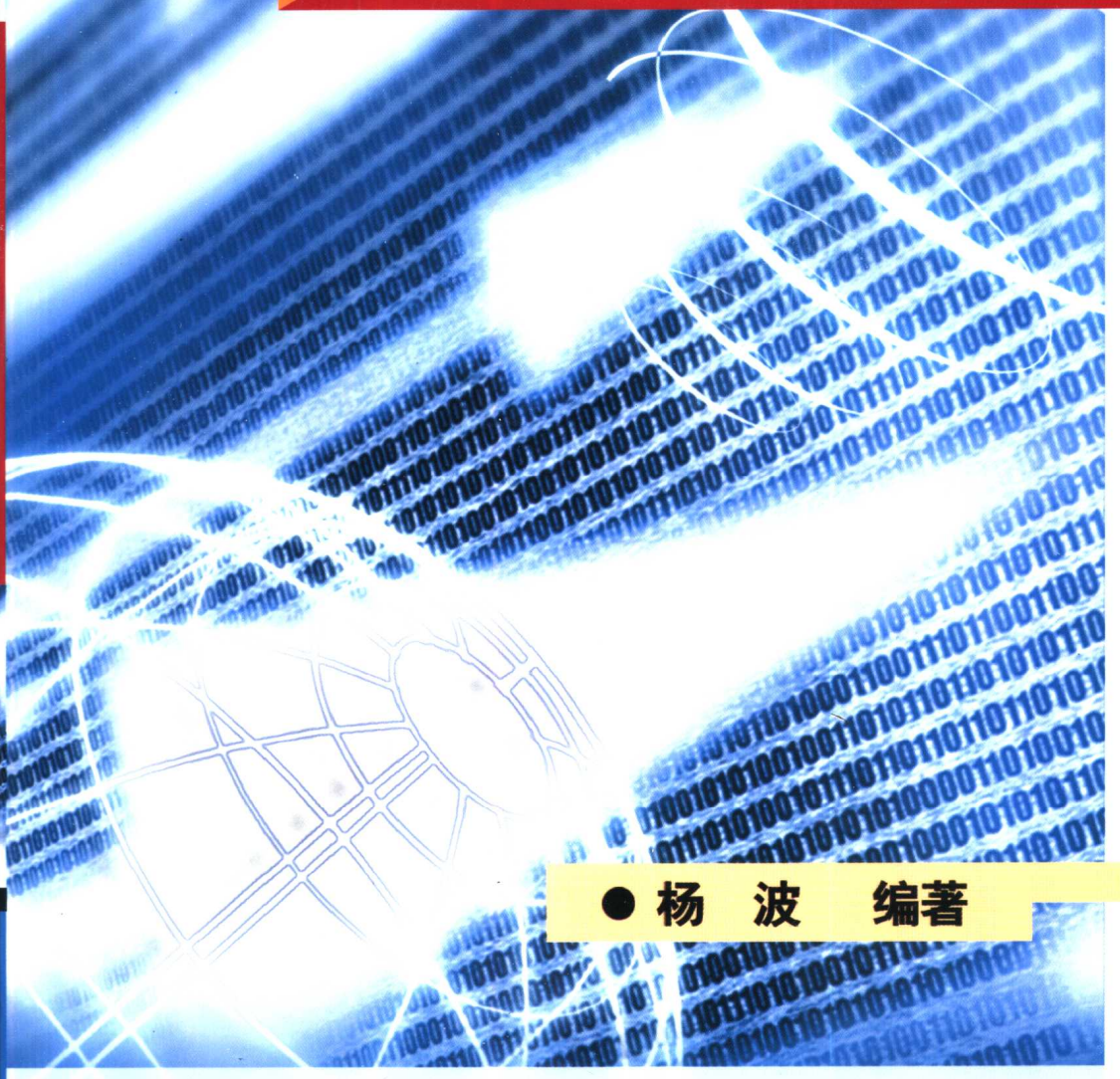
网络安全理论与应用

实用网络技术丛书



● 杨 波 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

实用网络技术丛书

网络安全理论与应用

杨 波 编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书包括两大部分，第2章到第6章为第一部分，介绍网络安全所需的密码学原理，包括加解密算法及其设计原理、网络加密与密钥管理、消息认证及杂凑函数、数字签字及认证协议。第7章到第13章为第二部分，介绍网络安全实用技术，包括Kerberos认证系统、X.509证书、PGP、S/MIME、IPSec、Web的安全性、防火墙、虚拟专用网的安全性、电子商务的安全性等。

本书可作为高等学校有关专业本科生和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

图书在版编目(CIP)数据

网络安全理论与应用/杨波编著．－北京：电子工业出版社，2002.1
(实用网络技术丛书)
ISBN 7-5053-7008-1

Ⅰ．网… Ⅱ．杨… 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(2001)第062158号

丛 书 名：实用网络技术丛书
书　　名：**网络安全理论与应用**
编 著 者：杨　波
责任编辑：竺南直
特约编辑：魏永昌
排版制作：电子工业出版社计算机排版室
印 刷 者：北京四季青印刷厂
装 订 者：河北省涿州桃园装订厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路173信箱　邮编100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：18　字数：460千字
版　　次：2002年1月第1版　2002年1月第1次印刷
书　　号：ISBN 7-5053-7008-1/TN·1468
印　　数：4 000册　　定价：26.00元

凡购买电子工业出版社的图书，如有缺页、倒页、脱页、所附磁盘或光盘有问题者，请向购买书店调换；若书店售缺，请与本社发行部联系调换。电话　68279077

前　言

随着计算机和通信技术的发展，网络已成为全球信息基础设施的主要组成部分。它为人们交换信息，促进科学、技术、文化、教育、生产的发展，对现代人类生活质量的提高都带来了深刻的影响。同时，网络作为一把双刃剑，在推动人类进步的同时，也给保障国家安全带来了极大的挑战。计算机网络犯罪事件已屡见不鲜，且呈上升趋势。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。

网络安全是一个综合、交叉的学科领域。它要利用数学、电子、信息、通信、计算机等诸多学科的长期知识积累和最新发展成果。网络安全研究的内容很多，它涉及安全体系结构、安全协议、密码理论、信息分析、安全监控、应急处理等，其中密码是网络安全的关键技术。本书分为两大部分，第一部分介绍网络安全所需的密码学原理，包括加解密算法及其设计原理、公钥密码、网络加密与密钥管理、消息认证及杂凑函数、数字签字及认证协议。第二部分介绍网络安全实用技术，包括 Kerberos 认证系统、X.509 证书、PGP、S/MIME、IPSec、Web 的安全性、防火墙、虚拟专用网的安全性、电子商务的安全性等。

本书在编写过程中，得到了西安电子科技大学通信工程学院裴昌幸教授、电子工业出版社竺南直博士的大力支持，张彤博士、毛剑博士为本书提供了部分资料，秦兴成硕士、苏晓龙硕士、李勇硕士、华翔硕士为本书的输入做了大量的工作，作者对他们表示感谢。同时还感谢国家自然科学基金对本书的资助。

编著者

2001 年 6 月

目　录

第1章 引 言

- 网络安全面临的威胁
- 网络入侵者和病毒
- 网络安全的模型

1.1　网络安全面临的威胁

1.1.1　安全威胁

Internet 为人类交换信息，促进科学、技术、文化、教育、生产的发展，提高现代人的生活质量提供了极大的便利，但同时对国家、单位和个人的信息安全带来了极大的威胁。由于因特网的全球性、开放性、无缝连通性、共享性、动态性发展，使得任何人都可以自由地接入 Internet，其中有善者，也有恶者。恶者会采用各种攻击手段进行破坏活动。网络安全面临的攻击有独立的犯罪者、有组织的犯罪集团和国家情报机构。对网络的攻击具有以下新特点：无边界性、突发性、蔓延性和隐蔽性。因此我们考虑网络安全，就要首先知道网络安全面临有哪些威胁。

网络安全所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。

自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。这些无目的的事件，有时会直接威胁网络的安全，影响信息的存储媒体。

我们主要讨论人为威胁，也就是说对网络的人为攻击。这些攻击手段都是通过寻找系统的弱点，以便达到破坏、欺骗、窃取数据等目的，造成经济上和政治上不可估量的损失。

图 1.1（a）表示网络中两个计算机系统之间的正常信息流，图 1.1（b）至（e）说明以下四类基本的攻击类型。

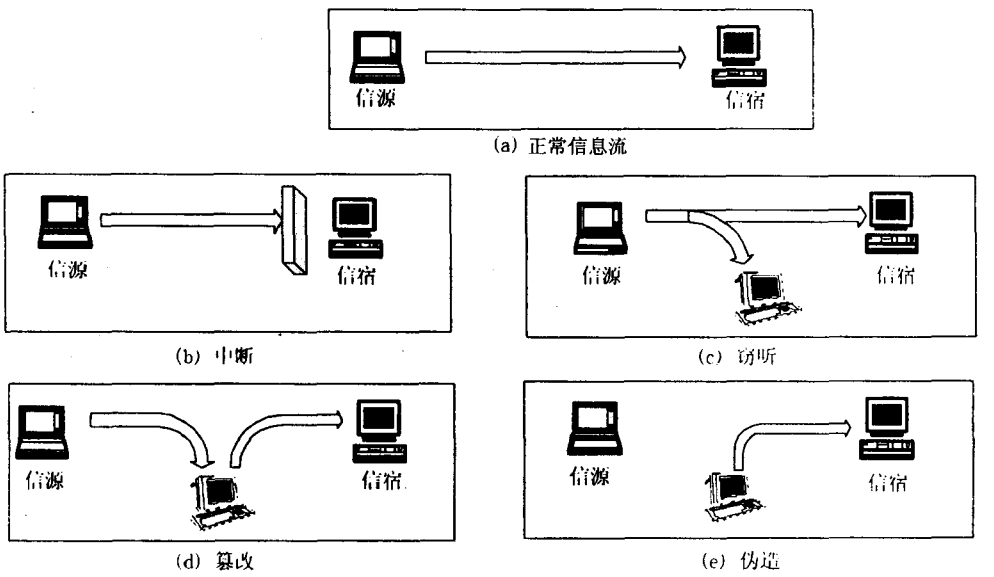


图 1.1　攻击类型示意图

① 中断：是对系统的可用性进行攻击，如破坏计算机硬件、线路或文件管理系统。

② 窃听：是对系统的保密性进行攻击，如搭线窃听、对文件或程序的非法拷贝。

③ 篡改：是对系统的完整性进行攻击，如修改数据文件中的数据、替换某一程序使其执行不同的功能、修改网络中传送的消息内容。

④ 伪造：是对系统的真实性进行攻击。如在网络中插入伪造的消息或在文件中插入伪造的记录。

攻击类型又可分为被动攻击和主动攻击，如图 1.2 所示。

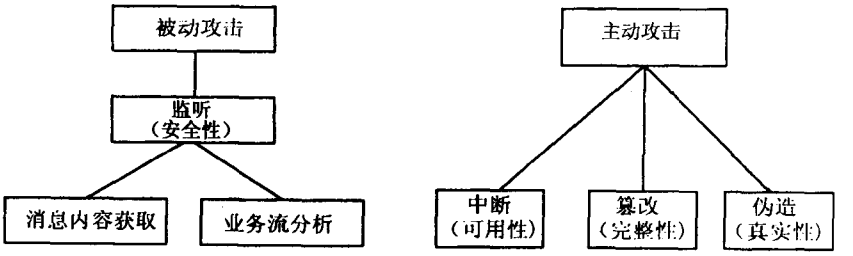


图 1.2 被动攻击和主动攻击

1. 被动攻击

被动攻击相应于攻击类型中的窃听，敌手的目标是窃取传输中的信息。被动攻击又分为两类，一类是获取消息的内容，很容易理解；第二类是进行业务流分析，假如我们通过某种手段，比如加密，使得敌手从截获的消息无法得到消息的真实内容，然而敌手却有可能获得消息的格式、确定通信双方的位置和身份以及通信的次数和消息的长度，这些信息可能对通信双方来说是敏感的，例如公司间的合作关系可能是保密的、电子函件用户可能不想让他人知道自己正在和谁通信、电子现金的支付者可能不想让别人知道自己正在消费、Web 浏览器用户也可能不愿意让别人知道自己正在浏览哪一站点。

被动攻击因不对传输的消息做任何修改，因而是难以检测的，所以抗击这种攻击的重点在于预防而非检测。

2. 主动攻击

这种攻击包括对数据流的某些篡改或产生某些假的数据流。主动攻击又可分为以下四个子类。

① 假冒：某个实体（人或者系统）假装成另外一个实体，以使某一防线的守卫者相信它是一个合法的实体，此后便可僭取合法用户的权利和特权。这是侵入安全防线最为常用的方法。

② 重放：攻击者对截获的某次合法数据进行拷贝，以后出于非法的目的而重新发送。

③ 消息的篡改：指某一通信数据在传输过程中被改变、删除或替代，如“允许甲读账目文件”改为“允许乙读账目文件”。

④ 业务拒绝：对通信设备的使用和管理被无条件地拒绝。这种攻击可能有一个特定的目标，例如某个实体对到某一特定终端的所有消息都予以阻止。还有一类业务拒绝是对整个网络实施破坏，例如使网络瘫痪或用大量无用信息使其资源耗尽。

绝对防止主动攻击是十分困难的，因为需要随时随地对通信设备和通信线路进行物理保护，因此抗击主动攻击的主要途径是检测，以及对此攻击造成的破坏进行恢复。

1.1.2 安全业务

在网络通信中，主要的安全防护措施称作安全业务，有以下 5 种。

① 保密业务：保护数据以防被动攻击。保护方式可根据保护范围的大小分为若干级，其中最高级保护可在一定时间范围内保护两个用户之间传输的所有数据，低级保护包括对单个消息的保护或对一个消息中某个特定域的保护。保密业务还有对业务流实施保密，防止敌手进行业务流分析以获得通信的信源、信宿、次数、消息长度和其他信息。

② 认证业务：用于保证通信的真实性。在单向通信的情况下，认证业务的功能是使接收者相信消息确实是由它自己所声称的那个信源发出的。在双向通信的情况下，如计算机终端和主机的连接，在连接开始时，认证服务则使通信双方都相信对方是真实的（即的确是它所声称的实体）；其次，认证业务还保证通信双方的通信连接不能被第三方介入，以假冒其中的一方而进行非授权的传输或接收。

③ 完整性业务：完整性业务和保密业务一样，也能应用于消息流、单个消息或一个消息的某一选定域。用于消息流的完整性业务目的在于保证所接收的消息未经复制、插入、篡改、重排或重放，因而是和所发出的消息完全一样的；这种服务还能对已毁坏的数据进行恢复，所以这种业务主要是针对对消息流的篡改和业务拒绝的。应用于单个消息或一个消息某一选定域的完整性业务仅用来防止对消息的篡改。

④ 不可否认业务：用于防止通信双方中的某一方对所传输消息的否认，因此，一个消息发出后，接收者能够证明这一消息的确是由通信的另一方发出的。类似地，当一个消息被接收后，发出者能够证明这一消息的确已被通信的另一方接收了。

⑤ 访问控制：访问控制的目标是防止对网络资源的非授权访问，控制的实现方式是认证，即检查欲访问某一资源的用户是否具有访问权。

1.2 网络入侵者和病毒

网络安全的人为威胁主要来自用户（恶意的或无恶意的）和恶意软件的非法侵入，入侵网络的用户也称为黑客，黑客可能是某个无恶意的人，其目的仅仅是以破译和进入一个计算机系统为满足，或者是某个心怀不满的雇员，其目的是对计算机系统实施破坏，也可能是一个犯罪分子，其目的是非法窃取系统资源（如窃取信用卡号或非法资金传送），对数据进行未授权的修改或破坏计算机系统。

恶意软件是病毒、蠕虫等恶意程序，分为两类，如图 1.3 所示，一类需要主程序，另一类不需要。前者是某个程序中的一段，不能独立于实际的应用程序或系统程序；后者是能被操作系统调度和运行的独立程序。

对恶意软件也可根据其能否自我复制来进行分类。不能自我复制的是程序段，这种程序段在主程序被调用执行时就可激活；能够自我复制的或者是程序段（病毒）或者是独立的程序（蠕虫、细菌等），当这种程序段或独立的程序被执行时，可能复制一个或多个自己的副本，以后这些副本可在这一系统或其他系统中被激活。以上仅是大致分类，因为逻辑炸弹或特洛伊木马可能是病毒或蠕虫的一部分。下面对恶意程序作一简单介绍。

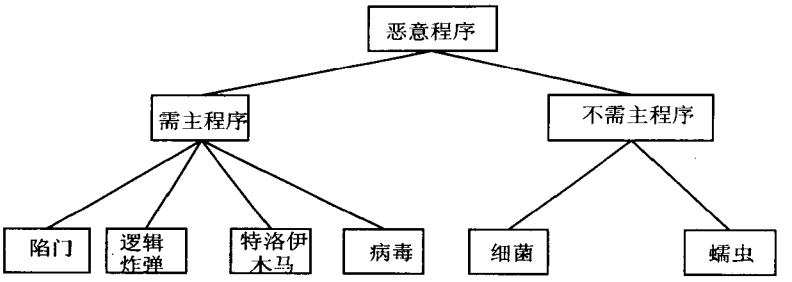


图 1.3 恶意程序分类

1. 陷门

陷门是进入程序的秘密入口，掌握陷门的人可不经过通常的安全访问程序而访问该程序。陷门通常是由程序员调试程序时合法使用的，程序员在调试具有认证功能且设置很长的应用程序时，也许希望有特别的权限或避免所有必要的设置和认证，因此希望有一种激活程序的方法。陷门是识别某些特定输入序列的码或通过运行某个特定用户 ID 或一个不可能事件序列能激活的码。

陷门一旦被原来的程序员利用，或者被无意或有意的人发现将会带来严重的安全后果。比如，可能利用陷门在程序中建立隐蔽通道，甚至植入一些隐蔽的恶意程序。非法利用陷门可以使原来相互隔离的网络信息形成某种潜在的关联，进而可以非法访问网络，达到窃取、篡改、伪造和破坏信息等目的，甚至造成网络的大面积瘫痪。

2. 逻辑炸弹

逻辑炸弹是早于病毒和蠕虫出现的最早的恶意程序之一，它是镶嵌于合法程序并且设置了“爆炸”条件的代码。一旦满足设置的条件（例如某个特定文件的存在或缺省、某个特定的日期、运行应用程序的某个特定的用户等），逻辑炸弹可能会修改或删除数据甚至整个文件，造成死机甚至网络瘫痪。

3. 特洛伊木马

特洛伊木马是包含在有用程序中的隐藏码，当有用程序被调用时，这种隐藏码将执行某些有害功能。

特洛伊木马能用于间接实现非授权用户不能直接实现的功能，例如一用户欲访问共享系统中另一用户的文件，他可建立一个特洛伊木马程序，该程序执行时能修改被访问用户文件的访问许可权限，使得任一用户都能读这一文件。特洛伊木马一般难于被发现，例如编译程序中的特洛伊木马程序，可在编译某个程序（如系统登录程序）时在其中插入附加的码，这个码在登录程序中就建立了一个陷门以便特洛伊木马的作者使用某个特定的口令登录系统。这种特洛伊木马程序无法通过读登录程序的源代码而被发现。

特洛伊木马另一个常见的目的是毁坏数据。含有特洛伊木马程序的有用程序在执行某个有用功能时，其中的特洛伊木马也许正在悄悄地删除用户的文件。

4. 病毒

病毒是一个程序，它能通过修改其他程序而将其感染。其中修改过程包括病毒程序本身的复制，复制得到的副本又可继续感染其他程序。

生物病毒是遗传代码 DNA 或 RNA 的一个片段。它能进入并欺骗生物细胞，从而由生

物细胞为其复制成千上万个副本。与生物病毒类似，计算机病毒也可被复制。驻留在机器中的病毒可暂时控制计算机的磁盘操作系统，被感染的计算机一旦与其他软件接触，病毒将给这一软件复制自己的一个新副本。因此病毒的感染可通过用户之间交换磁盘或在网络中发送程序而得以蔓延。

5. 蠕虫

网络中的蠕虫程序通过网络连接关系从一个系统蔓延到另一系统。系统中，网络蠕虫一旦被激活，其行为或者与病毒或细菌一样、或者在网络中植入特洛伊木马程序、或者直接进行破坏活动。

为了复制自己，网络蠕虫需利用某种网络载体，例如：

① 电子邮件：网络蠕虫可通过电子邮件将自己复制到其他系统。

② 远程执行能力：蠕虫可将自己复制到另一系统。

③ 远程登录能力：蠕虫可像用户一样登录到某个远程系统，然后又将自己从这一系统复制到另一系统。

和计算机病毒一样，网络蠕虫也有以下四个阶段：潜伏阶段、传播阶段、激活阶段和执行阶段。传播阶段一般有以下方式：

① 检查主表或类似的远程系统地址库，以搜索并感染其他系统。

② 建立和远程系统的连接。

③ 将自己复制到远程系统并引起副本运行。

网络蠕虫在将自己复制到某个系统时，也可能检查这个系统以前是否已被感染。在多道程序系统中，蠕虫可能会将自己伪装成一个系统程序或使用某些不被系统操作员注意的其他名称。

6. 细菌

细菌是不明显危害其他文件的程序，它们的惟一目的是复制自己。一个典型的细菌程序在多道程序系统中可能仅同时建立自己的两个副本，或者建立两个新文件，每个新文件都是细菌程序最初源文件的副本，而每个副本又继续建立两个新的副本。如此下去，细菌数目指数地增长，最终占据所有处理器、存储器或磁盘空间，拒绝用户对这些资源的访问。

1.3　网络安全的模型

图 1.4 表示网络安全的基本模型。

通信双方欲传递某个消息，需通过以下方式建立一个逻辑上的信息通道，首先在网络中定义从发方到收方的一个路由，然后在该路由上共同执行通信协议。

如果需要保护所传信息以防敌手对其保密性、认证性等构成的威胁，则需要考虑通信的安全性。安全传输技术有以下两个基本成分。

① 消息的安全传输：包括对消息的加密和认证。加密的目的是将消息搞乱以使敌手无法读懂，认证的目的是检查发送者的身分。

② 通信双方共享的某些秘密信息，如加密密钥。

为获得消息的安全传输，可能还需要一个可信的第三方，其作用可能是负责向通信双方分布秘密信息或者在通信双方有争议时进行仲裁。