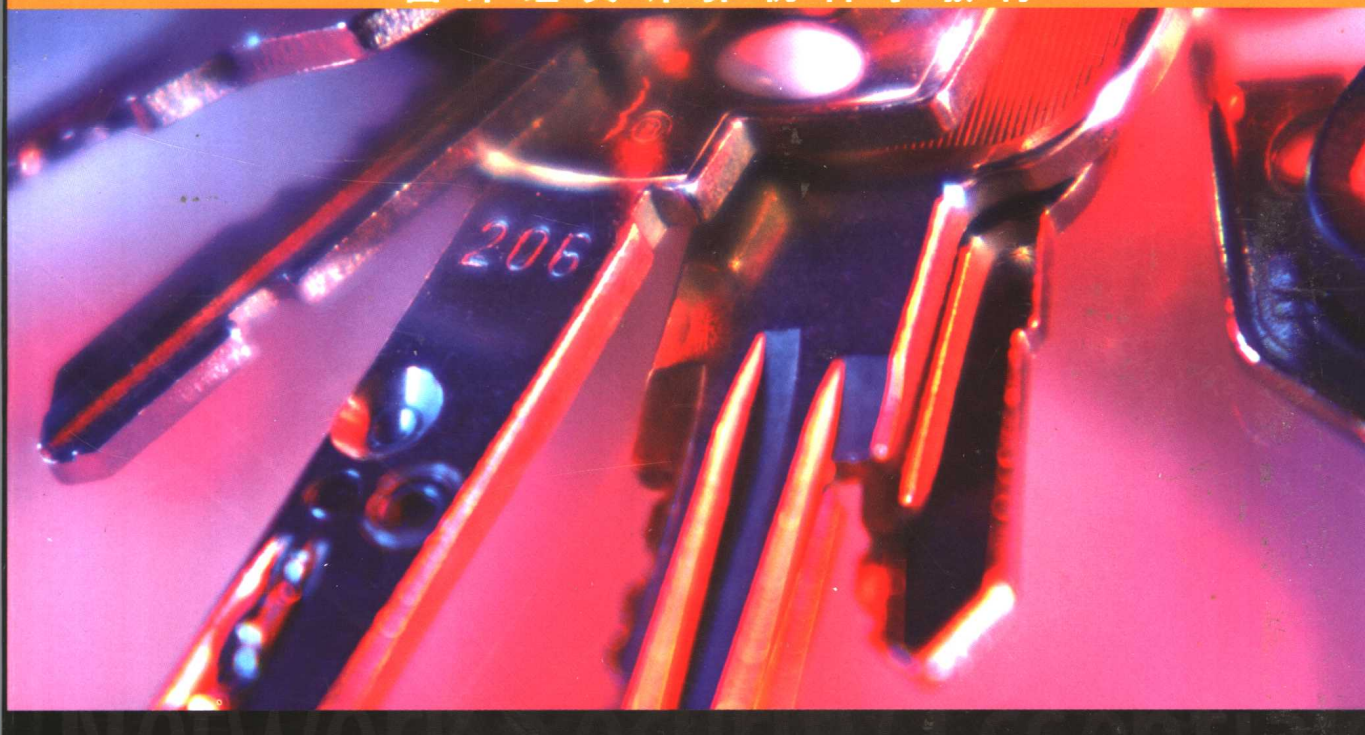
国外经典计算机科学教材



Network Security Essentials
Applications and Standards

网络安全基础
应用与标准
（第二版）

[美] William Stallings 著
张 英 王景新 译

PEARSON Prentice Hall
中国电力出版社
www.infopower.com.cn

国外经典计算机科学教材

Network Security Essentials
Applications and Standards

网络安全基础
应用与标准
（第二版）

[美] William Stallings 著
张 英 王景新 译

中国电力出版社
www.infopower.com.cn

Network Security Essentials: Application and Standards, 2e (ISBN 0-13-035128-8)
William Stallings

北京市版权局著作权合同登记号 图字：01-2004-1299 号

图书在版编目（CIP）数据
网络安全基础 /（美）斯特林 （Stallings, W.）著；张英，王景新译. —北京：中国电力出版社，2004
（国外经典计算机科学教材系列）
ISBN 7-5083-2269-X
Ⅰ.网... Ⅱ.①斯...②张...③王... 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（2004）第 041954 号

丛 书 名：国外经典计算机科学教材系列
书　　名：网络安全基础
编　　著：（美）William Stallings
翻　　译：张英　王景新
责任编辑：牛贵华
出版发行：中国电力出版社
　　地址：北京市三里河路6号　　邮政编码：100044
　　电话：（010）88515918　　传　　真：（010）88518169
印　　刷：北京丰源印刷厂
开　　本：787×1092　1/16　　印　　张：20.5　　字　　数：462 千字
书　　号：ISBN 7-5083-2269-X
版　　次：2004 年 6 月北京第 1 版　　2004 年 6 月第 1 次印刷
定　　价：32.00 元

译 者 序

网络的发展在给人们的生活带来巨大便利的同时也带来了巨大的安全隐患，出于政治的、经济的、文化的、商业利益的需要以及好奇心的驱动，网络上的安全事件层出不穷，且有愈演愈烈之势。尤其近几年来，各种新型病毒、垃圾邮件、黑客攻击事件的发生频率急剧上升，所造成的危害也越来越大。网络被攻陷意味着机密数据的丢失和损坏，小而言之将给个人或公司带来经济利益上的损失，大而言之将影响一个国家的政治、经济和文化安全，因此，各个国家都普遍重视对网络安全问题的研究，以期在日益走到前台的信息战中占据优势地位，保护好自己的信息防线。

本书的原作者是一位在网络安全领域有较大影响的著名学者和安全技术专家，这本书是他的最新力作。我们翻译本书的主要目的是想为国内读者提供一本较为完备的网络安全参考书籍，为计算机和通信专业以及一切对网络安全问题感兴趣的大学生朋友提供一本内容全面丰富、讲解细致到位、深度恰如其分的网络安全教科书。此外，本书在写作时特别注意吸收当前最新的信息安全领域研究成果，因此本书对致力于在安全领域进行深入研究的研究生和专业安全人士也有一定的参考价值。

本书的最大特点是内容全面而实用，包括了密码学、电子邮件安全、IPSec 协议、Web 安全、网络管理与安全、入侵检测、恶意软件、防火墙等内容，这些技术基本涵盖了网络安全的所有内容。通过阅读本书，读者可以较快地对网络安全有一个整体的清晰概念，并可以将其中的很多概念和技术直接应用到构建安全网络系统的实际工作之中。此外，本书还提供了丰富的资源链接，通过这些网上资源，有兴趣的读者可以进一步加深对网络安全的学习和理解。

在本书的翻译过程中，我们本着对读者认真负责的精神，力求做到技术内涵的准确无误和专业术语的规范统一，力求做到翻译的准确性和灵活性的有效结合。

本书由张英、王景新组织翻译。参与本书翻译的还有宋新、肖和平、张杰良、杨定新、汪东和于大东等，全书最后由张英统稿。**Be Flying 工作室**负责人肖国尊负责本书翻译质量和进度的控制。由于我们的水平有限，错误与不到位之处在所难免。敬请广大读者提供反馈意见，读者可以将意见 e-mail 至 be-flying@sohu.com，我们会仔细对待读者的每一封邮件，以求进一步提高今后译作的质量。

译 者

前 言

“假如让我来表述的话，结是一个连接更为紧密的东西。我们致力于完美的蝴蝶效应。如果你允许我的话——”

“在这样的一个时刻，Jeeves，这又有什么关系呢？你有没有意识到，Little 先生自己的幸福正在按比例停止？”

“不再会有结不再重要的时刻了，先生。”

——P. G. Wodehouse，选自《Very Good, Jeeves!》

在这样一个充满全球电子互连，充满病毒和电脑黑客，充满电子窃听和电子犯罪的时代里，安全已经成为非常重要的问题。有两个趋势一起导致本书对这个主题进行了详细论述。第一，计算机系统和网络互连的蓬勃发展，已经在信息存储和利用系统通信方面，提高了组织和个体之间的依赖性。这样会使人们更加强烈地意识到需要保护数据和资源免受泄漏，需要保证数据和信息的认证以及需要保护系统免于受到基于网络的袭击。第二，密码学和网络安全技术已经成熟，从而开发出了实际而有效的应用程序来确保网络的安全。

目标

本书的目标是为网络安全的应用和标准提供一个实用的综述。重点放在 Internet 和公司网络中广泛使用的应用以及已经广泛采用的标准，尤其是 Internet 标准。

本书面向的读者

本书适合于科研人员和专业人士阅读。如果用作教科书，则对于计算机科学、计算机工程和电子工程专业本科生来说，本书可以作为一个学期的网络安全课程。本书也可以用作基本参考书，并且适合于自学。

本书的组织

本书按照以下三部分进行组织：

第一部分“密码学”：简要地叙述了密码学算法以及基于网络安全应用的协议，包括加密、hash 函数、数字签名和密钥交换。

第二部分“网络安全应用”：讲述了重要的网络安全工具和应用，包括 Kerberos、X.509v3 鉴定、PGP、S/MIME、IP 安全、SSL/TLS、SET 和 SNMPv3。

第三部分“系统安全”：关注系统级的安全问题，包括计算机入侵者和病毒的威胁和对策，

以及防火墙和可信系统（trusted system）的使用。

此外，本书还包含了一个比较全面的术语表、一个经常使用的缩略语表和参考书目。每一章都含有家庭作业、复习题、关键术语列表，以及用于深入学习的读物和网址。

更为详细的逐章概括将在每部分的开始给出。

为教师和学生提供的 Internet 服务

本书有一个网页用来提供对学生和教师的支持。该网页包括相关网址的链接、本书 PDF（Adobe Acrobat）格式文档中的图表的幻灯片和本书的 Internet 邮递列表的签约信息。该网页地址是 WilliamStallings.com/NetSec2e.html。该网页已经建立起了 Internet 邮递列表，这样使用本书的教师之间或者教师与作者之间就可以交换信息、建议和问题了。一旦发现排印错误或者其他的错误，将会在 WilliamStallings.com 上为本书列出一张勘误表。此外，位于 WilliamStallings.com/StudentSupport.html 的计算机科学的学生资源站点，可以为计算机科学的学生和专业人员提供文档、信息和有用的链接。

用于教授网络安全的方案

对于很多教师来说，密码学或者安全课程的一个重要构成就是教学方案或者方案的设计，这样学生就可以获得内行的经验以加强对教材中概念的理解。本书对该课程的方案组成部分提供了非常好的支持。教师的手册不仅包括如何分配和构建方案的指导，还包括一个广泛包含本书中主题的建议方案：

- **研究方案**：一系列的研究作业，用于指导学生研究 Internet 的一个特定的主题并且写一篇报告
- **编程方案**：一系列的编程项目，它们覆盖的主题范围广泛并且能够在任何平台上用任何语言来实现
- **阅读/报告作业**：为每一章列出一张文献列表，分配给学生阅读并且让他们写出一个简短的报告。

参见附录 B 以获得更详细的信息。

与《Cryptography and Network Security，Third Edition》的关系

本书是《*Cryptography and Network Security, Third Edition*》（CNS3e）的一个派生作品。CNS3e 详细地讲述了密码学，包括对算法和重要数学部分的详细分析，这些内容将近有 400 页。与此相反，本书（NSE2e）只在第 2 章和第 3 章对这些主题提供了简要的叙述。NSE2e 包括了所有 CNS3e 除算法和数学分析以外的其余材料。NSE2e 还包括了 SNMP 安全，而在 CNS3e 中却没有涉及这方面的内容。因此，NSE2e 适于作为大学课程，也适合专业读者阅读，因为他们多数只是关心网络安全的应用，而不需要深入了解密码学的理论和原理。

目　录

第二部分 网络安全应用

第三部分 系统安全

第1章 引 言

空间、时间和力量必须被视为这种防御理论的基本元素，而这三者的结合使得防御问题成为一个相当复杂的问题。因此，去发现一个固定的出发点会十分困难。

——Carl Von Clausewitz，选自《On War》

故用兵之法，无恃其不来，恃吾有以待之；无恃其不攻，恃吾有所不可攻也。

——孙子，选自《孙子兵法》

在过去的几十年里，组织机构内部的**信息安全（information security）**需求经历了两个主要的变化。在广泛使用数据处理设备之前，对于机构有意义的信息安全主要是通过物理和行政管理的方式来实现的。前者的一个例子就是使用带有暗码锁的结实的文件柜来保存敏感文档。后者的一个例子就是在雇用人员的过程中采用人员筛选的办法。

随着计算机的引入，人们需要对于保存在计算机上的文件和其他信息采用自动工具进行保护。这对于共享系统来说尤其重要，例如分时系统（time-sharing system），并且对于能够通过公共电话网络、数据网络或者 Internet 访问的系统来说，这种需求变得更加迫切。那些用于保护数据和阻止电脑黑客的工具统称为**计算机安全（computer security）**。

影响安全的第二个主要变化就是分布式系统（distributed system）的引入、网络的使用和在终端用户与计算机以及计算机与计算机之间用于传送数据的通信设施的使用。于是，需要在数据的传送期间采取安全措施来保护这些数据。事实上，术语**网络安全（network security）**在某种程度上存在着误导，因为实际上，所有的企业、政府和学术研究组织都要通过互连的网络集合来互连数据处理设备。这样的集合通常称为 internet[①]，并且使用术语 **internet 安全（internet security）**。

在这两种形式的安全之间没有清晰的界限。例如，在信息系统上最常见的攻击类型就是计算机病毒。病毒可以物理地引进系统，也就是当病毒到达磁盘后再加载到计算机中。病毒还可以通过网络引入。在任何情况下，一旦病毒入驻计算机系统，就需要内部的计算机安全工具来发现病毒并恢复系统。

本书集中论述 internet 安全，它所包含的措施可以用于阻止（deter）、预防（prevent）、检测（detect）和纠正（correct）与信息交互有关的安全侵犯（security violation）。这里对 internet 安全进行的是宽泛的叙述，包括了多种可能性。为了让读者对本书所覆盖的领域有一个概要的

① 我们使用具有小写字母 i 的术语 internet 来表示任何网络的互连集合。公司的 intranet 就是 internet 的一个例子。具有大写字母 I 的 Internet 可能就是某个组织用来创建它的 internet 的设施之一。

了解，考虑下列安全侵犯的实例：

（1）用户 A 向用户 B 传送一个文件。该文件包含需要保护以免泄漏的敏感信息（如工资单记录）。并没有获得授权来读取该文件的用户 C 能够监控该文件的传送，并且能够在传送的过程中获得文件的副本。

（2）网络管理员 D 在自己的管理下向计算机 E 发送消息。该消息指示计算机 E 更新授权文件，使它包含一些能够访问该计算机的新用户。用户 F 截取该消息，增加或者删除了一些项从而改变了消息的内容，然后将更改后的消息发送给 E，计算机 E 会认为该消息是来自管理员 D 的消息并且对授权文件进行相应的更新。

（3）用户 F 不是截取消息，而是创建一条具有他所期望的项的消息，并且把这条消息传送到 E，仿佛该消息来自于管理员 D。计算机 E 会认为该消息就是来自管理员 D 的消息，并且对授权文件进行相应的更新。

（4）在没有发出任何警告的情况下解雇某个雇员。人事管理员向服务器系统发送一条消息以注销该雇员的账户。在注销完成的时候，服务器就会向雇员的文件发送一个通知以确认该动作。该雇员能够截取这条消息，并且延迟该消息足够长的时间以访问服务器并取回敏感信息。这个雇员然后转发该消息，采取行动并且发出确认。可能在相当长的一段时间里都不会有人注意到该雇员的行为。

（5）客户向股票经纪人发送一条包含各种交易指示的消息。随后，股价下跌，客户否认曾经发送过该消息。

尽管这个列表不可能穷举安全侵犯的所有可能类型，但是它说明了网络安全内容的范围。

互联网络的安全既引人注意又极为复杂。下面列举了一些原因：

（1）与通信和网络有关的安全并不像初学者所见到的那么简单。需求看起来很直接；的确，安全服务中的大部分主要需求都能够使用含义明显的词来表示：机密性（confidentiality）、认证（authentication）、非否认（nonrepudiation）和完整性（integrity）。但是，用来满足这些需求的机制却是相当复杂的，而且理解这些机制将会涉及非常深奥的理论。

（2）在开发某种特定的安全机制或算法的时候，必须始终要考虑针对这些安全功能所存在的潜在攻击。在很多情况下，通过以完全不同的方式来观察问题，可以设计成功的攻击，以便发掘在该机制中所存在的意外的弱点。

（3）由于第（2）点的原因，用于提供特定服务的过程通常都不能依照直觉进行：不能明显地从特定需求的叙述中获得所需的精确技术。只有在考虑了各种对策之后，所采用的策略才有意义。

（4）人们已经设计了各种各样的安全机制，因此十分有必要确定这些安全机制的适用场合。无论是从物理安置（例如，某些安全机制需要用于网络的哪个位置上）的角度还是从逻辑[例如，安全机制应该在体系结构的哪个或者哪些层上实现，比如 TCP/IP（传输控制协议/网络协议）层]的角度来看，都需要确定安全机制的适用场合。

（5）安全机制通常涉及不止一种具体算法或协议。安全机制通常还要求参与者拥有一些机密的信息（例如密钥），这就会引入机密信息的产生、分配和保护问题。同样也存在对通信

协议的依赖，这些协议的行为会使得安全机制的开发复杂化。例如，如果安全机制的正确功能需要对消息从发送者到达接收者的时间设置限制，那么任何引入各种无法预知的延迟的协议或者网络都可能使得该时间限制变得没有意义。

因此，互联网络的安全需要考虑的问题很多。本章对构建本书剩余部分内容的主题提供一个总的概述。我们首先概要地论述网络安全服务和机制以及存在的攻击类型。然后，开发一个通用而全面的模型，在模型里面我们可以见到安全服务和机制。

1.1 OSI 安全体系结构

为了能够有效地获得某机构的安全需求并且评价和选择各种安全产品及策略，负责安全的管理员需要一些系统的方法来定义安全需求和描述满足这些需求的方法。在集中的数据处理环境下，这项工作是相当困难的；由于局域和广域网络的使用，这个问题变得更加复杂。

ITU-T[②]推荐标准 X.800，即 OSI 安全体系结构（Security Architecture for OSI），定义了这样的系统方法。对于管理员来说，OSI 安全体系结构用于组织提供安全的任务是有用的。此外，由于这种体系结构是作为国际标准来开发的，所以，计算机和通信厂商都在为他们的产品和服务开发与这种结构化服务和机制的定义有关的安全特性。

对于我们来说，OSI 安全体系结构对本书中所涉及的一些概念提供了有用的、或许有些抽象的概述。OSI 安全体系结构集中于安全袭击、机制和服务。它们可以简要地定义如下：

表 1-1 威胁和攻击（RFC 2828）

威胁 指潜在的安全侵犯，当具有能够破坏安全和造成损害的环境、能力、行为或事件的时候就存在着威胁。也就是说，威胁就是能够产生攻击的可能危险。
攻击 指对系统安全的攻击，它起源于明智的威胁；也就是说，一种明智的行为，致力于（尤其是从方法和技术的角度来说）避开安全服务并且侵犯系统的安全策略。

- **安全攻击（security attack）**：损害机构所拥有信息的安全的任何行为。
- **安全机制（security mechanism）**：设计用于检测、预防安全攻击或者恢复系统的机制。
- **安全服务（security service）**：用于提高机构的数据处理系统安全和信息传输安全的服务。这些服务致力于抵御安全攻击，并且它们采用一种或者多种安全机制来提供服务。

在文献中，术语“威胁（threat）”和“攻击（attack）”通常或多或少地用于表示同一件事情。表 1-1 提供的定义来自于 RFC 2828，《*Internet Security Glossary*》。

② 国际电信同盟（ITU）电信标准部（ITU-T）是一个由联合国发起的机构，它开发的标准称为推荐标准，与电信和开放系统互联（OSI）有关。

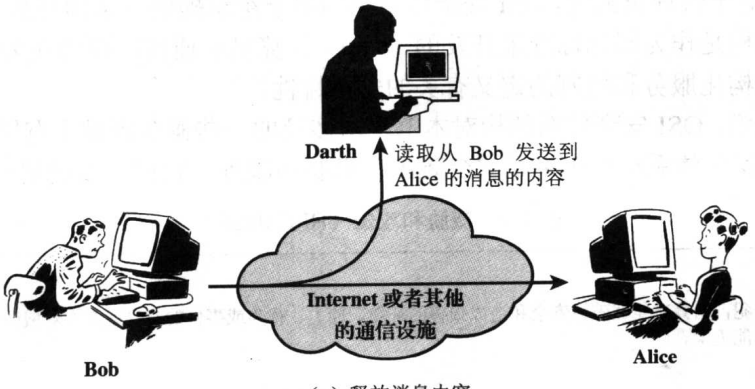
1.2 安全攻击

用于对安全攻击分类的一个有用的方式就是使用术语被动攻击（passive attack）和主动攻击（active attack），在 X.800 和 RFC2828 中都采用了这种分类方法。被动攻击试图学习或者使用来自系统的信息，但并不影响系统的资源。主动攻击试图改变系统的资源或者影响系统的操作。

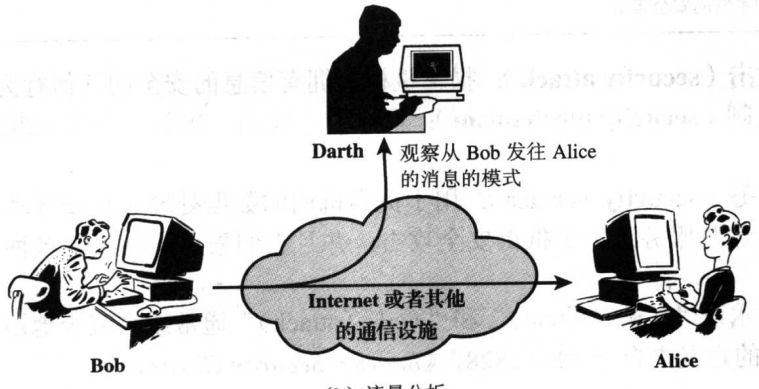
1.2.1 被动攻击

被动攻击具有偷听或者监控传输的性质。对手的目的就是获得正在传输的信息。被动攻击的两种类型是释放消息内容和流量分析。

释放消息内容（release of massage contents）很容易理解（如图 1-1a 所示）。电话会谈、电子邮件消息和传输的文件都可能包含敏感或者机密信息。我们应该防止对手了解到这些传输信息的内容。



（a）释放消息内容



（b）流量分析

图 1-1 被动攻击

流量分析（traffic analysis）是第二种类型的被动攻击，这种攻击更加巧妙（如图 1-1b 所示）。假定我们有办法屏蔽消息或者其他信息流的内容，这样对于对手来说，即使他们获得了消息也不能从中提取出信息。屏蔽内容的常见技术就是加密。如果我们采用了密码保护，那么对手仍然能够观察消息的模式。对手能够确定通信主机的地址和身份，并且能够观察到正在交互的消息的频率和长度。这些信息可以用于猜测正在发生的通信的本质。

被动攻击是很难检测到的，因为这种攻击并不对数据作任何更改。通常来说，消息流的发送和接收都是以透明的方式进行的，无论是发送方还是接收方都没有意识到第三方的存在，也没有意识到第三方已经读取了消息或者观察了流量的模式。然而，我们仍旧可以预防对手进行成功的攻击，这通常是通过采用加密的方法来实现的。因此，处理被动攻击的重点就是预防而不是检测。

1.2.2 主动攻击

主动攻击与对数据流作出一些更改或者伪造假的数据流有关，主动攻击可以分为四类：伪装（masquerade）、重放（replay）、更改消息内容（modification of messages）和拒绝服务（denial of service）。

伪装发生于一个实体假装成为另一个不同的实体的场合（如图 1-2a 所示）。伪装攻击通常

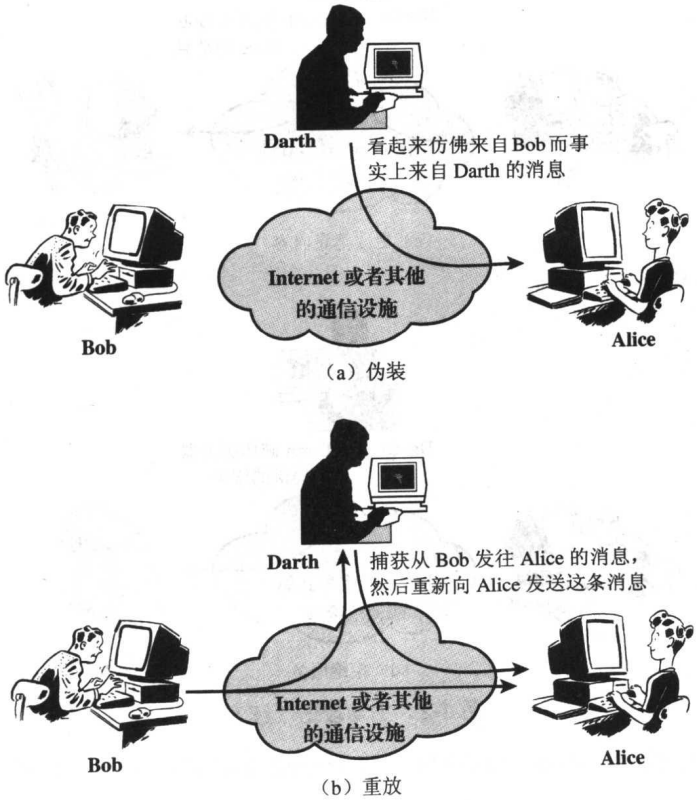


图 1-2 主动攻击

还包含另一种其他形式的主动攻击。例如，攻击者首先捕获认证序列，然后在发生了有效认证序列之后重放该序列，这样就可以通过模仿具有某些特权的实体使得不具有这些特权的授权实体获得这些特权。

重放是指被动地捕获数据单元然后按照原来的顺序重新传送，从而产生未经授权的效果（如图 1-2b 所示）。

更改消息内容就是指更改合法消息的一部分，或者延迟或重新排序消息，以产生未经授权的效果（如图 1-2c 所示）。例如，消息的含义是“允许 John Smith 阅读机密文件 accounts”，把它更改为“允许 Fred Brown 阅读机密文件 accounts”。

拒绝服务可以阻止或者禁止对通信设备的正常使用或管理（如图 1-2d 所示）。这种攻击可能具有明确的目标；例如，一个实体可以删除直接去往某一特定目的地的所有消息（例如，安全检查服务）。另一种形式的拒绝服务攻击就是使整个网络瘫痪，或者是通过禁用网络或者是通过超载消息来降低网络的性能。

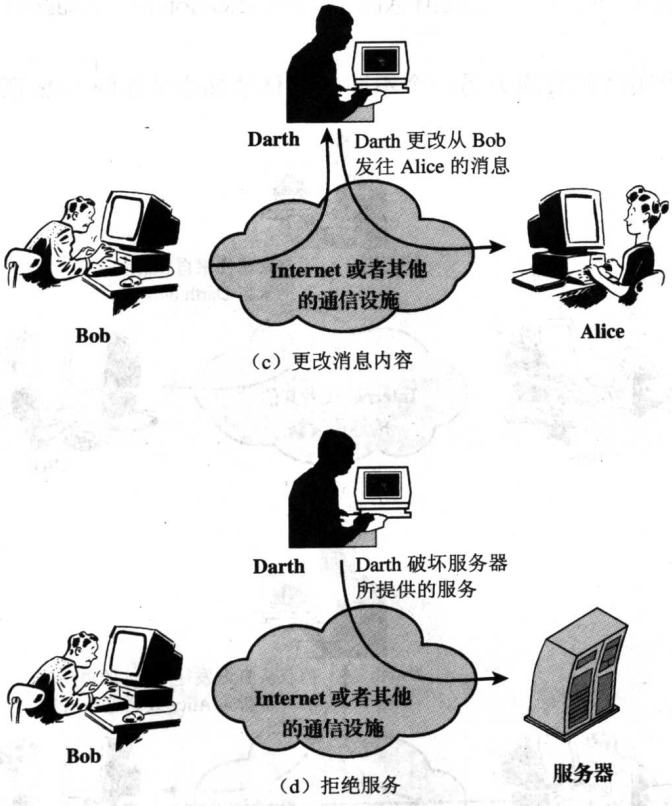


图 1-2 主动攻击（续）

主动攻击具有与被动攻击相反的特性。鉴于被动攻击难以检测，所采取的措施就是预防被动攻击获得成功。另一方面，绝对地预防主动攻击是相当困难的，因为如果这样做的话，就

需要在所有的时间对所有的通信设施和路径进行物理保护。取而代之的是，预防主动攻击的目标变成了检测主动攻击并且恢复主动攻击所造成的瘫痪或者延迟。因为检测具有威慑的作用，从而也可能具有预防的作用。

1.3 安全服务

X.800 所定义的安全服务是指由通信开放系统的协议层提供的服务，这些服务能够确保为系统或者数据传输提供足够的安全。在 RFC 2828 中或许可以找到关于安全服务的更加清晰的定义，定义如下：由系统提供的处理或者通信服务，能够对系统资源实施某种特定的保护；安全服务实现安全策略，而安全机制实现安全服务。

X.800 将这些服务分为五个类别和十四种具体的服务（见表 1-2）。我们依次研究每一种类别[③]。

表 1-2 安全服务（X.800）

认证 确保通信实体就是所声称的实体。 **对等实体认证** 结合逻辑连接一起使用，能够提供对连接实体身份的信任。 **数据源认证** 在无连接传输中，确保所接收的数据源是所声称的数据源。 **访问控制** 预防未经授权就使用资源（也就是说，这种服务用来控制谁可以访问资源，在什么条件下可以发生访问以及可以对资源的哪些方面进行访问）。 **数据机密性** 防止数据在未经授权的情况下发生泄漏。 **连接机密性** 保护在连接上的所有用户数据。 **无连接机密性** 保护所有单一数据块中的用户数据。 **选择字段（Selective-Field）的机密性** 在连接上的或者单个数据块中的所有用户数据的被选字段的机密性。 **流量机密性** 保护可能从流量的观察中获得的信息。	**数据完整性** 确保接收的数据与授权实体发送的数据一致（即不会发生更改、插入、删除或者重放）。 **具有恢复能力的连接完整性** 对在连接上的所有用户数据提供完整性服务，并且按照完全的数据顺序检测任何对数据的更改、插入、删除或者重放，具有恢复的能力。 **不具恢复能力的连接完整性** 与上面相同，但是只提供检测，不具备恢复的能力。 **选择字段的连接完整性** 对在连接上传输的数据块中用户数据的被选字段提供完整性，并且采用确定被选字段是否被更改、插入、删除或者重放的形式。 **无连接的完整性** 对于单个无连接的数据块提供完整性服务，且采取检测数据更改的形式。此外，可能会提供有限形式的重放检测。 **选择字段的无连接完整性** 对于在单个无连接数据块中的被选字段提供完整性服务；采取确定被选字段是否被更改的形式。 **非否认服务** 针对否认操作提供保护，通过在通信中参与全部或者部分通信的一个实体来实现。 **非否认服务，源** 证明消息是由指定当事人发送的。 **非否认服务，目的** 证明消息是由指定当事人接收的。

③ 在安全文献中，关于这里的很多术语都没有统一的约定。例如，术语*完整性*（*integrity*）有的时候用来表示信息安全的所有方面。术语*认证*（*authentication*）有的时候既用来表示身份验证又用来表示在本章中讨论的完整性服务下面所列出的所有功能。我们在这里使用的术语与 X.800 和 FRC2828 一致。