网络信息安全理论与技术

Theory and Technology for Network Information Security

主编　雷建云　张 勇　李海凤

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

网络信息安全理论与技术

Theory and Technology for Network Information Security

主　编　雷建云　张　勇　李海凤
副主编（按姓氏笔画为序）李海荣　邹　磊　杨　静　程显生　魏长宝

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

图书在版编目(CIP)数据

网络信息安全理论与技术/雷建云,张勇,李海凤主编. —北京:中国商务出版社,2009.2

ISBN 978-7-5103-0047-9

Ⅰ.网… Ⅱ.①雷…②张…③李… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2009)第 024918 号

网络信息安全理论与技术

主　编　雷建云　张　勇　李海凤

副主编　李海荣　邹　磊　杨　静

　　程显生　魏长宝

中国商务出版社出版

(北京市东城区安定门外大街东后巷 28 号)

邮政编码:100710

电话:010—64269744(编辑室)

　　010—64266119(发行部)

　　010—64295501

　　010—64263201(零售、邮购)

网址:www.cctpress.com

Email:cctp@cctpress.com

北京中商图出版物发行有限责任公司发行

三河市铭浩彩色印装有限公司印刷

787 毫米×1092 毫米　16 开本

24.375 印张　624 千字

2009 年 3 月第 1 版

2009 年 3 月第 1 次印刷

ISBN 978-7-5103-0047-9

定价:38.00 元

前　言

随着计算机和网络技术日新月异的发展，网络信息安全问题日益突出。伴随着信息技术的发展与应用，信息安全的内涵也在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，继而发展成为攻、防、测、控、管、评等多方面的理论与技术。

网络信息安全问题已成为一个很严肃的话题。面对越来越严重的威胁，加速培养网络信息安全方面的人才是构建并完善网络安全教育的关键。除了具备专业知识外，还应具有良好的网络文化道德，懂得网络安全法规。

本书共分 12 章。第 1 章为网络信息安全概论，介绍网络信息安全的根源、概念、特征、基本原则、存在的不安全因素和未来的发展趋势。第 2、3 章介绍密码学基础、密码技术。第 4 章讲数字签名的含义与实现方法；介绍认证的实现与身份认证技术；分析了数字签名的算法及发展前景。第 5 章讲模式识别的基础理论。第 6 章先概述黑客的相关知识，继而对常用的黑客攻防技术进行说明，主要包括网络扫描、监听、拒绝服务攻击、IP 地址欺骗、缓冲区溢出、后门及特洛伊木马等技术。第 7 章讲病毒的定义、分类、工作原理及反病毒技术等知识。第 8、9 章讲防火墙和入侵检测技术。第 10 章介绍信息隐藏的概念、过程、基本要求，还对隐写术、阈下信道、隐信道和隐匿通信基本知识及流行的数字水印技术作了阐述。第 11 章讲安全协议的分析和设计的基本理论。第 12 章介绍典型的安全协议，包括 IPSec、Kerberos、SSL、X.509、RADIUS 和 SET 协议。本书力求系统而完整的向读者讲述网络信息安全是一个具体的问题，是一个具有可操作性的现实问题。

全书由雷建云、张勇、李海凤担任主编，由李海荣、邹磊、杨静、程显生、魏长宝（按姓氏笔画为序）担任副主编，并由雷建云、张勇、李海凤负责统稿。其具体分工如下：

第 8 章第 1～6 节，第 9 章，第 10 章：雷建云（中南民族大学）；

第 3 章第 3 节，第 4 章，第 5 章，第 6 章：张勇（淮海工学院计算机工程学院）；

第 2 章，第 3 章第 1～2 节与第 4～7 节：李海凤（天津职业大学）；

第 12 章第 1 节与第 6 节：李海荣（内蒙古科技大学）；

第 11 章，第 12 章第 4 节：邹磊（湖北中医药高等专科学校）；

第 1 章，第 8 章第 7～8 节，第 12 章第 5 节：杨静（天津城市建设学院）；

第 7 章第 1～2 节，第 12 章第 3 节：程显生（内蒙古农业大学职业技术学院）；

第 7 章第 3～4 节，第 12 章第 2 节：魏长宝（黄淮学院）。

由于作者水平有限，编写时间仓促，书中难免有疏漏和错误，恳请广大读者批评指正。

编者

2009 年 1 月

目　录

第 1 章　网络信息安全概论

1.1　网络信息安全

1.1.1　网络信息安全问题的产生

现代计算机网络具有开放性、互联性、多样性、终端分布不均匀性等特征，致使网络易受黑客、恶意软件和其他不轨的攻击。因此，要提高计算机网络的防御能力，加强网络的安全措施非常迫切而且必要，否则该网络将是个无用的，甚至会危及国家安全的网络。归结起来，导致网络安全问题日益严重的根源主要有以下几个方面：

1. 网络协议的特性和协议自身的安全缺陷

覆盖全球的因特网，以其 TCP/IP 协议开放性与共享性方便了各种计算机网络的入网互联，极大地拓宽了资源共享的可能性。但由于早期网络协议以开放性和共享性为主要目标而对安全问题的忽视，以及 Internet 在使用和管理上的相对无序状态，导致目前网络安全受到了严重威胁，安全事故屡有发生。

网络协议自身的安全缺陷主要是指协议和业务的不安全。导致协议不安全的主要原因，一方面是 Internet 从建立开始就缺乏安全的总体构想和设计。因为 Internet 起源的初衷是方便学术交流和信息沟通，并非商业目的。Internet 所使用的 TCP/IP 协议是在假定的可信环境下，为网络互联而专门设计的，本身缺乏安全措施。TCP/IP 协议的 IP 层没有安全认证和保密机制（只基于 IP 地址进行数据包的寻址，无认证和保密机制）；在传输层，TCP 连接能被欺骗、截取和操纵，而 UDP 易受 IP 源路由和拒绝服务的攻击。另一方面，协议本身可能会泄露口令，连接可能成为被盗用的目标。

2. 操作系统和应用程序的复杂性

由于网络和终端硬件设备的不断升级换代以及计算机功能的不断增强，现代操作系统和应用程序变得越来越庞大而复杂，导致的一个不良后果就是操作系统和应用程序本身存在许多安全漏洞和隐患。另外，操作系统和应用系统的复杂性也为对它们的配置不当而引发安全问题埋下了伏笔，甚至它们的默认安装和配置也成为安全的一大隐患。

3. 物理安全问题

网络设备和计算机系统本身的物理安全隐患，如灰尘、潮湿、雷击和电磁泄露等，也是网络信息安全出现问题的重要根源之一。

4.人与管理问题

人是信息活动的主体，是引起网络信息安全问题最主要的因素之一，这可以从以下三个方面来理解。第一，人为的无意失误主要是指用户安全配置不当造成的安全漏洞，包括用户安全意识不强、用户口令选择不当、用户将自己的账号信息与别人共享和用户在使用软件时未按要求进行正确的设置等。第二，人为的恶意黑客攻击，是网络信息安全面临的最大威胁。在英文中，黑客有两个概念：Hacker 和 Cracker。一般来说，Hacker 是这样一类人，他们对钱财和权利蔑视，而对网络技术本身非常专注，他们在网上进行探测性的行动，帮助人们找到网络的漏洞，可以说他们是这个领域的绅士。但是 Cracker 不一样，他们要么是为了满足自己的私欲，要么是受雇于一些商业机构，具有攻击性和破坏性。他们修改网页，窃取机密数据，甚至破坏整个网络系统。因其危害性较大，Cracker 已成为网络安全真正的，也是主要的防范对象。这类人闯入计算机网络系统盗取信息，故意破坏他人财产，使服务器中断。他们对电脑非常着迷，自认为比他人聪明，因此，随心所欲地闯入某些信息禁区，开玩笑或恶作剧，甚至干出违法的事。他们将此看做一种智力挑战，好玩有趣，但当有利可图时，很多人往往抵制不住诱惑而走上犯罪的道路。信息战也是黑客开展攻击的一个非常重要的原由。第三，管理不善也是一个重要因素。对网络信息系统的严格管理是避免受到攻击的重要措施。据统计，在美国，90％以上的 IT 企业对黑客攻击准备不足，75％～85％的网站都抵挡不住黑客的攻击。管理的缺陷也可能导致系统内部人员泄露机密，由此一些不法分子获取可乘之机。

1.1.2 网络信息安全的概念

1.网络信息安全的定义

网络信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的边缘学科。从广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。通用的定义为：网络信息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，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能够连续、可靠、正常地运行，网络服务不中断。

2.网络信息安全的其他含义

值得注意的是，网络信息安全是一个相对的概念，是指在信息安全期内保证其在传输和存储时不被非法访问。绝对的安全是不存在的，其意义与所保护的对象有关，在不同的环境会有不同的解释。

(1)信息系统安全

信息系统安全即信息处理和传输系统的安全。包括计算机机房环境的保护，法律、政策的保护，计算机结构设计上的安全考虑，硬件系统的可靠、安全运行，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，避免由于电磁泄露而产生信息泄露、干扰他人或受他人干扰。其本质是保护系统的合法操作和正常运行。

(2)系统信息安全

系统信息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，数据加密等。

(3)信息传播安全

信息传播安全主要指传播后果的安全，包括信息过滤、不良信息的过滤等，侧重于防止和控制非法、有害信息传播产生的后果，避免在公共信道上信息传输时产生信息失控的现象，以维护信息道德、法律和国家的利益。

(4)信息内容安全

信息内容安全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、假冒、诈骗等有损于合法用户的行为，以保护用户的利益和隐私。

可见，如果从普通用户、网络管理员、安全保密部门、教育以及社会意识形态等不同的角度来理解，网络信息安全的含义也会有差别。本书所涉及的网络信息安全的含义是通过各种计算机、网络、加密技术和信息安全技术，保护在公共通信网络中传输、交换和存储的信息的机密性、完整性和真实性，并对信息的传播及内容具有控制能力。

1.1.3　网络信息安全的特征

1. 保密性

保密性是指信息不被泄露给非授权的用户、实体或进程，不被非法利用。信息的保密性包括传输过程中的保密性和存储时的保密性。

数据在传输过程中可以被窃听和分析，这就需要用加密技术对原始明文进行处理，加密后的密文能够保证在传输、使用和转换的过程中不被第三方非法获取，即使获取了也无法破解，只有掌握解密密钥的合法用户才能将其恢复成明文，从而确保数据的保密性；存储时的保密性可以通过访问控制来实现，管理员可以根据不同的数据类型和应用需求，对用户和数据进行分类，设置成不同的访问模式。

2. 完整性

完整性是指数据未经授权不能进行改变的特性，即信息在存储或传输过程中不被非法修改、破坏和丢失，并且能够判别出数据是否已被改变。其目的是保证信息系统上的数据处于一种完整和未受损的状态，不会因有意或无意的事件而被改变或丢失。一旦数据的完整性不保，则其可用性必将丧失。

数据的完整性可通过访问控制、数据备份和冗余设置来实现。

3. 可用性

可用性是指可被授权实体访问并按需求使用的特性，即当需要时授权者总能够存取所需要的信息，攻击者不能占用所有的资源而妨碍授权者的使用。拒绝服务攻击、病毒等都可以破坏数据的可用性。

其中，按需使用可通过认证和鉴别技术来实现，以保证每个实体的真实、可靠性，但要确保实时、正常的服务似乎是不太可能的，除了备份和冗余设置技术以外，目前还没有找到更有效的办法。

4. 不可否认性

不可否认性(也称不可抵赖性)是指对通信双方信息真实性的安全要求,信息行为人要对自己的行为负责,即通信双方均不可抵赖。包括:源发证明,它给信息接收者提供证据,使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞;交付证明,它给信息发送者提供证据,使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

不可否认性通常用数字签名技术来实现。

5. 可控性

可控性是指可以控制授权范围内的信息流向及行为方式,对信息的传播及内容具有控制能力。

可控性可通过访问控制等技术来实现。

1.2 安全体系结构与模型

安全体系结构、安全框架、安全模型及安全技术等的相互关联构成了安全服务的基础,同时它们又可以相互任意组合,能够提供更强大的安全服务。

1.2.1 OSI 安全体系结构

国际标准化组织于 1989 年对 OSI 开放互联环境的安全性进行了深入的研究,在此基础上提出了 OSI 安全体系,作为研究设计计算机网络系统以及评估和改进现有系统的理论依据。OSI 安全体系定义了安全服务、安全机制、管理及有关安全方面的其他问题。此外,它还定义了各种安全机制以及安全服务在 OSI 中的层位置。

1. 安全服务

为应对现实中的种种情况,OSI 定义了 11 种威胁,并在对威胁进行分析的基础上,规定了 5 种标准的安全服务。

(1)对象认证安全服务

用于识别对象的身份和对身份的证实。OSI 环境可提供对等实体认证和信源认证等安全服务。对等实体认证是用来验证在某一关联的实体中,对等实体与其声称是一致的,它可以确认对等实体没有假冒身份;而信源认证是用于验证所收到的数据来源与所声称的来源是否一致,它不提供防止数据中途被修改的功能。

(2)访问控制安全服务

提供对越权使用资源的防御措施。访问控制主要可分为自主访问控制、强制访问控制两类。实现机制可以是基于访问控制属性的访问控制表、基于安全标签或用户和资源分档的多级访问控制等。

(3)数据保密性安全服务

它是针对信息泄漏而采取的防御措施,可分为信息保密、选择段保密和业务流保密。它的基础是数据加密机制的选择。

(4)数据完整性安全服务

防止非法篡改信息，如修改、复制、插入和删除等。它有5种形式：可恢复连接完整性、无恢复连接完整性、选择字段连接完整性、无连接完整性和选择字段无连接完整性。

(5)防抵赖性安全服务

它是针对对方抵赖的防范措施，用来证实发生过的操作，它可分为对发送防抵赖、对递交防抵赖和进行公证。

2. 安全机制

一个安全策略和安全服务可以单个使用，也可以组合起来使用，在上述提到的安全服务中可以借助以下安全机制：

(1)加密机制

借助各种加密算法对存放的数据和流通中的信息进行加密。DES算法已通过硬件实现，效率非常高。

(2)数字签名

采用公钥体制，使用私钥进行数字签名，使用公钥对签名信息进行证实。

(3)访问控制机制

根据访问者的身份和有关信息，决定实体的访问权限。

(4)数据完整性机制

判断信息在传输过程中是否被篡改过，与加密机制有关。

(5)认证交换机制

用来实现同级之间的认证。

(6)防业务流量分析机制

通过填充冗余的业务流量来防止攻击者对流量进行分析，填充过的流量需通过加密进行保护。

(7)路由控制机制

防止不利的信息通过路由，目前典型的应用为网络层防火墙。

(8)公证机制

由公证人(第三方)参与数字签名，它以通信双方对第三方都绝对信任为前提。

3. 安全管理

为了更有效地运用安全服务，需要有其他措施来支持它们的操作，这些措施即为安全管理。安全管理是对安全服务和安全机制进行管理，把管理信息分配到有关的安全服务和安全机制中去，并收集与它们大的操作有关的信息。

OSI概念化的安全体系结构是一个多层次的结构，它本身是面对对象的，给用户提供了各种安全应用，安全应用由安全服务来实现，而安全服务又是由各种安全机制来实现的。OSI提供了每一类安全服务所需要的各种安全机制，而安全机制如何提供安全服务的细节可以在安全框架内找到。

1.2.2　网络信息安全体系框架

信息是资源的抽象，用以表达资源，并可以被用来进行处理、存储和传输。例如，学生档案信息是对学生的抽象，它由专门人员进行登记，用电子数据文件对这些资源进行存储，并通过网络

系统进行传输。

1. 网络信息系统中的资源

我们将网络信息系统中的资源分为 3 种：

(1)人：信息系统的决策者、使用者和管理者

人类资源主要提供智力的服务以及体力的服务。虽然每个人都是由一些生理组织系统组成的，结构上差别不大，但他们所能提供的智力和体力服务却大不相同，这是由于他们各自的知识体系不同造成的。同时由于人类是高智能的系统，他们具有更为复杂的社会关系，这些都将是社会工程所要研究的内容。在目前以技术为主的网络信息系统中，将人按角色和权限进行划分，其实也暗中提出了对相应人类资源的知识和社会职责的要求。

(2)应用：由一些业务逻辑组件及界面组件组成

所谓应用，是指面向业务的技术资源。这些技术组成一个处理与人类业务相关的信息。应用虽然也表现为软件或硬件组件，但我们通常更看中的是它能为人类解决什么样的问题。甚至可以说，应用是将一部分人类执行业务的逻辑或智能用技术的形式进行了实现，而随着人工智能技术的发展，这些技术中所体现的智能将越来越高，面向的业务范围也越来越广。计算机和网络技术最早是由一些科学家所使用的，那时的业务更像是一些技术领域的业务，后来将业务扩展到商务等实际应用领域。目前，我们的业务应用还处于相对初级的阶段，但它的扩展是未来发展的主要方向，并且将会更个性化、更智能化。

(3)支撑：为开发应用组件而提供技术上支撑的资源，包括网络设施、操作系统软件等

支撑类资源更多的是一些具体的技术，为应用类资源的实现提供服务。这类资源也有它们自己要处理的信息，例如路由技术就需要处理路由资源等。支撑类资源往往种类繁多，但在信息系统中，它们一般包括一系列的物理设施、电子设施、网络技术、操作系统等。

应用和支撑之间的区别：应用资源是以逻辑驱动技术，而支撑资源是以技术驱动逻辑。

2. 网络信息安全任务

网络安全的任务是保障各种网络资源(局域网资源、边界资源和网络基础设施)的稳定、可靠地运行和受控、合法地使用。

信息安全的任务是保障信息在存储、传输、处理等过程中的安全。具体的有：

(1)机密性(confidentiality)：指防止非授权用户获得有用的信息的特性。

(2)完整性(integrity)：指数据没有遭到非授权的更改和破坏。

(3)不可抵赖性(non-repudiation)：指实体不能抵赖其发送、接受某信息或参与某活动事实的特性。

(4)可用性(availability)：指保证授权用户对资源合法使用的特性。

3. 网络信息安全机制

网络信息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。

在网络信息安全领域，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 1－1 所示。

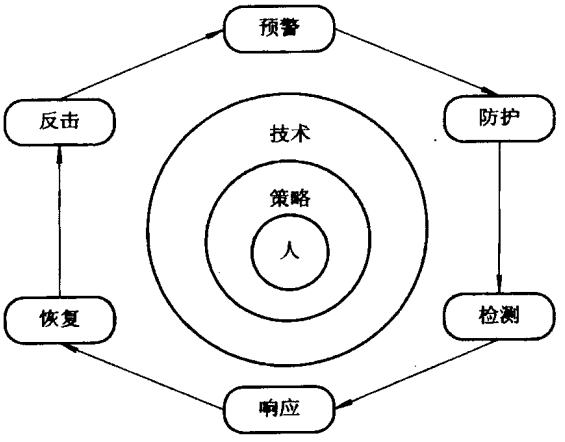

图 1－1　安全机制之间的关系

网络信息安全中层机制有：身份认证、授权、加密、网络隔离、高可用性、内容分析等。

网络信息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。网络信息安全具体应用域有：防火墙应用、入侵检测、反病毒软件、文件共享安全应用等。

安全服务（安全任务）、安全机制和安全应用域是网络信息安全系统的三要素，它们的关系可以用一个三维坐标进行表述，如图 1－2 所示。

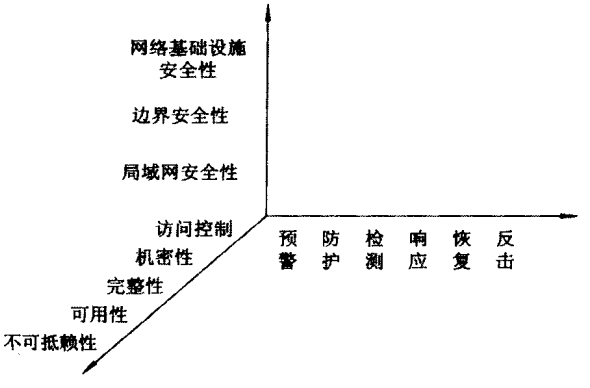

图 1－2　安全服务、安全机制和安全应用域之间的关系

4. 安全体系结构框架

网络信息安全体系结构框架反映了信息系统安全需求和体系结构的共性，其构成要素是安全特性、系统单元及 OSI 参考模型的结构层次。图 1－3 所示为三维信息系统安全体系结构框架。

(1)安全特性

安全特性描述了信息系统的安全机制，包括身份鉴别、访问控制、数据保密、数据完整性、防止否认、审计管理、可用性和可靠性等。

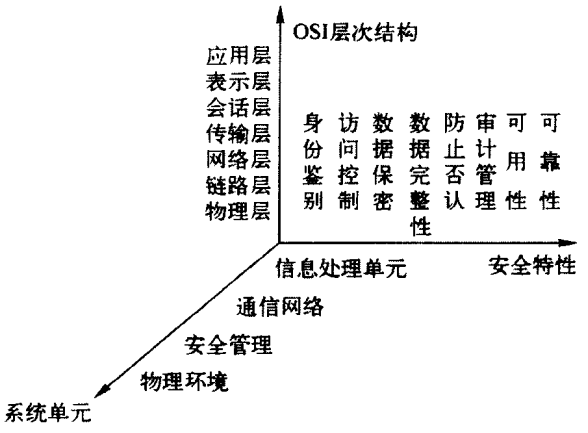

图 1—3　三维信息系统安全体系结构框架

(2)系统单元

系统单元除包括网络信息系统各组成部分外,还包括使用和管理信息系统的物理和行政环境。具体分为信息处理单元、通信网络、安全管理和物理环境 4 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。

(3)OSI 参考模型的结构层次

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。网络体系的不同层次的主体和客体及其控制是不同的。

①链路层负责建立点到点通信,主体是链路的端节点,客体是数据帧,可采用链路加密保证通信安全。

②网络层负责流量的路由控制,主体是网络或主机,客体是数据包或分组,可以采用防火墙技术控制流量在网络边界的传输;采用 IP 加密传输信道技术 IPsec,在两个网络节点间建立透明的安全加密信道。

③传输层负责建立端到端的进程通信,主体是进程,客体是虚电路,可采用安全套接层 SSL 技术实现进程间的安全服务和加密信道。

④应用层的主体是用户及其应用,客体是文件,可采用能提供各种安全服务的中间件技术,提供身份鉴别、访问控制、数据保密和数据完整性等安全服务,以保证信息和应用的安全。

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应包括身份认证、授权管理、安全防御、安全检测和加密 5 个子系统。

5. 防范体系框架结构

为了能够有效地了解用户的安全需求，选择各种安全产品和策略，有必要建立一些系统的方法来进行网络安全防范。网络安全防范体系的科学性、可行性是其可顺利实施的保障。图 1－4 给出了基于 DISSP 扩展的一个三维安全防范技术体系框架结构。第一维是安全服务，给出了 8 种安全属性。第二维是系统单元，给出了信息网络系统的组成。第三维是结构层次，给出并扩展了国际标准化组织 OSI 的开放系统互联(OSI)模型。

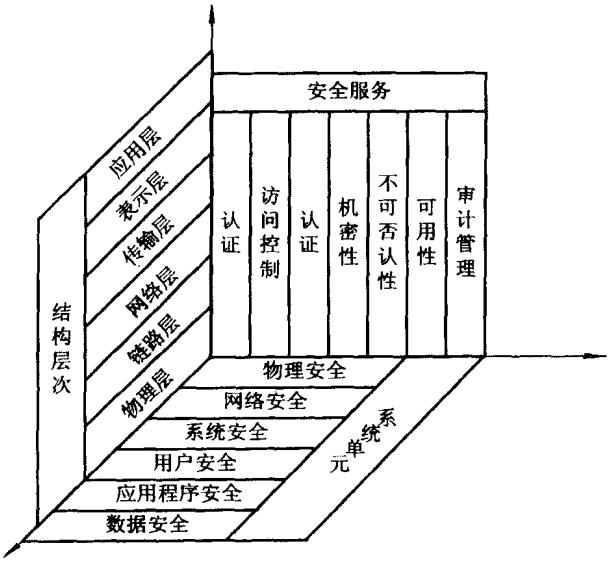

图 1－4　安全防范技术体系框架结构

1.2.3　网络信息安全模型

由于网络信息系统受到的攻击日趋频繁，所以安全的概念不能仅仅局限于信息的保护，需要的是对整个网络信息系统的保护和防御，以确保它们的安全性，包括对系统的保护、检测和反应能力等。

总的来说，安全模型已经从以前的被动保护转到了现在的主动防御，强调整个生命周期的防御和恢复。PDR 模型就是最早提出的体现这样一种思想的安全模型。所谓 PDR 模型是指基于防护(Protection)、检测(Detection)和响应(Reaction)的安全模型。

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。该模型即可量化、可由数学证明、基于时间的、以 PDR 为核心的安全模型，亦称为 P2DR 模型。这里，P2DR 是 Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)的缩写，如图 1－5 所示。

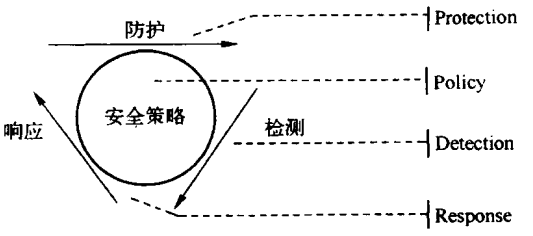

图 1－5　P2DR 安全模型

1. 安全策略

根据风险分析产生的安全策略描述了系统中哪些资源要得到保护，以及如何实现对它们的保护等。安全策略是 P2DR 安全模型的核心，所有的防护、检测、响应都是依据安全策略实施的，企业安全策略为安全管理提供方向和支持手段。

2. 防护

通过修复系统漏洞、正确设计、开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监视等手段来防止恶意威胁。

3. 检测

在 P2DR 模型中，检测是非常重要的一个环节，检测是动态响应和加强防护的依据，它也是强制落实安全策略的有力工具，通过不断地检测和监控网络和系统，来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

4. 响应

紧急响应在安全系统中占有最重要的地位，是解决安全潜在问题最有效的办法。从某种意义上讲，安全问题就是要解决紧急安全和异常处理问题。

信息系统的安全是基于时间特性的，P2DR 安全模型的特点就在于动态性和基于时间的特性。下面先定义几个时间值：

攻击时间 Pt：表示从入侵开始到侵入系统的时间。攻击时间的衡量特性包括入侵能力和系统脆弱性两个方面。高水平的入侵及安全薄弱的系统都能增强攻击的有效性，使攻击时间 Pt 缩短。

检测时间 Dt：系统安全检测包括系统的安全隐患和潜在攻击检测，以利于系统的安全评测。改进检测算法和设计可缩短 Dt，提高对抗攻击的效率。检测系统按计划完成所有检测的时间为一个检测周期。网络与防护是相互关联的，适当的防护措施可有效缩短检测时间。

响应时间 Rt：包括检测到系统漏洞或监控到非法攻击到系统启动处理措施的时间。例如，一个监控系统的响应可能包括监视、切换、跟踪、报警、反击等内容；而安全事件的后处理（如恢复、总结等）不纳入事件响应的范畴之内。