第一章　计算机系统安全概述

1.1　计算机系统安全的概念

1.1.1　世界范围内日益严重的安全问题

信息技术和信息产业正在改变传统的生产、经营和生活方式，信息已成为社会发展的重要战略资源。电子商务、电子政务、电子税务、电子银行、电子海关、电子证券、网络书店、网上拍卖、网络购物、网络防伪、CTI(Computer Telephony Integration,计算机电信集成)、网上交易、网上选举等网络信息系统将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络信息系统的依赖也日益增强，信息网络已经成为社会发展的重要保证。

在计算机应用日益广泛和深入的同时，计算机网络的安全问题日益复杂和突出。网络的脆弱性和复杂性增加了威胁和攻击的可能性。从以下记录可以看出网络信息的安全问题已经变得越来越重要。

1986 年初在巴基斯坦的拉合尔(Lahore),巴锡特(Basit)和阿姆杰德(Amjad)两兄弟编写的 Pakistan 病毒(即 Brain)在一年内流传到了世界各地。

1988 年 11 月，美国康乃尔大学的学生 Morris 编制的名为蠕虫计算机病毒通过英特网传播，致使网络中约 7000 台计算机被传染,Internet 不能正常运行，造成经济损失约 1 亿美元。迫使美国政府立即做出反应，国防部成立了计算机应急行动小组。这是一次非常典型的计算机病毒入侵计算机网络的事件。

1996 年 12 月 29 日，黑客侵入美国空军的全球网网址并将其主页肆意改动，迫使美国国防部一度关闭了其他 80 多个军方网址。

1998 年 6月 16 日，黑客入侵了上海某信息网的 8 台服务器，破译了网络大部分工作人员的口令和 500 多个合法用户的帐号和密码，其中包括两台服务器上超级用户的帐号和密码。

1998 年 10 月 27 日，刚刚开通的由中国人权研究会与中国国际互连网新闻中心联合创办的‘中国人权研究会’网页,被‘黑客’严重篡改。

2000 年 3 月 6 日晚 6 时 50 分，美国白宫网站主页被黑。

2001 年南海撞机事件引发中美黑客大战。中美双方各有数千网站被黑。

事实上，相当多的网络入侵或攻击并没有被发现。即使被发现了，由于这样或那样的原因，人们并不愿意公开它。

关于攻击者，我们经常听到黑客这个词，那么黑客到底是指哪些人呢？

黑客的定义有多种。现在黑客一词在信息安全范畴内的普遍含义是特指对电脑系统的非法侵入者。黑客对自己的定义是：黑客（hacker）就是那些对技术的局限性有充分认识的人。黑客大都是程序员，他们具有操作系统和编程语言方面的高级知识，乐于探索可编程系统的细节，并且不断提高他们能力，知道系统中的漏洞及其原因所在；他们不断追求更深的知识，并公开他们的发现，与其他人分享，专业黑客都是很有才华的源代码创作者。美国警方把所有涉及到“利用”“借助”“通过”或“阻挠”计算机的犯罪行为都定为 hacking。中国的一些黑客自称红客（honker）。

入侵者（cracker）是指怀着不良的企图，闯入甚至破坏远程机器系统完整性的人。入侵者利用获得的非法访问权，破坏重要数据，拒绝合法用户服务请求，或为了自己的目的制造麻烦。黑客、入侵者我们不加区分。

黑客技术也就是安全技术，无论是攻是防，黑客技术均体现了安全技术的积极意义。黑客技术是信息安全技术中最活跃、最能动的技术，它在威胁网络安全的同时又能造福于安全、关键在于要将技术和行为分开。从目前的技术发展看黑客技术往往是所有技术方案中最直接、最简洁、最出乎意料的那种。当然其作用的两面性也十分突出，对信息安全问题，不能低估，低估会给我们带来直接损失；同时也不能高估，高估会带来间接损失。对黑客技术也要有这种辩证的认识。黑客攻击的动机和目的因人、因国家、因情景而异，黑客技术的作用也因人而异，我们反对使用黑客技术未经允许入侵他人系统，同时也反对因为有人使用黑客技术从事犯罪活动就否定这一技术。

对计算机系统的侵入与破坏带来了传统犯罪以外的另一种新的犯罪形态——计算机犯罪。

1.1.2 计算机系统安全的概念

从技术角度看，计算机系统安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。我们首先介绍以下几个概念。

计算机系统（Computer System）也称计算机信息系统（Computer Information System），是由计算机及其相关的和配套的设备、设施（含网络）构成的，并按一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。计算机系统安全（Computer System Security）中的“安全”一词是指将服务与资源的脆弱性降到最低限度。脆弱性是指计算机系统的任何弱点。

国际标准化组织（ISO）将“计算机安全”定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”此概念偏重于静态信息保护。也有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。

在美国国家信息基础设施（NII）的文献中，给出了安全的五个属性：可用性、可靠性、完整性、保密性和不可抵赖性。这五个属性适用于国家信息基础设施的教育、娱乐、医疗、运输、国家安全、电力供给及分配、通信等广泛的领域。这五个属性定义如下：

可用性（Availability）：得到授权的实体在需要时可访问资源和服务。可用性是指无论何时，只要用户需要，信息系统必须是可用的，也就是说信息系统不能拒绝服务。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的（话音、数据、文字和图像等），有时还要求时效性。网络必须随时满足用户通信的要求。攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用访问控制机制，阻止非授权用户进入网络，从而保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

可靠性（Reliability）：可靠性是指系统在规定条件下和规定时间内、完成规定功能的概率。可靠性是网络安全最基本的要求之一，网络不可靠，事故不断，也就谈不上网络的安全。目前，对于网络可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备，采取合理的冗余备份措施仍是最基本的可靠性对策，然而，有许多故障和事故，则与软件可靠性、人员可靠性和环境可靠性有关。

完整性（Integrity）：信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏的特性。只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被篡改。即信息的内容不能为未授权的第三方修改。信息在存储或传输时不被修改、破坏，不出现信息包的丢失、乱序等。

保密性（Confidentiality）：保密性是指确保信息不暴露给未授权的实体或进程。即信息的内容不会被未授权的第三方所知。这里所指的信息不但包括国家秘密，而且包括各种社会团体、企业组织的工作秘密及商业秘密，个人的秘密和个人私密（如浏览习惯、购物习惯）。防止信息失窃和泄露的保障技术称为保密技术。

不可抵赖性（Non－Repudiation）：也称作不可否认性。不可抵赖性是面向通信双方（人、实体或进程）信息真实同一的安全要求，它包括收、发双方均不可抵赖。一是源发证明，它提供给信息接收者以证据，这将使发送者谎称未发送过这

些信息或者否认它的内容的企图不能得逞；二是交付证明，它提供给信息发送者以证据，这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。

除此之外计算机网络信息系统的其他安全属性还包括：

可控性：可控性就是对信息及信息系统实施安全监控。管理机构对危害国家信息的来往、使用加密手段从事非法的通信活动等进行监视审计，对信息的传播及内容具有控制能力。

可审查性：使用审计、监控、防抵赖等安全机制，使得使用者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，并能够对网络出现的安全问题提供调查依据和手段。审计是通过对网络上发生的各种访问情况记录日志，并对日志进行统计分析，是对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。审计的主要对象为用户、主机和节点，主要内容为访问的主体、客体、时间和成败情况等。

认证：保证信息使用者和信息服务者都是真实声称者，防止冒充和重演的攻击。

访问控制：保证信息资源不被非授权地使用。访问控制根据主体和客体之间的访问授权关系，对访问过程做出限制。

安全工作的目的就是为了在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，维护计算机系统安全。我们应当保障计算机及其相关的和配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。计算机系统安全涉及物理安全（实体安全）、运行安全和信息安全三个方面。

（1）物理安全（Physical Security）

保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。特别是避免由于电磁泄漏产生信息泄露，从而干扰他人或受他人干扰。物理安全包括环境安全，设备安全和媒体安全三个方面。

（2）运行安全（Operation Security）

为保障系统功能的安全实现，提供一套安全措施（如风险分析，审计跟踪，备份与恢复，应急等）来保护信息处理过程的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存贮、处理和传输的信息造成破坏和损失。运行安全包括风险分析、审计跟踪、备份与恢复、应急四个方面。

风险分析是指为了使计算机信息系统能安全地运行，首先了解影响计算机信息系统安全运行的诸多因素和存在的风险，从而进行风险分析，找出克服这些风险的方法。

审计跟踪是利用计算机信息系统所提供的审计跟踪工具，对计算机信息系统的工作过程进行详尽的跟踪记录，同时保存好审计记录和审计日志，并从中发现和及时解决问题，保证计算机信息系统安全可靠地运行。这就要求系统管理员要认真负责，切实保存、维护和管理审计日志。

应急措施和备份恢复应同时考虑。首先要根据所用信息系统的功能特性和灾难特点制定包括应急反应、备份操作、恢复措施三个方面内容的应急计划，一旦发生灾害事件，就可按计划方案最大限度地恢复计算机系统的正常运行。

(3) 信息安全(Information Security)

防止信息财产被故意地或偶然地非授权泄露、更改、破坏或使信息被非法的系统辨识、控制。即确保信息的完整性、保密性、可用性和可控性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别七个方面。

网络信息既有存储于网络节点上的信息资源，即静态信息；又有传播于网络节点间的信息，即动态信息。而这些静态信息和动态信息中有些是开放的，如广告、公共信息等，有些是保密的，如私人间的通信、政府及军事部门、商业机密等。信息根据敏感性可分为以下类别。

非保密的：不需保护。其实例包括出版的年度报告、新闻信件等。

内部使用的：在公司和组织内部不需保护，可任意使用，但不对外。实例包括策略、标准、备忘录和组织内部的电话记录本等。

受限制的：包括那些泄漏后不会损害公司和组织的最高利益的信息。例如客户数据和预算信息等。

保密的：包括那些泄漏后会严重损害公司和组织利益的信息。例如市场策略和专用软件等。保密数据根据其保密程度可分为秘密、机密、绝密三类。敏感性程度依次递增这是按照泄漏后对公司和组织利益的损害程度来排序的。

计算机系统的安全保护工作的重点是维护国家事务、经济建设、国防建设、尖端科学技术等重要领域的计算机信息系统的安全。

我国公安部主管全国计算机信息系统安全保护工作。国家安全部、国家保密局和国务院其他有关部门，在国务院规定的职责范围内做好计算机信息系统安全保护的有关工作。计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。计算机信息系统的使用单位应当建立健全安全管理制度，负责本单位计算机信息系统的安全保护工作。

1.1.3 国内外计算机系统安全标准

国际性的标准化组织主要有国际标准化组织(ISO)、国际电器技术委员会(IEC)及国际电信联盟(ITU)所属的电信标准化组(ITU－TS)。

美国国防部的可信计算机系统评价准则(Trusted Computer System Evaluation Criteria TCSEC,桔皮书)是计算机系统安全评估的第一个正式标准,具有划时代的意义。该准则于1970年由美国国防科学委员会提出,并于1985年12月由美国国防部公布。TCSEC将安全分为4个方面:安全政策、可说明性、安全保障和文档。该标准将以上4个方面分为7个安全级别,按安全程度从最低到最高依次是D、C1、C2、B1、B2、B3、A1。

D类:最低保护。无需任何安全措施。属于这个级别的操作系统有:DOS、Windows、Apple的Macintosh System7.1.

C1类:自决的安全保护。系统能够把用户和数据隔开,用户可以根据需要采用系统提供的访问控制措施来保护自己的数据,系统中必有一个防止破坏的区域,其中包含安全功能。用户拥有注册帐号和口令,系统通过帐号和口令来识别用户是否合法,并决定用户对程序和信息拥有什么样的访问权。

C2类:访问控制保护。控制粒度更细使得允许或拒绝任何用户访问单个文件成为可能。系统必须对所有的注册、文件的打开、建立和删除进行记录。审计跟踪必须追踪到每个用户对每个目标的访问。能够达到C2级的常见操作系统有:Unix系统、XENIX、Windows NT。

B1类:有标签的安全保护。系统中的每个对象都有一个敏感性标签而每个用户都有一个许可级别。许可级别定义了用户可处理的敏感性标签。系统中的每个文件都按内容分类并标有敏感性标签,任何对用户许可级别和成员分类的更改都受到严格控制。较流行的B1级操作系统是OSF/1。

B2类:结构化保护。系统的设计和实现要经过彻底的测试和审查。系统应结构化为明确而独立的模块,实施最少特权原则。必须对所有目标和实体实施访问控制。政策要有专职人员负责实施,要进行隐蔽信道分析。系统必须维护一个保护域,保护系统的完整性,防止外部干扰。目前,UnixWare 2.1/ES作为国内独立开发的具有自主版权的高安全性Unix系统,其安全等级为B2级。

B3类:安全域。系统的安全功能足够小,以利广泛测试。必须满足参考监视器需求以传递所有的主体到客体的访问。要有安全管理员,审计机制扩展到用信号通知安全相关事件,还要有恢复规程,系统高度抗侵扰。

A1类:核实保护。最初设计系统就充分考虑安全性。有“正式安全策略模型”,其中包括由公理组成的数学证明。系统的顶级技术规格必须与模型相对应,系统还包括分发控制和隐蔽信道分析。

1991年，欧共体发布了信息技术安全评价准则（Information Technology Security Evaluation Criteria，ITSEC）。1993 年，加拿大发布了加拿大可信计算机产品评价准则（CTCPEC），CTCPEC 综合了 TCSEC 和 ITSEC 两个准则的优点。同年，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了美国信息技术安全评价联邦准则（FC）。ITSEC 与 TCSEC 不同，其观点是应当分别衡量安全的功能和安全的保障，而不应象 TCSEC 那样混合考虑安全的功能和安全的保障。因此，ITSEC 对每个系统赋予两种等级："F"（functionality）即安全功能等级，"E"（European assurance）即安全保障等级。另外，TCSEC 把保密作为安全的重点，而 ITSEC 则把完整性、可用性与保密性作为同等重要的因素。CTCPEC 标准将安全需求分为 4 个层次：机密性、完整性、可靠性和可说明性。FC 参照了 CTCPEC 及 TCSEC，在美国的政府、民间和商业领域得到广泛应用。1993 年 6月，上述国家共同起草了一份通用准则（CC），并将 CC 推广为国际标准。1999 年 10 月 CC v2.1 版发布，并且成为 ISO 标准。CC 结合了 FC 及 ITSEC 的主要特征，它强调将安全的功能与保障分离，并将功能需求分为 9 类 63 族，将保障分为 7 类 29 族。

ISO 在安全体系结构方面制定了国际标准 ISO7498－2－1989《信息处理系统开放系统互连基本参考模型第 2 部分安全体系结构》。该标准提供了安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

国内由公安部主持制定、国家技术标准局发布的国家标准 GB17895－1999《计算机信息系统安全保护等级划分准则》。该准则将信息系统安全分为 5 个等级，分别是：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。我国红旗安全操作系统 2.0 已通过中华人民共和国公安部计算机信息系统产品质量监督检验中心的认证，达到信息安全第三级的要求。

1.2 安全威胁

1.2.1 安全威胁的种类

安全威胁是指对安全的一种潜在的侵害。威胁的实施称为攻击。一般认为，目前计算机系统安全面临的威胁主要表现在三类：信息泄露、拒绝服务、信息破坏。其中信息泄露、信息破坏也可能造成系统拒绝服务。

信息泄漏：指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括：信

息在传输中丢失或泄漏（如利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息）；信息在存储介质中丢失或泄漏；通过建立隐蔽隧道等窃取敏感信息等。

信息破坏：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

拒绝服务：它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

安全威胁可能来自各方面。影响、危害计算机系统安全的因素分自然和人为两类。

自然因素包括：各种自然灾害，如水、火、雷、电、风暴、烟尘、虫害、鼠害、海啸和地震等；系统的环境和场地条件，如温度、湿度、电源、地线和其他防护设施不良造成的威胁；电磁辐射和电磁干扰的威胁；硬件设备自然老化，可靠性下降的威胁。

人为因素又有无意和故意之分。无意事件包括：操作失误（操作不当、误用媒体、设置错误）、意外损失（电力线搭接、电火花干扰）、编程缺陷（经验不足、检查漏项、不兼容文件）、意外丢失（被盗、被非法复制、丢失媒体）、管理不善（维护不利、管理松驰）、无意破坏（无意损坏、意外删除等）。人为故意的破坏包括：敌对势力、各种计算机犯罪。

1. 从威胁的来源看可分为内部威胁和外部威胁

造成网络安全的威胁的原因可能是多方面的，有来自外部，也有可能来自企业网络内部。

内部威胁。80％的计算机犯罪都和系统安全遭受损害的内部攻击有密切的关系。内部人员对机构的运作、结构熟悉，导致攻击不易被发觉，内部人员最容易接触敏感信息，危害的往往是机构最核心的数据、资源等。各机构的信息安全保护措施一般是“防外不防内”。能用来防止内部威胁的保护方法包括：对工作人员进行仔细审查；制订完善的安全策略；增强访问控制系统；审计跟踪以提高检测出这种攻击的可能性。

外部威胁。外部威胁的实施也称远程攻击。外部攻击可以使用的办法如：搭线；截取辐射；冒充为系统的授权用户，或冒充为系统的组成部分；为鉴别或访问控制机制设置旁路；利用系统漏洞攻击等。

2. 从造成的结果上看可以分成主动威胁和被动威胁

被动威胁。这种威胁对信息的非授权泄露而未改变系统状态。如信息窃

取、密码破译、信息流量分析等。被动威胁的实现不会导致对系统中所含信息的任何篡改，而且系统的操作与状态也不受改变，但有用的信息可能被盗窃并被用于非法目的。使用消极的搭线窃听办法以观察在通信线路上传送的信息就是被动威胁的一种实现。

主动威胁。这种威胁是对系统的状态进行故意的非授权的改变。对系统的主动威胁涉及到系统中所含信息的篡改，或对系统的状态或操作的改变。一个非授权的用户不怀好意地改动路由选择表就是主动威胁的一个例子。与安全有关的主动威胁的例子可能是：入侵、篡改消息、重发消息、插入伪消息、重放、阻塞、抵赖、病毒、冒充已授权实体以及服务拒绝等。主动攻击会直接进入信息系统内部，往往可影响系统的运行，造成巨大的损失，并给信息网络带来灾难性的后果。

3. 从威胁的动机上看分为偶发性威胁与故意性威胁

偶发性威胁。偶发性威胁是指那些不带预谋企图的威胁。偶发性威胁的实例包括自然灾害、系统故障、操作失误和软件出错。人为的无意失误包括：操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的帐号随意转借他人或与别人共享等都会对网络安全带来威胁。

故意性威胁。故意性威胁是指对计算机系统的有意图、有目的的威胁。范围可从使用易行的监视工具进行随意的检测到使用特别的系统知识进行精心的攻击。一种故意的威胁如果实现就可认为是一种“攻击”。人为的恶意攻击：这是计算机网络所面临的最大威胁，敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。由于网络软件不可能是百分之百的无缺陷和无漏洞的，这些漏洞和缺陷恰恰是攻击者进行攻击的首选目标。

4. 从威胁的严重性可分为三级

C 级威胁。个体单点攻击，攻击的范围、深度和能够完成的攻击任务不太复杂，往往是黑客行为，虽然这种攻击可以逐步实施自动化、平台化，但攻击点是一点，作用有限，通常攻击的是标准化网络和系统。

B 级威胁。有组织分布式协同攻击。多点、多技术和协同攻击，相互掩护，危害大，难于对付。已经采用多种网络攻击技术。能够攻击一些专用网络，非标准网络，攻击软件本身并没有组织化，较少实施或不能实施战术。

A 级威胁。信息战是指通过一切手段（可控计算机病毒、信息炸弹、远程攻击软件、网络攻击平台、使用多技术体制的网络、使用包括卫星通信在内的一切

可利用的通信网络)破坏对方信息系统的作战方式。如通过破解信息，为其所用 突破安全系统,破坏信息的真实和完整性 通过干扰阻止信息的传递 通过信息炸弹等手段使信息系统瘫痪。其实施一定的战术。

1.2.2 威胁的表现形式

1. 假冒

假冒是指通过出示伪造的凭证来冒充别的对象，进入系统盗窃信息或进行破坏。假冒攻击的表现形式主要有盗窃密钥、访问明码形式的口令或者记录授权序列并在以后重放。假冒具有很大的危害性，因为它回避了用于结构化授权访问的信任关系。

假冒常与某些别的主动攻击形式一起使用，特别是消息的重演与篡改（伪造），构成对用户的诈骗。例如，鉴别序列能够被截获，并在一个有效的鉴别序列发生之后被重演。特权很少的实体为了得到额外的特权可能使用冒充装扮成具有这些特权的实体。

假冒带来极大的危害。以假冒的身份访问计算机系统，非授权用户 A 声称是另一用户 B,然后以 B 的名义访问服务与资源， A 窃取了 B 的合法利益，如果 A 破坏了计算机系统，则 A 不会承担责任，这必然损坏了 B 的声誉。再如进程 A 以伪装的身份欺骗与它通信的进程 B，如伪装成著名的售货商的进程要求购物进程提供信用卡号、银行帐号，这不仅损害购物者的利益，也损害了售货商的声誉。

2. 未授权访问

未授权访问是指未经授权的实体获得了某个对象的服务或资源。未授权访问通常是通过在不安全通道上截获正在传输的信息或者利用对象的固有弱点来实现的。

非授权访问没有预先经过同意，就使用网络或计算机资源，有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

3. 拒绝服务(DoS)

DoS 是指服务的中断，系统的可用性遭到破坏，中断原因可能是对象被破坏或暂时性不可用。当一个实体不能执行它的正当功能，或它的动作妨碍了别的实体执行它们的正当功能的时候便发生服务拒绝。这种攻击可能是一般性的，比如一个实体抑制所有的消息，也可能是有具体目标的，例如一个实体抑制所有流向某一特定目的的端的消息，如安全审计服务。这种攻击可以是对通信业务

流的抑制，或产生额外的通信业务流。也可能制造出试图破坏网络操作的消息，特别是如果网络具有中继实体，这些中继实体根据从别的中继实体那里接收到的状态报告来做出路由选择的决定。

例如，用户进程通过消耗过多的计算机系统的计算资源来发动拒绝服务攻击，如非授权者重复施放无用数据、占据处理器资源和磁盘空间、对系统无休止地访问，“狂轰烂炸”造成系统阻塞，无法进行正常的信息处理，直至系统瘫痪。或者使用计算机系统的弱点蓄意运行攻击脚本。当然也存在用户进程无意的程序错误造成系统拒绝服务。

4. 否认（抵赖）

在一次通信中涉及到的那些实体之一事后不承认参加了该通信的全部或一部分。不管原因是故意的还是意外的，都会导致严重的争执，造成责任混乱。

可以采用数字签名等技术措施来防止抗抵赖行为。

5. 窃听

窃听是信息泄露的表现。可通过物理搭线、拦截广播数据包、后门、接收辐射信号进行实施。对窃听的预防非常困难，发现窃听几乎不可能，其严重性非常高。非授权者利用信息处理、传送、存储中存在的安全漏洞（例如通过卫星和电台窃收无线信号、电磁辐射泄漏等）截收或窃取各种信息。由于卫星等无线信号可在全球进行窃收，因此必须加以重视。我国有关部门明确规定，在无线信道上传输秘密信息时必须安装加密机进行加密保护。

辐射是电磁信号泄露。电缆线路和附加装置（计算机、打印机、调制解调器、监视器、键盘、连接器、放大器和分接盒）泄露一些信号，在若干距离上，泄露的信号能成为可读的数据。可以将调谐到低波段的 AM 收音机保持吱吱的叫声，并靠近计算机。将发现当计算机接通电源自检时，收音机产生不同的声音，而当给出各种不同的指令时，收音机产生另外的声音。收音机也能从监视器、打印机收取信号。

6. 篡改

非授权者用各种手段对信息系统中的数据进行增加、删改、插入等非授权操作，破坏数据的完整性，以达到其恶意目的。当所传送的内容被改变而未发觉，并导致一种非授权后果时出现消息篡改。

7. 复制与重放（重演）

当一个消息，或部分消息为了产生非授权效果而被重复时将出现重演。其实是非授权者先记录系统中的合法信息、然后在适当时候进行重放，以搅乱系统的正常运行，或达到其恶意目的。由于记录的是合法信息，因而如果不采取有效措施，将难以辨认真伪。例如，一个含有鉴别信息的有效消息可能为另一个实体

所重演，目的是鉴别它自己（把它当作其他实体）。恶意系统可以克隆一个实体或实体产生的信息。如截获订单，然后反复发出订单。

8. 业务流量、流向分析

非授权者在信息网络中通过业务流量或业务流向分析来掌握信息网络或整体部署的敏感信息。虽然这种攻击没有窃取到信息内容，但仍然可获取许多有价值的情报。可以通过业务流量填充抵御这种攻击。

9. 隐蔽信道（阈下信道、隐通道）

系统设计的一些信道来合法传送信息，这些信道为公开通道，隐蔽信道是通过公开通道传送隐蔽信息的一种秘密方法，即信息隐藏。未经授权的用户可用隐蔽信道传送机密信息。如一个重要雇员用文件名传送公司秘密信息时，将文件名编码。如果文件名对外部用户是可访问的。则未经授权用户可将收到的在文件名中编码的信息解码，而了解信息内容。用于传送文件名的信道被滥用为传输某些秘密信息，这种操作不受访问控制机制限制。

隐蔽信道既可传送未经授权信息，又不违反访问控制和其他安全机制。隐蔽信道不容易探测，即使探测到，也很难清除。例如：隐蔽存储信道采用某些存储机制，将信息传送到未授权用户。即一个进程直接或间接写一个存储地址，另一个进程直接或间接读一个存储地址的隐蔽信道。隐蔽计时信道采用计时程序来传送未经授权的信息。在该信道下一个进程通过调整自身对系统资源的使用，向另一个进程传送未经授权的信息。这个进程同时影响了第二个进程观察到的实际响应时间。Gustavus Simmons 发明了传统数字签名算法中隐蔽信道的概念，隐蔽消息隐藏在看似正常数字签名的文本中，其他人不仅不能读隐蔽信道消息，而且也不知道隐蔽信道消息已经出现。

10. 人为失误

最常见的事故是人的失误。人为错误、意外事故、疏漏错误或权限错误预防非常困难，具有很大的危害，几乎没有什么安全措施能防止或弥补这类错误。

比如误格式化、误删除造成数据丢失；比如把一些表格、磁带、磁盘、信用卡信息、多层打字信件用的复写纸粗心地作为垃圾丢弃造成机密泄露；比如使用过时或不准确的信息（过时的软件版本、过时的病毒库）导致弱点暴露，等等。

11. 自然灾害与人为破坏

如雷电、地震、火灾、水灾、恐怖活动、偷窃、战争等。

12. 逻辑炸弹

逻辑炸弹是指修改计算机程序，使它在某种特殊条件下按某种不同的方式运行。在正常条件下程序运行正常，但如果某特殊条件出现，程序就会按不同于

预期的方式运行。预防逻辑炸弹几乎不可能，发现也很困难，破坏性极大。

13. 后门（陷门）

后门是进入系统的一种方法，通常由系统的设计者利用应用系统的开发时机，故意设置机关，用以监视计算机系统，但有时也因偶然考虑不周而存在（如漏洞）。后门也是程序设计、调试、测试或维修期间编程员使用的常用检验手段。例如当程序运行时，在正确的时间按下正确的键，或提供正确的参数，就会对预定的事件或事件序列产生非授权的影响。发现后门非常困难。因为证明程序满足规范的要求是困难的，证明在任何其他情况下，该程序不做任何别的事情是更困难的（如不含后门、没有逻辑炸弹）.

14. 恶意代码

恶意代码包括病毒、蠕虫、特洛伊木马、逻辑炸弹、恶意 Java 程序、愚弄和下流玩笑程序、恶意 Active X 控件以及 Web 脚本等。如 Web 页面放入了恶意代码，在访问者不知情的情况下，自动修改 IE 默认首页、标题内容、鼠标右键项目等。可以通过加强计算机病毒检测功能进行查杀。

15. 不良信息

互联网给人们的工作、学习、生活带来了极大便利，但在信息的海洋中，还夹杂着一些不良内容，包括色情、暴力、毒品、邪教、赌博等。对付这些不良内容的通常做法就是拦截，采用信息过滤技术进行访问控制。一方面，对页面进行监控，对出现的词汇进行逻辑判断，完成对不良信息的查杀；另一方面，通过预置不良网址禁止使用者登录。由于决策者对不良信息定义的标准可能不同，好的过滤系统应该允许管理员自定义设置。

1.3 安全模型

1.3.1 P^2DR 安全模型

安全具有动态性。安全的概念是相对的，任何一个系统都具有潜在的危险，没有绝对的安全，安全程度随着时间的变化而改变。在一个特定的时期内，在一定的安全策略下，系统是安全的。但是随着时间的演化和环境的变迁（如攻击技术的进步、新漏洞的暴露），系统可能会变得不安全。因此需要适应变化的环境并能做出相应的调整以确保安全防护。

安全具有整体性。安全包括了物理层、网络层、系统层、应用层以及管理层五个方面。从技术上来说，系统的安全由安全的软件系统、防火墙、网络监控、信

息审计、通信加密、灾难恢复、安全扫描等多个安全组件来保证的。单独的安全组件只能提供部分的安全功能。无论缺少哪一个安全组件都不能构成完整的安全系统。当我们用各种技术手段，加固一个网络防护系统时，必须要考虑到相应的安全策略以及如何适应快速的响应机制和恢复措施。安全是一个系统工程，是一个整体的概念，必须保证网络设备和各个组件的整体安全性。传统的信息安全技术仅仅强调系统自身的加固和防护，忽视了安全的整体性。

美国国际互联网安全系统公司(ISS)认为没有一种技术可完全消除网络中的安全漏洞。系统的安全实际上是理想中的安全策略和实际的执行之间的一个平衡，提出了一个可适应网络安全模型 ANSM(Adaptive Network Security Model)——P^2DR 安全模型。第一是策略(Policy),第二是保护(Protection),第三是检测(Detection)，第四是响应(Response)。如图 1.1 所示。

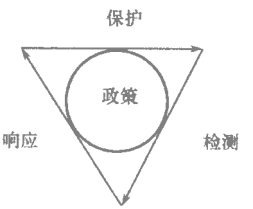

图 1.1 P^2DR 安全模型

该模型是在整体的安全策略的控制和指导下在综合运用防护工具的同时，利用检测工具了解和评估系统的安全状态，通过适当的反应将系统调整到相对最安全和风险最低的状态。P^2DR 强调在监控、检测、响应、防护等环节的循环过程，通过这种循环达到保持安全水平的目的。P^2DR 安全模型是整体的动态的安全模型，所以称为可适应安全模型。

模型的基本描述为：

安全 = 风险分析 + 执行策略 + 系统实施 + 漏洞监测 + 实时响应

1. 策略

安全策略是 P^2DR 安全模型的核心，所有的防护、检测、响应都是依据安全策略实施的，安全策略为安全管理提供管理方向和支持手段。策略体系的建立包括安全策略的制订、评估、执行等。制订可行的安全策略取决于对网络信息系统的了解程度。

2. 保护

保护就是采用一切手段保护信息系统的保密性、完整性、可用性、可控性和不可否认性。应该依据不同等级的系统安全要求来完善系统的安全功能、安全

机制。通常采用传统的静态安全技术及方法来实现，主要有防火墙、加密、认证等方法。

保护主要在边界提高抵御能力。界定网络信息系统的边界通常是困难的。一方面，系统是随着业务的发展不断扩张或变化的；另一方面，要保护无处不在的网络基础设施成本是很高的。边界防卫通常将安全边界设在需要保护的信息周边，例如存储和处理信息的计算机系统的外围，重点阻止诸如冒名顶替、线路窃听等试图‘越界’的行为，相关的技术包括数据加密、数据完整性、数字签名、主体认证、访问控制和公证仲裁等。这些技术都与密码技术密切相关。

边界保护技术可分为物理实体的保护技术和信息保护（防泄露、防破坏）技术。

物理实体的保护技术。这类技术主要是对有形的信息载体实施保护，使之不被窃取、复制或丢失。如磁盘信息消除技术，室内防盗报警技术，密码锁、指纹锁、眼底锁等。信息载体的传输、使用、保管、销毁等各个环节都可应用这类技术。

信息保护技术。这类技术主要是对信息的处理过程和传输过程实施保护，使之不被非法入侵、外传、窃听、干扰、破坏、拷贝。

对信息处理的保护主要有二种技术：一种是计算机软、硬件的加密和保护技术，如计算机口令字验证、数据库存取控制技术、审计跟踪技术、密码技术、防病毒技术等；另一种是计算机网络保密技术，主要指用于防止内部网秘密信息非法外传的保密网关、安全路由器、防火墙等。

对信息传输的保护也有两种技术：一种是对信息传输信道采取措施，如专网通信技术、跳频通信技术（扩展频谱通信技术）、光纤通信技术、辐射屏蔽和干扰技术等，以增加窃听的难度；另一种是对传递的信息使用密码技术进行加密，使窃听者即使截获信息也无法知悉其真实内容。常用的加密设备有电话保密机、传真保密机、IP 密码机、线路密码机、电子邮件密码系统等。

3. 检测

检测是动态响应和加强防护的依据，是强制落实安全策略的工具，通过不断地检测和监控网络及系统，来发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。网络的安全风险是实时存在的，检测的对象主要针对系统自身的脆弱性及外部威胁。利用检测工具了解和评估系统的安全状态。

检测包括：检查系统存在的脆弱性；在计算机系统运行过程中，检查、测试信息是否发生泄漏、系统是否遭到入侵，并找出泄漏的原因和攻击的来源。如计算机网络入侵检测、信息传输检查、电子邮件监视、电磁泄漏辐射检测、屏蔽效果测试、磁介质消磁效果验证等。

入侵检测是发现渗透企图和入侵行为。在近年发生的网络攻击事件中，突

破边界防卫系统的案例并不多见，攻击者的攻击行动主要是利用各种漏洞。人们通过入侵检测尽早发现入侵行为，并予以防范。入侵检测基于入侵者的攻击行为与合法用户的正常行为有着明显的不同，实现对入侵行为的检测和告警，以及对入侵者的跟踪定位和行为取证。

4. 响应

在检测到安全漏洞之后必须及时做出正确的响应，从而把系统调整到安全状态 对于危及安全的事件、行为、过程，及时做出处理，杜绝危害进一步扩大，使系统力求提供正常的服务。例如关闭受到攻击的服务器。

从某种意义上讲，安全问题就是要解决紧急响应和异常处理问题。通过建立反应机制，提高实时性，形成快速响应的能力。需要制订紧急响应的方案，做好紧急响应方案中的一切准备工作。

1997 年，基于 P^2DR 安全模型，ISS 推出了可适应性网络安全解决方案——SAFEsuite 套件。SAFEsuite 套件系列包括漏洞评估工具互联网扫描器（Internet Scanner）、系统扫描器（System Scanner）、数据库扫描器（Database Scanner）、实时监控工具实时监控（RealSecure）和 SAFEsuite 套件决策软件（SAFEsuite Decisions）。

SAFEsuite 套件通过对 Web 站点、防火墙、路由器、外部网络、操作系统、联网的 Unix 系统，以及 Windows NT 主机和工作站的安全风险监测和响应，实现对整个企业信息的保护。它同时可以检测出各种系统漏洞，诸如密码泄露、程序认证、操作系统与数据库系统配置及常见的与用户有关的安全弱点，并提出相应的修补措施。

互联网扫描器通过对网络安全弱点全面和自主地检测与分析，能够迅速找到安全漏洞并修复。网络扫描器对所有网络中的附属设备进行扫描，将风险分为高、中、低 3 个等级并生成针对不同管理对象的报表。

系统扫描器是基于主机的安全评估系统。系统扫描器通过对内部网络安全弱点的全面分析，协助企业进行安全风险管理。区别于静态的安全策略，系统扫描器对主机进行一系列的设置检查，使其可真正预防潜在安全风险问题，其中包括易猜出的密码、用户权限、服务器设置以及其他含有攻击隐患的可疑点。该产品的扫描对象是操作系统。

数据库扫描器是针对数据库管理系统风险的评估检测工具。用户可利用它来建立数据库的安全规则，通过运行审核程序来提供有关安全风险和位置的简明报告。

实时入侵监控器是一个集成了基于网络和基于主机的入侵检测和响应系统。它包含 3 个部件：网络引擎（基于网络的监控器，RealSecure Network Engine）、系统代理（基于主机的监控器，RealSecure System Agent）和管理控制台（RealSecure Manager Console）。RealSecure Engine 运行在专门的工作站上，对网络入侵进行检

测和响应。RealSecure Agent 是基于主机的防范系统，是对 RealSecure Engine 的补充。RealSecure Manager Console 是 RealSecure 系统的控制台。可以对多台 RealSecure 网络引擎和系统代理进行管理。

1.3.2 PDRR 安全模型

近年美国国防部提出了“信息安全保障体系”概念，其重要内容包括：概括了网络安全的整个环节，即保护（Protect）、检测（Detect）、响应（React）、恢复（Restore）提出了人、政策（包括法律、法规、制度、管理）和技术三大要素归纳了网络安全的主要内涵，即鉴别、保密、完整性、可用性、不可抵赖性、责任可核查性和可恢复性；提出了信息安全的几个重点领域，即关键基础设施的网络安全（包括电信、油气管网、交通、供水、金融等）、内容的信息安全（包括反病毒、电子信箱安全和有害内容过滤等）和电子商务的信息安全；认为密码理论和技术是核心，安全协议是桥梁，安全体系结构是基础，安全的芯片是关键，监控管理是保障，攻击和评测的理论和实践是考验。如图 1.2 所示。

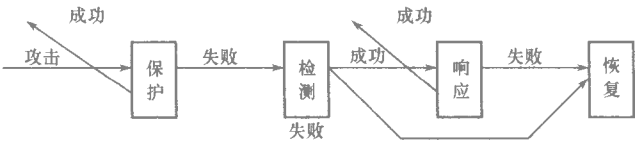

图 1.2 PDRR 安全模型

PDRR 模型引进了时间的概念。

保护时间 Pt：表示从入侵开始到成功侵入系统的时间，即攻击所需时间。高水平的入侵及安全薄弱的系统都能导致攻击的有效性，使保护时间 Pt 缩短。

检测时间 Dt：系统安全检测包括发现系统的安全隐患和潜在攻击检测。改进检测算法和设计可缩短 Dt。适当的防护措施可有效缩短检测时间。

响应时间 Rt：包括检测到系统漏洞或监控到非法攻击到系统启动处理措施的时间。例如一个监控系统的响应可能包括监视、切换、跟踪、报警、反攻等内容。而安全事件的后处理（如恢复、事后总结等）不纳入事件响应的范畴之内。

PDRR模型用数学公式的方法简明地解析了安全的概念：系统的保护时间应大于系统检测到入侵行为的时间加上系统响应时间，即 $Pt > Dt + Rt$。也就是在入侵者危害安全目标之前就能够被检测到并及时处理。巩固的防护系统与快速的反应结合起来，就是真正的安全。例如，防盗门只能延长被攻破的时间。如果警卫人员能够在防盗系统被攻破之前作出迅速反应，那么这个系统就是安全的。这实际上给出了安全的一个全新的定义：及时的检测和响应就是安全。根