第 1 章　计算机网络安全

随着计算机技术、网络技术以及信息技术的迅猛发展，计算机网络与人们工作和生活的联系也愈来愈紧密。通过网络，人们可以和远在天涯的朋友互发函件；通过网络，人们可以浏览世界各地的报刊杂志，搜索自己所需的信息……。但与此同时人们也发现自己的计算机系统不断的受到侵害，其形式的多样化，令人防不胜防，给有关部门造成了巨大的损失。因此，为使计算机系统和计算机网络系统不受破坏，提高系统的安全性已成为必须解决的问题。因此，每个计算机用户都应该掌握一定的计算机网络安全技术以使计算机系统长时间、安全、稳定地运行。

1.1　网络安全的概念

计算机网络安全问题是一个错综复杂的问题，它涉及到系统故障以及有意或无意的破坏等。为了确保计算机网络安全，需要采取物理措施、管理措施和技术等多方面措施。

计算机网络安全的保护对像主要是数据、资源和声誉。

1.1.1　数据

数据有 3 个独立的特征：保密性、完整性和可用性。其中保密性是头等重要的。每个单位的计算机系统里都会储存一些重要数据，如军事行动计划、产品的设计和配方、财务记录、人事档案等。有高度机密数据的机器很容易在网上被识别出来，换句话说，“黑客”很容易发现想要攻击的目标。

对于那些不需要保密的数据，还要考虑数据的完整性和可用性。如果数据文件被删除一部分，则该数据文件一般不能用，如果数据文件被篡改，则数据文件一般情况下绝对不可用。有时，数据不得不重建，但有时它们是不可重建的，这是因为有些数据是不可复得的。

无论是丢失数据还是数据被篡改，都会使系统遭受损失，有些损失则是在短时间内无法补救的，甚至永远无法补救，这些损失包括其他人对系统管理者的信任和对其所属机构的信任。

1.1.2　资源

这里所说的资源是指计算机网络的硬件资源和软件资源。大多数用户都想单独使用自己的计算机或向其他的使用者收费使用，对于后一种情况，管理者则需要承

担安全性方面的责任。

入侵者绝非善意的使用者，他们入侵是想完成某一任务，例如大量占用被入侵者的内存、磁盘空间或 CPU 运行时间等。当被入侵者在运行某一程序时，就会因以上原因而无法运行。

计算机的所有者在计算机资源上花费了大量的时间、精力及金钱，因此有权利决定怎样使用这些资源，这样就对计算机系统提出了安全问题的要求。

1.1.3 声誉

有时，入侵者会冒充被入侵者的身份出现在因特网上，做出被入侵者不知道的事情，而这些看起来好像是被入侵者所为。结果可能会导致其他站点或法律机构责问被入侵者为什么正在试图破坏他们的系统，其后果有时候是严重的并往往使被入侵者遭受损失。入侵者也会盗用被入侵者的名义发送电子函件邮寄新闻消息。一般情况下，这些入侵者是故意的，是不可信任的，但即使只有少数人相信，也必然要耗费大量的时间和精力消除其影响，被入侵者和所在机构的形象也可能会因此受到严重损害。

伪造电子函件新闻是很容易的。如果它产生于外部伪造站点，将容易被发现，但如果它来自于一个已经获取站点访问权的入侵者，那么它看起来确实像是被入侵者发的。外部伪造者不能访问的各种细节，一个入侵者却可以访问到这些细节，他可以获取被入侵者全部的电子函件列表，并可以知道被入侵者给谁发过电子函件。

此外，大多数的入侵者会企图将被入侵者的机器连接到其他机器上，这将使下一个受害者以为被入侵者是入侵者。许多入侵者也会利用被入侵者的站点散布盗版软件或色情内容，使被入侵者的名字与盗版、入侵和色情等相联系，要想恢复清白更是不容易的。

总之，网络安全的目的就是最大限度地保障计算机网络不受侵犯，使系统能够正常运行。

1.2 网络安全的目的和功能

1.2.1 网络安全的目的

计算机网络安全就是研究如何保障计算机资源的安全，即计算机的系统资源和信息资源的安全。影响计算机网络安全的因素主要有以下几种：

实体安全，即系统设备及相关设施运行正常，系统服务适时。包括环境、建筑、设备、电磁辐射、数据介质安全及火灾报警等。

运行安全，即系统资源和信息资源使用合法。包括电源、空调、人事管理、机房管理、出入控制、数据与介质管理、运行管理等。

数据安全，即系统的数据或信息完整、有效、使用合法，不被破坏和泄漏。包括输入输出数据安全、进入识别、访问控制、加密、审计与追踪、备份与恢复等。

软件安全，即软件（网络软件、操作系统资料）完整。包括软件开发规程、软件安全测试、软件的修改和复制等。

通信安全，即计算机通信和网络的安全。包括线路、传输、接口、终端与工作站、路由器的安全等。

1.2.2 网络安全的功能和措施

计算机网络安全问题是一个很复杂的问题，任何时候都不会有一劳永逸的解决措施。因为计算机的安全与反安全会一直地进行下去，故要使计算机网络具有较高安全性，需要将计算机系统的各种安全防护技术（如实体安全防护技术、防电磁辐射泄漏技术、硬软件防护技术、防火墙技术、数据保密变换以及安全管理与法律制裁等）结合使用，对计算机系统进行综合分层防护，从而提高计算机网络的整体防护水平。分层防护的原理见图 1-1,其中最外层是社会层，主要通过法律、管理、伦理道德教育等措施来减少犯罪几率；由外及内，分别是实体安全防护层、电磁防护层、硬软件防护层、通信和网络防护层、数据保密变换层等。

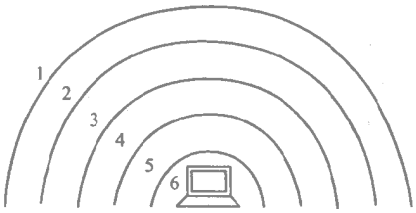

图 1-1 计算机及网络的分层防护

1—社会层 2—实体安全防护层 3—电磁防护层 4—硬软件防护层 5—通信和网络防护层 6—数据保密变换层

加强计算机安全管理的法规建设，建立和健全各项规章制度是保障计算机网络安全的重要一环。利用制定人员的管理制度，加强人员审查，在组织管理上避免单独作业，操作与设计分离等制度和措施降低了作案的可能性。

1. 实体安全防护

为了保障计算机系统的正常工作，首先是保护硬件环境，这包括不间断供电设备、空调、防静电设施和防火设施等。

建立物理屏障，阻止非法入侵者接近计算机系统是行之有效的防护措施。这些措施有进入识别、区域隔离和边界防护等。当今的进入识别技术有密码锁、磁卡等身份识别措施。为了防伪造，新型磁卡也称为“灵巧卡”带有智能化单片机（即微

处理器）。最近又出现了指纹识别、视网膜识别和语音识别等手段，这些手段有效的阻止了非法入侵事件的发生。以上所说的防护都属于边界防护的范畴。而所谓的边界防护是指设置障碍，构造安全警戒区等防护方法。

2. 软件安全环境防护

1978 年的美国佛罗里达计算机犯罪法是世界上第一部计算机犯罪法。首次将计算机犯罪定为侵犯知识产权罪。现在，计算机软件已列入知识产权的范畴，受到法律的保护。对计算机犯罪定罪和量刑产生的威慑力可使有犯罪企图的人产生畏惧心理，使计算机犯罪减少，有利于计算机网络的安全。

建立和健全计算机网络安全的各项规章制度，是保障计算机安全的有力措施。另外，加强道德教育对于计算机网络安全也十分重要。

3. 电磁防护

（1）电磁干扰和兼容　计算机是一种电子设备，在工作时向外辐射电磁波，同时又受到其他电子设备的干扰，这种干扰强到一定程度，就会影响计算机的正常工作。

电磁干扰有两种途径：电磁辐射和电磁传导。电子设备辐射的电磁波通过电路耦合引入到另一台电子设备中引起干扰。电磁传导是通过连接的导线、电源线、信号线等耦合而引起相互之间的干扰。

计算机及其元器件是在一定电磁干扰环境下工作的，所谓电磁兼容性就是电子设备或系统在一定的电磁环境下互相兼顾、相容的能力。如果设备的电磁兼容性很差，在电磁干扰的环境里就不能正常工作；如果是机载、弹载设备就会造成飞机、导弹失事。我国已将电磁兼容性作为强制性标准来执行。

（2）现代战争与电磁防护　现代战争的重要特征之一是改变了传统的靠硬武器决胜的观念，而广泛采用电子战等作战手段。即以电子侦察、电子伪装和电子攻击等手段，与地面行动相配合，硬杀伤与软杀伤相结合，形成协同作战的整体威力。海湾战争是这方面的典型战例。

从 1991年的 1 月 17 日开始到 1991 年 2 月 24 日的海湾战争中，由于以美国为首的多国部队事先采用了电子侦察、电子干扰和电子伪装，精确制导与反辐射武器，使伊军通信中断，指挥失灵。因此，在这场仅为 42 天的战争中，多国部队死伤 120 余人，而伊方死伤六七千人；多国部队损失飞机 43 架，而伊方损失 171 架；多国部队损失舰艇 2 艘，而伊方损失舰艇 50余艘，坦克 3000 多辆，装甲车 1800 多辆，大炮 2000 门。伊方工事和防线半小时被突破。

这个战例说明，以电子信号欺骗和电子干扰为主的软杀伤武器已走向战场。以打钢铁为主的战争正向以打芯片为主的战争转化，如果电子设备没有电磁防护功能，很难取得战争的胜利。

（3）电磁防护的措施　为提高电子设备的抗干扰能力，除在芯片、部件上提高抗干扰能力外，主要的措施有屏蔽、隔离、滤波、吸波和接地等，其中屏蔽是应用最多的方法。

电磁波经封闭的金属板之后，大部分能量被吸收、反射和再发射，最终传到板内的能量就很小了，这样内部的设备或电路就免受强电磁干扰从而得到保护。

滤波是另一种重要的方法。滤波电路是一种无源网络，它可让一定频率范围内的电信号通过而阻止其他频率的电信号，从而起到滤波作用。在有导线连接或阻抗耦合的情况下，进出线采用滤波器可阻止强干扰。

吸波是采用铁氧体等滤波材料，在空间很小的情况下起到类似滤波器的作用。

隔离是将系统内的电路分别处理，将强辐射源、信号处理单元等隔离开，单独处理，从而减弱系统内部和系统向外的电磁发射。

接地对电磁兼容来说十分重要。它不仅可起到保护作用，而且可使屏蔽体、滤波器等集聚的电荷迅速排放到大地，从而减小干扰，作为电磁兼容要求的地线需单独埋放。

（4）计算机的信息泄漏　1985 年在法国举办的“计算机与通信安全”国际会议上，荷兰的一位工程师现场演示了用一套稍加改装的设备和黑白电视机还原 1Km 以外的机房内计算机显示屏上的信息。这说明计算机的电磁辐射造成信息泄漏的危险是存在的。

计算机信息泄漏主要是通过传导发射和向空间的发射、辐射传播出去的。由信息泄漏得到的情报比其他方式更为隐蔽、准确和及时，也更为危险。

美、俄等国经多年研究，研究出了“抑制信息处理设备的噪声泄漏技术，简称信息泄漏防护技术（TEMPEST 技术,美国 NACSIM5100A）。20 世纪 80 年代以来，美国市场上陆续出现了一种符合 TEMPEST 标准的军用通信设备，并逐步形成商品化、标准化生产。

TEMPEST 技术是综合性很强的技术，包括泄漏信息分析、预测、接收、识别、复原、防护、测试和安全评估等项技术，涉及到多个学科领域。它是在传统的电磁兼容理论的基础上发展起来的，但是比传统的抑制电磁干扰的要求要高得多，其技术实现上也更复杂。它所关心的是如何避免泄漏出有用的信息，即红信号。一般认为显示器的视频信号，打印机打印头的驱动信号、磁头读写信号、键盘输入信号以及信号线上的输入输出信号等为红信号，须重点保护。

电磁防护层主要是通过种种措施，提高计算机和电磁兼容性，提高设备的抗干扰能力，以使计算机能抵抗强电磁干扰，同时将计算机的电磁泄漏发射降到最低，不致将红信号泄漏出去。

4．硬件软件防护

（1）硬件防护　硬件是指计算机系统的物理构成，硬件防护一般是指在计算

机硬件上采取措施或通过增加硬件来防护。具体措施有为计算机加锁、加专门的信息保护卡，例如防病毒卡、防拷贝卡、加插座式的数据变换硬件和安装在并行口上的加密狗等。

（2）软件防护　软件防护主要指通过计算机软件提供安全防护功能。系统软件是软件的重要组成部分，计算机系统的安全在很大程度上依赖于操作系统本身的安全和它为系统提供的安全防护功能。近年来按照可信计算机安全评估准则（TCSEC）的要求进行安全操作系统的改进，在安全防护方面增加了许多功能，有效地提高了系统的安全性。传统的 UNIX 操作系统经重新设计安全内核，达到了 B 级安全标准。

操作系统提供的安全防卫功能主要有个人身份鉴别、存取控制授权矩阵、隔离控制和监视程序控制等。这几种方法主要用于访问控制和系统隔离，系统要判定用户是否合法，享有何种特权，对计算机资源可进行什么类型的访问操作（读、写运行等），同时规定用户与信息密级和资源类型相适应的授权。另外，通过软件使系统隔离，避免安全隐患的扩散，从而保证信息系统的安全。

在国内外使用很普遍的防病毒软件是软件防护的一个例子。绝大多数网络系统均装有这类防护软件，一开机先扫描，通过后再继续执行。一旦有外来盘插入使用，要先详细检查，无问题后方可进入。

5. 计算机通信及互连网的安全防护

（1）通信安全　计算机通信安全主要包括：线路安全、传输安全、数据保密变换、辐射安全、技术安全和终端安全。内部和外部通信线路是敌对势力窃取信息的重要目标。为保护线路安全，除采取物理防护措施外，还可采用报警等技术措施。

数据传输必须安全可靠，为此，对传输初始化、测试、校验和纠错等有一系列要求。对注册、语言保密和通信量分析等也要采取相应措施。

网络特别是因特网更加开放，有些防护措施，对网上站点、网上主机和工作站是适合的，而对于互连网上的内部网的安全，则应有更完善的技术手段来保证。

（2）互连网的安全　防火墙是适应互连网的发展而出现的一种安全防护技术，它是内部网和外部网之间实施安全防范的系统，也是一种访问控制机制。防火墙通常安装在被保护的内部网与互连网的连接点上。从互连网或内部网上产生的任何活动都必须经过防火墙，并由防火墙来确定这些活动是否可以接受。

防火墙的防护规则是：一切未被允许的就是禁止的；一切未被禁止的就是允许的。

6. 密码技术

密码技术又称为数据保密变换，它是计算机系统对信息进行保护的最可靠方法。

密码保护层是计算机安全防护的最内层也是最重要的一层。物理环境防护，电磁防护，硬件和软件防护，通信和网络防护，可阻止了大部分入侵事件，但它不是万无一失，仍有个别入侵会成功，故计算机系统仍存在着隐患。通过密码技术可将信息屏蔽起来，虽然极少数人可窃取到信息，但由于密码技术的保护，使这些加密信息很难识别，即使可以识别，也因要花极大的代价而无实际意义。

密码设计的基本思想是伪装信息，它使无关人员无法理解信息的真正意义。密码设计的核心是密码算法和密钥。密码算法是一些公式和运算关系等，密钥是算法中的可变参数。改变了密钥也就改变了明文和密文之间的数学关系。所谓加密就是将明文变成密文，而解密是将密文恢复为明文。

对于密码算法来说，衡量其好坏的尺度是保密强度。如果总推不出明文，此算法即为理论上不可破译。如果推出明文需在时间和经济上付出不可能付出的代价，则此算法实际上不可破译。

现代密码学的一个基本原则是：一切秘密寓于密钥之中，加密算法可以公开，密码设备可以丢失，但密钥绝对不可丢失。

7. 网络安全服务

网络安全服务是主要的安全防护措施。下面是五种通用的安全服务。

（1）认证　认证服务提供了关于某个实体（人和物）身份的保证，某个实体声称具有一个特定的身份时，认证服务将提供某种方法来证实这一声明是正确的。口令是一种提供认证的常用方法。

认证是一种重要的安全服务。它是其他安全服务的第一关。认证是对付假冒攻击的有效方法，它分为两种情形：

1）身份由参与某次通信连接或会话远端的一方提交。这种情况下的认证服务称作实体认证。这种认证只是简单地认证实体本身的身份，不会和实体将要进行什么活动联系起来。因此，它的作用是有限的。在实际工作中，实体认证通常会产生一个明确的结果，允许实体进行其他活动或通信。例如，在实体认证过程中将产生一个对称的密钥，可以用来解密一个文件进行读写，或者与其他实体建立一个安全通信通道。实体身份一旦获得认证，就可以和访问控制列表中的权限关联起来，决定能否进行访问。

2）身份是由声称它是某个数据项的发送者的那个实体所提交的。此身份连同数据项一起发送给接收者。这种情况下的认证服务称作数据起源认证。它认证某个指定的数据项是否来源于某个指定的实体。它不是孤立地认证一个实体，也不是为了允许实体执行下一步操作而认证他的身份，而是为了确定被认证的实体与一些特定数据项之间不可分割的联系。

在达到基本的安全目标方面，上述两种类型的认证服务都具有重要的作用。其中数据起源认证是保证部分完整性目标的直接方法，即保证知道某个数据项的真

起源。

实体认证的一个重要实例是人员认证，即对处于网络终端上的某个人进行认证。需要特别指出的是，在某个终端上，不同人员之间容易互相替代。在区分单个人方面，可以采用一些特别技术。

（2）访问控制　访问控制就是拒绝未授权者对计算机网络的任何资源进行访问。未授权访问包括未经授权的使用、泄漏、修改、销毁以及颁发指令等。访问控制直接支持机密性、完整性、可用性以及合法使用的安全目标，它对机密性、完整性和合法使用所起的作用是十分明显的。它对可用性所起的作用取决于对以下几种用户进行有效的控制：

1）影响网络可用性的网络管理指令的颁发者。

2）滥用资源以达到占用资源目的的人。

3）可以用于拒绝服务攻击信息的获得者。

访问控制既是通信安全的问题，又是计算机操作系统的安全问题。由于必须在系统之间传输访问控制信息，所以它对通信协议具有很高的要求。访问控制的一般模型假定一些主动的实体，称为发起者或主体。他们试图访问的一些资源，称作目标或客体。

授权决策控制着哪些发起者在何种条件下，为了什么目的，可以访问哪些目标。这些决策以某一访问控制策略的形式反映出来。访问请求通过某个访问控制机制而得到过滤。一个访问控制机制模型由实施功能和决策功能两部分组成，OSI 访问控制模型（ISO/IEC10181-3 标准）就使用了这些概念，如图 1-2 所示。实际上，这两个组成部分的物理构成可能差别很大。通常，某些构成是将两个组成部分放在一起的，然而，在这些组成部分之间常常要传输访问控制信息，访问控制服务为这一通信提供了保证。

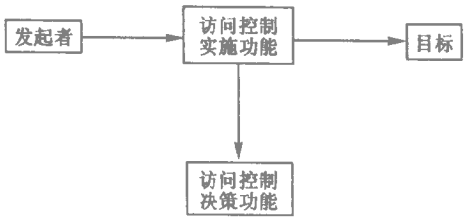

图 1-2　访问控制模型的基本组成

访问控制的另一个作用是保护敏感信息不经过有风险的环境传送。这涉及到对网络的业务流或消息所实施的路由控制。所谓路由控制是指选路规则，选择或绕过指定的网络、连接或中继。访问控制服务的深入讨论依赖于两个因素：访问控制策略的类型和各组成部分的物理构成。

（3）机密性　机密性服务就是保护信息不泄漏或不暴露给那些未授权的人或

组织。

在存储和通信中的某一数据项构成了某种形式的信息通道。然而，在计算机通信环境中，它不是惟一的信息通道，其他信息通道包括以下几种：

1）观察某一数据项的存在与否。

2）观察某一数据项的大小。

3）观察某一数据项的动态变化（如数据项内容、存在、大小等）。

例如，“导弹已经发射”的信息可用下列的任何一种方法故意或无意地传送。

1）用 1 比特数据项：1 表示“导弹已发射”，0 表示“导弹仍未发射”。

2）在某一文件目录中，名为“导弹发射报告”的文件存在与否。

3）利用包含导弹发射记录的表的大小。

4）通过观察导弹发射的英里计数器继续增加的事实。

要达到保密的目的，就必须防止信息通过这些信息通道被泄漏出去。在计算机通信安全中，应注意区分两种类型的机密性服务：数据机密性服务（例如，使用加密手段）使得攻击者想要从某个数据项中推出敏感信息是十分困难的；业务流机密性服务使得攻击者想要通过观察网络的业务流来获得敏感信息也十分困难。

根据对什么样的数据项进行加密，数据机密性服务又可分成几种类型，其中重要的有以下几种。

1）连接机密性服务，它是对某个连接上传输的所有数据进行加密。

2）无连接机密性服务，它是对构成一个无连接数据单元的所有数据进行加密。

3）选择字段机密性服务，它仅对某个数据单元中所指定的字段进行加密。

（4）完整性　完整性服务是对安全威胁所采取的一类防护措施，这种威胁就是以某种违反安全策略的方式，改变数据的价值和存在。改变数据的价值是指对数据进行修改和重新排序；而改变数据的存在是指新增或删除它。无论哪种威胁都有可能导致严重后果。考虑一台与其控制银行进行通信的自动提款机（ATM）。如果完整性考虑得不周全，可以想像在通信联系中可能会有人通过插入他自己的设备采用各种手段进行破坏：

1）首先修改从 ATM 传到银行的提取请求消息中的提取现金数量（如将￥100 改为￥10），然后修改从银行到 ATM 的认可消息中的数量（修改到原来的数量￥100），这样就使得 ATM 支付出的数量比记录在银行的贷款的数量多。

2）重复先前的 ATM 的提取物理过程，不通过银行重复先前的 ATM 的传输记录来作出所有回答。这样，ATM 就又支付了一次，而在银行没有贷款。

3）在从 ATM 到银行的支付阶段产生一条消息“取消传输——现金支付失败”（即使现金已被成功地支付）。

4）删除所有从银行到 ATM 的黑名单（BLACK-LIST）通知，然后在离线的时间里用一个空卡进行提取。

与机密性服务一样，数据完整性服务的一个重要特征是它的具体分类，即对哪

些数据采用完整性服务，它有以下三种重要类型。

1）连接完整性服务。它是对某个连接上传输的所有数据进行检验。

2）无连接完整性服务。它是对构成一个无连接数据单元的所有数据进行完整性检验。

3）选择字段完整性服务。它对某个数据单元中所指的字段进行完整性检验。

所有的完整性服务都能对付新增或修改数据的企图，但是它不一定都能对付复制和删除数据。复制是由重放攻击造成的。无连接和选择字段完整性服务主要是为了检测对部分数据的修改。连接完整性服务要求能够防止在某一连接内重放数据，但它仍然存在弱点。因为某个入侵者可能重放一个完整的连接。检测对某些数据的删除至少与检测重放攻击一样难。因此在说明一种数据完整性服务时要特别注意。

一个完整性服务也许会提供“恢复”的选择。在这种情况下，当在某个连接内检测到完整性被破坏的时候，该服务将试图“恢复”数据。例如，通信将返回到某一检测点并重新开始。

（5）非否认性非否认服务与其他安全服务有根本区别，其主要目的是保护通信用户免遭来自系统中其他合法用户的威胁，而不是来自未知攻击者的威胁。“否认”最早被定义成一种威胁，它是指参与某次交换的一方事后不诚实地否认曾发生过本次交换。非否认服务就是用来对付这种威胁的。

事实上，非否认服务并不能消除服务的否认，也就是说，它并不能防止一方否认另一方对某件已发生的事情所作出的声明。它所能够做的只是提供无可辩驳的证据，以支持快速解决任何这样的纠纷。

非否认服务的出发点并不是仅仅因为在通信各方之间存在着相互欺骗的可能性。它也反映了这样一个现实，即没有任一个系统是完备的，而且也可能出现通信双方数据最终达不成一致协议的情况。

纸文件（如合同、报价单、标书、订单、货运清单和支票等）在商业活动中发挥着巨大的作用。然而在对它进行处理的进程中，会发生许多问题。例如：邮递过程中的文件丢失，收信者在作出处理之前将收到的文件丢失，在某一机构内部或在机构间的文件传递活动被收买，伪造文件，有关某个文件有争议的签署日期等等。

为了系统地处理以上所出现的问题，采用了许多不同的机制，诸如签名，公证签名，收据邮戳以及挂号邮件等。

在进行电子化商业活动时，情况与此类似。非否认服务提供了保护机制。因为在电子化处理文件时，常常涉及更多的人，所以在某些方面，电子化作业所出现的问题比纸张作业所出现的问题更难以解决。由于采用了较为复杂的数据签名技术。使得电子作业所出现的问题反而更容易解决。

原则上，非否认服务适用于任何一种能够影响两方或更多方的事件。通常，这些纠纷涉及某一事件是否发生了？是在什么时候发生的？有哪几方参与了这一事件以及与此事件有关的信息是什么？在数据网络环境下，非否认服务可以分为以下两

种不同情况：

1）起源的否认。这是一种关于“特定的某一方是否产生了某一特定的数据项”的纠纷或关于产生时间的纠纷。

2）传递的否认。这是一种“某一特定的数据项是否被传送给某特定一方”的纠纷及关于产生时间的纠纷。

1.3 网络安全的潜在威胁

1.3.1 安全威胁的基本概念

安全威胁是指某个人、物、事件对某一资源的机密性、完整性、可用性或合法性使用所造成的危害。

安全威胁可以分为故意威胁和偶然威胁，所谓偶然威胁是指由偶然因素造成的威胁（如信息被发往错误的地址）。而故意威胁又可进一步分为被动威胁和主动威胁，被动威胁是只对信息进行监听（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中货币的数量）。

1. 被动威胁

被动威胁不改变系统中的数据，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，被动威胁留下的痕迹很少，或者根本没有留下痕迹，因而很难发现被动威胁。然而，被动威胁通常是可以预防的，而且预防也是对付这种威胁的基本手段。

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，或者通过读数据包头（通信量分析）以确定信源方和目的方的位置和身份两个方面。当然，如果一条信息已经存放在主机系统的文件中，那么被动威胁可能导致入侵文件系统来获取已经存储的信息。

对付被动威胁的重要方法是采用加密技术。如果没有解密密钥，所获取的信息是看不懂的。加密是通过使用代码和密钥来实现的，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的每一个词和句子。而密码使用一个算法将数据信息译成难以破解的密文，密码技术容易实现自动化，因而常常被计算机网络系统所采用，常规的加密法是将原始数据换成难懂的密文，要实现这一转换，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。发送方和接受方都要拥有密钥，因此，密钥的管理十分重要，密钥必须有足够的复杂度，以防从密文中破解信息。

对于网络而言，有两种基本的加密方法：链路加密和端到端加密。链路加密是指数据加密独立于通信链路。链路加密的优点是整个分组（包括分组头信息）都被

加密，因而传输的是密文，其缺点是中间接点的数据是明文，由此产生了接点安全性的问题，用户很难甚至根本无法控制其安全性。端到端的加密发生在数据分组的原地址和目的地址处，这种加密方法照顾了中间接点数据的安全，但数据分组头是未经加密的明文。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接点处是明文，而数据信息永远不会是明文，对端到端的加密方法稍加变化，即在一个加密文件中永久存放数据，这种系统可用于替代或补充以上两种加密方法。

加密和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方和接受方要求拥有相同的密钥，对称算法的缺点在于算法和密钥必须保密。另外，密钥必须从一个人传达到另一个人，这就产生了安全性威胁。然而，该算法的主要优点是可以建立某种鉴定系统，减少由于伪造信息所带来的问题。

替代对称算法的一种新方法是非对称的加密系统，最早出现在 1976 年，公开密钥算法就是这一算法的衍生物。非对称算法的优点是：第二个密钥，即解密密钥，只有接受方知道，并且接受者需要进行解密运算，在这样的系统中加密和解密算法以及加密密钥可以是公开的，解密密钥与加密密钥是有关系的，但它是巨大的密钥空间中的一随机样本，使敌对方无法通过一个密钥算出另一个密钥。

数据加密性标准（DES），是一种使用最广泛的算法，它可在硬盘设备上实现，用来为数字的、二进制编码的信息做加密。需要注意的是，加密通常发生在 OSI 模型中的物理层，而解密可以用于任何一层。

被动威胁的第二种形式与通信量分析安全性有关，如果一个入侵者可以阅读数据包头，那么他就可以得知数据的源地址和目的地址，即使消息是加密的。使用链路加密，可以降低或清除这种可能性，加密只能限制阅读头信息和消息，而有些重要的信息可以从通信量分析中得到，例如可以得到进入或离开某个中间接点的通信总量，而加密不能解决这些问题。一个可能的对策是，通过生成连续的随机数流或密文流来填充通信链路，使侵入者很难区分有用数据和无用的噪声，从而使计算实际的通信总量十分困难。

2. 主动威胁

主动威胁通常要比被动威胁更加严重，因为主动威胁并不是简单的读取数据信息的内容，而是有意的改动数据控制信号，或者有意伪造数据。对于主动威胁我们所关心的问题是：消息服务的破坏，假冒和信息流的修改。

主动侵入可以发生在通信线路的任何一处，如电缆、微波链路、卫星信路、路由接点、主机和客户的计算机系统都可能成为主动入侵的对象。然而，要对整个线路设置广泛的物理防范设施是不可能的。我们注意到主动威胁只有在实现物理访问时才能进行，在这种情况下，这种物理访问可能是在数百千米之外的一个目标通过拨号访问终端进行的，或者是通过无线电信道进行的，而线路刺探（一种未经授权

就与通信线路进行连接并对数据进行非法访问的行为）有时可能不需要任何一台设备就可以与电缆进行物理连接。阻止主动入侵是非常困难的，挫败主动入侵的安全性目标只能是迅速检测和恢复由于这种侵入而造成的信息延误和系统瓦解。

第一种侵入方式是破坏或者延误大部分以至全部信息。这是一个通信系统所面临的最明显的主动威胁，在信息社会里，发生这样的事件很容易导致重大的损失。

第二种侵入方式是假冒。它通过假装成授权的客户或主机来获得系统的访问权，在系统与对等用户进行通信时以获得数据或服务。入侵者的目的是使目标系统相信，正与它进行通信的确实是它所希望的主机或客户。

主动威胁的第三种方法是修改消息流。在这种情况下，入侵者可能对消息进行有选择地修改、删除、延误重新排序，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会遭到破坏。

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并要通过接收方的再计算。 如果发送方和接收方的校验和不同，则常常需要重新传输该数据包。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，也可以通过差错纠正测试。然而，被加密的明文也可能被修改以形成一个不同的校验和。MDC只是检测消息流的一种方式，还有另外几种校验方式被统称为MAA（信息鉴别算法）。

1.3.2 潜在威胁

1. 基本威胁

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。常见的 4种基本威胁如下：

（1）信息泄漏　信息被泄漏或透露给某个未授权的实体。

（2）完整性破坏　未经授权，数据被修改或破坏。

（3）拒绝服务　对数据或其他资源的合法访问被无条件阻止，这可能是由于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，从而导致系统资源对合法的用户也是不可使用；也可能是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　某一资源未经授权而被使用。

2. 主要的可实现威胁

主要的可实现威胁可以分为渗入威胁和植入威胁。

主要的渗入威胁有如下几种。

（1）假冒　某个实体（人或系统）假装成另外一个不同的实体。黑客大多采用这种方法。

（2）旁路控制　利用系统缺陷或安全上的脆弱之处，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。

主要的植入威胁有如下几种。

（1）特洛伊木马（Torjan Horse）软件中含有不易觉察的程序段，当它被执行时，会破坏用户的安全性。

（2）陷门　在某个系统或文件中设置“机关”，也可以说是一段非法的系统程序，它的目的是为入侵者提供后门。

3. 潜在威胁

通过对各种威胁进行分析，可以发现某些特定的威胁可以导致更基本的威胁发生，这些特定威胁称为潜在威胁。例如对于信息泄漏这样一种基本威胁，可以找出以下几种潜在的威胁：

1）窃听。

2）业务流分析。

3）人员疏忽。

4）媒体清理。

图1-3描绘出了一些典型威胁以及它们之间的相互关系。

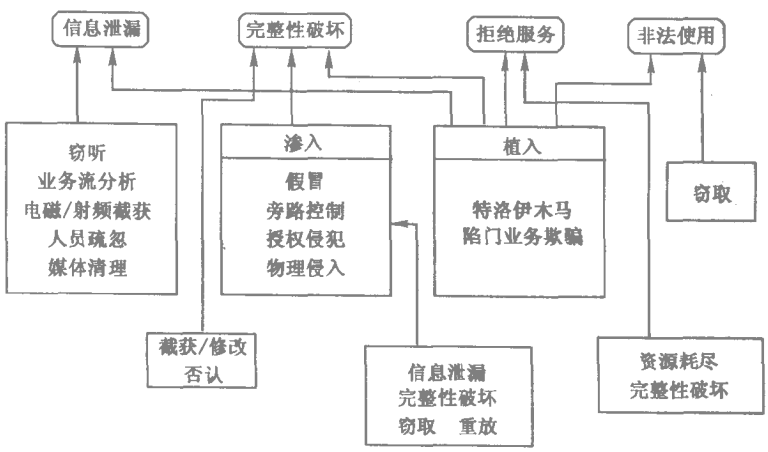

图1-3　典型的潜在威胁及其相互关系

通过调查分析可知，下面几种威胁是最主要的威胁：授权侵犯、假冒、旁路控制、特洛伊木马、陷门和媒体清理等。

1.4 网络安全的策略

当安全具体化时，它有一定范围，这个范围便是属于某个组织的处理和通信资源的集合，称为安全区域。在某一安全区域内，应该有一个关于安全问题的总体目标和规划，这就是安全策略。下面将要讨论的是抽象策略而不是具体策略。

1.4.1 最小特权原则

最小特权原则是基本的安全原则。最小特权原则就是在保证完成工作任务的前提下，应该具有的最小权力。

在因特网中，有很多最小特权的例子。例如：并不是每个用户都需要得到每一项因特网服务；并不是每个用户都需要知道机器的 root 口令 并不是每个系统管理员都需要知道所有系统的 root 口令：并不是每个系统都需要存取每个其他系统的文件。

在最小特权的原则下，应当尽量减少各种操作所需的特权，例如：如果某用户所要做的事情只是重新设置打印系统，就不要给他 root 口令，而应是写一段特权程序，使该用户只可以运行它来重新设置打印系统。

很多因特网上的安全问题是由于没有遵循最小特权原则造成的。例如，在 Sendmail 程序中存在着许多安全问题，由于 Sendmail 程序运行 Setuid root 命令，使得对 Sendmail 的侵袭就因此获得方便。因为它是作为 root 用户来操作的，所以 Sendmail 引起了入侵者的高度重视，而事实上它只不过是一个可以使工作方便的程序。总之最小特权原则就是不但要尽量简化有特权的程序，而且当一个复杂的程序要求特权时，就应把需要特权的部分从这个复杂的程序中分离和独立出来。

解决网络安全的很多方案都是强制使用最小特权战略方法。例如一个数据过滤系统只允许要求服务的数据包进入。

实行最小特权时有两个问题。一是当它不符合正使用的程序和协议特点时，实施可能很复杂，必须确认已成功地施行了最小特权；二是最终分配的特权可能要小于最小特权，这将使有些任务无法完成。

1.4.2 多道防线

为了保障计算机网络安全，需要多道防线进行防御，因为任何防御技术都不是绝对保险的，建立多层防御机制，能有效地提高安全系数。

例如，在一个有多个数据包过滤器组成的结构中，两个过滤器需要做不同的事情，可以设置第二个过滤器来拒绝通过第一个过滤器的数据包。如果第一个过滤器正常工作，那些数据包不会到达第二个；而如果第一个过滤器有问题，则还有第二层保护。再如，如果不想让用户向某一台机器发函件，那么，不仅要过滤掉数据包，而且还要删除机器中的函件程序。

1.4.3 阻塞点

阻塞点是强迫侵袭者必须通过一个可以由系统监控的通道。在因特网安全系统中，位于某一局域网和因特网之间的防火墙就是这样一个阻塞点。任何一个因特网上的侵袭者必须通过这个防御通道。

如果入侵者可以绕过阻塞点，那么阻塞点将不起作用，这是需要认真注意的。一个次级的因特网连接甚至一个间接连接，比如通过连接到另一个公司接入因特网，便是一个危险的缺口，因为因特网的入侵者可能找到与被入侵网络相连的间接通道。

1.4.4 最薄弱环节

链的强度取决于它的最薄弱环节，入侵者总是要找出防御的弱点并集中精力对其进行攻击，所以要采取有效措施消除它们。

最薄弱环节是经常存在的，解决的方法是使那段连接尽量坚固，并在发生危险前保持均衡的强度。

主机安全保护模式会受到阻塞点和最薄弱环节之间相互制约作用的影响，这些消极影响是难以消除的，如果没有阻塞点则意味着有很多链接，而它们中的大部分实际上是很薄弱的。

1.4.5 失效保护机制

失效保护机制就是如果系统运行错误，那么就会停止服务，拒绝用户访问。这可能会导致合法用户无法访问系统，但这是可接受的折衷办法。

例如，如果一个数据包过滤器出现故障，那么它将不会让任何一个数据包进入；如果一个代理程序出现故障，那它就不会提供任何服务。另一方面，一些基于主机的数据包过滤系统允许将数据包分别传送到运行数据包过滤应用和代理服务应用的机器上。这种系统的工作方式是：若数据包过滤器功能发生故障，则将数据包传送到提供代理服务应用的地方，但这种方式是不符合失效保护原则的。

在网络安全中失效保护原则的最大应用就是根据安全的需要选择网络状态。这个状态本质上就是对安全保护的总要求。以下是常用的两个基本的失效保护状态。

（1）默认拒绝状态　即只指明所允许的事情，而其他一切皆禁止。从安全角度讲，默认拒绝状态是合适的，因为它是一个失效保护状态，它认为不了解的事情可能会带来危害。

在默认拒绝状态下，默认禁止做任何事。然后，如果想允许什么服务，必须做如下工作。

1）检查用户所需要的服务。

2）考虑与这些服务有关的安全保护措施和安全的提供方式。

3）允许这些服务。

从分析一项服务的安全保护做起，解决安全保护和用户需求之间的矛盾，然后根据用户需求分析和改进服务的安全保护措施，最终提供一个合适的解决方案。

（2）默认许可状态　即没有明确禁止的就是许可的。

大多数用户和管理者更喜欢默认许可状态。他们倾向于所有的服务应被默认许可，而那些确定的、易出故障的操作是禁止的，例如：

1）禁止 NFS 穿过防火墙。

2）禁止未接受安全保护意识培训的用户进行 WWW 访问。

3）禁止用户安装非授权服务器。

默认许可要求告诉什么是危险的，列举出不能做的几件事，并允许他们做其他任何一件事。

首先，它要求事先精确地知道有哪些特定的危险，而且必须向用户解释这些危险，并了解怎样预防这些危险。但推测出因特网上有哪些危险是根本不可能的。如果不知道什么是问题，也就没有问题被加在“禁止”清单中，这样的话，它就会错误地运行下去，直到发现有人在入侵。

其次，默认许可状态往往会导致防火墙维护者和用户之间逐步升级的角逐。防护者准备防范用户的一举一动，用户却提出新的但却是危险的行为方式，这个过程会循环往复，一直进行下去。

另外，那些从默认许可状态中受益的人可能是潜在的入侵者，因为防火墙的维护者不可能堵住所有的安全漏洞，他们总是处于“防火斗争”状态中，而无暇顾及入侵者的行动。

例如，在文件共享问题中，用户的第一个反应可能是使用 NFS，但 NFS 是不安全的。假设它是默认许可的，而用户又不知道运行 NFS 穿过系统的防火墙是危险的，用户将认为 NFS 是个好办法。另一方面，如果系统状态是默认拒绝，那么用户建立 NFS 的企图将不会成功，这时需要向用户解释原因，并建议使用更安全的通信方式，比如 FTP。

1.4.6 普遍参与

普通参与就像社会治安中的“群防群治”，如果网络用户能普遍参与安全工作，那么整个网络的安全机制就更有效。如果某个用户可以轻易地从安全保护机制中退出，那么入侵者很有可能会先入侵内部人员系统，然后再从内部入侵网络。例如，有人为了绕过防火墙，在内部网络和因特网之间建立了一个“后门”连接，那么世界上任意一个防火墙都无法保护该网络的安全。购买一台调制解调器，从因特网上获得免费的 PPP 或 SLIP 软件，然后每月向当地因特网服务商缴纳一定的费用，就