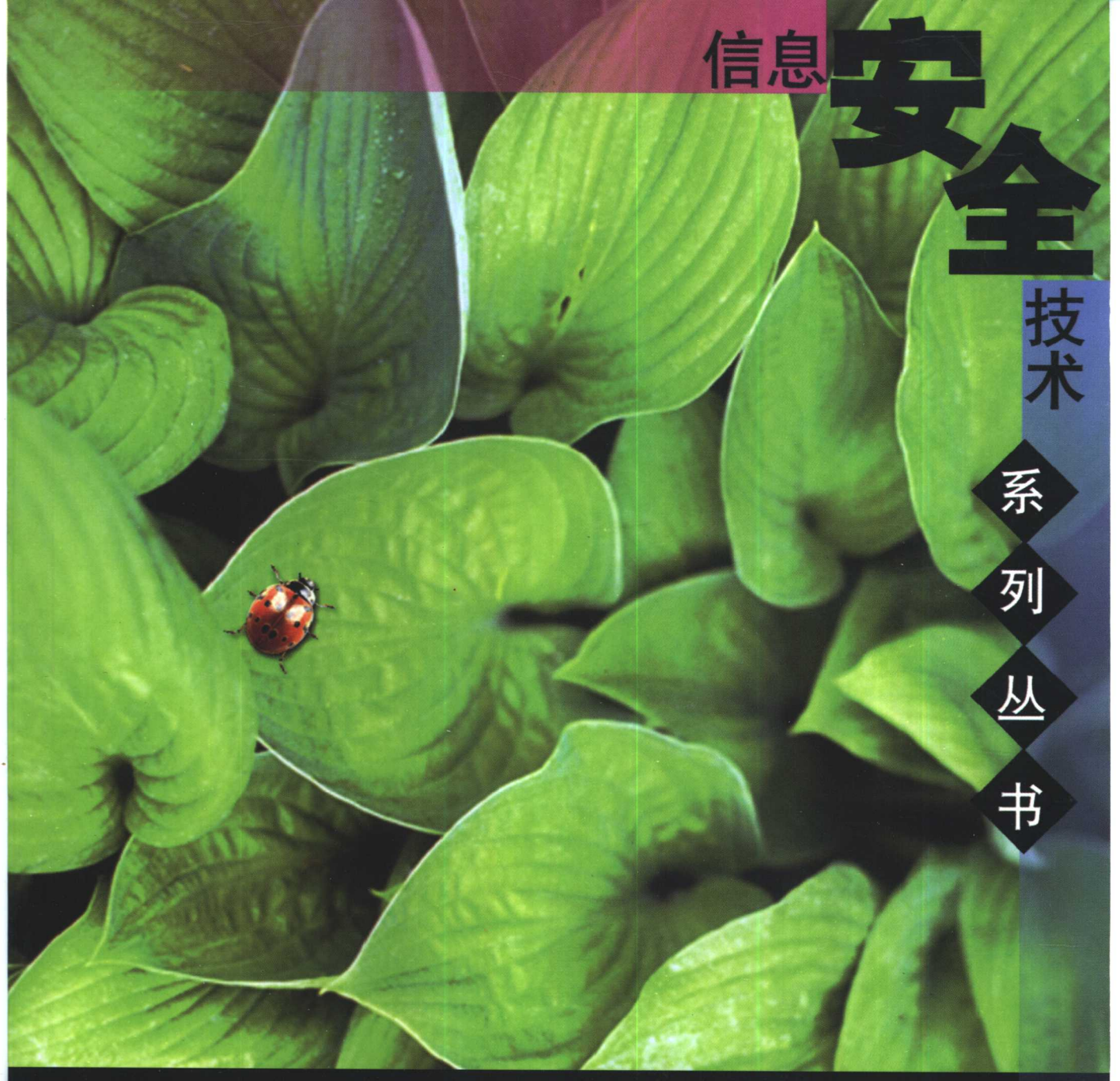
信息安全技术系列丛书



# 计算机通信网络安全

冯登国

清华大学出版社
http://www.tup.tsinghua.edu.cn

信息安全技术系列丛书

# 计算机通信网络安全

冯登国

国家重点基础研究发展规化项目资助(项目编号:G1999035800)
国家杰出青年科学基金项目资助(项目编号:60025205)

清华大学出版社

(京)新登字 158 号

## 内 容 简 介

本书主要介绍了一系列安全技术和用于保护计算机网络的安全协议、安全解决方案。主要包括两方面的内容:一方面是基本术语、概念、方法和技术的介绍,如密码技术,实现安全服务的方法,IDS 技术和 PKI 技术等;另一方面是已有一些标准组织标准化了的安全协议和技术,如 OSI 安全体系结构和框架,OSI 层安全协议,Internet 安全协议和网络安全管理协议等。

本书可作为计算机、通信、信息安全、密码学等专业的博士生、硕士生和本科生的教科书,也可供从事相关专业的教学、科研和工程技术人员参考。



**书　名**:计算机通信网络安全
**作　者**:冯登国
**出版者**:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
**印刷者**:北京人民文学印刷厂
**发行者**:新华书店总店北京发行所
**开　本**:787×1092 1/16　**印张**:15.75　**字数**:360 千字
**版　次**:2001 年 3 月第 1 版　2001 年 3 月第 1 次印刷
**书　号**:ISBN 7-302-04245-4/TP・2495
**印　数**:0001～8000
**定　价**:22.00 元

# 前　言

信息系统包括信息存储系统(如数据库)、信息处理系统(如计算机)和信息传输系统(如通信网络)等,它的安全是一个错综复杂的问题,涉及面非常广。威胁信息系统安全的因素很多,有自然灾害、各种故障以及各种有意或无意的破坏等。为了确保信息系统的安全,需要从多方面着手,采取各种措施,比如物理措施、管理措施和技术措施等。计算机通信网络是一种有着广泛应用的信息传输系统,它是计算机与通信技术相结合的产物,它的安全性至关重要。特别是以 Internet 为代表的计算机通信网络正在成为未来全球信息系统的最重要的基础设施,如果它的安全性解决不好,将直接影响到社会稳定和国家安全。

从 Internet 的发展来看,最初是美国军方出于预防核战争对军事指挥系统的毁灭性打击提出的研究课题,其后将军事用途分离出去,单纯研究在科研教育的校园环境中解决互连、互通、互操作的技术问题。在校园环境中,理想的技术、信息共享主义使 Internet 的发展忽略了安全问题。20 世纪 90 年代后,Internet 从校园环境走上了社会应用,商业应用的需要使人们意识到了忽视安全的危害。尤其是在网上存在利益的今天,一些不良行为从另一个方面向人们揭示了信息系统的脆弱性,引起人们对信息安全的空前重视。

人们有些什么信息安全的需求呢? 首先人们意识到的是信息保密,这是一个古已有之的需要,近代历史上成为战争的情报军事手段和政府专用技术。在传统信息环境中,普通人通过邮政系统发封信件,为了个人隐私还要装上个信封。可是到了使用数字化电子信息,以 0、1 比特串编码,在网上传来传去,连个"信封"都没有,我们发的电子邮件都是"明信片",哪还有什么秘密可讲。这就是信息安全中的**机密性**需求。

人们进一步认识到,在传统社会中,不相识的人们相互建立信任需要介绍信,并且在上面签上名盖上章。但是在电子信息环境中如何签名盖章,怎么知道信息真实的发送者和接收者,怎么知道信息是真实的,并且在法律意义上做到责任的不可抵赖,这就成为人们归纳的信息安全中的**完整性和非否认性**需求。

人们还意识到信息和信息系统都是它的所有者花费代价建设起来的。但是,存在着由于计算机病毒或其他人为的原因可能造成的对主人的拒绝服务,被他人滥用机时或信息的情况。这就成为信息安全中的**可用性**需求。

由于社会中存在不法分子,以及地球上各国之间还时有由于意识形态和利益冲突造成的敌对行为,政府对社会的监控管理行为(如搭线监听犯罪分子的通信),在社会广泛使用信息安全设施和装置时可能受到严重影响,以至不能实施。这就出现了信息安全中的**可控性**需求。

本书着重从技术角度出发,针对计算机通信网络的安全需求,系统介绍了解决计算机通信网络安全的一些关键技术和实现方法,同时也介绍了一些国际上比较流行的标准安全技术和协议。本书的特点是作者结合国内外现有的相关书籍及实际工作中的研究与开发经验,将信息安全理论和技术特别是密码理论和技术融于网络实际应用之中,旨在让从

事信息安全理论研究的学者了解具体应用环境，以使理论研究更加实用、更加广泛；同时让从事信息安全系统和产品开发的人员了解信息安全中的关键理论和技术，以设计和开发出更好、更安全的系统和产品。当然，能否达到这些目标，还有待于读者检验。

本书在写作过程中，得到了清华大学出版社的大力支持，在此表示感谢。

作　者

2000 年 10 月 18 日于北京

# 目　录

# 第1章

# 绪　论

## 1.1　典型的网络安全需求

目前网络安全已不再是军方和政府要害部门的一种特殊需求。实际上，所有的网络应用环境包括银行、电子交易、政府(无密级的)、公共电信载体和互联/专用(或私有)网络都有网络安全的需求。关于这些典型环境的安全需求参见表1.1.1。

表1.1.1　典型的网络安全需求

| 应用环境 | 需　求 |
| --- | --- |
| 所有网络 | 阻止外部的入侵(黑客) |
| 银行 | 避免欺诈或交易的意外修改<br>识别零售交易的顾客<br>保护个人识别号(PIN)以免泄漏<br>确保顾客的秘密 |
| 电子交易 | 确保交易的起源和完整性<br>保护共同的秘密<br>为交易提供合法的电子签名 |
| 政府 | 避免无密级而敏感的信息的未授权泄漏或修改<br>为政府文件提供电子签名 |
| 公共电信载体 | 对授权的个人限制访问管理功能<br>避免服务中断<br>保护用户的秘密 |
| 互联/专用网络 | 保护团体/个人的秘密<br>确保消息的真实性 |

## 1.2　安全与开放系统

从词义上看，网络安全与开放系统似乎是矛盾的，但事实并非如此。开放系统的概念代表了购买者多年来对封闭的、独立的计算机系统以及通信硬件和软件的经销商们所寄予的厚望。人们期望可以自由地选择经销商来购买不同的系统部件，而这些部件可以有机地组合起来以满足购买者的需要。因此，开放系统的发展与应用和许多标准的制定密

切相关。

计算机联网是与开放系统并肩发展起来的。开放系统的标志是开放系统互连(Open System Interconnection,OSI)模型的提出。自从20世纪70年代以来,这个模型得到了不断的发展和完善,从而成为全球公认的计算机通信协议标准。除了OSI标准外,另外一些标准化组织也建立了开放系统网络协议。最为有名的当属Internet协会,它提出了著名的TCP/IP协议。通过围绕开放系统互连所开展的标准化活动,使得不同的厂家所提供的设备进行互连成为可能。

将安全保护措施渗透到开放系统网络中是一个比较新的尝试。事实证明,这是一项十分复杂的任务。之所以说它复杂,主要是因为它代表了两种技术的完美结合——安全技术的应用与通信协议的设计。为了给开放系统网络提供安全保证,就必须将安全技术与安全协议相结合,而安全协议则是一般的网络协议的重要组成部分。

当前,我们要做的主要工作是在下列的三个较宽的领域内,设计或建立一些兼容的或作为补充的标准:1)安全技术;2)一般用途的安全协议;3)特殊用途的安全协议,如银行、电子邮件等应用。

与以上领域有关的标准主要来自以下四个方面:

① 有关信息技术的国际标准。这些标准是由以下组织建立的:国际标准化组织(International Organization for Standardization—IOS),国际电子技术协会(International Electrotechnical Commission—IEC,网址为:www.iec.ch),国际电信联合会(International Telecommunication Union—ITU,原称CCITT)和电气与电子工程师协会(Institute of Electrical and Electronics Engineers—IEEE);

② 银行工业标准。这些标准或者是由ISO国际性地开发的,或者是由美国国家标准协会(American National Standards Institute—ANSI)面向美国国内的应用而开发的;

③ 国家政府标准。这些标准是由各国政府制定的;

④ Internet标准。这些标准是由Internet协会开发的。

## 1.3 网络安全策略

在介绍安全策略这个概念之前,我们先介绍安全区域这一概念。所谓一个安全区域通常是指属于某个组织的处理和通信资源之集。安全策略是指在某个安全区域内,用于所有与安全活动相关的一套规则。这些规则是由此安全区域中所设立的一个权威机构来建立的。

安全策略是一个很广泛的概念,这一术语以许多不同的方式用于各种文献和标准之中。OSI安全体系结构中将安全策略定义为安全服务应达到的各种准则。一些近来的分析表明,安全策略有以下几个不同的等级:

① 安全策略目标:是某个机构对所要保护的特定资源要达到的目的所进行的描述;

② 机构安全策略:是一套法律、规则和实际操作方法,用于规范某个机构如何来管理、保护和分配资源以达到安全策略的既定目标;

③ 系统安全策略:所描述的是如何将某个特定的信息技术系统付诸工程实现,以支

持此机构的安全策略要求。

在本书中，术语“安全策略”的使用通常是指系统安全策略等级。但是我们必须明白它仅仅是较广的安全策略概念的一个组成部分。

下面我们对影响网络系统和部件设计的安全策略的几个主要方面作一简要介绍。

### 1.3.1 授权

授权(authorization)是一个安全策略的基本组成部分。所谓授权是指赋予主体(用户、终端、程序等)对客体(数据、程序等)的支配权力，它等于规定了谁可以对什么做些什么。授权描述在机构安全策略等级上的一些例子如下：

① 文件 Project-X-Status 只能由 D. Feng 修改，并由 D. Feng，J. Jing 和 Project－X 计划小组中的成员阅读；

② 一个人事记录只能由人事部的职员进行新增和修改，并且只能由人事部职员、执行经理和该记录所属于的那个人阅读；

③ 在一个有机密、秘密和绝密等密级的多级安全系统中，只有所持许可证级别等于或高于此密级的人员，才有权访问此密级中的信息。

这些安全策略的描述也对各类防护措施提出了要求。例如，采用人事防护措施来决定人们的许可证级别。在计算机和通信系统中，主要的要求是通过一种被称作“访问控制策略”的系统安全策略反映出来。

### 1.3.2 访问控制策略

访问控制策略(access control policies)隶属于系统安全策略，它迫使在计算机系统和网络中自动地执行授权。以上有关授权描述的①，②和③分别对应于以下不同的访问控制策略。

① 基于身份的策略：该策略允许或拒绝对明确区分的个体或群体进行访问；

② 基于角色的策略：该策略是基于身份的策略的一种变形，它给每个个体分配角色，并基于这些角色来使用授权机制；

③ 多级策略：该策略是基于信息敏感性的等级以及工作人员许可证等级而制定的一般规则。

访问控制策略有时也被分成强制访问控制策略和自主访问控制策略两类。强制访问控制策略是由安全区域的权威机构强制实施的，任何用户都不能回避它。强制访问控制策略在军事上和其他政府机密环境最为常用，上述的策略③就是一个例子。自主访问控制策略为一些特殊的用户提供了对资源(例如信息)的访问权，这些用户可以利用此权限控制对资源进行访问。上述的策略①和②就是自主访问控制策略的两个例子。在机密环境中，自主访问控制策略用于强制执行“须知(need to know)”最小特权策略(least privilege policy)或最小泄漏策略(least exposure policy)，前者只授予主体为执行任务所必需的信息或处理能力；后者按原则向主体提供机密信息，并且主体承担保护信息的责任。

### 1.3.3 责任

支撑所有安全策略的一个根本原则是责任(Accountability)。受到安全策略制约的任何个体在执行任务时,需要对它们的行为负责任。这与人事安全有十分重要的关联。某些网络防护措施,包括认证工作人员的身份以及与这种身份相关的活动,都直接地支持这一原则。

## 1.4 安全威胁与防护措施

### 1.4.1 基本概念

所谓安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性或合法使用所造成的危害。某种攻击就是某种威胁的具体实现。

所谓防护措施是指保护资源免受威胁的一些物理控制、机制、策略和过程。脆弱性是指在防护措施中和在缺少防护措施时系统所具有的弱点。

所谓风险是关于某个已知的、可能引发某种成功攻击的脆弱性的代价的测度。当某个脆弱的资源的价值高,以及成功攻击的概率高时,风险也就高;反之,当某个脆弱的资源的价值低,以及成功攻击的概率低时,风险也就低。风险分析能够提供定量的方法来确定防护措施的支出是否应予以保证。

安全威胁有时可以被分成故意的(如黑客渗透)和偶然的(如信息被发往错误的地址)两类。故意的威胁又可以进一步被分成被动的和主动的两类。被动威胁包括只对信息进行监听(如搭线窃听),而不对其进行修改,主动威胁包括对信息进行故意的修改(如改动某次金融会话过程中货币的数量)。总的来说,被动攻击比主动攻击更容易以更少的花费付诸工程实现。

### 1.4.2 安全威胁

目前还没有统一的方法来对各种威胁加以区别和进行分类,也难以搞清各种威胁之间的相互联系。不同威胁的存在及其重要性是随环境的变化而变化的。然而,为了解释网络安全服务的作用,人们总结了现代计算机网络以及通信过程中常遇到的一些威胁。

**1. 基本的威胁**

信息安全的基本目标是实现信息的机密性、完整性、可用性以及资源的合法使用。下面所要介绍的四个基本的安全威胁直接反映出了这四个安全目标。

① 信息泄漏:信息被泄漏或透露给某个未授权的实体。这种威胁主要来自诸如窃听、搭线或其他更加错综复杂的信息探测攻击;

② 完整性破坏:数据的一致性通过未授权的创建、修改或破坏而受到损坏;

③ 拒绝服务:对信息或其他资源的合法访问被无条件地阻止。这可能是由于以下攻

击所致：攻击者通过对系统进行非法的、根本无法成功的访问尝试而产生过量的负载，从而导致系统的资源对合法用户也是不可使用的。也可能由于系统在物理上或逻辑上受到破坏而中断服务；

④ 非法使用：某一资源被某个未授权的人或以某一未授权的方式使用。这种威胁的例子有：侵入某个计算机系统的攻击者会利用此系统作为盗用电信服务的基点或者作为侵入其他系统的出发点。

**2. 主要的可实现的威胁**

在安全威胁中，主要的可实现的威胁是十分重要的，因为任何这类威胁的某一实现会直接导致任何基本威胁的某一实现。因而，这些威胁使基本的威胁成为可能。主要的可实现的威胁包括渗入威胁和植入威胁。

主要的渗入威胁有：

① 假冒：某个实体（人或系统）假装成另外一个不同的实体。这是渗入某个安全防线的最为通用的方法。某个未授权的实体提示某一防线的守卫者，使其相信它是一个合法的实体，此后便攫取了此合法用户的权利和特权。黑客大多采用假冒攻击；

② 旁路控制：为了获得未授权的权利和特权，某个攻击者会发掘系统的缺陷或安全上的脆弱之处。例如，攻击者通过各种手段发现原本应保密，但是却又暴露出来的一些系统“特征”。利用这些“特征”，攻击者可以绕过防线守卫者渗入系统内部；

③ 授权侵犯：被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他未授权的目的，这也称作“内部威胁”。

主要的植入威胁有：

① 特洛伊木马（Torjan Horse）：软件中含有觉察不出的或无害的程序段，当它被执行时，会破坏用户的安全性。例如，一个外表上具有合法目的的软件应用程序，如文本编辑，它还具有一个暗藏的目的，就是将用户的文件拷贝到一个隐藏的秘密文件中，这种应用程序称为特洛伊木马，此后，植入特洛伊木马的那个人可以阅读到该用户的文件；

② 陷门：在某个系统或某个文件中设置的“机关”，使得当提供特定的输入数据时，允许违反安全策略。例如，一个登录处理子系统允许处理一个特定的用户识别号，以绕过通常的口令检查。

**3. 潜在威胁**

如果在某个给定环境对任何一种基本威胁或者主要的可实现的威胁进行分析，我们就能够发现某些特定的潜在威胁，而任意一种潜在威胁都可能导致一些更基本的威胁的发生。例如，如果考虑信息泄漏这样一种基本威胁，我们有可能找出以下几种潜在威胁（不考虑主要的可实现的威胁）：

① 窃听；

② 业务流分析；

③ 人员疏忽；

④ 媒体清理。

图 1.4.1 给出了一些典型的威胁以及它们之间的相互关系。注意，图中的路径可能

回旋。例如，假冒威胁可以构成所有基本威胁的基础。然而，假冒威胁本身也有信息泄漏的潜在威胁(因为信息泄漏可能暴露某个口令，而用此口令能够实施假冒)。表 1.4.1 给出了各种威胁之间的区别。

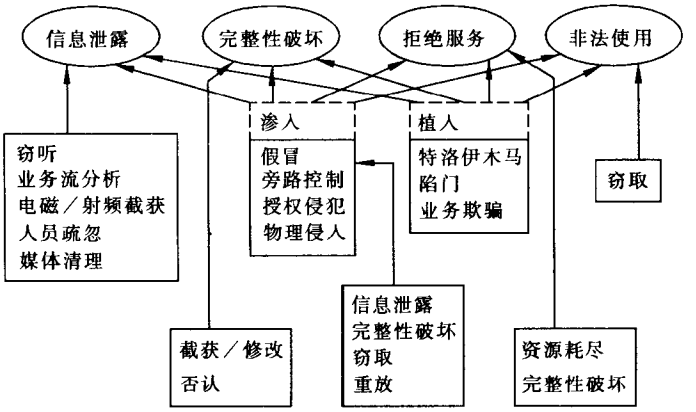



图 1.4.1　典型的潜在威胁及其相互关系

**表 1.4.1　典型的网络安全威胁**

| 威　胁 | 描　　述 |
|---|---|
| 授权侵犯* | 为某一特定目的授权使用一个系统的人却将该系统用作其他未授权的目的 |
| 旁路控制 | 攻击者发掘系统的缺陷或安全脆弱性 |
| 拒绝服务* | 对信息或其他资源的合法访问被无条件的拒绝或推迟与时间密切相关的操作 |
| 窃听* | 信息从被监视的通信过程中泄露出去 |
| 电磁/射频截获 | 信息从电子或机电设备所发出的无线射频或其他电磁场辐射中被提取出来 |
| 非法使用 | 资源被某个未授权的人或者以未授权的方式使用 |
| 人员疏忽 | 一个授权的人为了金钱或利益或由于粗心将信息泄露给一个未授权的人 |
| 信息泄露* | 信息被泄露或暴露给某个未授权的实体 |
| 完整性破坏* | 数据的一致性通过对数据进行未授权的创建、修改或破坏而受到损坏 |
| 截获/修改* | 某一通信数据项在传输过程中被改变、删除或替代 |
| 假冒* | 一个实体(人或系统)假装成另一个不同的实体 |
| 媒体清理 | 信息被从废弃的或打印过的媒体中获得 |
| 物理侵入 | 一个侵入者通过绕过物理控制而获得对系统的访问 |
| 重放* | 出于非法的目的而重新发送截获的合法通信数据项的拷贝 |
| 否认* | 参与某次通信交换的一方，事后错误地否认曾经发生过此次交换 |
| 资源耗尽 | 某一资源(如访问接口)被故意超负荷地使用，导致其他用户的服务被中断 |
| 服务欺骗 | 某一伪系统或系统部件欺骗合法的用户，或系统自愿地放弃敏感信息 |
| 窃取 | 某一安全攸关的物品，如令牌或身份卡被盗 |
| 业务流分析* | 通过对通信业务流模式进行观察(有，无，数量，方向，频率)而造成信息被泄露给未授权的实体 |
| 陷门 | 将某一“特征”设立于某个系统或系统部件之中，使得在提供特定的输入数据时，允许安全策略被违反 |
| 特洛伊木马 | 含有觉察不出或无害程序段的软件，当它被运行时，会损害用户的安全 |

其中带“*”号的威胁表示通信网络安全中可能发生的威胁。

通过调查分析表明，在现实生活中，下面几种威胁是最主要的威胁：

① 授权侵犯；

② 假冒；

③ 旁路控制；

④ 特洛伊木马或陷门；

⑤ 媒体清理。

当然，在具体实施攻击时，攻击者往往将几种攻击结合起来使用，Internet 蠕虫(Internet Worm)就是将旁路控制与假冒攻击结合起来的一种威胁。在这种威胁中，旁路控制涉及对 Berkeley UNIX 操作系统的已知缺陷的利用，而假冒则涉及对用户口令的破译。

### 1.4.3 防护措施

在通信网络安全领域中，有许多类型的安全防护措施。除了采取密码技术的防护措施以外，还有以下几类防护措施：

① 物理安全：门锁或其他物理访问控制；敏感设备的防窜扰；环境控制；

② 人员安全：职位敏感性识别；雇员筛选过程；安全性训练和安全意识；

③ 管理安全：控制软件从外国进口；调查安全泄露、检查审计追踪以及检查责任控制的工作程序；

④ 媒体安全：保护信息的存储；控制敏感信息的记录、再生和销毁；确保废弃的纸张或含有敏感信息的磁性介质得到安全的销毁；对媒体进行扫描，以便发现病毒；

⑤ 辐射安全：射频(RF)及其他电磁(EM)辐射控制(亦被称作 TEMPEST 保护)；

⑥ 生命周期控制：可信系统的设计、实现、评估和担保；程序设计标准及控制；文档控制。

一个安全系统的强度是与其最弱链路的强度相同。为了提供有效的安全性，我们需要将属于不同种类的威胁对抗措施联合起来使用。例如，当用户将口令遗忘在某个不安全的地方，或者受到欺骗而将口令暴露给某个未知的电话用户时，用于对付假冒攻击的口令系统即使技术上是完备的也将是无效的。

保护措施可用来对付大多数的安全威胁，但是每个防护措施均要付出代价。一个网络用户或代理人需要仔细考虑这样一个问题，即为了防止某一攻击所付出的代价是否值得。例如，在商业网络中，一般不考虑对付电磁(EM)或射频泄露，因为对商用来说其风险是很小的，而且其防护措施又十分昂贵(但在一个机密环境中，我们会得出不同的结论)。对于某一特定的网络环境，究竟采用什么安全防护措施，这种决策的作出属于风险管理的范畴。目前，人们已经开发出了各种定性的和定量的风险管理工具。

### 1.4.4 病毒

所谓病毒(viruses)是指一段可执行的程序代码，通过对其他程序进行修改，可以“感