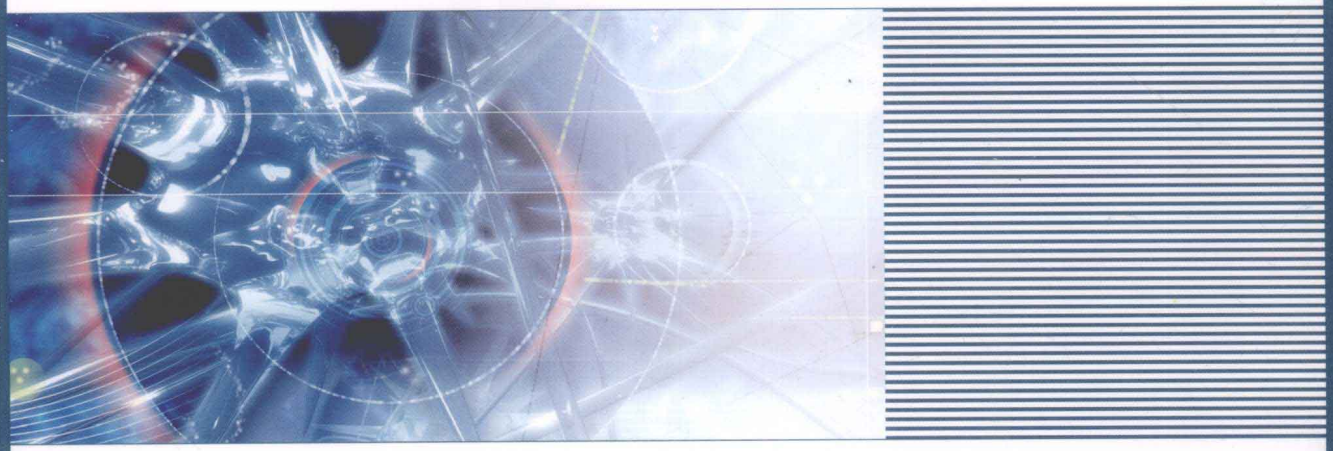
21世纪高等院校网络工程规划教材

21st Century University Planned Textbooks of Network Engineering



计算机网络安全

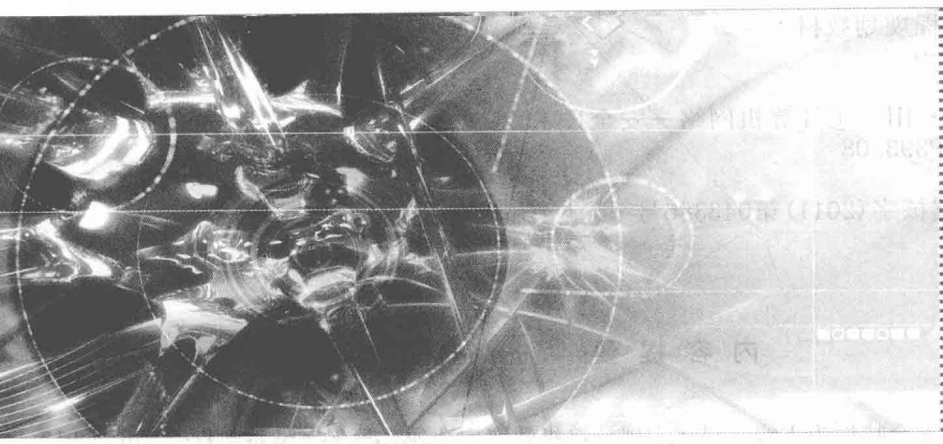
Computer Network Security

田立勤 编著

- 以计算机网络安全特性为主线
- 讲述实现网络安全的六大机制
- 融入网络安全最新知识和技术

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等院校网络工程规划教材
21st Century University Planned Textbooks of Network Engineering



计算机网络安全

Computer Network Security

田立勤 编著

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

计算机网络安全 / 田立勤编著. -- 北京 : 人民邮电出版社, 2011.5
21世纪高等院校网络工程规划教材
ISBN 978-7-115-25017-9

Ⅰ. ①计… Ⅱ. ①田… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第043386号

内 容 提 要

本书以保障计算机网络的安全特性为主线，讲述实现计算机网络安全的数据保密性、数据完整性、用户不可抵赖性、用户身份可鉴别性、网络访问的可控性和网络可用性六大机制，并安排了5个网络安全综合实验。每章后配有较多的习题供读者思考与复习，题型主要包括填空题、选择题和简答题，其中填空题和选择题都提供了参考答案，简答题可以通过学习教材找到相应的答案。

本书内容新颖、深入浅出、实例丰富，所有的介绍都紧密联系具体的应用。本书可作为高等学校计算机、电子商务、网络通信类专业课程的本科和研究生教学用书，也可作为培养企业网络信息化人才的实用教材。本书还可作为相关的计算机网络安全方面的科技工作者的实用参考书。

21世纪高等院校网络工程规划教材

计算机网络安全

◆ 编　　著　田立勤
责任编辑　刘　博

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷

◆ 开本：787×1092　1/16
印张：14　　2011年5月第1版
字数：347千字　　2011年5月河北第1次印刷

ISBN 978-7-115-25017-9

定价：28.00元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

前　言

网络安全特性是描述和评价网络安全的重要指标，它为网络安全的定量评价与分析提供基础，其机制的实现是网络安全的根本保证，本教材以六大网络安全基本特性（数据保密性、数据完整性、用户不可抵赖性、用户身份可鉴别性、网络可用性、网络访问的可控性）为主线贯穿整个网络，对上述网络安全的特性的作用、含义、基本实现思路、评价标准、具体实现机制、机制优缺点的评价、改进策略和应用实例等进行了详细的讲述。

在讲述每章的安全保障机制过程中，首先综述该机制在网络安全中的作用、地位、基本含义和实现的基本思路；然后给出评价标准，并根据评价标准按照循序渐进解决问题的思路，从基本机制开始讲述；接着分析和评价该机制的缺点和不足，进而提出新的机制，如此反复，不断完善；最后从若干机制中得出比较成熟可行的网络安全机制，同时讲述该机制在网络安全中的应用实例。

全书内容在强调系统性、完整性的同时，注重融入网络安全的最新知识和技术。本书内容丰富、图文并茂、深入浅出。希望能帮助读者较全面地掌握计算机网络安全的基本方法，并提高网络安全应用能力。

本书的建议课时是 56 或者 64 学时，第 1 章网络安全概述建议 4 学时，第 2 章数据保密特性机制建议 8～10 学时，第 3 章数据完整特性机制建议 4 学时，第 4 章用户不可抵赖性机制建议 4 学时，第 5 章用户身份可鉴别性机制建议 4 学时，第 6 章网络访问的可控性机制建议 8～10 学时，第 7 章网络可用性机制建议 4 学时，第 8 章计算机网络安全实验建议 16～18 学时，附录 B 计算机网络安全辩证观的讨论课建议 4～6 学时，当然也可以根据实际教学情况重新划分学时。

在本书的编写过程中，作者参阅了一些著作与文献，已列在书后的参考文献中，还有一些内容是在本门课程的讲课过程中逐渐积累和引用的，在此对其作者和出版者表示衷心的感谢！另外，作者在青海师范大学任职校长助理期间，学校提供了良好的写作环境，使得本书最后的统稿过程进展非常顺利，书稿按时完成，在此表示感谢！

作　者

2011 年 3 月

目　录

第 1 章　网络安全概述

1.1　网络安全与网络安全特性

随着 Internet 的迅猛发展和信息技术在人类社会生活各方面的广泛应用，信息网络的基础性、全局性作用得到日益增强。网络已发展成为建设和谐社会的一项重要基础设施，在通信、交通、金融、应急服务、能源调度、电力调度等方面发挥重要作用，如图 1-1 所示。

网络安全是网络应用中必须解决的问题，目前网络安全已经上升到关系国家主权和安全的高度，成为影响社会经济可持续发展的重要因素。我国明确提出“加强宽带通信网、数字电视网和下一代互联网等信息基础设施建设，推进三网融合，健全信息安全保障体系”。国家信息化领导小组召开的第三次会议也着重强调了保障信息网络安全和促进信息化发展的重要性，首次将保障信息网络安全确定为国家信息化战略的核心内容。事实上，这也是对世界各国积极制定网络空间安全战略的一种反应，如美国的《国家计算机空间安全战略》安全计划就明确地将网络安全提升到了关系国家安全的战略高度，此外还有《日本信息安全技术对策》、《法国信息网络安全管理体系》、《韩国信息通信构建保护法》等。

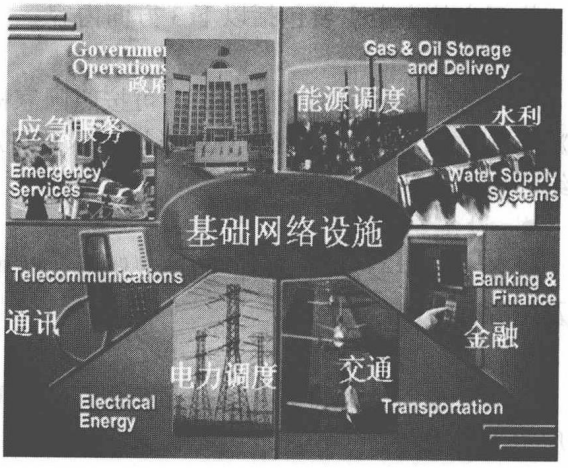


图 1-1　计算机网络的基础作用

随着信息通信技术的演进和发展，网络信息安全的内涵不断延伸，从最初的信息保密性发展到信息的完整性、可用性和不可否认性，进而又发展到系统服务的安全性，包括网络的可靠性、可维护性、可用性、可控性以及行为的可信性等，随之出现了多种不同的安全防范机制，例如，防火墙、入侵检测和防病毒等。虽然安全防范的技术不断增多增强，但是恶意攻击和恶意程序的破坏并没有因此而减少或减弱。为保证信息安全，人们只好把防火墙、入侵检测、病毒防范等做得越来越复杂，但是随着维护与管理复杂度的增加，整个信息系统变得更加复杂和难以维护，也使得信息系统的使用效率大大降低，因此网络正面临着严峻的安全挑战。网络的安全特性是描述和评价网络安全的重要指标，它为网络安全的定量评价与分析提供基础，其机制的实现是保障网络安全的主要途径，所以网络安全特性的准确含义、实现思路、评价标准、具体实现机制以及机制的评价与改进成为提高网络安全的重要内容。

1.2 网络安全的含义

定义 1.1 网络安全 泛指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改和泄漏，系统能够连续、可靠、正常地运行，网络服务不被中断。

网络安全的内容包括系统安全和信息安全两部分。系统安全主要指网络设备的硬件、操作系统和应用软件的安全。信息安全主要指各种信息的存储、传输安全，具体体现在信息的保密性、完整性及不可抵赖性方面。通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。所以，建立网络安全保护措施的目的是确保经过网络传输和交换的数据不会发生增加、修改、丢失和泄露等。

网络安全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、数论和信息论等多种学科的综合性学科。从内容看，网络安全包括以下 4 个方面。

1. 物理实体安全

物理实体安全主要包括以下 3 方面内容。

- 环境安全

对系统所在环境的安全保护，可按照国家标准 GB 50173—93《电子计算机机房设计规范》、国标 GB 2887—89《计算站场地技术条件》和 GB 9361—88《计算站场地安全要求》对网络环境进行环境安全设置。

- 设备安全

设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

- 存储介质安全

存储介质安全的目的是保护存储在存储介质上的信息，包括存储介质数据的安全及存储介质本身的安全。

存储介质数据的安全是指对存储介质数据的保护，包括 3 方面。①存储介质数据的安全删除，包括存储介质的物理销毁（如存储介质粉碎等）和存储介质数据的彻底销毁（如消磁等），防止存储介质数据删除或销毁后被他人恢复而泄露信息。②存储介质数据的防盗，防止存储介质数据被非法复制等。③存储介质数据的防毁，防止意外或故意的破坏使存储介质数据丢失。

2. 软件安全

软件安全主要指保护网络系统的系统软件与应用软件不被非法复制、篡改和不受病毒的侵害等。例如，将加密技术应用于程序的运行，通过对程序的运行实行加密保护，可以防止软件被非法复制以及软件安全机制被破坏。

3. 数据安全

数据安全主要指保护网络中的数据不被非法存取，确保其完整性和保密性。数据的完整性是指阻止非法实体对交换数据的修改、插入和删除；数据的保密性是指为了防止网络中各个系统之间交换的数据被截获或被非法存取而造成泄密，提供加密保护。

4. 安全管理

网络安全管理主要是以技术为基础，配以行政手段的管理活动。在安全问题中有相当一部分事件不是因为技术原因而是由于管理原因造成的。例如，管理规章制度的不健全、操作规程不合理和安全事件预防措施不得力等。只有在采取安全技术的同时采取有力的安全管理措施才能保证网络的安全性。安全管理的对象是整个系统而不是系统中的某个或某些元素。一般说来，系统的所有构成要素都是管理的对象，从系统内部看，安全管理涉及计算机、网络、操作、人事和信息资源；从外部环境看，安全管理涉及法律、道德、文化传统和社会制度等方面的内容。确保网络安全的措施一般包括采取网络安全保障机制，建立安全管理制度，开展安全审计，进行风险分析等。

1.3　网络安全特性

网络的安全特性是描述和评价网络安全的主要指标，为网络安全的定量评价与分析提供基础，其机制的实现是网络安全的根本任务，在网络安全中主要包括以下 9 个基本特性。

1. 网络的可靠性

网络的可靠性（Reliability）是提供正确服务的连续性，可以描述为系统在一个特定时间内能够持续执行特定任务的概率，侧重分析服务正常运行的连续性。它是指从开始运行到某时刻 t 这段时间内能够正常运行的概率。在给定的时间间隔和给定条件下，系统能正确实现其功能的概率称为可靠度。平均无故障时间 MTBF（Meantime Between Failures）是指两次故障之间能正常工作的平均值。故障既可能是元器件故障、软件故障，也可能是人为攻击造成的系统故障。可靠性分析主要依赖于软硬件故障发生的频率和模型的结构。设系统执行特定服务功能的状态集合为 S_R，系统在时间 t 所处的状态为 $X(t)$，初始状态为 $X(0)\in S_R$，取 $\tau=\inf\{t: X(t)\in S_R\}$ 则可靠性表示为：

$$R(t)=P\{\tau>t\} \tag{1.1}$$

2. 网络的可用性

网络的可用性（Availability）是可以提供正确服务的能力，是为可修复系统提出的，是对系统服务正常和异常状态交互变化过程的一种量化，是可靠性和可维护性的综合描述，系统可靠性越高，可维护性越好，可用性越高。根据可用性与时间的关系，可用性分为瞬时可用性和稳态可用性。

- 瞬时可用性的形式化计算

设系统正常服务状态的集合为 S_A，系统在时间 t 所处的状态为 $X(t)$，则瞬态可用性描述系统在任意时刻可提供正常服务的概率为：

$$A_I(t)=P\{X(t)\in S_A\} \tag{1.2}$$

- 稳态可用性的形式化计算

稳态可用性描述在一段时间内系统可用来正常执行有效服务的程度：

$$A_S=\lim_{t\to\infty}A_I(t)=\lim_{t\to\infty}\frac{\int_0^t A_I(u)\mathrm{d}u}{t} \tag{1.3}$$

注意可靠性和可用性的区别，一个具有低可靠性的系统可能具有高可用性，例如，一个

系统在每小时失效一次，但在 1 秒后即可恢复正常。该系统的平均故障间隔时间是 1 小时，显然有很低的可靠性，然而，可用性却很高：$A = 3599/3600 = 0.99972$。

一般情况下，可用性不等于可靠性，只有在系统一直处于正常连续运行的理想状态下，两者才是一样的。

3. 网络的可维护性

网络的可维护性（Maintainability）指网络失效后在规定时间内可修复到规定功能的能力，反映网络可维护性高低的参数是表示在单位时间内完成修复的概率（修复率）和平均修复时间 MTTR。

4. 网络访问的可控性

网络访问的可控性（Controllability）是指控制网络信息的流向以及用户的行为方式，是对所管辖的网络、主机和资源的访问行为进行有效的控制和管理。它分为高层访问控制和低层访问控制。高层访问控制是指在应用层层面的访问控制，是通过对用户口令、用户权限、资源属性的检查和对比来实现的。低层访问控制是指在传输层及以下层面的基于网络协议的访问控制，依据通信协议中的某些特征信息来禁止或允许对网络的访问。例如，防火墙就属于低层访问控制。

5. 数据的保密性

数据的保密性（Confidentiality）是指在网络安全性中，系统信息等不被未授权的用户获知。当网络系统受到某种确定攻击的影响时，如果可以明确区分哪些系统状态满足保密性，就可以量化网络系统保密性。假定 S_C 为满足保密性的状态集合，则网络系统保密性 C 可用概率表示为：

$$C = \sum_{i \in S_C} \pi_i \tag{1.4}$$

6. 数据的完整性

数据的完整性（Integrity）是指在网络安全性中，阻止非法实体对交换数据的修改、插入和删除。当网络系统受到某种确定攻击的影响时，如果可以明确区分哪些系统状态满足完整性，就可以量化网络系统完整性。假定 S_I 分别为满足完整性的状态集合，则网络系统完整性 I 可表示为：

$$I = \sum_{i \in S_I} \pi_i \tag{1.5}$$

7. 用户身份的可鉴别性

用户身份的可鉴别性（Authentication）是指对用户身份的合法性、真实性进行确认，以防假冒。这里用户还可以是用户所在的组或代表用户的进程。

8. 用户的不可抵赖性

用户的不可抵赖性（Non-Repudiation）是指防止发送方在发送数据后抵赖自己曾发送过此数据，或者接收方在收到数据后抵赖自己曾收到过此数据。常见的抵赖行为有：①A 向 B 发了信息 M，但不承认曾经发过；②A 向 B 发了信息 M0，却说发的是 M1；③B 收到了 A 发来的信息 M，但不承认收到；④B 收到了 A 发来的信息 M0，却说收到的是 M1。这里的用户可以是发送方或接收方。

9. 用户行为的可信性

用户身份的可鉴别性并不能保证行为本身一定是可信的，例如，在基于云计算的数字化电子资源订购方面，一些用户（例如，大学里的学生）常常使用网络下载工具大批量下载购买的电子资源或者私设代理服务器牟取非法所得等。这里，用户的身份是真实、可鉴别的（通常是根据 IP 地址确认用户的身份），但用户的行为不一定是可信的，我们常常看到一些电子资源使用的用户因为不当的行为而被警告甚至账户封闭。这些就是用户行为的可信性（Behavior Trustworthiness）。

除了这些安全特性外，目前研究者还提出了网络的可生存性、可管性、脆弱性和可信性等，但我们认为在这些众多的安全特性里面，这 9 个特性是基本特性，本书主要论述了这 9 个基本特性的实现机制与评价。上述提出的一些新特性有的可以归类到这些基本特性中，例如，可生存性可以认为是网络攻击下的可用性，当然有些安全特性还不能很好地对应，需要继续研究。

在后面的章节中，我们对上述网络安全特性的含义、基本实现思路、评价标准、具体实现机制、机制的优缺点的评价以及改进方法进行了详细讲述，并对相关的最新研究进行了论述。由于网络的可靠性和可维护性是网络可用性的两方面，网络的可靠性越高，可维护性越好，可用性就一定越高，因此将这两方面的内容放在网络的可用性里统一进行讲述。

1.4　主要安全威胁

网络威胁较多，这里只介绍主要安全威胁，包括以下 11 种。

1. 信息泄漏

信息泄漏是指敏感数据在有意或无意中被泄漏、丢失或透露给某个未授权的实体。信息泄漏通常包括：信息在传输中被丢失或泄漏（如利用电磁泄漏或搭线窃听等方式截获信息）；通过网络攻击进入存放敏感信息的主机后非法复制；通过对信息的流向、流量、通信频度和长度等参数的分析，推测出有用信息（如用户口令、账号等重要信息）。

2. 完整性破坏

完整性破坏是指非法实体对交换数据进行修改、插入、替换和删除，攻击者可以从 4 方面破坏信息的完整性。

- 修改：改变信息流的次序、时序、流向、内容和形式。
- 删除：删除消息全部或者其中的一部分。
- 插入：在消息中插入一些无意义或者有害的内容。
- 替换：非法实体用自己的信息全部替换原信息。

3. 服务拒绝（DoS，Denial of Service）

服务拒绝是指网络系统的服务能力下降或者丧失。这可能由两方面的原因造成。一是受到攻击所致，攻击者通过对系统进行非法的、根本无法成功的持续访问尝试而产生过量的系统负载，从而导致系统资源对合法用户的服务能力下降或者丧失；二是由于系统或组件在物理上或者逻辑上遭到破坏而中断服务。

4. 未授权访问

未授权访问是指未授权实体非法访问系统资源或授权实体超越权限访问系统资源。例如，有意避开系统访问控制机制，对信息设备及资源进行非法操作或运行；擅自扩大权限，越权访问系统资源。非法访问主要以假冒和盗用合法用户身份方式，非法进入网络系统进行违法操作。

5. 假冒

假冒是指某个未授权的实体（人或系统）假装成另一个不同的可能授权实体，使系统相信其是一个合法的用户，进而非法获取系统的访问权限或得到额外的特权。假冒通常与某些其他主动攻击形式一起使用，特别是消息的重放与篡改。攻击者可以进行下列假冒。

- 假冒管理者发布命令或调阅密件。
- 假冒主机欺骗合法主机及合法用户。
- 假冒网络控制程序套取或修改使用权限、口令、密钥等信息，越权使用网络设备和资源。
- 接管合法用户欺骗系统，占用或支配合法用户资源。

6. 网络可用性的破坏

网络可用性的破坏是指破坏网络可以提供正确服务的能力，攻击者可以从下列 3 方面破坏系统的可用性。

- 使合法用户不能正常访问网络资源。
- 使有严格时间要求的服务不能及时得到响应。
- 摧毁系统。例如，破坏网络系统的设备、切断通信线路或者破坏网络系统结构等。

7. 重放

重放是指攻击者对截获的某次合法数据进行备份，而后出于非法目的进行重新发送。例如，实体 A 可以重放含有 B 实体的鉴别信息，以证明它是 B 实体，达到假冒 B 的目的。

8. 后门

后门也称陷门，一般是指在程序或系统设计时插入的一小段程序。从操作系统到应用程序，任何一个环节都有可能被开发者留下“后门”，后门是一个模块的秘密入口，这个秘密入口并没有记入文档，因此，用户并不知道后门的存在。在程序开发期间后门是为了测试这个模块或是为了更改和增强模块的功能而设定的。在软件交付使用时，有的程序员没有去掉它，这样居心不良的人就可以隐蔽地访问它了。后门一旦被人利用，将会带来严重的安全后果。利用后门可以在程序中建立隐蔽通道，植入一些隐蔽的病毒程序。利用后门还可以使原来相互隔离的网络信息形成某种隐蔽的关联，进而可以非法访问网络，达到窃取、更改、伪造和破坏信息资料的目的，甚至还可能造成系统大面积瘫痪。

9. 特洛伊木马

特洛伊木马是指一类恶意的妨害安全的计算机程序，这类程序表面上在执行一个任务，实际上却在执行其他任务。与一般应用程序一样，特洛伊木马能实现任何软件的功能，如复制、删除文件，格式化硬盘，发送电子邮件等，实际上往往会导致意想不到的后果。例如，

它有时在一个合法的登录前伪造一个登录现场，提示用户输入用户名和口令，然后将账户和口令保存至一个文件中，显示登录错误，退出特洛伊木马程序。用户还以为是自己错了，再试一次时才正常登录了，这样用户无意之中就将自己的账号和密码泄露给了恶意用户。更为恶性的特洛伊木马会对系统进行全面的破坏。

10. 抵赖

抵赖是指通信的某一方出于某种目的而不承认发送或者接收过某些消息。

11. 通信量分析

数据交换量的突然改变也可能泄露有用信息，通信量分析是指攻击者根据数据交换的出现、消失、数量或频率变化而提取用户有用信息。例如，当公司开始出售它在股票市场上的份额时，在消息公开以前的准备阶段中，公司可能与银行有大量通信。因此，对购买该股票感兴趣的人就可以密切关注公司与银行之间的数据流量以确定是否可以购买。

1.5　网络的不安全因素

网络出现安全问题的原因主要有内因和外因两方面。内因是计算机系统和网络自身的脆弱性和网络的开放性，外因是威胁存在的普遍性和管理的困难性。

1. 计算机系统和网络自身的脆弱性

计算机系统和网络在各个阶段都有其自身的脆弱性。在设计阶段没有考虑安全或没有考虑周全，后补的时候网络已经应用开来；在实现阶段存在漏洞与后门；在维护与配置阶段，不当操作，特别是安全管理人员的误操作和故意非法操作会对系统造成更大的危害。Internet 的数据传输是基于 TCP/IP 通信协议进行的，这些协议缺乏使传输过程中的信息受到保护的安全措施。

2. 网络和系统的开放性

网络和系统的开放性包括以下几项。

- 网络的全球连通性。
- 系统的开放性和通用性。
- 统一网络协议：例如大多是 TCP/IP。
- 统一的操作系统平台：例如大多是 UNIX、Windows 等操作系统。
- 统一的应用系统：例如大多是 Office 、浏览器和电子邮件等应用软件。

这种网络和系统的开放性导致的危险是：在一个系统中发现的安全问题，在类似系统中可能存在、重现，这为攻击者提供了便利条件。

3. 威胁存在的普遍性

威胁存在的普遍性主要包括如下 5 个方面。

（1）内部操作不当

信息系统内部工作人员操作不当，特别是系统管理员和安全管理员出现管理配置的操作失误，可能造成重大安全事故。由于大多数的网络用户并非计算机专业人员，他们只是将计算机作为一个工具，加上缺乏必要的安全意识，使他们可能出现一些错误的操作，比如将网

络口令张贴在计算机上，使用家庭成员名称、个人生日等作为口令等，口令很容易被攻击者或者被其他恶意用户破解，从而造成损失。

（2）黑客攻击

在《中华人民共和国公共安全行业标准》中，黑客被定义为："对计算机信息系统进行非授权访问的人员。"黑客攻击早在主机终端时代就已经出现。随着因特网的发展，现代黑客从以系统为主的攻击转变到以网络为主的攻击。新的手法包括：通过网络监听，获取网上用户的账号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，进而取得合法资格；利用 UNIX 操作系统提供的守护进程的默认账户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等。

（3）恶意程序

恶意程序包括下列 3 种。

① 病毒

病毒（Virus）就是程序代码段，它连接到合法程序代码中，在合法程序代码运行时运行。它可以启动应用层攻击或网络层攻击。病毒可以影响计算机中的其他程序或同一网络中其他计算机上的程序，可以删除当前用户计算机上的所有文件，同时病毒具有自动传播的性质。病毒也可以由特定事件触发（如在每天上午 9 时自动执行）。通常，病毒会导致计算机与网络系统损坏，可以用良好的备份与恢复过程控制病毒对系统的破坏。

② 蠕虫

蠕虫（Worm）不进行任何破坏性操作，只是耗尽系统资源，使其停滞。蠕虫与病毒相似，但实际上是另一种实现方法。病毒修改程序（连接到被攻击的程序上），而蠕虫并不修改程序，只是不断复制自己。蠕虫复制速度很快，最终会使相应计算机与网络变得很慢，直到停滞。蠕虫攻击的基本目的不同于病毒，它是想通过吃掉所有资源使相应计算机与网络变得无法使用。

③ 特洛伊木马

特洛伊木马（Trojan horse）像病毒一样隐藏代码，但它具有不同的目的。病毒的主要目的是对目标计算机或网络进行某种修改，特洛伊木马则是为了向攻击者显示某种保密信息。特洛伊木马一词源于希腊士兵的故事，他们隐藏在一个大木马中，特洛伊市民把木马搬进城里，不知道其中藏了士兵。希腊士兵进入特洛伊城后，打开城门，把其他希腊士兵放了进来。同样，特洛伊木马可能把自己连接到登录屏幕代码中。用户输入用户名和口令信息时，特洛伊木马捕获这些信息，将其发送给攻击者，而输入用户名和口令信息的用户并不知道，然后攻击者可以用这个用户名和口令访问系统。

（4）拒绝服务攻击

拒绝服务攻击也属于一种破坏性攻击，它使合法用户无法进行正常访问。例如，非法用户可能向一个服务器发出太多的登录请求，快速连续地发出一个个随机用户 ID，使网络拥堵，其他合法用户无法访问这个网络。

（5）其他因素

网络受到威胁还涉及其他因素，包括自然灾害、物理故障、信息的窃听、篡改与重发、系统入侵、攻击方法易用性和工具易用性等。

4. 安全管理的困难

目前网络和系统管理工作变得越来越困难，主要原因包括以下 5 点。

（1）内部管理漏洞

信息系统内部缺乏健全的管理制度或制度执行不力，给内部工作人员违规和犯罪留下机会。其中以系统管理员和安全管理员的恶意违规和犯罪造成的危害最大。例如，内部人员利用隧道技术与外部人员实施内外勾结的犯罪，这是防火墙和监控系统难以防范的。此外，内部工作人员的恶意违规，造成网络和站点拥塞、无序运行甚至瘫痪。与来自外部的威胁相比，来自内部的攻击和犯罪更难防范，而且是网络安全威胁的主要来源，据统计，大约 80%的安全威胁均来自于系统内部。

（2）安全政策不明确

安全政策目标不明，责任不清，例如出现安全问题不容易分清是谁的责任等。

（3）动态的变化环境

企业业务发展，人员流动，原有的内部人员对网络的破坏等。

（4）社会问题、道德问题和立法问题

道德素质跟不上也是网络安全的隐患，例如，确定什么样的网络行为是违法的不够明确。

（5）国际间的协作、政治、文化、法律的不同

不同国家对网络行为的理解是不一样的，这给国际间的合作打击网络犯罪带来障碍。

1.6　网络攻击类型

网络攻击按攻击方式可分为被动攻击和主动攻击两类。

1. 被动攻击

被动攻击（Passive Attacks）只是窃听或监视数据传输，即取得中途的信息，这里的被动指攻击者不对数据进行任何修改。事实上，这也使被动攻击很难被发现，因此，处理被动攻击的一般方法是防止而不是探测与纠正。如图 1-2 所示，被动攻击分为消息内容泄漏和通信量分析两类。

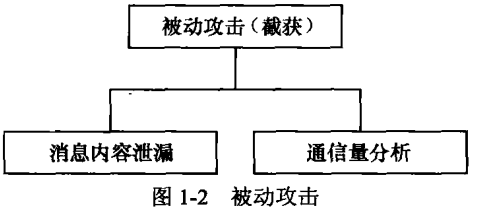


图 1-2　被动攻击

消息内容泄漏很容易理解。当发送消息时，我们希望只有对方才能访问，否则消息内容会被其他人看到。利用某种安全机制，可以防止消息内容泄漏。例如，可以用加密方式加密要发送的消息，使消息内容只有指定人员才能理解。如果传递许多加密的消息，那么攻击者虽然不知道准确的明文信息，但是可以猜出某种模式的相似性，从而猜出消息内容，这种对加密消息的分析就是通信量分析。

2. 主动攻击

主动攻击（Active Attacks）是以某种方式修改消息内容或生成假消息。这种攻击很难防止，但是容易被发现和恢复。这些攻击包括中断、篡改和伪造。在主动攻击中，会以某种方式篡改消息内容，主动攻击的原理如图 1-3 所示，主动攻击的分类如图 1-4 所示。中断是攻击者截断信息的传输，使信息不能或不能按时到达接收方；篡改是指攻击者非法对信息的来源和信息的内容进行增、删、改；伪造就是非法实体假冒成另一个合法实体，例如，用户 C 可能假冒用户 A，向用户 B 发一个消息，用户 B 可能相信这个消息来自用户 A。