全芯片是关键，监控管理是保障，攻击和评测的理论与实践是考验。

5. ISO/OSI 安全体系

1982 年，开放系统互连（OSI）参考模型建立之初，ISO 就开始进行 OSI 安全体系结构的研究。1989 年 12 月 ISO 颁布了计算机信息系统互连标准的第二部分，即 ISO7498-2 标准，并首次确定了开放系统互连参考模型的安全体系结构。我国将其称为 GB/T9387-2 标准，并予以执行。ISO/OSI 安全体系包括安全服务、安全机制、安全管理和安全层次 4 部分内容。其中，安全机制是 ISO/OSI 安全体系的核心内容，通过安全机制实现了 ISO/OSI 安全体系中的安全服务和安全管理，而安全层次描述了安全服务的位置。

（1）安全服务

ISO/OSI 安全体系提供了 5 种安全服务：认证服务、数据机密性服务、数据完整性服务、访问控制服务和不可否认性服务。

（2）安全机制

ISO/OSI 安全体系中的安全机制分为特殊安全机制和通用安全机制两大类。特殊安全机制包括加密机制、数字签名、访问控制、数据完整性、鉴别交换、业务流量填充、路由机制和公证机制。

（3）安全管理

ISO/OSI 安全体系中的安全管理包括 3 个方面的内容：系统安全管理、安全服务管理和安全机制管理。

① 系统安全管理：涉及整体 OSI 安全环境的管理。其包括总体安全策略的管理、OSI 安全环境之间的安全信息交换、安全服务管理和安全机制管理的交互作用、安全事件的管理、安全审计管理和安全恢复管理等。

② 安全服务管理：涉及特定安全服务的管理，其包括对某种安全服务定义其安全目标、指定安全服务可使用的安全机制、通过适当的安全机制管理调动需要的安全机制、系统安全管理以及安全机制管理相互作用。

③ 安全机制管理：涉及特定的安全机制的管理。其包括密钥管理、加密管理、数字签名管理、访问控制管理、数据完整性管理、鉴别管理、业务流填充管理和公证管理等。

（4）安全层次

ISO/OSI 安全体系是通过在不同的网络层上分布不同的安全机制来实现的，这些安全机制是满足相应的安全服务所必须的，其在不同的网络层的分布情况如图 1-4 所示。

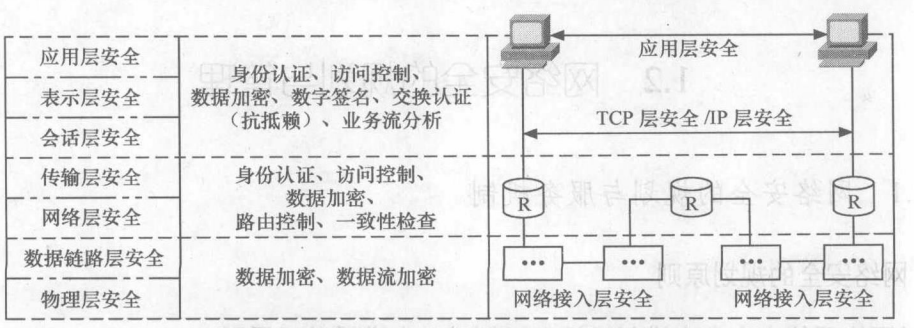


图 1-4 网络安全层次模型及各层主要安全机制分布