信息安全特性：

保密性

完整性

可用性

可控性

可审查性

安全威胁：黑客技术，病毒技术

DDoS攻击（分布式拒绝服务攻击）、APT攻击（高级持续性威胁攻击）

ISO安全体系结构：

安全服务：

五大类安全服务：

认证：实体认证、数据源认证

访问控制服务：防止非授权访问

数据保密性服务

数据完整性服务

不可否认（不可抵赖）性服务

安全机制：

八大类安全机制：

加密机制

数字签名机制

访问控制机制

数据完整性机制

鉴别交换机制

业务填充机制

路由控制机制

公证机制

安全管理：

三大管理：

系统安全管理

安全服务管理

安全机制管理

PDRR模型：

Protection主要内容：

加密机制、数字签名机制、访问控制机制、认证机制、信息隐藏、防火墙技术等

Detection 主要内容：

入侵检测、系统脆弱性检测、数据完整性检测、攻击性检测等

Recovery 主要内容：

数据备份、数据修复、系统回复等

Response 主要内容：

应急策略、应急手段、应急机制、入侵过程分析、安全状态评估等

PPDR模型（基于时间的安全模型、可量化、可证明）：  
Polocy（安全策略）、Protection（防护）、Detection（检测）、Response（响应）

安全 = 风险分析 + 执行策略 + 系统实施 + 漏洞检测 + 实时响应

Pt>Dt+Rt

Pt:防护时间 Dt:检测时间 Rt:响应时间

Et>Dt+Rt

Et:暴露时间

安全的定义：及时地检测和响应、及时地检测和恢复

TCSEC标准（7个级别，安全级别越高可信度越高）：

D级：无保护级

C级：自主保护级

C1为机动安全保护，C2为控制访问保护

B级：强制保护级

B1为标签安全、B2为结构保护、B3为安全域

A级：验证保护级

ITSEC标准（欧洲）

CTCPEC评价标准（加拿大）

FC（美国联邦准则）

CC标准（联合公共准则）

BS7799标准（英国）

计算机信息系统安全保护等级划分准则（中国）：

五个等级：

自主保护级

系统审计保护级

安全标记保护级

结构化保护级

访问验证保护级

密码体制组成部分：

1. 明文空间P（Plaintext）
2. 密文空间C（Ciphertext）
3. 密钥空间K（Key）
4. 加密算法E（Encryption）
5. 解密算法D（Decode）

古典密码体系处理方法：替换和置换

现代密码体系处理方法：算法本身

对称密码机制特点：

优点：加密、解密处理速度快，保密度高

缺点：

1. 密钥分发过程复杂，代价高、
2. 多人通信密钥组合数量大
3. 必须统一密钥才能发送保密信息
4. 数字签名困难

常见对称加密机制：

DES算法：

长度：56位

特点：

1. 分组加密算法，已64位分组
2. 对称算法
3. 有效密钥长度：56位
4. 先代替后置换
5. 易于实现

IDEA算法（安全）

长度：64位

密钥：128位

AES算法

长度：128位

密钥：可变（128，192，256）

常见非对称加密机制：

RSA密码

安全性：基于分解大整数的困难性假定

Diffie-Hellman密钥交换协议

EIGamal公钥密码技术

密钥类型：

密钥层次结构参考P68 图3-1

会话密钥：两个通信终端用户一次通话或交换数据时使用的密钥。

特点：位于密码系统的最底层，仅对临时通话或交换数据使用。

密钥加密密钥（次主密钥、二级密钥）

主密钥：

位于最高层

作用：对密钥加密密钥、会话密钥或其他下层密钥的保护

密钥的保密存储方法：

基于密钥的软保护

基于硬件的物理保护

按照密钥层次结构分类：

1. 基本密钥
2. 会话密钥
3. 密钥加密密钥
4. 主机主密钥
5. 公钥体制下，由公开密钥、秘密密钥、签名密钥之分

三级密钥：用于数据加密的密钥

二级密钥（密钥加密密钥）：保护三级密钥

一级密钥（密钥保护密钥）：保护二级密钥

密钥生存期越短，越危险，理论上来说一级密钥最安全

密钥分割：

1. 不同密级的数据之间
2. 不同业务部门、业务系统之间
3. 上下级机关之间
4. 应用系统和管理系统之间

实现方式：

静态分割：在注入密钥时给定密钥连通范围，只能使用注入的密钥

动态分割：密钥分配中心定期向规定范围内的用户加密传送一个用于控制分配范围的密钥，收到什么，使用什么

密钥主要经历的阶段：

1. 生成（可能会登记）
2. 分配
3. 使用
4. 更新
5. 替换
6. 撤销
7. 销毁

密钥管理主要过程：密钥的生成、保护、分发

密钥的生成方式：

在安全环境下（防止对密钥的非授权访问）分为：

1. 由中心集中分配（有边界生产）
2. 个人分散生产（无边界生产）

密钥的存储：

1. 专用媒体（软盘、芯片）
2. 用对方的公钥建立密钥环，各自分散保存（PGP）
3. 公钥存放在公用媒体中（KDC）

密钥备份：在密钥使用期内，存储一个受保护的拷贝，用于恢复遭到破坏的密钥

密钥恢复：当密钥由于某种原因被破坏，在还未泄露之前，从它的备份重新得到密钥

密钥分配方法：

1. 由A选定，通过物理方法传递给B
2. 可信赖的第三方C选取并通过物理方法发送给A,B
3. A,B实现已有密钥，一方选取新密钥，用已有密钥加密新密钥发送给对方
4. A,B都有一个可信赖的第三方C的保密信道，C可选取密钥发给A,B
5. A,B在可信赖的第三方C发布自己的公钥，用彼此公钥进行保密通信

具体的见P74

集中式密钥分配方案：KDC

分布式密钥分配方案

消息摘要：输入相同的明文数据，经过相同的信息摘要算法会得到相同的、唯一的一组数据

一种保证明文无法篡改、完整性的算法

主要特点：

1. 长度固定
2. 随机性
3. 输入不同消息摘要不同，输入相同消息摘要相同
4. 单向性，明文—>消息摘要
5. 算法越好，碰撞越少

Hash函数

特点：定长、单向、抗碰撞

数字签名

特点：

1. 可信性
2. 不可伪造性
3. 不可复制性
4. 完整性（不可改变）
5. 不可抵赖性

完整过程：签名和鉴别

步骤：P85 图4-3

分类：

1.直接方式 2.仲裁方式

认证技术：

安全技术：

标识：代表实体的身份，确保实体在系统中唯一性和可辨认性

鉴别：对实体身份真实性进行识别

认证信息类型：

1. 所知道的
2. 所拥有的
3. 生物特征信息
4. 上下文信息

认证分类：

1. 单向
2. 双向
3. 第三方

认证方法：

what are you know

what you have

who you are

认证形式：

1. 静态密码
2. IC卡
3. 短信密码
4. 动态口令牌
5. USB Key
6. 数字签名
7. 生物识别技术
8. 双因素身份认证

Kerberos：（采用对称密钥加密技术）

设计目标：

1. 安全性
2. 可靠性
3. 用户透明性
4. 可伸缩性

基本实体：

1. Kerberos客户机
2. 认证服务器（AS）
3. 票据许可服务器（TGS）
4. 应用服务器

AS和TGS统称为KDC

认证过程：P95 图4-8

PKI：

定义：公钥基础设施，是指公开密钥的概念和技术来实施和提供安全服务的具有普适性的安全基础设施。

X.509中为有别于权限管理基础设施（PMI），定义为支持公开密钥管理并能支持认证、加密、完整性和可追究性服务的基础设施。

安全服务：

1. 认证，采用数字签名技术
2. 完整性，采用数字签名和消息认证码或MAC（对称发呢组木马或密码杂凑函数）
3. 机密性，采用类似于完整性服务的机制
4. 不可否认性，数字签名

系统组成：

1. PKI策略
2. 软硬件系统
3. 证书认证中心（CA）
4. 注册机构（RA）
5. 证书发布系统
6. PKI应用

信任基础：

证书认证中心CA：

作用：发放证书、规定证书的有效期和通过发布证书废除列表（CRL）确保必

要时可以废除证书。

CA签发证书作用：用户身份和公钥进行捆绑

CRL：警告其他用户不要再使用这个公钥（证书撤销）所使用的方法

数字证书

权威性电子文档，是由具有权威性、可信任性及公正性的第三方机构（CA）所颁发的。

具体表示：

CA《A》= CA{V,SN,AI,CA,UCA,A,UA,Ap,TA}

V：证书版本号

SN：证书序列号

AI：签名算法标识符

UCA：CA 可选唯一标识符

UA：用户A可选唯一标识符

Ap：A的公钥

TA：证书有效期

内容：

证书版本号：X.509证书格式版本

证书序列号

签名算法标识符

签发机构名

有效期

证书用户名

持有者公开密钥信息

签发着唯一标识符

持有者唯一标识符

签名值

生命周期：生产，使用，存储，更新，撤销

漏洞（脆弱性）：计算机系统安全方面的缺陷，使系统或应用数据保密性、完整性、可用性、访问控制等面临威胁。

POC：对某些想法的一个较短而不完整的实现，以证明其可行性，示范其原理，其目的使验证一些概念或理论。

零日漏洞：还没有补丁的安全漏洞，零日攻击指利用这种漏洞的攻击

攻击第一个步骤：信息收集

ARP欺骗：

分类：1.对路由器ARP cache表 2.对内网PC的网关

主要原因：

1. 设计之初没考虑安全问题
2. 无状态性
3. 缓存未进行定时更新

防范：

1. 网关建立静态IP/MAC对应关系，各主机建立MAC数据库
2. 建立DHCP服务器
3. IDS监听网络安全

社会工程学：黑客心理学应用，利用的是人而不是系统、软件或网络协议漏洞

口令攻击：

主动口令攻击：

1. 字典攻击
2. 强力攻击
3. 组合攻击

被动口令攻击：

1. 网络数据流监听
2. 重放
3. 钓鱼攻击

防范：

1. 选择安全密码
2. 防止口令猜测攻击
3. 设置安全策略：
4. 强制密码历史
5. 密码最长使用期限
6. 密码最短使用期限
7. 密码长度最小值
8. 采用加密通信协议
9. 使用软键盘输入口令

拒绝服务攻击：攻击者想办法让目标机器停止提供服务或资源访问

服务：系统提供，用户需求的功能

拒绝服务（DoS）：任何对服务的干涉，使得其可用性降低或失去可用性

拒绝服务攻击：造成DoS的攻击行为

目的：使计算机或网络无法提供正常服务

分布式拒绝服务攻击（DDoS）：攻击发出点是分布式的

恶意代码：故意执行危害信息安全的恶意任务的代码

常见类型：

1. 蠕虫病毒：

可复制，可独立程序，自动运行

1. 逻辑炸弹
2. 特洛伊木马：

可独立程序，服务端（放入目的地），控制器（客户）端

1. 漏洞
2. 下载器
3. 玩笑程序

危害：

1. 破坏数据
2. 占用磁盘存储空间
3. 抢占系统资源
4. 影响计算机运行速度

生存周期：程序设计-传播-感染-触发-运行-消亡

触发机制：

1. 日期
2. 时间
3. 键盘
4. 感染
5. 启动
6. 访问磁盘次数
7. 调用中断功能
8. CPU/主板型号

病毒命名规则：

<病毒前缀>,<病毒名>,<病毒后缀>

常见病毒前缀：

系统病毒：Win32、PE、Win95、W32、W95

蠕虫病毒：Worm

木马病毒：Trojan

脚本病毒：Script

宏病毒：Macro

后门病毒：Backdoor

病毒种植程序病毒：Dropper

破坏性程序病毒：Harm

玩笑病毒：Joke

捆绑机病毒：Binder

访问控制技术：

访问控制：针对越权使用资源的防御措施

策略：

1. 自主访问控制（DAC）:基于身份的访问控制（IBAC），根据主题的身份及允许访问的权限进行决策

特点：灵活性高，大量采用

缺点：安全性最低

分类：1.基于个人 2.基于组

1. 强制访问控制（MAC）：基于规则的访问控制（RBAC），对安全属性的划分
2. 基于角色的访问控制（RBAC）
3. 多级策略：
4. 最高秘密级
5. 秘密级
6. 机密级
7. 无级别级

实现方法：

1. 访问控制表（ACL）
2. 访问能力表
3. 安全标签
4. 基于口令的机制

防火墙：设置在被保护网络和外部网络之间的一道屏障，是不同网络或网络安全域之间信息的唯一出入口。

作用：用来阻断来自外部的本网络的威胁和入侵，保护本网络的安全

三块网卡连接：

1. 内网（受信网络）
2. 外网（非受信网络）：Internet
3. 非军事区（DMZ）：存放向外提供服务的服务器

功能：

1. 网络安全的保障
2. 控制对主机系统的访问
3. 强化网络安全策略（集中安全性）
4. 对网络的存取和访问进行监控审计

附加功能：

NAT：网络地址翻译

VPN：虚拟专用网

缺点：

1. 不能防范来自内部网络的攻击
2. 不能防范不经由防火墙的攻击
3. 不能防范感染了病毒的软件或文件的传输
4. 不能防范利用标准网络协议中的缺陷进行的攻击
5. 不能防范利用服务器系统漏洞进行的攻击
6. 不能防范新的网络安全问题
7. 限制了有用的网络服务

基本结构：

1. 屏蔽路由器
2. 双宿主机防火墙
3. 屏蔽主机防火墙（分单目和多目壁垒）
4. 屏蔽子网防火墙

防火墙类型（顺序优先）：

1. 数据包过滤防火墙
2. 代理网关：

应用层网关（代理服务器）：

优点：

1. 支持可靠用户认证，提供详细注册信息
2. 过滤规则更容易配置和测试
3. 详细的日志和安全审计功能
4. 隐藏内网IP地址，保护内部主机
5. 解决合法IP地址不够用的问题

缺点：

1. 有限的连续性
2. 有限的技术
3. 性能下降
4. 应用程序必须有代理服务程序安全控制
5. 必须安装软件
6. 状态检测

入侵检测技术：通过收集操作系统、系统程序、应用程序、网络包等信息，发现系统中违背安全策略或危及系统安全的行为

分类：

1. 基于误用：依赖于攻击模式库，会漏包
2. 基于异常：构造异常行为集合，会出错

入侵检测系统：

组成：

1. 数据采集模块
2. 入侵分析引擎模块
3. 应用处理模块
4. 管理配置模块
5. 辅助模块

分类：

1. 基于主机
2. 基于网络
3. 分布式

网路态势感知：通过收集系统网络环境中各种安全要素信息，并对这些信息进行数据融合分析后，能够对系统网络的态势有一个整体上的认知，同时能够对系统网络安全一段时间内的安全趋势进行预测的过程。

VPN：通过一个公共网络（Internet）建立一个临时的、安全的连接，一条穿过混乱的公共网络的安全稳定的隧道。0

作用：

1. 实现远程用户访问
2. 实现网络互联
3. 连接企业内部网络计算机

特点：

1. 安全保障
2. 服务质量保障（QoS）
3. 可扩充性和灵活性
4. 可管理性

主要技术：

1.隧道技术：通过使用互联网络的基础设施再网络之间传递数据的方式。

分类：

1. 第二层隧道：数据链路层利用ATM或Frame Replay技术来实现
2. 第三层隧道：使用包作为数据交换单位
3. 会话层隧道

2.安全技术

建立方式：

1. Host对Host
2. Host对VPN网关
3. VPN网关对VPN网关
4. Remote User对VPN网关