第 5 章　信息安全基础

信息安全最初用于保护信息系统中处理和传递的秘密数据，随着操作系统、数据库技术和信息系统的广泛应用，安全概念扩充到完整性；访问控制技术变得更加重要，因此强调计算机系统安全；网络的发展使信息系统的应用范围不断扩大，必须要考虑网络安全；近年来信息安全又增加了新内容，即面向应用的内容安全。随着云计算等新的计算模式的出现，信息安全技术不断向前发展，也面临新的挑战。本章回顾信息安全的发展历史，介绍信息安全基本概念，讲述信息安全机制，信息安全体系结构，介绍计算机网络安全和典型的攻击与防御技术，最后探讨信息安全面临的新挑战。

5.1　信息安全概述

5.1.1　信息安全的发展历史

“信息安全”最初是指信息的保密性。在 20 世纪主机时代，人们需要保护的主要是设在专用机房内的主机以及重要数据，信息安全主要是指信息的保密性、完整性和可用性。20 世纪 80 年代以后，特别是进入 20 世纪 90 年代，随着互联网的飞速发展，信息安全的内涵也发生了巨大变化，它既面向数据、设备、网络、环境，也面向使用者，不但包含以前信息安全内涵的延续，例如面向数据的安全概念即保密性、完整性和可用性；也包含新内涵内容的提出，例如面向使用者、设备、网络、环境的安全概念即可控性、不可否认性、可靠性等。目前，信息安全已涉及攻击、防范、监测、控制、管理、评估等多方面的基础理论和实施技术，其中，密码技术和管理技术是信息安全的核心；安全标准和系统评估是信息安全的基础。可以说，现代信息安全是一个综合利用数学、物理、管理、通信和计算机等诸多学科成果的交叉学科领域，是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共信息安全、国家信息安全的总和。

本节通过一些重要发展事件的回顾，介绍信息安全研究领域的发展，经历了通信保密、系统安全、网络安全与信息保障以及云计算安全等阶段。

1. 通信保密阶段（20 世纪 40 年代～20 世纪 70 年代）

信息安全最初用于保护信息系统中处理和传递的秘密数据，注重机密性，因此主要强调的是通信安全。通信保密阶段以密码学研究为主，重在数据安全层面的研究。密码学的发展历程大致经历了三个阶段：古代加密方法、古典密码和近代密码。

1）古代加密方法

从某种意义上说，战争是科学技术进步的催化剂。人类自从有了战争，就面临着通信安

全的需求，密码技术源远流长。密码的使用已有几千年的历史，埃及人是最早使用特别的象形文字作为信息编码的人。早在公元前1世纪，恺撒大帝就曾用过一种代换式密码——Caesar密码。

古代加密方法大约起源于公元前440年，出现在古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。密码学用于通信的另一个记录是斯巴达人于公元前400年应用Scytale加密工具在军官间传递秘密信息。Scytale实际上是一个锥形指挥棒，周围环绕一张羊皮纸，将要保密的信息写在羊皮纸上。解下羊皮纸，上面的消息杂乱无章、无法理解，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息。

由上述可见，自从有了文字以来，人们为了某种需要总是想法设法隐藏某些信息，以起到保证信息安全的目的。这些古代加密方法体现了后来发展起来的密码学的若干要素，但其只能限制在一定范围内使用。

古代加密方法主要基于手工的方式实现，因此称为密码学发展的手工阶段。

2）古典加密方法

古典密码的加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形，它比古代加密方法复杂，其变化较小。古典密码的代表密码体制主要有：单表代替密码、多表代替密码及转轮密码。Caesar密码就是一种典型的单表加密体制；多表代替密码有Vigenere密码、Hill密码；著名的Enigma密码就是第二次世界大战中使用的转轮密码。

到了20世纪20年代，随着机械和机电技术的成熟，以及电报和无线电需求的出现，引起了密码设备方面的一场革命——发明了转轮密码机（简称转轮机，Rotor）。转轮机的出现是密码学发展的重要标志之一。几千年来，对密码算法的研究和实现主要是通过手工计算来完成的。随着转轮机的出现，传统密码学有了很大的进展，利用机械转轮可以开发出极其复杂的加密系统。1921年以后的十几年里，Hebern构造了一系列稳步改进的转轮机，投入美国海军的试用评估，并申请了第一个转轮机的专利。

德国的Arthur Scherbius于1919年设计出了历史上最著名的密码机——Enigma机，英国在第二次世界大战期间发明并使用TYPEX密码机，瑞典的Boris Caesar Wilhelm Hagelin发明的Hagelin C-36型密码机于1936年制造，密钥周期长度为3 900 255。对于纯机械的密码机来说，这已非常不简单。

3）近代加密方法

1949年，信息论创始人Shannon发表的论文“保密通信的信息理论”将密码学的研究引入了科学的轨道。1975年1月15日，对计算机系统和网络进行加密的DES（Data Encryption Standard，数据加密标准）由美国国家标准局颁布为国家标准，这是密码术历史上一个具有里程碑意义的事件。1976年，当时在美国斯坦福大学的迪菲（Diffie）和赫尔曼（Hellman）两人提出了公开密钥密码的新思想（论文*New Direction in Cryptography*，密码学的新方向），把密钥分为加密公钥和解密私钥，奠定了公钥密码学的基础。1977年，美国的里维斯特（Ronald Rivest）、沙米尔（Adi Shamir）和阿德勒曼（Len Adleman）提出了第一个较完善的公钥密码体制——RSA体制，这是一种建立在大数因子分解基础上的算法，这

是密码学的一场革命。

公钥密码体制的理论价值：第一，突破 Shannon 理论，从计算复杂性上刻画密码算法的强度。第二，它把传统密码算法中两个密钥管理中的保密性要求，转换为保护其中一个的保密性，保护另一个的完整性的要求。第三，它把传统密码算法中的密钥归属从通信两方变为一个单独的用户，从而使密钥的管理复杂度有了较大下降。

公钥密码体制在应用上的价值：第一，密码学的研究已经逐步超越了数据的通信保密性范围，同时开展了对数据的完整性、数字签名技术的研究，已成为最核心的密码技术。第二，随着计算机及其网络的发展，密码学已逐步成为计算机安全、网络安全的重要支柱，使得数据安全成为信息安全的核心内容，超越了以往物理安全占据计算机安全主导地位的状态。

2. 计算机系统安全阶段(20 世纪 70 年代～20 世纪 80 年代)

自从进入计算机时代，信息安全研究目标扩展到计算机系统安全。将密码技术应用到计算机通信保护的同时，开始针对信息系统的安全进行研究，重在物理安全层与运行安全层，兼顾数据安全层。随着数据库技术和信息系统的广泛应用，信息安全概念从仅侧重机密性扩充到完整性，访问控制技术变得更加重要。20 世纪 70 年代，访问控制技术取得了突破性的成果。同时，信息安全学术界形成了以安全模型分析与验证为理论基础、以信息安全产品为主要构件、以安全域建设为主要目标的安全防护体系思想；不仅涌现出安全操作系统、安全数据库管理系统、防火墙为代表的信息安全产品，同时形成了相关的信息安全产品测评标准，以及基于安全标准的测评认证制度与市场准入制度，实现了信息安全产品的特殊监管。

1969 年，B. Lampson 提出了访问控制矩阵模型，1973 年，D. Bell 和 L. Lapadula 创立了一种模拟军事安全策略的计算机操作模型——BLP 模型。由于 BLP 模型是针对机密性，所以，1977 年提出了针对完整性的 Biba 模型，1987 年提出了侧重完整性和商业应用的 Clark-Wilson 模型。1996 年提出了 RBAC96，2000 年提出了 NISTRBAC 引用参考标准，权限管理基础设施(PMI)使得访问控制在网络环境下的实施更加方便。

1985 年，美国国防部公布可信计算机系统评估准则(Trusted Computer Security Evaluation Criteria，TESEC)即橘皮书。该标准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 最初只是军用标准，后来延至民用领域。

为了建立一个各国都能接受的通用的信息安全产品和系统的安全性评估准则，1993 年 6 月，美国政府同加拿大及欧共体共同起草单一的通用准则(The Common Criteria for Information Technology security Evaluation，简称 CC 标准)，并将其推到国际标准。它综合了美国的 TCSEC、欧洲的 ITSEC、加拿大的 CTCPEC、美国的 FC 等信息安全准则，形成了一个更全面的框架。

我国国家质量技术监督局也于 1999 年发布了计算机信息系统安全保护等级划分准则(Classified Criteria for Security Protection of Computer Information System)的国家标准，序号为 GB 17859—1999，评估准则的制定为我们评估、开发研究计算机系统安全提供了指导准则。

3. 网络信息安全阶段

20世纪60年代开始，美国国防部的高级研究计划局（Advance Research Projects Agency，ARPA）开始建立ARPANET，ARPANET就是Internet的前身。Internet的迅猛发展始于20世纪90年代，由欧洲原子核研究组织CERN开发的万维网WWW被广泛使用在Internet上，大大方便了广大非网络专业人员对网络的使用，成为Internet发展的指数级增长的主要驱动力。今天的Internet已不再是计算机人员和军事部门进行科研的领域，而是变成了一个开发和使用信息资源的覆盖全球的信息海洋，覆盖了社会生活的方方面面，构成了一个信息社会的缩影。目前，互联网正从IPv4向IPv6跨越。然而Internet也有其固有的缺点，如网络无整体规划和设计，网络拓扑结构不清晰以及容错及可靠性的缺乏，而这些对于商业领域的不少应用是至关重要的。安全性问题是困扰Internet用户发展的另一主要因素。计算机病毒、网络蠕虫的广泛传播，计算机网络黑客的恶意攻击，DDoS攻击的强大破坏力、网上窃密和犯罪的增多，使得网络安全性问题关系到未来网络应用的深入发展。当信息技术快速步入网络时代，跨地域、跨管理域的协作不可避免，多个系统之间存在频繁交互或大规模数据流动，专一、严格的信息控制策略变得不合时宜，信息安全领域随即进入了以立体防御、深度防御为核心思想的信息安全保障的时代，形成了以预警、攻击防护、响应、恢复为主要特征的全生命周期安全管理，出现了大规模网络攻击与防护、互联网安全监管等各项新的研究内容。安全管理也由信息安全产品测评发展到大规模信息系统的整体风险评估与等级保护等。在这一阶段，开始针对信息安全体系进行研究，重在运行安全与数据安全层，兼顾内容安全层。

因此，网络安全的研究涉及安全策略、移动代码、指令保护、密码学、操作系统、软件工程和网络安全管理等内容。

4. 信息安全保障阶段

进入20世纪90年代，随着网络技术的进一步发展，超大型网络迫使人们必须从整体安全的角度去考虑信息安全问题。网络的开放性、广域性等特征把人们对信息安全的需求，延展到可用性、完整性、真实性、机密性和不可否认性等更全面的范畴。同时，随着网络黑客、病毒等技术层出不穷、变化多端，人们发现任何信息安全技术和手段都存在弱点，传统的“防火墙＋补丁”这样的纯技术方案无法完全抵御来自各方的威胁，必须寻找一种可持续的保护机制，对信息和信息系统进行全方位、动态的保护。1989年，美国卡内基·梅隆大学计算机应急小组开始研究如何从静态信息安全防护向动态防护转变。之后，美国国防部在其信息安全及网络战防御理论探索中吸收这一思想，并于1995年提出了“信息保障”（Information Assurance，IA）的概念。1996年，美国国防部（DoD）在国防部令S-3600.1中对信息保障做如下定义：保护和防御信息及信息系统，确保其可用性，完整性，保密性，可认证性，不可否认性等特性。这包括在信息系统中融入保护、检测、响应功能，并提供信息系统的恢复功能。这就是信息保障的PDRR模型，其5个技术环节分别如下。

（1）预警：根据以前掌握的系统脆弱性和当前了解的犯罪趋势预测未来可能受到的攻击及危害。能不能预警客观存在着空间差、时间差、知识差、能力差的问题。预警的技术支持包括：威胁分析、脆弱性分析、资产评估、风险分析、漏洞修补、预警协调。

(2) P(保护,Protect):采用可能采取的手段保障信息的保密性、完整性、可用性、可控性和不可否认性。技术手段包括:网络安全、操作系统安全、数据库系统安全访问控制、口令等保密性和完整性技术。

(3) D(检测,Detect):利用高级技术提供的工具检查系统检测可能存在的黑客攻击、白领犯罪、病毒泛滥等脆弱性。技术手段:病毒检测、漏洞扫描、入侵检测、用户身份鉴别等。

(4) R(响应,React):对危及安全的事件、行为、过程及时做出响应处理,杜绝危害的进一步蔓延扩大,力求系统尚能提供正常服务。技术手段:监视、关闭、切换、跟踪、报警、修改配置、联动、阻断等。

(5) R(恢复,Restore):一旦系统遭到破坏,尽快恢复系统功能,尽早提供正常的服务。技术手段:备份、恢复等。

1998 年 5 月,美国公布了由国家安全局 NSA 起草的 *Information Assurance Technical Framework*(信息保障技术框架),旨在为保护美国政府和工业界的信息与技术设施提供技术指南。1999 年 8 月 31 日,IATF 论坛发布了 IATF 2.0 版本,2000 年 9 月 22 日又推出了 IATF 3.0 版本。

5. 云计算安全阶段

云计算以动态的服务计算为主要技术特征,以灵活的"服务合约"为核心商业特征,是信息技术领域正在发生的重大变革。这种变革为信息安全领域带来了巨大的冲击。

(1) 在云平台中运行的各类云应用没有固定不变的基础设施,没有固定不变的安全边界,难以实现用户数据安全与隐私保护;

(2) 云服务所涉及的资源由多个管理者所有,存在利益冲突,无法统一规划部署安全防护措施;

(3) 云平台中数据与计算高度集中,安全措施必须满足海量信息处理需求。

由于当前信息安全领域仍缺乏针对此类问题的充分研究,尚难为安全的云服务提供必要的理论技术与产品支撑,因此,未来在信息安全学术界与产业界共同的关注及推动下,信息安全领域将围绕云服务的"安全服务品质协议"的制定、交付验证、第三方检验等,逐渐发展形成一种新型的技术体系与管理体系与之相适应,这标志着信息安全领域一个新的时代的到来。从目前来看,实现云计算安全至少应解决关键技术、标准与法规建设以及国家监督管理制度等多个层次的挑战。下面分别予以简要阐述。

挑战 1:建立以数据安全和隐私保护为主要目标的云安全技术框架。

当前,云计算平台的各个层次,如主机系统层、网络层以及 Web 应用层等都存在相应安全威胁,但这类通用安全问题在信息安全领域已得到较为充分的研究,并具有比较成熟的产品。研究云计算安全需要重点分析与解决云计算的服务计算模式、动态虚拟化管理方式以及多租户共享运营模式等对数据安全与隐私保护带来的挑战。

挑战 2:建立以安全目标验证、安全服务等级测评为核心的云计算安全标准及其测评体系。

建立安全指导标准及其测评技术体系是实现云计算安全的另一个重要支柱。云计算安全标准是度量云用户安全目标与云服务商安全服务能力的尺度,也是安全服务提供商构建安全服务的重要参考。基于标准的"安全服务品质协议",可以依据科学的测评方法检测与

评估，在出现安全事故时快速实现责任认定，避免产生责任推诿。

挑战3：建立可控的云计算安全监管体系。

科学技术是把双刃剑，云计算在为人们带来巨大好处的同时也带来巨大的破坏性能力。而网络空间又是继领土权、领空权、领海权、太空权之后的第5维国家主权，是任何主权国家必须自主掌控的重要资源。因此，应在发展云计算产业的同时大力发展云计算监控技术体系，牢牢掌握技术主动权，防止其被竞争对手控制与利用。

5.1.2 信息安全基本概念

1. 信息安全的定义

信息安全领域的发展历程已多次证明，信息技术的重大变革将直接影响信息安全领域的发展进程。从通信保密到系统安全，从网络安全到信息安全保障，信息安全定义随着网络与信息技术的发展而不断发生变化，其含义也在动态地发生变化。

从理念上看，以前信息安全强调的是“规避风险”，即防止发生并提供保护，破坏发生时无法挽回；而信息保障强调的是“风险管理”，即综合运用保护、探测、响应和恢复等多种措施，使得信息在攻击突破某层防御后，仍能确保一定级别的可用性、完整性、真实性、机密性和不可否认性，并能及时对破坏进行修复。以前信息安全通常是单一或多种技术手段的简单累加，而信息保障则是对加密、访问控制、防火墙、安全路由等技术的综合运用，更注重入侵检测和灾难恢复技术。

信息安全逐渐演变成一个综合、交叉的学科领域，不再仅限于对传统意义上的网络和计算机技术进行研究，必须要综合利用数学、物理、通信、计算机以及经济学等诸多学科的长期知识积累和最新发展成果，进行自主创新研究，并提出系统的、完整的、协同的解决方案。例如，防电磁辐射、密码技术、数字签名、信息安全成本和收益等方面的研究都分别涉及并综合了计算机、物理学、数学以及经济学上的一些原理。但是严格来说信息安全并没有明确的定义，而只有一些相关的描述。

国际标准化委员会定义的信息安全概念是：为数据处理系统而采取的技术和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。

ISO/IEC 17799定义信息安全是：通过实施一组控制而达到的，包括策略、措施、过程，组织结构及软件功能，是对机密性、完整性和可用性保护的一种特性。机密性确保信息只能被授权访问方所接收，完整性即保护信息处理手段的正确与完整，可用性确保授权用户在需要时能够访问信息相关资源。

我国相关立法给出的定义是：保障计算机及其相关的和配套的设备、设施（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，以维护计算机系统的安全。

从上述定义看，信息安全涵盖两个层次：第一，从信息层次来看，信息安全要保证信息的完整性和保密性。完整性即保证信息的来源、去向、内容真实无误；保密性即保证信息不会被非法泄漏与扩散。第二，从网络层次来看，要达到可用性和可控性。可用性即保证网络和信息系统随时可用，运行过程不出现故障，并且在遇到意外情况时能够尽量减少损失，并

尽早恢复正常；可控性即对网络信息的传播具有控制能力。

2. 安全服务

计算机信息系统的安全目标主要有：保密性、完整性、身份识别、可用性、不可否认性等。其中，机密性、完整性和可用性是信息安全的三个核心安全目标，这5个安全目标对应着5种基本的安全服务。对这5个安全目标的解释随着他们所处环境的不同而不同。在某种特定的环境下，对某种安全服务的解释也是由个体需求、习惯和特定组织的法律所决定的。

1）机密性

NIST关于机密性的定义：机密性是指对信息或资源的隐藏。信息保密的需求源自计算机在敏感领域的使用，比如政府或企业。即，机密性指确保信息资源仅被合法的用户、实体或进程访问，使信息不泄漏给未授权的用户、实体或进程。

2）完整性

NIST关于完整性的定义：完整性指的是数据或资源的可信度，通常使用防止非授权的或者未经授权的数据改变来表达完整性。完整性指信息资源只能由授权方式或以授权的方式修改，在存储或传输过程中不丢失、不被破坏。完整性的破坏一般来自三个方面：未授权、未预期、无意。

3）可用性

NIST关于可用性的定义：可用性是指对信息或资源的期望使用能力。即：信息可被合法用户访问并按要求的特性使用而不遭拒绝服务。可用的对象包括：信息、服务和IT资源。

4）不可否认性

不可否认性指信息的发送者无法否认已发出的信息或信息的部分内容，信息的接收者无法否认已经接收的信息或信息的部分内容。无论是授权的使用还是非授权的使用，事后都应该是有据可查的。对于非授权的使用，必须是非授权的使用者无法否认或抵赖的，这应该是信息安全的最后一个重要环节。

5）认证

认证是安全的最基本要素。信息系统的目的就是供使用者使用，但只能给获得授权的使用者使用，因此，首先必须知道来访者的身份。使用者可以是人、设备和相关系统，无论是什么样的使用者，安全的第一要素就是对其进行认证。在信息化系统中，对每一个可能的入口都必须采取认证措施，对无法采取认证措施的入口必须完全堵死，从而防堵每一个安全漏洞。

这5种安全服务已经基本上覆盖了现有的攻击。但应当说明的是，5种安全目标绝对没有覆盖未来发现的攻击行为。这一点同其他学科不大一样，因为攻、防本身是在不断变化发展的。不同行业不同用户对于上述安全目标有不同的侧重。

5.1.3 信息安全攻击

TX.800标准将常说的网络安全(Network Security)进行逻辑上的分别定义，即安全攻

击（Security Attack）是指损害机构所拥有信息的安全的任何行为；安全机制（Security Mechanism）是指设计用于检测、预防安全攻击或者恢复系统的机制；安全服务（Security Service）是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务。给定一类应用对安全需求归结为一些基本要素，称为安全目标（安全服务），目标通过合理配置安全机制实现。

针对信息安全的三个核心要素——机密性、完整性、可用性，它们会被安全攻击所威胁。根据上述三类安全目标将攻击划分成以下几个分类。

1. 威胁机密性的攻击

1）窃听

窃听指在未经授权的情况下访问或拦截信息。例如，一个在网络上传输的文件可能含有机密信息，某未经授权的实体就有可能拦截该传输并利用其内容以牟利。为避免被窃听，通常使用本章中讨论的加密技术，就可以使文件成为对拦截者不可解的信息。

用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。

2）流量分析

窃听和数据分析是指攻击者通过对通信线路或通信设备的监听，或通过对通信量（通信数据流）的大小、方向频率的观察，经过适当分析，直接推断出秘密信息，达到信息窃取的目的。例如，可以获得发送者或者接收者的电子地址（如电子邮箱地址），也可以通过收集通信双方的信息来猜测交易的本质。流量分析攻击通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

2. 威胁完整性的攻击

1）篡改

拦截或访问信息后，攻击者可以修改信息使其对己有利。例如，某客户为一笔交易给银行发送信息，攻击者即可拦截信息并将其改变为对己有利的交易形式。值得注意的是，有时攻击者只要简单地删除或拖延信息就能给网络造成危害并从中牟利。

2）伪装

伪装或欺骗就是攻击者假扮成某人。例如，攻击者伪装为银行的客户，从而盗取银行客户的银行卡密码和个人身份证号码。有时攻击者也可能伪装为接收方。例如，当用户设法联系某银行的时候，另外一个地址伪装为银行，从用户那里得到某些相关的信息。

插入、重放：攻击者通过把网络传输中的数据截获后存储起来并在以后重新传送，或把伪造的数据插入到信道中，使得接收方收到一些不应当收到的数据。这种攻击通常也是为了达到假冒或破坏的目的。但是通常比截获/修改的难度大，一旦攻击成功，危害性也大。

3）否认

这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。

3. 威胁可用性的攻击

威胁可用性的攻击指对信息或其他资源的合法访问被无条件地阻止。典型的威胁可用性的攻击是拒绝服务攻击(DoS)。拒绝服务攻击的目的是摧毁计算机系统的部分乃至全部进程,或者非法抢占系统的计算资源,导致程序或服务不能运行,从而使系统不能为合法用户提供正常的服务。目前,最有杀伤力的拒绝服务攻击是网络上的分布式拒绝服务(DDoS)攻击。

网络拒绝服务是指攻击者通过对数据或资源的干扰、非法占用、超负荷使用,对网络或服务基础设施的摧毁,造成系统永久或暂时不可用,合法用户被拒绝或需要额外等待,从而实现破坏的目的。许多常见的拒绝服务攻击都是由网络协议(如 IP 协议)本身存在的安全漏洞和软件实现中考虑不周共同引起的。例如,TCP SYN 攻击,利用了 TCP 连接需要分配的内存,多次同步将使其他连接不能分配到足够内存,从而导致了系统暂时不可用。

计算系统受到上述类型的攻击可能是黑客或敌手操作实现的,也可能是网络蠕虫或其他恶意程序造成的。典型示例有 SYN Flood 攻击、Ping Flood 攻击、Land 攻击等。

4. 其他类型的攻击

除了上面明确分类的攻击之外,还存在很多其他类型的攻击,如:信息泄漏,非法使用(非授权访问),假冒,旁路控制,授权侵犯,特洛伊木马,陷阱门,计算机病毒,人员不慎,媒体废弃信,物理侵入,窃取,业务欺骗等。这些攻击都不同程度地对系统造成威胁。

5. 主动攻击与被动攻击

根据在系统中的作用,威胁信息系统的攻击可以划分为两大类:主动攻击和被动攻击。

1) 被动攻击

在被动攻击中,攻击者的目的只是获取信息,这意味着攻击者不会篡改或危害系统。系统可以不中断其正常运行。然而,攻击可能危害信息的发送者或者接收者。威胁信息机密性的攻击——窃听和流量分析均属于被动攻击。信息的暴露会危害信息的发送者或接收者,但是系统不会受到影响。因此,在信息发送者或接收者发现机密信息已经泄漏之前,要发现这种攻击是很困难的。然而,被动攻击可以通过对信息进行加密而避免。

被动攻击主要是收集信息而不是进行访问,数据的合法用户对这种活动一点儿也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。报文内容泄漏、通信分析法等属于被动攻击。

2) 主动攻击

主动攻击可能改变信息或危害系统。威胁信息完整性和有效性的就是主动攻击。主动攻击通常易于检测但却难于防范,因为攻击者可以通过多种方法发起攻击。主动攻击包含攻击者访问他所需信息的故意行为。拒绝服务攻击、信息篡改、资源使用、欺骗等属于主动攻击。

这样分类不是说主动攻击不能收集信息或被动攻击不能被用来访问系统。多数情况下这两种类型被联合用于入侵一个站点。但是,大多数被动攻击不一定包括可被跟踪的行为,因此更难被发现。从另一个角度看,主动攻击容易被发现但多数公司都没有发现,所以发现被动攻击的机会几乎是零。

5.1.4 安全策略

计算机系统的安全策略是为描述系统的安全需求而制定的对用户行为进行约束的一套严谨的规则，这些规则是对允许什么、禁止什么的规定，是指在某个安全区域内（一个安全区域，通常是指属于某个组织的一系列处理和通信资源），用于所有与安全相关活动的一套规则。这些规则是由此安全区域中所设立的一个安全权力机构建立的，并由安全控制机构来描述、实施或实现。

信息安全策略是一组规则，它们定义了一个组织要实现的安全目标和实现这些安全目标的途径。信息安全策略可以划分为两个部分：问题策略（Issue Policy）和功能策略（Functional Policy）。问题策略描述了一个组织所关心的安全领域和对这些领域内安全问题的基本态度。功能策略描述如何解决所关心的问题，包括制定具体的硬件和软件配置规格说明、使用策略以及雇员行为策略。

信息安全策略必须有清晰和完全的文档描述，必须有相应的措施保证信息安全策略得到强制执行。在组织内部，必须有行政措施保证既定的信息安全策略被不打折扣地执行，管理层不能允许任何违反组织信息安全策略的行为存在，另一方面，也需要根据业务情况的变化不断地修改和补充信息安全策略。

信息安全策略的内容应该有别于技术方案，信息安全策略只是描述一个组织保证信息安全的途径的指导性文件，它不涉及具体做什么和如何做的问题，只需指出要完成的目标。信息安全策略是原则性的和不涉及具体细节，对于整个组织提供全局性指导，为具体的安全措施和规定提供一个全局性框架。在信息安全策略中不规定使用什么具体技术，也不描述技术配置参数。信息安全策略的另外一个特性就是可以被审核，即能够对组织内各个部门信息安全策略的遵守程度给出评价。

信息安全策略的描述语言应该是简洁的、非技术性的和具有指导性的。比如，一个涉及对敏感信息加密的信息安全策略条目可以这样描述："任何类别为机密的信息，无论存储在计算机中，还是通过公共网络传输时，必须使用本公司信息安全部门指定的加密硬件或者加密软件予以保护。"这个叙述没有涉及加密算法和密钥长度，所以当旧的加密算法被替换，新的加密算法被公布的时候，无须对信息安全策略进行修改。

5.1.5 安全机制

安全机制是实施安全策略的方法、工具或者规程。安全机制是指用来保护系统免受侦听、阻止安全攻击及恢复系统的机制。通常，信息安全机制包括三个大类：防护机制、检测机制与恢复机制。安全机制可通过密码、软件、硬件、策略以及物理安全来实现。在体系上可分为密码技术、安全控制技术（如访问控制技术、口令控制技术）和安全防护技术（防火墙技术、计算机网络病毒防治技术、信息泄漏防护技术）。

1. 加密技术

加密技术能为数据或通信信息流提供机密性。同时对其他安全机制的实现起主导作用

或辅助作用。可通过对称密码或者公钥密码实现。

1）对称密码

信息的发送方和接收方用同一个密钥去加密和解密数据。它的最大优势是加/解密速度快，适合于对大数据量进行加密，但密钥管理困难。如果通信的双方能够确保专用密钥在密钥交换阶段未曾泄漏，那么机密性和报文完整性就可以通过这种加密方法加密机密信息、随报文一起发送报文摘要或报文散列值来实现。

2）非对称加密

使用一对密钥来分别完成加密和解密操作，其中一个公开发布（即公钥），另一个由用户自己秘密保存（即私钥）。信息交换的过程是：甲方生成一对密钥并将其中的一把作为公钥向其他交易方公开，得到该公钥的乙方使用该密钥对信息进行加密后再发送给甲方，甲方再用自己保存的私钥对加密信息进行解密。

3）密钥管理

加密机制的使用产生了密钥管理的需求，从而产生出了密钥管理机制。密钥管理技术划分为以下三类。

（1）对称密钥管理。对称加密是基于共同保守秘密来实现的。采用对称加密技术的贸易双方必须要保证采用的是相同的密钥，要保证彼此密钥的交换是安全可靠的，同时还要设定防止密钥泄密和更改密钥的程序。这样，对称密钥的管理和分发工作将变成一件潜在危险的和烦琐的过程。通过公开密钥加密技术实现对称密钥的管理使相应的管理变得简单和更加安全，同时还解决了纯对称密钥模式中存在的可靠性问题和鉴别问题。

（2）公开密钥管理/数字证书。贸易伙伴间可以使用数字证书（公开密钥证书）来交换公开密钥。国际电信联盟（ITU）制定的标准 X.509 对数字证书定义，该标准等同于国际标准化组织（ISO）与国际电工委员会（IEC）联合发布的 ISO/IEC 9594-8：195 标准。数字证书通常包含唯一标识证书所有者（即贸易方）的名称、唯一标识证书发布者的名称、证书所有者的公开密钥、证书发布者的数字签名、证书的有效期及证书的序列号等。证书发布者一般称为证书管理机构（CA），它是贸易各方都信赖的机构。数字证书能够起到标识贸易方的作用，是目前电子商务广泛采用的技术之一。

（3）密钥管理相关的标准规范。目前国际有关的标准化机构都着手制定关于密钥管理的技术标准规范。ISO 与 IEC 下属的信息技术委员会（JTC1）已起草了关于密钥管理的国际标准规范。该规范主要由三部分组成：一是密钥管理框架；二是采用对称技术的机制；三是采用非对称技术的机制。该规范现已进入到国际标准草案表决阶段，并将很快成为正式的国际标准。

2. 信息的完整性

完整性证明是在数据的传输过程中，验证收到的数据是否与原来数据保持完全一致的手段。有两类消息的鉴别：数据单元的完整性鉴别和数据流的完整性鉴别。数据单元的鉴别是数据的生成者（或发送者）计算的普通分组校验码、用传统密码算法计算的鉴别码、用公钥密码算法计算的鉴别码，附着在数据单元后面，数据的使用者（或接收者）完成对应的计算（可与生成者的相同或不同），从而检验数据是否被篡改或假冒。

3. 数字签名

数字签名也称电子签名，如同出示手写签名一样，能起到电子文件认证、核准和生效的作用。其实现方式是把散列函数和公开密钥算法结合起来，发送方从报文文本中生成一个散列值，并用自己的私钥对这个散列值进行加密，形成发送方的数字签名；然后，将这个数字签名作为报文的附件和报文一起发送给报文的接收方；报文的接收方首先从接收到的原始报文中计算出散列值，接着再用发送方的公开密钥来对报文附加的数字签名进行解密；如果这两个散列值相同，那么接收方就能确认该数字签名是发送方的。数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充、篡改等问题。

4. 身份识别

各种系统通常为用户设定一个用户名或标识符的索引值。身份识别就是后续交互中当前用户对其标识符一致性的一个证明过程，通常是用交互式协议实现的。常用的身份识别技术如下。

（1）口令：验证方提示证明方输入口令，证明方输入后由验证方进行真伪识别。

（2）密码身份识别协议：使用密码技术，可以构造出多种身份识别协议，如挑战-应答协议、零知识证明、数字签名识别协议等。

（3）使用证明者的特征或拥有物的身份识别协议：如指纹、面容、虹膜等生物特征，身份证、IC卡等拥有物的识别协议。当然这些特征或拥有物独一无二的概率很大。

5. 流量填充

通信量通常会泄漏信息。为了防止敌手对通信量的分析，需要在空闲的信道上发送一些无用的信息，以便蒙蔽敌手（当然填充的信息经常要使用机密性服务），这就称为通信量填充机制。在专用通信线路上这种机制非常重要，但在公用信道中则要依据环境而定。信息隐藏则是把信息隐藏到看似与之无关的消息（如图像文件等）中，以便蒙蔽敌手，通常也要和密码技术结合才能保证不被敌手发现。通信量填充和信息隐藏是一组对偶的机制。前者发送有形式无内容的消息，而后者发送有内容“无”形式的消息，以达到扰乱的目的。

6. 路由控制

路由控制是对于信息的流经路径的选择，为一些重要信息指定路径，例如通过特定的安全子网、中继或连接设备，也可能是要绕开某些不安全的子网、中继或连接设备。这种路由可以是预先安排的或者作为恢复的一种方式而由端系统动态指定。路由控制则是一种一般的通信环境保护。恰当的路由控制可以提升环境的安全性，从而可能会因此简化其他安全机制实施的复杂性。

7. 公证

在两方或多方通信中，公证机制可以提供数据的完整性，发/收方的身份识别和时间同步等服务。通信各方共同信赖的公证机构，称为可信第三方，它保存通信方的必要信息，并以一种可验证的方式提供上述服务。通信各方选择可信第三方指定的加密、数字签名和完整

性机制，并和可信第三方做少量的交互，实现对通信的公证保护。例如证书权威机构 CA，通过为各通信方提供公钥证书和相关的目录、验证服务，从而实现了一部分公证机构的职能。

8. 访问控制

访问控制机制使用实体的标识、类别（如所属的实体集合）或能力，从而确定权限、授予访问权。按用户身份及其所归属的某预定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。其功能主要有以下几种：①防止非法的主体进入受保护的网络资源；②允许合法用户访问受保护的网络资源；③防止合法的用户对受保护的网络资源进行非授权的访问。访问控制机制基于下列几种技术：访问信息库、识别信息库、能力信息表、安全等级。

9. 事件检测与安全审计

事件检测对所有用户与安全相关的行为进行记录，以便对系统的安全进行审计。与安全相关的事件检测，包括对明显违反安全规则的事件和正常完成事件的检测。其处理过程首先是对事件集合给出一种定义，这种定义是关于事件特征的描述，而这些特征又应当是易于捕获的。一旦检测到安全相关的事件，则进行事件报告（本地的和远程的）和存档。安全审计则在专门的事件检测存档和系统日志中提取信息，进行分析、存档和报告，是事件检测的归纳和提升。安全审计的目的是为了改进信息系统的安全策略、控制相关进程，同时也是执行相关的恢复操作的依据。对于分布式的事件检测或审计，要建立事件报告信息和存档信息的语义和表示标准，以便信息的交换。目前经常提到的漏洞扫描和入侵检测都属于事件检测和审计的范畴。

10. 恢复机制

恢复包括对数据的恢复和对网络计算机系统运行状态的恢复。数据恢复，电子数据恢复是指通过技术手段，将保存在台式计算机硬盘、笔记本硬盘、服务器硬盘、存储磁带库、移动硬盘、U 盘、数码存储卡、MP3 等设备上丢失的电子数据进行抢救和恢复的技术。计算机系统运行状态恢复是指把系统恢复到安全状态之下。

5.1.6 信息安全体系结构

体系结构是由英文单词 architecture 翻译而来，其最常用的解释就是“建筑”。可见，与任何一个“建筑”相类似，一个体系结构应该包括一组组件及其组件之间的联系。从系统工程的观点看，任何复杂的系统都是由相对简单的、具有层次结构的基本元素组成。这些基本元素彼此之间存在着复杂的相互作用，某些元素还可能具有非常复杂的内部结构。该解释帮助我们理解体系结构的重点所在，即元素及其关系。

信息安全体系结构是针对信息系统而言的，一般信息系统的安全体系结构是系统信息安全功能定义、设计、实施和验证的基础，该体系结构应在反映整个信息系统安全策略的基础上，描述该系统安全组件及其相关组件相互间的逻辑关系和功能分配。这种描述的合理性和准确性将直接关系信息系统安全策略的实现效果。

结合上述基本定义，信息系统安全由技术体系、管理体系和组织体系组成，如图5-1所示，该体系结构包括三个层面：技术体系、组织机构体系与管理体系。这三个层面互为三棱锥，缺一不可。

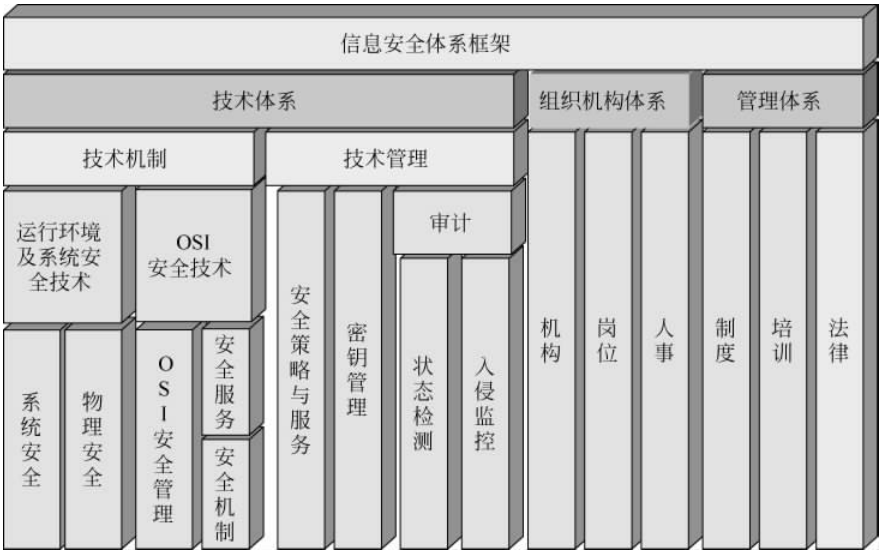

图5-1　信息安全体系框架

技术体系包含以下安全技术。

1. 物理安全技术

信息系统的建筑物、机房条件及硬件设备条件满足信息系统的机械防护安全；通过对电力供应设备以及信息系统组件的抗电磁干扰和电磁泄漏性能的选择性措施达到相应的安全目的。物理安全技术运用于物理保障环境（含系统组件的物理环境）。

2. 系统安全技术

通过对信息系统与安全相关组件的操作系统的安全性选择措施或自主控制，使信息系统安全组件的软件工作平台达到相应的安全等级，一方面避免操作平台自身的脆弱性和漏洞引发的风险，另一方面阻塞任何形式的非授权行为对信息系统安全组件的入侵或接管系统管理权。硬件机制主要包括PC物理保护、基于硬件的访问控制技术、可信计算与安全芯片、硬件防辐射技术和计算机运行环境安全问题。操作系统安全机制主要包括存储保护、用户认证和访问控制技术。数据库系统安全主要包括数据库的安全性、完整性、并发控制、备份与恢复等安全机制。

3. 网络安全技术（网络层安全）

网络安全技术主要体现在网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段、网络设施防病毒、防火墙与入侵检测系统、网络隔离技术、网络安全协议等。

4. 应用安全技术(应用层安全)

应用安全技术主要由提供服务所采用的应用软件和数据的安全性产生,包括 Web 服务、电子邮件系统、DNS 等,以及因编程不当引起的缓冲区漏洞,开发安全的应用系统的编程方法、软件保护的技术措施,还包括病毒对系统的威胁。

5. 管理安全性(管理层安全)

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个网络的安全,严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

组织体系结构是信息系统安全的组织保障系统,由机构、岗位和人事三个模块构成一个体系。管理机构的设置分为三个层次:决策层、管理层和执行层。决策层是信息系统安全的领导机构,负责本单位信息安全的策略制定及其宏观调控。通常由单位主管信息系统的负责人负责,由行使国家安全、公安、机要和保密等职能的部门负责人和信息系统主要负责人组成。

管理层是决策层的日常管理机关,根据决策层的信息安全策略,全面规划并且协调各力量实施信息系统的安全方案,制定、修改安全策略,处理安全事故,设置安全岗位。执行层是在管理层的协调下具体负责某一个或几个特定安全事务的群体,负责具体事务的操作与落实。岗位是信息系统安全管理机关根据系统安全需要设定的负责某一个或某几个安全事务的职位。人事机构是根据管理机构设定的岗位,对岗位上在职、待职和离职的雇员进行素质教育、业绩考核和安全监管的机构。人员是信息安全实施的主体,其活动在国家有关安全的法律、法规、政策范围内进行。随着人们对信息安全重视程度的提高,“人是第一位的”已经成为一个逐渐被接受的观点。这里所说的人包括信息安全保障目标的实现过程中所有的相关人员,例如,机构信息安全保障目标的制定与实施人员,业务系统的设计、开发、维护和管理人员,这些系统(或产品)的用户,可能存在的网络入侵人员,信息安全事件报告、分析、处理人员,信息安全法律顾问等。

俗话说,“三分技术,七分管理”,可见管理在信息安全保障中的重要性。管理是信息系统安全的灵魂。信息系统安全的管理体系由法律管理、制度管理和培训管理三个部分组成。

教育培训是培育信息安全公众或专业人才的重要手段,我国近些年来在信息安全正规教育方面也推出了一些相应的科目与专业,国家各级以及社会化的信息安全培训也得到了开展,但这些仍然是不够的,社会教育深入与细化程度与美国等发达国家比较仍有差距。

5.2 计算机网络安全

5.2.1 网络安全协议

前述网络的 OSI 模型是一种抽象的概念模型,而 TCP/IP 是目前网络的主流,其 4 层结构模型(应用层、传输层、网络层和网络接口层)是网络安全的主要研究参考对象。

计算机网络设计之初主要是为了方便资源的共享等应用，没有考虑网络的安全性问题，在 TCP/IP 中有许多的安全问题，主要包括以下几个方面。

（1）TCP/IP 不能提供可靠的身份识别。在协议中使用 IP 地址作为网络结点的唯一标识，而 IP 地址很容易被伪造和篡改，因此通信双方只能采用另外的技术手段来确认对方的真实身份。

（2）TCP/IP 对数据都没有加密，一个数据包在传输过程中会经过很多路由器和网段，在其中的任何一个环节都可能被窃听。更严重的是，现有大部分协议都是明文在网络上传输的，攻击者只需简单安装一个网络嗅探器，就可以得到通过本结点的所有网络数据包。

（3）TCP/IP 中缺乏可靠的信息完整性验证手段。在 IP 中仅对 IP 头实现校验和保护。在 UDP 中，对整个报文的校验和检查是可选的。因为攻击者可以对报文内容进行修改后，重新计算校验和。另外，TCP 的序列号也可以被随意修改，从而可以在源数据流中添加和删除数据。

（4）TCP/IP 设计的一个基本原则是自觉原则，协议中没有提供任何机制来控制资源分配，因此，攻击者可以通过发送大量的垃圾数据包来阻塞网络，也可以发送大量的连接请求对服务器造成拒绝服务攻击。

（5）TCP/IP 中缺乏对路由协议的鉴别，因此可以利用修改数据包中的路由信息来误导网络数据的传输。

（6）在实现 TCP、UDP 时中还存在许多安全隐患。例如，TCP 的三次握手过程可能导致系统受到 SYN Flood 攻击，UDP 是面向无连接的协议，攻击者极易利用 UDP 发起 IP 源路由和拒绝服务攻击。

（7）TCP/IP 设计问题导致其上层的应用协议存在许多安全问题。通过修改网络数据包影响信息的完整性，通过窃听网络数据影响信息的机密性；通过 IP 欺骗、TCP 会话劫持影响信息的真实性，另外还可以对网络服务及网络传输进行阻塞，造成拒绝服务。

因此，为了保障网络系统的安全，采取的主要措施有如下几种。

1. 协议安全

针对 TCP/IP 中存在的许多安全缺陷，必须使用加密技术、鉴别技术等来实现必要的安全协议。安全协议可以放置在 TCP/IP 协议栈的各层中（见图 5-2），如 IPSec 位于 IP 层，SSL 协议位于 TCP 与应用层之间，应用层针对不同的应用有一系列的安全协议，如 PGP、SET 等。

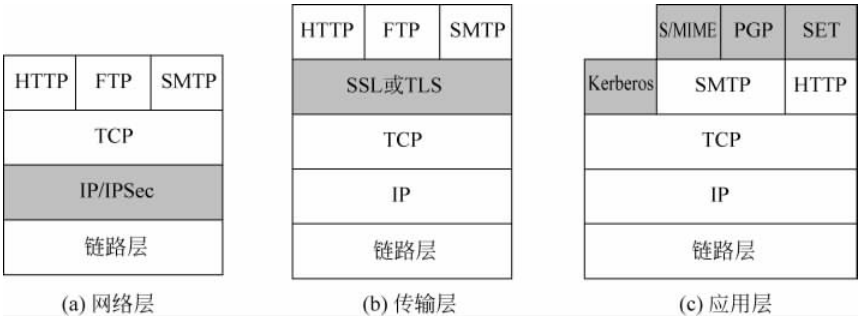

图 5-2　一些典型的安全通信协议所处的位置

2. 访问控制

网络的主要功能是资源共享，但共享是在一定范围、一定权限内的共享，因此需要严格控制非法的访问，保护资源的合法使用。一般通过定义有效的安全策略，控制网络内部资源的合法使用和实施网络边界安全设施来实现。

3. 系统安全

软件系统包括操作系统、应用系统。软件系统存在着一些有意或无意的缺陷，因此既要在设计阶段引入安全概念，也要在具体实现时减少缺陷，编写安全的代码，才能有效提高系统的安全性。

4. 其他安全技术

上述三类安全措施，并不能完全保障网络系统的安全，还需要有针对网络系统安全威胁的检测和恢复技术，如入侵检测、防病毒等安全专项技术。

5.2.2 VPN

1. VPN 概述

随着信息数字化、网络化应用的发展，内部局域网 Intranet 依托 Internet 进行通信，出差人员需要随时随地访问单位的 Intranet 获得信息；分布在各地的下属分支机构需要与总部的 Intranet 互通信息；合作伙伴、产品供应商等需要与企业的 Intranet 连接，互通信息。

早期只能通过租用专线、建立拨号服务等方式解决上述需求，费用昂贵，而且扩展性不好，不能很好地满足机构规模扩大等的需要。现在使用的 VPN(Virtual Private Network，虚拟专用网)，是指通过在一个公用网络(如 Internet 等)中建立一条安全、专用的虚拟通道，连接异地的两个网络，构成逻辑上的虚拟子网。通过 VPN 从异地连接到机构的 Intranet，就像在本地 Intranet 上一样。其中，V(Virtual)是相对于传统的物理专线而言，VPN 是通过公用网络建立一个逻辑上的、虚拟的专线，实现物理专线所具有的功效；P(Private)，顾名思义，是指私有专用的特性，一方面是只有经过授权的用户才能够建立或使用 VPN 通道，另一方面是通道内的数据进行了加密，不会被第三者获取利用；N(Network)，表明这是一种组网技术，也就是说为了应用 VPN，需要有相应的设备、软件来支撑。

VPN 因其安全可靠、容易部署、价格低廉等优点，已经被越来越广泛地应用。

(1) 安全可靠。VPN 对通信数据进行了加密认证，有效地保证了数据通过公用网络传输时的安全性，保证数据不会被未授权的人员篡改。

(2) 易于部署。VPN 只是在结点部署 VPN 设备，然后通过公用网络建立起犹如置身于内部网络的安全连接。如果要与新的网络建立 VPN 通信，只需增加 VPN 设备，改变相关配置即可。与专线连接相比较，特别是在需要安全连接的网络越来越多时，VPN 的实施就要简单很多，费用也可以节约很多。

(3) 成本低廉。如果通过专线进行网络间的安全连接，租金昂贵。而 VPN 通过公共网

络建立安全连接，只需一次性投入 VPN 设备，价格也比较便宜，大大节约了通信成本。

2. VPN 技术原理

VPN 是通过公用网络来传输企业内部数据，因此需要确保传输的数据不会被窃取、篡改，其安全性的保证主要通过密码技术、身份鉴别技术、隧道技术和密钥管理技术。在此主要介绍 VPN 的基本技术——隧道技术。

所谓隧道，类似于点到点连接技术，在源结点对数据进行加密封装，然后通过在一个公用网络（如 Internet）中建立一条数据通道——隧道，将数据传送到目标结点，目标结点对数据包进行反解，得到原始数据包。

隧道由隧道协议形成，主要有在链路层进行隧道处理的第二层隧道协议，以及在网络层进行隧道处理的第三层隧道协议。

第二层隧道协议是先把需要传输的协议包封装到 PPP 中，再把新生成的 PPP 包封装到隧道协议包中，然后通过第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等，其中 L2TP 是目前的 IETF 标准。第三层隧道协议是把需要传输的协议包直接封装到隧道协议包中，新生成的数据包通过第三层协议进行传输。第三层隧道协议有 IPSec。

第二层隧道协议一般包括创建、维护和终止三个过程，它们的报文相应有控制报文与数据报文两种。而第三层隧道协议则不对隧道进行维护。

隧道建立以后，就可以通过隧道，利用隧道数据传输协议传输数据。例如，当隧道客户端向服务器端发送数据时，客户端首先对数据包进行封装，加上一个隧道数据传送协议包报头，然后把封装的数据通过公共网络发送到隧道的服务器端。隧道服务器端收到数据包之后，去掉隧道数据传输协议包报头，然后将数据包转发到目标网络。

为实现在专用或公共 IP 网络上的安全传输，以加密为例，IPSec 隧道模式使用安全方式封装整个 IP 包，然后对加密的负载再次封装在明文 IP 包内，通过网络发送到隧道服务器端。隧道服务器对接收到的数据包进行处理，在去除明文 IP 包头，对内容进行解密之后，获得最初的负载 IP 包。负载 IP 包在经过正常处理之后被路由到位于目标网络的目的地。

3. VPN 的应用

VPN 在实际应用中，主要有三种应用模式，分别是企业内部型 VPN（Intranet VPN）、企业扩展型 VPN（Extranet VPN）和远程访问型（Access VPN）。

1）Intranet VPN

Intranet VPN 应用于企业内部两个或多个异地网络的互联，实施一样的安全策略。两个异地网络通过 VPN 安全隧道进行通信，在一个局域网中访问异地的另一个局域网时，如同在本地网络一样，如图 5-3 所示。

2）Extranet VPN

Extranet VPN 应用于企业网络与合作者、客户等网络的互联，与 Intranet VPN 不同的是，它要与不同单位的内部网络建立连接，需要应用不同的协议，对不同的网络要有不同的安全策略，如图 5-4 所示。

3）Access VPN

Access VPN 应用于远程办公，是个人通过互联网与企业网络的互联。如员工出差外

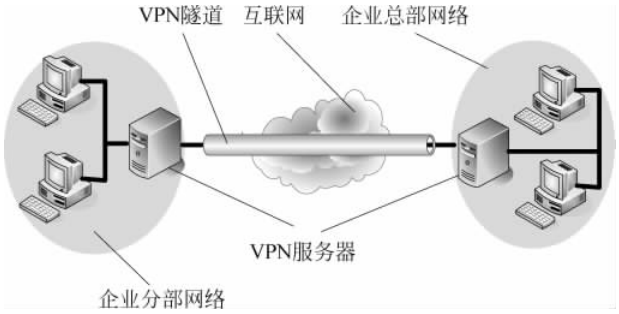

图 5-3 Intranet VPN

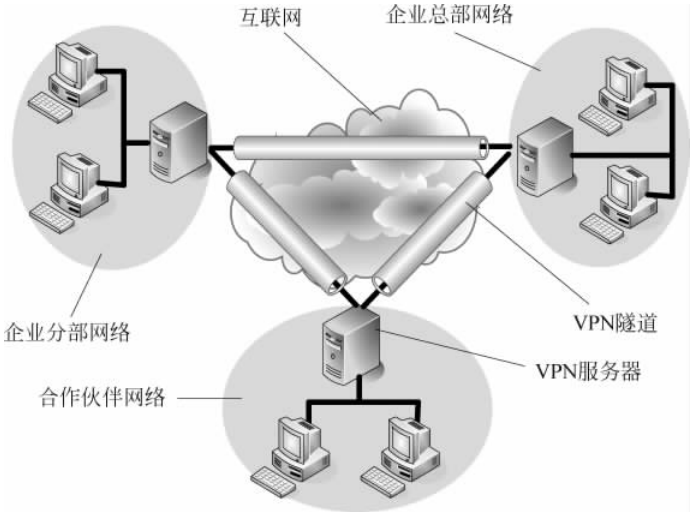

图 5-4 Extranet VPN

地,或在客户工作环境,或在家里时,首先通过拨号、ISDN、ADSL 等方式连接互联网,然后再通过 VPN 连接企业网络,如同工作在企业内部网络中,实现远程办公,如图 5-5 所示。

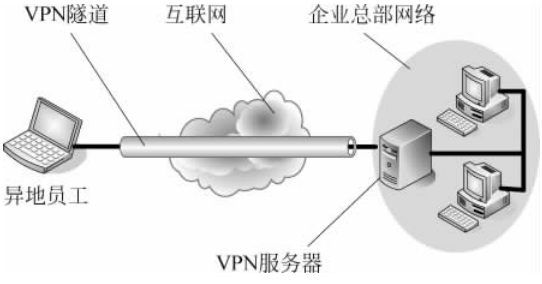

图 5-5 Access VPN

5.2.3 防火墙

1. 概述

随着计算机的应用由单机发展到网络,安全问题日益严重。计算机单机防护的方式已

经不能适应计算机网络发展的需要，计算机系统的信息安全防护由单机防护向网络防护发展。防火墙是计算机网络中的边境检查站，如图5-6所示，受防火墙保护的是内部网络。也就是说，防火墙是部署在两个网络之间的一个或一组部件，要求所有进出内部网络的数据流都通过它，并根据安全策略进行检查，只有符合安全策略、被授权的数据流才可通过，由此保护内部网络安全。它是一种按照预先制定的安全策略来进行访问控制的软件或设备，主要是用来阻止外部网络对内部网络的侵扰，是一种逻辑隔离部件，而不是物理隔离部件。

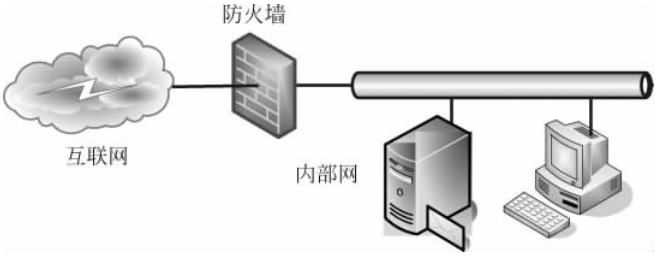

图5-6　防火墙在网络中的位置

1）防火墙的防护机制

防火墙作为计算机网络中的边境检查站，被部署在网络的边界，在内部网络与外部网络之间形成隔离，防范外部网络对内部网络的威胁，起到一种边界保护的机制。但内部网络的相互访问，因没有穿越防火墙，所以防火墙是无法进行控制的。防火墙要起到边界保护的作用，要求做到如下几点。

（1）所有进出内部网络的通信，都必须经过防火墙

防火墙作为网络边界的安全防护设备，其发挥作用的前提是能够对进出内部网络的所有通信进行检查、控制，如果在受保护的网络内，可以通过拨号上网，该通信绕过了防火墙的检查，将使防火墙失去防护作用。

（2）所有通过防火墙的通信，都必须经过安全策略的过滤

即使所有进出内部网络的通信都经过了防火墙，但如果对这些通信不按照安全策略进行检查，或者安全策略的配置漏洞百出、自相矛盾，则防火墙将形同虚设，无法起到应有的防护作用。

（3）防火墙本身是安全可靠的

虽然防火墙对所有进出内部网络的通信，按照安全策略都进行了严格的检查，但如果防火墙自身存在安全漏洞，那么黑客就可以通过防火墙的安全漏洞，控制甚至摧毁防火墙。

2）防火墙的形态

防火墙的访问控制通过一组特别的安全部件实现，其形态有以下几种。

（1）纯软件。防火墙是运行在通用计算机上的纯软件，简单易用，配置灵活，但因底层操作系统是一个通用型的系统，其数据处理能力、安全性能水平都比较低。

（2）纯硬件。为解决纯软件防火墙的不足，设计人员将防火墙软件固化在专门设计的硬件上，数据处理能力与安全性能水平都得到很大的提高。但因来自网络的威胁不断变化，防火墙的安全策略、配置等也需要经常进行调整，而纯硬件防火墙的调整非常困难。

（3）软硬件结合。结合上述两种防火墙的优点，针对防火墙的特殊要求，对硬件、操作系统进行裁减，设计、开发出防火墙专用的硬件、安全操作系统平台，然后在此平台上运行防

火墙软件。

在实际应用中，上述三种形态的防火墙，可以根据各自的特点应用于不同安全要求的情形，如纯软件防火墙可以应用于个人主机上，纯硬件防火墙可以应用于数据处理性能要求高、安全策略比较稳定的情况等。

3）防火墙的功能

防火墙是一种网络边界保护型的安全设备，为了达到安全保护内部网络的目的，一般具有如下一些功能。

（1）访问控制。这是防火墙最基本最重要的功能。防火墙通过身份识别，辨别请求访问内部网络者的身份，然后根据该用户所获得的授权，控制其访问授权范围的内容，保护网络的内部信息。防火墙还可以对所提供的网络服务进行控制，通过限制一些不安全的服务，减少威胁，提高网络安全的保护程度。

（2）内容控制。防火墙可以对穿越防火墙的数据内容进行控制，阻止不安全的数据内容进入内部网络，影响内部网络的安全。病毒、木马等经常隐藏在可执行文件或 ActiveX 控件中，通过限制内部人员从外网下载，就可减少威胁。

（3）安全日志。因所有进出内部网络的通信都必须经过防火墙，故防火墙可以完整地记录网络通信情况。通过分析、审计日志文件，可以发现潜在的威胁，并及时调整安全策略进行防范；还可以在发生网络破坏事件时，发现破坏者。

（4）集中管理。防火墙需要针对不同的网络情况与安全需求，制定不同的安全策略，并且还要根据情况的变化改进安全策略。在一个网络的安全防护体系中，会有多台防火墙分布式部署，便于进行集中管理，实施统一的安全策略，避免出现安全漏洞。

（5）其他附加功能。此外，防火墙还有其他一些附加功能，如支持 VPN、NAT 等。

① VPN(Virtual Private Network，虚拟专用网)：因防火墙所处的位置是网络的出入口，它是支持 VPN 连接的理想接点。目前许多防火墙都提供 VPN 连接功能。

② NAT(Network Address Translation，网络地址转换)：将内部网络的 IP 地址，转换为外部网络 IP 地址的技术。此技术主要是为了解决 IPv4 的 IP 地址即将耗尽的问题，通过 NAT 可大大节约对外部网络 IP 地址的使用，减缓耗尽 IP 地址的速度。NAT 相当于网络级的代理：将内部网络计算机的 IP 地址转换成防火墙的 IP 地址，代表内部网络的计算机与外部网络通信，从而使黑客无法获取内部网络计算机的 IP 地址，也就无法有针对性地实施攻击。

2. 安全策略与规则

Digital 公司 1986 年在 Internet 上安装了全球第一个商用防火墙系统后，相关技术与应用得到了快速的发展，经历包过滤技术、状态检测技术、代理服务技术等历程。防火墙都是以安全策略及其展开的过滤规则为基础，实现防火墙的访问控制目的。

访问的畅通与控制是网络边界安全策略的一对矛盾，组建网络的目的就是为了提供方便的访问功能，提供多种服务，保证网络传输的性能；而控制则是要检查、拒绝未授权的访问或服务，保护内部网络的安全。防火墙的基本控制策略有以下两类。

（1）没有被明确允许的，就是禁止的。这是一种以控制为中心的控制策略。

（2）没有被明确禁止的，就是允许的。这是一种以畅通访问为中心的控制策略。

制定一个网络安全策略，有如下一些基本步骤。

（1）确定内部网络访问控制的策略，是以控制为中心，还是以畅通访问为中心，并结合具体情况进行修订；

（2）明确网络内需要保护的资产（服务器、路由器、软件、数据等）情况，分析潜在的风险；

（3）明确安全审计内容，以便将这些内容记录在日志文件中；

（4）定义可执行、可接受的安全策略；

（5）验证策略的一致性；

（6）注意安全策略的使用范围、时间；

（7）安全事件的响应。

3. 防火墙的局限性

如上所述，防火墙虽然能在网络边界对受保护网络进行很好的保护，但并不能解决所有的安全问题。首先，防火墙只是一种边界安全保护系统，要保证边界的所有出口都有防火墙的保护，才能形成对网络边界内环境的防护。其次，防火墙只能保护边界内的环境，通信数据在穿越边界出去后，将失去防火墙的防护。而内部人员发起的攻击，因没有经过防火墙，所以防火墙也无法提供防护。最后，防火墙的配置是基于已知攻击知识制定的，因此无法对一些新的攻击进行防护，需要经常更新配置。防火墙对通信内容的控制很弱，因此其对病毒、蠕虫、木马等恶意代码的防护能力很弱。

因此，不能认为安装了防火墙，内部网络的安全问题就可以彻底解决了，需要结合其他安全技术，构建不同层次、不同深度的防御体系。

4. 防火墙的发展趋势

防火墙是信息安全领域最成熟、应用最广的产品之一，但随着相关技术的发展，防火墙技术也在不断发展，以适应新的安全需求。

1）分布式防火墙

防火墙一般部署在网络的边界，无法对网络内部计算机之间的访问进行监测、控制，为了解决这一问题，提出了分布式防火墙的概念。分布式防火墙是一种新的防火墙体系结构，在内外网络边界、内部网各子网之间、关键主机等不同结点分布式部署防火墙，通过管理中心进行统一监测、控制。

2）网络安全技术的集成与融合

传统包过滤技术仅检查 TCP/IP 数据包的报头信息，不能检查隐藏在数据包内容里的恶意行为，如垃圾邮件、不良信息、病毒、木马程序等，无法适应安全需求的发展，在此背景下产生了全面的数据包检查技术。除了检查报头信息后，还引入模式识别、人工智能等技术，对数据包内容进行辨识，判别其是否携带不良信息和恶意代码，从而阻止这些数据包通过防火墙。

另外，新的网络协议、服务的出现，也促使防火墙技术要发展相应的处理机制来适应。如 IPv6 的迅速发展，使网络边界更加复杂，基于 IPv4 的防火墙技术肯定无法满足需求。攻击技术不断变化，新的病毒、蠕虫、木马程序等恶意代码层出不穷，仅靠防火墙单一技术已经

不能满足网络安全的需求，因此防火墙技术正逐渐与入侵检测技术、防病毒技术、抗攻击技术（如抗 DDoS 攻击等）、VPN、PKI 等集成、融合，成为一个更加全面、完善的网络安全防御体系，能更加有效地保护内部网络的安全。

3）高性能的硬件平台技术

防火墙的访问与控制的矛盾还体现在安全性与效率上，一般来说，安全性越高，效率就越低。而网络传输速度越来越高、应用越来越丰富，防火墙作为网络边界的访问控制设备，成为性能的瓶颈。可以通过采用一些高性能、多处理器、并行处理硬件平台，将不同的处理任务分配给不同的处理器并行处理，可以有效地提高防火墙的处理性能。或者可以通过设计新的防火墙专用硬件平台、技术架构，解决日益严重的安全与效率矛盾。

5.2.4 入侵检测

如果攻击者成功地绕过防御措施，渗透到网络中，如何检测出攻击行为呢？以上所介绍的防御措施对于内部人员所发送的攻击是无济于事的，而有研究显示，绝大部分的安全事件是由内部人员引起的。入侵检测系统（Intrusion Detection System，IDS）通过监视受保护系统或网络的状态和活动，发现正在进行或已发生的攻击，起到信息保障体系结构中检测的作用。

1. 入侵检测的基本原理

1980 年，J. Anderson 在他的那篇被誉为入侵检测的开山之作的文章 *Computer Security Threat Monitoring and Surveillance* 中首次提出了创建安全审计记录和在此基础上的计算机威胁监控系统的基本构想。首先定义成功的攻击称为渗透，为了创建安全审计记录，他对入侵威胁进行了分类，指出来自内部的渗透者是系统安全的主要隐患，按照检测难度递增，把攻击分为假冒者（假冒他人的内部用户），误用者（合法用户误用了对系统或数据的访问），秘密用户（获取了对系统的管理控制）。至于来自外部的渗透者，当他们成功地突破了目标系统的访问控制后，相应的威胁就转变为内部的威胁。

假冒者盗用他人账户信息。他对系统的访问可以看成是对系统的“额外”使用，直觉上，他对系统的访问行为轮廓应该和他所冒充的用户有所不同，因此一个自然的检测方法是在审计记录中为系统的每个合法用户建立一个正常行为轮廓，当检测系统发现当前用户的行为和他的正常行为轮廓有较大偏差时，就应该及时提醒系统安全管理员。这样的检测方法称为异常检测。

误用者是合法用户对系统或数据的越权访问。与授权用户的行为相比，这些越权举动可能在统计上没有显著的区别，因此通过比较当前行为和正常行为轮廓以发现可能的入侵行为的做法，要比假冒者情景困难。然而，如果这些越权举动构成明显的入侵行为，则可以通过事先刻画已知攻击的特征，将越权举动和这些特征相匹配，从而检测出攻击。这种方法称为误用检测。

秘密用户拥有对系统的管理控制权。可以利用他的权限来躲避审计记录，因此很难通过安全审计记录来检测出所发生的攻击，除非他的秘密行动显示出上述两类攻击者的特征。

综上所述，异常检测和误用检测是入侵检测的两种主要分析模型，其中，用户正常行为

轮廓的建立主要是基于统计的方法，而攻击特征的刻画主要是基于规则。对于假冒者偏向于采用异常检测的方法，对于有不当行为的合法用户偏向于采用误用检测的方法，但在实践中往往采用两种方法的混合使用。

2. 入侵检测的数据源

入侵检测的数据源，是反映受保护系统运行状态的记录和动态数据。最初主要是基于主机的，但从20世纪90年代开始，网络数据逐渐成为商用入侵检测系统最为通用的数据源，相应的两类入侵检测系统分别称为基于主机和基于网络的入侵检测系统。

基于主机的数据源主要包括：①操作系统审计记录，由专门的操作系统机制产生的系统事件的记录；②系统日志，由系统程序产生的用于记录系统或应用程序事件的文件。

操作系统的审计记录是系统活动的信息集合，它按照时间顺序组成数个审计文件，每个文件由审计记录组成，每条记录描述了一次单独的系统事件，由若干个域（又称审计标记）组成。当系统中的用户采取动作或调用进程时，引起的系统调用或命令执行，此时审计系统就会产生对应的审计记录。大多数商用操作系统的审计记录是按照可信产品评估程序的标准设计和开发的，具有低层次和细节化的特征，因此成为基于主机的入侵检测系统首选数据源。

系统日志是反映系统事件和设置的文件。例如，UNIX提供通用的服务syslog（用于支持产生和更新事件日志）；Sun Solaris中的lastlog（记录用户最近的登录，成功或不成功）、pacct（记录用户执行的命令和资源使用的情况）。和操作系统的审计记录相比，系统日志存在如下的安全隐患：产生系统日志的软件通常作为应用程序而不是操作系统的子程序运行，易于遭到恶意的破坏和修改；系统日志通常存储在系统未经保护的目录中，而且以文本的形式存储，而审计记录则经过加密和校验处理，为防止篡改提供了保护机制。

但另一方面，系统日志和审计记录相比，具有较强的可读性；而在某些特殊的环境下，可能无法获得操作系统的审计记录或不能对审计记录进行正确的解释，此时系统日志就成为系统安全管理必不可少的信息来源。

网络数据是当前商用入侵检测系统最为通用的数据来源。当网络数据流在检测系统所保护的网段中传播时，采用特殊的数据提取技术，收集网段中传播的数据，作为检测系统的数据来源。和基于主机的数据源相比，它具有如下突出的优势：网络数据是通过网络监听的方式获得的，由于网络嗅探器所做的工作仅仅是从网络中读取传输的数据包，因此对被保护系统的性能影响很小，而且无须改变原有的系统和网络结构；网络监视器与受保护主机的操作系统无关。相比之下，基于主机的入侵检测系统必须针对不同的操作系统开发相应的版本。

3. 入侵检测系统的一般框架

入侵检测系统的一般框架如图5-7所示，其中各部分功能介绍如下。

（1）审计数据收集：数据源主要是前面所讨论的基于主机和基于网络两个来源。

（2）数据处理（检测）：主要的检测模型是前文所介绍的误用检测和异常检测，它们所采用的主要分析方法分别是基于规则和基于统计。在应用这些方法之前，常常对审计数据进行预处理。

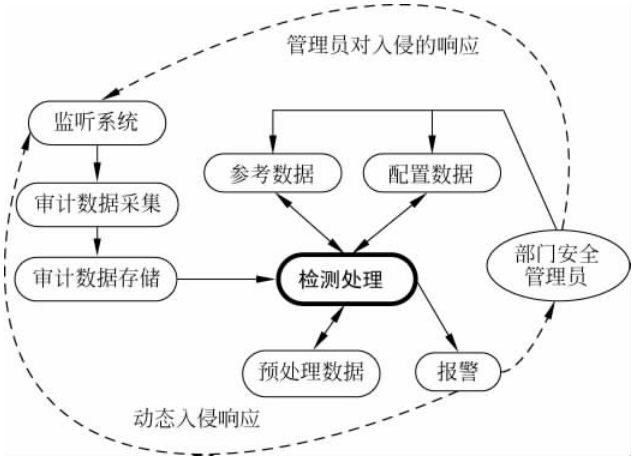

图 5-7 入侵检测系统的一般框架

(3) 参考数据：主要包括已知攻击的特征和用户正常行为的轮廓，而检测引擎会不断地更新这些数据。

(4) 报警：该模块处理由整个系统产生的所有输出，结果可以是对怀疑行动的自动响应，但最为普遍的是通知系统安全管理员。

(5) 配置数据：主要指影响检测系统操作的状态，例如审计数据的来源和收集方法，如何响应入侵等。系统安全管理员是通过配置数据来控制入侵检测系统的运行。

(6) 审计数据存储与预处理：是为后期数据处理提供方便的数据检索和状态保存而设置的，可以看成数据处理的一部分。

4. 入侵检测系统的体系结构

入侵检测系统的体系结构可以分为主机型、网络型和分布式三种，其中，主机型和网络型都属于集中式系统。

1) 主机型入侵检测系统

主机型入侵检测系统位于受保护的计算机中，监控该机的运行：主要的监控源包括操作系统审计记录和系统日志。在许多情况下，入侵检测系统只提供一些泛泛的报警。系统管理员可以配置入侵检测系统使得它将下列类型的变化作为可报道的安全事件：与安全相关的应用有变化，如 UNIX 操作系统中文件系统完整性检查软件工具 Tripwire；存放关键数据的文件夹发生变化等。一旦配置得当，主机型入侵检测系统能够比较可靠地工作。

2) 网络型入侵检测系统

网络型入侵检测系统的任务是在网络数据中发现攻击的特征或异常行为。局域网普遍采用的是基于广播机制的以太网协议，该协议保证传输的数据包能被统一冲突域内的所有主机接收，基于网络的入侵检测正是利用了以太网的这一特性。以太网卡通常有正常模式和杂收模式两种。在正常模式下主机仅处理以本机为目标的数据包，而在杂收模式下网卡可以接收所处网段内传输的所有数据包，不管这些数据包的目的地址是否为本机。基于网络的入侵检测系统必须利用以太网卡的杂收模式，通过抓包工具，获得经过所处网段的所有数据信息，从而实现获得网络数据的功能。

网络型入侵检测系统监控整个网段的网络数据流，因此与主机型入侵检测系统相比，需要复杂的配置和维护，同时，网络型入侵检测系统也比主机型入侵检测系统更容易产生误报，但网络型入侵检测系统擅长对付基于网络协议的攻击手段。

3）分布式入侵检测系统

主机型和网络型入侵检测系统在检测攻击方面各有千秋：网络型入侵检测系统擅长对付基于网络协议的攻击手段，如 SYN Flood，Ping of Death 等，而如果要精确地检测出一些常见的攻击，如缓冲区溢出，则离不开主机上的审计记录，因此对一个网段的保护需要两种入侵检测系统的合作。同时，对于大型或复杂的网络，或协作的攻击，如分布式拒绝服务攻击，需要多个检测器之间的协作，这些因素导致了分布式入侵检测系统的诞生和发展。

5. 入侵检测的发展趋势

入侵检测的第一个发展趋势是高性能网络入侵检测技术。随着网络宽带的快速增长及多媒体应用的日益普及，网络入侵检测系统面临着巨大的“千兆线速”性能压力。虽然网络入侵检测系统通常以并联方式接入网络，但是如果其处理速度跟不上网络数据的传输速度，则由于大量丢包而导致的攻击漏报将严重影响系统的准确性和有效性。

目前对网络入侵检测系统性能方面的考虑主要有如下几个方面：避开某些性能瓶颈，如开发“零备份”网卡抓包驱动程序以尽量减少内存备份次数，避免内存备份性能瓶颈；依赖有状态的协议分析尽量缩小特征字符串匹配的范围；通过优化算法提高处理性能，如使用并行模式匹配算法提高特征检测的性能；通过引入计算集群和负载均衡算法，使用更多的计算资源来提升整体性能适应千兆高速网络。

入侵检测的第二个发展趋势是入侵检测系统报警信息后处理开始成为一个研究热点。入侵检测系统发出的一个报警是建立在观察到由入侵者的一个攻击步骤所导致的现象的基础上，因此被称为“第一级”安全报警。目前，这些报警存在的主要问题是弱语义以及高漏报率和高误报率。考虑到实际的需要应该是一个关于系统安全状况的全局图景，但这些问题的解决显然不能单靠改进检测引擎实现，因此随着当前网络系统的复杂化和大型化、检测器的数量增加和多样化，以及随之产生的庞大的安全信息、利用网络发起协调攻击的日益盛行、入侵检测系统的体系结构由集中向分布式发展等，显得更加重要。

通常入侵检测系统的报警只能代表可能的（几个）攻击事件，换句话说，报警和其背后的攻击动作之间并不是一一对应的，因此报警信息后处理的主要任务之一是通过综合分析多个报警，从而对它们所对应的可能攻击事件做出（相对于单个孤立的报警而言）更为精确的判断。目前主要采取的分析方法有较为简单的报警聚类和需要机器学习或知识库支持的关联分析。

入侵检测的第三个发展趋势是入侵检测系统与其他安全工具联动，例如，入侵检测系统在检测到攻击时可以通过联动协议修改防火墙的规则以阻断连接。

5.3 典型攻击与防御技术简介

目前常用的网络攻击手段有社会工程学攻击、物理攻击、暴力攻击、利用 Unicode 漏洞攻击和利用缓冲区溢出漏洞攻击、拒绝服务攻击等技术。

5.3.1 社会工程学攻击

社会工程是使用计谋和假情报去获得密码和其他敏感信息的科学，研究一个站点的策略其中之一就是尽可能多地了解这个组织的个体，因此黑客不断试图寻找更加精妙的方法从他们希望渗透的组织那里获得信息。

例如，一组高中学生曾经想要进入一个当地的公司的计算机网络，他们拟定了一个表格，调查看上去显得是无害的个人信息，例如所有秘书和行政人员和他们的配偶、孩子的名字，这些从学生转变成的黑客说这种简单的调查是他们社会研究工作的一部分。利用这份表格这些学生能够快速地进入系统，因为网络上的大多数人是使用宠物和他们配偶的名字作为密码。

目前社会工程学攻击主要包括两种方式：打电话请求密码和伪造 E-mail。

1）打电话请求密码

尽管不像前面讨论的策略那样聪明，打电话寻问密码也经常奏效。在社会工程中那些黑客冒充失去密码的合法雇员，经常通过这种简单的方法重新获得密码。

2）伪造 E-mail

使用 Telnet，一个黑客可以截取任何一个身份证发送 E-mail 的全部信息，这样的 E-mail 消息是真的，因为它发自于一个合法的用户。在这种情形下这些信息显得是绝对真实的。黑客可以伪造这些。一个冒充系统管理员或经理的黑客就能较为轻松地获得大量的信息，黑客就能实施他们的恶意阴谋。

5.3.2 物理攻击与防范

物理安全是保护一些比较重要的设备不被接触。物理安全比较难防，因为攻击往往来自能够接触到物理设备的用户。

1）获取管理员密码

系统管理员登录系统以后，离开计算机时没有锁定计算机，或者直接以自己的账号登录，然后让别人使用，这是非常危险的，因为这样可以轻易获取管理员密码。例如，使用 FindPass 等工具可以对该系统进程 winlogon. exe 进行解码，然后将当前用户的密码显示出来。所以，只要可以侵入某个系统，获取管理员或者超级用户的密码是可能的。

2）权限提升

有时候，管理员为了安全，给其他用户建立一个普通用户账号，认为这样就安全了。其实不然，用普通用户账号登录后，可以利用工具 GetAdmin. exe 将自己加到管理员组或者新建一个具有管理员权限的用户。

例如，普通用户建立管理员账号。建立一个账号 Hacker，该用户为普通用户。用 Hacker 账户登录系统，在系统中执行程序 GetAdmin. exe，程序自动读取所有用户列表，新建一个管理员组的用户名“IAMHacker”。注销当前用户，使用 IAMHacker 登录，密码为空，登录以后可看到所在用户组就是 Administrators 组。这样一个普通用户就成功新建了

一个管理员账号。所以只要物理上接触了某计算机系统，就可以马上获得该系统超级用户的权限。

5.3.3 暴力攻击

针对一个安全系统进行暴力攻击需要大量的时间，需要极大的意志力和决心。然而，由于不适宜的安全设置和策略，一些系统非常易于暴露在这种攻击之下。不过暴力攻击经常容易被侦测到，因为攻击时经常需要重复连接。

字典攻击是最常见的一种暴力攻击。如果黑客试图通过使用传统的暴力攻击方法去获得密码的话，将不得不尝试每种可能的字符，包括大小写、数字和通配符等。字典攻击通过仅使用某种具体的密码来缩小尝试的范围，大多数的用户使用标准单词作为一个密码，一个字典攻击试图通过利用包含单词列表的文件去破解密码。强壮的密码则通过结合大小写字母、数字和通配符来击败字典攻击。一次字典攻击能否成功，很大因素取决于字典文件。一个好的字典文件可以高效快速地得到密码。攻击不同的公司、不通地域的计算机，可以根据公司管理员的姓氏以及家人的生日，作为字典文件的一部分，公司以及部门的简称一般也可以作为字典文件的一部分，这样可以大大提高破解效率。一个字典文件本身就是一个标准的文本文件，其中的每一行就代表一个可能的密码。目前有很多工具软件专门来创建字典文件，也有各种不同的专门软件，暴力破解操作系统密码、邮箱密码或者 Office、WinZip、WinRAR 等文档密码。

5.3.4 缓冲区溢出攻击

目前最流行的一种攻击技术就是缓冲区溢出攻击。当目标操作系统收到了超过它的最大能接收的信息量的时候，将发生缓冲区溢出。这些多余的数据将使程序的缓冲区溢出，然后覆盖实际的程序数据，缓冲区溢出使目标系统的程序被修改，经过这种修改的结果是在系统上产生一个后门。这项攻击对技术要求比较高，但是攻击的过程却非常简单。缓冲区溢出原理很简单，比如程序：

```
void function(char * szPara1)
{
    char buff[16];
    strcpy(buffer,szPara1);
}
```

程序中利用 strcpy 函数将 szPara1 中的内容复制到 buff 中，只要 szPara1 的长度大于16，就会造成缓冲区溢出。存在 strcpy 函数这样问题的 C 语言函数还有：strcat()、gets()、scanf()等。当然，随便往缓冲区填写数据使它溢出一般只会出现“分段错误”，而不能达到攻击的目的。最常见的手段是通过制造缓冲区溢出使程序运行一个用户 shell，再通过 shell 执行其他命令，如果该 shell 有管理员权限，就可以对系统进行任意操作。

比较著名的缓冲区溢出漏洞有 RPC(Remote Procedure Call，远程过程调用)漏洞溢出和 IIS 漏洞溢出。

5.3.5 恶意代码

不必要的代码(Unwanted Code)是指没有作用却会带来危险的代码,一个最安全的定义是把所有不必要的代码都看作是恶意的,不必要代码比恶意代码具有更宽泛的含义,包括所有可能与某个组织安全策略相冲突的软件。恶意代码(Malicious Code)或者叫恶意软件Malware(Malicious Software)具有如下共同特征:①恶意是目的;②本身是程序;③通过执行发生作用。

有些恶作剧程序或者游戏程序不能看作是恶意代码。对滤过性病毒的特征进行讨论的文献很多,尽管它们数量很多,但是机理比较近似,在防病毒程序的防护范围之内,更值得注意的是非滤过性病毒。

1. 恶意代码分类

恶意代码可以按照两种标准分类,从两个角度进行分类。一种分类标准是,恶意代码是否需要宿主,即特定的应用程序、工具程序或系统程序。需要宿主的恶意代码具有依附性,不能脱离宿主而独立运行;不需要宿主的恶意代码具有独立性,可不依赖宿主而独立运行。另一种分类标准是,恶意代码是否能够自我复制。不能自我复制的恶意代码是不感染的,能够自我复制的恶意代码是可感染的。由此,可以得出以下4大类恶意代码。

1) 不感染的依附性恶意代码

(1) 特洛伊木马。在计算机领域,特洛伊木马是一段吸引人而不为人警惕的程序,但它们可以执行某些秘密的任务。大多数安全专家统一认可的定义是:特洛伊木马是一段能实现有用或必需的功能的程序,但是同时还完成一些不为人知的功能,而这些额外的功能往往是有害的。

特洛伊木马一般没有自我复制的机制,所以不会自动复制本身。电子新闻组和电子邮件是特洛伊木马的主要传播途径。特洛伊木马的欺骗性是其得以传播的根本原因。特洛伊木马经常伪装成游戏软件、搞笑程序、屏保、非法软件等,上传到电子新闻组或通过电子邮件直接传播,很容易被不知情的用户接收和继续传播。

(2) 逻辑炸弹。是一段具有破坏性的代码,事先预置于较大的程序中,等待某扳机时间发生触发其破坏行为。扳机事件可以是特殊日期,也可以是指定事件。逻辑炸弹往往被怀有报复心理的人使用,通过启动逻辑炸弹来损伤对方利益。一旦逻辑炸弹被触发,就会造成数据或文件的改变或删除、计算机死机等事件。

(3) 后门或陷门。它是进入系统或程序的一个秘密入口,它能够通过识别某种特定的输入序列或特定账户,使访问者绕过安全检查,直接获得访问权利,并且通常高于普通用户的特权。程序员为了调试和测试程序一直合法地使用后门,但当程序员或他所在的公司另有企图时,后门就变成一种威胁。

2) 不感染的独立型恶意代码

(1) 点滴器

点滴器是为传送和安装其他恶意代码而设计的程序,它本身不具有直接的感染性和破坏性。点滴器专门对抗反病毒检测,使用了加密手段,以阻止反病毒程序发现它们。当特定

事件出现时，它便启动，将自身包含的恶意代码释放出来。

（2）繁殖器

繁殖器是为制造恶意代码而设计的程序，通过这个程序，只要简单地从菜单中选择想要的功能，就可以制造恶意代码，不需要任何程序设计能力。事实上，它只是把某些已经设计好的恶意代码模块按照使用者的选择组合起来而已，没有任何创造新代码的能力。因此，检测由繁殖器产生的任何病毒都比较容易，只要通过搜索一个字符串，每种组合都可以发现。

（3）恶作剧

恶作剧是为欺骗使用者而设计的程序，它侮辱使用者或让其做出不明智的举动。恶作剧通过“心理破坏”达到“现实破坏”。一般只是娱乐而已。严重的问题是有些恶作剧会让受骗者相信他的数据正在丢失或系统已经损坏需要重新安装，导致用户去进行系统重装等不明智举动而产生损失。

3）可感染的依附性恶意代码

计算机病毒是一段附着在其他程序上的可以进行自我繁殖的代码。由此可见，计算机病毒既具有依附性，又具有感染性。

4）可感染的独立性恶意代码

（1）计算机蠕虫

计算机蠕虫是一种通过计算机网络能够自我复制和扩散的程序。蠕虫与病毒的区别在于“附着”。蠕虫不需要宿主，不会与其他特定程序混合。

（2）计算机细菌

计算机细菌是一种在计算机系统中不断复制自己的程序，一个典型的细菌是在多任务系统中生成它的两个副本，然后同时执行这两个副本，这一过程递归循环，最终会占用全部的处理器时间和内存或磁盘空间，从而导致计算机资源耗尽，无法为用户服务。

2. 计算机病毒

20世纪60年代初，美国贝尔实验室的三位程序员编写了一个名为“磁芯大战”的游戏，游戏中通过复制自身来摆脱对方的控制，这就是所谓“病毒”的第一个雏形。20世纪70年代，美国作家雷恩在其出版的《P1的青春》一书中构思了一种能够自我复制的计算机程序，并第一次称之为“计算机病毒”。1983年11月，在国际计算机安全学术研讨会上，美国计算机专家首次将病毒程序在VAX/750计算机上进行了实验，世界上第一个计算机病毒就这样出生在实验室中。20世纪80年代后期，巴基斯坦有两个以编程为生的兄弟，他们为了打击那些盗版软件的使用者，设计出了一个名为“巴基斯坦智囊”的病毒，这就是世界上流行的第一个真正的病毒。1994年2月18日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》。在该条例的第二十八条中明确指出：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”这个定义具有法律性、权威性。根据这个定义，计算机病毒是一种计算机程序，它不仅能破坏计算机系统，而且能够传染到其他系统。计算机病毒通常隐藏在其他正常程序中，能生成自身的备份并将其插入其他的程序中，对计算机系统进行恶意的破坏。

计算机病毒不是天然存在的，是某些人利用计算机软、硬件所固有的脆弱性，编制的具

有破坏功能的程序。计算机病毒能通过某种途径潜伏在计算机存储介质(或程序)里,当达到某种条件时即被激活,它用修改其他程序的方法将自己的精确备份或者可能演化的形式放入其他程序中,从而感染它们,对计算机资源进行破坏。

计算机病毒具有以下几个特点。

1) 寄生性

计算机病毒寄生在其他程序之中,当执行这个程序时,病毒就起破坏作用,而在未启动这个程序之前,它是不易被人发觉的。

2) 传染性

传染性是病毒的基本特征。计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机,在某些情况下造成被感染的计算机工作失常甚至瘫痪。计算机病毒代码一旦进入计算机并得以执行,它就会搜寻其他符合其传染条件的程序或存储介质,确定目标后再将自身代码插入其中,达到自我繁殖的目的。只要一台计算机染毒,如不及时处理,那么病毒会在这台计算机上迅速扩散,其中的大量文件(一般是可执行文件)会被感染。而被感染的文件又成了新的传染源,再与其他机器进行数据交换或通过网络接触,病毒会继续传染。

3) 潜伏性

有些病毒像定时炸弹一样,让它什么时间发作是预先设计好的。比如黑色星期五病毒,不到预定时间一点儿都觉察不出来,等到条件具备的时候一下子就爆炸开来,对系统进行破坏。潜伏性的第一种表现是指,病毒程序不用专用检测程序是检查不出来的,因此病毒可以静静地躲在磁盘或磁带里待上几天,甚至几年,一旦时机成熟,得到运行机会,就又要四处繁殖、扩散,继续为害。潜伏性的第二种表现是指,计算机病毒的内部往往有一种触发机制,不满足触发条件时,计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足,有的在屏幕上显示信息、图形或特殊标识,有的则执行破坏系统的操作,如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

4) 隐蔽性

计算机病毒具有很强的隐蔽性,有的可以通过病毒软件检查出来,有的根本就查不出来,有的时隐时现、变化无常,这类病毒处理起来通常很困难。

5) 破坏性

计算机中毒后,可能会导致正常的程序无法运行,把计算机内的文件删除或受到不同程度的损坏。通常表现为:增、删、改、移。

6) 可触发性

病毒因某个事件或数值的出现,诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己,病毒必须潜伏,少做动作。如果完全不动,一直潜伏的话,病毒既不能感染也不能进行破坏,便失去了杀伤力。病毒既要隐蔽又要维持杀伤力,它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件,这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时,触发机制检查预定条件是否满足,如果满足,启动感染或破坏动作,使病毒进行感染或攻击;如果不满足,使病毒继续潜伏。

目前病毒主要通过以下在三种途径进行传播。

（1）通过不可移动的计算机硬件设备进行传播，这类病毒虽然极少，但破坏力却极强，目前尚没有较好的检测手段对付。

（2）通过移动存储介质传播，包括光盘、U盘和移动硬盘等，用户之间在互相复制文件的同时也造成了病毒的扩散。

（3）通过计算机网络进行传播。计算机病毒附着在正常文件中通过网络进入一个又一个系统，其传播速度呈几何级数增长，是目前病毒传播的首要途径。

3. 计算机病毒的工作机制

从本质上来看，病毒程序可以执行其他程序所能执行的一切功能。但是，与普通程序又不同的是病毒必须将自身附着在其他程序上。病毒程序所依附的其他程序称为宿主程序。当用户运行宿主程序时，病毒程序被激活，并开始执行。一旦病毒程序被执行，它就能执行一切意想不到的功能（如感染其他程序、删除文件等）。从病毒程序的生命周期来看，它一般会经历4个阶段：潜伏阶段、传染阶段、触发阶段和发作阶段。在潜伏阶段，病毒程序处于休眠状态，用户根本感觉不到病毒的存在，但并非所有病毒均会经历潜伏阶段。如果某些事件发生（如特定的日期、某个特定的程序被执行等），病毒就会被激活，并从而进入传染阶段。处于传染阶段的病毒，将感染其他程序——将自身程序复制到其他程序或者磁盘的某个区域上。经过传染阶段，病毒程序已经具备运行的条件，一旦病毒被激活，则进入触发阶段。

如图5-8所示，典型的计算机病毒程序由病毒引导模块、病毒传染模块和病毒表现模块三部分组成，其中，病毒感染模块包括激活传染条件判断模块和传染功能实现模块，病毒表现模块包括触发表现条件判断模块和表现功能实现模块。

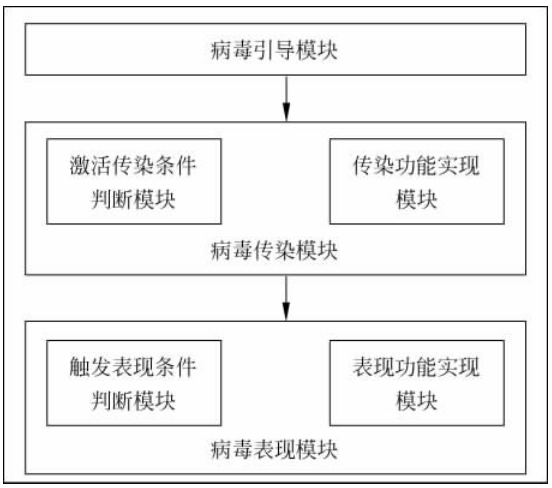

图5-8　病毒程序的典型组成示意图

1）计算机病毒的引导模块

计算机病毒引导模块主要实现将计算机病毒程序引入计算机内存，并使得传染和表现模块处于活动状态。引导模块需要提供自保护功能，从而避免在内存中的自身代码不被覆盖或清除。一旦引导模块将计算机病毒程序引入内存后，它还将为传染模块和表现模块设置相应的启动条件，以便在适当的时候或者合适的条件下激活传染模块或者触发表现模块。

2）计算机病毒的传染模块

计算机病毒的传染模块有两个功能：其一是依据引导模块设置的条件，判断当前系统环境是否满足传染条件；其二是如果传染条件满足，则启动传染功能，将计算机病毒程序附加到其他宿主程序上。相应地，传染模块也分为传染条件判断子模块和传染功能实现子模块两个部分。

3）计算机病毒的表现模块

计算机病毒的表现模块功能也包括两个部分：其一是根据引导模块设置的触发条件，判断当前系统环境是否满足所需要的触发条件；其二是一旦触发条件满足，则启动计算机病毒程序，按照预定的计划执行（如删除程序、盗取数据等）。

对于计算机病毒的被动传染而言，其传染过程是随着复制磁盘或文件工作的进行而进行的。而对于计算机病毒的主动传染而言，其传染过程是：在系统运行时，计算机病毒通过计算机病毒载体即系统的外存储器进入系统的内存储器，常驻内存，并在系统内存中监视系统的运行。

4. 典型计算机病毒的检测技术

在与病毒的对抗中，及早发现病毒很重要。早发现，早处置，可以减少损失。检测病毒的方法有：特征代码法、校验和法、行为监测法、软件模拟法，这些方法依据的原理不同，实现时所需开销不同，检测范围不同，各有所长。

（1）比较法是用原始备份与被检测的引导扇区或被检测的文件进行比较。

① 长度比较法及内容比较法

病毒感染系统或文件，必然引起系统或文件的变化，既包括长度的变化，又包括内容的变化。因此，将无毒的系统或文件与被检测的系统或文件的长度和内容进行比较，即可发现病毒。长度比较法和内容比较法就是从长度和内容两方面进行比较而得名。以长度或内容是否变化作为检测病毒的依据，在许多场合是有效的。但是，长度比较法和内容比较法有其局限性，只检查可疑系统或文件的长度和内容是不充分的。因为长度和内容的变化可能是合法的，有些普通的命令可以引起长度和内容变化；另外，某些病毒感染文件时，宿主文件长度可保持不变。

上述情况下，长度比较法和内容比较法不能区别程序的正常变化和病毒攻击引起的变化，不能识别保持宿主程序长度不变的病毒，无法判定为何种病毒。实践表明，将长度比较法、内容比较法作为检测病毒的手段之一，与其他方法配合使用，效果更好。

② 内存比较法

这是一种对内存驻留病毒进行检测的方法。由于病毒驻留于内存，必须在内存中申请一定的空间，并对该空间进行占用、保护。因此，通过对内存的检测，观察其空间变化，与正常系统内存的占用和空间进行比较，可以判定是否有病毒驻留其间。但无法判定为何种病毒。此法对于那些隐蔽型病毒无效。

③ 中断比较法

病毒为实现其隐蔽和传染破坏的目的，常采用“截留盗用”技术，更改、接管中断向量，让系统中断向量转向执行病毒控制部分。因此，将正常系统的中断向量与有毒系统的中断向量进行比较，可以发现是否有病毒修改和盗用中断向量。

（2）将正常文件的内容，计算其校验和，将该校验和写入文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前，检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法，它既可发现已知病毒又可发现未知病毒。但是，它不能识别病毒类，不能报出病毒名称。由于病毒感染并非文件内容改变的唯一的非他性原因，文件内容的改变有可能是正常程序引起的，所以校验和法常常误报警，而且此种方法也会影响文件的运行速度。

校验和法的优点是：方法简单，能发现未知病毒、被查文件的细微变化也能发现。其缺点是：病毒感染的确会引起文件内容变化，但是校验和法对文件内容的变化太敏感，又不能区分正常程序引起的变动，而频繁报警。用监视文件的校验和来检测病毒，不是最好的方法。这种方法当遇到软件版本更新、变更口令以及修改运行参数时都会误报警。校验和法对隐蔽性病毒无效。隐蔽性病毒进驻内存后，会自动剥去染毒程序中的病毒代码，使校验和法受骗，对一个有毒文件算出正常校验和。

（3）扫描法是用每一种病毒体含有的特定字符串对被检测的对象进行扫描。如果在被检测对象内部发现了某一种特定字符串，就表明发现了该字符串所代表的病毒。扫描法包括特征代码扫描法、特征字扫描法。

① 特征代码扫描法

病毒扫描软件由两部分组成：一部分是病毒代码库，含有经过特别选定的各种计算机病毒的代码串；另一部分是利用该代码库进行扫描的扫描程序。病毒扫描程序能识别的计算机病毒的数目完全取决于病毒代码库内所含病毒的种类有多少。显而易见，库中病毒代码种类越多，扫描程序能认出的病毒就越多。病毒代码串的选择是非常重要的。

② 特征字扫描法

计算机病毒特征字扫描法是基于特征串扫描法发展起来的一种新方法。它工作起来速度更快、误报警更少。特征字扫描只需从病毒体内抽取很少几个关键的特征字，组成特征字库。由于需要处理的字节很少，而又不必进行串匹配，大大加快了识别速度，当被处理的程序很大时表现更突出。类似于检测生物病毒的生物活性，特征字识别法更注意计算机病毒的“程序活性”，减少了错报的可能性。

（4）利用病毒的特有行为特征性来监测病毒的方法，称为行为监测法。通过对病毒多年的观察、研究，有一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现了病毒行为，立即报警。

（5）感染实验是一种简单实用的检测病毒方法。这种方法的原理是利用了病毒的最重要的基本特征：感染特性。所有的病毒都会进行感染，如果不会感染，就不称其为病毒。如果系统中有异常行为，最新版的检测工具也查不出病毒时，就可以做感染实验，运行可疑系统中的程序后，再运行一些确切知道不带毒的正常程序，然后观察这些正常程序的长度和校验和，如果发现有的程序增长，或者校验和变化，就可断言系统中有病毒。

（6）多态性病毒每次感染都修改其病毒密码，对付这种病毒，特征代码法失效。因为多态性病毒代码实施密码化，而且每次所用密钥不同，把染毒文件中的病毒代码相互比较，也无法找出相同的可能作为特征的稳定代码。为了检测多态性病毒，现已研制了新的检测法——软件模拟法。它是一种软件分析器，用软件方法来模拟和分析程序的运行。

（7）一般使用分析法的人不是普通用户，而是反病毒技术人员。使用分析法的目的在

于：①确认被观察的磁盘引导区和程序中是否含有病毒；②确认病毒的类型和种类，判定其是否是一种新病毒；③搞清楚病毒体的大致结构，提取特征识别用的字符串或特征字，用于增添到病毒代码库供病毒扫描和识别程序用；④详细分析病毒代码，为制定相应的反病毒措施制定方案。上述4个目的按顺序排列起来，正好大致是使用分析法的工作顺序。使用分析法要求具有比较全面的有关PC、DOS结构和功能调用以及关于病毒方面的各种知识。

5. 计算机病毒的预防

(1) 建立良好的安全习惯。对一些来历不明的邮件及附件不要打开，不要上一些不太了解的网站、不要执行从Internet下载后未经杀毒处理的软件等，这些必要的习惯会使计算机更安全。

(2) 关闭或删除系统中不需要的服务。默认情况下，许多操作系统会安装一些辅助服务，如FTP客户端、Telnet和Web服务器。这些服务为攻击者提供了方便，而又对用户没有太大用处，如果删除它们，就能大大减少被攻击的可能性。

(3) 经常升级安全补丁。据统计，有80%的网络病毒是通过系统安全漏洞进行传播的，像蠕虫王、冲击波、震荡波等，所以应该定期到微软网站去下载最新的安全补丁，以防患未然。

(4) 使用复杂的密码。有许多网络病毒就是通过猜测简单密码的方式攻击系统的，因此使用复杂的密码，将会大大提高计算机的安全系数。

(5) 迅速隔离受感染的计算机。当计算机发现病毒或异常时应立刻断网，以防止计算机受到更多的感染，或者成为传播源，再次感染其他计算机。

(6) 了解一些病毒知识。这样就可以及时发现新病毒并采取相应措施，在关键时刻使自己的计算机免受病毒破坏。如果能了解一些注册表知识，就可以定期看一看注册表的自启动项是否有可疑键值；如果了解一些内存知识，就可以经常看看内存中是否有可疑程序。

(7) 最好安装专业的杀毒软件进行全面监控。在病毒日益增多的今天，使用杀毒软件进行防毒，是越来越经济的选择，不过用户在安装了反病毒软件之后，应该经常进行升级，将一些主要监控经常打开(如邮件监控)，内存监控等，遇到问题要上报，这样才能真正保障计算机的安全。

(8) 用户还应该安装个人防火墙软件进行防黑。由于网络的发展，用户计算机面临的黑客攻击问题也越来越严重，许多网络病毒都采用了黑客的方法来攻击用户计算机，因此，用户还应该安装个人防火墙软件，将安全级别设为中、高，这样才能有效地防止网络上的黑客攻击。

6. 计算机病毒的新特点

从某种意义上说，21世纪是计算机病毒与反病毒激烈角逐的时代，而智能化、人性化、隐蔽化、多样化也在逐渐成为新世纪计算机病毒的发展趋势。也出现了新的专用病毒生成工具以及攻击反病毒软件的病毒。随着Internet的发展和普及，在网络环境下的病毒出现了新的发展趋势。

(1) 盗取用户各类账号，获取经济利益成为推动病毒发展的最大动力。

现在的病毒编写者不再是单纯炫耀个人技术，而是通过盗取用户的各类账号获取经济利益为目的。灰鸽子入侵用户计算机后，即可窃取QQ、网络游戏、网上银行的账号密码等信息，给用户带来直接经济损失。2007年的网游大盗是专门盗取网游账号和密码的病毒，玩家计算机一旦中了此类病毒，就可能导致网游账号和数以千元甚至万元的虚拟装备莫明其妙地转到他人手中，总的损失估计达千万美元。另外，在世界各国都有成功截获针对银行网上账号和密码的病毒的事例，此类病毒会专门盗取银行的网上账号和密码，给用户造成巨大的经济损失。

（2）不断出现以窃取个人隐私、商业机密等重要信息为目的的病毒。

灰鸽子病毒感染那些存放商业机密的计算机后，攻击者就会窃取有价值的商业机密文件等，偷偷将这些文件进行贩卖，充当商业间谍。另外，黑客利用灰鸽子病毒还可以完全控制被感染者计算机，一旦发现对用户比较隐私的文件，立刻将其转移到其他地方，还可以通过远程控制用户计算机上的摄像头偷窥用户隐私，然后对用户进行勒索。又如白雪公主病毒，一旦计算机被其感染，内部的所有数据、信息以及核心机密都将在病毒制造者面前暴露无遗而任其为所欲为。

（3）新一代网络病毒破坏性更大。

新一代病毒可以修改文件、通信端口、用户密码，挤占内存，还可以利用恶意程序实现远程控制等。例如，CIH病毒破坏主板上的BIOS和硬盘数据；爱虫病毒会自动向通讯簿中的所有电子邮件地址发送病毒邮件副本，阻塞邮件服务器，估计全球损失超过100亿美元。2004年爆发的震荡波在短短的时间内就给全球造成了数千万美元的损失。2006年年底爆发的熊猫烧香在几天就造成了巨大的社会危害和经济损失。有的病毒甚至可造成计算机系统和网络被人控制，带来不可估量的损失。

（4）震网病毒——Stuxnet病毒。

Stuxnet病毒于2010年6月首次被检测出来，是第一个专门攻击真实世界中基础设施的“蠕虫”病毒，比如发电站和水厂。它利用了微软操作系统中至少4个漏洞，其中有三个全新的零日漏洞；伪造驱动程序的数字签名；通过一套完整的入侵和传播流程，突破工业专用局域网的物理限制；利用WinCC系统的两个漏洞，对其开展破坏性攻击。它是第一个直接破坏现实世界中工业基础设施的恶意代码。据赛门铁克公司的统计，目前全球已有约四万五千个网络被该蠕虫感染，其中，60%的受害主机位于伊朗境内。伊朗政府已经确认该国的布什尔核电站遭到Stuxnet蠕虫的攻击。

5.3.6 拒绝服务攻击

1. 拒绝服务攻击的概念

凡是造成目标计算机拒绝提供服务的攻击都称为DoS(Denial of Service，拒绝服务攻击)攻击，其目的是使目标计算机或网络无法提供正常的服务。最常见的DoS攻击是：计算机网络带宽攻击和连通性攻击。带宽攻击是以极大的通信量冲击网络，使网络所有可用的带宽都被消耗掉，最后导致合法用户的请求无法通过。连通性攻击指用大量的连接请求冲击计算机，最终导致计算机无法再处理合法用户的请求。

比较著名的拒绝服务攻击包括：SYN 风暴、Smurf 攻击和利用处理程序错误进行攻击等。SYN flooding 和 Smurf 攻击利用 TCP/IP 中的设计弱点，通过强行引入大量的网络包来占用带宽，迫使目标受害主机拒绝对正常的服务请求进行响应。利用 TCP/IP 实现中的处理程序错误进行攻击，即故意错误地设定数据包头的一些重要字段，将这些错误的 IP 数据包发送出去。

在接收数据端，服务程序通常都存在一些问题，因而在将接收到的数据包组装成一个完整的数据包的过程中，就会使系统宕机、挂起或崩溃，从而无法继续提供服务。这些攻击包括广为人知的 Ping of Death，十分流行的 Teardrop 攻击和 Land 攻击、Bonk 攻击、Boink 攻击及 OOB 攻击等。

(1) Ping of Death 攻击。攻击者故意创造一个长度大于 65 535B(IP 协议中规定最大的 IP 包长为 65 535B)的 ping 包，并将该包发送到目标受害主机，由于目标主机的服务程序无法处理过大的包，而引起系统崩溃、挂起或重启。

从早先版本的 Windows 上就可以运行 Ping of Death。在命令行下只需输入："ping -l 65550 攻击目标"即可。Windows 还有一个漏洞就是它不但在收到这种无效数据时会崩溃，而且可以在偶然的情况下生成这种数据。这种攻击已经不适用了，目前所有的操作系统都对此进行了修补或升级。

(2) Teardrop 攻击。一个 IP 分组在网络中传播的时候，由于沿途各个链路的最大传输单元不同，路由器常常会对 IP 包进行分组，即将一个包分成一些片断，使每段都足够小，以便通过这个狭窄的链路。每个片段将具有自己完整的 IP 包头，其大部分内容和最初的包头相同，一个很典型的不同在于包头中还包含偏移量字段。随后各片段将沿各自的路径独立地转发到目的地，在目的地最终将各个片段进行重组。这就是所谓的 IP 包的分段重组技术。Teardrop 攻击就是利用 IP 包的分段重组技术在系统实现中的一个错误。

(3) Land 攻击。Land 也是一个十分有效的攻击工具，它对当前流行的大部分操作系统及一部分路由器都有相当的攻击能力。攻击者利用目标受害系统的自身资源实现攻击意图。由于目标受害系统具有漏洞和通信协议的弱点，这就给攻击者提供了攻击的机会。

这种类型的攻击利用 TCP/IP 实现中的处理程序错误进行攻击，因此最有效最直接的防御方法是尽早发现潜在的错误并及时修正这些错误。在当前的软件行业里，太多的程序存在安全问题。从长远的角度考虑，在编制软件的时候应更多地考虑安全问题，程序员应使用安全编程技巧，全面分析预测程序运行时可能出现的情况。同时测试也不能只局限在功能测试，应更多地考虑安全问题。换句话说，应该在软件开发的各个环节都灌输安全意识和法则，提高代码质量，减少安全漏洞。

2. 分布式拒绝服务攻击

DDoS(Distributed Denial of Service，分布式拒绝服务)攻击，是对拒绝服务攻击的发展，攻击者控制大量的攻击源，然后同时向攻击目标发起的一种拒绝服务攻击。海量的信息会使得攻击目标带宽迅速消失殆尽。分布式拒绝服务攻击技术发展十分迅速，由于其隐蔽性和分布性很难被识别和防御，响应和取证更加困难。

攻击过程主要有两个步骤：攻占代理主机和向目标发起攻击。具体说来可分为以下几个步骤：①探测扫描大量主机以寻找可入侵主机；②入侵有安全漏洞的主机并获取控制

权；③在每台被入侵主机中安装攻击所用的客户进程或守护进程；④向安装有客户进程的主控端主机发出命令，由它们来控制代理主机上的守护进程进行协同入侵，如图 5-9 所示。

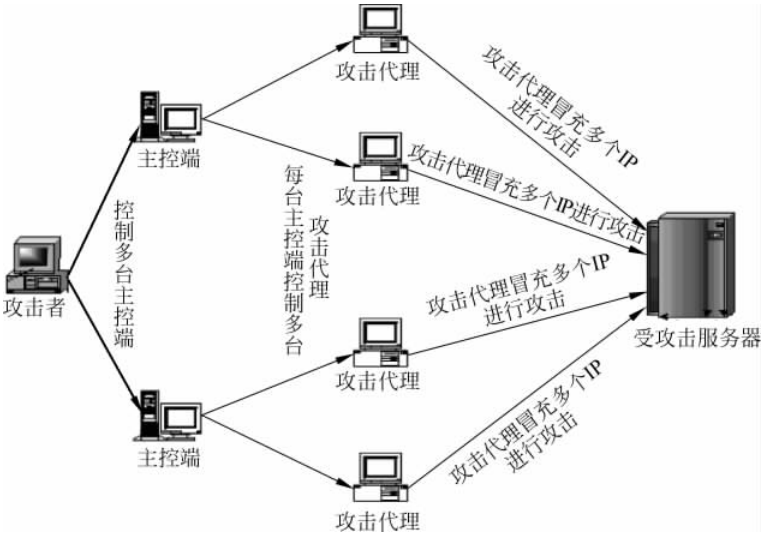

图 5-9　DDoS 攻击示意图

攻击者所用的计算机是攻击主控台，可以是网络上的任何一台主机，甚至可以是一个活动的便携机。攻击者操纵整个攻击过程，它向主控端发送攻击命令。主控端是攻击者非法侵入并控制的一些主机，这些主机还分别控制大量的客户主机。主控端主机的上面安装了特定的程序，因此它们可以接收攻击者发来的特殊指令，并且可以把这些命令发送到代理主机上。代理端同样也是攻击者侵入并控制的一批主机，它们上面运行攻击器程序，接收和运行主控端发来的命令。代理端主机是攻击的执行者，真正向受害者主机发送攻击。

相对于一般的拒绝服务攻击，分布式拒绝服务攻击有以下特点：①由于集中成百上千台机器同时进行攻击，其攻击力是十分巨大的。即使像 Yahoo!、Sina 等应用了可以将负荷分摊到每个服务器的集群服务器(Cluster Server)技术，也难以抵挡这种攻击。②多层攻击网络结构使被攻击主机很难发现攻击者，而且大部分装有主控进程和守护进程的机器的合法用户并不知道自己是整个拒绝服务攻击网络中的一部分，即使被攻击主机监测到也无济于事。

DDoS 所利用的协议漏洞主要有以下几种。

(1) 利用 IP 源路由信息的攻击。由于 TCP/IP 体系中对 IP 数据包的源地址不进行验证，所以攻击者可以控制其众多代理端用捏造的 IP 地址发出攻击报文，并指明到达目标站点的传送路由，产生数据包溢出。

(2) 利用 RIP 的攻击。RIP 是应用最广泛的路由协议，采用 RIP 的路由器会定时广播本地路由表到邻接的路由器，以刷新路由信息。通常站点接收到新路由时直接采纳，这使攻击者有机可乘。

(3) 利用 ICMP 的攻击。绝大多数监视工具不显示 ICMP 包的数据部分，或不解析 ICMP 类型字段，所以 ICMP 数据包往往能直接通过防火墙。例如，从攻击软件 TFN(Tribe Flood Network)客户端到守护程序端的通信可直接通过 ICMP-ECHOREPLY(Type0)数

据包完成。可直接用于发起攻击的 ICMP 报文还有：ICMP 重定向报文(Type5)、ICMP 目的站点不可达报文(Type3)、数据包超时报文(Type11)。

攻击者最常使用的分布式拒绝服务攻击程序主要有：Trinoo、TFN、TFN2K 等。

(1) Trinoo 攻击。Trinoo 是一种用 UDP 包进行攻击的工具软件。与针对某特定端口的一般 UDP flood 攻击相比，Trinoo 攻击随机指向目标端的各个 UDP 端口，产生大量 ICMP 不可到达报文，严重增加目标主机负担并占用带宽，使对目标主机的正常访问无法进行。

(2) TFN(Tribe Flood Network)攻击。TFN 是第一个公开的 UNIX DDoS 工具，由主控端程序和代理端程序两部分组成，其利用 ICMP 给主控端或代理端下命令，其来源可以做假。它可以发动 SYN flood、UDP flood、ICMP flood 及 Smurf 等攻击。

(3) TFN2K 攻击。TFN2K 是 TFN 的增强版，它增加了许多新功能：单向的对主控端的控制通道，主控端无法发现代理端地址；针对脆弱路由器的攻击手段；更强的加密功能，基于 Base64 编码，AES 加密随机选择目的端口。

3. 分布式反弹拒绝服务攻击

反弹技术就是利用反弹服务器实现攻击的技术。所谓反弹服务器(Reflector)是指当收到一个请求数据报后就会产生一个回应数据报的主机。例如所有的 Web 服务器、DNS 服务器和路由服务器都是反弹服务器。攻击者可以利用这些回应的数据报对目标机器发动 DDoS 攻击。

反弹服务器攻击过程和传统的 DDoS 攻击过程相似，如图 5-10 所示，如前面所述的 4 个步骤中，只是第 4 步改为：攻击者锁定大量的可以作为反弹服务器的服务器群，攻击命令发出后，代理守护进程向已锁定的反弹服务器群发送大量的欺骗请求数据包，其源地址为受害服务器或目标服务器。

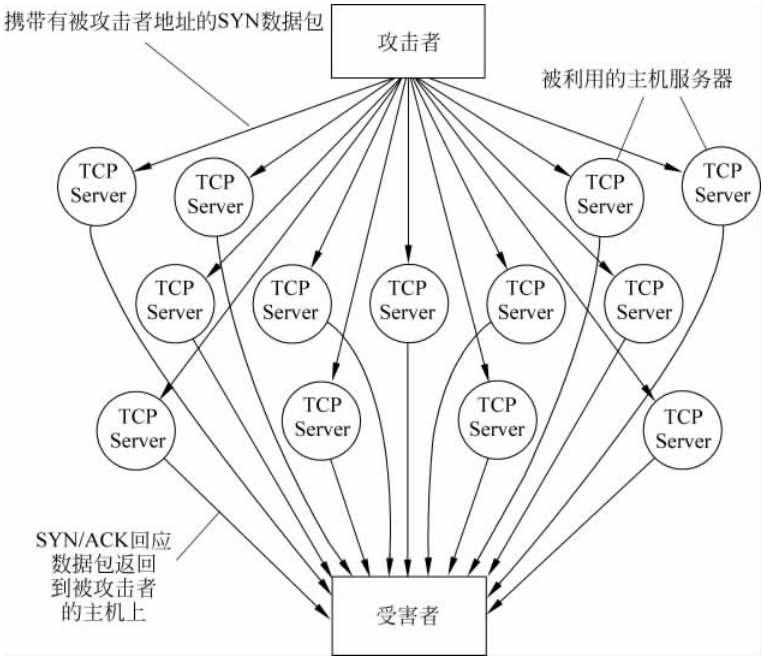

图 5-10　DDoS 攻击示意图

与传统 DDoS 攻击相比，①DRDoS 攻击更加难以抵御。实际上它的攻击网络结构和传统的相比多了第 4 层——被锁定的反弹服务器层。反弹服务器的数量可以远比驻有守护进程的代理服务器多，故反弹技术可以使攻击时的洪水流量变弱，最终才在目标机汇合为大量的洪水，其攻击规模也比传统 DDoS 攻击大得多。②目标机更难追查到攻击来源。目标机接收到的攻击数据报的源 IP 是真实的，反弹服务器追查到的数据报源 IP 是假的。又由于反弹服务器上收发数据报的流量较小（远小于代理服务器发送的数量），所以，服务器根据网络流量来自动检测是否为 DDoS 攻击源的这种机制将不起作用。

4. 拒绝服务攻击的防范

拒绝服务攻击会造成时间和金钱上的重大损失，但因为 Internet 上绝大多数网络都不限制源地址，伪造源地址非常容易；通过攻击代理的攻击，只能找到攻击代理的位置；各种反弹式攻击，无法定位源攻击者。所以完全阻止拒绝服务攻击是不可能的。不过防范工作可以减少被攻击的机会。

（1）有效完善的设计网络：分散服务器的位置，避免被攻击时的瘫痪；设置负载均衡、反向代理、L4/L7 交换机的，加强对外提供服务的能力；有些 L4/L7 交换机本身具备一定的防范拒绝服务攻击能力。

（2）带宽限制：限制特定协议占用的带宽，但这并不是完善的方法。

（3）及时安装厂商补丁——减少被攻击的机会。

（4）运行尽可能少的服务。

（5）只允许必要的通信，设置严格的防火墙策略，封锁所有无用的数据；封锁敌意 IP 地址。

（6）不要让自己的网络系统成为攻击者的帮凶。

（7）保持网络安全：让攻击者无法非法获得对主机系统的访问。

（8）安装入侵检测系统，尽早地检测到攻击，使用漏洞扫描工具，及早发现系统的弱点、漏洞并修补。

（9）网络出口过滤：在路由器上进行过滤。入口过滤：所有源地址是保留地址的数据包全部丢弃；所有源地址是本地网络地址的数据包全部丢弃。出口过滤：所有源地址不是本地网络的数据包全部丢弃。

（10）防止本地网络用户伪造 IP 地址攻击别人。

5.4 信息安全面临的新挑战

尽管当前信息安全科学技术得到了很大的发展，但是，信息技术和应用的不断发展变化也给其带来了巨大挑战，这些挑战主要有如下几个方面。

1. 通用计算设备的计算能力越来越强带来的挑战

当前的信息安全技术特别是密码技术与计算技术密切相关，其安全性本质上是计算安全性，由于当前通用计算设备的计算能力不断增强，对很多方面的安全性带来了巨大挑战。例如，DNA 软件系统可以联合、协调多台空闲的普通计算机，对文件加密口令和密钥进行穷搜，已经能够以正常的代价成功实施多类攻击；又如，量子计算机的不断发展向主要依赖数

论的公钥密码算法带来了挑战，而新型的替代密码算法尚不成熟。

2. 计算环境日益复杂多样带来的挑战

随着网络高速化、无线化、移动化和设备小开支化的发展，信息安全的计算环境可能附加越来越多的制约，往往约束了常用方法的实施，而实用化的新方法往往又受到质疑。例如，传感器网络由于其潜在的军事用途，常常需要比较高的安全性，但由于结点的计算能力、功耗和尺寸均受到制约，因此难以实施通用的安全方法。当前，所谓轻量级密码的研究正试图寻找安全和计算环境之间合理的平衡手段，然而尚有待于发展。

3. 信息技术发展本身带来的问题

信息技术在给人们带来方便和信息共享的同时，也带来了安全问题，如密码分析者大量利用信息技术本身提供的计算和决策方法实施破解，网络攻击者利用网络技术本身设计大量的攻击工具、病毒和垃圾邮件；由于信息技术带来的信息共享、复制和传播能力，造成了当前难以对数字版权进行管理的局面。因此，美国计算研究协会(CRA)认为，创建无所不在的安全网络需求是对信息安全的巨大挑战。

4. 网络与系统攻击的复杂性和动态性仍较难把握

信息安全发展到今天，在对网络与系统攻击防护的理论研究方面仍然处于相对困难的状态，这些理论仍然较难完全刻画网络与系统攻击行为的复杂性和动态性，直接造成了防护方法主要依靠经验的局面，“道高一尺，魔高一丈”的情况时常发生。

5. 理论、技术与需求的差异性

随着计算环境、技术条件、应用场合和性能要求的复杂化，需要理论研究考虑更多的情况，这在一定程度上加大了研究的难度。在应用中，当前对宽带网络的高速安全处理还存在诸多困难，处理速度还很难跟上带宽的增长，此外，政府和军事部门的高安全要求与技术能够解决的安全问题之间尚存在差距。

习题

一、选择题

1. 网络系统的安全威胁主要来自_____。

   A. 黑客攻击　　B. 计算机病毒

   C. 操作系统安全漏洞　　D. 以上都是

2. 下面各项中，_____不属于网络安全技术。

   A. 数据加密技术　　B. 防火墙技术

   C. 病毒防治技术　　D. 实验室安全技术

3. 计算机病毒是计算机系统中一类隐藏在_____上蓄意破坏的捣乱程序。

   A. 内存　　B. 硬盘　　C. 存储介质　　D. 网络

4. 防火墙用于将 Internet 和内部网络隔离，_____。

A. 是防止 Internet 火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

5. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于_____。

A. 对称加密技术　　B. 分组密码技术

C. 公钥加密技术　　D. 非对称加密技术

二、填空题

1. 信息安全研究领域的发展，经历了_____、_____、_____以及_____等阶段。

2. 信息保障的 PDRR 模型，其 5 个技术环节为_____、_____、_____、_____、_____。

3. 计算机信息系统的安全目标主要有：_____、_____、_____、_____和_____等。

4. 根据在系统中的作用，威胁信息系统的攻击可以划分为两大类：_____和_____。

5. 组织体系结构是信息系统安全的组织保障系统，由_____、_____和_____三个模块构成一个体系。

6. VPN 在实际应用中，主要有三种应用模式，分别是_____、_____和_____。

7. 防火墙的体系结构主要有：_____、_____、_____和_____。

8. J. Anderson 对入侵威胁进行了分类，指出来自内部的渗透者是系统安全的主要隐患，按照检测难度递增，把攻击分为_____（假冒他人的内部用户），_____（合法用户误用了对系统或数据的访问），_____（获取了对系统的管理控制）。

9. 计算机病毒具有以下几个特点：_____、_____、_____、_____、_____和_____。

三、简答题

1. 信息安全经历了哪几个发展阶段？每个阶段中的标志性事件是什么？

2. 信息安全的含义是什么？信息安全的安全目标包括哪几个？分别举例说明。

3. 安全策略与安全机制的关系是什么？常见的安全机制包括哪些？

4. 根据自己日常使用计算机和上网的经历，谈谈对信息安全含义的理解。

5. IPSec 主要有哪两种使用方式？每种方式的实用环境如何？

6. 防火墙的技术有哪些？试描述各种技术的特点并给出适用的场景。请说明防火墙在网络安全中的局限性。

7. 描述 VPN 的技术特点。

8. 简述恶意代码的分类，简述计算机病毒的发展。

9. 简述常见的计算机病毒检测方法与原理。