目录

项目 7 物理环境安全 / 117

项目 8 电子货币安全 / 139

项目 9 网络支付安全 / 179

项目 1 信息安全概论

知识目标

1. 理解信息安全的基本概念。
2. 了解信息安全的体系结构。
3. 了解信息安全存在的隐患。
4. 了解信息安全攻击形式。
5. 了解信息安全基本属性。
6. 理解信息安全管理体制。

能力目标

1. 掌握信息安全常用技术。
2. 掌握信息安全加密原理。
3. 掌握信息安全验证系统。

知识导图

笔记

项目导入

随着计算机技术的飞速发展、5G 的市场化应用，信息化网络已经成为社会发展的重要保证。信息化网络涉及国家政府、军事、文教等诸多领域，许多信息是政府宏观调控决策、商业经济、能源资源数据、科研数据等重要决策依据。其中有很多是敏感信息，甚至是国家机密，难免会吸引来自世界各地的各种人为攻击（例如信息泄露、信息窃取、数据篡改、数据删添、计算机病毒等）。网络信息安全关系国家安全主权、社会稳定、民族文化继承和发扬等重要问题，随着全球信息化步伐的加快已经上升为我国的战略高度，而信息安全对抗愈演愈烈归根到底就是信息安全人才的竞争。信息安全基础是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科，也是信息安全入门者的必备知识。

任务 1.1 信息安全与网络安全

子任务 1.1.1 信息安全的定义

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，系统连续可靠正常地运行，信息服务不中断等。 信息安全作为一门学科涉及的范围广，是一门交叉复合型极强的学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多领域多种学科。

子任务 1.1.2 网络安全的定义

狭义来讲，网络安全是通过各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和保密性。但网络安全的具体含义会随着“角度”的变化而变化。从用户（个人、企业等）的角度来讲，是个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的侵犯；从网络管理者的角度来讲，是对本地网络信息的访问、读、写等操作控制的威胁；从安全保密的角度来讲，是对国家、社会产生的危害；从网络安全意识形态来讲，是保持社会稳定、绿色网络环境健康发展的管理与持续。

子任务 1.1.3 信息安全的发展历程

1. 通信保密阶段

该阶段为 20 世纪 40 年代至 70 年代，又称为通信安全时代，重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性。主要安全威胁是搭线窃听、密码学分析。主要保护措施是加密技术。主要标志是 1949 年 Shannon 发表的《保密通信的信息理论》、1976 年 Diffie 和 Hellman 在 *New Directions in Cryptography* 一文中所提出的公钥密码体制、1977 年美国国家标准局公布的数据加密标准（DES）。

2. 计算机安全阶段

该阶段为 20 世纪 70 年代至 80 年代，重点是确保计算机系统中硬件、软件及正在处

理、存储、传输信息的机密性、完整性和可用性。主要安全威胁扩展到非法访问、恶意代码、脆弱口令等。主要保护措施是安全操作系统设计技术（TCB）。主要标志是 1985 年美国国防部（DoD）公布的可信计算机系统评估准则（橘皮书 TCSEC）将操作系统的安全级别分为 4 类 7 个级别（D、C1、C2、B1、B2、B3、A1），后补充红皮书 TNI（1987）和紫皮书 TDI（1991）等，构成彩虹（Rainbow）系列。

笔记

3. 信息技术安全阶段

该阶段为 20 世纪 80 年代至 90 年代，重点是保护信息，确保信息在存储、处理、传输过程中及信息系统中不被破坏，确保合法用户的服务和限制非授权用户的服务，以及必要的防御攻击的措施，强调信息的保密性、完整性、可控性、可用性等。主要安全威胁发展到网络入侵、病毒破坏、信息对抗的攻击等。主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、PKI、VPN、安全管理等。主要标志是提出了新的安全评估准则 CC（ISO 15408、GB/T 18336）。

4. 信息保障阶段

该阶段始于 20 世纪 90 年代后期，重点放在保障国家信息基础设施不被破坏，确保信息基础设施在受到攻击的前提下能够最大限度地发挥作用，强调系统的鲁棒性和容灾特性。主要安全威胁发展到集团有组织地对信息基础设施进行攻击等。主要保护措施是灾备技术、建设面向网络恐怖与网络犯罪的国际法律秩序与国际联动的网络安全事件的应急响应技术。主要标志是美国推出的“保护美国计算机空间”（PDD-63）的体系框架。

子任务 1.1.4　网络安全的重要性与要素

1. 网络安全的重要性

（1）计算机存储、数据处理是有关国家安全的政治、经济、军事、国防的情况及一些部门、机构、组织的机密信息，是个人的敏感信息、隐私，因此成为敌对势力、不法分子的攻击目标。

（2）计算机系统功能的日益完善和速度的不断提高，系统组成越来越复杂，系统规模越来越大，特别是 Internet 的迅速发展，存取控制、逻辑连接数量不断增加，软件规模空前膨胀，任何隐含的缺陷、失误都能造成巨大损失。

（3）人们对计算机系统的需求不断扩大，需求在许多方面都是不可逆转、不可替代的，而计算机系统使用的场所正在转向工业、农业、野外、天空、海上、宇宙空间、核辐射环境等，这些环境都比机房恶劣，出错率和故障的增多必将导致可靠性和安全性的降低。

（4）计算机系统的广泛应用，各类应用人员队伍迅速发展壮大，教育和培训却往往跟不上知识更新的需要，操作人员、编程人员和系统分析人员的失误或缺乏经验都会造成系统的安全功能不足。

（5）计算机网络安全问题涉及许多学科领域，既包括自然科学，又包括社会科学。就计算机系统的应用而言，安全技术涉及计算机技术、通信技术、存取控制技术、校验认证技术、容错技术、加密技术、防病毒技术、抗干扰技术、防泄露技术等，因此是一个非常复杂的综合问题，并且其技术、方法和措施都要随着系统应用环境的变化而不断变化。

（6）从认识论的角度看，人们往往首先关注系统功能，然后才被动地从现象注意系统

笔记

应用的安全问题，因此普遍存在着重应用、轻安全、法律意识淡薄的现象。计算机系统的安全是相对不安全而言的，许多危险、隐患和攻击都是隐蔽的、潜在的、难以明确却又广泛存在的，这也使得目前不少网络信息系统都存在先天性的安全漏洞和安全威胁，有些甚至产生了非常严重的后果。

2. 网络安全的基本要素

（1）机密性（保密性）：是指不能非授权访问，通过访问控制来阻止非授权用户获取机密信息，保证信息在非授权访问的过程中确保信息不暴露给未授权的实体或进程。

（2）完整性：只有得到允许的人才能修改实体或进程，并且能够判别出实体或进程是否已被修改。完整性鉴别机制，保证只有得到允许的人才能修改数据。防篡改。

（3）可用性：得到授权的实体可获得服务，攻击者不能占用所有的资源而阻碍授权者的工作。用访问控制机制，阻止非授权用户进入网络，使静态信息可见，动态信息可操作。防中断。

（4）可鉴别性（可审查性）：对危害国家信息（包括利用加密的非法通信活动）的监视审计，控制授权范围内的信息流向及行为方式。使用授权机制，控制信息传播范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控性。

（5）不可抵赖性：是对出现安全问题提供调查的依据和手段，使攻击者、抵赖者、破坏者“逃不脱”，建立有效的责任机制，防止用户否认其行为，做到可追溯，这一点在电子商务中极其重要。

任务 1.2 信息安全的隐患因素

在网络高速发展的今天，人们在享受网络便捷所带来的益处的同时，网络的安全也日益受到威胁。网络攻击行为日趋复杂，各种方法相互融合，使网络安全防御更加困难。黑客攻击行为组织性更强，攻击目标从单纯地追求“荣耀感”向获取多方面实际利益的方向转移，网上木马、间谍程序、恶意网站、网络仿冒等不断出现和日趋泛滥。

智能手机、平板电脑等无线终端的处理能力和功能通用性提高，5G 的投入使用，移动终端网络攻击已经开始出现，并将进一步发展。总之，网络安全问题变得更加错综复杂，影响将不断扩大，网络威胁如果不加以防范，会严重地影响整个网络的应用。

子任务 1.2.1 隐患原因

（1）开放性的网络环境：Internet 的开放性，使网络变成众矢之的，可能遭受各方面的攻击；Internet 的国际性使网络可能遭受本地用户或远程用户、国外用户或国内用户等的攻击；Internet 的自由性没有给网络的使用者规定任何的条款，导致用户“太自由了”，自由的下载，自由的访问，自由的发布；Internet 使用的“傻瓜性”使任何人都可以方便地访问网络，基本不需要技术，只要会移动鼠标就可以上网冲浪，这就给用户带来很多的隐患。

（2）协议本身的缺陷：网络应用层服务的隐患；IP 层通信的易欺骗性；针对 ARP 的欺骗性。

（3）操作系统的漏洞：系统模型本身的缺陷；操作系统存在 BUG ；操作系统程序配置不正确。

（4）人为因素：缺乏安全意识，缺少网络应对能力，有相当一部分人存在侥幸心理，认为自己的电脑中没有什么重要的东西，不会被别人黑，重装系统后觉得防范很麻烦，所以不认真对待安全问题，造成的隐患就特别多。

（5）设备不安全：对于购买的国外的网络产品，到底有没有留后门根本无法得知，这对于缺乏自主技术支撑、依赖进口的国家而言，无疑是最大的安全隐患。

（6）线路不安全：不管是有线介质（双绞线、光纤等），还是无线介质（微波、红外、卫星、WiFi 等），窃听其中一小段线路的信息是可行的，没有绝对安全的通信线路。

笔记

子任务 1.2.2　攻击分类

1. 主动攻击

主动攻击是指攻击者非法访问其所需信息的故意行为。例如，远程登录到指定机器的端口，找出公司运行的邮件服务器的信息；伪造无效 IP 地址连接服务器，接收到错误 IP 地址的系统浪费时间去连接非法地址等。攻击者在主动做一些不利于公司系统的事情。正因为如此，寻找攻击者是很容易的。主动攻击包括拒绝服务攻击、信息篡改、资源使用、欺骗等。

2. 被动攻击

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般不会觉察到。被动攻击方法包括嗅探、信息收集等。

从攻击的目的来看，包括拒绝服务攻击（DoS）、获取系统权限的攻击、获取敏感信息的攻击；从攻击的切入点来看，包括缓冲区溢出攻击、系统设置漏洞的攻击等；从攻击的纵向实施过程来看，包括获取初级权限攻击、提升最高权限的攻击、后门攻击、跳板攻击等；从攻击的类型来看，包括对各种操作系统的攻击、对网络设备的攻击、对特定应用系统的攻击等。

子任务 1.2.3　缺陷分类

1. 技术缺陷

现有的各种网络安全技术都是针对网络安全问题的某一个或几个方面来设计，它只能相应地在一定程度上解决这一个或几个方面的网络安全问题，无法防范和解决其他的问题，更不可能提供对整个网络系统有效的保护。如身份认证和访问控制技术只能解决确认网络用户身份的问题，但却无法防止确认用户之间传递的信息是否安全的问题，而计算机病毒防范技术只能防范计算机病毒对网络和系统的危害，但却无法识别和确认网络上用户的身份等。

现有的各种网络安全技术中，防火墙技术可以在一定程度上解决一些网络安全问题，但防火墙本身存在局限性，其最大的局限性就是防火墙自身不能保证其准许放行的数据是否安全。

同时，防火墙还存在以下一些弱点：

（1）不能防御来自内部的攻击：来自内部的攻击者是从网络内部发起攻击的，他们的攻击行为不通过防火墙，而防火墙只是隔离内部网与 Internet 上的主机，监控内部网和 Internet 之间的，而对内部网上的情况不做检查，因而对内部的攻击无能为力。

注意

入侵检测技术也存在着局限性，其最大的局限性就是漏报和误报严重，它不能称为一个可以信赖的安全工具，而只是一个参考工具。

（2）不能防御绕过防火墙的攻击行为：从根本上讲，防火墙是一种被动的防御手段，只能守株待兔式地对通过它的数据报进行检查，如果其数据由于某种原因没有通过防火墙，则防火墙就不会采取任何的措施。

（3）不能防御完全新的威胁：防火墙只能防御已知的威胁，但是人们发现可信赖的服务中存在新的侵袭方法，可信赖的服务就变成不可信赖的了。

（4）防火墙不能防御数据驱动的攻击：虽然防火墙扫描分析所有通过的信息，但是这种扫描分析多半是针对 IP 地址和端口号或者协议内容的，而非数据细节。这样一来，基于数据驱动的攻击，例如病毒，可以附在诸如电子邮件之类的方式进入计算机的系统中并发动攻击。

2. 配置缺陷

对于交换机和路由器而言，它们的主要作用是进行数据的转发，因此在设备自身的安全性方面考虑的就不是很周全。在默认的情况下，交换机和路由器的许多网络服务端口都是打开的，这就等于为黑客预留了进入的通道。

3. 策略缺陷

计算机信息安全问题主要在于信息技术和管理制度两个方面，所以相应的安全防范策略也必须从这两个方面入手，形成技术与管理、操作与监管并行的系统化安全保障体系。

4. 人为缺陷

人为缺陷即人为攻击，是指通过攻击系统的弱点，以便达到破坏、欺骗、窃取数据等的目的，使得网络信息的保密性、完整性、可靠性、可控性、可用性等受到伤害，造成经济上和政治上不可估量的损失。

人为攻击又分为偶然事故和恶意攻击两种。偶然事故虽然没有明显的恶意企图和目的，但它仍会使信息受到严重破坏。恶意攻击是有目的的破坏。

恶意攻击又分为被动攻击和主动攻击两种。被动攻击是指在不干扰网络信息系统正常工作的情况下，进行侦收、截获、窃取、破译和业务流量分析及电磁泄漏等。主动攻击是指以各种方式有选择地破坏信息，如修改、删除、伪造、添加、重放、乱序、冒充、制造病毒等。

子任务 1.2.4 攻击形式

现在攻击个人计算机的木马软件很多，功能比以前更多，使用智能化，危害也比以前更严峻，要想使自己的计算机安全，就扎好自己的篱笆，看好自己的门，计算机也有自己的门，我们称之为端口。

在 Internet 上，各主机间通过 TCP/IP 协议发送和接收数据包，各个数据包根据其目的主机 IP 地址来进行互联网络中的路由选择。可见，把数据包顺利地传送到目的主机是没有问题的。我们知道大多数操作系统都支持多程序（进程）同时运行，那么目的主机应该把接收到的数据包传送给众多同时运行的进程中的哪一个，端口机制便由此被引入进来。

本地操作系统会给那些有需求的进程分配协议端口（protocal port，即我们常说的端口），每个协议端口由一个正整数标识，如 80、139、445 等。当目的主机接收到数据报后，将根据报文首部的目的端口号，把数据发送到相应端口，而与此端口相对应的那个进程将会领取数据并等待下一组数据的到来。

1. 端口

在网络上冲浪，别人和你聊天，你发电子邮件，必须要有共同的协议，这个协议就是 TCP/IP 协议，任何网络软件的通信都基于 TCP/IP 协议。如果把互联网比作公路网，计算机就是路边的房屋，房屋要有门你才可以进出，TCP/IP 协议规定，计算机可以有 256 × 256 扇门，即从 0 到 65535 号“门”，TCP/IP 协议把它称作“端口”。当你发电子邮件的时候，E-mail 软件把信件送到了邮件服务器的 25 号端口；当你收信的时候，E-mail 软件是从邮件服务器的 110 号端口这扇门进去取信，你现在看到的我写的东西，是进入服务器的 80 端口。新安装好的个人计算机打开的端口号是 139 端口，你上网的时候，就是通过这个端口与外界联系的。

黑客通过端口进入计算机，基于 TCP/IP 协议通过某个端口进入个人计算机。如果计算机设置了共享目录，那么黑客就可以通过 139 端口进入你的计算机。除了 139 端口以外，如果没有别的端口是开放的，黑客还可以通过特洛伊木马进入你的计算机。

2. 特洛伊木马

特洛伊木马是一种典型的木马软件，称为 netspy.exe。如果你不小心运行了 netspy.exe，以后每次打开计算机的时候都会运行它，然后 netspy.exe 又在你的计算机上开了一扇“门”，“门”的编号是 7306 端口，如果 7306 端口是开放的，就可以用软件进入到计算机。特洛伊木马本身就是为了入侵个人计算机而做的，藏在计算机中和工作的时候是很隐蔽的，它的运行和黑客的入侵，不会在计算机的屏幕上显示出任何痕迹。Windows 本身没有监视网络的软件，所以不借助软件，是不知道特洛伊木马的存在和黑客的入侵的。

3. netbus 木马

杀毒软件可以删除木马，Netvrv 病毒防护墙可以删除 netspy.exe 和 bo.exe 木马，但是不能删除 netbus 木马。

netbus 木马的客户端有两种，开放的都是 12345 端口，一种以 Mring.exe 为代表（472，576 字节），一种以 SysEdit.exe 为代表（494，592 字节）。Mring.exe 一旦被运行以后，每次启动都将运行它，Windows 将它放在了注册表中，打开 C：/Windows/regedit.exe... 进入 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 找到 Mring.exe，然后删除这个键值，再到 Windows 中找到 Mring.exe 删除。Mring.exe 可能会被黑客改变名字，字节长度也被改变，但是在注册表中的位置不会改变。

子任务 1.2.5　传播方式

1. 网络媒体信息观点

无论是信息量，还是观点数量，网络媒体都已超过传统媒体，成为社会舆论的重要发源地。一些事件在网上披露后，引起网民强烈反应，推动事件得到处理，例如华南虎伪照被揭穿、许霆 ATM 取款案被改判、“躲猫猫”事件被查处等。网上不仅有正面信息，也有流言、谣言、假新闻等负面信息，如果不善加管理和引导，会对社会舆论产生负面影响。

2. 网络论坛发酵

网民在网络论坛中的真实面目和身份被各种符号所代替，具有隐匿性，可以毫无顾忌地发表意见。各种观念在网上集合、交汇、碰撞，夹杂着有害的、负面的杂音和噪音。网

笔记

笔记

络论坛成为“意见市场”，帖子成为“意见广告”。在论坛讨论中，兴趣观点比较相近的网民更容易聚集在一起，形成独特的政治场。这种政治场不断放大网民意见，形成“集体狂欢”，出现舆论一边倒的极化现象。网站论坛成为网络舆论发酵器，累积情绪，直至引发社会行动，实现从虚拟政治到现实政治的转换。

3. 网络通信隐秘传递

网络通信（包括电子邮件和即时通信）是互联网的重要功能，具有隐秘性、快捷性等特点。电子邮件使用简便、投递迅速、易于保存、全球畅通，可以传播文字、声音、图像等多种资料，可以一对一、一对多传递，极大地改变了信息传播方式。电子邮件在给人们带来诸多便利的同时，也被境内外敌对势力加以利用。

4. 网络检索强力搜寻

百度、谷歌、搜狐等搜索引擎具有强大的信息检索功能，可以在瞬间检索上百亿张网页，搜寻相关信息，给人们的学习、研究、工作、生活带来极大便利。搜索引擎已成为网络监督的重要手段。

5. 网络博客传播思想

博客是近年来增幅最大的言论载体。个人上网写博客正在形成一个新的文化奇观。Web 2.0 的推广，实现了“去中心化”的非线性传播，打破了网络出版的限制，消除了网民交流的中间环节，每个网民都可以成为传播发起节点，人人是记者、人人是作家、人人是编辑、人人办刊物。不但各类网站纷纷开设博客频道，而且出现了专门的博客网站。通过博客传播的观点已经并将继续影响社会思潮。

6. 各大 SNS 网络站点

交友网站和网络社区使网民出现分众化趋势，为相同兴趣（例如郊游）的网民组织活动提供平台，丰富网民生活。网络站点也成为集体上访等群体行动的组织平台。网络传播信息迅速、高效、广泛，使得集体活动十分便捷。

任务 1.3 网络安全模型与标准

子任务 1.3.1 网络安全模型

网络安全模型是动态网络安全过程的抽象描述。通过对安全模型的研究，了解安全动态过程的构成因素，是构建合理而实用的安全策略体系的前提之一。为了达到安全防范的目标，需要合理的网络安全模型，以指导网络安全工作的部署和管理。目前，在网络安全领域存在较多的网络安全模型，下面介绍常见的 PDRR 模型和 PPDR 模型。

1. PDRR 安全模型

PDRR 是美国国防部提出的常见安全模型，它概括了网络安全的整个环节，即防护（Protect）、检测（Detect）、响应（React）、恢复（Restore）。这 4 个部分构成了一个动态的信息安全周期，如图 1-1 所示。

笔记

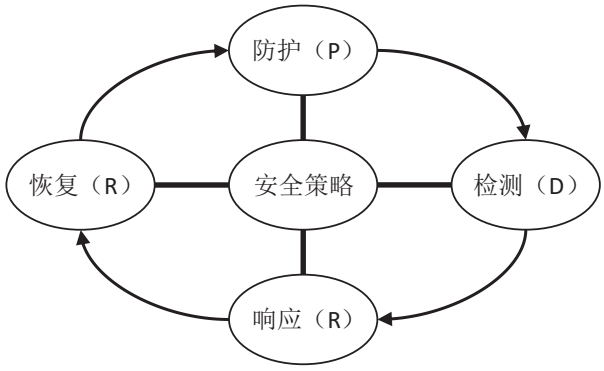

图 1-1　动态的信息安全周期

2. PPDR 安全模型

PPDR 是美国国际互联网安全系统公司提出的可适应网络安全模型，它包括策略（Policy）、保护（Protection）、检测（Detection）、响应（Response）4 个部分。PPDR 模型如图 1-2 所示。

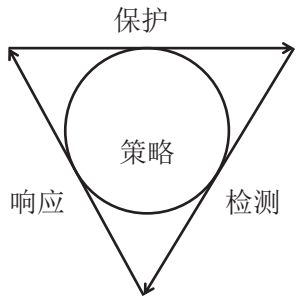

图 1-2　PPDR 安全模型

子任务 1.3.2 网络安全标准

1. TCSEC 标准

美国国防部的可信计算机系统评价准则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。它将安全分为 4 个方面：安全政策、可说明性、安全保障和文档。该标准将以上 4 个方面分为 7 个安全级别，按安全程度从最低到最高依次是 D、C1、C2、B1、B2、B3、A，如表 1-1 所示。

表 1-1　可信计算机系统评价准则

类别	级别	名称	主要特征
D	D	低级保护	保护措施很少，没有安全功能
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强调存取控制，安全标识
	B2	结构化保护	面向安全的体系结构 较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述、验证和隐秘通道分析

2. 我国的安全标准

我国的安全标准是由公安部主持制定、国家技术标准局发布的国家标准《计算机信息系统安全保护等级划分准则》(GB 17895—1999)。该准则将信息系统安全分为以下 5 个等级：

（1）用户自主保护级。

（2）系统审计保护级。

（3）安全标记保护级。

（4）结构化保护级。

（5）访问验证保护级。

笔记

任务 1.4 信息系统安全体系

子任务 1.4.1 信息系统架构及协议

信息系统本身由系统主体和客体组成，存在不同程度的脆弱性，这就为各种动机的攻击提供了入侵、骚扰或破坏信息系统的途径和方法。所谓信息系统的脆弱性，是指信息系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因而可能导致系统受到破坏、更改、泄露和功能失效，从而使信息系统处于异常状态，甚至崩溃瘫痪等。具体分析如下。

1. 硬件组件

信息系统硬件组件的安全隐患多来源于设计，主要表现为物理安全方面的问题。各种计算机或网络设备（如主机、CRT、电缆、Hub、路由器、微波线路等），除难以抗拒的自然灾害外，温度、湿度、尘埃、静电、电磁场等也可能造成信息的泄露或失效。信息系统在工作时，向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。

2. 软件组件

软件组件的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及软件过长、过大，不可避免地存在安全脆弱性。

软件组件可分为三类，即操作平台软件、应用平台软件和应用业务软件。这三类软件以层次结构构成软件组件体系。操作平台软件处于基础层，维系着系统组件运行的平台，因此操作平台软件的任何风险都可能直接危及或被转移或延伸到应用平台软件。所以，对信息系统安全所需的操作平台软件的安全等级要求不得低于系统安全等级要求，特别是信息系统的安全服务组件的操作系统安全等级必须至少高于系统安全一个等级，强烈建议安全服务组件的操作系统不得直接采用商业级或普遍使用的操作系统。应用平台软件处于中间层次，是在操作平台支撑下运行的支持和管理应用业务的软件。一方面，应用平台软件可能受到来自操作平台软件风险的影响；另一方面，应用平台软件的任何风险可直接危及或传递给应用业务软件。因此应用平台软件的安全特性也至关重要。在提供自身安全保护的同时，应用平台软件还必须为应用软件提供必要的安全服务功能。应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险都直接表现为信息系统的风险。

3. 网络和通信协议

在当今的网络通信协议中，局域网和专用网络的通信协议具有相对封闭性，因为它不能直接与异构网络连接和通信。这样的“封闭”网络本身基于两个原因比开放式的 Internet 的安全特性好，一是网络体系的相对封闭性降低了从外部网络或站点直接攻入系统的可能性，但信息的电磁泄漏性和基于协议分析的搭线截获问题仍然存在；二是专用网络自身具有较为成熟的身份鉴别、访问控制和权限分割等安全机制。安全问题最多的网络和通信协议是基于 TCP/IP 协议栈的 Internet 及其通信协议，因为任何接入 Internet 的计算

机网络协议以及利用公共通信基础设施构建的内联网 / 外联网，在理论上和技术实践上已无真正的物理界限，同时在地缘上也没有真正的国界。国与国之间、组织与组织之间，以及个人与个人之间的网络界限是依靠协议、约定和管理关系进行逻辑划分的，因而是一种虚拟的网络现实；而支持 Internet 运行的 TCP/IP 协议栈原本只考虑互联互通和资源共享的问题，并未考虑也无法兼容解决来自网际中的大量安全问题。Internet 何以存在如此多的安全隐患，TCP/IP 协议栈的脆弱性和漏洞，首先要理解与 Internet 有关的安全脆弱性和漏洞存在的原因和分布情况，需从网络技术发展历史和 TCP/IP 协议栈的研究初衷、使用背景及发展驱动力等方面分析。

笔记

（1）缺乏对用户身份的鉴别。TCP/IP 协议的机制性安全隐患之一是缺乏对通信双方真实身份的鉴别机制。由于 TCP/IP 协议使用 IP 地址作为网络节点的唯一标识，而 IP 地址的使用和管理又存在很多问题，IP 地址是由 Internet 信息中心（InterNIC）分发的，其数据包的源地址很容易被发现，且 IP 地址隐含了所使用的子网掩码，攻击者据此可以画出目标网络的轮廓。因此使用标准 IP 地址的网络拓扑对 Internet 来说是暴露的。并且 IP 地址很容易被伪造和被更改，且 TCP/IP 协议没有对 IP 包中源地址真实性的鉴别机制和保密机制。因此 Internet 上任何主机都可以产生一个带有任意源 IP 地址的 IP 包，从而假冒另一个主机进行地址欺骗。

（2）缺乏对路由协议的鉴别认证。TCP/IP 在 IP 层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护，因此可以通过 Internet 利用路由信息修改网络传输路径，误导网络分组传输。

（3）TCP/UDP 的缺陷。TCP/IP 协议规定了 TCP/UDP 是基于 IP 协议上的传输协议，TCP 分段和 UDP 数据包是封装在 IP 包中在网上传输的，除可能面临 IP 层所遇到的安全威胁外，还存在下列 TCP/UDP 实现中的安全隐患。

建立一个完整的 TCP 连接，需要经历“三次握手”过程。在客户 / 服务器模式的“三次握手”过程中，假如客户的 IP 地址是假的，是不可达的，那么 TCP 不能完成该次连接所需的“三次握手”，使 TCP 连接处于“半开”状态。攻击者利用这一弱点可实施如 TCP SYN Flooding 攻击的“拒绝服务”攻击。TCP 提供可靠连接是通过初始序列号和鉴别机制来实现的。每一个合法的 TCP 连接都有一个客户 / 服务器双方共享的唯一序列号作为标识和鉴别。初始序列号一般由随机数发生器产生，但问题出在很多操作系统（如 UNIX）在实现 TCP 连接初始序列号的方法中所产生的序列号并不是真正随机的，而是一个具有一定规律、可猜测或计算的数字。对攻击者来说，猜出了初始序列号并掌握了目标 IP 地址之后，就可以对目标实施 IP Spoofing 攻击，而 IP Spoofing 攻击很难检测，因此此类攻击危害极大。UDP 是一个无连接控制协议，极易受 IP 源路由和拒绝服务型攻击。在 TCP/IP 协议层结构中，应用层位于最顶部，因此下层的安全缺陷必然导致应用层的安全出现漏洞甚至崩溃；而各种应用层服务协议（如 Finger、FTP、Telnet、E-mail、DNS、SNMP 等）本身也存在许多安全隐患，这些隐患涉及鉴别、访问控制、完整性和机密性等多个方面，极易引起针对基于 TCP/IP 应用的攻击。

笔记

子任务 1.4.2 信息系统安全内容及策略

1. 物理安全

网络的物理安全是整个网络系统安全的前提。在网络工程建设中，由于网络系统属于弱电工程，耐压值很低，因此，在网络工程的设计和施工中，必须优先考虑保护人和网络设备不受电、火灾和雷击的侵害；考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统和绝缘线、裸体线以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。总体来说，物理安全的风险主要有：地震、水灾、火灾等环境安全；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用性的硬件；双机多冗余的设计；机房环境及报警系统、安全意识等设备与媒体的安全，因此要注意这些安全隐患，同时还要尽量避免网络的物理安全风险。

2. 网络安全

这里的网络安全主要是指网络拓扑结构设计影响的网络系统的安全性。假如在外部和内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也影响在同一网络上的许多其他系统。透过网络传播，还会影响到连上 Internet/Intranet 的其他的网络；影响所及，还可能涉及法律、金融等安全敏感领域。因此，在设计时有必要将公开服务器（Web、DNS、E-mail 等）和外网及内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

3. 系统安全

所谓系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows 系统或者其他任何商用的 UNIX 操作系统，其开发厂商必须有其后门。因此，我们可以得出如下结论：没有安全的操作系统。不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统。因此不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置，而且必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

4. 应用安全

应用安全涉及方面很多，以 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案有 sendmail、Netscape Messaging Server、Software Com Post.Office、Lotus Notes、Exchange Server、SUN CIMS 等不下二十种；其安全手段涉及 LDAP、DES、RSA 等各种方式。应用系统是不断发展且应用类型是不断增加的。在应用系统的安全性上，主要考虑尽可能建立安全的系统平台，而且通过专业的安全工具不断发现漏洞，修补漏洞，提高系统的安全性。

信息的安全性涉及机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。在某些网络系统中，涉及很多机密信息，如果一些重要信息遭到窃取或破坏，它的经济、社会影响和政治影响将是很严重的。因此，对用户使用计算机必须进行身份认证，对于重要信息的通信必须授权，传输必须加密。采用多层次的访问控制与权限控

制手段，实现对数据的安全保护；采用加密技术，保证网上传输的信息（包括管理员口令与账户、上传信息等）的机密性与完整性。

笔记

5. 管理安全

管理安全是网络安全中最重要的部分。责权不明、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是制定健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络便成了首要任务。一旦上述的安全隐患成为事实，所造成的对整个网络的损失都是难以估计的。因此，网络的安全建设是网络建设过程中重要的一环。

任务 1.5　网络安全的威胁及防护体系

子任务 1.5.1　网络安全的威胁

所谓网络安全的威胁是指某个实体（人、事件、程序等）对某一资源的机密性、完整性、可用性在合法使用时可能造成的危害。这些可能出现的危害，通过一定的攻击手段来实现。

网络安全的主要威胁有非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等。

子任务 1.5.2　网络安全的防护体系

网络安全防护体系是由安全操作系统、应用系统、防火墙、网络监控、安全扫描、通信加密、网络反病毒等多个安全组件共同组成的，每个组件只能完成其中部分功能，我们要构建一个进不来、拿不走、改不了、看不懂、跑不了的绿色安全网络环境。

1. 入侵检测 IDS

通过计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象，同时做出响应。入侵检测作为一种积极主动的安全防护技术，能很好地弥补防火墙的不足，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高信息安全基础结构的完整性。它的主要作用如下：

（1）监视、分析用户及系统活动。

（2）审计系统构造和弱点。

（3）统计分析异常行为模式。

（4）评估重要系统和数据文件的完整性。审计跟踪管理操作系统，并识别用户违反安全策略的行为。

笔记

2. 数据加密

计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。密码是实现秘密通信的主要手段，是隐蔽语言、文字、图像的特种符号。凡是用特种符号按照通信双方约定的方法把电文的原形隐蔽起来，不为第三者所识别的通信方式统称为密码通信。在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能了解信息的内容，从而保证信息传输的安全。

数据信息保密性安全规范用于保障重要业务数据信息的安全传递与处理应用，确保数据信息能够被安全、方便、透明地使用。

（1）密码安全。密码的使用应该遵循以下原则。

①不能将密码写下来，不能通过电子邮件传输。

②不能使用缺省设置的密码。

③不能将密码告诉别人。

④如果系统的密码泄露了，必须立即更改。

⑤密码要以加密形式保存，加密算法强度要高且不可逆。

⑥系统应该强制指定密码的策略，包括密码的最短有效期、最长有效期、最短长度、复杂性等。

⑦如果需要特殊用户的口令（例如 UNIX 下的 Oracle），要禁止通过该用户进行交互式登录。

⑧在要求较高的情况下可以使用强度更高的认证机制，例如双因素认证。

⑨要定时运行密码检查器检查口令强度，对于保存机密和绝密信息的系统应该每周检查一次口令强度；其他系统应该每月检查一次。

（2）密钥安全。密钥管理对于有效使用密码技术至关重要。密钥的丢失和泄露可能会损害数据信息的保密性、重要性和完整性。因此，应采取加密技术等措施来有效保护密钥，以免密钥被非法修改和破坏；还应对生成、存储和归档保存密钥的设备采取物理保护。此外，必须使用经过业务平台部门批准的加密机制进行密钥分发，并记录密钥的分发过程，以便审计跟踪，统一对密钥、证书进行管理。

密钥的管理应该基于以下流程。

①密钥产生：为不同的密码系统和不同的应用生成密钥。

②密钥证书：生成并获取密钥证书。

③密钥分发：向目标用户分发密钥，包括在收到密钥时如何将之激活。

④密钥存储：为当前或近期使用的密钥或备份密钥提供安全存储，包括授权用户如何访问密钥。

⑤密钥变更：包括密钥变更时机及变更规则，处置被泄露的密钥。

⑥密钥撤销：包括如何收回或者去激活密钥，如在密钥已被泄露或者相关运维操作员离开业务平台部门时（在这种情况下，应当归档密钥）。

⑦密钥恢复：作为业务平台连续性管理的一部分，对丢失或破坏的密钥进行恢复。

⑧密钥归档：归档密钥，以用于归档或备份的数据信息。

⑨密钥销毁：密钥销毁将删除该密钥管理下数据信息客体的所有记录，将无法恢复，因此，在密钥销毁前，应确认由此密钥保护的数据信息不再需要。

笔记

3. 口令

防止未授权用户进入网络的第一步就是使用口令，虽然口令安全仅仅是整个网络安全的一部分，但其重要性却不能否认。而且，由于口令认证的代价低、易于实现和用户界面友好等特点，使得它是保护信息网络的一个重要方法。传统的口令认证方案是每个用户都拥有一个身份号码 ID 和一个秘密的口令 PW，每当一个用户申请登录网络系统时，系统就要求用户提供一个有效的 ID 和相应的口令。最简单的认证方法是预先构造一个存储每个用户 ID 和相关口令的口令表。在一个口令认证方案中，每个网络用户设为 U_i，在登录阶段提交其 ID_i 和口令 PW_i，以申请登录系统。传统的认证方法是系统检索口令表以检查提交的口令是否与事先保存在口令表中的一致。如果一致，则用户 U_i 被认为是一个已获授权的用户，并被允许进入系统；否则，用户的登录请求被拒绝。

4. CA 认证证书

证书实际是由证书签证机关（CA）签发的对用户公钥的认证。证书的内容包括：电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期等。目前，证书的格式和验证方法普遍遵循 X.509 国际标准。

一个标准的 X.509 数字证书包含证书的版本信息、证书的序列号（唯一的）、证书使用的签名算法、证书的发行机构名称及私钥签名、证书的有效期、证书的使用者及其公钥信息。

5. 数字签名

RSA 公钥体制可实现对数字信息的数字签名。信息发送者用其私钥对从所传报文中提取出的特征数据（或称数字指纹）进行 RSA 算法操作，以保证发信人无法抵赖曾发过该信息（即不可抵赖性），同时也确保信息报文在传递过程中未被篡改（即完整性）。当信息接收者收到报文后，就可以用发送者的公钥对数字签名进行验证。

在数字签名中有重要作用的数字指纹是通过一类特殊的散列函数（Hash 函数）生成的。对这些 Hash 函数的特殊要求如下：

（1）接受的输入报文数据没有长度限制。

（2）对任何输入报文数据生成固定长度的摘要（数字指纹）输出。

（3）从报文能方便地算出摘要。

（4）难以对指定的摘要生成一个报文，而由该报文可以算出该指定的摘要。

（5）难以生成两个不同的报文具有相同的摘要。

CA 认证验证过程，收方在收到信息后用如下的步骤验证您的签名。

（1）使用自己的私钥将信息转为明文。

（2）使用发信方的公钥从数字签名部分得到原摘要。

（3）收方对您所发送的源信息进行 Hash 运算，也产生一个摘要。

（4）收方比较两个摘要，如果两者相同，则可以证明信息签名者的身份；如果两摘要内容不符，可能对摘要进行签名所用的私钥不是签名者的私钥，这就表明信息的签名者不可信，也可能收到的信息根本就不是签名者发送的信息，信息在传输过程中已经遭到破坏或篡改。

6. 访问控制技术

访问控制技术可防止对任何资源进行未授权的访问，从而使计算机系统在合法的范围内使用。亦指通过用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或

笔记

限制对某些控制功能的使用的一种技术，如 UniNAC 网络准入控制系统的原理就是基于此技术之上。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。

访问控制（Access Control）指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段。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。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之一，也是主体依据某些控制策略或权限对客体本身或其资源进行的不同授权访问。

访问控制包括三个要素：主体、客体和控制策略。

（1）主体 S（Subject）是指提出访问资源具体请求，是某一操作动作的发起者，但不一定是动作的执行者，可能是某一用户，也可以是用户启动的进程、服务和设备等。

（2）客体 O（Object）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。客体可以是信息、文件、记录等集合体，也可以是网络上硬件设施、无限通信中的终端，甚至可以包含另外一个客体。

（3）控制策略 A（Attribution）是主体对客体的相关访问规则集合，即属性集合。访问策略体现了一种授权行为，也是客体对主体某些操作行为的默认。

7. 网络监控

网络监控，是针对局域网内的计算机进行监视和控制，Emulex 针对内部的计算机上互联网活动（上网监控）以及非上网相关的内部行为与资产等过程管理（内网监控）互联网的飞速发展，互联网的使用越来越普遍，网络和互联网不仅成为企业内部的沟通桥梁，也是企业和外部进行各类业务往来的重要管道。

8. 病毒防护

（1）经常进行数据备份，特别是一些非常重要的数据及文件，以避免被病毒侵入后无法恢复。

（2）对于新购置的计算机、硬盘、软件等，先用查毒软件检测后方可使用。

（3）尽量避免在无防毒软件的机器上或公用机器上使用可移动磁盘，以免感染病毒。

（4）对计算机的使用权限进行严格控制，禁止来历不明的人和软件进入系统。

（5）采用一套公认最好的病毒查杀软件，以便在对文件和磁盘操作时进行实时监控，及时控制病毒的入侵，并及时可靠地升级反病毒产品。

9. 电子加密

置乱技术是数据加密的一种方法。通过置乱技术，可以将数字信号变得杂乱无章，使非法获取者无法确知该数字信号的正确组织形式，无法从其中获得有用的信息。基于 DirectShow 对视频进行一系列的采集、分帧、合成等处理，同时采用 Arnold 变换对单帧图像进行置乱操作，使得置乱后的视频表现为黑白噪声的形式。所建立的视频处理框架可以处理各种格式的视频，如 AVI、MPEG 等格式的视频信号，置乱后的视频可以抵抗一定程度的压缩、帧处理等操作。

10. 数字水印

数字水印的基本思想是利用人类感觉器官的不敏感，以及数字信号本身存在的冗余，在图像音频和视频等数字产品中嵌入秘密的信息以便记录其版权，同时嵌入的信息能够抵抗一些攻击而生存下来，以达到版权认证和保护的功能。数字水印并不改变数字产品的基

本特性和使用价值。一个完整的数字水印系统应包含三个基本部分：水印的生成、嵌入和水印的提取或检测。水印嵌入算法利用对称密钥或公开密钥实现把水印嵌入到原始载体信息中，得到隐秘载体。水印检测 / 提取算法利用相应的密钥从隐蔽载体中检测或恢复出水印，没有解密密钥，攻击者很难从隐秘载体中发现和修改水印。

根据水印所附载体的不同，可以将数字水印划分为图像水印、音频水印、视频水印、文本水印和用于三维网格模型的网格水印及软件水印等。

笔记

任务 1.6　信息安全管理制度示例

信息安全涉及国家政府、军事、文教等诸多领域，存储、传输和处理众多信息是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要的信息。而维护信息安全，保证信息安全环境稳定，必先制定相关信息管理制度。下面通过三个具体的管理制度示例来了解信息安全管理的制度。

子任务 1.6.1　计算机管理制度示例

为保证计算机的正常运行，确保计算机安全运行，根据国家、省、市有关法律法规和政策规定，结合本项目部实际情况，制定本制度。计算机分为涉密和非涉密两类，涉密计算机指主要用于储存或传输有关人事、财务、经济运行、信息安全等涉及国家、单位秘密、危害国家安全的图文信息的计算机。非涉密计算机指用于储存或传输可以向社会公开发表或公布的图文信息的计算机。信息安全科、运行科、人事科和机关财务各一台计算机按照涉密要求进行管理。

（1）涉密的计算机内的重要文件由专人集中加密保存，不得随意复制和解密，未经加密的重要文件不能存放在与国际联网的计算机上。

（2）对需要保存的涉密信息，可到信息安全科转存到光盘或其他可移动的介质上。存储涉密信息的介质应当按照所存储信息的最高密级标明密级，并按相应密级的文件管理。

（3）存储过国家秘密信息的计算机媒体的维修应保证所存储的国家秘密信息不被泄露。对报废的磁盘和其他存储设备中的秘密信息由技术人员进行彻底清除。

（4）涉密的计算机信息如需打印输出必须到信息安全科专用打印机打印输出，打印出的文件应当按照相应密级的文件管理；打印过程中产生的残、次、废页应当及时在信息安全科专用设备粉碎销毁。

（5）对信息载体（软盘、光盘等）及计算机处理的业务报表、技术数据、图纸要有专人负责保存，按规定使用、借阅、移交、销毁。

子任务 1.6.2　机房管理制度示例

为确保计算机网络（内部信息平台）系统安全、高效运行和各类设备运行处于良好状态，正确使用和维护各种设备、管理有章、职责明确，特制定本制度。

（1）机房属重要涉密岗位，必须严格执行国家、省、市保密局有关保守国家秘密和密码工作的规定。

（2）严禁在网络服务器上安装一切与工作无关的软件。严禁将外来不明的磁盘、光

笔记

盘、软件在网络服务器上使用。严禁在网络上运行或传播一切法律法规禁止、有损国家机关形象以及涉及国家秘密、危害国家安全的软件或图文信息。

（3）无关人员不准进入机房，不准违规操作和使用机房设备，不准私自将机房设备带离机房。机关科（室）需借用机房设备的，机房工作人员必须上报，经分管领导同意，并办理有关登记手续后方可借出。

（4）做好机房设备的日常维护工作，严禁在机房内吸烟，不准在机房堆放杂物和垃圾，保持机房室内整洁。下班时，必须关闭不用的设备及电源，锁好机房门窗，方可离开。

子任务 1.6.3 网络安全管理制度示例

为加强局域网计算机及网络安全管理，确保网络安全稳定运行，切实提高工作效率，促进信息化建设的健康发展，现结合实际情况，制定本管理规定。信息化领导小组办公室是计算机及网络系统的管理部门，履行管理职能。

（1）未经网管批准，任何人不得改变网络（内部信息平台）拓扑结构、网络（内部信息平台）设备布置、服务器、路由器配置和网络（内部信息平台）参数。

（2）任何人不得进入未经许可的计算机系统更改系统信息和用户数据。

（3）机关局域网上任何人不得利用计算机技术侵占用户合法利益，不得制作、复制和传播妨害单位稳定的有关信息。

（4）各科室应定期对本科室计算机系统和相关业务数据进行备份以备发生故障时进行恢复。

知识拓展

信息安全大事件

2010 年，“维基解密”网站在《纽约时报》《卫报》和《镜报》配合下，在网上公开了多达 9.2 万份的驻阿富汗美军秘密文件，引起轩然大波。

2011 年，堪称中国互联网史上最大泄密事件发生。12 月中旬，CSDN 网站用户数据库被黑客在网上公开，大约 600 余万个注册邮箱账号和与之对应的明文密码泄露。2012 年 1 月 12 日，CSDN 泄密的两名嫌疑人被刑事拘留。

2013 年 6 月 5 日，美国前中情局（CIA）职员爱德华·斯诺登披露给媒体两份绝密资料。一份资料称美国国家安全局有一项代号为“棱镜”的秘密项目，要求电信巨头威瑞森公司必须每天上交数百万用户的通话记录。另一份资料更加惊人，美国国家安全局和联邦调查局通过进入微软、谷歌、苹果等九大网络巨头的服务器，监控美国公民的电子邮件、聊天记录等秘密资料。

2014 年 4 月 8 日，“地震级”网络灾难降临，在微软 XP 操作系统正式停止服务同一天，互联网筑墙被划出一道致命裂口——常用于电商、支付类接口等安全极高网站的网络安全协议 OpenSSL 被曝存在高危漏洞，众多使用 https 的网站均可能受到影响。在“心脏出血”漏洞逐渐修补结束后，由于用户很多软件中也存在该漏洞，黑客攻击目标存在从服务器转身客户端的可能性，下一步有可能出现“血崩”攻击。

2015 年，美国人事管理局 (OPM)2700 万政府雇员及申请人信息泄露；美国第二大医疗保险公司 Anth 谍软件公司 Hacking Team 被黑，包含多个零日漏洞、入侵工具和大量工作邮件及客户名单的 400G 数据被传到网上任意下载。

2016 年 10 月，黑客挟持成千上万物联网设备对美国 DNS 服务商 Dyn 发动了三波流量攻击，使得 Dyn 多个数据中心服务器受到影响，导致美国大部分网站都出现无法访问情况，包括亚马孙、Etsy、GitHub、Shopify、Twitter 、Netflix、Airbnb 等热门网站，此次的 DDoS 攻击让很多人觉得整个互联网都陷入了瘫痪。

2017 年 5 月，勒索病毒全面爆发，在十几个小时内，全球共有 74 个国家的至少 4.5 万台电脑中招。此类病毒可以归结为敲诈病毒，在一定时间内持续攻击用户电脑，一旦攻击成功，造成的损失无法抵挡，需要支付大额赎金才能恢复数据，当然也不排除支付赎金后被骗的情况发生。

2018 年，勒索软件的质量和数量不断攀升，成为网络攻击的一种新常态。我们将继续看到一些物联网设备被用于僵尸网络活动。不安全的设备仍有很多，对黑客们而言是极易攻击的目标。

2019 年 2 月，国内某人脸识别公司发生了大规模的数据泄露，预估泄露人脸数据达 250 万条，近 700 万条包含个人姓名、身份证号码、性别、家庭住址和照片等重要个人信息遭泄露。据悉，此公司利用深度学习和人工智能等技术在监控视频中用于人脸识别和人物画像分析。由于生物特征的唯一性，如人脸、虹膜、指纹等特征信息一旦泄露，后果非常严重。

2019 年 12 月，以《信息安全技术 网络安全等级保护基本要求》《信息安全技术 网络安全等级保护安全设计技术要求》《信息安全技术 网络安全等级保护测评要求》等相关标准为主要内容的“等保 2.0”正式实施。