网络信息安全原理

WANGLUOXINXIANQUANYUANLI

梅 挺 著

科学出版社
www.sciencep.com

网络信息安全原理

梅 挺 著

科 学 出 版 社
北 京

内 容 提 要

本书具有科学严谨的体系结构，内容丰富，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网络安全原理与实践技术。

本书可作为网络安全领域的科技人员与信息系统安全管理的参考用书，也可作为高等院校研究生教材使用。

图书在版编目（CIP）数据

网络信息安全原理 /梅挺著.—北京:科学出版社，2009
ISBN 978-7-03-025861-8

Ⅰ.信… Ⅱ.梅… 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 193632 号

网络信息安全原理

梅 挺 著

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
四川煤田地质制图印刷厂印刷
科学出版社发行 各地新华书店经销
*
2009 年 10 月第 一 版 开本：16（787×1092）
2009 年 10 月第一次印刷 印张：14 1/2
印数：1—1 500 字数：280 千字

定价：39.00 元

前　言

随着 Internet 的迅猛发展和信息社会的到来，网络已经影响到社会的政治、经济、文化、军事和社会生活的各个方面。以网络方式获取信息或交流信息已成为现代信息社会的一个重要特征。同时，随着人们对网络信息系统依赖的日益增强，网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。

在人类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显得十分迫切和重要，它不仅关系到战争的胜负、国家的安危、科技的进步、经济的发展，而且也关系到每个人的切身利益。但是，网络作为一把双刃剑，在加速人类社会信息化的同时，也给信息安全保障带来了极大的挑战。网络犯罪事件已屡见不鲜，且呈逐年上升趋势。特别，随着电子商务、电子现金、数字货币、网络银行等业务的兴起以及各种专用网（如金融网）的建设，伴随着这些业务产生的互联网和网络信息的安全问题，也已成为人们关注的热点问题。

当前，我国的网络安全正面临着严峻的挑战：一方面随着电子政务工程的启动，电子商务的开展以及国家关键基础设施的网络化，使得现有的网络安全设施建设日益滞后；另一方面，黑客入侵、病毒传播以及形形色色的网络攻击事件日益增多，且成功率一直居高不下，从侧面反映出广大网民的网络防护意识和网络安全知识的欠缺。针对这种现状，作者在总结多年的实践经验和从事网络安全研究成果的基础上编写了本书。

网络安全技术是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。因此，网络安全研究的内容十分广泛，它涉及密码学理论、安全体系结构、安全协议、网络信息分析、网络安全监控、应急处理等，其中密码学理论是网络安全的关键技术。本书全面阐述了网络安全原理和实践技术，主要包括：网络安全技术知识、密码技术、访问控制和防火墙技术、入侵检测与安全审计技术、黑客与病毒防范技术、操作系统安全技术、数据库系统安全技术等诸多知识。

本书是以 PDRR 模型为基础进行撰写的。PDRR 网络安全模型中，网络安全体系结构分成四部分：防护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）。从这个模型看，网络安全的建设是这样一个有机的过程：在信息安全管理政策的指导下，通过风险评估，明确需要防护的信息、网络基础设施和资产，然后利用入侵检测系统来发现外界的攻击和入侵，对已经发生的入侵，进行应急响

应和恢复。PDRR 模型可以明确网络安全的每个组件在实际架构中的角色和定位，有利于作为指南寻找未来研究和应用中的突破点。在安全防护部分重点介绍：系统安全防护、网络安全防护和信息安全防护。系统安全防护指的是操作系统的安全防护；网络安全防护中重点介绍网络安全管理政策、网络安全风险评估以及网络设备的访问权限控制；而信息安全防护则介绍信息安全当中的一些重要概念和内容。检测部分的主要内容是入侵检测系统的理论，包括入侵检测系统的概念、技术和评估以及入侵检测系统的发展前景。在响应和恢复部分中，重点介绍计算机紧急响应小组的建立及其业务，对于一个规模较大的网络来说，这样的一个组织的存在和运作是非常重要的。本书注意保持“新技术”这一特点，介绍目前网络安全当中新技术的进展情况。

本书具有科学严谨的体系结构，内容丰富，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网络安全原理与实践技术。

本书得到了成都医学院学术著作出版基金资助，也是我主持的四川省教育厅资助项目“加密与纠错编码相结合——代数编码在现代密码学中的应用研究”的成果之一。本书还得到了张仕斌教授和易勇教授的关心，也参阅了一些专家的研究成果，在此深表谢意。由于撰写时间仓促，书中疏漏之处在所难免，欢迎专家、读者批评指正。

作 者

2009 年 9 月

目　录

第1章　网络信息安全概述

1.1　网络信息安全基础知识

1.1.1 网络信息安全的内涵

在网络出现以前，信息安全指对信息的机密性、完整性和可获性的保护，即面向数据的安全。互联网出现以后，信息安全除了上述概念以外，其内涵又扩展到面向用户的安全，即鉴别、授权、访问控制、抗否认性和可服务性以及内容的个人隐私、知识产权等的保护。这两者的结合就是现代的信息安全体系结构。

网络安全从本质上讲就是网络上信息的安全，指网络系统的硬件、软件及其系统中的数据安全。网络信息的传输、存储、处理和使用都要求处于安全的状态。

1.1.2 网络信息安全的特征

网络信息安全根据其本质的界定，应具有以下的基本特征：

① 保密性：保密性是指信息不泄漏给非授权的个人、实体和过程，或供其使用的特性。

② 完整性：完整性是指信息未经授权不能被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。对网络信息安全进行攻击其最终目的就是破坏信息的完整性。

③ 可用性：可用性是指合法用户访问并能按要求顺序使用信息的特性，即保证合法用户在需要时可以访问到信息及相关资产。

④ 可控性：可控性是指授权机构对信息的内容及传播具有控制能力的特性，可以控制授权范围内的信息流向以及方式。

⑤ 可审查性：在信息交流过程结束后，通信双方不能抵赖曾经做出的行为，也不能否认曾经接收到对方的信息。

1.1.3 网络信息安全的关键技术

网络信息安全的关键技术主要包括主机安全技术、身份认证技术、访问控制技术、加密技术、防火墙技术、安全审计技术与安全管理技术等。在以后的章节中，我们将介绍现在常见几种技术。

1.1.4 网络信息安全分类

网络信息安全根据不同的分类方法有多种不同的分类，表1-1就是其中的一种分类。

表 1-1 网络信息安全的分类

技 术	分 类		说 明
信息安全	监察安全	监控查验	发现违规
			确定入侵
			定位损害
			监控威胁
		犯罪起诉	起诉
			量刑
		纠偏建议	
	管理安全	技术管理安全	多级安全用户鉴别术的管理
			多级安全加密术的管理
			密铜管理术的管理
		行政管理安全	人员管理
			系统管理
		应急管理安全	应急的措施组织
			入侵的自卫与反击
	技术安全	实体安全	环境安全(温度、湿度、气压等)
			建筑安全(防雷、防水、防鼠等)
			网络与设备安全
		软件安全	软件的安全开发与安装
			软件的安全复制与升级
			软件加密
			软件安全性能测试
		数据安全	数据加密
			数据存储安全
			数据备份
		运行安全	访问控制
			审计跟踪
			入侵告警与系统恢复等
	立法安全	有关信息安全的政策、法令、法规	
	认知安全	办学	
		奖惩	
		信息安全宣传与普及教育	

1.1.5 网络信息安全问题的根源

1. 网络安全事故发生的原因

网络安全事故发生的 5 个原因如下：

① 现有网络系统和协议还是不健全、不完善、不安全的。

② 思想麻痹，没有清醒地意识到黑客入侵导致的严重后果，舍不得投入必要的人力、财力和物力来加强网络的安全性。

③ 没有采用正确的安全策略和安全机制。

④ 缺乏先进的网络安全技术、工具、手段和产品。

⑤ 缺乏先进的灾难恢复措施和备份意识。

2. 局域网（站点）安全事故发生的原因

局域网（站点）安全事故发生的 5 个原因如下：

① 网络系统的流量。
② 网络提供的和使用的服务。
③ 网络与 Internet 的连接方式。
④ 网络的知名度。
⑤ 网络对安全事故的准备情况。

1.1.6 网络信息安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。实现网络安全，不但要靠先进的技术，而且也得靠严格的管理、法律约束和安全教育，主要包括以下内容：

① 威严的法律：安全的基石是社会法律、法规和手段，即通过建立与信息安全相关的法律和法规，使不法分子慑于法律，不敢轻举妄动。

② 先进的技术：先进的技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类。选择相应的安全机制，然后集成先进的安全技术。

③ 严格的管理：各网络使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

网络安全策略是一个系统的概念，它是网络安全系统的灵魂与核心，任何可靠的网络安全系统都是构架在各种安全技术集成的基础之上，而网络安全策略的提出，正是为了实现这种技术的集成。可以说网络安全策略是我们为了保护网络安全而制定的一系列法律、法规和措施的总和。当前制定的网络安全策略主要包含 5 个方面的策略。

1. 物理安全策略

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件设备和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限，防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种盗劫、破坏活动的发生。

2. 访问控制策略

访问控制策略是网络安全防范的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到安全保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。它主要由入网访问控制、网络权限控制、目录级安全控制、属性安全控制、网络服务安全控制、网络检测和锁定控制及网络端口和节点的安全控制组成。

① 入网访问控制：入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为三个步骤：用户名的识别与验证；用户口令的识别与验证；用户帐号的缺省限制检查。三个关卡中只要任何一关未过，该用户便不能进入该网络。

② 网络的权限控制：网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。我们可以根据访问权将用户分为：特殊用户（系统管理员）、一般用户和审计用户。

③ 目录级安全控制：网络应允许控制用户对目录、文件、设备的访问。用户在目录级制定的权限对所有文件和子目录有效，用户还可进一步制定对目录下的子目录和文件的权限。访问权限一般有 8 种：系统管理员权限、读权限、写权限、创建权限、删除权限、修改权限、文件查找权限和存取控制权限。8 种访问权限的有效组合可以让用户有效地完成任务，同时又能有效的控制用户对服务器资源的访问，从而加强了网络和服务器的安全。

④ 属性安全控制：当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性设置可以覆盖已经指定的任何受托者指派的有效权限。属性往往可以控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除文件或目录、查看目录和文件、执行文件、共享、系统属性等。网络的属性可以保护重要的目录和文件防止用户对目录和文件的误删除、执行、修改、显示等。

⑤ 网络服务器安全控制：是在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以安装和删除软件等操作。服务器的安全控制包括可以设置口令来锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限定、非法访问者检测和关闭的时间间隔等。

⑥ 网络检测和锁定控制：网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形、文字或声音等形式报警，以引起管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该帐号将被自动锁定。

⑦ 网络端口和结点的安全控制：网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护，并以加密的形式来识别结点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

3. 防火墙控制

它是控制进出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

4. 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。常用的方法有链路加密、端到端加密和节点加密三种。链路加密的目的是保护网络结点之间的链路信息安全；端到端加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

5. 网络安全管理策略

在网络安全中，除了采用上述措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络的安全、可靠地运行，将起到十分有效的作用。网络的安全管理策略包括：确定安全管理的等级和安全管理的范围；制定有关网络使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。

随着网络技术的发展，计算机网络将日益成为工业、农业和国防等方面的重要信息交

换手段，渗透到社会生活的各个领域。因此认清网络的脆弱性和潜在威胁，采取强有力的安全策略，对于保障网络的安全性将变得十分重要。

1.2 网络信息安全体系结构与模型

1.2.1 ISO/OSI 安全体系结构

1982年，开放系统互联（OSI）参考模型建立之初，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联标准的第二部分，即ISO7498-2标准，并首次确定了开放系统互联（OSI）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安全体系结构包括了三部分内容：安全服务、安全机制和安全管理。

1. 安全服务

安全服务是由参与通信的开放系统的某一层所提供的服务，它确保了该系统或数据传输具有足够的安全性。ISO 安全体系结构确定了 5 大类安全服务：认证、访问控制、数据保密性、数据完整性和不可否认（抗抵赖）性，下面分别介绍。

（1）认证服务

这种安全服务提供某个实体的身份保证。该服务有两种类型：对等实体认证和数据源认证。

① 对等实体认证：这种安全服务由(N)层提供时，(N+1)层实体可确信其对等实体是它所需要的(N+1)层实体。该服务在建立连接或数据传输期间的某些时刻使用，以确认一个或多个其他实体连接的一个或多个实体的身份。该服务在使用期内让使用者确信：某个实体没有试图冒充别的实体，而且没有试图非法重放以前的某个连接。它们可以实施单向或双向对等实体的认证，既可以带有效期校验，也可以不带，以提供不同程度的保护。

② 数据源认证：在通信的某个环节中，需要确认某个数据是由某个发送者发送的。当这种安全服务由(N)层提供时，可向(N+1)层实体证实数据源正是它所需要的对等(N+1)层实体。这种服务对数据单元的来源能够提供确认，但不提供防止数据单元复制或篡改的保护。

（2）访问控制服务

这种安全服务提供的保护，就是对某一些确知身份限制对某些资源（这些资源可能是通过 OSI 协议可访问的 OSI 资源或非 OSI 资源）的访问。这种安全服务可用于对某个资源的各类访问（如通信资源的利用，信息资源的阅读、书写或删除，处理资源的执行等）或用于对某些资源的所有访问。

访问控制是实现授权的一种方法，它涉及通信和系统的安全问题。它对通信协议有很高的要求。

（3）数据保密性服务

这种安全服务能够提供保护，使得信息不泄漏、不暴露给那些未授权就想掌握该信息的实体。

① 连接保密性：这种安全服务向某个(N)连接的所有(N)用户数据提供保密性。

② 无连接保密性：这种安全服务向单个无连接(N)安全数据单元(SDU)中的所有(N)用

户数据提供保密性。

③ 选择字段保密性：这种安全服务向(N)连接上的(N)用户数据内或单个无连接(N)SDU 中的被选字段提供保密性。

④ 业务流保密性：这种安全服务防止通过观察业务流以得到有用的保密信息。

（4）数据完整性服务

这种安全服务保护数据在存储和传输中的完整性。主要有以下几类：

① 带恢复的连接完整性：这种安全服务向某个(N)连接上的所有(N)用户数据保证其完整性。它检测对某个完整的 SDU 序列内任何一个数据遭到的任何篡改、插入、删除或重放，同时还可以补救恢复。

② 不带恢复的连接完整性：与带恢复的连接完整性服务相同，但不能补救恢复。

③ 选择字段连接完整性：这种安全服务向在某个连接中传输的某个(N)SDU 的(N)用户数据内的被选字段提供完整性保护，并能确定这些字段是否经过篡改、插入、删除或重放。

④ 无连接完整性：这种安全服务由(N)层提供，向提出请求的(N+1)层实体提供无连接中的数据完整性保证。并能确定收到的 SDU 是否经过篡改；另外，还可以对重放情况进行一定程度的检测。

⑤ 选择字段无连接完整性：这种安全服务对单个无连接 SDU 中的被选字段的保证其完整性，并能确定被选字段是否经过篡改、插入、删除或重放。

（5）不可否认服务（抗抵赖）

它主要保护通信系统不会遭到自系统中其他合法用户的威胁，而不是来自未知攻击者的威胁。

① 数据源的抗抵赖：向数据接收者提供数据来源的证据，以防止发送者否认发送该数据或其内容的任何企图。

② 传递过程的抗抵赖：向数据发送者提供数据已到目的地的证据，以防止收信者否认接收该数据或其内容的任何事后的企图。

2. 安全机制

为了支持以上的安全服务，ISO 安全体系结构定义了 8 大类安全机制：加密、数据签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务填充机制、路由控制机制和公证机制，这些安全机制可以设置在适当的层次上，以便提供某些安全服务。

（1）加密机制

加密可向数据或业务流信息提供保密性，并能对其他安全机制起作用或对它们进行补充。加密算法可以是可逆或不可逆的，可逆加密算法有以下两大类：

① 对称（单钥）加密体制：对于这种加密体制，加密与解密用同一个密钥。

② 非对称（双钥或公钥）加密体制：对于这种加密体制，加密与解密用不同的密钥，这种加密系统的两个密钥有时被称为“公钥”和“私钥”。

（2）数字签名机制

这种安全机制由两个过程构成：对数据单元签名过程和验证签名的数据单元过程。第一个过程可以利用签名者私有的（即独有和保密的）信息，而第二个过程则要利用公之于众的规程和信息，但通过它们并不能推出签名者的私有信息。

（3）访问控制机制

这种安全机制可以利用某个实体经鉴别的身份或关于该实体的信息（如某个已知实体