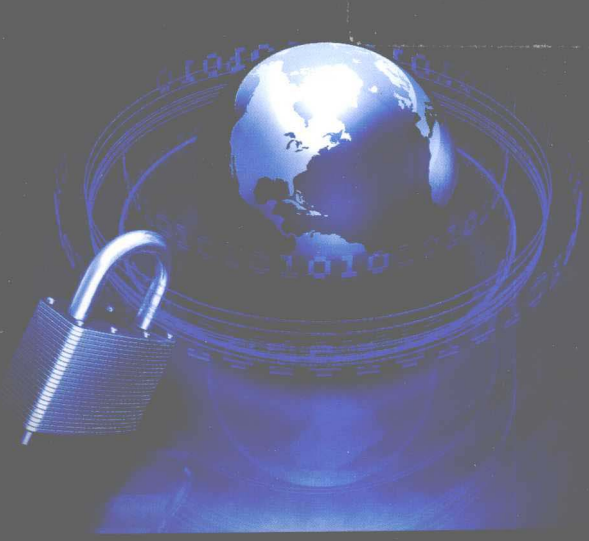
软件研发精品译丛

Network Security
Current Status and Future Directions

网络安全：现状与展望

Christos Douligeris
Dimitrios N. Serpanos 著

范九伦 王 娟 赵 锋 译
李昌华 审



科学出版社
www.sciencep.com

软件研发精品译丛

网络安全：现状与展望

Network Security
Current Status and Future Directions

Christos Douligeris
Dimitrios N. Serpanos

范九伦　王　娟　赵　锋　译

科学出版社
北京

内 容 简 介

本书由网络安全领域的知名专家编写，涵盖了有关网络安全领域最新研究进展，包括当前研究现状、面临的挑战，以及热点的研究方向和方法。全书内容分为四个主要部分：互联网安全，安全服务，移动通信与安全，以及信任、匿名和隐私。每个部分都包含若干章节，分别讲述相关领域的最新研究结果和发展趋势。为了阅读方便，本书在附录中为入门读者提供了必备的背景知识，包括密码学入门、法律、网络安全标准。

本书可作为信息安全、密码学、通信、计算机等相关专业高年级本科生、研究生的参考书，也可供网络安全研究人员和专业技术人员阅读参考。

图书在版编目(CIP)数据

网络安全：现状与展望/(美)杜里格瑞斯(Douligeris,C.)等著；范九伦，王娟，赵锋译. —北京：科学出版社，2010.8

(软件研发精品译丛)

书名原文：Network Security Current Status and Future Directions

ISBN 978-7-03-028684-0

Ⅰ.①网… Ⅱ.①杜… ②范… ③王… ④赵… 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（2010）第 161381 号

责任编辑：任 静 王志欣/责任校对：包志虹

责任印制：赵 博/封面设计：耕者设计工作室

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

新蕾印刷厂印刷

科学出版社发行 各地新华书店经销

*

2010 年 8 月第 一 版 开本：B5(720×1000)

2010 年 8 月第一次印刷 印张：33

印数：1—3 000 字数：648 000

定价：66.00 元

(如有印装质量问题，我社负责调换)

前　言

在规模日益增长的互联世界中，网络安全举足轻重。

通过对有线和无线通信系统及其协议的改善，可以获得高速度、高可用性、低成本的通信服务，这促进了高速骨干网的发展，并且为专有和公共网络的终端用户带来海量信息。如今，人们在家里就能收发实时数据，从而获得高质量的通信和全方位服务。开发、部署和管理大规模可靠网络方面的进展，不仅促成了新服务的出现，同时构建了一种能够提供广泛的消费性服务的底层网络架构。相比传统网络架构提供的服务，其价格更为低廉。所有这些网络的发展演变，尤其是互联网这一公共网络的发展，正在改变全球经济。

在公共和专有网络上大量部署的网络服务中，必然涉及包含个人数据甚至敏感数据的交易和服务。一些简单的日常业务，按次计费和有线电视电话等，都能通过电话银行、网上银行和信用卡完成支付。这类业务不仅需要高度保护交易中敏感数据的安全性，同时还必须确保网络服务的完整性和可用性。

通常，提高服务安全性和可靠性的典型做法，就是配置比公共网络更易保护的专用网。然而，互联网的出现改变了电子商务的运作模式，它能提供各种灵活简便和价格低廉的服务。为了最大限度地发挥多方面的优势，连专用网也接入了互联网。因此，在网络融合互联的大环境下，网络安全的重要性显著增强。

随着人们观念的转变，金融、市政、军事等各方面，以网络为中心的系统已经替代了传统的分布式系统，同时异构式网络和系统的使用需求日益增多，这些系统的复杂性暴露了安全方面的重大漏洞和问题。传统的网络通信中使用多层次协议方法，由于缺乏设计和实施安全终端系统的有效方法，导致了安全管理和执行方面的弱点和难点。从网络自身到操作系统，攻击者不断发现各种漏洞，并利用它们破坏系统和服务。

为了解决这些问题，研究人员致力于设计和实现安全处理系统和网络，从而部署安全服务。针对这类复杂的并且通常是异构网络及系统，基于传统的研究方法有很多种，研究人员的研究方向多元化，研究层面也各不相同。目前已有的几种安全方法包括安全协议、安全协议的实现机制、安全服务（如电话）、防火墙和入侵检测系统（IDS）等。

本书阐述了网络安全的几个方面，包括当前一些研究热点的现状、发展方向及面临的挑战。书中所给出的方法代表了当前技术的发展水平。这些方法是由该领域的权威专家描述的，包含了从互联网协议到防火墙，从移动通信系统到入侵

检测系统等多个前沿研究领域的发展趋势。

本书按照当前研究所面临的挑战和未来的发展方向，可将其分为四部分：互联网安全、安全服务、移动通信与安全，以及信任、匿名和隐私。在每个部分的一些章节中讲述了主要的研究结果和发展趋势。需要强调的是，本书还在 3 个附录中为新入门读者讲述了关键的背景知识，内容包括：密码学基础、法律、网络安全标准。对新兴的全球网络世界中网络安全的角色、约束和局限性有兴趣的读者，可以参考附录内容。

我们感谢本书评审，他们为本书提供了许多有建设性的意见，提高了本书的外观和质量。最后，感谢 IEEE 出版社的支持以及为本书最终出版所提供的优质服务。我们希望这本书能为所有对网络安全感兴趣的读者提供有价值的参考。

作　者

2007 年 3 月

目　录

第二篇　安全服务

第三篇 移动通信与安全

第四篇　信任、匿名和隐私

第一篇　互联网安全

互联网的规模不断增大，大量服务也随之涌现。然而，恶意入侵者也由此实施各种攻击，以破坏互联网基础设施的完整性，获取网络用户的隐私信息。针对互联网用户的数据通信，人们提出了大量的方法以确保数据的保密性、完整性、数据源认证、不可否认性以及可用性。在这一部分，我们将讲述网络安全的许多方面，包括可能的威胁和主动攻击及其应对方法。具体的，我们将重点讨论安全路由、防火墙、虚拟专用网（VPN）、网际协议（IP）层安全、入侵检测系统（IDS）、入侵防御系统（IPS）、拒绝服务（DoS）攻击以及主动网络的相关安全问题。

路由是指分组从源地址到达目的地址的转发过程，它是网络最重要的功能。我们将介绍能够用来获取安全路由的网络技术，同时也将描述企图扰乱分组转发服务的可能威胁。此外，我们还会介绍抵御威胁的防范措施和网络技术的保护机制，并给出二者的共同点。

防火墙是一个由组件构成的集合，用它可以实现组织策略，控制网络数据的进出。此部分将介绍网络防火墙的概念、冗余问题、性能问题及其内部部署形式（分布式防火墙、个人防火墙、第 2 层防火墙等）。

接下来，我们将讨论 VPN 技术。VPN 技术是为分布式网络实体提供安全通信的一种有效手段。具体来讲，本部分将讲述 VPN 涉及的各个方面，包括其部署、分类及配置等。同时，还将讨论 VPN 的安全机制和相关研究热点。

IPSec（IP Security）建立了一种安全方案。该方案通过互联网的基本特征实现数据的保密性、完整性、数据源认证和可用性，并被广泛部署在互联网上。我们将对 IPSec 做详细的介绍，包括它如何确保与应用和套接层的安全特征无关的 IP 分组的隐私和完整性。

此外，我们还将全面介绍作为第二层防线的 IDS 技术。这一部分的重点是基于网络的入侵检测系统（NIDS）和基于主机的 IDS 的比较。我们将给出 NIDS 的定义及历史背景，随后对其发展趋势和目前的研究热点进行讨论。接着，我们将讲述防火墙和 IDS 的集合体 IPS，并对 IDS 和 IPS 进行比较。

可用性的一个重要挑战是 DoS 攻击。DoS 攻击已成为当今互联网最主要的威胁和最难解决的安全问题。DoS 攻击的主要目的是通过限制对机器或服务的访问以干扰服务的执行。本部分将研究 DoS 攻击的问题，并给出其动机和防御方法。另外，我们还介绍了分布式 DoS 攻击，并给出著名 DDoS 工具的基本特点、

DDoS 攻击的各种类型和该攻击的各种防御机制。

主动网络是一种新的网络技术，它使得网络节点拥有编程能力，而且能实现网络内的自动寻址。这种技术导致了动态自适应网络的产生。这种网络能够提供网络服务、分布式进程和管理等的动态建立和动态执行。主动网络可用来设计两种安全机构。第一种是自适应 VPN 框架结构，该结构能够提供灵活的便携式服务，并且能在动态环境下提供符合要求的安全通道的专用 VPN 机制。第二种结构则是通过使用主动网络在 VPN 内部署安全多播。

无论是对现实中的安全问题，还是对处于研究阶段的安全问题，本书都将给予介绍。第 2 章将讨论互联网上信息的安全路由面临的问题。第 3 章讲述高效防火墙的设计技术，同时讨论其开发过程中产生的主要问题。第 4 章分析使用 VPN 的安全优势。第 5 章详细介绍 IPSec 协议在 IP 环境下如何提高安全性。第 6 章和第 7 章分析检测和保护网络免受攻击的技术。第 8 章讲述 DoS 和 DDoS 攻击。第 9 章给出一个参考框架以验证上述技术的测试平台。

1 计算机网络安全：基本背景和当前热点

Panayiotis Kotzanikolaou, Christos Douligeris

1.1 网络安全中的一些术语

本章的目的是介绍网络安全的一些基本术语，并引导读者了解整本书的其他部分。本章为不熟悉信息技术和网络安全概念的初学者提供该领域的一些基本知识。同时，还提供了一套通用的术语和定义，便于那些已经掌握网络安全基本知识的读者对后续章节有一个共同的认识。当然，已掌握网络和 IT 安全的专业读者可以跳过本章，直接进行其他章节的学习。

网络安全从广义上讲可以分为两个部分，即安全和网络。安全可能有多种定义。牛津词典中是这样解释“安全”一词的：“安全就是远离危险和恐惧”。安全还可以按照以下方式来定义：

（1）没有风险，没有威胁感的状态。

（2）风险或威胁的预防。

（3）确保信任感和确定性。

在传统的信息论里[1]，安全是通过一些基本的安全属性来定义的，即“保密性”、“完整性”和“可用性”。保密性是指保护信息内容不被信息的合法所有者以外的非授权用户知道。非授权用户通常是指所谓的未经授权的用户。还有一些术语，比如“隐私”已被人们看做是保密性的同义词。但实际上隐私一词只表现了个人的一种权利，并没有量化的定义。完整性是指保护信息免受非法用户的更改。可用性就是指保护信息免受未授权的暂时的或永久的阻断。

基本的安全属性还包括“认证”和“不可否认”。认证可分为对等实体认证和数据源认证。对等实体认证是指确认实体（也可以叫做主体）的身份。这里的实体可能是人、机器或其他资产（如软件程序）。数据源认证是指确认信息的来源。不可否认则是指确保参与者不能对其之前的行为进行否认。对安全属性的详细描述读者可以参考一些安全标准，例如 ISO/IEC（国际标准化组织/国际电工委员会）的 7498-2 安全建议[2]和 ITU-T（国际电信联盟）的 X.800 安全建议[3]。

在实际的执行过程中，IT 安全涉及信息“资产”[4]的保护。在传统的 IT 风险分析术语中，资产是“值得”保护的对象或资源。资产可以是硬件（如计算机、网络基础设施的组成部分、组装主机的配件）、数据（如电子文档、数据

库），或者是软件（如应用软件、配置文件）。对资产的保护可以通过几个安全机制来实现，即从安全威胁和漏洞出发，着眼于预防、检测或恢复。安全威胁是指任何对资产产生危害的事件。如果安全威胁得以实现，那么 IT 系统或网络将遭受安全攻击。攻击者或威胁代理是指任何实施攻击的主体或实体。威胁的影响取决于实现这一威胁可能给资产或资产所有者带来损失的程度。安全漏洞是指系统中任何使资产容易受威胁的特征。威胁、漏洞和资产的结合为威胁实现的可能和威胁实现的影响提供了一种可量化的方法。这种量化方法得到的结果就是众所周知的安全风险。因此，安全机制提供了降低系统安全风险的能力。值得注意的是，系统和网络的安全不单只依赖于安全机制的技术层面。在几乎所有的信息系统和网络中，我们常需要把规程和组织措施与技术机制相结合，以达到预期的安全目标。

计算机网络（或简称网络）是许多相互联系的计算机的集合。如果两个或两个以上的计算机系统可以通过共享的访问媒介相互发送和接收数据，那么它们就可以被看做是连接的。计算机网络中的通信实体通常被称为代理、主体或实体。这些实体可以进一步分为用户、主机和进程：

用户是指计算机网络中对其行为负责的人。

主机是指计算机网络中可寻址的实体。网络中的每个主机都有一个唯一的地址。

进程是指可执行程序的实例。它一般用于客户端-服务器模式，以区分客户和服务器上运行的不同程序。客户进程就是要求网络服务的进程；服务器进程就是提供网络服务的进程，例如一个在后台持续运行的守护进程就可以提供一种服务。

如果连接计算机之间的媒介是某种物理电缆（例如铜电缆或光纤电缆），那么该网络就被称为有线网络或固定网络。另一方面，如果访问媒介是依靠空气进行传播的某种信号（如无线电通信），那么该网络被称为无线网络。网络也可以根据其地理覆盖范围的大小分为个人区域网（PAN）、局域网（LAN）、城域网（MAN）或广域网（WAN）。

无论网络的访问媒介及覆盖范围如何，网络安全都需要实现两个安全目标，即计算机系统安全和通信安全：

（1）计算机系统安全的目标是保护信息资产免受未授权用户或恶意用户的使用，同时保护存储在计算机系统的信息免受未经授权的泄露、篡改或破坏。

（2）通信安全的目标是保护信息在通过通信媒介的传输过程中免受未经授权的泄露、篡改或破坏。

1.2 ISO/OSI 网络参考模型

为了对网络运行方式有更深层次的认识，网络参考模型应运而生。它将相近的功能进行集成，并抽象成我们所熟知的“层”。每一层都可以与其他网络主机的相同层进行通信。在同一主机上，每一层都能通过接口与其上下层进行通信。这一抽象模型简化并严格定义了必要的网络行为。

ISO 开放系统互连（OSI）参考模型[5]将网络划分为 7 层，并定义了层间接口。每一层都依靠下一层提供的服务，直到物理网络接口卡和网线。同时，每一层又为其上一层提供服务，直到正在运行的应用程序。需要指出的是，并不是所有的协议栈都包括所有 7 层。最常用的协议族——传输控制协议/网际协议（TCP/IP 协议）就只有 5 层，没有表示层和会话层。这两个层的功能已经融合到了它们的上下层。

开放系统互连参考模型的 7 层结构从上到下可简单描述如下。

第 7 层：应用层。该层负责处理应用程序的通信问题。它确定和建立了有效的通信主体，并负责实现与用户交互的接口。应用层协议的实例包括会话初始化协议（SIP）、超文本传输协议（HTTP）、文件传输协议（FTP）、简单邮件传输协议（SMTP）以及远程登录（Telnet）。

第 6 层：表示层。该层负责为其上的应用层提交数据。本质上说，它是对数据进行转化，并且完成诸如数据的压缩与解压缩、数据的加密与解密等任务。这一层的著名标准和协议包括 ASCII、ZIP、JPEG、TIFF、RTP 和 MIDI 等。

第 5 层：会话层。该层负责初始化两台电脑之间的联系并建立通信链路。它将待发送的数据进行格式化，并且维护端到端的连接。会话层协议的两个实例就是远程过程调用（RPC）和安全套接字层（SSL）协议。

第 4 层：传输层。该层定义了网络物理地址的寻址方式、主机间连接的建立方法，以及网络通信的处理方法。该层也支持端到端的完整会话，并为上一层的会话建立提供支持机制。广为人知的传输控制协议（TCP）和用户数据报协议（UDP）就部署在这一层，使用越来越广泛的串流控制传输协议（SCTP）也部署在该层。

第 3 层：网络层。该层负责网络主机之间的路由选择和数据转发。其主要功能是将数据片段，即所谓数据“包”从源主机传递到目的主机。该层也包括错误检测、信息路由选择以及流量控制的管理。网际协议（IP）属于这一层。

第 2 层：数据链路层。该层定义了一台主机访问网络所要遵守的条件。它为主机之间的连接建立物理通道。它确保信息转发到正确的设备，并为物理层转化比特流数据。部署在该层的典型协议有以太网和令牌环。