第1章 网络安全概述

本章主要讲述网络安全的定义，分析网络安全面临的诸多威胁因素，以及对网络安全的需求，并介绍网络安全发展的阶段历程。同时，对网络攻击的原理、攻击的实施过程和攻击的分类形式进行简要的分析描述，并针对常见的网络安全防护技术的原理、功能、主要类别以及缺陷不足进行简要探讨。在接下来的各章中，将围绕这些网络攻击方式和防御手段展开详细描述。

1.1 网络安全

伴随着互联网技术发展而来的网络空间领域已经成为全球最大的信息交互和共享平台，在网络空间领域中，系统连接的服务和对象可以无限互联、数据规模庞大且增长迅速、信息之间流通高速且广泛、接入网络空间中的应用也无限增长，这些现象已经成为影响关键信息基础设施甚至国家安全的网络安全问题。

1.1.1 网络安全定义

> 如果把一封信锁在保险柜中，把保险柜藏在纽约的某个地方，然后告诉你去读这封信。这并不是安全的，而是隐藏。相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置。而你还是无法打开保险柜去读这封信，这样才是安全的。
>
> ——Bruce Schneier

1. 安全的含义

安全是一种状态，一种与危险相对的状态，泛指不受到威胁，也没有危险、危害以及损失。通过持续的危险识别和风险管理过程，将人员伤害或财产损失的风险降低并保持在可接受的水平或其以下，使得其客观上不存在威胁，主观上也不存在恐惧，即不担心其正常状态受到影响。

安全的含义在人类生产过程中则是指将系统的运行状态对人类的生命、财产、环境可能产生的损害控制在人类不感觉难受的水平以下的状态。人类的整体与生存环境资源和谐相处，互相不伤害，不存在危险隐患。

2. 网络安全

网络安全是指网络系统中的硬件、软件以及系统中的数据受到保护，使得网络系统中的信息不因偶然或恶意的原因而遭到破坏、更改、泄露，网络系统连续可靠正常地运行，网络服务不中断。网络安全的核心任务就是保证网络信息内容的安全，通过计算机技术、网络技术、通信技术、密码技术等一系列安全技术确保信息内容在公用网络中的可靠传输、交换和存储。网络安全涉及的领域包括网络空间安全、主机安全、内容安全、Web 安全、移动安全、大数据安全、物联网安全等，在这些领域中，网络安全负责的相关工作内容包括网络攻击的防御、设备主机的安全、信息传播的舆情控制、信息的储存与交换安全、网络病毒防护、数据备份与恢复等。概括地说，网络安全就是在网络环境下能够识别和消除不安全因素的能力，通过采用各种技术手段和管理措施，使得网络系统能够正常运行，从而确保网络中数据信息的安全性。

网络安全的具体含义会随着不同角度的变化而变化：

（1）广义角度的网络安全，涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，主要保障网络系统中的软件、硬件与信息资源的安全性。

（2）从用户（如个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性、真实性和不可否认性的保护，这样可以避免其他人或对手利用窃听、冒充、篡改、抵赖等手段造成信息的泄露、破坏和伪造，侵犯用户的利益和隐私。

（3）从网络运行和管理者角度来说，他们希望本地信息网正常运行，能够为合法用户提供正常网络服务，不受到外网攻击，可以避免计算机病毒、拒绝服务、网络资源非法占用、远程控制与非法授权访问等安全威胁，提供及时发现安全问题与制止攻击行为的安全手段。

（4）对安全保密部门来说，加强数据信息的安全保密，提高人民的防间谍、防渗透、防泄密、反颠覆的意识和能力是主要工作目标，他们希望通过对非法的、有害的或涉及国家机密的信息进行过滤和防止，避免通过网络泄露关于国家安全或商业机密的信息，对企业造成经济损失，对国家造成损失，对社会造成危害。

（5）从社会教育和意识形态角度来讲，应避免网络中不健康内容的传播，正确引导积极向上的网络文化，网络安全主要保障信息内容的合法与健康，控制包含不良内容的信息在网络中传播。

3. 网络安全主体内容

网络安全的主要目的是保障网络中的数据和通信的安全性。其中，数据安全性是指在数字信息的整个生命周期中保护数字信息不受未经授权的访问、损坏或盗窃；通信安全是一系列保护措施，通过各种计算机、网络、密码技术和信息安全技术，确保在通信网络中传输、交换和存储信息的完整性、真实性、保密性和实效性，并对信息的传播及内容具有控制能力。

在信息传输、存储与处理的整个过程中，网络安全的要求是提高信息在物理和逻辑上的防护、监控、反应恢复能力和对抗能力。在这个过程中，网络安全的主体内容表现为运行系统安全、网络的安全、网络中信息内容的安全以及网络中信息传播的安全。

1）运行系统安全

运行系统安全保证信息处理和传输系统的安全，其本质是保护系统的合法操作和正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的消息造成破坏和损失。运行系统安全包括计算机系统机房环境的保护、计算机结构设计安全性考虑、硬件系统的可靠安全运行、计算机操作系统和应用软件的安全、数据库系统的安全、电磁泄漏防护和法律政策的保护等。

2）网络的安全

网络的安全即保障网络中系统信息的安全，其中包括用户认证、用户访问权限控制、数据访问权限、模式控制和安全审计、恶意代码防护等。

3）网络中信息内容的安全

网络中信息内容的安全侧重于保护信息的保密性、真实性、完整性、未经授权的访问和安全性，主要涉及信息传输的安全性、信息存储的安全性以及网络传输的信息内容的审计。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，其本质是保护用户的利益和隐私。

4）网络中信息传播安全

网路中信息传播安全即信息传播后果的安全，侧重于防止和控制由非法、有害的信息进行传播所产生的后果，避免公用网络中自由传输信息的失控。

4. 网络安全的特性

网络安全从其本质上来讲就是网络中的信息安全，网络信息安全主要表现出的特性包括保密性、完整性、可用性、可靠性、可控性、可审查性和不可抵赖性。

（1）保密性：确保信息或资源不被泄露或呈现给非授权的人。

（2）完整性：保证信息在传输和存储的过程中不会被非授权操作删除、修改、伪造。

（3）可用性：确保合法用户的正常请求能及时正确地得到服务或回应。

（4）可靠性：系统在规定条件下和规定时间内完成规定功能的概率。

（5）可控性：对网络信息的传播及内容具有可控制能力。

（6）可审查性：出安全问题时提供依据和手段。

（7）不可抵赖性：也称作不可否认性，是指在信息交互过程中参与者的真实同一性，即所有参与者都不能否认或抵赖曾经完成过的操作和承诺。

1.1.2　网络安全的需求

近年来，随着移动互联网的飞速发展，网络已经与人们的日常生活紧密联系在一起，但在其背后隐藏的网络安全状况却不容忽视，在使用网络的过程中，往往由于未能正确认识网络中的安全问题，安全防范意识薄弱，以致在日常操作中出现了一些不规范的行为，给网络安全带来隐患，给用户造成损失和伤害。

1. 网络安全的威胁因素

1）信息系统的脆弱性

信息系统自身安全的脆弱性是指信息系统的硬件资源、通信资源、软件及信息资源

等存在一些固有的弱点。非授权用户利用这些脆弱性可对网络系统进行非法访问，这种非法访问会使系统内数据的完整性受到威胁，也可能使信息遭到破坏而使得服务功能失效，更为严重的是有价值的信息被窃取而不留任何痕迹，从而使系统处于异常状态，甚至崩溃瘫痪等。信息系统的脆弱性可以从硬件组件层面、软件组件层面、网络和通信协议层面分别进行分析。

（1）硬件组件层面。硬件组件的安全隐患主要包括硬件设备的电磁泄漏性、网络存储介质的脆弱性、介质的剩磁效应等。在设计、选购硬件时，应尽可能减少或消除硬件组件的安全隐患。

（2）软件组件层面。软件组件的安全隐患来源于设计和软件工程实施中遗留的问题，例如数据库系统设计的脆弱性、软件设计中不必要的功能冗余、软件设计没有按照信息系统安全等级要求进行模块化设计，甚至不同设备构成的不同系统之间的相互协调都会存在各种不同的安全问题。

（3）网络和通信协议层面。TCP/IP 协议簇是目前使用最广泛的协议，但因为其设计原则是简单、可扩展，且只考虑了互联互通和资源共享而未考虑应用环境是否可信任，已经暴露出许多安全问题。况且网络系统的通信线路应对威胁的能力非常低，可以轻而易举地被非法用户利用，如对线路进行物理破坏、搭线窃听等。

2）操作系统和软件安全漏洞

操作系统作为系统资源的控制和管理器，其作用是负责调度、监控和管理系统中各种独立的硬件，使得它们可以协调工作、合理高效地满足用户同时使用多种系统资源的需求；应用软件则是为满足用户不同领域、不同问题的应用需求而提供的软件，可以拓宽计算机系统的应用领域，放大硬件的功能。安全漏洞则是指计算机系统在硬件、软件、协议等的具体实现或系统安全策略上存在的缺陷和错误，如操作系统的动态链接、创建进程、空密码、超级用户和 RPC（Remote Procedure Call，远程过程调用）等方面的缺陷以及应用软件的跨站脚本、SQL 注入、弱口令及 HTTP 报头篡改等。这些漏洞一旦被发现或者被攻击者利用，就可以使得攻击者在未授权的情况下访问系统，并通过网络植入木马、病毒等方式来攻击或控制整个系统，窃取其中的重要资料和信息，从而对系统安全造成严重危害。

漏洞在网络环境中影响到的范围很大，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换而言之，在这些不同的软硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

3）信息面临的安全威胁

网络安全的基本目标是实现信息的机密性、完整性、可用性、可控性和可审查性。对信息基本目标的威胁即是网络安全威胁，这些威胁可能来自各种渠道，如信息泄露、信息完整性破坏、陷阱门、媒体废弃、非授权访问、拒绝服务、窃听、假冒、授权侵犯、抵赖、业务流分析、信息安全法律法规不完善等，常见的威胁如下：

（1）信息丢失：病毒感染或者黑客攻击都会导致文件被删除和数据被破坏，从而造

成关键信息丢失。通过对信息安全威胁的分析可以知道，造成信息数据丢失的原因主要有软件系统故障、软件漏洞、误操作、病毒感染、黑客攻击、计算机犯罪、自然灾害等。

（2）信息泄露：信息泄露指敏感信息在有意或无意中被泄露给某个未授权的实体。敏感信息主要包括个人基本信息、设备信息、账户信息、社会关系信息和网络行为信息等，泄露通常发生在信息的传递、存储、使用过程中。

（3）信息完整性破坏：以未授权的非法手段取得信息，通过创建、修改、删除和重放等操作使信息的完整性受到破坏。

（4）陷阱门：通常是编程人员在设计实现时有意建立的访问系统的手段。当程序运行时，在特定的时间输入特定的指令，或提供特定的参数，就能绕过程序提供的安全检测和错误跟踪检查，从而获得目标信息。

（5）拒绝服务：是指信息或信息系统资源等可利用价值或提供服务能力的下降或丧失，通常是受到攻击所致。攻击者通过对系统进行大量非法的、根本无法成功的访问尝试而产生过量的系统负载，从而导致系统的资源对合法用户的服务能力下降，或者信息系统组件在物理或逻辑上受到破坏而中断服务。

（6）未授权访问：未授权实体非法访问信息系统资源，或授权实体超越权限访问信息系统资源。非法访问主要有假冒和盗用合法用户身份攻击、非法进入网络系统进行违法操作，合法用户以未授权的方式进行操作等形式。

（7）业务流分析：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. 网络安全需求

近年来网络的快速普及，以其开放、共享的特性对社会的影响越来越大，网络中各种新业务的兴起，以及各种专业用网的建设，使得敏感信息的安全保密工作越来越重要。随着我国信息化进程脚步的加快，利用计算机及网络发起的信息安全事件频繁出现，并呈现逐年攀升的趋势，因此必须采取有力的措施来保护计算机网络的安全。

计算机病毒、木马、蠕虫和黑客攻击等的日益流行，对国家政治、经济和社会造成危害，并对 Internet 及国家关键信息系统构成严重威胁。绝大多数的安全威胁是利用系统或软件中存在的安全漏洞来达到破坏系统、窃取机密信息等目的。此外，网络攻击者具备的技术条件和手段不断增强，使得联合攻击急剧增多，新一代网络蠕虫和计算机病毒层出不穷，同时，病毒传播的趋利性日益突出、病毒的反杀能力不断增强。尽管当前的网络安全技术与过去相比有了长足的进步，但总体形势不容乐观。特别是网络环境中的组织管理规范的缺乏导致网络攻击快速增长，从普通个人上升到企业公司，从军队到国家都受到不同程度的影响。从另一个层面讲，网络安全与我们个人、企业甚至国家的利益息息相关，网络安全的地位越来越重要，网络安全的需求已被提升到国家安全的战略高度。

1.1.3　网络安全的发展过程

1. 4 个发展阶段

网络安全的总体发展历程可分为 4 个阶段，分别是通信加密阶段、信息安全阶段、

信息保障阶段和网络空间安全阶段，随着通信技术演进及移动互联网发展，网络安全关注点逐渐由信息数据的加密技术延伸至网络空间安全本身，各阶段信息如图 1-1 所示。

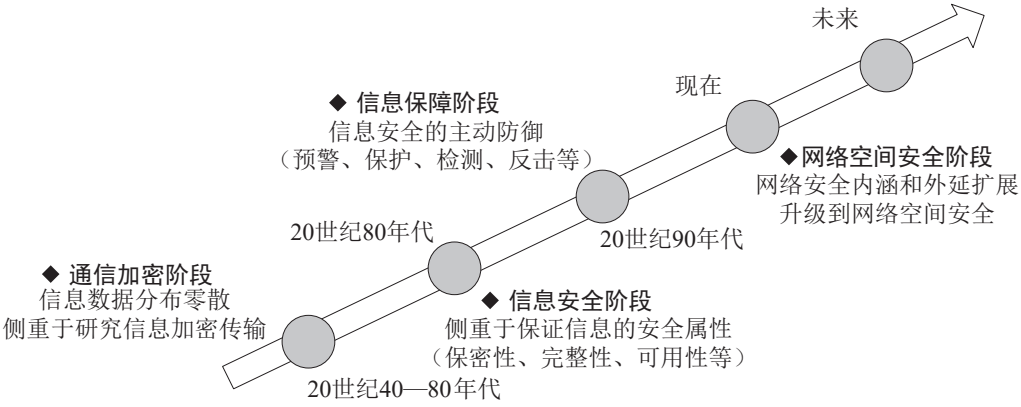


图 1-1　网络安全的发展阶段

1）通信加密阶段

20 世纪 40—80 年代时期，通信技术不发达，面对电话、电报、传真等信息交换场景中存在的安全问题，人们强调的是信息的保密性，即信息只能为授权者使用而不泄露给未经授权者的特性。在这一阶段，网络安全的重点研究是如何对信息进行编码后保证在通信信道上安全的传输，从而防止被信源、信宿以外的对象通过窃听通信信道而获取信息。对信息的保密处理依赖于密码技术，对信息安全理论和技术的研究侧重于密码技术，主要应用的是信道编解码和密码技术。

对于我国而言，只有少数专业单位进行密码技术的研究和开发，而且研究开发工作本身也是秘密进行的。直到 1984 年召开了“第一届中国密码学术会议”，掀起了国民研究密码学的热潮。

2）信息安全阶段

20 世纪 80 年代时期，计算机和网络技术的应用进入了实用化和规模化阶段。这一阶段计算机病毒出现并广泛传播，恶意程序、垃圾邮件的现象也相当普遍，随着网络技术的发展和应用，计算机病毒、蠕虫和木马等恶意代码通过网络传播，造成了更大范围的危害。于是，防治垃圾邮件，阻止计算机病毒等恶意代码的传播，保障网络安全成为社会对信息安全的迫切需要。除了通信保密之外，计算机操作系统安全、分布式系统安全和网络系统安全的重要性和紧迫性逐渐凸现出来。为了解决这些安全问题，出现了计算机安全、软件保护等安全新内容和新技术，同时出现了防火墙、入侵检测、漏洞扫描及 VPN 网络安全技术。人们对网络安全的关注已经逐渐转变为信息安全（Information Security）阶段，具有代表性的成果就是美国的 TCSEC 和欧洲的 ITSEC 测评标准。这一阶段的网络安全主要目标是保证网络信息的保密性、完整性、可用性、可控性和不可否认性。

3）信息保障阶段

20 世纪 90 年代，人类社会开始进入信息化时代。随着各种大型应用信息系统相继出现并广泛应用，信息科学技术和产业空前繁荣，社会的信息化程度大大提高。这些都

对信息的安全提出了更新更高的要求。网络安全不再局限于对信息的静态保护，而是需要对整个信息和信息系统进行保护和防御。在这一阶段，信息安全的重点工作是研究防御手段，具体可以分为 4 类：主动防御、纵深防御、深度防御、泛在防御，其中包括了预警、保护、检测、响应、恢复以及反击的整个过程。通过对攻击的行为进行分析提供报警信息以及设置多层重叠的安全防线，并对攻击者和目标之间的信息环境进行分层，在每一层都搭建由技术手段和管理等综合措施构成的一道道“屏障”，实现对信息和信息系统的安全属性及功能、效率进行保障。

在信息保障的概念中，人、技术和管理被称为信息保障三大要素。其中，人是信息保障的基础，信息系统是人建立的，同时也是为人服务的，受人的行为影响。技术是信息保障的核心，任何信息系统都势必存在一些安全隐患。管理是信息保障的关键，没有完善的信息安全管理规章制度及法律法规，就无法保障信息安全。通过运用源于人、管理、技术等因素所形成的保护能力、检测能力、反应能力、恢复能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

4）网络空间安全阶段

现阶段，随着企业信息化程度持续提升，自动化和远程办公的需求激增，网络安全关注点逐渐延伸至网络空间本身，2015 年起，网络安全行业正式进入“网络空间安全”时代。行业焦点逐步从前半场关注网络边界安全开始转移到关注网络空间安全的两个核心领域：内容安全及数据安全。我国的网络安全的重点工作主要包括国家安全、信息基础设施安全、信息系统和数据安全等。网络空间安全不仅拓展了信息安全的领域，也更加重视信息安全的重要性，把信息安全上升到国家安全层面。

总之，网络安全不是一个孤立静止的概念，具有系统性、相对性和动态性，其内涵随着人类信息技术、计算机技术及网络技术的发展而不断发展，如何有效地保障网络安全是一个长期的且不断发展的持久话题。

2. 行业未来发展趋势

网络安全行业是国家重点发展的战略产业，政策的大力支持为行业的发展创造了良好的环境和发展机遇。近年来国家有关部门相继出台了《网络安全法》《信息安全技术—网络安全等级保护基本要求》等一系列法规和政策，为网络安全产业的发展营造了良好的政策环境。

在未来，网络安全始终是不可缺少的重要组成部分，在整个网络安全产业中占有举足轻重的地位。网络安全行业市场规模仍会保持高增长，未来安全软件和服务增长空间更大；万物互联，安全需求提升，构建解决保密、信任、隐私等固有安全问题的新范式，真正实现网络安全与物理安全的深度融合；构建协同联动的网络安全防线，面对网络安全事件、应急处置、追踪溯源等需求持续增加，将重点加速厂商间有效的防御联动机制建立；同时，随着网络安全向更深层次渗透，更加细分化的技术领域、产品需求使得更多的技术创新不断涌现出来。因此未来网络安全事业的发展前景将更加广阔。

1.2 网络攻击

网络的传播性和共享性使得信息的处理和传递突破了时间和地域的限制，但与此同时，在错综复杂的网络环境中，攻击者利用系统安全漏洞进行病毒勒索和攻击，对系统安全运行、信息的传播、信息内容和网络的安全造成困扰，带来了更多的网络安全威胁。网络攻击就是产生网络安全威胁的根源，只有了解网络攻击的内涵才能深刻理解网络安全。

1.2.1 网络攻击定义

网络攻击是指针对计算机信息系统、计算机网络或个人计算机设备在没有得到授权的情况下偷取或访问数据的任何类型的进攻动作。通过利用信息系统自身存在的安全漏洞和安全缺陷等尝试访问或者进入网络系统，其目的是破坏网络中信息的保密性、完整性、可用性等，最终致使计算机网络和系统崩溃、失效或错误运行。

1.2.2 网络攻击分析视角

网络规模的飞速扩大、网络结构和协议日趋复杂、网络应用领域和用户群体不断扩大，导致出现了各种目的的网络攻击，造成的损失也越来越大。研究网络攻击，一方面可以对现有的攻击方式做出合理分类，研究其共性与特性，以便制定出合理的安全策略，更好地保护网络系统安全；另一方面，网络安全关系到小至个人的利益，大至国家的安全。对网络攻击技术的研究就是为了尽最大的努力为个人、国家创造一个良好的网络环境，让网络更好地为广大用户服务。

对一次网络攻击进行完整的分析，通常包括网络攻击的发起人、网络攻击实施过程、攻击者收益以及受害者伤害这 4 个分析视角。

1. 网络攻击的发起人

网络攻击的发起人，也称为攻击者，是导致网络攻击事件发生的主要人员。他们常常为了达到某些特定的目的策划发起网络攻击，他们使用的技术方法、攻击手段以及自身所具备的能力也各不相同。常见的网络攻击发起人有如下类别。

1）脚本小子

脚本小子是侵入计算机进行破坏的人，但他们的技术能力往往有限，缺乏挖掘漏洞的能力，只是简单地运行其他攻击者创建的攻击脚本，脚本小子通常也是单独作战，所以他们造成的攻击伤害往往较低。通过基本的安全控制措施，如定期打补丁、安全软件、防火墙和入侵防御系统等，可以轻松击败脚本小子。

2）黑客

黑客通常是指对计算机组成原理、编程、网络和攻防技术方面具有高度理解的人，在一般意义上，黑客是指企图非法进入计算机系统的人。在信息安全里，常见的黑客又可以根据发起网络攻击的动机分为黑帽黑客、白帽黑客、灰帽黑客、红帽黑客。

（1）黑帽黑客：指以非法目的进行网络攻击的人，他们利用自己的技术技能从事犯

罪活动。他们的动机是通常是为了经济利益。他们进入网络中进行破坏、伪造、修改或窃取数据，使网络无法为授权用户提供正常服务。黑帽黑客这个名字来源于一些经典的黑白电影中，坏角色总是戴着黑帽子，很容易被识别。

（2）白帽黑客：指那些专门研究或者从事网络、计算机技术防御的人，他们使用自己的黑客技术来维护网络安全，测试网络和系统的性能来判定它们能够承受入侵的强弱程度。大型企业组织经常雇用白帽黑客来发现其系统中的安全漏洞，以保护其业务免受网络攻击的侵害。

（3）灰帽黑客：指那些懂得技术防御原理，并且有实力突破这些防御的人。与白帽黑客和黑帽黑客不同的是，灰帽黑客倾向于展示他们的技能并获得宣传。他们通常只是对系统感到好奇，并试图不顾隐私或法律而获得访问权限。他们往往将黑客行为作为一种业余爱好或者义务来做，希望通过他们的黑客行为来警告一些网络或者系统漏洞，以达到警示别人的目的。因此，他们的行为没有任何恶意。

（4）红帽黑客：红帽黑客也称红客，是属于白帽和灰帽范畴的，但红帽黑客以正义、道德、进步、强大为宗旨，以热爱祖国、坚持正义、开拓进取为精神支柱，所以，并不能简单将红帽黑客归于两者中的任何一类。红客们通常会利用自己掌握的技术维护网络的安全，并对外来的进攻进行还击。在一个国家的网络或者计算机受到国外其他黑客的攻击时，第一时间做出反应、并敢于针对这些攻击行为做出激烈回应的，往往是这些红客们。

3）网络间谍

网络间谍是指有目的的被雇用入侵计算机盗窃信息的人，具有与黑客类似优秀的计算机技术，而且发起攻击的动机一般都是经济性的。网络间谍包括但不仅限于利用监视、窃取等手段获得在网络中传输、存储的通信数据或其他信息，他们不会像脚本小子或黑客那样随意寻找攻击目标，而是被雇用去攻击特定含有敏感信息的目标，在没有被任何人发现的前提下，侵入目标系统获取信息。

4）网络罪犯

网络罪犯是指借助于计算机技术对系统或信息进行攻击、破坏或利用网络进行其他犯罪行为的人，他们通常是一些网络诈骗、网络恐怖主义和其他形式的网络勒索的幕后操作人员。利用编程、加解密技术、法律法规的漏洞等在网络上实施的犯罪，危害网络及其信息的安全与秩序。网络犯罪分子具备的技术手段复杂，可以从脚本小子到有组织的帮派，并且主要是受金钱利益的驱使。

5）内部人员

网络和信息系统最大的安全威胁之一是来自内部人员，因为内部人员通常非常熟悉系统，并且比一般攻击者拥有更高的访问权限，掌握着大量的核心数据和密码。内部人员引起的网络攻击现象有以下几种原因：内部人员可能因为丢失了公司的笔记本计算机，或将商业文件寄到了错误地址产生信息泄露；员工可能会因为工作相关的负面事件或遭到开除而怀恨在心，并因此进行了蓄意报复等。

2. 网络攻击实施过程

网络攻击的重点分析视角就是网络攻击的实施过程，网络攻击实施过程中的主要步骤包括：收集攻击目标信息、端口和漏洞扫描、获取攻击目标访问权限、隐藏攻击源、

实施攻击、种植后门、清除攻击痕迹等，按照攻击的不同作用阶段可以将攻击过程分为攻击准备阶段、攻击实施阶段和攻击善后阶段，具体如图 1-2 所示。

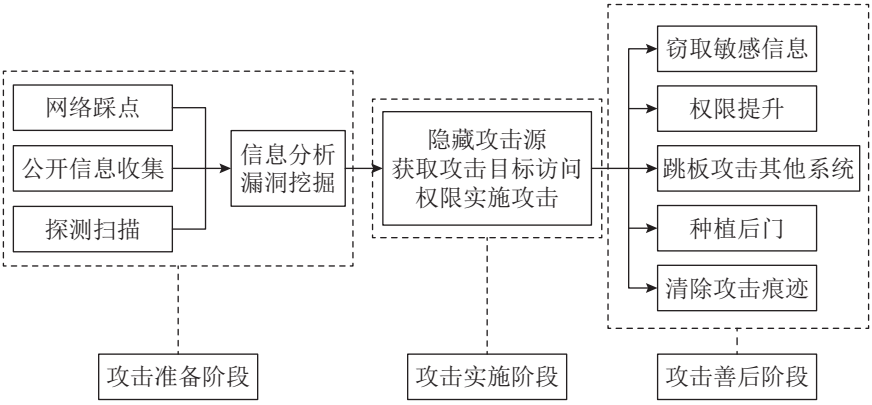


图 1-2　网络攻击的实施过程

1）攻击准备阶段

攻击者在进行一次完整的攻击之前，首先要确定攻击想要达到什么样的目的或造成什么样的后果，比较常见的攻击目的有破坏型和入侵型两种，破坏型攻击是指只破坏目标系统使之不能正常工作，而不能随意控制目标上的系统运行；入侵型攻击是指攻击者一旦掌握了权限就可以对攻击目标做任何动作，包括破坏性质的攻击。接着攻击者开始收集关于攻击目标的信息，这些信息包括公开的信息和主动嗅探的信息，如目标的操作系统类型、系统的漏洞信息以及攻击入口的信息等。

在已收集信息的基础上，就可以对目标系统进行全面的分析，包括目标主机所提供的服务分析、目标主机的操作系统分析、目标主机中可以被利用的漏洞分析以及目标主机其他弱点信息的挖掘与分析。在众多网络攻击的准备阶段中，攻击者考虑最多的是选择哪类平台、利用哪种漏洞发起攻击。

2）攻击实施阶段

攻击准备阶段确定了攻击的平台和利用的漏洞之后，攻击就进入了实施阶段。在此阶段中，系统的某些资源被攻击者选择作为网络攻击的对象，称为作用点，攻击的作用点在很大程度上体现了攻击者的目的，且一次攻击可以有多个作用点，即同时攻击系统的多个目标。对于不同攻击目的具有不同的攻击实施方式，如果为破坏性攻击，则一般直接利用工具发动攻击。如果为入侵性攻击，往往需要利用收集到的信息先找到系统漏洞，然后利用漏洞获取尽可能高的权限之后再实施网络攻击。

实施的网络攻击包括非法访问提取、网络钓鱼、病毒传播、种植木马等，实施攻击的一般步骤为先隐藏攻击发起的位置，接着利用收集到的信息登录目标系统，然后利用漏洞或者其他方法获得目标系统更高的控制权，最后进行非法活动、窃取网络资源或者以目标系统为跳板向其他系统发起新的攻击。

3）攻击善后阶段

在实现攻击的目的后，攻击者为了能长时间地保留对目标系统的访问控制权限，一般会留下后门。此外，攻击者为了自身的隐蔽性，通常会采取各种措施来隐藏攻击入侵

的痕迹。此时攻击者在获得系统最高管理员权限的基础上可以任意修改系统上的文件，所以攻击者如果想隐匿自己的踪迹，最简单的方法就是删除日志文件、删除操作记录、隐藏文件等。

3. 攻击者收益

攻击者发起网络攻击的动机和目的多种多样，如为了提升自身的网络技术、出于好奇心理或者为了到达某些目的，但更多的原因是为了经济收益。网络黑客实施攻击的目的通常可概括为两种：一是为了得到经济利益；二是为了满足精神需求。经济利益是指获取金钱和财物；精神需求是指满足心理欲望。常见的攻击者的目标以及能够获取的收益有以下几个方面：

1）获取信息

重要信息经常成为攻击者的目标，通过对信息的访问获取，攻击者可以凭借拥有的信息来获取利益，也可以使用、破坏或篡改这些信息，这是一种很恶劣的攻击行为，因为不真实的或者错误的信息都将对用户造成很大的损失。例如，专有信息、信用卡信息、个人隐私和政府机密信息等经常成为攻击者的目标。

2）控制系统资源

系统资源也是导致系统成为攻击目标的原因所在。这些资源可能是非常丰富的、独一无二的，如专业硬件、专用服务器、高性能的计算系统以及高速网络系统等。攻击者可以利用这些资源来实现自己的企图。控制系统资源同时意味着获取了系统的超级用户的权限，这对攻击者也是一个极大的诱惑。在 UNIX 系统中拥有这种权限就可以随意进行网络监听，在一个局域网中，掌握了主机的超级用户权限也就可以说掌握了整个子网。

3）经济收益

经济收益一直是引发网络攻击背后的主要动机。受经济利益的驱使，目前实施网络攻击行为的各个环节已经形成了一个完整的产业链，即黑色产业链。如针对个人网上银行的攻击，其中有负责木马软件制作人员，有负责植入木马的人员以及负责转账和异地取现人员等，巨大的经济收益使得网络犯罪组织化、规模化、公开化，网络攻击事件频发。

4. 受害者伤害

网络攻击的结果就是攻击对目标所造成的伤害，也是受害者所能感受到的攻击带来的影响，例如对目标系统的软、硬件资源、其中的信息及系统运行服务造成了哪些方面的影响、影响的严重程度以及是否还会有其他后续表现等，主要体现在攻击结果、破坏强度和传播性这 3 个方面。

（1）攻击结果即攻击者对目标系统的攻击之后导致的后果，如直接导致的经济损失、业务损失、网络环境的破坏、信息的非法收集、系统的非法使用等。

（2）破坏强度则是攻击对目标系统的各部分服务正常运行的影响程度，当攻击者侵入网络中的计算机系统后，窃取机密数据和盗用特权或破坏重要数据使系统功能得不到充分发挥、提供的服务不能正常运行甚至系统瘫痪。

（3）传播性主要考虑网络攻击是否会利用当前系统作为跳板继续对其他目标发起新的攻击。这就需要注意网络中信息的来源和去向是否真实，内容是否被改动，以及是否泄露等。例如在网络中传播病毒可以通过公共匿名 FTP 文件传送，也可以通过邮件和邮件的附加文件形式传播。

1.2.3 网络攻击的分类

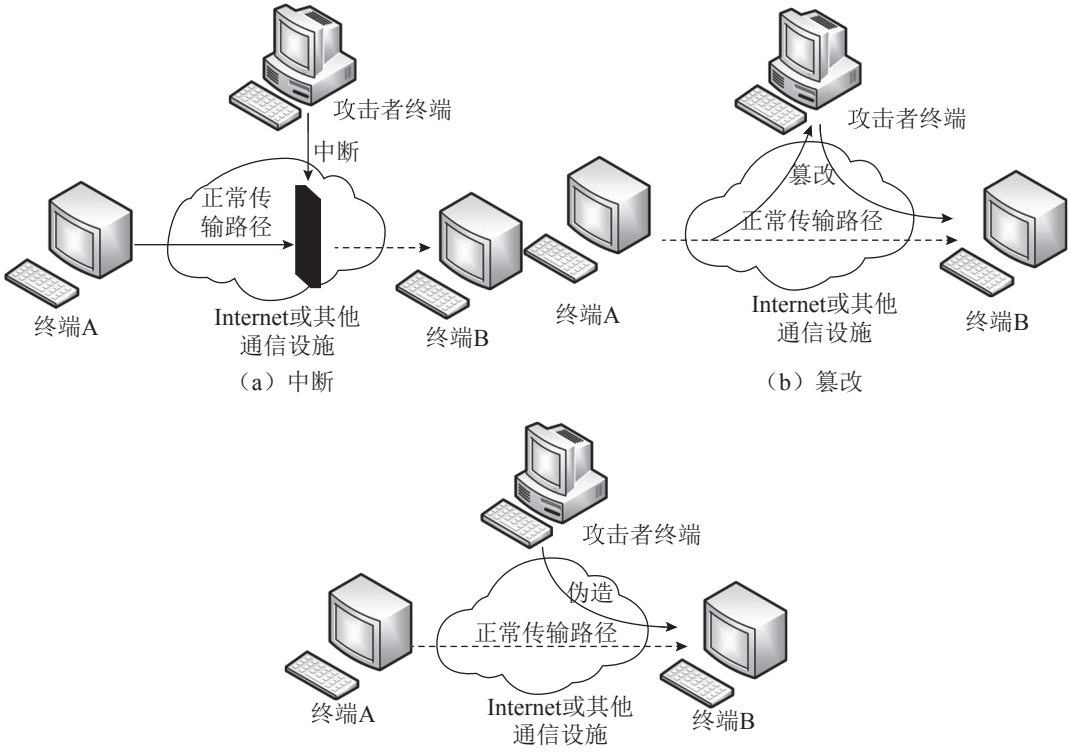
网络攻击根据不同的视角可以有多种分类方式，其中最为常见的是将网络攻击分为主动攻击和被动攻击，网络攻击也包含其他不同的分类方法，具体情况如下。

1. 主动攻击和被动攻击

1）主动攻击

主动攻击是指攻击者通过网络攻击信息来源的真实性、数据传输的完整性，以及系统服务的可用性，使系统无法正常运行。主动攻击容易被发现，但是比较难阻止，所以对付主动攻击应该及时发现，并采取响应措施使系统恢复正常。

主动攻击原理包括中断、篡改和伪造，如图 1-3 所示，中断是指截获由发送方发送的数据，将有效数据中断，使接收方无法接收到数据；篡改是指将发送方发送的数据进行篡改，从而影响接收方所接收的信息；伪造是指发送杜撰的数据以欺骗接收方。常见的主动攻击有拒绝服务攻击、分布式拒绝服务攻击、篡改信息、欺骗攻击、重放攻击等攻击方法。



（a）中断　　（b）篡改

（c）伪造

图 1-3　主动攻击原理

（1）拒绝服务攻击：即常说的 DoS（Denial-of-Service attack），通常是对目标发送大量伪造信息实施破坏，其目的在于使目标设备的网络或系统资源耗尽，使服务暂时中断或停止，导致其用户无法正常访问使用。

（2）分布式拒绝服务攻击：是指处于不同位置的多个攻击者同时向一个或数个目标发动 DoS 攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对目标同时实施攻击。它利用网络协议和操作系统的一些缺陷，采用欺骗和伪装的策略来进行网络攻击，使网站服务器充斥大量要求处理的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以致瘫痪而停止提供正常的网络服务。

（3）篡改信息：一个合法消息的某些部分被蓄意地修改、插入、删除、伪造、乱序，以致形成虚假信息，通常用以产生一个未经授权的效果。如修改传输消息中的数据或对已经存储在主机中数据信息进行篡改。

（4）欺骗攻击：是指利用假冒、伪造的身份信息与其他主机进行合法的通信或者发送假的报文，使受到欺骗攻击的主机出现错误行为；或者伪造一系列假的网络地址顶替真正的主机为用户提供网络服务，以此方法获得访问用户的合法信息后加以利用，转而攻击主机的网络欺骗行为。常见的主要方式有 ARP 欺骗、IP 欺骗、域名欺骗、Web 欺骗及电子邮件欺骗等。

（5）重放攻击：是指攻击者将一些发送主机曾经发送给接收主机的数据包，在未来某个时刻再次发送给接收主机。主要用于破坏接收主机的认证正确性。攻击者事先利用网络监听或者其他方式窃取网络中传输的认证数据，之后再把它重新发给服务器进行认证服务。

2）被动攻击

被动攻击是一种在不影响正常数据通信的情况下，通过监听截获由发送方发送到接收方的有效数据，从而对网络系统造成间接的影响，其原理如图 1-4 所示。被动攻击是对信息的保密性进行攻击或泄露数据信息，不会对其传输造成影响，这也导致数据的合法用户对这种活动不易觉察，同时由于被动攻击只是试图获取和利用数据信息，不会对系统资源造成修改和破坏，所以留下的痕迹很少或者不留下痕迹，这导致被动攻击难以被检测到，但采取安全防护措施可有效阻止被动攻击。主要的被动攻击有窃听、流量分析等。

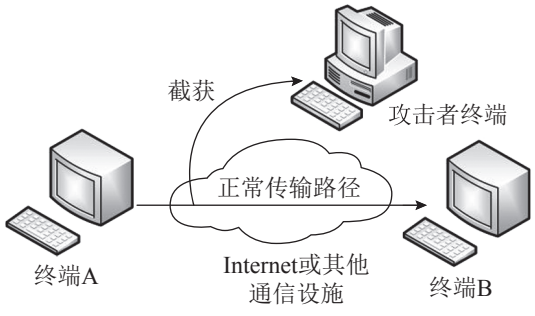


图 1-4　被动攻击原理

（1）窃听：也称为嗅探或侦听攻击，是比较常用的攻击手段。以太网是一个广播型的网络，这就使得一台主机可以捕获以太网上所有的报文和帧，并且只须将以太网卡设

置成杂收模式，然后主机就可以将捕获的所有信息传送到上层，以供进一步分析。这种攻击不会影响网络中信息的正常传输过程，并且对网络和主机都是透明的。窃听还可以通过高灵敏接收装置接收网络站点辐射的电磁波或网络连接设备辐射的电磁波，通过对电磁信号的分析恢复原数据信号从而获得极有价值的信息。

（2）流量分析：当网络中传输的敏感信息都经过加密保护时，即使攻击者截获这些消息，也无法直接获取消息的真实内容。然而攻击者可以通过观察这些数据报流量的模式，分析确定出通信双方的位置、通信次数及消息的长度等相关信息，这种攻击方式称为流量分析。

2. 攻击向量分类方式

攻击向量是攻击者用来获取本地或远程网络和计算机的一种方法，是一种路径或手段，攻击者可以通过攻击向量访问计算机或网络服务器以传递有效负载或恶意结果。攻击向量使得攻击者能够利用系统漏洞、人为因素等发起网络攻击。攻击向量的类别包括有计算机病毒、蠕虫、木马程序、网络钓鱼、拒绝服务攻击、物理攻击、网络攻击、密码攻击、信息收集攻击等，具体信息如表 1-1 所示。

表 1-1　攻击向量及其具体手段

攻击向量	目标形式	具体手段
计算机病毒	系统的软、硬件资源	网络病毒、文件病毒、系统病毒、引导型病毒、宏病毒、多态病毒等
蠕虫	对系统的控制、监视和破坏，勒索钱财，彰显技术	利用漏洞主动攻击，通过网络、电子邮件、移动存储设备等传播
木马程序	窃取、篡改信息，监控与开展间谍活动	网络下载、代理木马、FTP 木马、网页浏览入侵、远程入侵等
网络钓鱼	引诱敏感信息，获取经济利益、网络诈骗	电子邮件、鱼叉式网络钓鱼、语音电话钓鱼、短信网络钓鱼、悬浮弹窗、域欺骗、聊天软件等
拒绝服务攻击	阻止计算机和网络提供正常服务	网络带宽消耗攻击、连通性攻击、泪滴攻击、僵尸网络攻击、应用程序级洪水攻击、修改配置文件等
物理攻击	网络中的硬件和实体设备	侧信道分析、电磁场攻击、功耗攻击等
网络攻击	数据信息、网络协议、网络用户	网络欺骗攻击、会话劫持、网络协议漏洞攻击、应用程序攻击、Web 攻击等
密码攻击	获取密码，恢复明文	暴力破解、凭证填充、唯密文攻击等
信息收集攻击	目标对象、网络位置、拓扑结构等详细信息	扫描技术、网络拓扑探测、Web 搜索与挖掘、嗅探 Sniffer 等

（1）计算机病毒：编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机正常使用并且能够自我复制的指令或程序代码。

（2）蠕虫：一种能够不利用受感染文件传播的自我复制程序，它不需要附着在其他程序上，而是独立存在的，通常，蠕虫通过系统漏洞或电子邮件传播。

（3）木马程序：表面上是正常的程序软件，实际目的却是危害安全并导致严重破坏

的计算机程序，木马通常具有远程控制能力。

（4）网络钓鱼：通过伪造信息获得受害者的信任并且响应。

（5）拒绝服务攻击：阻止合法用户访问使用主机或网络服务的攻击。

（6）物理攻击：破坏或摧毁网络系统架构、计算机硬件部件的攻击。

（7）网络攻击：通过网络协议攻击网络或通过网络服务攻击网络用户等。

（8）密码攻击：通常是获取密钥或恢复明文的攻击。

（9）信息收集攻击：在攻击中不对目标本身造成直接伤害，但获取目标重要信息用于进一步入侵攻击。

3. 访问级别分类方式

根据攻击者为发起网络攻击所需的目标系统上的访问权限级别对网络攻击进行分类。采用 3 级分类法从不需要访问权限到需要一般用户访问权限，再到需要 Root 访问权限，对常见的攻击方式进行如下分类：

1）不需要访问权限

（1）计算机病毒。

（2）拒绝服务攻击。

（3）分布式拒绝服务攻击。

（4）缓冲区溢出攻击。

（5）网络钓鱼攻击。

2）需要一般用户访问权限

（1）密码攻击：获取用户密码的攻击方式包括字典攻击、暴力破解、彩虹表或者使用目标系统相同的加密方法对比密文结果。

（2）嗅探攻击：攻击者能够凭借有限的权限访问目标系统并嗅探网络流量以捕获网络中传输的数据信息，包括网络传递的身份验证凭证等。攻击者还可以在系统中留下嗅探器充当后台进程，一旦程序运行就不需要攻击者停留在受感染的目标系统中，如果用户名、密码和电子邮件等涉密信息在未加密的网络中传输，嗅探器会自动收集这些信息。

（3）干扰攻击：从合法权限登录的账户可以发起的干扰攻击包括篡改数据、删除文件、更改伪造数据或文档、更改用户密码，以及向网络中其他合法账户发送垃圾邮件等。

3）需要 Root 访问权限

（1）后门程序：后门程序指那些绕过安全性检测而获取对程序或系统访问权限的程序方法。在软件的开发阶段常常会创建后门程序以便可以修改程序设计中的缺陷，但这也成为安全风险，容易被攻击者当成漏洞进行攻击。

（2）Rootkit 程序：Rootkit 是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息。Rootkit 一般都和木马、后门等其他恶意程序结合使用。因此，攻击者可以伪装目标与攻击计算机之间的通信，还可以利用此恶意软件发现通过网络连接的其他计算机的用户名和密码。

（3）蠕虫：蠕虫病毒本身是一个需要以一定身份权限执行的程序。因此通过系统漏

洞进行感染是其手段，提升权限是其企图，重复感染是其目的。

（4）键盘记录器：键盘记录器攻击用于记录用户在键盘上输入的敏感信息，例如账户密码信息。此方法需要获取 Root 权限。键盘记录软件有 keylog、Snake Keylogger 等。在 Root 账号下通过编译键盘记录程序或者执行编译好的键盘记录程序，当 Root 用户登录时，程序自动捕获 Root 账号输入的密码。

4. 漏洞视角分类方式

漏洞是指一个系统在硬件、软件、协议或系统安全策略上存在的弱点，它可能来自应用软件、操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷、逻辑流程上的不合理之处。这些缺陷、错误以及不合理之处可能被有意或无意地利用，从而使攻击者能够在未授权的情况下访问或破坏系统。常见的网络安全漏洞的种类分为软件漏洞、结构设计漏洞、配置漏洞、管理漏洞、信任漏洞等。

1）软件漏洞

任何一款软件系统或多或少都存在一定的脆弱性，这种脆弱性可能是由于软件系统本身设计缺陷带来的，也有可能是由于软件程序实现时没有满足设计时的安全要求，导致出现了软件漏洞。常见的软件漏洞有：跨站脚本攻击 XSS、跨站请求伪造 CSRF、Cookie 挟持和 HTTP 头篡改、SQL 注入攻击、缓冲区溢出、身份验证漏洞、敏感数据泄露等。

2）结构设计漏洞

系统的基本结构设计是有缺陷的，例如 2017 年 5 月，国外安全研究人员发现在 Linux 环境下，可以通过 sudo 指令实现本地提权的漏洞，它几乎影响所有 Linux 系统；网络中由于忽略了安全问题，或者没有采取有效的网络安全措施，使网络系统处于不设防的状态也是结构设计漏洞；另外在一些重要网段结构搭建中，交换机和集线器等网络设备设置不当，也会造成网络流量被不法获取。

3）配置漏洞

由于操作系统、应用服务器、数据库服务器、应用程序、中间件及相关应用程序所使用的框架的不安全配置，造成恶意用户能够利用这些配置漏洞对应用系统进行攻击，窃取系统敏感信息、尝试控制服务器。例如系统的不正确配置导致打开多个易受攻击的网络端口。网络中由于忽略了安全策略的制定或者在网络环境发生变化后，没有及时更改内部安全配置造成的配置漏洞。

4）管理漏洞

网络管理者由于管理工作的疏忽或其他个人因素造成的安全漏洞，例如长期不更改系统密码造成入侵攻击。网络管理者要充分认识网络安全的重要性，在日常的工作中针对发生的安全问题进行及时的管理维护，并提升自己的安全管理意识。

5）信任漏洞

信任漏洞是因为过分信任网络环境中的合作设备而不进行相应的鉴权流程，因此一旦某个合作方设备被入侵，攻击者很容易将网络攻击传播至整个互相信任的设备链上，使网络安全遭受到严重威胁。

5. 攻击位置分类方式

根据攻击者发起网络攻击时在网络环境中的位置可以将网络攻击分为远程攻击、本地攻击和伪远程攻击。

（1）远程攻击：指攻击者通过各种手段从该子网以外的地方向该子网或者该子网内的系统发动攻击。

（2）本地攻击：指公司、企业等内部人员，通过所在的局域网向本单位的其他系统发动攻击或者进行非法越权访问。

（3）伪远程攻击：指内部人员为了掩盖攻击者的身份，在获取攻击目标的一些必要信息后，从外部远程发起攻击造成一种外部入侵的现象。

6. 攻击目标分类方式

网络攻击的目标可以分为硬件目标、软件目标和网络目标。

（1）硬件目标：主要包括计算机设备、网络设备和外围设备等。计算机设备的攻击目标是计算机硬件组件，如计算机主板和硬盘等；网络设备的攻击目标有路由器、交换机等；外围设备的攻击目标有扫描仪、打印机、光驱等。

（2）软件目标：主要包括操作系统和应用程序。操作系统的攻击目标有操作系统的权限提升、内网渗透、远程漏洞等；应用程序的攻击目标有程序代码注入、SQL 注入、脚本攻击、会话劫持、数据文件伪造等。

（3）网络目标：主要是以网络资源或网络协议为攻击目标。如对网络中的链路带宽资源攻击的拒绝服务攻击，对传输层协议攻击的 TCP RST 攻击、TCP 会话劫持攻击；网络层协议的 IP 源地址欺骗、ARP 欺骗和 ICMP 路由重定向攻击等。

1.3　网络安全防护技术

现今互联网技术不断发展的形势下，伴随着的网络安全问题也日益凸显，网络安全形势不容乐观。以僵尸网络、间谍软件、木马后门等为代表的各类恶意代码威胁逐渐扩大；拒绝服务攻击、网络欺骗、垃圾邮件等安全事件屡见不鲜，与此同时，网络犯罪的集团化、产业化的趋势以及对攻击者的技术水平要求越来越低导致网络安全事件数量保持逐年的显著上升趋势。网络安全事件的频繁上演，不仅给人们的生活增加困扰和麻烦，甚至危害国家安全。这是一场无形的战斗。在这场斗争中，安全防护技术是最为关键的防御手段，提高安全防护技术就是保障网络安全的根本所在。

1.3.1　网络安全防护技术定义

网络安全防护技术是指保护系统硬件、软件、内部数据、服务的一种网络安全技术。通过多种网络管理手段和技术手段对系统进行有效的介入控制，确保网络系统运行的安全状态，以及保证数据信息在网络环境中的安全特性。网络安全防护技术主要包括物理安全分析技术、网络结构安全分析技术、系统安全分析技术、管理安全分析技术，以及其他安全服务和安全机制策略等。

1.3.2 网络安全防护分析视角

网络安全防护问题已成为社会关注的焦点。一方面，网络技术已经成为整个社会经济和企业生存发展的重要基础，但这其中的安全性问题日益凸现；另一方面，政府机构、企业和用户对网络技术的稳定性、可维护性和可发展性提出了越来越迫切的需求。因此，网络安全防护已经刻不容缓，同时网络技术的安全性问题还是一个关系到国家主权和安全、社会的稳定、民族文化的继承和发扬的重要问题，没有网络安全就没有国家安全。网络安全防护技术为维护国家网络安全提供了重要的技术支持，为支撑经济社会发展构建坚实的安全屏障。

网络安全防护的主要任务是对网络攻击的预防、检测和响应。在遭受网络攻击之前，安全防护的主要工作内容是针对网络设备的管理和技术建立各种预防措施，如通过制定网络设备安全管理措施、规划网络平台安全策略、建立可靠鉴别机制等预防攻击者对网络系统的非法授权访问；系统在遭受到网络攻击时，网络安全防护应该能够采取各种网络安全技术检测出正在发生的网络攻击行为，同时有效应对网络攻击并控制攻击的影响和范围；在攻击发生之后，网络安全防护的工作除了作出攻击响应外，还应该快速地恢复网络系统的功能服务，以及做好攻击现场的保护，以便于分析攻击源，防止相同的攻击行为再次发生，必要时可以进行网络反击等。

1. 网络安全防护的体系层次

攻击者发起攻击的目标对象可能是网络信息系统中的物理设备、操作系统、网络服务、应用程序和管理措施等，作为全方位的、整体的网络安全防护体系也是具有分层的结构。如图 1-5 所示，针对网络攻击不同目标涉及不同的安全问题，将网络安全防护的体系层次划分为物理层安全防护、系统层安全防护、网络层安全防护、应用层安全防护和管理层安全防护。

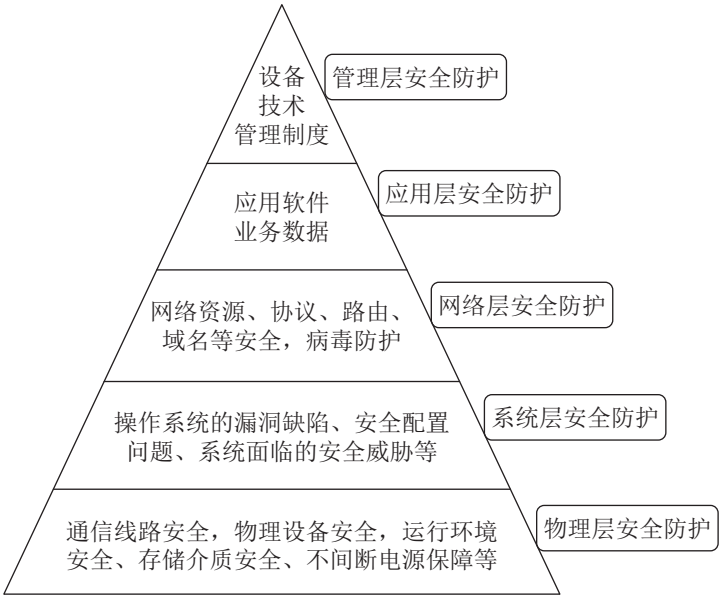


图 1-5　网络安全防护的体系层次

1）物理层安全防护

主要是针对网络信息系统的物理环境安全防护，保护系统设备、设施及其他媒体免遭环境事故和人为操作失误导致的破坏。物理层安全包括通信线路安全、物理设备安全、存储介质安全、机房安全等，主要体现在通信线路的安全性（搭线窃听、电磁干扰、人为破坏）、软硬件设备安全性（设备丢失、拆卸破坏、替换）、备份与恢复能力、设备的运行环境（温度、湿度、烟尘）、不间断电源保障等各方面。物理层安全防护是整个网络信息系统安全必须的前提条件。物理环境安全的防护措施包括物理隔离、设备和线路冗余、通信屏蔽、机房和账户安全管理等。

2）系统层安全防护

主要是针对操作系统的安全防护。操作系统是用来管理系统资源、控制程序的执行、提供人机交互服务的一种软件，是将计算机系统硬件与其运行的程序软件和用户之间连接的桥梁，可以说没有操作系统就没有计算机和网络，因此系统层安全防护是整个网络安全的基础条件。系统层的安全问题主要表现在操作系统本身的缺陷（后门程序、访问控制、系统漏洞）、操作系统的安全配置问题、外部主动攻击（病毒、木马、蠕虫）等对操作系统的安全威胁。操作系统安全的防护措施包括制定安全策略、补丁程序、终端防护软件、个人防火墙等。

3）网络层安全防护

主要是针对网络系统的安全防护，网络系统主要用于建立通信连接和进行信息传输。该层次的安全问题主要体现在网络层身份认证、网络资源访问控制、数据保密性与完整性、网络安全协议、安全路由、防病毒技术等。网络层安全的防护措施包括防火墙、VPN、入侵检测、抗 DDoS 等。

4）应用层安全防护

主要是针对系统中应用程序的安全防护。应用层安全问题主要体现在使用的应用软件安全性（Web 应用安全、Web 服务端安全、HTTP 协议安全、电子邮件安全、DNS 安全、前端页面安全、后端接口安全）和数据的安全性（数据库安全、恶意代码、SQL 注入），此外还包括病毒对系统的威胁。应用层安全的防护措施包括 Web 应用防火墙、前端网页防篡改、输入输出验证过滤、数据库加密、安全审计、恶意代码检测等。

5）管理层安全防护

主要是针对系统管理制度的安全防护，管理的制度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网络信息系统面临的安全威胁。管理层安全的防护措施包括网络安全技术和设备的管理、安全管理制度、安全管理机构、部门与人员的组织规则等。

网络安全防护的工作机制可以分为 3 个步骤：安全风险评估、安全加固、网络安全部署。其中，安全风险评估指根据国家风险评估相关管理要求和技术标准，对网络信息系统的设备、存储、处理和传输的信息的保密性、完整性、可用性等安全属性进行科学、公正评估的过程。涉及网络信息系统的脆弱性、可能面临的安全威胁及其带来的实际影响，并根据可能造成的影响确定网络安全风险等级。对系统进行风险评估一方面可以了解系统存在的潜在风险，为系统安全策略的确定、安全加固提供依据；另一方面可

以为系统安全测试提供检验目标。安全加固是以风险评估的检测结果为依据，对信息系统存在的安全问题逐一排查清除，同时对系统性能进行优化配置，杜绝系统再次面临安全威胁。安全加固作为一种积极主动的安全防护手段，将信息系统安全防护的五层体系层次建立在符合安全需求的安全状态，提高系统整体的健壮性和安全性，提升系统安全防范水平。网络安全部署是在信息系统中进行安全技术产品的部署，如防火墙产品、VPN、IDS、IPS 等，可以对网络信息系统起到更可靠的保护作用，提供更强的安全监测和防护能力。

2. 网络安全防护的设计原则

在网络安全防护体系的设计过程中，根据阻止网络攻击发生的需求、需要达到的安全目标及对应安全机制所需的安全服务等因素，同时综合考虑网络安全技术的可实施性、可管理性、可扩展性、系统均衡性等方面，提出网络安全防护体系在整体设计过程中应遵循以下原则。

1）木桶原则

木桶原则是指要对网络安全进行全面均衡的保护。网络信息系统是一个复杂的计算机系统，攻击者极大可能利用“木桶短板效应”在系统中最薄弱的地方发起攻击。防护体系任何一方面的缺失或不完全都有可能影响到保护效果，因此需要充分、全面、完整地对系统的安全防护进行设计分析，提高整个系统的“安全最低点”的防护能力。

2）整体性原则

整体性原则是指在进行安全防护策略设计时需要考虑各种安全配套措施的整体一致性，要求网络信息系统在遭受到攻击破坏时，能够尽可能地快速恢复系统中心服务，减少损失。因此，安全防护体系的整体性应该包括安全检测机制、安全防护机制和安全恢复机制。

3）均衡性原则

对任何网络信息系统，绝对安全是很难达到的，所以需要建立合理实用的安全性与系统安全需求的平衡体系。安全防护设计要正确处理系统的安全需求、风险与代价的关系，做到安全性与可用性相均衡。

4）可用性原则

安全防护体系的各种措施需要支持主流的系统，同时应该易于安装、管理和维护，且不能影响系统的正常运行。

5）等级性原则

一个完善的安全防护体系应该具有不同安全层次和安全级别，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级，对系统实现结构分层，从而针对不同级别的安全对象，提供全面、可选的安全防护机制，以满足网络信息系统中不同层次的各种安全需求。

6）一致性原则

网络信息系统是一个采用开放标准和技术的庞大系统工程，所以安全防护体系的设计同样也需要遵循一系列的标准，这样才能确保与信息系统的一致性，使其能够和信息系统安全地互联互通、信息共享。

7）可扩展性原则

安全防护体系的总体设计不仅要满足近期网络安全目标，也要为网络的进一步发展留有扩展的余地，也就是说安全防护体系需要有根据网络安全的变化调整或增强安全防护措施的扩展能力，适应新的网络环境，满足新的网络安全需求。

1.3.3　网络安全防护技术常见类型

针对目前众多种类的网络攻击方式，网络安全防护技术都提出了相应的解决方案。现今的主流的网络安全技术有以下几类。

1. 防火墙技术

尽管近年来各种新颖的网络安全技术在不断出现，但目前防火墙仍然是网络安全防护中最常用的技术。防火墙是一种特殊的网络安全部件，通常是包含软件部分和硬件部分的一个或多个系统的组合。防火墙一般设置在被保护网络和其他网络的边界之间形成一道安全屏障，在网络中的位置一般如图 1-6 所示。通过合理设置防火墙的安全区域、安全策略、会话表等，可以允许、拒绝或重新定向经过防火墙的数据流，避免网络攻击干扰系统运行或窃取敏感数据，保障网络内部的安全，同时防火墙本身具有较强的抗攻击能力，并且只有授权的管理员方可对其进行管理控制，所以可以说防火墙是网络信息系统的第一道防线。

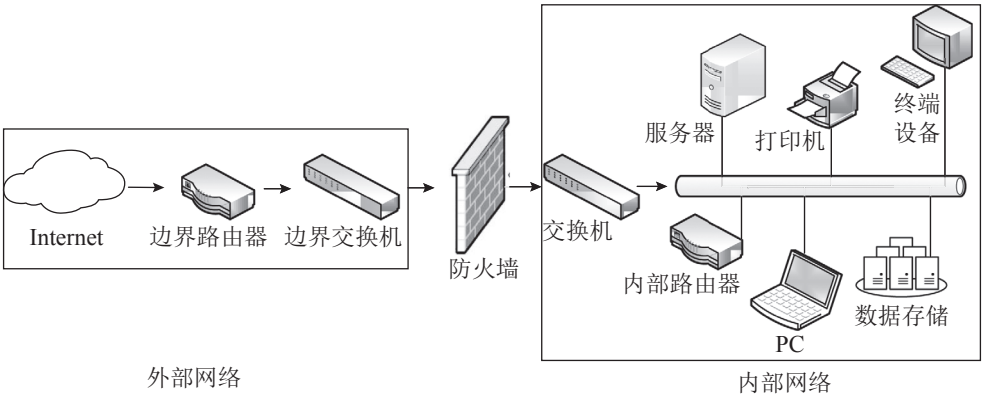


图 1-6　防火墙在网络中的位置

1）防火墙的主要功能

防火墙实现的技术包括会话管理、包过滤、安全区域管理、安全策略、网络地址转换、DoS 防御、状态检测、应用服务代理、协议分析等，对其概括的主要功能如下。

（1）网络隔离：通过利用防火墙将网络划分成内网和外网两个部分，实现对内网重点网段的隔离，从而限制来自外部网络未经授权的访问，降低外网的探测能力，以及阻止局部重点或敏感网络安全问题对内网造成影响。同时，隐私数据的安全是内网非常关心的问题，使用防火墙可以阻塞内网中的那些隐私数据的泄露，如显示了主机的所有用户信息的 Finger、DNS 服务信息等。防火墙同样可以通过关闭不使用的端口、禁止来自特殊站点的访问、网络地址转换等达到网络隔离的效果。

（2）强化网络安全策略：防火墙设备在网络中所处的位置，正好为信息系统提供了一个多种安全技术的集成支撑平台。通过以防火墙为中心的安全方案配置，可以将多种安全软件，如口令检查、加密、身份认证、安全审计等集中部署在防火墙上。与在各个主机上分散部署安全软件的方案相比，防火墙的集中安全管理更经济、更有效，简化了系统管理人员的操作，从而强化了网络安全策略的配置实行。

（3）记录网络活动和监控审计：由于防火墙处于内网与外网的边界之间，即涉及内部网络和外部网络之间的所有访问、所有信息传输都需要经过防火墙，所以防火墙可以记录这些行为并做出日志记录，同时能够把数据进行汇总分析，从而得出网络访问的统计性数据，如果统计的数据里面含有可疑性的动作，防火墙能进行适当的报警，并显示网络可能受到的相关的监测和攻击方面的详细信息。另外，防火墙还可以通过统计数据提供某个网络的使用情况和误用情况，这不仅可以让网络管理员清楚防火墙是否能够抵挡对内网的探测和攻击，是否需要更改防火墙的控制策略；还可以为该网络使用的需求分析和可能存在的威胁分析提供有价值的参考数据。

（4）网络安全的保障：一个防火墙作为网络中的阻塞点和控制点能极大地提高一个内部网络的安全性，因为防火墙具有内容控制、服务控制、方向控制、行为控制、用户控制等功能，能够根据数据内容进行过滤控制，能够控制可访问的服务类型、控制服务和报文等信息流通过的方向、控制访问服务的方式、控制访问网络的用户等，保障网络环境变得更安全。

2）防火墙的分类

防火墙的类别多种多样，其根据不同的分类依据的分类方式如下。

（1）按防火墙的软硬件形式可以分为：软件防火墙、硬件防火墙、芯片级防火墙。

（2）按防火墙的工作原理可以分为：包过滤防火墙、电路级网关、应用代理防火墙、状态检查防火墙。

（3）按防火墙具体实现的体系可以分为：多重宿主主机体系、筛选路由器体系、屏蔽主机体系、屏蔽子网体系和其他实现体系结构的防火墙。

（4）按防火墙应用的部署位置可以分为：边界防火墙、个人防火墙、分布式防火墙。

（5）按防火墙保护的对象可以分为：单机防火墙和网络防火墙。

3）防火墙的缺陷

由于网络的开放共享性，防火墙也存在一定的缺陷，例如，防火墙一般无法防范数据驱动型攻击，并且对绕过它的攻击行为也无法阻止。此外，防火墙无法处理病毒，不能防止感染了病毒的软件或文件的传输，只能依靠安装反病毒软件来应对。基于控制策略和过滤技术的影响，防火墙所带来的网络安全性的提高往往以牺牲网络服务的灵活性、多样性和开放性为代价。

2. IDS 技术

入侵检测系统（Intrusion Detection System）是一种对网络中传输的信息流以及主机系统的输入输出流进行监视，在发现可疑信息传输时或各种攻击企图、攻击行为时发出警报的网络安全设备。与其他网络安全设备的不同之处便在于，IDS 是一种积极主动的

安全防护技术。提供对内部攻击、外部攻击和误操作的实时防护，在计算机网络和系统受到危害之前进行报警、拦截和响应。做一个形象的比喻：假如防火墙是一幢大楼的门锁，那么 IDS 就是这幢大楼里的监控系统。一旦有人试图进入大楼，或内部人员有越界行为，监视系统都能发现这些情况并进行相应的警告。

1）IDS 的功能

（1）具有对网络流量的监测与分析功能，监测用户在网络中的活动，并分析用户在信息系统中的活动状态。

（2）对系统构造和弱点进行审计，对未发现的系统漏洞特征进行预报警功能。

（3）对操作系统日志的审计追踪管理，并识别用户违反安全策略的行为活动。

（4）评估系统关键资源和数据文件的完整性功能，通过检查关键数据文件的完整性，识别并报告数据文件的改动情况。

（5）根据已知攻击的特征模式识别攻击行为，并向控制台报警，为防御提供依据。

（6）具有特征库的在线升级功能以及自定义特征的响应功能。能够在线更新入侵特征库；并根据用户自定义，经过系统过滤，对警报事件及时响应。

2）IDS 的分类

（1）根据入侵检测系统的模型和部署方式的不同，IDS 分为基于主机的 IDS、基于网络的 IDS，以及由两者取长补短发展而来的分布式 IDS。

（2）根据入侵检测系统实现的方式不同，IDS 可以分为基于统计分析的 IDS、基于模式识别的 IDS、基于规则检测的 IDS、基于状态检查的 IDS 和基于启发式的 IDS。

（3）根据入侵检测系统检测方法的不同，IDS 可以分为异常检测 IDS 和误用检测 IDS。

3）IDS 的缺陷

IDS 技术普遍采用预设置式、特征分析式的工作原理，所以检测规则的更新总是落后于攻击手段的更新，无法完全弥补主动防御系统的缺陷和漏洞。对于高负载的网络或主机系统，IDS 容易造成较大的漏报警率，且报警信息只有通过人为的补充才有意义，缺乏数据来源准确定位能力和有效的响应处理机制。对于未知攻击的检测能力不足，例如基于误用检测方法的 IDS 很难检测到未知的攻击行为；而基于异常检测方法的 IDS 只能在一定程度上检测到新的攻击行为，但一般很难给新的攻击定性。

IDS 的缺陷，反而成就了 IPS（Intrusion Prevention System，入侵防御系统）的发展，IPS 技术可以深度感知并检测流经的数据流量，对恶意报文进行丢弃以阻断攻击，对滥用报文进行限流以保护网络带宽资源，对网络进行多层、深层、主动的防护以有效保证网络安全。简单地理解，IPS 等于防火墙加上入侵检测系统，但并不代表 IPS 可以替代防火墙或 IDS。防火墙在基于 TCP/IP 协议的过滤方面表现非常出色，IDS 提供的全面审计资料对于攻击还原、入侵取证、异常事件识别、网络故障排除等都有很重要的作用。

3. 虚拟专用网技术

虚拟专用网（Virtual Private Network，VPN）是指在公共网络上，通过隧道技术建立一个临时的、安全的网络，为用户提供的与专用网络具有相同通信功能的安全数据通

道。“虚拟”是相对传统的物理专用网络而言，VPN 是利用 Internet 等公共网络资源和设备建立的一条逻辑上专用数据通道。“专用网络”是指虚拟出来的网络并非任何连接在公共网络上的用户都能使用，只有经过特定企业或个人授权的用户才可以使用。能够使运行在 VPN 之上的商业应用享有几乎和专用网络同样的安全性、可靠性、优先级别和可管理性。虚拟专用网的应用场景如图 1-7 所示。

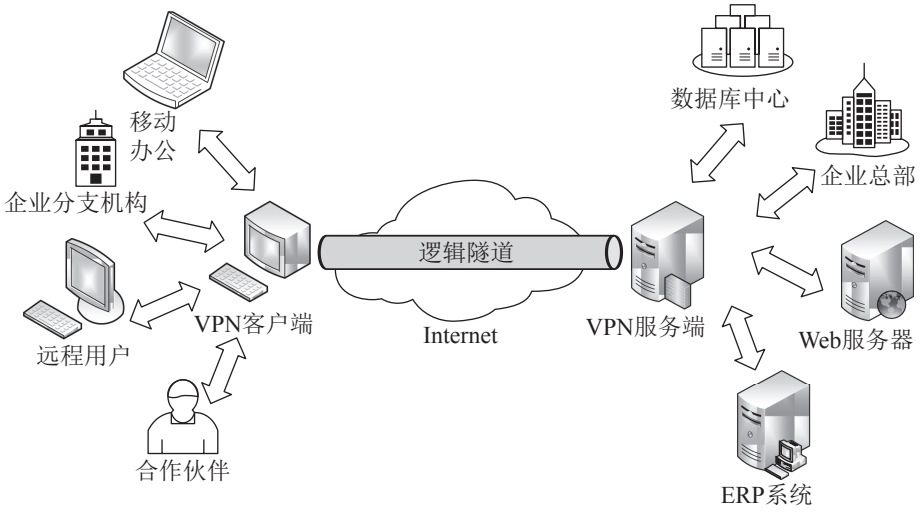


图 1-7　虚拟专用网的应用场景

1）VPN 技术特点

（1）安全性高：VPN 通过建立一个逻辑的、点对点的隧道实现在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，并利用加密技术对经过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证了数据的私有性和安全性。

（2）成本较低：与传统的广域网相比，虚拟专用网能够降低远程用户的连接成本，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴。此外，虚拟专用网固定的通信成本有助于企业更好地了解自己的运营开支。虚拟专用网还提供低成本的全球网络机会。

（3）服务质量保证：VPN 可以为企业提供不同等级的服务质量保证。如对于移动办公用户，VPN 网络可以提供广泛的连接和覆盖性；而对于拥有众多分支机构的企业，交互式专线 VPN 网络能提供良好的稳定性。在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。

（4）可扩展性和灵活性：由于 VPN 为逻辑上的网络，物理网络中增加或修改节点，不影响 VPN 的部署，虚拟专用网还可以支持通过各种网络的任何类型数据流，支持多种类型的传输媒介，可以同时满足传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

（5）可管理性：不论分公司或远程访问用户都只须通过一个公用网络端口或 Internet 路径即可进入企业网络获得所需的带宽，并且网络管理的主要工作将由公用网

承担。所以从用户角度和运营商角度都可以方便地进行 VPN 的管理维护。

2）VPN 关键安全技术

VPN 采用的关键安全技术包括隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术。

（1）隧道技术：是 VPN 的基本技术之一，类似于点对点通信技术。隧道（Tunnel）是一个虚拟的点对点的连接，一个 Tunnel 提供了一条使封装的数据报文能够传输的通路，并且在一个 Tunnel 的两端可以分别对数据报文进行封装及解封装。隧道技术其实是一种封装技术，它利用一种网络协议来传输另一种网络协议，即利用一种网络传输协议，将其他协议产生的数据报文封装在它自己的报文中，然后利用公网的建立的隧道传输，在隧道另一端进行解封装，从而完成数据的安全可靠性传输。隧道是由隧道协议建立的，常见的隧道协议有 PPTP、L2TP、L2F、VTP、IPSec 协议等。

（2）加解密技术：通过加密技术保证信息的机密性、完整性、鉴别性和不可否认性，使用相应的密钥解密后得到明文，使信息只对允许可读的接收者获取，以防止私有化信息在网络中被拦截和窃取。信息的加解密技术是数据通信中一项比较成熟的技术，VPN 可直接利用现有技术，国内的 VPN 设备通常采用国产加密算法进行加 / 解密。

（3）密钥管理技术：密钥管理过程中涉及密钥生成、密钥分发、验证密钥、更新密钥、密钥存储、密钥销毁等一系列过程。密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取，现行密钥管理技术主要分为 SKIP 与 ISAKMP/OAKLEY 两种。SKIP 主要是利用 Diffie-Hellman 规则在网络上传输密钥；后者为密钥安全分发协议，在一个 ISAKMP/OAKLEY 交换过程中，双方对验证和数据安全方式达成一致，进行相互验证，然后生成一个用于随后的数据加密的共享密钥。

（4）使用者与设备身份认证技术：最常用的身份认证方式包括使用用户名与密码或卡片式认证等方式，也可以同时采用多种方式进行认证。这些方法主要用于移动办公的用户远程接入的情况。通过对用户的身份进行认证，确保接入内部网络的用户是合法用户，而非恶意用户。

4. 网络安全扫描技术

网络安全扫描技术是指通过使用特定的安全扫描器，对系统风险进行评估，寻找可能对系统造成损害的安全漏洞，从而降低系统的安全风险的一种网络安全技术。利用安全扫描技术，可以对局域网络、操作系统、Web 网站、信息系统服务及防火墙等进行扫描，系统管理员根据扫描结果可以及时了解在运行的网络系统中存在的不安全的配置及网络服务，如操作系统上可能存在的导致遭受网络攻击的安全漏洞、主机系统中被安装了恶意程序、防火墙的错误配置等，通过安全扫描技术及时发现这些安全问题，可以有效避免遭受攻击行为，做到防患于未然。

网络安全扫描技术主要有端口扫描技术、弱口令扫描技术、操作系统探测以及漏洞扫描技术等。

（1）端口扫描技术：就是逐个对一段端口或指定的端口进行扫描，一个端口就是一个通信通道，也就是一个潜在的入侵通道。端口扫描的原理是使用 TCP/IP，向远程目标主机的某一端口发送探测数据包，并记录目标主机的响应状态，从而判断端口的开关

状态，通过查看记录就可以知道目标主机上都安装了哪些服务。通过端口扫描，可以搜集到很多关于目标主机的各种很有参考价值的信息。

（2）弱口令扫描技术：弱口令是指易于猜测、破解或长期不变更的密码，如“1111”等简单的口令、自己的姓名、生日等。口令检测是网络安全扫描工具的一部分，它要做的就是判断用户口令是否为弱口令。因为系统中弱口令现象是普遍存在的，攻击者通过暴力破解就可以登录目标主机。所以弱口令扫描是网络安全扫描的重要环节。

（3）操作系统探测：通过采取一定的技术手段，通过网络远程探测目标主机上安装的操作系统类型及其版本号的方法。在确定了操作系统的类型和具体版本号后，可以为进一步发现安全漏洞和渗透攻击提供条件。协议栈指纹分析（Stack Fingerprinting）是一种主流的操作系统类型探测手段，其实现原理是通过网络连接获取唯一标识某一操作系统的一组特征信息，将探测或网络嗅探所得到的指纹特征信息在数据库中进行比对，就可以精确地确定其操作系统的类型和版本号等。操作系统探测技术还有获取标识信息探测技术、ICMP 响应分析探测技术等。

（4）漏洞扫描技术：是指基于漏洞数据库，对指定的目标系统的安全脆弱性进行扫描，进而发现系统漏洞的一种安全检测技术。漏洞扫描技术是建立在端口扫描技术的基础之上的，在获得目标主机 TCP/IP 端口和其对应的网络访问服务的相关信息后，与提供的漏洞库进行匹配，如果满足匹配条件，则视为漏洞存在。漏洞扫描技术和防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。

5. 访问控制技术

访问控制是信息安全中重要的一个技术领域。所谓访问控制就是通过某种方法手段对访问行为进行允许或限制，从而对系统中重要资源的访问进行有效的控制，防止攻击者入侵或者合法用户的不慎操作对其造成的破坏。访问控制定义了在信息系统中，主体对于客体能够进行哪些操作和动作。这里的主体是指提出访问资源请求的发起者，包括用户、账户、程序、进程等；而客体是指被访问资源的实体，所有可以被操作的信息、资源、对象都可以是客体；操作和动作则是客体对主体的授权行为，包括读取、写入、删除、执行等。访问控制是系统保密性、完整性、可用性和合法使用性的重要基础，是网络安全防范和资源保护的关键策略。

1）访问控制的主要功能

访问控制的主要目的是限制主体对客体的访问，从而保证系统数据资源在合法用户授权范围内有效的使用和管理，防止非法的主体使用受保护的网络资源，或防止合法用户对受保护的网络资源进行非授权的访问。访问控制需要对主体身份合法性进行验证，同时利用控制策略对访问行为进行控制和管理，还需要对越权操作进行监控审计。因此，访问控制的内容包括认证、控制策略和安全审计。

（1）认证：主体与客体之间相互的认证识别。

（2）控制策略：通过合理设定控制规则集合，确保主体对客体在授权范围内的合法使用。

（3）安全审计：根据访问权限，对主体有关活动或行为进行系统的、独立的检查验证，并做出相应评价与审计。

2）访问控制策略

访问控制主要有自主访问控制、强制访问控制和基于角色的访问控制3种典型类型。

（1）自主访问控制（Discretionary Access Control）：由客体的拥有者对客体进行管理，决定是否将自己的客体访问权或部分访问权授予其他主体。也就是说，在自主访问控制下，用户可以按自己的意愿，有选择地赋予其他用户访问特定资源的权限，可以设置文件和共享资源，对自己创建的相关资源，可以授权给指定用户或撤销指定用户访问权限。这种机制的好处是权限管理灵活，缺点是权限可以不受控制的传播，因此容易成为攻击者的目标。Linux，UNIX 和 Windows 等操作系统的文件管理中都提供了对自主访问控制模型 DAC 的支持。

（2）强制访问控制（Mandatory Access Control）：一种由操作系统约束的访问控制，目的是限制主体或发起者访问或对对象或目标执行某种操作的能力。强制访问控制中不允许客体的拥有者随意修改或授予客体相应的权限，而是通过强制的方式为每个客体分别授予权限。而授予权限主要是依据主体和客体的安全级别，以及具体的策略来进行。强制访问控制的优点是管理集中，适用于对安全性要求高的应用环境，另外，强制访问控制通过信息的单向流动来防止信息扩散，可以有效抵御对系统保密性的攻击。强制访问控制的缺点在于安全级别间强制性太强，权限的变更非常不方便。常见的强制访问控制模型有 BLP 模型、Biba 模型。

（3）基于角色的访问控制（Role-based Access Control）：在用户集合与权限集合之间建立一个角色集合，每种角色对应一组相应的权限。一旦用户被分配了角色后，该用户就拥有此角色的所有操作权限。根据角色授权，不必在每次创建用户时都进行分配权限的操作，只要分配用户相应的角色即可，而且由于角色 / 权限之间的变更比角色 / 用户关系之间的变更相对要少得多，减小了授权管理的复杂性，降低了系统的开销。常见的基于角色访问控制模型有 RBAC0 模型、RBAC1 模型等。

6. 病毒防护技术

在网络环境中，防范病毒问题显得尤其重要。计算机病毒具有较强执行能力，通过寄生在其他可执行程序上，当程序执行时，与其争夺系统的控制权实施破坏，同时它还具有复制能力，感染性强，特别是网络环境下，传播性极强。计算机病毒的潜伏周期较长并且病毒对系统的攻击是主动触发的。系统一旦感染病毒会导致数据信息很大程度被破坏、服务终止、系统崩溃，甚至造成重大经济损失。

病毒防护技术工具是系统安全的必备组件。它可以加强资源和服务的合法保护，加密数据信息的安全，全面提升系统的防御能力，同时能够辨识已知的恶意文件代码，并且在造成破坏前阻止它们，可以对系统进行全方位的监测、防护，并及时采取行动来预防计算机病毒入侵，将病毒带来的灾害和损失降到最低。常见的病毒防护方法包括对系统文件和目录安全性扫描，系统实时在线扫描、安装防火墙、安装杀毒软件、重要数据信息备份、养成良好的计算机使用习惯等。

目前常用的计算机病毒防护技术主要包括病毒预防技术、病毒检测技术及病毒清除技术。

（1）病毒预防技术。通过一定的技术手段防止计算机病毒进入系统内存或磁盘对系统正常运行造成干扰和破坏。目前主要有静态判定技术和动态判定技术两种。具体来说，就是根据病毒的规则进行分类处理，而后在程序运作中凡有类似的规则出现则认定是计算机病毒。病毒预防技术手段包括磁盘引导区保护、加密可执行程序、读写控制技术、系统监控技术等。

（2）病毒检测技术。常用的计算机病毒检测技术：①搜索法：对被检测的对象进行扫描搜索，如果在对象内部发现了某种病毒体含有的特定字符串，就表明发现了该病毒。②特征对比法：将程序的关键字、程序段内容、大小、日期等综合为一个特征码，追踪记录每个程序的特征码是否遭更改以判断是否被感染。③软件仿真扫描法：对于在每次传染时都将自身以不同的随机数加密隐藏的病毒，传统搜索法根本就无法找到它，通过软件仿真 CPU 伪执行病毒程序，在其解密执行时再加以扫描发现该病毒。④分析法：利用反汇编工具和 DEBUG 等调试工具对计算机病毒执行前后的 CPU 指令进行静态分析和动态分析可发现新病毒，提取特征字串，制定防杀措施方案。

（3）病毒清除技术。这是计算机病毒检测技术发展的必然结果，病毒清除技术是使用最广泛的安全技术解决方案，它可以对病毒、木马等已知的对计算机有危害的程序代码进行清除，主要使用的技术包括脱壳技术、自我保护技术、文件修复技术、实时升级技术、主动防御技术、未知病毒启发技术、人工智能技术等。杀毒软件通常集成病毒扫描和清除、数据恢复、网络监控识别、主动防御等功能，是网络安全防护中的重要组成部分。目前常见的杀毒软件有金山毒霸、Bitdefender、360 安全卫士、ESET、Norton、腾讯电脑管家、Kaspersky 等。

1.4 网络安全保障

保障网络安全的重点工作就是网络安全防护体系和网络安全模型的建立与实现，前者是保障网络安全的直接手段，可以通过一系列的安全防护技术实现；而后者是对动态网络安全过程的抽象描述，通过描述系统行为与安全实现过程的构成因素以及这些因素之间的相互关系，然后以建模的方式构建安全模型，提高对成功实现关键安全需求的理解层次，最后就可以准确地给出解决安全问题的方法与过程。通常为了实现网络安全保障的目的，还会采取网络安全管理、网络安全策略、网络安全等级保护等措施。

1.4.1 网络安全模型

通信主体之间想要在网络中传递信息，首先需要建立一条逻辑通道，确定从发送端到接收端的路由，然后选择该路由上使用的通信协议，如 TCP/IP 等。为了在开放式的网络环境中能够保证信息被安全地传输，不被竞争对手或攻击者等窃取访问，则需要网络安全模型对信息传递过程提供安全机制和安全服务等动态的防护。

网络安全基本模型的结构如图 1-8 所示，其中主要包括两个基本部分：一是对被传送的信息通过安全技术进行转换，包括对信息的加密和认证等。对信息加密以便达到信

息的保密性，附加一些特征码以便进行发送者身份验证等；二是两个通信主体之间共享的某些秘密信息，对网络的其他用户是保密的，如加密密钥。为了使信息安全传输，通常还需要一个可信任的第三方，其作用是负责向通信双方分发秘密信息或者在通信主体双方发生争议时进行仲裁。

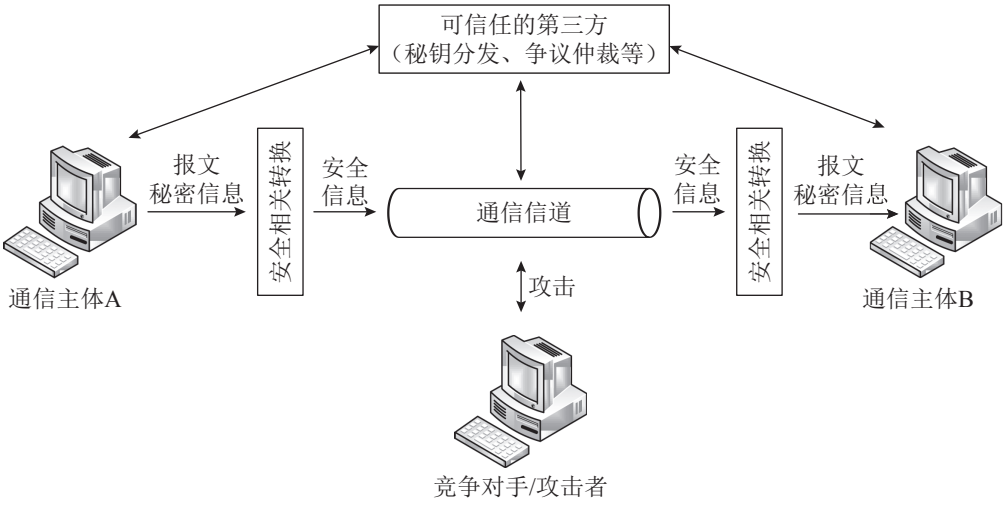


图 1-8　网络安全基本模型的结构

网络安全模型在系统安全建设中起着重要的指导作用，它能够精确而形象地描述信息系统的安全属性，准确地描述安全的重要方面与系统行为的关系，并且能够从中开发出一套安全性评估准则和关键的描述变量。安全模型的检测作用能够根据系统行为动态响应和加强系统安全防护，通过不断地检测和监控系统，来发现新的威胁和弱点，并通过循环反馈来及时做出有效的响应。当攻击者试图渗透进入系统时，安全模型的检测功能就发挥作用。同时安全模型的防护作用通过修复系统漏洞、配置安全策略预防安全事件的发生，通过定期检查发现可能存在的系统脆弱性；通过教育等手段防止用户和操作员对系统造成意外威胁；通过访问控制、监视等手段防止网络攻击。通常采用的防护手段包括数据加密、身份识别认证、访问控制、网络隔离、虚拟专用网技术、防火墙、安全扫描和数据备份与恢复等。网络安全模型检测作用与防护作用形成互补，维持整个网络的正常运行。常见的网络安全模型有 PPDR 安全模型、PDRR 安全模型、WPDRRC 安全模型等。

1. PPDR 安全模型

PPDR 安全模型由安全策略（Policy）、保护（Protection）、检测（Detection）和响应（Response）4 个主要部分组成。PPDR 安全模型结构如图 1-9 所示，模型提出了新的安全概念，即安全不能只依靠单纯的静态防护，也不能仅仅依靠单纯的安全技术手段来实现。模型将安全描述为对信息系统进行以风险分析、安全策略、系统实施、漏洞监视、实时响应为一个整体集合的安全防护过程，其中，安全策略描述系统的安全需求，以及如何组织各种安全机制实现系统的安全需求，是整个安全模型中的核心。

PPDR 安全模型基于的思想是在整体安全策略的控制和指导下，利用检测工具了解

和评估系统的安全状态，如漏洞评估、入侵检测等。通过对系统进行安全检测为安全策略的快速响应提供了依据，当发现系统有异常时，安全策略发起响应并综合运用防护工具将系统调整到安全风险最低的状态，从而达到保护系统安全的目的。PPDR 安全模型将安全策略、防护、检测和响应组成一个完整动态的安全循环，使得其在整体安全策略的指导下保证信息系统的安全。

（1）安全策略（Policy）：PPDR 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。安全策略为系统安全提供管理方向和支持手段，包括访问控制策略、加密通信策略、身份认证策略、备份与恢复策略等。建立安全策略体系是实现安全的首要工作，也是实现安全技术管理与规范的第一步，策略体系的建立包括安全策略的制定、评估与执行等。

（2）保护（Protection）：根据系统可能出现的安全问题而采取的预防措施，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。采用的防护技术通常包括防火墙、加密技术、身份认证、虚拟专用网技术等。保护的主要目标可以分为系统安全保护、网络安全保护和信息安全保护。

（3）检测（Detection）：是模型安全策略动态响应和加强防护的依据，是模型的第 2 个安全屏障。通过利用安全检测工具，不断地监视、分析、审计网络和系统的活动来发现新的威胁和弱点，了解判断网络系统的安全状态，使安全防护从被动防护演进到主动防御。检测是整个模型动态性的体现，通过循环反馈来及时对检测结果作出有效的响应。检测的对象主要包括：系统本身存在的脆弱性、信息是否发生泄露、系统是否遭到入侵等。在 PPDR 安全模型中，保护和检测之间具有互补关系。

（4）响应（Response）：响应就是在检测到安全漏洞或入侵攻击时，及时采取有效的处理措施，将网络系统的安全性调整到风险最低的状态。其主要方法包括关闭服务、跟踪、反击、消除影响等。通过建立响应机制和紧急响应方案，提高模型的安全防护能力。

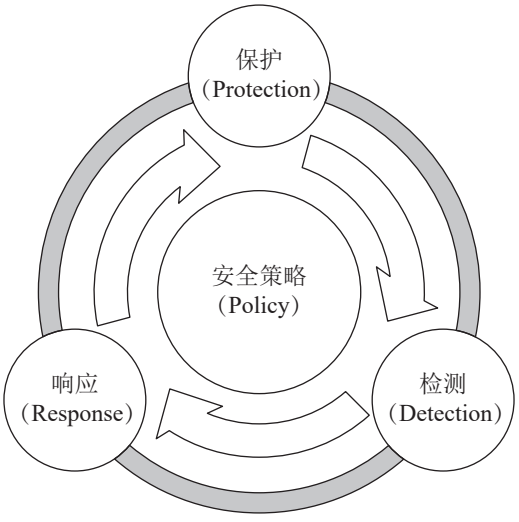


图 1-9　PPDR 安全模型结构

2. PDRR 安全模型

PDRR 安全模型是保护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）的有机结合，模型结构如图 1-10 所示。其中，防护、检测、响应机制与 PPDR 安全模型基本相同。恢复（Recovery）是指系统遭受攻击事件之后，把系统恢复到原来的状态或者比原来更安全的状态。恢复的过程中需要解决攻击所造成的影响评估、系统的重建以及采取恰当的技术措施抵御攻击，恢复的内容通常有数据备份、数据修复、系统恢复等。

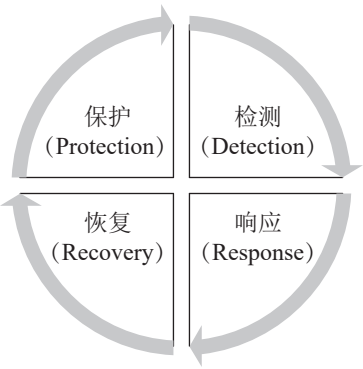


图 1-10　PDRR 安全模型结构

PDRR 安全模型改进了传统安全模型中只注重防护的单一安全防御思想，该模型强调的是故障自动恢复能力。在 PDRR 安全模型中，安全的概念已经从信息安全扩展到了信息保障，其内涵已经由传统的信息安全保密转变为主动安全防御。PDRR 安全模型把信息的安全保护作为基础，用检测手段来发现安全漏洞及时更正，同时采用应急响应措施对付各种攻击，在系统被入侵后采取相应的措施将系统恢复到正常状态，这样使信息的安全得到全方位的保障。PDRR 安全模型阐述了一个结论：安全的目标实际上就是尽可能地增加主动防御时间，尽量减少检测时间和响应时间，在遭受破坏后应尽快恢复以减少系统安全问题暴露时间。

3. WPDRRC 安全模型

WPDRRC 安全模型是由“国家高技术研究发展计划”信息安全专家组提出的适合中国国情的信息系统安全保障体系建设模型，该模型在 PDRR 安全模型的基础上增加了预警（Warning）和反击（Counterattack）两个环节。

（1）预警（Warning）：基于 IDS 技术、IPS 技术等，分析各种安全报警、日志信息，结合网络管理系统以及入侵防御系统实现对各种网络攻击事件的预警。

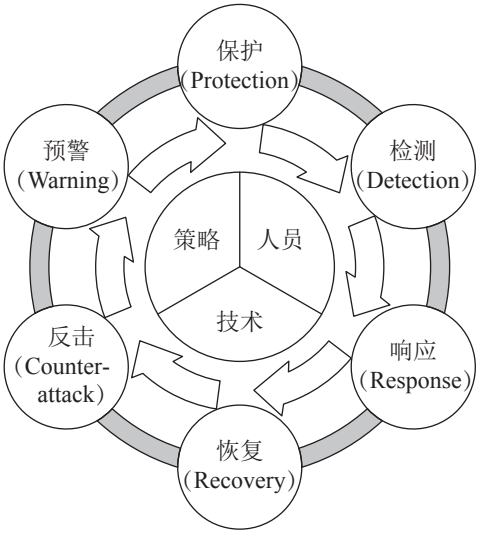


图 1-11　WPDRRC 安全模型结构

（2）反击（Counterattack）：采用溯源追踪技术对网络攻击进行追踪和画像，包括 IP 定位技术、ID 追踪术、域名注册信息溯源分析以及提取恶意样本特征进行同源分析等手段，还原出攻击路径，完成对攻击的溯源。通过这种方式，可以建立具备目的性的安全防护以及对安全威胁源的“反击”。

WPDRRC 安全模型结构如图 1-11 所示，WPDRRC 模型有 6 个环节和 3 大要素。6 个环节分别是预警、保护、检测、响应、恢复和反击，它们具有较强的时序性和动态性；3 大要素包括人员、策略和技术。人员是核心，策略是桥梁，技术是保证 WPDRRC 安全模型

全面地涵盖了各个安全因素，反映了各个安全组件之间的内在联系，并落实在模型 6 个环节的各个方面，将安全策略变为安全现实。

1.4.2 网络安全等级保护

网络安全等级保护是指对“网络”实施分等级保护、分等级监管，对网络中使用的网络安全产品实行按等级管理，对网络中发生的安全事件分等级响应和处置。这里的“网络”不仅仅包括由计算机或者其他相关信息终端设备组成的、按照一定的应用目标和规则对信息进行收集、存储、传输、交换、处理的系统，如基础信息网络、云计算平台系统、大数据应用平台、物联网、工业控制系统和采用移动互联网技术的系统等，还包含网络中其他设施、数据资源等重要保护对象。

网络安全等级保护制度其核心内容是对信息系统特别是对业务应用系统安全分等级、按标准进行建设、管理和监督。以构建先进高效的安全运营管理为中心，结合安全区域边界、安全计算环境、安全通信网络三重防护，然后形成以安全技术体系、安全管理体系、安全运营体系的整体的安全防御体系，保障重要信息资源和重要信息系统的安全。具体的等级保护制度方式是将风险评估、安全监测、通报预警、事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等重点措施全部纳入等级保护制度并实施；将网络基础设施、信息系统、网站、数据资源、云计算、物联网、移动互联网、工控系统、公众服务平台、智能设备等全部纳入等级保护和安全监管；将互联网企业的网络、系统、大数据等纳入等级保护管理。

网络安全等级保护制度是我国网络安全领域的基本国策、基本制度和基本方法，也是一套完整和完善的网络安全管理体系，贯穿网络信息系统的设计、开发、实现、运维、废弃等系统工程的整个生命周期。根据网络信息系统在国家安全、经济安全、社会稳定和保护公共利益等方面的重要程度，结合系统面临的风险、系统的安全保护要求和成本开销等因素，将其划分成不同的安全保护等级，采取相应的安全保护措施，以保障信息和信息系统的安全。

1. 网络安全等级保护的级别

网络安全等级保护总共分为五级，五级防护水平中第一级最低，第五级最高，具体级别如图 1-12 所示。

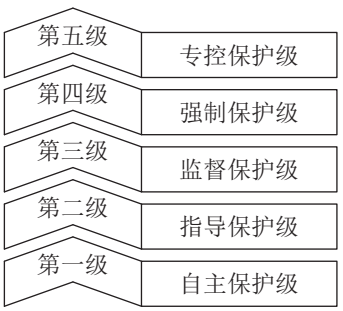


图 1-12　网络安全等级保护的级别

1）自主保护级

适用的场景是当信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。自主保护级能够防护使用较少资源威胁发起的攻击、一般的自然灾害，以及其他相当危害程度的威胁所造成的关键资源损害，并且在自身遭到损害后，能够恢复部分功能。第一级等级保护适用于小型私营、个体企业、中小学、乡镇所属信息系统、县级单位中一般的信息系统。

2）指导保护级

适用的场景是当信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。指导保护级能够防护外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。第二级等级保护适用于县级某些单位中的重要信息系统、地市级以上国家机关、企事业单位内部的信息系统。

3）监督保护级

适用的场景是当信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。监督保护级能够在统一安全策略下防护来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。第三级等级保护适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。

4）强制保护级

适用的场景是当信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。强制保护级能够在统一安全策略下防护来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能。第四级等级保护适用于国家重要领域、重要部门中的特别重要系统以及核心系统，如电力、电信、广电、铁路等重要部门的核心系统。

5）专控保护级

适用的场景是当信息系统受到破坏后，会对国家安全造成特别严重损害。专控保护级能够在统一安全策略下，在实施专用的安全保护的基础上，通过可验证设计增强系统的安全性，使其具有抗渗透能力，使数据信息免遭非授权的泄露和破坏，保证最高安全的系统服务。第五级等级保护适用于国家重要领域、重要部门中的极端重要系统。

2. 网络安全等级保护 2.0

2019 年 12 月 1 日正式实施网络安全等级保护 2.0。相较于等级保护 1.0 主要强调物理主机、应用、数据、传输等的安全制度，2.0 版本更加注重全方位主动防御、动态防御、整体防控和精准防护，在技术标准上增加了对云计算、移动互联、物联网、工业控制和大数据等新技术新应用的全覆盖，构成了“安全通用要求 + 新型应用安全扩展要求”要求内容，在聚焦于等级保护的基本要求时，更多用技术思维解读标准。等级保护 2.0 的基本要求、测评要求和安全设计技术要求框架结构更加统一，即形成了安全管理中心支持下的三重防护结构框架。新标准还强化了可信计算技术使用的要求，把可信验

证列入各个级别并逐级提出各个环节的主要可信验证要求。

等级保护 2.0 标准相比于 1.0 的主要变化如下。

（1）名称的变化：等级保护 2.0 将原来的名称《信息安全技术 信息系统安全等级保护基本要求》改为《信息安全技术 网络安全等级保护基本要求》。

（2）对象的变化：等级保护 1.0 的定级对象是信息系统，而等级保护 2.0 的定级对象更为广泛，包含信息系统、基础网络设施、云计算平台、大数据平台、物联网系统、工业控制系统、采用移动互联技术的网络等。

（3）安全要求的变化：基本要求的内容由安全要求变革为安全通用要求与安全扩展要求，各方面更加突出可信计算技术的应用，形成“一个中心，三重防护”的防御体系。等级保护 2.0 针对共性安全保护需求提出安全通用要求，如安全物理环境、安全通信网络、安全管理制度等。针对云计算、物联网、移动互联、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。

（4）内容变化：从等级保护 1.0 的定级、备案、建设整改、等级测评和监督检查 5 个规定动作，变更为 5 个规定动作加上新的安全要求，增加了风险评估、安全监测、通报预警、案 / 事件调查、数据防护、灾难备份、应急处置等。

（5）增加了云计算安全扩展要求：针对云计算的特点提出特殊保护要求，包括基础设施的位置、虚拟化安全保护、镜像和快照保护、云服务商选择和云计算环境管理等方面。

（6）增加了移动互联网安全扩展要求：针对移动互联的特点提出特殊保护要求，包括无线接入点的物理位置、移动终端管控、移动应用管控、移动应用软件采购、移动应用软件开发等方面。

（7）增加了物联网安全扩展要求：针对物联网的特点提出特殊保护要求，包括感知节点的物理防护、感知节点设备安全、感知网关节点设备安全、感知节点的管理、数据融合处理等方面。

（8）增加了工业控制系统安全扩展要求：针对工业控制系统的特点提出特殊保护要求，包括室外控制设备防护、工业控制系统网络架构安全、拨号使用控制、无线使用控制、控制设备安全等方面。

（9）增加了应用场景的说明：增加描述等级保护安全框架和关键技术、云计算应用场景、移动互联应用场景、物联网应用场景、工业控制系统应用场景和大数据应用场景。

3. 等级保护的重要意义

网络安全等级保护制度是国家网络安全工作的基本制度，是实现国家对重要网络、信息系统、数据资源实施重点保护的重大措施，是维护国家关键信息基础设施的重要手段。等级保护制度是集法律、政策、方针、方法论为一体的体系性的基本制度，将构建网络安全新的法律和政策体系、新的标准体系、新的技术支撑体系、新的人才队伍体系、新的教育训练体系和新的保障体系，帮助国家顺利部署达成等保新

时代。

网络安全等级保护的重要意义包括通过等级保护工作发现信息系统存在的安全隐患和不足，降低信息安全风险，提高信息系统的安全防护能力；满足国家相关法律法规和制度的要求，落实网络安全保护义务，合理规避风险；明确组织整改目标，改变网络中以往的单点防御模式，使得网络安全建设更加体系化；提高公民网络安全意识，树立计划安全防护思想；优化信息资源配置，重点保障基础信息网络和关系国家安全、经济安全、社会稳定等方面重要信息系统的安全。通过开展网络安全等级保护工作，能够切实提升网络安全防护能力，使信息系统和网络满足安全的基本要求，全方位助力网络安全发展。

1.5 小结

（1）网络安全就是网络环境下的信息安全。主要是保障数据和通信的安全，防止未授权的用户访问信息以及试图破坏与修改信息。

（2）网络安全的属性包括保密性、完整性、可用性、可靠性、可控性、可审查性和不可抵赖性。

（3）广义的网络安全是指网络系统中的软件、硬件与信息资源的安全性受到保护。它包括系统连续、可靠、正常地运行，网络服务不中断，系统的信息不因偶然的或恶意的原因而遭到破坏、更改和泄露。

（4）网络安全面临的威胁有系统自身的脆弱性、安全漏洞、管理的欠缺等原因提供给黑客入侵条件；恶意代码如病毒、蠕虫、木马、恶意脚本、系统后门、Rootkits 等；以及信息泄露、信息窃取和篡改、非授权访问、拒绝服务攻击、身份假冒、信息安全法律法规不完善等。

（5）网络攻击的步骤分为攻击准备阶段、攻击实施阶段、攻击善后阶段，具体包括信息搜集、隐藏攻击源、端口和漏洞扫描、获取目标访问权限、攻击实施、种植后门、痕迹清除等。

（6）网络安全防护的体系层次分为物理层安全防护、系统层安全防护、网络层安全防护、应用层安全防护和管理层安全防护。

（7）网络安全防护中，防御信息被窃取的安全措施是加密技术；防御传输消息被篡改的安全措施是完整性技术；防御信息被假冒的安全措施是认证技术；防御信息被抵赖的安全措施是数字签名技术。

（8）网络安全模型通过建模清楚地描述网络安全实现过程中涉及的因素以及这些因素之间的关系。

（9）网络安全等级保护指对国家秘密信息、法人和其他组织及公民的专有信息及公开信息和存储、传输、处理这些信息的网络系统分等级实行安全保护，对网络系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应处置。

1.6 习题

1. 在实际应用中是否遇到过网络安全问题？试分析造成安全问题的原因及对策。
2. 简述网络安全的发展历程。
3. 网络攻击中的病毒、蠕虫、木马以及后门之间存在怎样的区别与联系？
4. 基于访问控制技术的安全模型有哪些种类？分别适用于什么场景？
5. 简述系统层安全在计算机网络安全中的地位，并说明其包含的主要内容。
6. 谈谈网络安全体系设计遵循的基本原则。
7. 你认为的保障网络安全的技术措施还有哪些？