湖北省技能高考理论基础知识

计算机类

第三章

信息安全基础

第三章　信息安全基础

目　录
上一页
下一页
结　束

3.1 信息安全的概念及技术

3.1.1 信息安全的概念

3.1.2 信息安全面临的威胁

3.1.3 信息安全技术

※ 3.1.4 信息隐藏技术

目 录
上一页
下一页
结 束
返 回

3.1.1 信息安全的概念

1.信息安全的定义：

- 信息安全是指信息系统的硬件、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，提供的信息服务不中断。
- 信息安全包括实体安全（硬件安全）、软件安全和数据安全三个方面。

目 录
上一页
下一页
结 束
返 回

3.1.1 信息安全的概念

- 实体安全又称为物理安全，是指保护计算机设备，设施以及其他媒体免遭自然灾害，人为破坏和环境威胁的措施或过程，它由环境安全、设备安全、媒体安全三部分组成。
- 软件安全是指系统运行安全，为了保障系统功能的安全实现，提供一整套安全措施来保护信息处理过程。它通常由风险分析、备份与恢复、应急措施等技术手段来提供保障。
- 数据安全，是指计算机中保存及流通的数据的安全，保护计算机网络中的数据不被篡改、非法增删、复制、解密、显示、使用等。数据安全是保障网络安全最根本的目的。
- 信息安全包括四大要素：技术、制度、流程和人，其中人是这些因素中最薄弱的环节。

3.1.1 信息安全的概念

2.信息安全的特征：

可靠性、可用性、保密性、完整性、不可抵赖性、可控制性、可审查性

- （1）可靠性:是指系统在规定的条件下和规定的时间内,完成规定的功能的概率。
- （2）可用性:是指得到授权的实体在需要时可以得到所需要的资源和服务。
- （3）保密性:确保信息不暴露给未授权的实体或进程,即信息的内容不会被未授权的第三方所知,强调有用信息只被授权对象使用的特征。

目 录
上一页
下一页
结 束
返 回

3.1.1 信息安全的概念

- （3）保密性:确保信息不暴露给未授权的实体或进程,即信息的内容不会被未授权的第三方所知,强调有用信息只被授权对象使用的特征。信息加密技术是保障信息安全保密性的最基本、最核心的技术措施。
- （4）完整性:信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失。保障信息完整性的技术主要有身份认证技术、权限管理技术、数字签名技术等。
- （5）不可抵赖性:是指在信息交互过程中,确信参与者的真实同一性,所有参与者都不可能否认或抵赖曾经完成的操作和承诺。实现不可抵赖性的技术主要有身份认证、数字签名、第三方认证技术等。保证交易过程中的不可抵赖性是电子商务安全需求中的一个重要方面。

目 录
上一页
下一页
结 束
返 回

3.1.1 信息安全的概念

- （6）可控制性:是指对信息的传播及内容具有控制能力,可以维持正确信息的正常传播,也可以随时阻止错误信息,虚假信息的传播。可控性是信息安全工作中最难实现的属性。
- （7）可审查性:对出现的信息安全问题提供调查的依据和手段，按照一定的安全策略,利用记录、系统活动和用户活动等信息,检查、审查和检验操作事件的环境及活动,发现系统漏洞、入侵行为或改善系统性能的过程；主要用于系统测试和评估，事后的追责等。

目 录
上一页
下一页
结 束
返 回

3.1.1 信息安全的概念

3.信息安全工作的目的

- （1）用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。
- （2）使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。
- （3）使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。
- （4）使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而保证信息的完整性。
- （5）使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

目 录
上一页
下一页
结 束
返 回

3.1.2 信息安全面临的威胁

1.人为因素

- **被动攻击** 主要是用于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也不会觉察到，是针对系统的**保密性**进行的攻击。

抵制这种攻击的重点在于预防而非检测。

被动攻击一般采用窃听、监听、嗅探、信息收集、通信流量分析、截获等手段。

- **主动攻击**攻击者采用删除、增加、重放、伪造等主动手段向密码通信系统注入假消息的攻击。主动攻击包括拒绝服务攻击（DoS）、分布式拒绝服务（DDos）、信息篡改、欺骗、伪装、重放等攻击方法。

3.1.2 信息安全面临的威胁

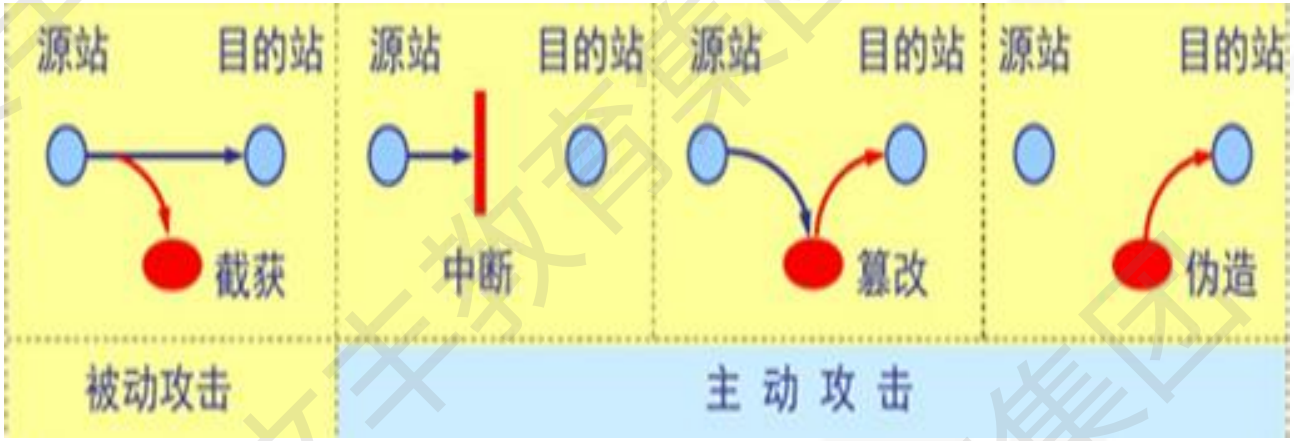

图3-1 被动攻击与主动攻击的区别

目 录
上一页
下一页
结 束
返 回

3.1.2 信息安全面临的威胁

2.技术因素

- **系统漏洞**由于软件程序的复杂性和编程的多样性，在网络信息系统的软件中很容易有意或无意地留下一些不易被发现的**系统漏洞**。**补丁**是专门修复这些**BUG**而设计的小程序
- **后门程序**一般是指那些绕过安全性控制而获取对程序或系统访问权的程序。
- 网络钓鱼其实就是网络上众多诱骗手法之中的一种，由于它的手段基本就是通过网络用一些诱饵（比如假冒的网站）等使用者上当，很像现实生活中的钓鱼过程，所以就被称之为“网络上的钓鱼”。

3.1.3 信息安全技术

一、数据加密技术

1.加密技术有关的概念

- 明文：指需要隐蔽的原始信息，明文可以被人们直接阅读，一般用P 表示。
- 密文：指加密后的报文，一般用C 表示。
- 密钥：加密算法和解密算法通常是在一组密钥控制下进行的。密钥一般用K 表示。加密算法所使用的密钥称为“加密密钥”；解密算法使用的密钥称为“解密密钥”。

3.1.3 信息安全技术

- 加密和解密：将“明文”的可读信息进行处理形成密码或“密文”的代码形式称为加密。加密的逆过程，即将“密文”或密码恢复成“明文”的过程称为“解密”。
- 加密算法和解密算法：对“明文”进行加密过程中使用的一组规则称为“加密算法”，一般用EK 表示；对密文进行解密过程中使用的一组规则称为“解密算法”，一般用DK 表示。
- 单钥加密：传统密码体制所用的加密密钥和解密密钥相同，或从一个可以推出另一个，被称为单钥或对称密码体制。
- 双钥加密：若加密密钥和解密密钥不相同，从一个难以推出另一个，则称为双钥或非对称密码体制。

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

2.目前流行的加密方法主要有：

对称加密和非对称加密算法、单向散列函数加密（Hash函数）。

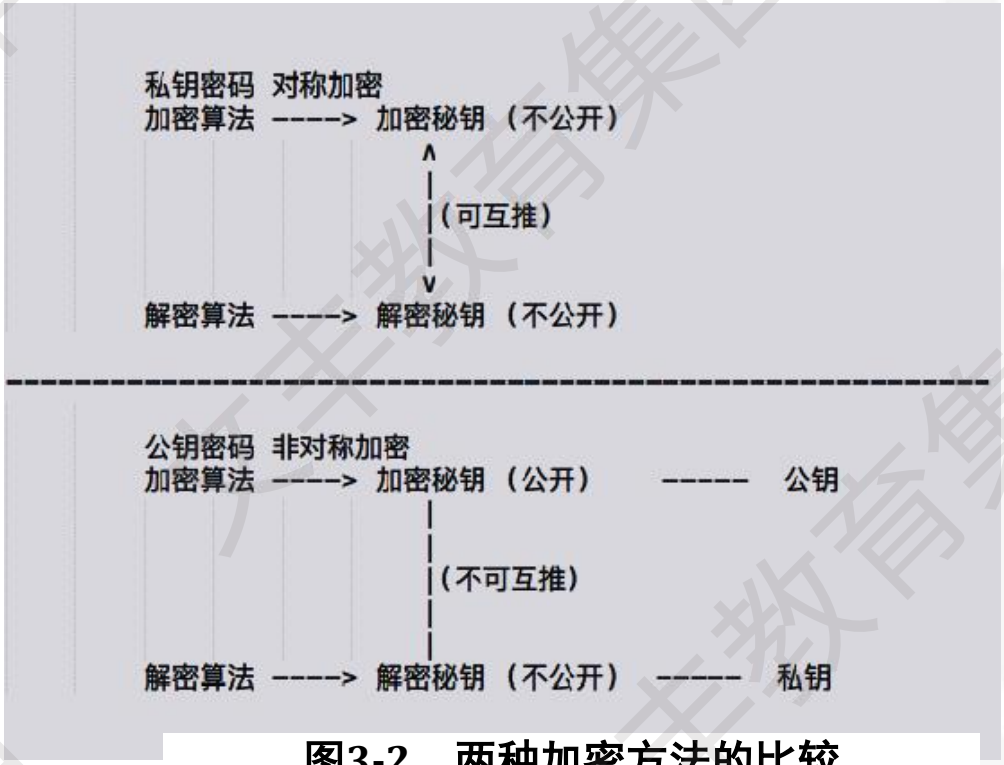

图3-2 两种加密方法的比较

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

（1）对称密钥加密

- 又称为私钥密钥加密或机密密钥加密。对称密钥加密的特征是：发件人用于加密和收件人用于解密的密钥是一样的或者很容易相互推出。
- 私钥的保密性必须基于密钥的保密，而非算法上。
- 对称密钥加密的典型算法是数据加密标准DES算法，是IBM公司1977年为美国政府研制的一种算法，以56位密钥为基础的密码块的加密技术。

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

（2）非对称密钥加密

- 又称为公钥加密。在公钥加密中，密钥被分解为一对（即一把公开密钥用于加密，一把专用密钥用于解密），在加密和解密过程使用不同的密钥。
- 该方式由解密密钥很容易计算出加密密钥，而由加密密钥很难甚至无法计算出解密密钥。
- 加密密钥公开，任何人均可使用加密密钥来加密消息，但只有拥有解密密钥的人才能解密消息。加密密钥称为公钥（Public Key），解密密钥又称为私钥（Private Key）。
- RSA系统是公钥系统的最具有典型意义的方法

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

（3）单向散列函数加密

- 又称为Hash函数、杂凑函数，是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。
- 著名的HASH加密算法有MD4、MD5和SHA1

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

二、身份认证

- 身份认证是证实主体的真实身份与其所声称的身份是否相符的过程
- 认证的目的：确保通信实体就是它所声称的那个实体，也就是鉴别用户身份
- 认证的作用：验证用户，对抗假冒；依据身份，实施控制；明确责任，便于审计

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

常用的身份认证方式有：

- 1.静态密码方式是指以用户名及密码认证的方式，是目前最简单最常用的身份认证方法。但是密码是静态不变的，容易被木马截获。
- 2.动态口令认证 动态口令是目前应用最广的一种身份识别方式,基于动态口令认证的方式主要有动态短信密码和动态口令牌(卡)两种方式,口令一次一密。比如现在很多的交易密码、登入密码等都使用手机短信进行动态密码验证。

3.1.3 信息安全技术

常用的身份认证方式有：

- 3.USB Key认证　采用软硬件相结合、一次一密的强双因素(两种认证方法)认证模式。
- 4.生物识别技术是指通过可测量的生物信息和行为等特征进行身份认证的一种技术。生物特征分为身体特征和行为特征两类，比如指纹识别、人脸识别、声音识别技术、视网膜识别技术等。

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

常用的身份认证方式有：

- 5.CA认证

CA（Certificate Authority）是证书授权的意思，是负责签发认证、管理证书的机构，是合法的、中立的、权威的、公正的第三方电子认证中心。CA给个人、企事业单位和政府机构签发数字证书，用来确认电子商务活动中各自的身份，并通过加密解密策略来实现网上安全的信息交换与安全交易。

CA认证技术的具体作用有：

（1）维护数据的保密性

（2）验证双方身份的真实性

（3）保证信息的完整性

3.1.3 信息安全技术

三、数字签名

- 数字签名是以电子形式存储于信息中或以附件或逻辑上与之有联系的数据，用于辨识数据签署人的身份，并表明签署人对数据中所包含信息的认可。
- 数字签名的功能：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖行为发生等。
- 数字签名算法主要有两部分组成：签名算法和验证算法。
- 数字签名算法标准：DSS（Digital Signature Standard）美国政府用来指定数字签名算法的一种标准。
- 目前常用的数字签名算法有RSA、DSA、ECDSA等。

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

三、数字签名

- 数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。
- 接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用HASH函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。
- 数字签名是个加密的过程，数字签名验证就是个解密的过程

目 录
上一页
下一页
结 束
返 回

3.1.3 信息安全技术

四、访问控制

- 定义：访问控制是指主体依据某些控制策略或权限对客体或其资源进行的不同授权访问。

解释：访问控制的目的是决定谁能够访问系统，能访问系统的何种资源以及访问这些资源时所具备的权限，是实现数据保密性和完整性机制的主要手段。

- 访问控制有两个重要过程：

(1)通过“鉴别”来检验主体的合法身份；

(2)通过“授权”来限制用户对资源的访问级别。

3.1.3 信息安全技术

四、访问控制

访问控制的类型有3种模式

- （1）自主访问控制DAC（Discretionary Access Control）

  主体对它所属的对象和运行的程序拥有全部的控制权。

- （2）强制访问控制MAC（Mandatory Access Control）

  管理员管理访问控制。管理员制定策略，用户不能改变它，策略定义了哪个主体能访问哪个对象。

- （3）基于角色的访问控制RBAC（Rule-Based Role-Based Access Control，RB-RBAC） 基于角色的访问控制是通过对角色的访问所进行的控制，使权限与角色相关联，用户通过成为适当角色的成员而得到其角色的权限，可极大地简化权限管理。

3.1.3 信息安全技术

四、访问控制

访问控制安全策略遵循的原则

- (1)最小特权原则；

  在主体执行操作时，按照主体所需权利的最小化原则分配给主体权力。

- (2)最小泄露原则；

  主体执行任务时，按其所需最小信息分配权限，以防泄密。

- (3)多级安全策略；

目 录
上一页
下一页
结 束
返 回

※ 3.1.4 信息隐藏技术

- 信息隐藏技术是利用载体信息的冗余性，将秘密信息隐藏于普通信息之中，通过普通信息的发布而将秘密信息发布出去，即将重要的信息隐藏于其它信息里面从而掩饰它的存在。
- 信息隐藏技术在现实中的应用主要有以下五个方面：（1）数据保密，（2）数据的不可抵赖性，（3）数据的完整性，（4）数字作品的版权保护，（5）防伪。
- 信息隐藏具有鲁棒性、不可检测性、透明性、安全性和自恢复性等特征。

目 录
上一页
下一页
结 束
返 回

3.2 网络安全与防火墙技术

3.2.1 网络安全的概念

3.2.2 防火墙技术

※3.2.3 虚拟专用网络(VPN)

3.2.4 黑客

3.2.5 木马

目 录
上一页
下一页
结 束
返 回

3.2.1 网络安全的概念

3.2.1 网络安全

计算机网络安全是指利用网络管理控制技术防止网络本身及网上传输的信息故意的或偶然的非授权泄露、更改、破坏、或使信息被非法系统辨认、控制。

1. 目前计算机网络安全存在的一些问题

- （1）系统漏洞
- （2）黑客入侵
- （3）计算机病毒的攻击
- （4）间谍软件的攻击
- （5）人为泄密

3.2.1 网络安全的概念

2.局域网攻击

局域网攻击是指攻击者利用局域网的一些机制攻击局域网内的其他用户。通常有ARP欺骗、DNS欺骗、NetBIOS名称欺骗、LLMNR欺骗和系统漏洞攻击等方式，以ARP欺骗攻击最为流行。

3.Internet网络常见攻击手段

Internet网络攻击常见手段有间谍软件、恶意流氓软件、垃圾邮件和Cookies文件泄密等。

目 录
上一页
下一页
结 束
返 回

3.2.2 防火墙技术

1. 防火墙的概念和功能

- 防火墙是一个由软件和硬件设备组合而成，在内部网和外部网之间、专用网与公共网之间构造的一个保护屏障，它是在Internet与Intranet之间建立起的一个安全网关(Scurity Gateway)，从而保护内部网免受非法用户的侵入。
- 防火墙应该具有以下功能:

（1）所有进出网络的通信流都应该通过防火墙；

（2）所有穿过防火墙的通信流都必须有安全策略的确认与授权。

3.2.2 防火墙技术

防火墙技术的弱点：

- 1. 防火墙可以阻断攻击，但不能消灭攻击源；
- 2. 防火墙不能抵抗最新的未设置策略的攻击漏洞；
- 3. 防火墙的并发连接数限制容易导致拥塞或者溢出；
- 4. 防火墙对服务器合法开放的端口的攻击大多无法阻止；
- 5. 防火墙对待内部主动发起连接的攻击一般无法阻止；
- 6. 防火墙本身也会出现问题和受到攻击；
- 7. 防火墙不处理病毒，但是有些防火墙可以过滤某些病毒。

目 录
上一页
下一页
结 束
返 回

3.2.2 防火墙技术

2. 防火墙的类型

- 基本型防火墙和复合型防火墙。
- 基本型防火墙包括包过滤防火墙和应用代理型防火墙；

包过滤防火墙可以用一般的路由器来实现，工作在OSI参考模型的网络层，利用IP地址进行数据包的过滤。

应用代理型防火墙，采用协议代理服务器来实现，一般是主机上运行的一个特殊程序。

- 复合防火墙将以上两种基本型防火墙结合使用，主要包括主机屏蔽防火墙和子网屏蔽防火墙。

主机屏蔽防火墙：一个应用型防火墙+一个包过滤防火墙

子网屏蔽防火墙：两个包过滤防火墙+一个应用型防火墙

※3.2.3　虚拟专用网络(VPN)

VPN的英文全称是“Virtual Private Network”　虚拟专用网络

VPN的功能是：在公用网络上建立专用网络，进行加密通讯

- (1)数据机密性保护,即在传输过程中对数据进行加密。数据机密性保护的传输过程
- (2)数据完整性保护,即在数据通信的接收端具有对接收到的数据进行数据包完整性校验。
- (3)数据源身份验证,是指VPN通信中在接收端可以验证确认收到的数据包是否是拥有权限的发送端发送的,主要是防止网络中的伪装攻击等事件。

目 录
上一页
下一页
结 束
返 回

※3.2.3　虚拟专用网络(VPN)

VPN的优点：

- (1)降低费用
- (2)增强的安全性
- (3)易用性
- (4)IP地址安全　　由于VPN是加密的,VPN数据包在Internet中传输时,Internet上的用户只看到公用的IP地址,看不到数据包内包含的专有网络地址,因此,远程专用网络上指定的地址是受到保护的。

目 录
上一页
下一页
结 束
返 回

3.2.4 黑客

- 黑客这个名词用来指入侵他人计算机系统，进行不法行为的计算机高手。
- 黑客的几种攻击手段：1.获取口令；2.放置特洛伊木马程序；3.WWW的欺骗技术；4.电子邮件攻击；5.通过一个节点来攻击其他节点；6.网络监听；7.寻找系统漏洞；8.利用帐号进行攻击；9.偷取特权。
- 入侵检测系统（intrusion detection system，简称“IDS”）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。

目 录
上一页
下一页
结 束
返 回

3.2.5 木马

- 木马是目前比较流行的计算机病毒，是一种基于远程控制的黑客工具
- 与一般的计算机病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件。
- 它通过将自身伪装，吸引用户下载执行，向施种木马者提供一个打开的被种主机的门户（端口，port），使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。
- 一般的计算机病毒重在破坏电脑的软硬件，而木马的重心则在于控制，也就是说控制电脑系统。

目 录
上一页
下一页
结 束
返 回

3.2.5 木马

木马的结构

- 一个完整的特洛伊木马程序包含了两部分：服务端（服务器部分，隐藏在感染了木马的用户机器上）和控制端（控制器部分，一般由黑客控制）。

运用木马进行网络入侵的基本过程

- 第一步，配置木马　　第二步，传播木马
- 第三步，运行木马　　第四步，信息泄露
- 第五步，建立连接　　第六步，远程控制

3.3 计算机病毒及防治

3.3.1 计算机病毒的概念及特征

3.3.2 计算机病毒的分类与命名

3.3.3 蠕虫病毒

目 录
上一页
下一页
结 束
返 回

3.3.1 计算机病毒的概念及特征

1. 计算机病毒的定义

- 在《中华人民共和国计算机信息系统安全保护条例》中明确定义，计算机病毒(Computer Virus)是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。

2. 计算机病毒的特征

- （1）传染性　　（2）隐蔽性
- （3）表现性（破坏性）　　（4）寄生性与潜伏性
- （5）可触发性　　（6）衍生性

3.3.1 计算机病毒的概念及特征

3. 计算机病毒的症状

- （1）机器不能正常启动
- （2）运行速度降低
- （3）存储空间迅速变小
- （4）文件内容和长度有所改变
- （5）经常出现“死机”现象
- （6）外部设备工作异常

4. 计算机病毒的结构

- 整个病毒代码虽短小但也包含四个部分：感染标志，引导模块，传染模块，表现模块(或称为破坏模块)。

3.3.1 计算机病毒的概念及特征

5. 计算机病毒的传播

- 最容易传播病毒的途径是通过计算机网络进行传播，其次是通过移动存储设备来传播
- 常用的反病毒软件

国外：美国赛门铁克公司的Norton Antivirus（诺顿）、McAfee（迈克菲）、PC-cillin（趋势），俄罗斯的Kaspersky（卡巴斯基）Anti-Virus（芬兰），斯洛伐克的NOD32等产品在国际上口碑较好

国内：瑞星、金山毒霸、KV3000（江民）、KILL，360安全卫士（奇虎）、QQ电脑管家等。

3.3.1 计算机病毒的概念及特征

6. 计算机病毒的清除

检测病毒的方法通常有四种

- （1）特征代码法
- （2）校验和法
- （3）行为监测法
- （4）软件模拟法

目 录
上一页
下一页
结 束
返 回

3.3.2 计算机病毒的分类与命名

1.按传染方式分为三种：

- 引导型病毒、文件型病毒、混合型病毒

2.按入侵途径分类，可以分为源码病毒、操作系统病毒、入侵病毒和外壳病毒等4种。

3.按计算机病毒的破坏性可分为：良性病毒和恶性病毒。

- 宏病毒是一种寄存在office文档或模板的宏中的计算机病毒。
- 脚本病毒是主要采用脚本语言设计的计算机病毒。现在流行的脚本病毒大都是利用JavaScript和VbScript脚本语言编写。脚本在现在的应用系统中特别是Internet应用中占据了重要地位，脚本病毒也成为互联网病毒中最为流行的网络病毒。

目 录
上一页
下一页
结 束

3.3.2 计算机病毒的分类与命名

计算机病毒命名的方法

- 一般格式为：〔前缀〕·〔病毒名〕·〔后缀〕

1.病毒前缀

- 病毒前缀是指一个病毒的种类，我们常见的有Script（代表脚本病毒）、Trojan（代表木马病毒）、Worm（代表蠕虫病毒）、Harm（代表破坏性程序）、Macro／WM／WM97／XM／XM97（代表宏病毒）、Win32／W32（代表系统病毒），一般DOS类型的病毒是没有前缀的。

2.病毒名　病毒名是指一个病毒名称

3.病毒后缀　病毒后缀是指一个病毒的变种特征，一般是采用英文中的26个字母来表示的。

3.3.3 蠕虫病毒

- 蠕虫病毒是一种常见的计算机病毒，它的病毒名称前缀是：Worm。它利用网络或者系统漏洞进行复制和传播，是一种通过网络传播的恶性病毒。
- 蠕虫病毒区别于普通病毒的特征：不利用文件寄生(有的只存在于内存中)，对主机或网络造成拒绝服务攻击，和黑客技术相结合等等。

目 录
上一页
下一页
结 束

3.3.3 蠕虫病毒

表3-1 蠕虫病毒与普通病毒的对比

	普通病毒	蠕虫
存在形式	寄生	独立个体
复制机制	插入到宿主程序（文件）中	自身的拷贝
传染机制	宿主程序运行	系统存在漏洞
搜索机制（传染目标）	主要是针对本地文件	主要是针对网络上的其他计算机
触发机制	计算机使用者	程序自身
影响重点	文件系统	网络性能、系统性能
计算机使用者角色	病毒传播中的关键环节	无关
防治措施	从宿主程序中清除	为系统打补丁

目 录
上一页
下一页
结 束

3.4 社会信息道德

3.4.1 计算机犯罪

3.4.2 网络道德

目 录
上一页
下一页
结 束

3.4.1 计算机犯罪

计算机犯罪是指行为人以计算机作为工具或以计算机资产作为攻击对象实施的严重危害社会的行为。计算机犯罪的特点：

- （1）犯罪智能化
- （2）犯罪隐蔽性
- （3）跨国性
- （4）匿名性
- （5）犯罪分子低龄化和内部人员多
- （6）犯罪后果严重

目 录
上一页
下一页
结 束

3.4.2 网络道德

网络道德是指以善恶为标准，通过社会舆论、内心信念和传统习惯来评价人们的上网行为，调节网络时空中人与人之间以及个人与社会之间关系的行为规范。

网络道德的基本原则

- （1）全民原则
- （2）兼容原则
- （3）互惠原则
- （4）自由原则

网络道德的特征：自主性、开放性、多元性。

目 录
上一页
下一页
结 束

3.5 版权与知识产权

3.5.1 知识产权的概念

3.5.2 计算机软件的知识产权

目 录
上一页
下一页
结 束

3.5.1 知识产权的概念

1. 定义

- 知识产权，指“权利人对其所创作的智力劳动成果所享有的专有权利”，一般只在有限时间期内有效。

2. 知识产权的特点

- （1）知识产权是一种无形财产
- （2）双重性：知识产权包括财产权和人身权的双重内容
- （3）知识产权具备专有性的特点
- （4）知识产权具备时间性的特点
- （5）知识产权具备地域性的特点
- （6）知识产权的获得需要法定的程序

目 录
上一页
下一页
结 束

3.5.2 计算机软件的知识产权

1. 定义

- 软件著作权包括人身权和财产权，人身权是指发表权、开发者身份权；财产权是指使用权、使用许可和获得报酬权、转让权。

2. 软件著作权的保护期限

- 《计算机软件保护条例》第十四条　　软件著作权自软件开发完成之日起产生。
- 自然人的软件著作权，保护期为自然人终生及其死亡后50年，截止于自然人死亡后第50年的12月31日；软件是合作开发的，截止于最后死亡的自然人死亡后第50年的12月31日。
- 法人或者其他组织的软件著作权，保护期为50年，截止于软件首次发表后第50年的12月31日，但软件自开发完成之日起50年内未发表的，本条例不再保护。

目 录
上一页
下一页
结 束

3.5.2 计算机软件的知识产权

3. 软件著作权人的确定

- 第九条　软件著作权属于软件开发者，本条例另有规定的除外。如无相反证明，在软件上署名的自然人、法人或者其他组织为开发者。
- 第十条　由两个以上的自然人、法人或者其他组织合作开发的软件，其著作权的归属由合作开发者签订书面合同约定。
- 第十一条　接受他人委托开发的软件，其著作权的归属由委托人与受托人签订书面合同约定；无书面合同或者合同未作明确约定的，其著作权由受托人享有。
- 第十二条　由国家机关下达任务开发的软件，著作权的归属与行使由项目任务书或者合同规定；项目任务书或者合同中未作明确规定的，软件著作权由接受任务的法人或者其他组织享有。

目 录
上一页
下一页
结 束

3.5.2 计算机软件的知识产权

4. 软件著作的“合理”使用许可

- 因课堂教学、科学研究、国家机关执行公务等非商业性目的的需要对软件进行少量的复制，可以不经软件著作权人或者其合法受让者的同意，不向其支付报酬。但使用时应当说明该软件的名称、开发者，并且不得侵犯著作权人或者其合法受让者依本条例所享有的其它各项权利。该复制品使用完毕后应当妥善保管、收回或者销毁，不得用于其它目的或者向他人提供。

目 录
上一页
下一页
结 束

3.5.3 软件版权的保护级别

- 1. 原版软件　享有完整保护权限。
- 2. 共享软件　免费分发的定期限试用软件，试用到期后购买使用权或停用，仅限试用，禁止牟利分发。
- 3. 免费软件　免费分发、免费使用的弱保护软件。
- 4. 自由软件　被版权所有者明确放弃作品财产权的、可以被任何人自由使用的软件。
- 绿色软件：是指不用安装，下载后直接可以使用的软件，删除后不留下任何痕迹，多数为免费软件。

目 录
上一页
下一页
结 束

谢谢使用！

目 录
上一页
下一页
结 束