高等学校信息安全专业规划教材

网络安全原理

叶 清 主编

WUHAN UNIVERSITY PRESS
武汉大学出版社

高等学校信息安全专业规划教材

网络安全原理

主　编　叶　清
副主编　黄高峰　严　博　付　伟
主　审　吴晓平

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

网络安全原理/叶清主编. —武汉：武汉大学出版社，2014.5
高等学校信息安全专业规划教材
ISBN 978-7-307-12982-5

Ⅰ.网… Ⅱ.叶… Ⅲ.计算机网络—安全技术—高等学校—教材
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2014)第 054450 号

责任编辑：方慧娜　　责任校对：鄢春梅　　版式设计：马　佳

出版发行：**武汉大学出版社**　(430072　武昌　珞珈山)
(电子邮件：cbs22@whu.edu.cn　网址：www.wdp.com.cn)
印刷：武汉中科兴业印务有限公司
开本：787×1092　1/16　印张：19　字数：482 千字　插页：1
版次：2014 年 5 月第 1 版　2014 年 5 月第 1 次印刷
ISBN 978-7-307-12982-5　定价：39.00 元

叶 清 1978年出生，工程博士，海军工程大学信息安全系副教授，硕士生导师，中国计算机学会会员。主要研究方向为无线传感网络安全关键技术。一直以来承担专业主干课程——网络安全原理的教学任务，具有丰富、宝贵的一手教学经验。近年来，在无线传感器网络安全路由协议、安全认证协议、密钥协商方案等方面进行了系统深入的研究，主持承担了多项科研项目，曾获得多项军队科技进步奖，在国际国内重要学术刊物和会议上发表论文30余篇。

前　言

网络信息安全问题自网络诞生之初，就一直是个困扰网络建设者和使用者的难题。随着网络应用的不断普及以及新兴网络技术的发展，再加上网络自身所具有的开放性和自由性等特点，人们在不断提高网络应用广泛性、便利性的同时，对网络平台的安全提出了更高的要求。网络信息安全已经越来越成为网络社会中的关键问题，是网络研究的重点和热点。

本书以培养网络安全方面的应用型人才为目标，将重点放在对网络安全基础知识的了解和对各种网络安全技术的应用之上，将理论、技术、应用融为一体，同时也兼顾到教材的先进性、实用性和可读性。

本书特点主要体现在以下三个方面。

首先，通俗易懂。计算机网络的技术性很强，网络安全技术本身也比较晦涩难懂，本书力求以通俗的语言和清晰的叙述方式，向读者介绍计算机网络安全的基本理论、基本知识和实用技术。

其次，突出实用。通过阅读本书，读者可掌握网络安全的基础知识，并了解设计和维护网络及其应用系统安全的基本手段和方法。本书在编写形式上突出了应用的需求，在每章结尾都附有练习题，部分章节还配有相关实训题，从而为教学和自主学习提供了方便。

再次，选材新颖。计算机应用技术和网络技术的发展是非常迅速的，本书在内容组织上力求靠近新知识、新技术的前沿，以使本书能较好地反映新理论和新技术。

本书共分 9 章，第 1 章介绍了一般性的网络安全概念，包括网络安全分析、网络安全威胁类型、网络安全措施、网络安全策略、网络安全技术的发展等，使读者能够对网络安全有一个整体的了解和认识。第 2 章介绍了有关网络安全通信协议的内容，比较系统地介绍了 TCP/IP 协议簇的安全架构以及传输层、应用层等协议层的常用经典安全通信协议，同时阐述了安全协议的主要形式化分析方法——BAN 逻辑。第 3 章主要介绍了网络身份认证技术、公钥基础设施(PKI)等知识内容，包括网络身份认证基础、网络身份认证技术方法以及 PKI 提供的安全服务、体系结构和信任模型。第 4 章介绍了主要网络服务如 DNS、WEB、Email、FTP、即时通信等服务的安全隐患与安全解决方案。第 5 章主要介绍了网络安全漏洞检测与防护，包括网络安全漏洞的基本内容、网络安全漏洞扫描技术与网络安全漏洞防护技术。第 6 章主要介绍了虚拟专用网(VPN)的基础知识、关键技术与解决方案。第 7 章介绍了防火墙知识，包括防火墙的基础知识、防火墙采用的关键技术、防火墙使用的体系结构以及防火墙的发展趋势。第 8 章介绍了入侵检测技术，包括入侵检测的基本概念、入侵检测系统分类、典型入侵检测技术、新型入侵检测技术，重点阐述了模式串匹配算法(单模式匹配、多模式匹配)及其在实际系统中的运用。第 9 章主要介绍了网络安全技术的新发展，包括云计算技术及其安全问题、物联网技术及其安全问题、P2P 技术及其安全问题。

本书由叶清担任主编，黄高峰、严博、付伟担任副主编。其中第 1、2、8 章由叶清编

写，第3、7章由严博编写，第4、6章由黄高峰编写，第5、9章由付伟编写，全书由叶清统稿、定稿。

由于编者水平有限，书中难免存在一些疏漏和不足，敬请广大读者指正。

编　者

2014年2月

目 录

第 1 章　网络安全概述

计算机网络安全不仅关系到国计民生，还与国家安全密切相关；不仅涉及国家政治、军事和经济各个方面，而且还影响到国家的安全和主权。因此，现代网络技术中最关键的也最容易被忽视的安全性问题，已经成为各国关注的焦点，也是热门研究和人才需求的新领域。只有在法律、管理、技术、道德各个方面采取切实可行的有效措施，共同努力，才能确保实现网络安全。

1.1　网络安全简介

1.1.1　网络安全概念

什么是网络安全？网络安全是指利用网络管理控制和技术措施，保证在网络环境中数据的机密性、完整性、网络服务可用性和可审查性受到保护。保证网络系统的硬件、软件及其系统中的数据资源得到完整、准确、连续的运行和服务不受到干扰破坏和非授权使用。网络安全问题实际上包括网络的系统安全和信息安全，而保护网络的信息安全是网络安全的最终目标和关键，因此，网络安全的实质是指网络的信息安全。

计算机网络安全是一门涉及计算机科学、网络技术、信息安全技术、通信技术、应用数学、密码技术和信息论等多学科的综合性学科，是信息安全学科的重要组成部分。

随着信息技术的发展与应用，信息安全的内涵在不断地延伸和变化，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，进而又发展为“攻击、防御、检测、控制、管理、评估”等多方面的基础理论和实施技术。

1.1.2　网络安全脆弱性与重要性

网络安全问题与计算机、网络的脆弱性密切相关，其脆弱性主要体现在以下几个方面。

(1)人为操作失误。主要包括操作人员对其安全配置不当造成的安全漏洞、用户安全意识不强、用户口令选择不慎、用户将自己的账号随意转借他人或与别人共享等。

(2)操作系统漏洞。操作系统结构体制本身不可避免地拥有漏洞。例如，可以远程创建和激活进程；一般操作系统都提供远程过程调用(RPC)服务，而提供的安全验证功能却很有限；对于操作系统安排的无口令入口，是为系统开发人员提供的边界入口，但这些入口也可能被黑客利用；操作系统还有隐藏的信道，也存在潜在的危险；尽管操作系统的缺陷可以通过版本的不断升级来克服，但系统的某一个安全漏洞就会使系统的所有安全控制变得毫无价值。

(3)网络。使用 TCP/IP 协议的网络所提供的 FTP、E-mail、RPC 和 NFS 都包含许多不安全因素，存在着许多漏洞。同时，网络的普及使信息共享达到了一个新的层次，也使信息

被泄露的机会大大增多。特别是 Internet 网络就是一个不设防的开放大系统。另外，数据处理的可访问性和资源共享的目的性是一对矛盾体，它使得计算机系统保密性难以保证。

(4)数据库。当前，大量的信息存储在各种各样的数据库中，然而，这些数据库系统在安全方面的考虑却很少。而且数据库管理系统安全必须与操作系统的安全相配套，但实际上有时却不是这样，造成了数据库不安全因素的存在。

1.1.3 网络安全目标

网络安全目标主要表现在系统的保密性、完整性、可靠性、可用性、不可抵赖性和可控性等方面。

(1)机密性。机密性是指网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性，即防止信息泄露给非授权个人或实体，信息只为授权用户所使用的特性。机密性是在可靠性和可用性的基础之上，保障网络信息安全的重要手段。常用的保密技术包括：防侦听(使对手侦听不到有用的信息)、防辐射(防止有用信息以各种途径辐射出去)、信息加密(在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息，也会因为没有密钥而无法读懂有效信息)、物理保密(利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露)。

(2)完整性。完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和正确传输。完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不受到各种原因的破坏。影响网络信息完整性的主要因素包括：设备故障、误码(传输、处理和存储过程中产生的误码；定时的稳定度和精度降低造成的误码；各种干扰源造成的误码)、人为攻击、计算机病毒等。

(3)可靠性。可靠性是网络信息系统能够在规定条件下和规定时间内完成规定功能的特性。可靠性是系统安全的最基本要求之一，也是所有网络信息系统的建设和运行目标。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演着重要的角色。因为系统失效的大部分原因是人为差错造成的，而人的行为要受到生理和心理、技术熟练程度、责任心和品德等方面的影响，因此，人员的教育、培养、训练、管理以及合理的人机界面是提高可靠性重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

(4)可用性。可用性是网络信息可授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。同时，可用性还应该满足以下要求：身份识别与确认、访问控制、业务流控制、路由选择控制、审计跟踪。

(5)不可抵赖性。不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确保参与者的真实同一性，即所有参与者都不能否认或抵赖曾经完成的操作和承诺。利用信

息资源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收了信息。

(6)可控性。可控性是对网络信息的传播及内容具有可控制能力的特性。

概括地说，网络安全目标是通过计算机、网络、密码技术和安全技术，保护在公用网络系统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

1.1.4　网络安全模型

1. P2DR 模型

P2DR 模型是由美国国际互联网安全系统公司提出的一个自适应的安全模型(Adaptive Network Security Model)，如图 1-1 所示。

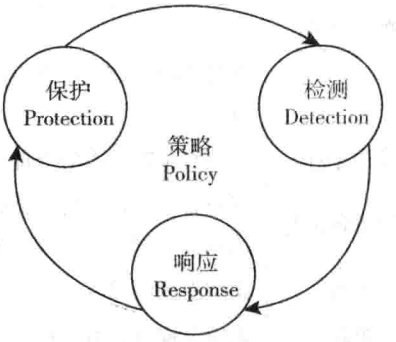

图 1-1　P2DR 安全模型

P2DR 模型包括 4 个主要部分，分别是：

(1)策略(Policy)。安全策略是整个 P2DR 模型的核心，所有的防护、检测、响应都是依据安全策略而实施的，安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制订、评估、执行等。制定可行的安全策略取决于对网络信息系统的了解程度。不同的网络需要不同的策略，在制定策略以前，需要全面考虑网络有哪些安全需求，分析网络存在哪些安全风险，了解网络的结构、规模，了解应用系统的用途和安全要求等。对这些问题做出详细回答，明确哪些资源是需要保护的，需要达到什么样的安全级别，并确定采用何种防护手段和实施办法，这就是针对网络的一份完整的安全策略。策略一旦制定，应当作为整个网络安全行为的准则。

(2)保护(Protection)。保护就是采用一切可能的手段来保护网络系统的保密性、完整性、可用性、可靠性和不可否认性。保护是预先组织可能引起攻击的条件产生，让攻击者无懈可击，良好的防护可以避免大多数入侵事件的发生。在安全策略的指导下，根据不同等级的系统安全要求来完善系统的安全功能和安全机制。通常采用传统的静态安全技术来实现。

(3)检测(Detection)。检测是动态响应和加强防护的依据，是强制落实安全策略的工具，通过不断检测和监控网络及系统来发现新的威胁和弱点，并利用循环反馈来及时左右有效的响应。网络安全风险是实时存在的，检测的对象主要针对系统自身的脆弱性及外部威胁，利用检测工具了解和评估系统的安全状态。

(4)响应(Response)。在检测到安全漏洞之后必须及时做出正确的响应，从而把系统调整到安全状态。对危及安全的时间、行为、过程，及时做出处理，杜绝危害进一步扩大，使系统尽快恢复到能提供正常服务的状态。常用响应方式如表 1-1 所示。

P2DR 模型是一种基于时间的安全理论，由于信息安全相关的所有活动，如攻击行为、防护行为、检测行为和响应行为等都要消耗时间，因此可以用时间来衡量一个体系的安全性和安全能力，继而可以用典型的数学公式来表达系统的安全性。

(1)Pt>Dt+Rt；Pt：系统为了保护安全目标设置各种保护的防护时间；Dt：系统能够检测到攻击所花费的时间；Rt：系统针对攻击做出响应的时间。从以上公式可以推出，如果防护时间 Pt 大于检测时间 Dt 与响应时间 Rt 之和，则认为系统是安全的，因为它在黑客攻击

危害系统之前就能够检测到并进行处理。

表 1-1　　常用的响应方式表

响应方式	响　应　规　则
记录	将终端执行策略所产生的事件信息写入数据库，审计操作人员对事件响应信息进行查询分析
发送邮件	系统将策略产生的事件信息以邮件的方式发送给管理员
发送本地消息	系统将终端执行管理策略产生的事件信息以消息的方式发送给终端使用人员，以便让使用人员了解信息，及时采取相应的解决措施
关机	系统发现终端有违规事件发生时，强制关闭终端主机
阻断	系统发现终端有违规事件发生时，启用内置防火墙阻断终端与其他主机的通信
报警	系统将终端执行策略产生的事件信息发送到指定的报警服务器上，让管理员及时了解代理主机的使用状态

(2) Et = Dt+Rt，if Pt = 0；Et：系统暴露在攻击状态的时间。假定系统的防护时间 Pt 为 0，如果系统突然遭受到破坏，则希望系统能够快速检测到威胁并迅速调整到正常状态，系统的检测时间 Dt 和响应时间 Rt 之和就是系统的暴露时间 Et。很显然，该时间越少越好，系统就越安全。

按照 P2DR 的观点，一个良好完整的动态安全体系，不仅需要恰当的防护，而且需要动态的检测机制，在发现问题时还需要及时做出响应，这样的一个体系需要在统一、一致的安全策略的指导下实施，由此形成一个完备的、闭环的动态自适应安全体系。然而，在现实应用中 P2DR 模型并没有完成其应有的功能，模型中的安全策略没有实质的内涵，策略的真正指导作用存在缺陷。这导致 P2DR 动态安全模型中的各种安全组件仍然是相互独立的功能模块，只能依赖人为因素的参与来实现动态的安全循环。更深入地考虑 P2DR 动态安全模型的缺陷，可以总结出以下 3 点：

(1) 策略核心没有相应的策略部署、实施平台给予支撑，无法实现真正意义上的基于策略的网络安全管理；

(2) 对动态网络安全的支持不足，自动化程度很低，安全事件的响应过程总是需要人为参与，响应速度慢、效率低、准确度差；

(3) 由于没有统一的管理平台，对大规模分布式系统的管理开销过高导致其可实现性很差，并且不能实现安全体系内部的信息共享和协作。

针对以上缺陷，可从以下 3 个方面对 P2DR 模型进行改进：

(1) 构建策略部署、管理体系结构，在结构中实现策略的自动分发、自动执行和运行时的自管理，使策略核心能够实现用户的操作行为和系统管理动作，满足用户意图及真正指导各安全组件的行为，实现基于策略的网络安全管理。

(2) 引入策略自适应管理、策略联动和安全事件关联分析的思想，满足网络安全的动态性，主要表现在 3 个方面：①依靠策略联动和安全事件关联分析的方法，实现由防护、检测和响应组成的动态安全循环，从而来保障网络安全；②网络安全的目标是动态变化的，支持部分或者全网范围内安全级别的动态调整；③安全目标实现所依赖的网络物理环境是动态可

调整的，网络的安全策略要能够迅速、方便地做出调整以适应新环境下的安全需求。

(3)添加统一管理控制台，实现对分布的被管对象和安全策略进行管理；统一定制安全策略，统一收集各被管对象的安全事件信息，并引入“域”的概念，有效地组织被管对象，实现被管系统的伸缩性，同时，实现了安全体系内部信息的高度共享和协作。

2. PDRR 模型

PDRR 是另一个常用的安全模型，也是得到较多认可的一个安全保障模型。它是美国国防部提出的“信息安全保护体系”中的重要内容，概括了网络安全的整个环节。PDRR 模型由 Protection(防护)、Detection(检测)、Response(响应)、Recovery(恢复)组成。

从工作机制上看，这四个部分是一个顺次发生的过程：首先采取各种措施对需要保护的对象进行安全防护，然后利用相应的检测手段对安全保护对象进行安全跟踪和检测以随时了解其安全状态。如果发现安全保护对象的安全状态发生改变，特别是由安全变为不安全，则马上采取应急措施对其进行处理，直至恢复安全保护对象的安全状态。

PDRR 模型如图 1-2 所示。按照这个模型，网络的安全建设是这样的一个有机的过程：在信息网络安全政策的指导下，通过风险评估，明确需要防护的信息资源、网络基础设施和资产等，明确要防护的内容及其主次等，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。

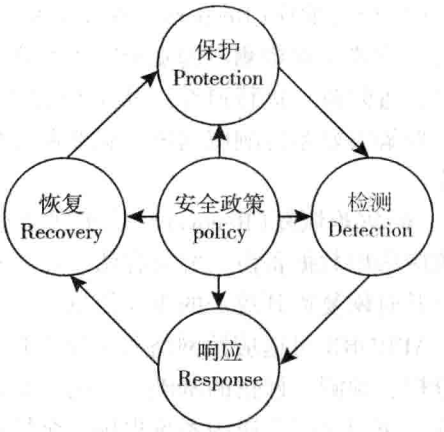

图 1-2　PDRR 安全模型

3. APPDRR 模型

网络的发展是动态的，不断有新的协议、操作系统、应用软件发布和应用，伴随着出现大量新的漏洞、病毒、攻击程序，因此相应的网络安全模型也必须是动态的，新的安全问题的出现需要新的技术来解决。为了发现网络服务器和设备中的新漏洞，不断查明网络中存在的安全风险和威胁，要求网络是一个自适应性的、动态的网络，即系统具有防护功能、实时入侵监控功能、漏洞扫描功能、系统安全决策功能和风险分析功能。由此，经典的自适应性动态网络安全模型——APPDRR 模型便产生了，APPDRR 模型如图 1-3 所示。

图 1-3　APPDRR 模型

(1)风险分析(Analysis)就是分析威胁发生的可能性和系统易于受到攻击的脆弱性，并估计可能由此造成的损失和影响的过程。主要包括风险确认、风险预测和风险评估三个方面。风险确认主要是及时发现网络系统中可能存在的风险，并对其进行分类。风险预测主要是预测风险发生时的直接损失和间接损失。风险评估主要是确定风险对整个网络系统的影响程度，从而确定需要优