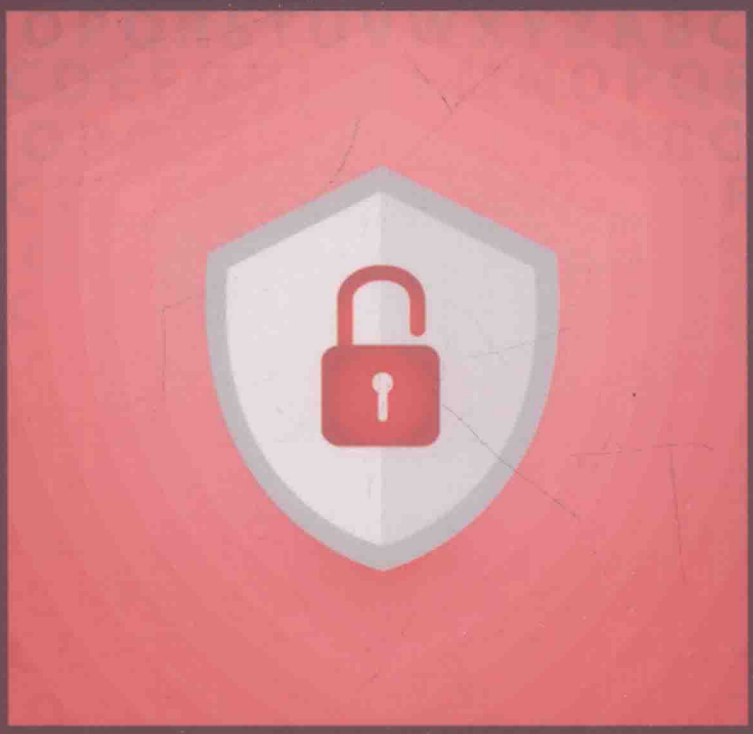
JISUANJI WANGLUO ANQUAN LILUN JI YINGYONG

计算机网络安全理论及应用

周德荣　田关伟　宋凌怡　编著



中国水利水电出版社
www.waterpub.com.cn

计算机网络安全
理论及应用

周德荣　田关伟　宋凌怡　编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书是作者结合多年的经验，吸取了国内外大量同类书刊的精华，并结合近年来计算机网络安全技术的发展而完成。本书系统地介绍了计算机网络攻防技术与安全管理，内容包括计算机网络安全概述、数字信息加密与认证技术、虚拟专用网与访问控制技术、无线网络安全、操作系统安全、电子邮件安全、防火墙、入侵检测技术与发展、计算机病毒及其防治、网络安全管理与评审等。

图书在版编目（CIP）数据

计算机网络安全理论及应用 / 周德荣，田关伟，宋凌怡编著. -- 北京 : 中国水利水电出版社，2016.2
ISBN 978-7-5170-4044-6

Ⅰ. ①计… Ⅱ. ①周… ②田… ③宋… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2016)第019291号

策划编辑：杨庆川　责任编辑：陈　洁　封面设计：崔　蕾

书　名	计算机网络安全理论及应用
作　者	周德荣　田关伟　宋凌怡　编著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座 100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京鑫海胜蓝数码科技有限公司
印　刷	三河市天润建兴印务有限公司
规　格	184mm×260mm　16开本　17印张　420千字
版　次	2016年2月第1版　2016年2月第1次印刷
印　数	0001—3000册
定　价	60.00元

凡购买我社图书，如有缺页、倒页、脱页的，本社发行部负责调换

前　言

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。随着计算机网络技术的发展，网络的安全问题越来越受到关注，网络安全已关系到国家安全和社会稳定等重要问题。

现如今计算机网络安全已引起世界各国的广泛关注，我国也在不断增加计算机网络安全方面的基础知识和网络安全技术应用知识等方面的研究投入。随着网络高新技术的不断发展，社会经济的建设与发展越来越依赖于计算机网络。与此同时，网络中的不安全因素对国民经济的威胁，甚至对国家和地区的威胁也日益严重。加快培养网络安全方面的应用型人才、广泛普及网络安全知识和掌握网络安全技术就突显重要。

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网络攻防技术，并通过研究实践完成。本书内容共分为 10 章，第 1 章为计算机网络安全概述，第 2 章为数字信息加密与认证技术，第 3 章为虚拟专用网与访问控制技术，第 4 章为无线网络安全，第 5 章为操作系统安全，第 6 章为电子邮件安全，第 7 章为防火墙，第 8 章为入侵检测技术与发展，第 9 章为计算机病毒及其防治，第 10 章为网络安全管理与评审。本书在介绍网络安全理论及其基础知识的同时，突出计算机网络安全方面的管理操作手法和手段，并尽量跟踪网络安全技术的最新成果与发展方向。

全书由周德荣、田关伟、宋凌怡撰写，具体分工如下：

第 2 章、第 6 章、第 7 章、第 9 章：周德荣（四川民族学院）；

第 1 章、第 8 章、第 10 章：田关伟（四川民族学院）；

第 3 章～第 5 章：宋凌怡（四川民族学院）。

由于网络安全的内容非常丰富，本书以“必需、够用”为基本原则，加强理论研究，为读者充分理解网络安全的基础理论以及培养读者解决网络安全问题的能力打下基础。本书讲究知识性、系统性、条理性、连贯性；力求激发读者兴趣，注重提示各知识之间的内在联系；精心组织内容，做到由浅入深，由易到难，删繁就简，突出重点。

本书的特点是文字简明、图表准确、通俗易懂，用循序渐进的方式叙述网络安全知识，对计算机网络安全的原理和技术难点的介绍适度，内容安排合理，逻辑性强。

本书在编撰时参考了大量的同类书籍和资料，对这些作者表示衷心的感谢。由于作者经验水平有限，加之计算机网络技术发展日新月异，书中疏漏不妥之处在所难免，恳请广大读者批评指正。

作者

2015 年 11 月

目　录

第 1 章　计算机网络安全概述

1.1　计算机网络安全的威胁

1.1.1　计算机网络安全

计算机网络安全所代表的含义较为广泛，所有关系到网络设备、网络信息以及网络安全方面的知识内容都属于计算机网络安全的范畴。计算机网络安全已经被计算机网络安全国际标准化组织(International Organization of Standards，IOS)定义[①]。

计算机网络安全是指对某个自动化信息系统的保护措施，其目的在于实现计算机网络系统资源的完整性可用性以及机密性(包括硬件、软件、固件、信息/数据、电信)。

这个定义包括三个关键的目标，它们组成了计算机网络安全的核心内容。

(1)机密性

维持施加在数据访问和泄露上的授权限制，包括保护个人隐私和私有信息的措施。机密性损失是指非授权的信息泄露。这个术语涵盖了如下两个相关的概念：

①数据机密性：保证私有的或机密的信息不会被泄露给未经授权的个体。

②隐私性：保证个人可以控制和影响与之相关的信息，这些信息有可能被收集、存储和泄露。

(2)完整性

防范不当的信息修改和破坏，包括保证信息的认证与授权。完整性损失是指未经授权的信息修改和破坏。这个术语涵盖了如下两个相关的概念：

①数据完整性：保证只能由某种特定的、已授权的方式来更改信息和代码。

②系统完整性：保证系统正常实现其预期功能，而不会被故意或偶然的非授权操作控制。

(3)可用性

保证及时且可靠地获取和使用信息，保证系统及时运转，其服务不会拒绝已授权的用户。可用性损失是指对信息或信息系统访问或使用的中断。

这三个概念组成了 CIA 三元组。它们体现了对于数据和信息计算服务的基本安全目标。例如，NIST(美国国家标准与技术研究院)的联邦信息的安全分级标准与信息系统(FIPS199)指出，机密性、完整性和可用性是信息和信息系统的三个安全目标。

1.1.2　计算机网络安全威胁

一般来讲，对上述 CIA 三元组在进行合法使用时对其进行攻击或者对其本身造成了损害的行为或者危害(一般通过攻击的行为方式来实现)都称之为计算机网络安全的威胁。

---

① 计算机网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

对于计算机或网络安全性的攻击，一般是通过在提供信息时查看计算机系统的功能来记录其特性。当信息从信源向信宿流动时，如图 1-1 所示列出了信息正常流动和受到各种类型攻击的情况。

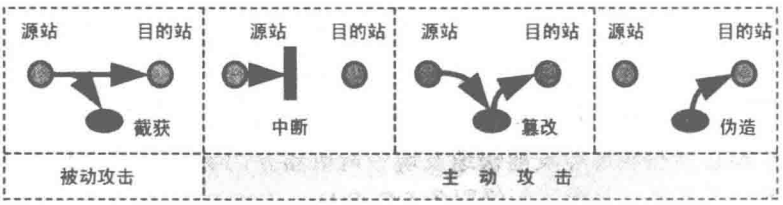


图 1-1　安全攻击

①中断是指系统资源遭到破坏或变得不能使用。

②截获是指未授权的实体得到了资源的访问权，这是对保密性的攻击。未授权实体可能是一个人、一个程序或一台计算机。

③篡改是指未授权的实体不仅得到了访问权，而且还篡改了资源，这是对完整性的攻击。

④伪造是指未授权的实体向系统中插入伪造的对象，这是对真实性的攻击。

几种威胁网络安全的方式如下所示：

(1)否认或抵赖

网络用户虚假地否认发送过的信息或接收到的信息。威胁源可以是用户和程序，受威胁对象是用户。

(2)破坏完整性

对正确存储的数据和通信的信息流进行非法的篡改、删除或插入等操作，从而使得数据的完整性遭到破坏。

(3)破坏机密性

用户通过搭线窃听、网络监听等方法非法获得网络中传输的非授权数据的内容，或者通过非法登录他人系统得到系统中的明文信息。

(4)信息量分析

攻击者通过观察通信中信息的形式，如信息长度、频率、来源地、目的地等，而不是通信的内容，来对通信进行分析。

(5)重放

攻击者利用身份认证机制中的漏洞，先把别人有用的密文消息记录下来，过一段时间后再发送出去，以达到假冒合法用户登录系统的目的。

(6)重定向

网络攻击者设法将信息发送端重定向到攻击者所在计算机，然后再转发给接收者。例如，攻击者伪造某个网上银行域名，用户却以为是真实网站，按要求输入账号和口令，攻击者就能获取相关信息。

(7)拒绝服务

攻击者对系统进行非法的、根本无法成功的大量访问尝试而使系统过载，从而导致系统不能对合法用户提供正常访问。

(8)恶意软件

通过非法篡改程序的方式来破坏操作系统、通信软件或应用程序，从而获得系统的控制权。恶意软件主要有病毒、蠕虫、特洛伊木马、间谍程序以及其他黑客程序等。

(9)社会工程

所谓社会工程(Social Engineering)，是指利用说服或欺骗的方式，让网络内部的人(如安全意识薄弱的职员)来提供必要的信息，从而获得对信息系统的访问。它其实是高级黑客技术的一种，往往使得看似处在严密防护下的网络系统出现致命的突破口。

除上述安全威胁之外，还可将网络安全威胁分为如图 1-2 所示的种类。

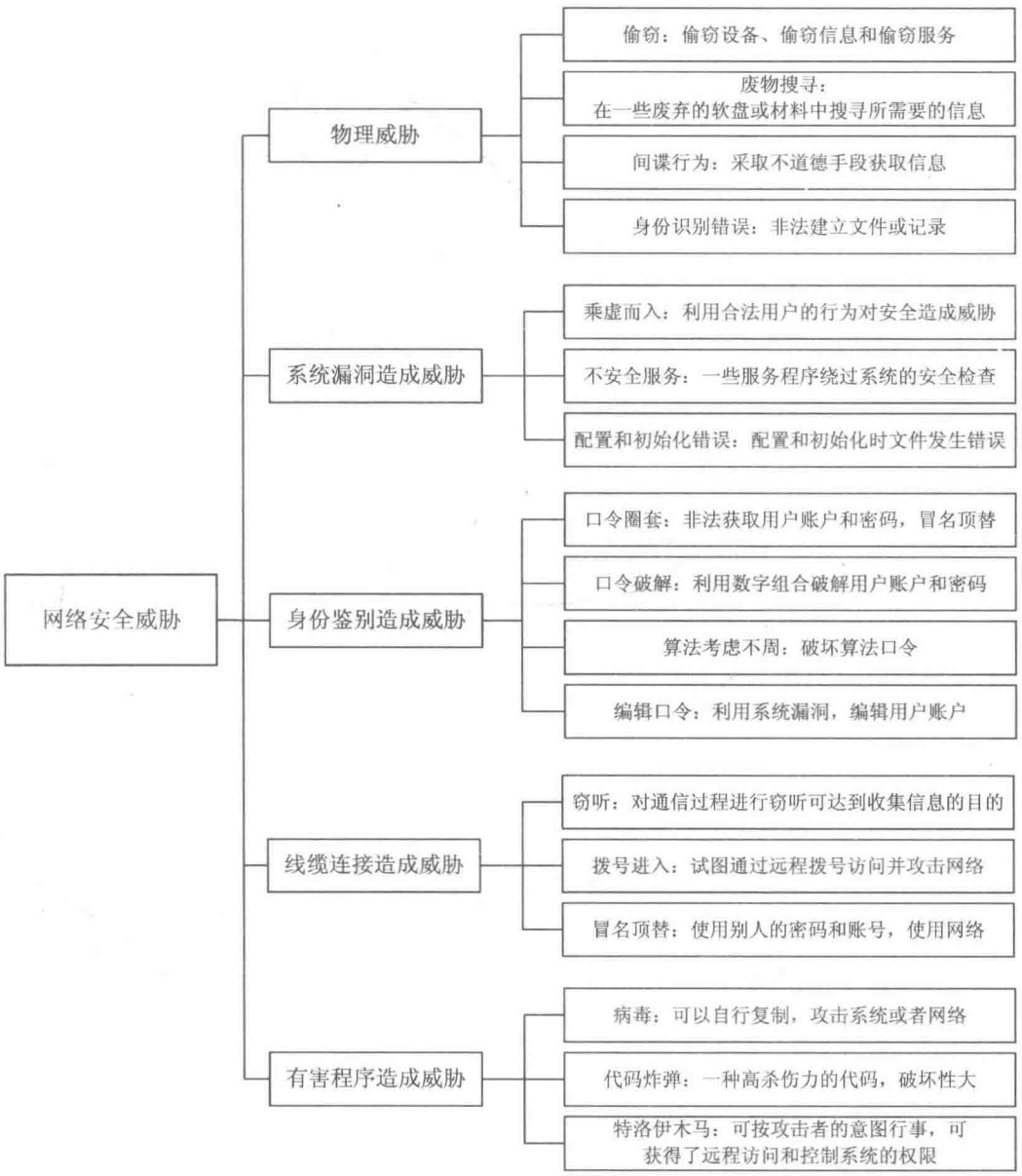


图 1-2　网络安全威胁的种类

1.2 计算机网络安全的体系结构与模型

计算机网络安全通常是由一系列安全机制来实现的。所谓安全机制，是指将安全技术实现逻辑抽象而成的一系列的模式。

在计算机网络安全领域，人们提出的高层机制主要有六种：预警、防护、检测、响应、恢复、反击。它们的关系如图 1-3 所示。

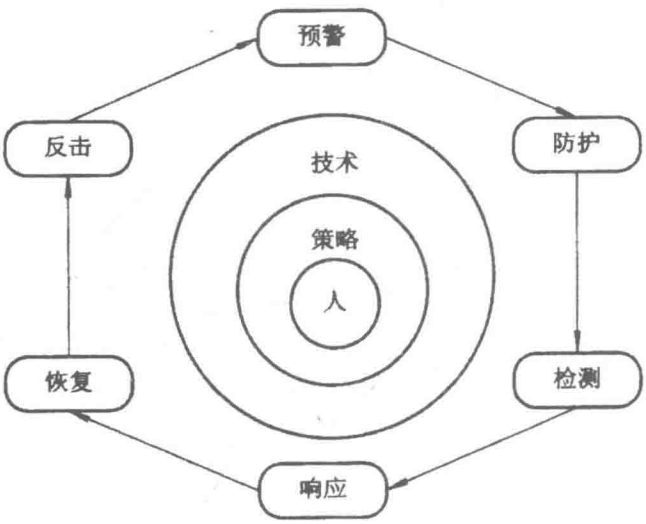


图 1-3 安全机制之间的关系

计算机网络安全中层机制有：身份认证、授权、加密、网络隔离、高可用性、内容分析等。

计算机网络安全基础应用域包括：网络基础设施安全、边界安全和局域网安全。计算机网络安全具体应用域有：防火墙应用、入侵检测、反病毒软件等。

安全服务(安全任务)、安全机制和安全应用域是计算机网络安全系统的三要素，它们的关系可以用一个三维坐标进行表述，如图 1-4 所示。

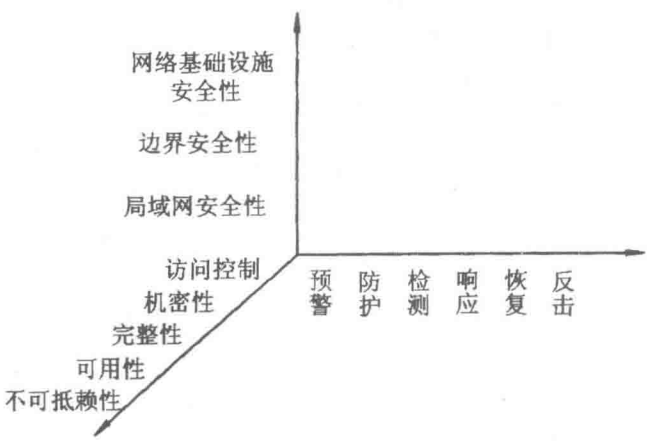


图 1-4 安全服务、安全机制和安全应用域之间的关系

1.2.1　计算机网络的安全体系结构

1. 安全体系结构框架

计算机网络安全体系结构框架如图 1-5 所示。

图 1-5　三维信息系统安全体系结构框架

由图 1-5 可以看出安全体系结构中安全特性以及系统单元的内容，其中系统单元包括如下四个部分：

①信息处理单元安全主要考虑计算机系统的安全，通过物理和行政管理的安全机制提供安全的本地用户环境，保护硬件的安全；通过防干扰、防辐射、容错检错等手段，保护软件的安全；通过用户身份鉴别、访问控制、完整性等机制保护信息的安全。

②通信网络安全为传输中的信息提供保护。通信网络安全涉及安全通信协议、密码机制、安全管理应用进程、安全管理数据库、分布式管理系统等内容。

③安全管理包括安全域的设置和管理、端系统的安全管理、安全服务管理和安全机制管理等。

④物理环境安全包括人员管理、物理环境管理和行政管理，还涉及环境安全服务配置以及系统管理员职责等。

最后的 OSI(Open System Interconnect，开放式系统互联)参考模型的结构层次是指各信息系统单元需要在 OSI 模型的各层次上采取不同的安全服务和安全机制，以满足不同的安全需求。

2. OSI 安全体系结构

网络体系的不同层次的主体和客体及其控制是不同的。在确立了安全服务和安全机制以后，根据信息系统的组成和 OSI 参考模型，就可以建立具体的安全框架。框架的确定主要反映在不同功能的安全子系统之中。通常，网络信息安全体系结构框架包括身份认证、授权管理、安全防御、安全检测和加密 5 个子系统。

对于管理员来说，OSI 安全体系结构作为一种组织提供安全服务的途径是非常有效的。更为重要的是，因为这个结构用作国际标准，计算机和通信厂商已经开发出符合这个结构化服务和机制标准的产品和服务安全特性。

OSI 安全模型为本书将要涉及的许多概念提供了一种有效的、简要的概览。OSI 安全模型关注安全攻击、机制和服务。

如图 1-6 所示给出了 OSI 网络层次、安全服务和安全机制之间的逻辑关系，定义了五大类安全服务，提供这些服务的八大类安全机制以及相应的开放系统互联的安全管理。

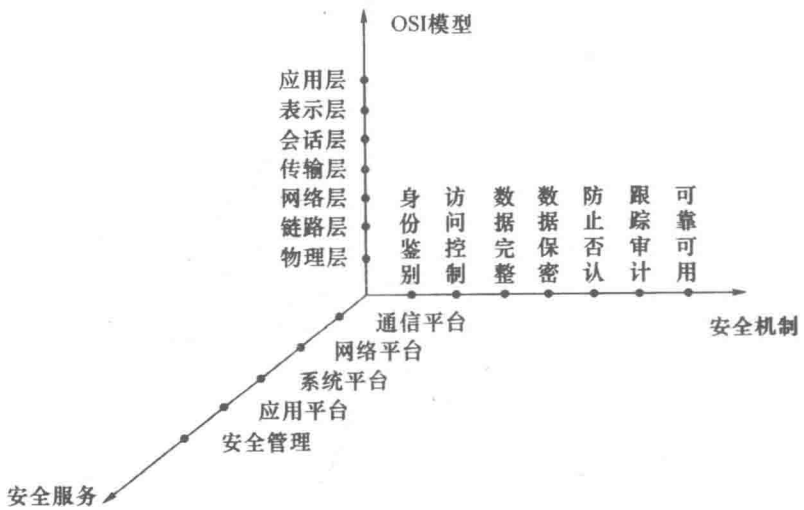


图 1-6　OSI 三维模型

1.2.2　计算机网络安全模型

消息将通过某种类型的互连网络从一方传输到另一方。这两方都是事务的主体，必须合作以便进行消息交换。可以通过在互连网络上定义一条从信息源到信息目的地之间的路由以及两个信息主体之间使用的某种通信协议(例如 TCP/IP)，来建立一条逻辑信息通道。如图 1-7 所示。

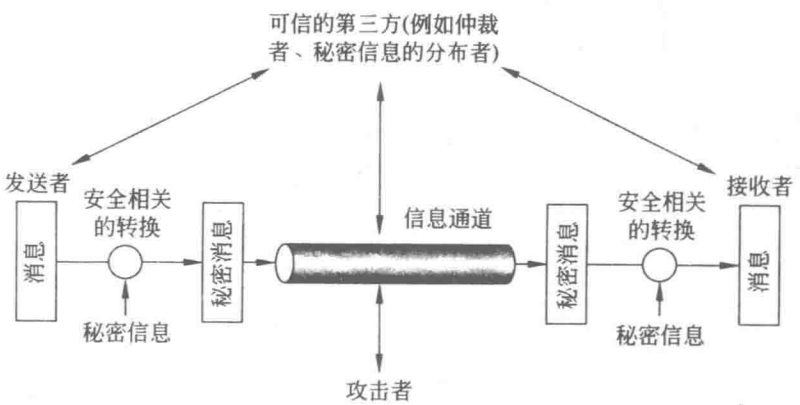


图 1-7　网络安全模型

当需要或者希望防范可能对信息机密性、真实性等产生威胁的攻击者的时候，安全方面的因素便会起作用。所有用于提供安全性的技术都包含以下两个主要部分：

①对待发送信息进行与安全相关的转换。其示例包括消息加密，它打乱了消息，使得对于攻击者而言该消息不可读；以及建立在消息内容上面的附加码，它可以用来验证发送者的身份。

②两个主体共享一些不希望被攻击者所知的秘密信息。其示例包括在消息变换中使用的加密密钥，它在传输之前用于打乱消息而在接收之后用于恢复消息。

1. P2DR 安全模型

网络信息系统包含的范围广泛，随着网络安全威胁的种类不断地增多，网络安全的范畴已经不单指信息的安全，已经扩展到整个网络信息系统的安全。因此，对网络系统的反应能力、响应能力都需要进行检测以便采取对应的保护措施。

目前，安全模型的趋势早已从被动防御转变为现在的主动防御，强调系统的防范攻击的能力。20 世纪末，出现了一种 P2DR 安全模型，该模型是基于策略(Policy)、防护(Protection)、检测(Detection)和响应(Response)的安全模型，如图 1-8 所示。

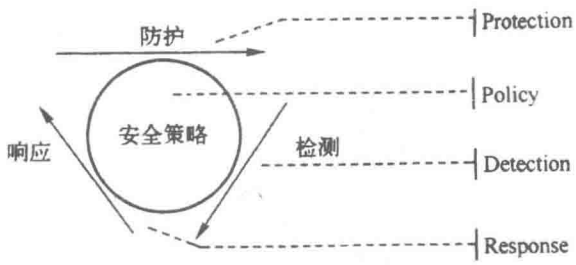


图 1-8　P2DR 安全模型

P2DR 模型的基本思想是使系统能达到一个最佳的状态：风险最低，防护能力最强。在安全策略的居中调度之下，综合运用防护工具，如防火墙、身份认证、加密技术等，结合系统检测工具，如入侵检测技术等全面评价系统的安全状态，并采取适当的措施和手段将系统调整至最佳状态。

(1)安全策略

安全策略是 P2DR 模型不可或缺的一部分，它不仅阐述了系统安全核心思想和指导方针，也是其他防护、检测、响应工具的依据。

(2)防护

防护就是根据系统的一系列性能，采取一定的技术提前预防可能遭受的安全攻击。防护技术主要分为主动防护技术和被动防护。主动防护技术主要有身份验证、访问控制等技术；被动防护技术主要有防护墙、入侵检测等技术。

(3)检测

防护技术并不能保证系统免受安全威胁，有时候一些攻击事件以及安全威胁是无法通过防护技术进行预防的。此时就需要检测技术将安全威胁检测出来。

(4)响应

系统一旦检测出有入侵行为,响应系统则开始响应,进行事件处理。P2DR 中的响应就是在已知入侵事件发生后进行的紧急响应(事件处理)。响应工作可由一个特殊部门负责,那就是计算机安全应急响应小组(Computer Emergency Response Team,CERT)。

通常情况下,系统的检测时间与响应时间越长,或对系统的攻击时间越短,则系统的暴露时间越长,系统就越不安全。因此系统要想达到安全状态,就需要尽量减少检测和响应时间。

2. 计算机网络安全防范模型

如图 1-9 显示了网络与信息安全防范模型。

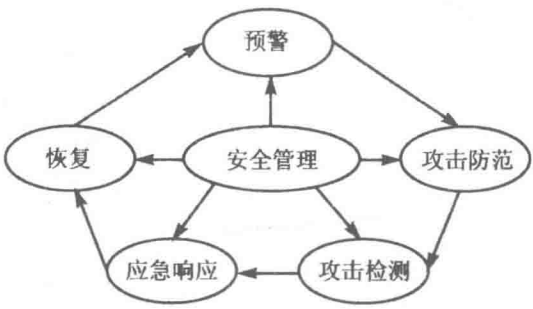


图 1-9　网络与信息安全防范模型

网络安全防御体系的工作流程大体上可以分为三个部分,即攻击前的防范、攻击过程中的防范以及攻击过程后的应对,如图 1-10 所示。

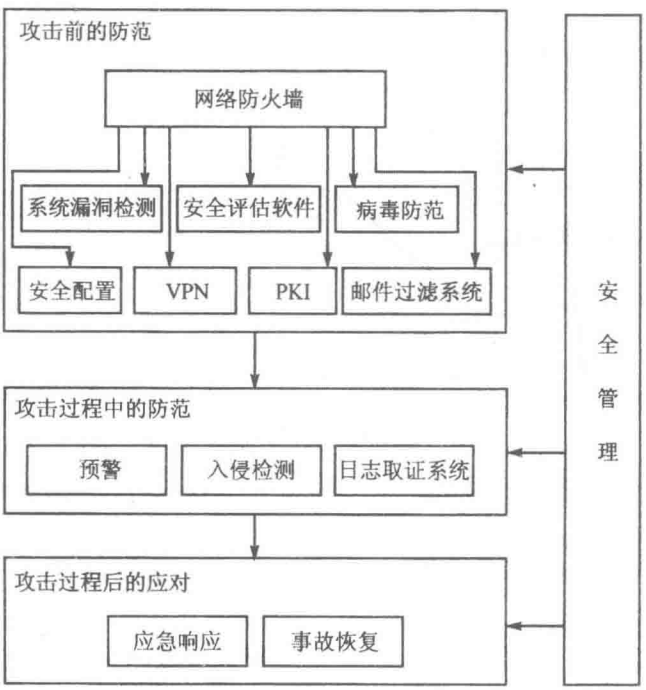


图 1-10　网络安全防御体系的工作流程

3. PDRR 网络安全模型

PDRR 是美国国防部提出的安全模型，它包含了网络安全的 4 个环节：Protection(防护)、Detection(检测)、Response(响应)和 Recovery(恢复)，如图 1-11 所示。PDRR 模式是一种公认的比较完善也比较有效的网络信息安全解决方案，可以用于政府、机关、企业等机构的网络系统。

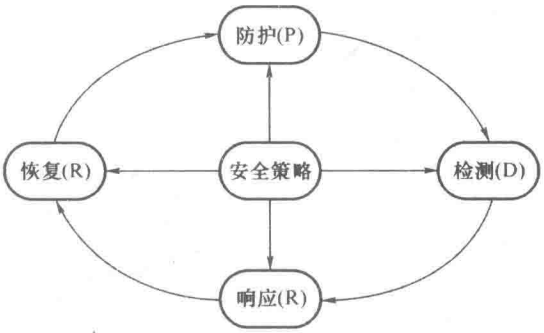


图 1-11　PDRR 安全模型

PDRR 模型与前述的 P2DR 模型有很多相似之处。其中 Protection(防护)和 Detection(检测)两个环节的基本思想是相同的，P2DR 模型中的 Response(响应)环节包含了紧急响应和恢复处理两部分，而在 PDRR 模型中 Response(响应)和 Recovery(恢复)是分开的，内容也有所扩展。

响应是在已知入侵事件发生后对其进行处理。在大型网络中，响应除了对已知的攻击采取应对措施外，还提供咨询、培训和技术支持。人们最熟悉的响应措施就是采用杀毒软件对因计算机病毒造成系统损害的处理。

恢复是 PDRR 网络信息安全解决方案中的最后环节。它是在攻击或入侵事件发生后，把系统恢复到原来的状态或比原来更安全的状态，把丢失的数据找回来。恢复是对入侵最有效的挽救措施。

P2DR 和 PDRR 安全模型都存在一定的缺陷。它们都更侧重于技术，而对诸如管理方面的因素并没有强调。模型中一个明显的不足就是忽略了内在的变化因素。

实际上，安全问题牵涉面广，除了涉及防护、检测、响应和恢复外，系统本身安全的“免疫力”的增强、系统和整个网络的优化以及人员素质的提升等，都是网络安全中应该考虑到的问题。网络安全体系应该是融合了技术和管理在内的一个可以全面解决安全问题的体系结构，它应该具有动态性、过程性、全面性、层次性和平衡性等特点。

1.3　计算机网络安全的现状和发展趋势

1.3.1　我国计算机网络安全的现状

1. 360 安全中心

360 互联网安全中心发布的《2015 年第三季度中国互联网安全报告》指出：

2015年第三季度，360互联网安全中心共截获PC端新增恶意程序样本1.0亿个，平均每天截获新增恶意程序样本112.6万个。截获安卓移动平台新增恶意程序样本558万个，平均每天截获新增手机恶意程序样本近6.07万个。

2015年第三季度，360互联网安全中心共拦截各类新增钓鱼网站352200个，虚假购物的占比最大，达到了39.9%，其次是虚假彩票13.5%。

2015年第三季度，360的PC和手机安全软件共为全国用户拦截钓鱼攻击100.2亿次，其中，PC端拦截量为80.2亿次，占80.0%，移动端为20.0亿次，占20.0%。移动端的钓鱼拦截量和拦截占比均创历史新高。

在新增钓鱼网站中，虚假购物的占比最大，达到了39.9%，其次是虚假彩票13.5%、假冒银行12.9%位列其后。而在钓鱼网站的拦截量方面，彩票钓鱼占到了73.8%，排名第一，其次是虚假购物9.3%、网站被黑5.4%。

2015年第三季度，360网站卫士共拦截各类网站漏洞攻击2.4亿次，受到漏洞攻击的网站数量为45.4万个；拦截各类DDoS攻击577.1Gb/s；拦截各类CC攻击438.4亿次。

2. 瑞星公司

瑞星2015年上半年中国信息安全报告指出，2015年上半年新增病毒样本1924万余个，共有2.1亿人次网民被病毒感染，有933万台电脑遭到病毒攻击，人均病毒感染次数为22.66次。

2015年1至6月，瑞星“云安全”系统截获挂马网站272万个(以网页个数统计)，与2014年同期相比下降了20.32%。在报告期内，瑞星“云安全”系统拦截挂马网站的攻击总计为2469万余次，与2014年同期相比下降了19.92%。

2015年1至6月，瑞星“云安全”系统共截获钓鱼网站337万个，比2014年同期下降了4.26%。在报告期内，瑞星“云安全”系统拦截钓鱼网站攻击1.3亿余人次，上半年平均每人访问钓鱼网站1.46次。

2015年钓鱼网站攻击相较于2014年及以前的钓鱼攻击，在数量上有所增加，主要通过以下手段：

①利用网购节进行钓鱼，假冒淘宝、京东、苏宁等大型网购平台，要求消费者浏览指定网站，骗取用户的账号、密码、支付密码、网银账户等。

②利用邮件、弹窗等形式发送钓鱼网站链接，以投资理财、留学咨询、职业介绍等名目诱使网民登录浏览，骗取钱财。

③利用移动终端的短信、微博、微信，发送短链接进行钓鱼。随着移动终端的使用率逐渐上升，很多钓鱼攻击者利用该类终端缺少防护的特点进行钓鱼攻击。

④篡改教育、公共事业类网站，伪装成百度百科，进行热播综艺节目场外抽奖钓鱼。

由上述可以看出，新发现安全漏洞的数量每年都在成倍地增加，而且新类型的安全漏洞也不断出现。现在网络安全攻击的自动化程度和速度都在不断进行提高，工具也越来越复杂，例如恶意代码不仅能实现自我复制，还能自动攻击内外网上的其他主机，并以受害者为攻击源继续攻击其他网络和主机。这种情形之下不仅攻击行为变得更难发现，防范也变得越发困难，对网络基础产生的威胁越来越大。

1.3.2　计算机网络安全的发展趋势

1. 我国网络信息安全的发展趋势

(1)必须建立自主产权的软硬件系统

虽然我国已经跻身于 IT 产品生产和消费的大国之列，以联想、华为为代表的企业已成功地打入欧美市场，但应该看到其产品的核心部分几乎都是国外的技术。我国所使用的操作系统也几乎都是国外的产品。在这些产品中都不同程度地存在着“后门”，建立在软硬件系统之上的信息安全，无论从什么角度来讲，安全性都值得怀疑。正是基于此，我国才不遗余力地独立开发“龙芯”CPU 和自主产权操作系统。

(2)必须研制高强度的保密算法

信息安全从本质上说与信息加密息息相关，但目前加密的核心技术也掌握在欧美国家之手，我国所使用算法的加密强度远不如欧美国家，严重地影响着中国信息化的进程。因此，研究高强度的加密算法非常重要，信息安全建设应与加密算法研制同步。同时，密钥管理理论和安全性证明方法的研究也应该重点关注。

(3)需要研制新一代的防火墙和入侵检测系统

新一代的产品可针对每台主机进行适时监测，不但能监测来自外部的入侵，也能监测来自内部的入侵，并能克服防火墙的缺陷。

(4)需要研制新一代的防病毒软件

网络给人带来方便的同时，也带来了病毒。对普通用户来讲，使用杀毒软件清除病毒可能是唯一的办法，但目前的杀毒技术在与病毒攻击技术的较量中还处于被动之中，所以有必要开发新一代的防毒软件，改变目前的尴尬局面。

(5)整体考量，统一规划

信息安全取决于系统中最薄弱的环节，“一枝独秀”并不意味着系统的安全，真正的安全建立在统一的网络安全架构基础之上，安全策略要从整体考量，安全方案需要统一规划。

2. 国际上网络信息安全的研究

(1)基础技术研究

该项研究的方向是对传统的安全基础技术研究，侧重在针对特殊应用的实用算法的分析、提出或改进、实现的研究。研究目的是掌握传统信息安全的数学工具，并可将其灵活地应用在实际系统中。例如，对大素数分解问题的研究、对 SET 协议的分析与研究、对协议形式化证明的研究、对 SSL 协议的分析与研究等，都是在这一主题下的工作。

(2)入侵及防范技术研究

该项研究主要研究网络层的攻击与防范技术，主要的技术种类如图 1-12 所示。目的是为了解决网络入侵检测所面临的攻击复杂性以及预报准确性等难题，为计算机网络安全形式化研究提供基础。

(3)系统安全体系及策略研究

该项研究主要研究应用层基础服务系统的安全整体策略，基于受保护基础服务的特点，提