目录

目 录

目录

目 录

单元一　信息安全

问题导入

随着计算机和网络技术的发展和普及，社会的信息化程度越来越高，信息资源也得到更大程度的共享。但随着信息化发展而来的网络信息安全问题也暴露出来，如果不能解决好这个问题，必将阻碍信息化发展进程。计算机和网络的使用可以为人类造福，也可以给人类带来危害，关键在于使用人采取的道德态度、遵循的行为规范和约束。

信息安全是指信息产生、制作、传播、收集、处理、选取等信息使用过程中的信息资源安全。建立信息安全意识，了解信息安全相关技术，掌握常用的信息安全应用，是现代信息社会对高素质技术技能人才的基本要求。

学习要点

1. 建立信息安全意识，能识别常见的网络欺诈行为。

2. 了解信息安全的基本概念，包括信息安全基本要素、网络安全等级保护等内容。

3. 了解信息安全相关技术，了解信息安全面临的常见威胁和常用的安全防御技术。

4. 了解常用网络安全设备的功能和部署方式。

5. 了解网络信息安全保障的一般思路。

6. 掌握利用系统安全中心配置防火墙的方法。

7. 掌握利用系统安全中心配置病毒防护的方法。

8. 掌握常用的第三方信息安全工具的使用方法，并能解决常见的安全问题。

本单元包含信息安全意识、信息安全防御技术、信息安全应用等内容。

任务一 信息安全概述

任务描述

信息安全本身包括的范围很大，大到国家政治军事机密安全，小到防范政府企业机密的泄露、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，任何一个安全漏洞都可以威胁全局安全。

本任务介绍信息安全的概念、影响因素、等级保护、信息道德与相关法规等。

学习目标

1. 了解信息安全的概念和影响因素。
2. 了解信息安全面临的主要威胁。
3. 了解信息安全策略。
4. 了解信息安全等级保护的基本知识。
5. 了解使用计算机和网络应遵守的道德规范。
6. 了解国家对知识产权和软件使用的要求，以及信息安全的相关法律法规。

任务实现

一、信息安全的概念

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续正常地运行，信息服务不中断，最终实现业务连续性。

二、信息安全的影响因素

信息安全的影响因素因素很多，主要有以下几个方面。

（1）硬件及物理因素：指系统硬件及环境的安全性，如机房设施、计算机主体、存储系统、辅助设备、数据通信设施以及存储介质的安全性。

（2）软件因素：指系统软件及环境的安全性，软件的非法删改、复制与窃取都可能造成系统损失、泄密等情况。例如，计算机病毒就是以软件为手段侵入系统造成破坏。

（3）人为因素：指人为操作、管理的安全性，包括工作人员的素质、责任心，严密的行政管理制度、法律法规等。防范人为因素方面的安全威胁，即是防范人为主动因素直接对系统安全所造成的威胁。

（4）数据因素：指数据信息在存储和传递过程中的安全性。数据因素是计算机犯罪

的核心途径，也是信息安全的重点。

（5）其他因素：信息和数据传输通道在传输过程中产生的电磁波辐射，可能被检测或接受，造成信息泄露；同时空间电磁波也可能对系统产生电磁干扰，影响系统的正常运行。此外，一些不可抗力的自然因素，也可能对系统的安全造成威胁。

在研究信息安全问题时，更关注于恶意的犯罪导致的对信息安全的威胁，如信息窃取、信息截取、信息伪造、信息篡改、拒绝服务攻击、行为否认、非授权访问和传播病毒等。

案例 1-1

超 2 亿国内个人信息在国外暗网论坛兜售

2021 年 1 月，国外安全研究团队 Cyble 发现多个帖子正在出售与中国公民有关的个人数据，经分析来自微博、QQ 等多个社交媒体。本次发现的几个帖子中与中国公民有关的记录总数超过 2 亿。

案例 1-2

可怕的“U 盘小偷”

在某大学期末考试期间，在一门全校公共课的考场上，监考老师发现了多起考试舞弊事件，涉及好几个系别。让人吃惊的是，学生舞弊的纸条上有着本次考试的全部试题及标准答案，也就是说试卷泄密了。后来报警调查后发现某系学生利用“U 盘小偷”程序盗走了老师 U 盘上的资料，并传播获得一定的收益。而后该学生被判刑并被开除学籍。

案例 1-3

美国 NASDAQ 事故

1994 年 8 月 1 日，由于一只松鼠通过位于该证券交易系统网络主计算机附近的一条电话线挖洞，造成电源紧急控制系统损坏，NASDAQ 电子交易系统“日均超过 3 亿股”的股票市场暂停营业近 34 分钟。

三、信息安全的目标

国际标准化组织定义信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。研究信息安全就是为了实现以下目标。

（1）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

（2）保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

（3）完整性：保证数据的一致性，防止数据被非法用户篡改。

（4）可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

（5）不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中极其重要。

（6）可控制性：对信息的传播及内容具有控制能力。

（7）可审查性：对出现的网络安全问题提供调查的依据和手段。

四、信息安全的主要威胁

信息安全威胁主要来自人为因素。常见的信息安全威胁有以下几个方面。

1. 信息泄露

网络中的数据文件或进行网络通信时，如果不采取任何保密措施，数据文件或通信内容就有可能被他人看到，造成信息泄露。如果是未经系统授权而使用网络或计算机资源，这就是非授权访问。或者内部人员安全意识差而泄露信息，这是一种内部泄露行为。

案例 1-4

全国首例利用微信清粉软件获取用户信息案宣判

2021 年 3 月 3 日，江苏南通通州公安对全国首例利用微信清粉软件非法获取微信用户信息案进行宣判。被害用户扫描“清粉”二维码是为了给微信通讯录“瘦身”，不料个人信息泄露。8 名被告人则以刷阅读量、售卖微信群聊二维码等方式非法获利 200 多万元。

2. 信息窃取

非法用户通过数据窃听、流量分析等各种手段窃取系统中的信息资源和敏感信息。例如，对通信线路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。业务流分析则是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。

案例 1-5

央视曝 App 偷听隐私

2021 年 1 月，央视节目中专家用模拟“App 偷听测试程序”发送一个 2 秒的语音，当手松开后，录音仍在继续，并生成一条 120 秒的语音，证实了当测试程序置于前台运行时，偷听是可以实现的。此外经过对比实验，发现在测试程序退至后台或在手机锁屏时，录音依然可持续一段时间。

3. 冒名顶替

通过欺骗通信系统或用户，达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。侵入者通常通过一个合法的用户账号和密码来获得网络服务。

4. 篡改信息

非法用户对合法用户之间的通信信息进行修改，生成伪造数据，再发给接收者。信息篡改是一种严重的主动威胁，其危害程度有时比主动攻击更甚。这种主动威胁可以发生在通信线路上的任何地方，如电缆、微波线路、卫星信道、路由节点、主机或客户计算机系统等。

5. 行为否认

行为否认又称抵赖。在网络中，合法用户在电子商务等交易活动中不能否认其曾经发出的报文。在传统的交易活动中，可以通过用户的亲笔签名或印章来保证合同的有效性。在网络中，要保证发送者对报文的不可抵赖是通过数字签名实现的。

6. 授权侵犯

被授权以某一目的使用某些资源的人，却将此授权用于非授权的目的，也称为内部攻击。

7. 恶意攻击

恶意攻击是当前网络中存在的最大信息安全威胁之一。一般通过“黑客”程序持续扫描指定的网段，查找计算机系统漏洞，从而传播病毒、设置木马，以达到控制对方计算机的目的。当黑客控制很多计算机后，通常会采用拒绝服务和注入漏洞的方式对网络进行攻击。

案例 1-6

西山居旗下逍遥网遭攻击致数据泄露

2021 年 3 月，西山居游戏发公告称，西山居旗下产品屡遭不法分子 DDoS 攻击、服务器入侵，导致部分用户账号和加密后的非明文密码等信息外泄，官方建议第一时间修改安全等级偏低的短位密码。

五、信息安全策略

信息安全策略是指为保证提供一定级别的安全保护所必须遵守的规则。为了保证信息安全，需要从先进的技术、法律约束、严格的管理和安全教育等着手，制定完善的规则。

1. 先进的技术

先进的信息安全技术是信息安全的根本保证，用户对自身面临威胁的风险性进行评估，然后对所需要的安全服务种类进行确定，通过相应的安全机制，集成先进的安全技术，形成全方位的安全系统。

2. 法律约束

法律法规是信息安全的基石，必须建立与网络安全相关的法律法规，对网络犯罪行为实施约束。《中华人民共和国计算机信息系统安全保护条例》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国网络安全法》等都是有关信息安全的法律法规。

3. 严格的管理

信息安全管理是提高信息安全的有效手段，对于计算机网络使用机构、企业和事业单位而言，必须建立相应的网络安全管理办法和安全管理系统，加强对内部信息安全的管理，建立起合适的安全审计和跟踪体系，提高网络安全意识。

4. 安全教育

要建立网络安全管理系统，在提供技术、制定法律、加强管理的基础上，还应加强安全教育，提高用户的安全意识，对网络攻击与攻击检测、网络安全防范、安全漏洞与安全对策、信息安全保密、系统内部安全防范、病毒防范、数据备份与恢复等有一定的了解，及时发现潜在问题，尽早解决安全隐患。

六、信息安全等级保护

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行保护的一种工作，要求不同安全等级的信息系统应具有不同的安全保护能力。

《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下五级，一至五级等级逐级增高。

第一级，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。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级，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。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。

第三级，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。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。

第四级，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。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

《中华人民共和国网络安全法》规定：“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。”

七、使用计算机应遵守的道德规范

在高度信息化的今天，信息已深入到社会生活的各个方面，信息安全不仅是安全管理人员的责任，同时也需要全社会的共同维护。在享受信息化带来的优质服务的同时，也需要遵守相应的道德规范和法律法规。

国外一些计算机和网络组织制定了一系列规范，比较著名的是美国计算机伦理学会制定的 10 条戒律。这些规范是一个计算机用户在任何情况下都应该遵循的最基本的行为准则。具体内容如下。

（1）不应该用计算机去伤害别人。

（2）不应该干扰别人的计算机工作。

（3）不应该窥探别人的文件。

（4）不应该用计算机进行偷窃。

（5）不应该用计算机作伪证。

（6）不应该使用或复制没有付费的软件。

（7）不应该未经许可而使用别人的计算机资源。

（8）不应该盗用别人的智力成果。

（9）应该考虑所编写程序的社会后果。

（10）应该以深思熟虑和慎重的方式来使用计算机。

八、网络社会应遵守的道德规范

我国的信息产业，特别是互联网行业发展迅速，目前我国已拥有世界上人数最多的网民群。在这种情况下，互联网的道德规范建立显得尤其重要。

从 2002 年起，中国互联网协会先后颁布了一系列行业自律规范，主要包括：《中国互联网行业自律公约》《互联网新闻信息服务自律公约》《互联网站禁止传播淫秽、色情等不良信息自律规范》《中国互联网协会公共电子邮件服务规范》《搜索引擎服务商抵制违法和不良信息自律规范》《中国互联网网络版权自律公约》《文明上网自律公约》《抵制恶意软件自律公约》《博客服务自律公约》《中国互联网协会反垃圾短信息自律公约》。

上述的公约规范与人类社会的其他道德规范一样，不仅要理解道德规范的基本原则，更要对这些基本原则深思熟虑，明白哪些应该做，哪些不应该做。

九、国家对知识产权和软件使用的规定

1990 年 9 月，我国颁布了《中华人民共和国著作权法》，把计算机软件列为享有著作权保护的产品。

1991 年 6 月，国务院发布了《计算机软件保护条例》，规定计算机软件是个人或者团体的智力产品，同专利、著作一样受法律保护。

任何未经授权的使用、复制都是非法的，按规定要受到法律的制裁。人们在使用计算机软件或数据时，应遵照国家有关法律规定，尊重其作品的版权，这是使用计算机的基本道德规范。

十、我国信息安全的相关法律法规

所有的社会行为都需要法律法规来规范和约束。随着网络的发展，我国各项涉及网络信息安全的法律法规也相继出台。

我国现行的信息安全法律体系包括以下四个方面。

1. 一般性法律规定

这类法律法规是指宪法、国家安全法、保守国家秘密法、治安管理处罚法、著作权法、专利法等。这些法律法规并没有专门对网络行为进行规定，但是，它所规范和约束的对象中包括了危害信息网络安全的行为。

2. 规范和惩罚网络犯罪的法律

这类法律包括《中华人民共和国刑法》《全国人大常委会关于维护互联网安全的决定》等。其中，刑法也是一般性法律规定，这里将其独立出来，作为规范和惩罚网络犯罪的法律规定。

3. 直接针对计算机信息网络安全的特别规定

这类法律法规主要有《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国计算机软件保护条例》等。

4. 具体规范信息网络安全技术、信息网络安全管理等方面的规定

这一类法律主要有《商用密码管理条例》《计算机信息系统安全专用产品检测和销售许可证管理办法》《计算机病毒防治管理办法》《计算机信息系统保密管理暂行规定》《计算机信息系统国际联网保密管理规定》《电子出版物管理规定》《金融机构计算机信息系统安全保护工作暂行规定》等。

2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议表决通过《中华人民共和国网络安全法》，2017 年 6 月 1 日起正式施行。《网络安全法》是中国网络安全领域的第一部专门法律，是保障网络安全的基本法，这是中国建立严格的网络治理指导方针的一个重要里程碑。《网络安全法》共有七章七十九条，内容十分丰富，具有六大突出亮点。

（1）明确了网络空间主权的原则。

（2）明确了网络产品和服务提供者的安全义务。

（3）明确了网络运营者的安全义务。

（4）进一步完善了个人信息保护规则。

（5）建立了关键信息基础设施安全保护制度。

（6）确立了关键信息基础设施重要数据跨境传输的规则。

《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

思考和训练

1. 思考影响信息安全的因素有哪些。

2. 结合你在工作和生活中遇到的问题，谈谈目前信息安全面临的主要威胁有哪些。

3. 为什么要对信息安全分等级进行保护？

4. 你认为使用计算机和网络应遵守哪些道德规范？

5. 上网查询国家对知识产权和软件使用的要求，以及信息安全的相关法律法规。

6. 上网查询影响信息安全的相关案例，对案例进行分析，判断其属于哪类威胁因素，指出产生的危害及处罚建议。

7. 上网查询斯诺登事件（也称“棱镜门”），了解事件背景、事件发展、事件影响，谈谈你的看法。

任务二　信息安全防御技术

任务描述

信息安全防御技术主要用于防止系统漏洞、防止外部黑客入侵、防御病毒破坏、对可疑访问进行有效控制等，同时还包含数据灾难与数据恢复技术，即在计算机发生意外或灾难时，可以使用备份还原及数据恢复技术将丢失的数据找回。

本任务将介绍几种典型的信息安全防御技术。

学习目标

1. 了解信息加密技术的基本知识。
2. 了解认证技术的基本知识。
3. 了解访问控制技术的基本知识。
4. 了解防火墙技术的基本知识。
5. 了解入侵检测技术的基本知识。
6. 了解云安全技术的基本知识。
7. 了解系统容灾技术的基本知识。

任务实现

一、加密技术

信息加密的目的是保护网络中的数据、文件、口令和控制信息，保护网上传输的数据。

1. 加密和解密

密码技术包含两方面内容，即加密和解密。

（1）加密就是研究、编写密码系统，把数据和信息转换为不可识别的密文的过程。

（2）解密就是研究密码系统的加密途径，恢复数据和信息的本来面目的过程。

加密和解密过程共同组成了加密系统，如图 1–2–1 所示。

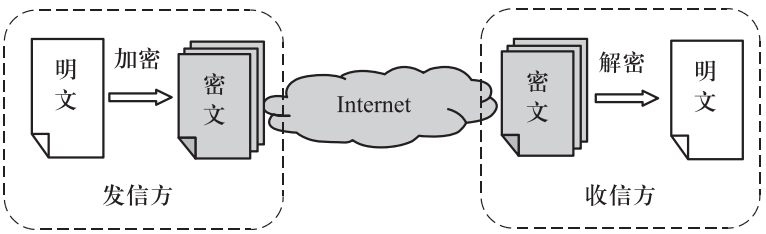

图 1–2–1　加密和解密过程

2. 对称密钥密码体制和非对称密钥密码体制

根据加密和解密过程是否使用相同的密钥，加密算法可分为对称密钥加密算法和非对称密钥加密算法。

（1）对称密钥加密算法。

在大多数的对称算法中，加密密钥和解密密钥是相同的，所以也称这种加密算法为秘密密钥算法或单密钥算法。它要求发送方和接收方在安全通信之前，商定一个密钥。对称加密技术如图 1–2–2 所示。

对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都可以对他们发送或接收的消息解密，所以密钥的保密性对通信的安全性至关重要。

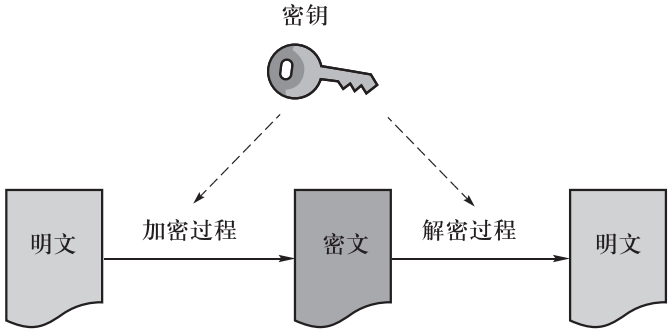

图 1–2–2　对称加密技术

（2）非对称密钥加密算法制（又称公开密钥加密算法）。

非对称加密算法需要两个密钥：公开密钥和私有密钥。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法称为非对称加密算法，如图 1–2–3 所示。

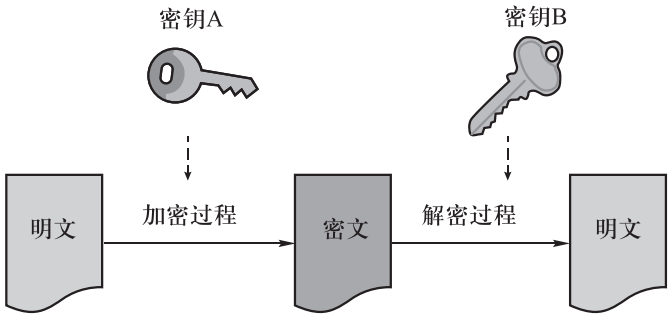

图 1–2–3　非对称加密技术

非对称加密算法比对称加密算法慢数千倍，但在保护通信安全方面，非对称加密算法更具优势。

二、认证技术

认证就是对于证据的辨认、核实、鉴别，以建立某种信任关系。在通信中，要涉及两方面：一方提供证据或标识，另一方对这些证据或标识的有效性进行辨认、核实、鉴别。

1. 数字签名

数字签名是数字世界中的一种信息认证技术，是公开密钥加密技术的一种应用，是根据某种协议来产生一个被签署文件的特征和签署人特征，以保证文件的真实性和有效性的数字技术，同时也可用来核实接收者是否有伪造、篡改行为。

2. 身份验证

身份验证是指通过一定的手段，完成对用户身份的确认。身份验证的方法很多，基本上可分为基于共享密钥的身份验证、基于生物学特征的身份验证、基于公开密钥加密算法的身份验证。不同的身份验证方法，其安全性也各有高低。

数字签名认证技术的基本原理，如图 1-2-4 所示。

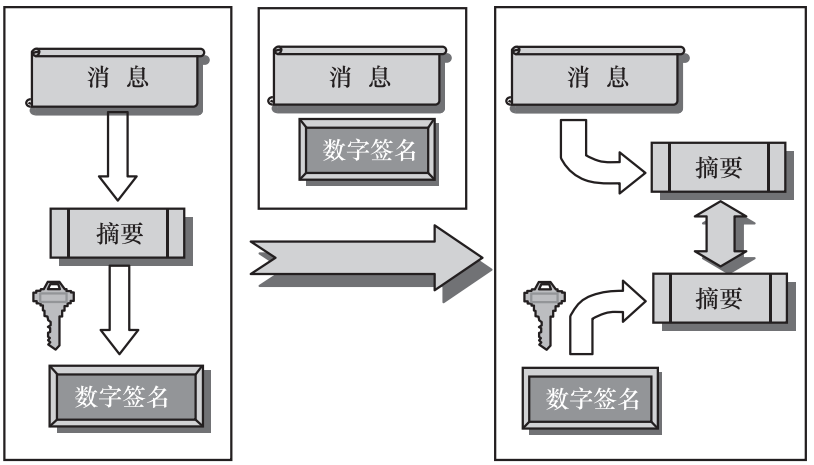

图 1-2-4　数字签名认证技术基本原理

三、访问控制技术

访问控制是对信息系统资源的访问范围及方式进行限制的策略。它是建立在身份认证之上的操作权限控制。

身份认证解决了访问者是否合法，但并非身份合法就什么都可以做，还要根据不同的访问者，规定他们分别可以访问哪些资源，以及对这些可以访问的资源可以用什么方式（读、写、执行、删除等）访问。

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，涉及的技术比较广，包括入网访问控制、网络权限控制、目录级安全控制、属性安全控制和服务器安全控制格式等多种手段。

例如，基于角色的访问控制技术，如图 1-2-5 所示。

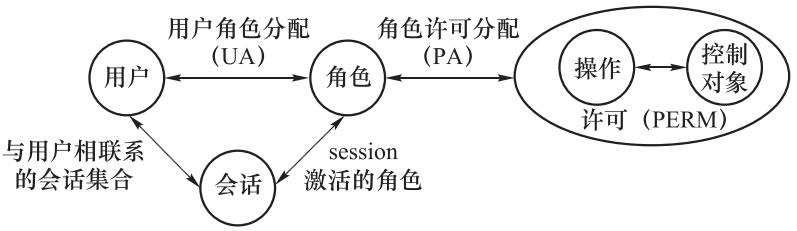

图 1-2-5　基于角色的访问控制技术

四、防火墙技术

防火墙是一种位于内部网络与外部网络之间的网络安全防护系统，如图 1–2–6 所示，可以依照特定的规则允许或限制传输的数据通过，主要用于对内部网和公众访问网进行隔离，使一个网络不受另一个网络的攻击。

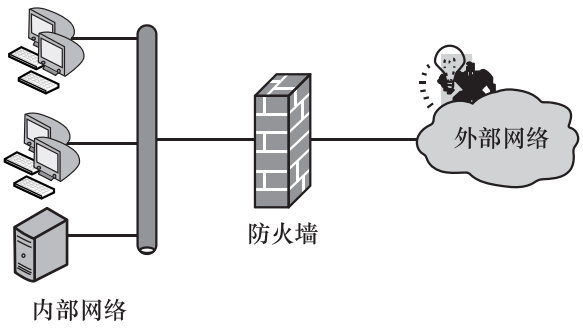

图 1–2–6　防火墙技术

防火墙的主要作用如下。

（1）可以限制他人进入内部网络，过滤掉不安全服务和非法用户。

（2）防止入侵者接近你的防御设施。

（3）限定用户访问特殊站点。

（4）为监视 Internet 安全提供方便。

目前防火墙技术已经在计算机网络得到广泛应用。

五、入侵检测

入侵检测系统（Intrusion Detection System，IDS）是一种对网络活动进行实时监测的专用系统。该系统处于防火墙之后，是防火墙之后的第二道安全闸门，如图 1–2–7 所示。通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

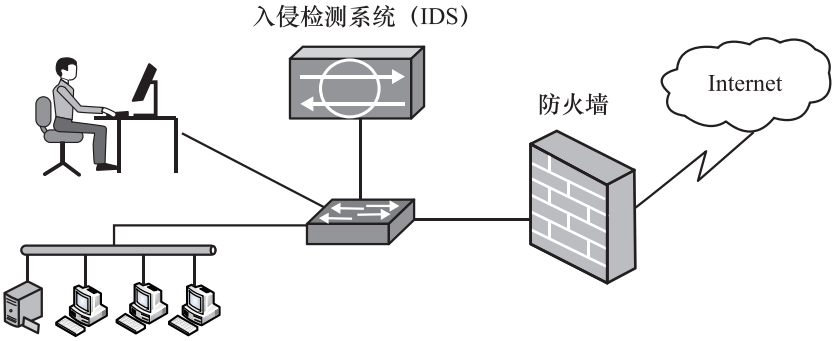

图 1–2–7　入侵检测系统

入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。入侵检测系统能够帮助网络系统快速发现攻击的发生，扩展了系统管理员的安全管理能力。