第一章　网络安全概述

在信息时代里，犯罪行为已逐步向高科技蔓延并迅速扩散，利用计算机进行犯罪的案例越来越多。因此，计算机的安全成为一个越来越引起世界各国关注的重要问题，但它也是一个十分复杂的课题。随着计算机在人类生活各领域中的广泛应用，计算机病毒也在不断产生和传播，计算机网络不断被非法入侵，重要情报资料被窃，甚至由此造成网络系统的瘫痪等，给各个国家以及众多公司造成巨大的经济损失，甚至危害到国家和地区的安全。

第一节　网络安全基础知识

以贝尔实验室为例谈一下网络安全。贝尔实验室工作大量地涉及到计算机和软件，大约 50%的雇员在从事软件或软件支持工作。他们拥有 1800 多台主机和比其技术人员人数还多的各种计算机终端。在贝尔系统内，有运行 3500 多万条有效编码的通信线路，因此，贝尔实验室是世界上最大的软件企业之一。

贝尔实验室的计算机环境包括：分布在不同地区的集中化的计算中心，它们一般装备的是大型电机和高档微机，分布在各部门的通常是小型机，直接由技术人员使用的是大量的专业工作站，一般是微型机。所有这些计算机均以各种方式联接成网，包括从高速通信专线联络到直接使用全国电信购的拨号通信线等，这就使雇员们甚至可以通过在家中的终端直接存取贝尔实验室的各种计算机资源。

一个严重的问题是，国外代理人、竞争者或其他任何人要想从连接于电信网络的计算机系统中获取信息都是可能的，这就提出了一个必须重视的计算机安全和保密问题。一般来说，威胁到计算机安全的有“单纯性电子干扰”、各种物理的干扰、通信线的开放、专业情报人员的长期探取以及拥有特权的系统管理人员的不负责等。其中，“单纯性电子干扰”是今天最普遍地威胁计算机安全的因素；而最令人担忧的是系统管理人员的失职，由于这个问题，可使所有采用的安全技术成为无效。

贝尔实验室所有的工作人员，都必须学会怎样有效地生产大型软件系统，并在保证软件产品的质量时，也建立有效的软件管理办法。这些方法包括安全方面的设计，如存取控制、防止及检测未授权的存取企图的检查能力等。

一、网络安全问题的提出

随着对计算机网络的依赖性越来越大，网络安全问题也日益明显。 1988 年 11 月 1 日，一个名叫罗伯特·莫里斯的康奈尔大学的研究生在互联网上投放了一种恶意的计算机程序“蠕虫”，这种蠕虫被释放到互联网后，便进行“自我复制”，在很短的时间内便使互联网上 10%的主机（大约 6 000 台）无法工作，损失可谓惨重。这一事件终于使人们意识到网络的安全问题。比如，美国国防部远景研究规划局便很快组建起计算机应急小组，专门对付“蠕虫”病毒作祟期间所引发的各种事故。网络安全问题也由此提到重要的工作日程。

在竞争日益激烈的今天，人们普遍关心的问题主要有 7种，在国外普遍称为 7P 问题。即：Privacy（隐私）、Piracy（盗版）、Pornography（色情）、Pricing（价格）、Policing（政策制订）、Psychological （心理学）、Protection of the Network（网络保护）。然而，这 7 种问题，可以说是从不同的角度提出的安全问题。而重要的则在于如何创造出一种安全的环境，使人们不再担心上网后便有可能蒙受损失或遭受攻击。当前，最为火爆的网络是互联网（Internet），“信息高速公路”便是以互联网为雏形的。然而，互联网最大的问题便是安全问题，它从问世起便是一个以“无政府”为口号的公用网络，谁都可以上去“漫游”一番或“冲浪”一回。

互联网并不是一种很具体的网络，而是由许许多多网络互相联接组成的一个网际网，它所采用的技术是 TCP/IP，其关键在于保证异种之间的通信；TCP/IP—— 传输控制协议（TCP—Transmission Control Protocol ）和互联协议（ IP—Internet Protocol）这一对协议，面对这样一个大型网络，自然会有许多问题，其中之一便是网络遭到非法入侵。

美国国家科学基金会于 1991 年取消了在互联网上不允许商业活动的限制。随着互联网的商业化，有许多公司、企业和机构也开始在互联网上进行业务活动。在进入互联网之前，这些公司有的已经有了自己的局域网或广域网，只是在传输协议上不一定是 TCP/IP 而已。由于每个公司、企事业单位等都有一些不能为外人或竞争者知道的数据，如特定的表单；销售计划、客户名单等，所以保密成了它们进入互联网的首先要解决的问题，因而“内部网”便应运而生。所谓“内部”指的是它不是一个公用网络，而是一个专用网络，但由于与互联网相连，就一定要用 TCP/IP 技术，而不能用原有的或一般的网络协议。然而，用 TCP/IP 技术的同时，却要求一般公众不能从外部的互联网，即一般意义下的互联网访问这个内部专用网，达到这一目的的关键便是“防火墙”技术。除此之外，在确保网络安全和数据安全方面，尚有数据加密技术和智能卡技术等。

二、网络安全的关键技术

互联网的兴起带领人们迈向信息社会，而内部网的浪潮则使人们在信息时代捕捉到新的商机。但是要想使商用网络在互联网上得以安全运行，先应建立或使原有的网络升级为内部网，而专用的内部网与公用的互联网的隔离则有赖于防火墙技术。

“防火墙”是一种形象的说法，其实它是一种计算机硬件和软件的组合，在互联网与内部网之间建立一个安全网关，从而保护内部网免受非法用户的侵入。

真正意义下的防火墙有两类：一类被称为标准防火墙，一类叫双家网关。标准防火墙系统包括一个 UNIX 工作站，该工作站的两端各接一个路由器进行缓冲。其中一个路由器的接口是外部世界，即公用网；而另一个则联接内部网。标准防火墙使用专门的软件，并要求较高的管理水平，而且在信息传输上有一定的延迟。而双家网关则是对标准防火墙的扩充，双家网关又称堡垒主机或应用层网关，它是一个单个的系统，却能同时完成标准防火墙的所有功能。其优点是能运行更复杂的应用，同时防止在互联网和内部系统之间建立的任何直接的连接，可以确保数据包不能直接从外部网络到达内部网络，反之亦然。

但是，防火墙策略难于防止黑客的攻击。

防火墙技术是内部网最重要的安全技术之一，其主要功能就是控制对受保护网络的非法访问。它通过监视、限制、更改通过网络的数据流，一方面尽可能屏蔽内部网的拓扑结

构，另一方面对内屏蔽外部危险站点，用于防范外对内、内对外的非法访问。但也有其明显的局限性，诸如：

（1）防火墙难于防内。防火墙的安全控制只能作用于外对内或内对外，即对外可屏蔽内部网的拓扑结构，封锁外部网上的用户连接内部网上的重要站点或某些端口；对内可屏蔽外部危险站点，但它很难解决内部网控制人员的安全问题，即防外不防内。而据权威部门统计结果表明，网络上的安全攻击事件有 70% 以上来自内部攻击。

（2）防火墙难于管理和配置，易造成安全漏洞。防火墙的管理及配置相当复杂，要想成功地维护防火墙，首先要求防火墙管理员对网络安全攻击的手段及其与系统配置的关系有相当深刻的了解。其次防火墙的安全策略无法进行集中管理。一般来说，由多个系统（路由器、过滤器、代理服务器、网关、堡垒主机）组成的防火墙，管理上有所疏忽是在所难免的。根据美国《财经》杂志统计资料表明， 30% 的入侵发生在有防火墙的情况下。

（3）防火墙的安全控制主要是基于 IP 地址的，难于在防火墙内外提供一致的安全策略。许多防火墙对用户的安全控制主要基于用户所用机器的 IP 地址而不是用户身份，这样就很难为同一用户在防火墙内外提供一致的安全控制策略，限制了企业网的物理范围。

（4）防火墙只实现了粗粒度的访问控制。防火墙只实现了粗粒度的访问控制，且不能与企业内部使用的其他安全机制（如访问控制）集成使用，这样，企业就必须采用为内部的身份验证和访问控制管理维护单独的数据库与防火墙配合使用的安全技术及数据加密技术。数据加密技术是为提高信息系统及数据的安全性和保密性、防止秘密数据被外部破译所采用的主要技术手段之一。随着信息技术的发展，网络安全与信息保密日益引起人们的关注。目前，国务院除了从法律上、管理上加强数据的安全保护外，从技术上分别在软件和硬件两方面采取措施，推动了数据加密技术和物理防范技术的不断发展。按作用不同，数据加密技术主要分为：数据传输，数据存储，数据完整性的鉴别，密钥管理技术。

在计算机安全检查表中，最后要强调的一点是，通过使用特殊的软件包来限制对各个用户文件的普通存取，以提高安全程度。人们可以使用软件来保护存于计算机文件中的信息，该软件限制了其他人存取非自己所有的文件，直到该文件的所有者明确准许其他人可以存取该文件时为止；限制存取的另一种方式是通过硬件完成，在接收到存取文件要求后，先询问并校核口令，然后访问列于目录中的授权用户标志号。

此外，有一些安全软件包也可跟踪可疑的未授权的存取企图，例如，多次试登录或请求别人的文件。显然，可以限制试登录的次数或对试探操作加上时间限制，在此之后，系统就自动地退出。

现有的各种技术提供了高水平的计算机安全，想要破译一些计算机的保密信息，其代价是非常昂贵的。当然，维护这样高级的计算机安全控制的代价也是非常昂贵的，通常是将各计算机隔离，但随着安全技术的进一步提高，将会大大有助于降低这种代价——即使整个安全控制对合法用户更透明一些。

防止和检测计算机通信线被渗透的技术，就像识别拨号系统一样简单。这种能力允许根据授权电话号码表来进行安全检查，也可提供追踪未授权存取企图的记录。这种识别已存在于现在的一些计算机化的业务通信系统中，但只限于在那些由这种系统服务的公司的通信线中。

此外，还可使用“信用卡终端”。它可提供便宜而又可防篡改的方式，对识别用户比

通用的口令具有更高程度的可靠性。这种简单的硬件可产生软件不能伪造的信号，这将能提高网络地址的安全程度。然而，计算机安全的最基本还是人的因素，正如前面多次指出的，人们需要尽更大的努力去提高人们对于计算机安全的认识。

关于防火墙的技术还将在以后的章节中详细介绍。

三、网络安全的组成

计算机网络安全包括物理安全和逻辑安全。

物理安全主要是指把文件服务器放到加锁的房间里，防止有破坏预谋的人接近物理设备。

逻辑安全是指使用密码及其他形式的软件保护，实现各种权限特性的安排。

实现物理安全需要加强对计算机机房的管理，如加强门卫制度、出入者身份检查、下班后锁门以及各种硬件安全手段等预防措施。

而对于逻辑安全则需要用口令字、文件许可、查账以及软件加密等方法来实现。

四、网络安全的目标

现在计算机网络安全的目标是：在安全和通信方便之间建立平衡。显然，要求计算机系统越安全，则对通信的限制和使用的难度就越大。而现代信息技术的发展又使通信线成为不可缺少的内容，它包括跨组织、跨学科、跨地区的以及全球的通信。

一般来说，公司或其他经营单位的安全措施应包括三个主要目标：

（1）对存取的控制；

（2）保持系统及数据的完整；

（3）能够对系统进行恢复和对数据进行备份（如果系统出事之时）。

换句话说，一种安全的信息技术系统要对用户的访问权限予以限制，同时避免应用软件或数据的破坏，更重要的是当系统失灵时能够重新启动系统并保存重要数据的备份。

计算机安全的重要性是毫无疑问的。但是计算机的安全程度应与所涉及的信息的价值相适应。应当有一个从低、中到高级的多层次的安全系统，分别对不同重要性的信息资料给予必要的不同级的保护。

例如，在贝尔实验室，高度机密的个人信息（如付税数据）是与其他各种数据完全相隔离的；对所有高度机密的数据的存取都被严格地控制着。善于保护计算机安全的另一个重要问题是：试图保护的信息—— 电子信息——本身的特殊性质。

最后一点要强调的是，必须责成各级机构的高层管理人员经常关注和强化计算机安全技术和保密措施。

关于计算机安全的考虑也是十分基本的：保护有价值的信息在存储于计算机文件中或在通信、数据线上传输时不会被窃取、删改和破坏；防止计算机机密和资源被未授权者使用；保持计算机用户和系统管理员的高度安全意识。总而言之，是要维护一套对整个计算机环境的一致性的有关的管理控制，包括计算机硬件、软件和有关的人员。

五、网络安全的评估

网络安全和数据保护这些防范措施都有一定的限度，并不是越安全就越可靠。因而，

在看一个内部网是否安全时不仅要考虑其手段，更重要的是对该网络所采取的各种措施，其中不光是物理防范，而且还有人员的素质等其他“软”因素，进行综合评估，从而得出是否安全的结论。

要想使一个商用内部网真正做到安全，光有防范措施是远远不够的。从某种意义上来说，对于内部网的内部管理并不亚于外部防范。因而，对一个网络的安全性而言，不仅要看它所采用的防范措施，而且还要看它的管理措施。只有将这两者综合起来考察，才能最终得出该网络是否安全的结论。

内部网和专线服务在连入互联网之前，对网络的安全措施和政策等公司管理层必须予以重视，否则一旦出现损失，后果可能是相当严重的。另外，公司管理层还必须想到公司内部，究竟是什么人以及出于什么目的才被允许到互联网进行存取。从国外最近的一次问卷调查来看，大约有 43%的答卷人回答说公司没有关于发送电子邮件的书面规定。由于通信网络是公司的资产，所以公司对员工们滥用通信网络应该负责。

那些希望建立内部网或希望与互联网相连的公司、企业和机构往往只注重对于外部入侵者的防范，认为那才是保证网络安全的“正道”，其实不然，可以试想一下，入网之前，单位肯定已经有电话、传真机或调制解调器等通信设施，肯定会对这些设备的使用作出了相应的规定。员工在什么情况下允许使用这些设施？是否有授权使用的口令？口令多长时间更改一次？是否有明文规定不允许使用容易被破译的口令？对于网络，情况亦然。因而，在网络使用的管理方面也应有章可循，否则很难避免员工自觉或不自觉地浪费公司的资源。

因而，对于信息系统不光要强调建设问题，更为重要的是信息系统建成后的安全问题。而对于安全问题更应未雨绸缪，事先防范。

商业经营离不开成本核算，因而评估机构在评估一个网络的安全风险时，首先要看所保护的是什么、要防范的是什么、在安全防护上能投入多少。只有把这些问题搞清楚，才能制定出一套综合的安全方案，并将该方案所需要的技术确定下来。在对一个网络进行评估之前，首先要弄清楚以下问题：

（1）确定单位内部是否已经有了一套有关网络安全的方案。

（2）如果有的话，将所有有关的书面文件汇总。

（3）确定所有知道网络安全方案的人。

（4）对已有的方案进行审查。

（5）仔细检查联入互联网后潜在的危险。

（6）明确规定哪些人或单位可以直接存取互联网资源。

（7）制定出一份覆盖以前所考虑到的所有问题的书面计划。

（8）确定所需的技术使网络安全方案能得以落实。

（9）购买并使用相应的技术。

（10）确保通知全部有关人员关于网络安全的方案。

只有当公司的网络安全方案最终确定下来，才能有效地选择相应的安全技术。安全也是一种投资，既然如此，就要想到性能价格比。比如选用防火墙技术，其安全级别和价格的关系等。

网络是否安全，有时并不是网络所有者自己完全清楚的。所以，许多公司要请第三方评估机构或专家来完成对网络安全的评估。这样做的好处是：能对自己所处的环境有个更

加清醒的认识，把未来可能的风险降到最小，目前网络安全评估的中介机构，在国外已经开始将网络的安全评估作为一个新的服务项目向社会推出。作为一种新兴的业务，其影响是否能向会计师事务所、审计师事务所之类的中介机构那样重要，尚需拭目以待。但有一点可以肯定，那就是网络上的商机同样也与风险同在。要想获得利润，就必须将安全问题解决。

总结有关计算机安全方法各主要方面，以下几点可供超级管理员评定自己单位的计算机系统的安全程度作参考。

（1）有谁知道用户的计算机的存取权？不要与他人（即使是用户的助理工作人员）共用口令。如果用户的同组人员需要存取其他人员的文件，他们也应当有自己的口令。

（2）用户的计算机拒绝未授权的远程计算机的请求吗？如果不拒绝，则应重新修改用户的计算机的许可设置，以改变这一情况。

（3）用户有系统管理员吗？管理和修改安全设计与设置是他（她）的工作职责吗？最安全的系统是那些配有责任心和能力都很强的系统管理员的计算机系统。

（4）用户将一些私人信息，如公司计划或个人审查资料存入计算机文件吗？假若出现糟糕的情况（如一个偶然浏览文件的人能读到用户所写入计算机的信息， 那么必须尽快将重要资料保存到其他地方。

（5）用户的同组严肃对待计算机的安全问题吗？必须确保他的同组用户懂得计算机安全的必要性以及应当怎样做才能保证计算机的安全。

除上述几项检查以外，还需进一步来检查以下各点：例如口令，除“一人一口令”外还可使用更复杂的口令来增加计算机的安全。许多计算机用户常常使用自己的姓，甚至配偶的姓或宠物的名字，或者生日作为口令，这种口令很不安全，因为任何一台计算机都能迅速地运行搜索完一个姓氏列表（即英语中 2 万个最普通的单词），以及所有可能的生日。更复杂的口令选择应是长于 6 个字符并同时含有数字和字母的口令，这样的口令将难于解密。口令也不应是“永久性”的，而应当以一定的时间间隔进行改变。如何修改将由所希望的系统安全的级别来决定。

这里值得强调的另一点是责任者的重要性。责任者是指所有涉入计算机系统的人，现用户、管理员和超级管理员。例如：计算机的任何使用都需要有超级用户给予的许可，以便能控制谁使用机器和机器用于做什么。因而，每一台机器应有一个授权用户表，此外，还须具有拨号存取方式的计算机上的公司目录表，目录表内容包括与具体计算机有关的机构标志、电话、系统管理员以及监督管理等。

计算机安全与保密问题是现代信息社会一个十分重要并具有普遍意义的问题，必须认真演习、掌握和发展有关的技术和方法。

网络的安全问题是在通向信息化社会的进程中遇到的，研究和解决这些问题已经远远不是单纯的技术问题，而是未来信息社会所面临的社会问题。我国目前正处在社会转型时期，信息网络建设正在全面铺开，因此，对目前这些所谓“网络安全”的“技术问题”进行“社会的”研究，无疑具有重要而又深远的意义。

随着网络的发展，关于网络的大量名词已经充斥了人们的生活。翻开报纸、打开电视、登上网络，人们会看到计算机攻击事件越来越多。人们经常可以听到从国外到国内，从政府机构到金融机构，种类繁多、各式各样的被入侵消息。

更令人担心的是，只有少量网络攻击得到了报道，大多数攻击由于被攻击者的种种顾虑，根本没有得到发布。在网络攻击成倍增长的今天，网络安全已经成为每个计算机用户的必备误程。

第二节　需要保护什么

当用户的计算机接入了因特网时，就已经把下面的内容置于风险之中：

（1）用户的数据；

（2）用户的资源；

（3）用户的声誉。

一、用户的数据

需要保护的数据有三个独立的特征：

（1）保密性：用户可能不希望别人知道它。

（2）完整性，用户很可能不想让别人改变它。

（3）可用性：用户希望自己能够使用它。

人们倾向于关注与保密性有关的风险，并且这些通常确实是大的风险。每个机构都有一些最重要的机密如产品设计、财务记录或学生档案等在计算机里。另一方面，用户可能发现，在自己的站点上，可以很容易地从连接到因特网的机器上识别出含有这种高度机密的数据的机器来。

假设使用这种方法能够识别用户的数据，而且因特网可访问的信息又没有什么保密内容。在这种情况下，为什么还要关心安全性问题呢？因为保密数据不是用户试图保护的惟一内容，用户还需要关心完整性和可用性。如果用户的数据中没有保密内容。用户不在乎它们是否会被篡改，也不介意别人能否得到它，那么用户又何必要浪费磁盘空间呢？

即使用户的数据不是特别机密，也有可能遭受被破坏和被修改的后果。其中有些后果是容易预计的：如果用户丢失了数据，将不得不重建数据；如果用户丢失的是以某种形式的销售数据，用户将损失销售额。这与用户丢失的数据是什么类型有关。不管这些数据是有关用户设计制造的产品，还是软件产品的源代码，用户都会因此而遭受损失。还有与任何安全事故有关的无形损失。最严重的是用户失去对系统及数据的信任，从而对用户的机构失去信任。

二、用户的资源

如果其他人要使用用户的计算机，而用户的计算机中存储的是自己不在乎的数据，那么用户很可能想要从这种使用中得到某些方面的好处。大多数人想使用自己的计算机，或向其他的使用者收费，但他们却无法期望从入侵者那里得到这些。

入侵者总声称他们仅仅使用多余的那部分资源。因此，他们的入侵不占用受害者任何东西，这种说法是没有根据的。首先，一个入侵者只使用那些多余的资源是不可能的。用户的系统可能看起来像有大量空闲的磁盘空间和成小时的未利用的计算时间，然而实际上用户可能正准备开始运行激活的程序，它将要使用每一数位和每一微秒。当用户想要使用

它们时入侵者却不能归还他正在使用的资源。

其次，用用户喜欢的方法使用自己的资源是用户的权利。计算机资源不同于自然资源，它们有限的资源不会因未被利用就被浪费或破坏。

三、用户的声誉

一个入侵者冒充用户的身份出现在因特网上，他做的任何事情看起来是出自于用户的所作所为，其后果将是无法预料的。

大多数时候将会产生这样的结果，其他站点或法律执行机构开始呼叫并责问为什么用户正试图破坏他们的系统。

有时候，这样的冒名顶替者使用户失去的价值比实际丢失的价值多得多。一个怀有仇视心理的入侵者，或乐于制造事端的入侵者，可能盗用用户的名义发送电子邮件或邮寄新闻消息。一般地，选择实现这个目的的人大多数是有敌意的，是不可信任的。但是，即使只是少数人相信这些消息，消除其影响要花很长时间，同时将会使用户的声誉及尊严受到影响。任何事情，甚至是极少的可信性消息，都会对用户的声誉造成永久的损害。

不经允许访问站点而伪造电子邮件或新闻是可能的，但是伪造的消息，如果它产生于外部的伪造站点，是很容易被揭露的。如果是来自一个已经获得站点访问权的入侵者的消息将看起来确实像是用户的，因为它们就是用户的。一个入侵者也将可访问到外部伪造者不能访问的各种细节。例如，入侵者将持有用户的全部可用电子邮件表并确实知道用户发送电子邮件给谁。

即使入侵者不使用用户的身份在用户的私人站点侵入，对用户的声誉也不是好事。在用户的组织中它动摇了人们对用户的信任。此外，大多数入侵者会企图从用户的机器进入到其他机器去，这将使成为他们的下一个受害者的其他机器认为用户的站点是计算机犯罪的平台。许多入侵者也将用被泄露的站点作为散布盗版软件或色情描写的站点。这两者哪一个都将不会使用户受人喜爱，无论如何都是用户的错，因为用户的名字已经与诸如入侵、软件盗版和色情描写等相联系，这是很难恢复清白的。

第三节　需要防备什么

在因特网上用户会面对哪些类型的侵袭？要对付哪些类型的入侵者？愚蠢低级的安全事故是怎样的？本节将详细介绍。

一、侵袭的类型

在系统上有许多类型的侵袭，这些侵袭有多种分类方法。在这一节里，把侵袭分成三种基本的类型：入侵、拒绝服务和盗窃信息。

（一）入侵

在用户的系统上最普通的侵袭是入侵。通过入侵，大多数侵袭者能像合法的用户一样使用用户的计算机。侵袭者有数十种获得访问的方法，其范围从公关侵袭（如果弄清了公司里某个上级的名字，就可以冒用其名呼叫系统管理员，并且告诉他现在就需要变更口令），到简单的猜测（尝试账户名称和口令组合直到获取一个正确的组合为止），以及不需

要知道账户名称与口令就进入系统的复杂的方法。

（二.)拒绝服务

拒绝服务是指在彻底地阻止用户使用自己的计算机的一种侵袭。

即使有最简单的和最普通的方法——淹没去实现拒绝服务侵袭，聪明的侵袭者也能禁止服务，给它们重定路由，或者替换它们。

封闭不可能避免所有拒绝服务侵袭。有时侵袭者的状况是“开始，我得胜；最后，你失去”，例如，在一定数量的登录企图失败之后，许多站点将账户设置成不能使用的状态，这能防止侵袭者以简单试口令的方法找到正确的口令。另一方面，它给侵袭者一个安装拒绝服务侵袭的容易的方法：他们简单地通过试图登录少数几次便锁住任何用户的账户。

拒绝服务侵袭的风险是司空见惯和不可避免的。如果用户接受来自外部的事物——电子邮件、电话呼叫、或者数据包--—都有可能被淹没。拒绝服务很有可能通过故意的或偶然事件发生。

幸运的是，有意的拒绝服务侵袭不是特别流行。这些低级拙劣的伎俩被许多侵袭者认为是不光彩的。他们可能被跟踪并冒一定的风险，而且没有为侵袭者带来信息或者使用用户的计算机的机会。有意的拒绝服务侵袭是对用户的站点特别愤怒的人干的，而在大多数站点这样的人十分稀少。

（三.）盗窃信息

有些侵袭使自己无需直接利用用户的计算机就可以获取数据信息。通常这些侵袭利用发放信息的因特网服务，使该服务提供比预计的更多的信息，或者使该服务将信息交给不该得到的人。许多因特网服务被设计用于本地网，并没有达到使信息安全地穿过因特网所具有的安全类型或等级。

信息盗窃不一定是主动的或者是需要特别技术的。想要查明个人信息的人可以通过简单地呼叫用户并提问，这是一种主动的信息盗窃。如果他们窃听了用户的电话这就是一种被动的信息盗窃。同样地，想要收集电子信息的人能够通过主动地查询或者能够通过被动地窃听网络并且等候通过的信息流动。

偷窃信息的大多数人试图得到许可对用户的计算机实施访问，他们查找用户名和口令。对他们来说，窃听网络是最容易得到信息的，这是网络上最简单的信息偷窃方式。用户名和口令信息在许多网络开始相互作用时，如人们所预料的那样出现并且这样的信息以同样的形式反复使用。

有若干种防备信息盗窃的措施。适当配置防火墙将使用户可以防备那些试图得到更多信息的人的入侵。但一旦用户已决定通过因特网给出信息，那么，要通过错误认证（有人要求授权，可他们是非法用户）或者通过防止嗅探（有人只是通过正确授权的通道读取信息）来防备那种非故意的读者获得信息是非常困难的。

二、侵袭者的类型

有许多方法可以对这些侵袭者进行分类，但人们对许多侵袭者确实不能做到准确定位，现在要对其类别作出快速的总结，其观点必定是相当陈旧的。然而，这些总结对于判别侵袭者的主要类别还是有用的。

所有侵袭者具有一定的共性。他们都不想被抓住，所以都试图隐蔽自己。如果他们获准访问用户的系统。他们将肯定企图保留那种访问权限，如果可能，一般都通过建立额外的途径得到访问。大多数侵袭者与有同样兴趣的其他人有某种联系，并且大多数将共享侵袭用户的系统得到的信息。

人们经常不加区别地使用“攻击者”和“黑客”两个词，人们说“我们被黑客入侵了”通常也就意味着“我们被恶意攻击了”。

但是，这两个词有显著区别。攻击者指想盗窃或破坏用户资源的人。攻击者可能是技术水平很高，也可能是个初学者。攻击者的活动更像间谍或破坏者。

黑客是一些对计算机及网络有很深入了解的人。黑客不仅仅满足于运行一些简单的程序，他们还要理解运行中的方方面面的问题，黑客是指希望深入系统的内部进行研究的人。在系统中进行渗透的办法既可能用于正当场合，也可能用于非法领域，由使用者的人品和动机决定。黑客的行为已经形成自己的文化，有自己的语言，并且接受社会实践的检验。正是他们的人格因素才使得外界的人们既可能把他们认做黑客，也可能认为是攻击者。其实，黑客更像一些技术革命者，像 Microsoft 的总裁比尔·盖茨一开始就是十足的黑客出身。

第四节　OSI 安全性体系结构

国际标准化组织（ISO）已经提出一个建议性标准的文件 DIS7498-2（OSI 参考模型第二部分 安全性体系结构），ISO 把它作为开放系统互连（OSI）标准的一部分。在安全性方面，可以提供重要的指导作用。 DIS7498-2包括下述内容：

（1）重要安全性要点清单。

（2）为组织提供安全性任务而给予的帮助。

（3）为实施者和购买者提供的指南。

（4）标准化安全性实施的办法。

ISO的这一标准的两个根本目的是：

（1）为 OSI 各层提供安全性要点的功能分配，从而指导基于 OSI 标准未来所做的增强提供一个结构框架，在这个框架之内供应商和消费者可以评估产品的安全性。

（2）在 OSI 标准提供的框架中，还定义了安全性服务和安全性机制。为了理解 ISO 所采取的方法，可以分安全性威胁、安全性服务和安全性机制三部分来讨论。

一、安全性威胁

损害一个机构或个人所拥有信息的安全，这种行为是安全性威胁。安全性威胁有两种类型：被动威胁和主动威胁。对这两种威胁的处理方法，稍有不同。

（一）被动威胁

通常被动威胁不改变系统中的数据，或者说，被动威胁只是读取系统中的信息，以从中获取利益。由于没有自发信息，被动威胁留下的可供追踪的痕迹很少，或者根本没有留下痕迹，因而很难被发现。然而，被动威胁通常可以预防，并且预防是阻止这种威胁进行的基本手段。

在一个网络中，被动威胁包括侵入者获取系统泄露的消息内容，或者侵入者通过读数据包（通信量分析）以确定信源方和目的方的位置和身份。当然，如果一条信息已经存放在主机系统的文件中，那么对系统的访问可能导致入侵系统来获取已经存储的信息。

阻止被动威胁的主要方法是采用加密技术，使得如果没有解密密钥，所获得的信息是看不懂的。加密是通过使用代码或密码来实现的，代码使用一个预定义的表来替换每条消息或消息的某一部分中每个词或句子。与之相比，密码使用一个可计算的算法将数据信息译成难以破译的密文。密码技术可以容易地实现自动化，因而常常被计算机和网络安全系统所采用。常规的加密方法是将原始数据转换成难懂的密文。实现这一转换，需要用到一个算法和控制这一算法的密钥。密钥由位串组成。发送者和接收者都要拥有密钥，因而密钥的管理也成为一个问题。算法必须有足够的复杂度，以排除从密文破译出的消息的可能。

从网络的角度看问题，有两种基本的加密方法：链路加密和端到端加密。链路加密指数据的加密独立于通信链路。这种链路对于简单的网络来说，可能是端到端的。端到端的加密，正如名字所提示的，发生在数据分组的源地址和目的地址处。这种加密方法在中间节点处照顾了数据的脆弱性，然而，数据分组头是明文。使用这两种加密方法的混合系统是最安全的，数据分组头只在端点和中间节点处是明文，而实质信息永远不会是明文。对端到端的加密方法稍做变化，就是在一个加密的文件中永久存放数据，这种系统可用于替代或补充其他两种加密方法。

密钥管理的任务是在一个密码系统中控制密钥的选择和分配。密钥是一段数字信息，它与加密算法相互作用，以控制信息的加密。因此，密钥必须妥善保护以防泄露。在常规的加密系统中通信链路的两端都有一份密钥的拷贝。因此有损害安全性的可能。通过经常更换密钥，可以把这种损害降低到一定限度内。公开密钥密码系统可以替代常规的加密方法，这种加密方法要用到两个密钥，一个用于加密过程，任何一个想加密信息的人都可以使用该密码。一个私用密钥用于解密过程，该密钥只被它的所有者所知晓。

加密／解密的传统方法是使用一个对称算法，在这个算法中加密信息的发送者和接收者要求拥有相同的密钥。对称算法的不利之处，在于算法和密钥必须保密。此外，密钥必须从一个人传达到另一个人，因而产生了安全性威胁。然而，该算法的主要优点是可以建立某种鉴定系统，以减少由于伪造信息所带来的问题。替代上述算法的一种新方法是使用一种非对称系统，公开密钥加密是这一方法的派生物。

虽然有专用加密算法在使用，然而使用最广泛的算法是数据加密标准（DES），DES是一种算法，它在电子硬件设备上实现，用来为数字的、二进制编码的信息做保密保护。需要注意的是，加密往往是发生在物理层（OSI 模型）中的，然而加密 可以在进行数据包的组装时用于任何一层或者所有层上。

被动威胁的第二种形式与通信量分析安全性有关。如果一个侵入者可以阅读数据包头，即使消息是加密的，他也可以得知数据的源地址和目的地址，然而使用链路加密，这种可能性可以降低或消除。加密只可能限制阅读头信息和消息，需要的信息可以从通信量分析本身得到。例如，可以得到进入或离开某个中间节点的通信总量，加密不能解决这个问题。一个可能的对策是，通过生成持续的随机数流或密文流来填充通信链路，因而一个侵入者很难区分有用的数据与噪声，这样使计算实际的通信总量十分困难或根本不可能。

（二）主动威胁

人们可以预感到，主动威胁通常要比被动威胁更加严重，因为主动威胁常常要有意地改动数据控制信号，或者有意地生成伪造的数据，主动威胁并不是简单地读取数据信号的内容。如果信息流被严重地改变了，显然会要导致损失，不过主动威胁是否一定要比被动威胁更加严重，还要看发生威胁所造成损害的程度。贸易机密或国防机密的失窃，即便是没有任何改动，也会造成巨大的损失。对于主动威胁来说，人们所关心的问题是：消息服务的破坏、假冒和消息流的修改。

主动侵入可以发生在通信路线上几乎任何一处，电缆、微波链路、卫星信道、路由节点、主机或客户计算机系统都可能成为主动侵入的对象。除非投入巨大的资金用于安全性，例如像在军事建设中所做的那样，否则，对整个线路设置广泛防范的物理设施是不可能的。事实上，即使在军事机构中，百分之百的保护也是不可能的。然而，无论用何种方法，主动威胁只有在可以实现物理访问时才能进行。在这种情况下，人们对“物理”的理解应该广泛一些，因为物理访问可能是在几百英里之外的一个目标通过拨号访问终端进行的，或者也可能是某个远程目标通过无线电信道进行的。线路刺探甚至并不需要有一台设备和电缆进行物理的连接，线路刺探是一种与通信线路进行非授权的连接以获取对数据进行非法访问的行为。因此可以想像，阻止主动侵入是非常困难的，挫败主动侵入的安全性目标应该是迅速检测和恢复由于这种侵入造成的系统瓦解和延误。

一个通信系统所面临的最明显的主动威胁或许是这样一种侵入，这种侵入可以破坏或者延误大部分以至全部信息。在现代信息社会里，发生这样的事件很容易导致大量资金的损失，甚至更严重。任何对于大部分消息具有潜在的破坏或实际的延误的行为都构成主动威胁。

另一种主动干扰网络的更加巧妙的办法是通过假冒进行的。假冒是一种通过假装成授权的客户或主机来获得对系统访问的企图。在这种情况下，侵入者假装成一个真正的主机、开关、路由器或类似的设备，旷日持久地等待与对等用户进行通信以获得数据或服务。努力假装成一个真正的用户是一种旧式的、没有道德的行为，目的是使目标系统真正相信正在与他进行通信的确实是他所希望的主机或客户所做的。假冒作为一种技术，既可以用于被动目的，也可以用于主动目的。它之所以被说成是“主动威胁”是因为他的目的常常是干扰破坏性质的。

主动威胁的第三种方法是通过对消息流的修改进行的。在这种情况下，入侵者可能有选择地修改、删除、延误、重排序以及复制真正的消息或插入虚假的消息。如果阻碍了数据分组中 CRC 差错校验码的传输，即使是加密的消息也可能受到破坏。用于传输的数据包是由协议软件形成的，它需要有一个或多个循环冗余校验和，该校验和要经过发送方的计算和接收方的再计算，如果发送方和接收方的校验和不同，通常需要重传该数据包。用与此类似的方式，可以在加密以前对消息内容的明文生成一个操作检验码（MDC）。这样即使数据包被改动，但是却通过了差错纠正测试。然而，明文的实际加密也会有充分的变动以形成一个不同的校验和。 MDC 是检测消息流修改的一种方式，存在几种不同的校验和可用于该目的，这种方法被称为 MAA（信息鉴别算法）。

二、安全性服务

安全性服务是一种活动，它用于增强信息系统和一个组织的信息传输的安全性。在 OSI 模型中，定义了 5 组服务：机密性、鉴别、完整性、无拒绝和访问控制。在一个分层通信体系结构中，例如在 OSI 模型中，安全性几乎可以建立在任何地方。OSI 安全性体系结构更加明确，它规定了每一层要提供的特定服务。安全性服务与 OSI 各层之间的关系，可参见表 1-1.

表 1-1　OSI 各层中安全性服务的位置

OSI 各层	机密性	通信流量的机密性	鉴　别	完整性	无拒绝	访问控制
应用层	Y	Y	Y	Y	Y	Y
表示层	Y	Y	Y		Y	Y
会话层						
传输层	Y		Y	Y		
网络层	Y	Y	Y	Y		Y
数据链路层	Y					
物理层	Y	Y				

机密性保证数据不能被非授权的个人、实体或进程所利用。一般来说，这种服务可以提供一种机制保护数据免遭被动侵入。机密性概念可以应用于整个消息或者消息内的字段中，在后一种情况中经常采用选择字段机密性这一术语。通信协议是使用面向连接的服务，还是使用无连接的服务对数据机密性会产生不同的影响。面向连接的服务建立一个虚拟连接，对用户来说好像有一条实际的端到端的电路，这种服务有时称为虚拟电路或虚拟连接。与面向连接的服务对象相对的是无连接服务，无连接的服务是一个服务类，它并不建立一条虚拟的或逻辑的连接，也不保证数据单元一定以特定的顺序传送，无连接的服务是灵活的、健壮的并且提供无连接的应用支持。无连接的应用需要路径服务，但是不需要面向连接的服务。

鉴别可以保证接收到的数据是真正的、与它被发送时是一致的，并且发送数据的源方是正确的。鉴别还包括对诸如远程终端上的人员、消息的改变者等人员身份的核实。数据源鉴别要确认所收到的数据的源方是否是所要求的。对等实体鉴别要确认所关联的对等实体是否是所要求的。OSI 比其他文件更加清楚地强调了这个问题，在 OSI 中，鉴别特指证实接收的数据就来自所要求的源方。数据源鉴别连同无连接的服务一起操作，而对等实体鉴别通常与面向连接的服务一起操作。在其他文件中，鉴别的思想可能和数据完整性混为一谈，但是在 OSI 中，这两者是泾渭分明的。

数据完整性可以保证数据不被以非授权的方式改变或破坏。数据完整性和鉴别这两个方面的概念结合得非常紧密，即便在 OSI 中也是如此。这种结合还延伸到用以支持服务的机制中。从表 1-1 中可以看到，相同的机制用于这两种服务。此外，这两种服务通常被同时要求。数据完整性和鉴别这两个方面都很强地依赖于把加密作为主要手段的安全机制。

与鉴别一样，数据完整性服务可以应用于整个消息，也可以应用于选择的字段上。根据消息的传输是按照面向连接的服务方式，还是无连接的服务方式，完整性问题有所不同。如果是用于面向连接的协议，那么数据完整性机制是以恢复机制的形式提供的。

通信实体之一涉及到通信拒绝，全部或部分地无法通信，称之为拒绝。与拒绝相对立，OSI 体系结构定义了一种安全性服务，称为无拒绝。这种服务可以以两种形式提供：起始点验证和传送验证。一种可以提供这两种形式的无拒绝的机制，是通过使用数字签名来实现的。数字签名是一个数，它依赖于消息的所有位以及一个保密密钥，可以使用一个公用密钥来检验数字签名的正确性（与鉴别不同，鉴别使用一个保密密钥来进行检验）。用于提供起始验证和传送验证的第二种机制，是通过由可信赖的第三方提供公证来实现的。

最后，访问控制可以用于通信的源方或目的方，或者沿线路上的某一地方。访问控制可以保护网络不被敌方访问信息服务。访问控制典型地发生在应用层，不过也可以在传输层或网络层中实现。有时希望访问控制为子网提供保护，使只有授权的实体才能够访问该子网，服务于传输层中的访问控制可以处理这一问题。

三、安全性机制

在前面讨论安全性服务时，人们已经遇到了许多安全性机制。安全性机制是操作系统、硬件和软件功能部件、管理程序以及它们的任意组合，用于为一个信息系统的任一部件来检测和防止被动与主动威胁。安全性机制与安全性服务有关，机制是用于实现服务的程序，OSI 定义的安全性服务与选择的机制之间的关系可参见表 1-2。例如，“机密性”服务可以通过使用加密、通信量填充和路由控制来实现。另一方面，“加密”不但可以是实现机密性服务的成分，而且还可以是“完整性”和“鉴别”服务的成分。

表 1-2　安全性服务与机制

服务	加密	数字签名	访问控制	数据完整性	鉴别	通信量填充	路由控制	公证
机密性	Y					Y	Y	
完整性	Y	Y		Y				
鉴别	Y	Y			Y			
访问控制			Y					
无拒绝		Y		Y				Y

在表 1-2 所示的各种安全机制中，加密有着最广泛的应用，并且可以提供最大程度的安全性。加密机制的主要应用是防止对机密性、完整性和鉴别的破坏。在一个通信环境中，可以通过口令使一个具有确定身份的人使用个人计算机或连接到主机的终端，这样的系统可以提供高度的安全性，甚至在一个拨号线路上也可以实现这一点。为数据的传输和存储建立加密系统耗费了人们巨大的精力。虽然文件本身可能是脆弱的，但是那些没有密钥的人是不可能访问数据的内容的。

有一些数字的鉴别技术可以用于网络安全中。在网络安全中，鉴别的范围可以是非常广泛的。鉴别从数据输入一直延伸到信息安全到达目的方。数据输入可以通过使用校验和

来校验，校验和是一个数据项的集合的和，可以用于差错校验。校验和也可以是一个若干数字或位的和，用于校验数据的完整性。循环冗余校验常常用于鉴别数据传输中发生的偶然差错。循环冗余校验是一个算法，它生成一个校验字段用于鉴别数据传输中可能发生的差错。然而，系统经常需要有更高的安全性，这时可以使用保密参数来校验数据的完整性。ISO 已经认识到需要有多种鉴别，从而导致几种鉴别算法或方法的发展，这些算法或方法中包括十进移位与相加（DSA）以及消息鉴别算法（MAA）。

数字签名是用于鉴别的一种日益重要的技术。数字签名是一个数，它依赖于消息的所有位以及一个保密密钥，它的正确性可以使用一个公开密钥来检验（作为对比，鉴别需要一个保密密钥来进行检验）。数字签名可以用于鉴别的目的，并且可以用于完整性服务和无拒绝服务。数字签名用于无拒绝服务时，是和公证一起使用的。公证是通过可信任的第三方来验证（鉴别）消息的，这种公证在逻辑上与传统的公证程序是相似的，只是在这种情况下公证通常是自动的程序。

对网络终端用户来说，最通常的安全性经历是通过使用口令来实现访问控制。口令是一个字或字符串，它是惟一的，用来对身份进行鉴别。在获得对数据的访问之前，通常要求一个程序、计算机操作员或者用户提交一个口令，以满足安全性要求。口令是保密的，与用户标识不同，用户标识常常为许多人知晓，如电话号码。口令也可以叫做通行字，口令系统常常会被人破译。与口令有很近的亲缘关系的是问卷，问卷是一种鉴定身份的方法。它使用授权的用户所知道的但不大可能被其他人知道的信息，例如询问用户亲属的名字，这是一种常见并且应用很广的例子。问卷的优点是它使用了记忆中的信息，缺点是要进行相当长的对话。

还有各种用于身份鉴别的产品，使用了比这里介绍过的方法更好的技术。例如，广泛出现的卡片系统，通过标记来进行鉴别。还有一些比较声音、手写签名、指纹的系统，上述技术都可以找到某些应用，但实现起来会增加花费。

实现安全性的一个更好的办法是把敏感的数据及对该数据的询问隔离在“专用的”并发网络中，使用另外的通信协议，同时采用加密和回叫技术。回叫系统通常是以直通方式实现的，这种系统使用特殊的调制解调器或者使用计算机在用户正常注册到一个应用之后，切断与用户的连接，然后将用户叫回到一个或多个授权的终端，在这些终端上用户可以访问和应用。然而，与许多其他的安全性系统一样，回叫技术也容易受到暗中破坏的攻击。还有一些有关的先进通信技术，如电话系统中的传呼转发，也与安全性系统有联系。

四、网络安全系统

决定网络在何处开始，是考虑如何适应网络安全性要求这个问题的一部分。常规确定网络构成的方法对这一问题并没有太多的帮助。通信网络可以定义为由设备和传输介质（无线电、电缆、光缆等）的全体组成的网。这些设备和传输介质对于在由通信信道连接的一串点上发送和接收信息是必要的。计算机网络是通过通信网络链接起来的一台或多台计算机，或者是互连的计算机系统与终端组成的一个系统。观察图 1-1，就会发现上述定义过于面向硬件了，因而，可以建议修改后的信息网络的定义是：由通信信道连接的一串点，其目的是通过一致的协议栈来发送和接收信息。

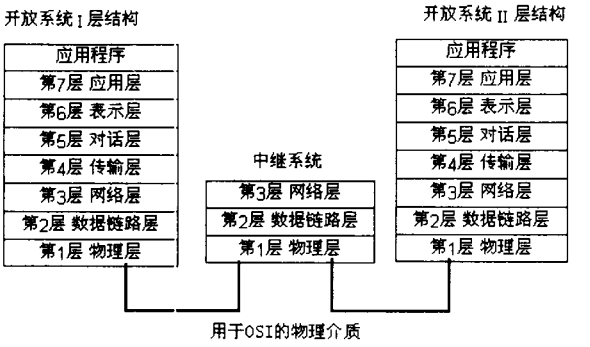

图 1-1　OSI 标准网络

如图 1-1 所示是一个简化的 OSI 网络，它包括三个点，两个是全开放系统，一个是中继。全开放系统可以是常规的通用计算机，或者也可以是特殊的控制设备。然而，这一模型的关键在于网络并不是在物理介质与计算机之间的调制解调器处结束的，而是在 OSI 协议栈的应用层结束的。物理介质可以是 LAN 的一部分、WAN 的一部分或者是两者混合体的一部分。此外还应该存在用于每个开放系统的操作系统（OS）、OSI 协议栈以及由 OS 和 OSI 协议栈支持的用户程序。与此类似，IBM 的 SNA 网络中不仅要有物理介质加上 3270 显示系统设备，而且要有适当的前端处理器（DEP）以及配套的软件，诸如 VTAM 之类的访问方式软件，还有实际使远程用户进行工作的远程处理（TP）监视器。TP 监视器上的硬件加上 SNA 协议才是严格意义上的网络组成部分。大型计算机通常并不是按照上面所述的逻辑来组织的，但是这些描述无疑都是正确的。

在 OSI 中，虽然某些安全性服务可以从 OSI 模型的几乎所有层提供，但是，全部的网络安全性服务都可以由第 7 层（应用层）来处理，信息的加密和解密基本上发生在第 6 层（表示层）中，指定的通信对象的鉴别发生在第 7 层（应用层），当然也可以发生在其他层上。

五、安全性措施的效果

信息安全性的缺乏成为互联网中的一个严重的风险，这一点在有关网络技术的刊物上有着广泛的讨论。有些链路供应商正在销售用于控制用户访问微型机与大型机应用的系统。因此用户在购买微型机—大型机软件包时，应该考虑安全性选择。一个适当的软件包应该在数据库级和终端或微型机级这两级上提供安全性。通常的安全性措施应该包括对用户注册和用户改变口令的安全性支持。

根据有关材料说明，广泛的组织计算产生了非法侵吞机密数据的极大可能性，这种侵吞可以通过把机密数据从驻留大型机的文件中拷贝到个人计算机的磁盘中实现。随着微型机数量的膨胀和远程访问技术的发展，使得数据安全性越来越成为人们所关心的问题。

此外，还有其他一些没有解决的安全性问题。首先，实际上任何一种安全措施对于该措施所保护的系统的性能都有着不利的影响。其次，有很多用户反对安全性措施，因为这些措施使得网络更加难用，用于大型机系统的传统的安全性程序使许多用户感到厌烦，因而他们坚持先把这些安全性程序移到微型机上，然后才移到部门 LAN 环境中。因为安全性的特点主要是把人排斥在外，而不是使人轻易进入。

第五节　网络安全的研究对象

计算机网络安全研究的对象主要内容包括保密性、安全协议设计和接入控制。

一、保密性

为用户提供安全可靠的通信是计算机网络最为重要的内容。尽管计算机网络安全不仅局限于保密性，不能提供保密性的网络肯定是不安全的。网络的保密性机制除为用户提供通信保密之外，也是许多其他安全机制的基础，如访问控制中登录口令的设计、安全通信协议的设计以及数字签名的设计等，为了实现这些设计都离不开密码的机制。

二、安全协议设计

计算机网络的安全协议是网络安全的一个重要方面。如为了防止假冒问题，就需要一种对等实体鉴别协议。如果网络通信协议存在通信安全上的缺陷，那么攻击者就可能不必攻破密码体制即可获得所需要的信息或服务。人们一直希望能够设计出安全的计算机网络系统，但不幸的是，系统的安全性是不可判定的。目前安全协议的设计方面，主要是针对具体的攻击设计安全的通信协议。这又引出一个问题，如何保证一个协议的安全性？协议安全性的保证通常有两种方法：一种用形式化来证明一个协议是安全的，另一种是用设计者的经验来判定的，所以对复杂的通信协议的安全性，目前主要采取找漏洞的分析方法。当然，也可以开发一些人工智能工具来辅助分析。对于简单的协议，可以通过限制攻击者的操作来对一些特定情况进行形式化的证明，但这种方法有很大的局限性。

三、接入控制

接入控制（Access Control）也叫做访问控制。计算机网络的一大优点就是能够资源共享，用户可通过网络来共享系统提供的各种资源。但如果这种接入是没有什么限制的，这将带来许多安全问题。所以有必要对接入网络的权限加以控制，并规定每一个用户的接入权限。由于网络是一些地理上分散的计算机系统通过通信线路互相连接起来的一个更为复杂的系统，它的接入控制机制比操作系统的访问控制机制更复杂，尤其在高安全性级别的多级安全性（multilevel security）情况下更是如此。

第六节　网络安全与级别

计算机网络安全的工作，美国与加拿大做得比较早，效果也不错。他们的安全标准都制定了 4个级别和 7个级别。现分别叙述如下。

一、美国计算机安全级别

美国计算机安全标准是由美国国防部开发的计算机安全标准，可信任计算机标准评估规则（Trusted Computer Standards Evaluation Criteria）黄皮书（Orange Book）。

这些级别均描述了计算机不同类型的物理安全、用户身份验证（authentication）、操