**第一章 信息安全保障概述**

**1.1信息安全保障背景**

1.1.1信息技术及其发展阶段

**信息技术两个方面**：生产：信息技术产业；应用：信息技术扩散

**信息技术核心**： 微电子技术，通信技术，计算机技术，网络技术

**信息技术的发展阶段：**

第一阶段，电讯技术的发明；第二阶段，计算机技术的发展；第三阶段，互联网的使用

1.1.2**信息技术的影响**

积极：社会发展，科技进步，人类生活

消极：信息泛滥，信息污染，信息犯罪

**1.2信息安全保障基础**

1.2.1

**信息安全发展阶段**

1.通信保密阶段（20世纪四十年代）：机密性，密码学

2.计算机安全阶段（20世纪六十和七十年代）：机密性、访问控制与认证，公钥密码学（Diffie Hellman，DES），计算机安全标准化（安全评估标准）

3.信息安全保障阶段：信息安全保障体系（IA），

PDRR模型：保护（protection）、检测（detection）、响应(response)、恢复（restore），我国PWDRRC模型：保护、预警（warning）、监测、应急、恢复、反击（counter-attack），BS/ISO 7799标准（有代表性的信息安全管理体系标准）：信息安全管理实施细则、信息安全管理体系规范

1.2.2

**信息安全的含义**

一是 运行系统的安全，

二是 系统信息的安全：口令鉴别、用户存取权限控制、数据存取权限方式控制、审计跟踪、数据加密等

**信息安全的基本属性**：完整性、机密性、可用性、可控制性、不可否认性

1.2.3信息系统面临的安全风险

1.2.4

**信息安全问题产生的根源**：

信息系统的复杂性，人为和环境的威胁

1.2.5信息安全的地位和作用

1.2.6

**信息安全技术（归纳为五类）**

核心基础安全技术：密码技术

安全基础设施技术：标识与认证技术，授权与访问控制技术

基础设施安全技术：主机系统安全技术，网络系统安全技术

应用安全技术：网络与系统安全攻击技术，网络与系统安全防护与响应技术，安全审计与责任认定技术，恶意代码监测与防护技术

支撑安全技术：信息安全评测技术，信息安全管理技术

**1.3信息安全保障体系**

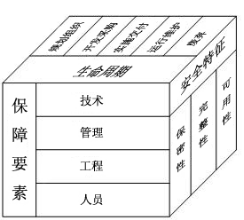
1.3.1

**信息安全保障体系框架**

生命周期：规划组织，开发采购，实施交付，运行维护，废弃

保障要素：技术，管理，工程，人员

安全特征：机密性，完整性，可用性



1.3.2**信息系统安全模型与技术框架**

**P2DR安全模型**：策略（policy），防护，检测，响应；

防护时间大于检测时间加上响应时间，

安全目标暴露时间=检测时间+响应时间，越小越好；

提高系统防护时间，降低检测时间和响应时间

**信息保障技术框架**（IATF）：

纵深防御策略的主要核心因素：人员，技术，操作；

四个技术框架焦点域：保护本地计算机，保护区域边界，保护网络及基础设施，保护支撑性基础设施

1.4信息安全保障基本实践

1.4.1国内外信息安全保障工作概况

1.4.2**信息安全保障工作的内容**

确定安全需求，设计和实施安全方案，进行信息安全评测，实施信息安全监控

**第二章 信息安全基础技术与原理**

**2.1密码技术**

2.1.1**对称密码与非对称密码**

对称密钥密码体制：发送方和接收方使用相同的密钥

非对称密钥密码体制(公开密钥密码体制)：发送方和接收方使用不同的密钥

**对称密钥体制的优缺点：**

加密处理速度快、保密度高；密钥管理分发复杂、代价高，数字签名困难

**对称密码分类**：

分组密码：一次加密一个明文分组：DES，IDEA，AES

序列密码：一次加密一位或者一个字符：RC4，SEAL

**加密方法**：

代换法：单表代换密码，多表代换；

置换法

**安全性：**

**攻击密码体制：**

穷举攻击法（对于密钥长度128位以上的密钥空间不再有效）

密码分析学

**攻击密码类型：**

唯密文攻击

已知明文攻击

选择明文攻击（加密算法一般要能够抵抗选择明文攻击才认为是最安全的，分析方法：差分分析和线性分析）

选择密文攻击

基本运算：异或，加，减，乘，查表

**对称密码设计的基本思想**：扩散，混淆；

**达到扩散和混淆目的的常见方法：**

乘积迭代：乘积密码，常见的乘积密码是迭代密码，DES，AES

**数据加密标准DES：**基于Feistel网络，派生算法3DES，有效密钥位数：56

**高级加密标准AES**：SP网络

**国际数据加密算法IDEA：**

利用128位密钥对64位的明文分组，经连续加密产生64位的密文分组

**分组密码工作模式**：

电子密码本模式ECB，

密码分组链模式CBC，

密码反馈模式CFB，

输出反馈模式OFB，

计数模式CTF

**非对称密码：**

基于难解问题设计密码是**非对称密码设计的主要思想**，NP问题 NPC问题

**非对称密码的优缺点：**

克服密钥分配上的困难、易于实现数字签名、安全性高

降低了加解密效率

**RSA算法（目前应用最广泛）：**

基于大合数 因式分解难的问题设计；

既可用于加密，又可用于数字签名；

**ElGamal算法**：基于离散对数求解困难的问题设计

**椭圆曲线密码ECC**：基于椭圆曲线 离散对数求解困难的问题设计

**总结：通常采用对称密码体制实现数字加密，公钥密码体制实现密钥管理的混合加密机制！**

**2.1.2 哈希函数**

单向密码体制，从一个明文到密文的不可逆的映射，只有加密过程，没有解密过程

可将任意长度的输入经过变换后得到固定长度的输出（其中的固定长度---称为原消息的消息摘要或散列）

**应用：**

消息认证（基于哈希函数的消息认证码）

数字签名（对消息摘要进行数字签名口令的安全性，数据完整性）

**消息摘要算法MD5**：可以对任意长度的明文，产生128位的消息摘要

**安全散列算法SHA：**160位

SHA比MD5更安全，SHA操作步骤较MD5更简单，SHA比MD5速度慢了25%，

**2.1.3数字签名**

通过密码技术实现，其安全性取决于密码体制的安全程度

**普通数字签名：**RSA，ElGamal，椭圆曲线数字签名算法等

**特殊数字签名：**盲签名，代理签名，群签名，不可否认签名，具有消息恢复功能的签名等

常对信息的摘要进行签名

**美国数字签名标准**DSS**的签名算法**DSA

**应用**：

鉴权：重放攻击

完整性：同形攻击

不可抵赖

**2.1.4密钥管理**

包括密钥的生成，存储，分配，启用与停用，控制，更新，撤销与销毁等诸多方面，密钥的分配与存储最为关键

借助加密，认证，签名，协议和公证等**技术**

**密钥的属性：**秘密性，完整性，真实性

**密钥产生：**噪声源技术（基于力学，基于电子学，基于混沌理论的密钥产生技术）；

**主密钥：**通过掷硬币、骰子，从随机数表中选数等随机方式产生，以保证密钥的随机性

**加密密钥的产生：**可以由机器自动产生，也可以由密钥操作员选定

**会话密钥的产生：**通过某种加密算法动态地产生

**密钥分配**

**密钥分配手段分类：人工**分发（物理分发），基于中心的密钥分发

**密钥属性分类：**秘密密钥分配，公开密钥分配

**密钥分配技术分类**：基于对称密码体制的密钥分配，基于公钥密码体制的密钥分配

**密钥信息交换方式：**人工密钥分发，基于中心密钥分发，密钥交换协议

**·1人工密钥分发：**主密钥

**·2基于中心的密钥分发：**

**1.实质：**利用公开密钥密码体制分配传统密码的密钥；

**2.可信第三方：**密钥分发中心KDC，密钥转换中心KTC；

**3**.**两种模型：**拉模型，推模型；

**·3最典型的密钥交换协议：**Diffie-Hellman算法

**公开密钥分配的方法：**公共发布；公用目录；公约授权：公钥管理机构；公钥证书：证书管理机构CA，目前最流行

密钥存储分为：

**公钥存储**

**私钥存储**：

用口令加密后存放在本地软盘或硬盘

存放在网络目录服务器中：私钥存储服务PKSS

智能卡存储

USB Key存储

**2.2认证技术**

**2.2.1消息认证**

**产生认证码的函数类型：**

消息加密：整个消息的密文作为认证码

消息认证码（MAC）：利用密钥对消息产生定长的值，并以该值作为认证码；基于DES的MAC算法

哈希函数：将任意长的消息映射为定长的哈希值，并以该哈希值作为认证码

**2.2.2身份认证**

**身份认证系统：**认证服务器、认证系统客户端、认证设备

系统主要通过身份认证协议（单向认证协议和双向认证协议）和认证系统软硬件进行实现

**认证手段：**  
 静态密码方式

动态口令认证：动态短信密码，动态口令牌（卡）

USB Key认证：挑战/应答模式，基于PKI体系的认证模式

生物识别技术

**认证协议：**基于口令的认证协议，基于对称密码的认证，基于公钥密码的认证

**2.3访问控制技术**

**访问控制模型：**

自主访问控制（DAC）：

访问矩阵模型：访问能力表（CL），访问控制表（ACL）；

商业环境中，大多数系统，如主流操作系统、防火墙等

强制访问控制（MAC）：

安全标签：具有偏序关系的等级分类标签，非等级分类标签，比较主体和客体的安全标签等级,访问控制安全标签列表（ACSLL）；

访问级别：最高秘密级，秘密级，机密级，无级别及；

Bell-Lapadula模型：只允许向下读、向上写，保证数据的保密性，

Biba不允许向下读、向上写，保护数据完整性；

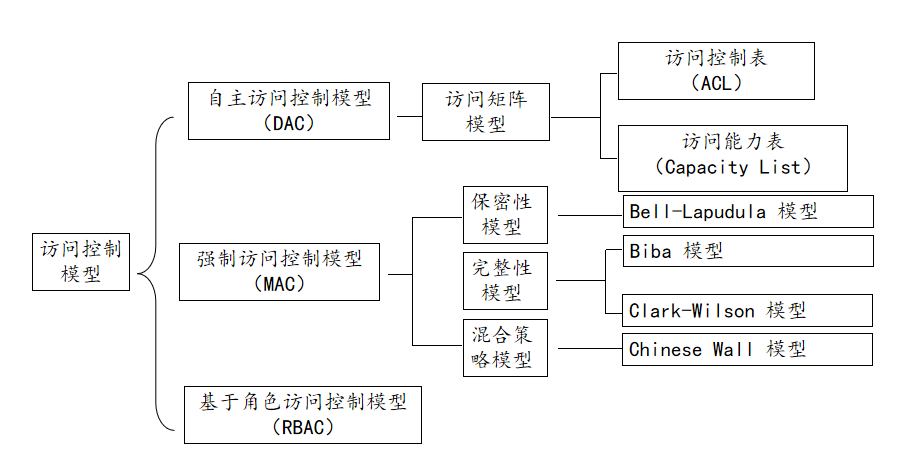
Chinese Wall模型：多边安全系统中的模型，包括了MAC和DAC的属性

基于角色的访问控制（RBAC）：

要素：用户，角色，许可；面向企业，大型数据库的权限管理；

用户不能自主的将访问权限授权给别的用户；

MAC基于多级安全需求，RBAC不是



2.3.2访问控制技术

**集中访问控制：**

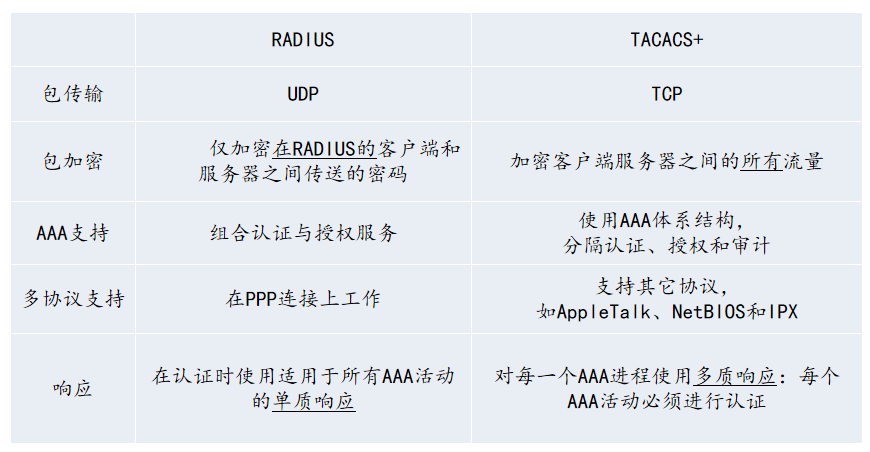
**运营的基础**：认证、授权、审计管理（AAA管理）

**AAA管理协议的组成部分：**

1.拨号用户远程认证服务RADIUS：提供集中式AAA管理；客户端/服务器协议，运行在应用层，使用UDP协议；组合认证与授权服务

2.终端访问控制器访问控制系统TACACS：TACACS+使用TCP；更复杂的认证步骤；分隔认证、授权、审计

3.Diameter：协议的实现和RADIUS类似，采用TCP协议，支持分布式审计



**非集中式访问控制：**

**三种分布式访问控制方法为：**

--单点登录SSO

--Kerberos协议：使用最广泛的身份验证协议；引入可信的第三方。Kerberos验证服务器；能提供网络信息的保密性和完整性保障；支持双向的身份认证

--SESAME：认证过程类似于Kerberos

**2.4审计和监控技术**

**2.4.1审计和监控基础**

**审计系统：**

1.日志记录器：收集数据，系统调用Syslog收集数据；

2.分析器：分析数据；

3.通告器：通报结果

**2.4.2审计和监控技术**

**1.恶意行为监控：**

主机监测：可监测的地址空间规模有限；

网络监测：蜜罐技术（软件honeyd），蜜网（诱捕网络）；

恶意代码诱捕系统的组成部分：高交互蜜罐、低交互蜜罐、主机行为监视模块

1. **网络信息内容审计：**

方法：网络舆情分析：舆情分析引擎、自动信息采集功能、数据清理功能；

技术：网络信息内容获取技术（嗅探技术）、网络内容还原分析技术；

模型：流水线模型、分段模型；

不良信息内容监控方法：网址、网页内容、图片过滤技术

**第三章 系统安全**

**3.1操作系统安全**

**3.1.1操作系统安全基础**

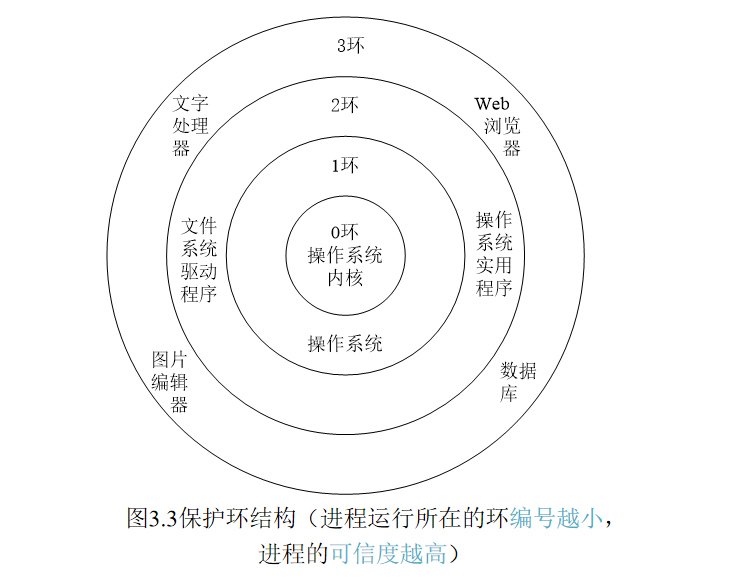
**基本安全实现机制**：

CPU模式和保护环：内核模式、用户模式

当操作系统为0环和1环执行指令时，它在管理员模式或内核模式下运行。

当操作系统为3环中的应用程序和进程执行指令时，它在用户模式下运行。

进程隔离：使用虚拟地址空间以达到系统对同时执行的进程进行隔离



**3.1.2操作系统安全实践**

**UNIX/Linux系统：**

--文件系统安全：

所有的事物都是文件：正规文件、目录、特殊文件（/dev下的设备文件）、链接、Sockets；文件系统安全基于i节点中的三层关键信息：

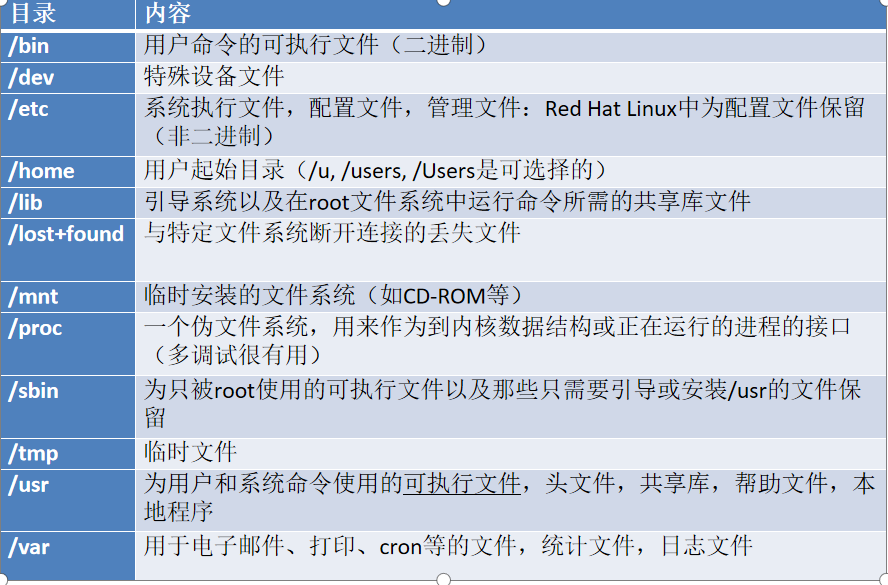
1.UID（文件拥有者），GID：（文件所在分组），模式；

2.模式位，权限位的八进制数表示；

3.设置SUID（使普通用户完成一些普通用户权限不能完成的事而设置）和SGID，体现在所有者或同组用户权限的可执行位上；chmod改变文件权限设置、chown、chgrp；unmask创建文件默认权限

--账号安全管理：/etc/passwd、/etc/shadow；伪用户账号；root账户管理：超级用户账户可不止一个，将UID和GID设置为0即可，使用可插入认证模块PAM进行认证登录

--日志与审计：日志系统：记录连接时间的日志：/var/log/wtmp、/var/run/utmp，进程统计：pacct与acct，错误日志：/var/log/messages



**Windows系统：**

Windows安全子系统：winlogon和图形化标识和验证GINA、本地安全认证、安全支持提供者的接口（SSPI）、认证包、安全支持提供者、网络登录服务、安全账号管理器（SAM）

登录验证：Kerberos

用户权力与权限：用户权限：目录权限、文件权限；共享权限

日志与审计：系统日志、应用程序日志、安全日志

安全策略：密码策略；锁定策略；审核策略；用户全力指派；安全选项；装载自定义安全模板；windows加密文件系统

**可信计算技术：**

可信计算平台联盟（TCPA），可信计算组织（TCG）

可信PC，可新平台模块（TPM），可信软件栈（TSS），可信网络连接（TNC）

可信平台模块（TPM）：具有密码运算能力和存储能力，是一个含有密码运算部件和存储部件的小型片上系统；物理可信、管理可信的；

可信密码模块（TCM）：中国

可信计算平台：三个层次：可信平台模块（信任根）、可信软件栈、可信平台应用软件； 我国：可信密码模块、可信密码模块服务模块、安全应用

可信网络连接（TNC）：开放性、安全性

**3.2数据库安全**

**3.1.1数据库安全基础**

**现代数据库运行环境：**多层体系结构，中间层完成对数据库访问的封装

**统计数据库安全:**目标是允许用户查询聚集类型的信息（例如合计、平均值等），但是不允许查询单个记录信息

**数据库安全功能：**

用户标识和鉴定

存取控制：

1. 自主存取控制：用户权限有两个要素组成：数据库对象和操作类型，GRANT语句向用户授予权限，REVOKE语句收回授予的权限，角色：权限的集合；
2. 强制存取控制：主体和客体，敏感度标记：许可证级别（主体）、密级（客体）， 首先要实现自主存取控制

审计：用户级审计、系统审计；AUDIT设置审计功能，NOAUDIT取消审计功能

数据加密

**视图与数据保密性：**将视图机制与授权机制结合起来使用，首先用视图机制屏蔽一部分保密数据，然后在视图上再进一步定义存取权限

**数据完整性：**

语义完整性，参照完整性，实体完整性

约束：优先于使用触发器、规则和默认值

默认值：CREATE DEFAULT

规则：CREATE RULE，USE EXEC sp\_bindefault，DROP RULE

事务处理：BEGAIN TRANSACTION，COMMIT，ROLLBACK；原子性、一致性、隔离性、持久性；自动处理事务、隐式事物、用户定义事物、分布式事务

**3.2.2数据库安全实践**

**数据库十大威胁：**

过度的特权滥用；合法的特权滥用；特权提升；平台漏洞；SQL注入；不健全的审计；拒绝服务；数据库通信协议漏洞；不健全的认证；备份数据库暴露

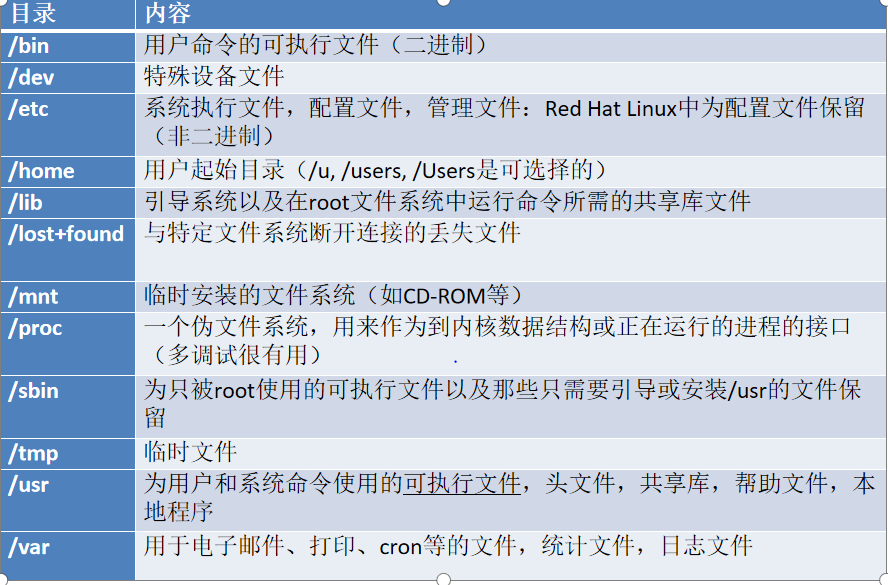
**安全防护体系：**事前检查，事中监控，事后审计

**数据库安全特性检查：**

端口扫描（服务发现）：对数据库开放端口进行扫描；渗透测试：黑盒式的安全监测，攻击性测试，对象是数据库的身份验证系统和服务监听系统，监听器安全特性分析、用户名和密码渗透、漏洞分析；

内部安全监测：安全员数据、内部审计、安全配置检查、漏洞检测、版本补丁检测

**数据库运行安全监控：**网络嗅探器、数据库分析器、SQL分析器、安全审计



**第四章 网络安全**

**4.1网络安全基础**

**4.1.1 TCP/IP体系架构**

**4.1.2网络协议**

数据链路层协议：地址解析协议（ARP），逆向地址解析协议（RARP）

网络层协议：IP协议， Internet控制报文协议（ICMP）：发送出错和控制消息，提供了一个错误侦测与回馈机制

传输层协议：TCP协议，UDP协议

应用层协议：HTTP，SMTP和POP3，DNS

**4.2网络安全威胁技术**

**4.2.1扫描技术**

互联网信息搜集

IP地址扫描：操作系统命令ping（网络故障诊断命令）、tracer，自动化的扫描工具Namp 、Superscan

端口扫描：Namp软件；TCP全连接扫描，TCP SYN扫描，TCP FIN扫描，UDP的ICMP端口不可达扫描，ICMP扫描；乱序扫描和慢速扫描

漏洞扫描：网络漏洞扫描：模拟攻击技术；主机漏洞扫描：漏洞特征匹配技术、补丁安装信息的检测

弱口令扫描：基于字典攻击的弱口令扫描技术、基因穷举攻击的弱口令扫描技术

综合漏洞扫描：Nessus

扫描防范技术：防火墙，用安全监测工具对扫描行为进行监测

**4.2.2网络嗅探**

非主动类信息获取攻击技术

防范：实现对网络传输数据的加密，VPN、SSL、SSH等加密和传输的技术和设备，利用网络设备的物理或者逻辑隔离的手段

**4.2.3网络协议欺骗**

IP地址欺骗：和其他攻击技术相结合

ARP欺骗：中间人欺骗（局域网环境内实施），伪装成网关欺骗（主要针对局域网内部主机与外网通信的情况）；防范：MAC地址与IP地址双向静态绑定

TCP欺骗：将外部计算机伪装成合法计算机；

非盲攻击：网络嗅探，已知目标主机的初始序列号

盲攻击：攻击者和目标主机不在同一个网络上

DNS欺骗：基于DNS服务器的欺骗，基于用户计算机的DNS欺骗

**4.2.4诱骗式攻击**

网站挂马：

攻击者成功入侵网站服务器，具有了网站中网页的修改权限

技术：框架挂马：直接加在框架代码和框架嵌套挂马；JS脚本挂马；b ody挂马；伪装欺骗挂马

防范：Web服务器，用户计算机

诱骗下载：

主要方式：多媒体类文件下载，网络游戏软件和插件下载，热门应用软件下载，电子书爱好者，P2P种子文件

文件捆绑技术：多文件捆绑方式，资源融合捆绑方式，漏洞利用捆绑方式

钓鱼网站

社会工程

**4.2.5软件漏洞攻击利用技术**

软件漏洞：操作系统服务程序漏洞，文件处理软件漏洞，浏览器软件漏洞，其他软件漏洞

软件漏洞攻击利用技术：直接网络攻击；诱骗式网络攻击：基于网站的诱骗式网络攻击，网络传播本地诱骗点击攻击

**4.2.6拒绝服务攻击**

实现方式：利用目标主机自身存在的拒绝服务性漏洞进行攻击，耗尽目标主机CPU和内存等计算机资源的攻击，耗尽目标主机网络带宽的攻击

分类：

IP层协议的攻击：发送ICMP协议的请求数据包，

Smurf攻击；

TCP协议的攻击：利用TCP本身的缺陷实施的攻击，包括SYN-Flood和ACK-Flood攻击，使用伪造的源IP地址，利用TCP全连接发起的攻击，僵尸主机；

UDP协议的攻击；

应用层协议的攻击：脚本洪水攻击

分布式拒绝服务（DDos）：攻击者，主控端，代理端，僵尸网络

防范：支持DDos防御功能的防火墙

**4.2.7 Web脚本攻击**

针对Web服务器端应用系统的攻击技术：

注入攻击：SQL注入，代码注入，命令注入，LDAP注入，XPath注入；防范：遵循数据与代码分离的原则

访问控制攻击，非授权的认证和会话攻击

针对Web客户端的攻击技术：

跨站脚本攻击（XSS）：反射型XSS（非持久性的跨站脚本攻击），存储型XSS（持久型的跨站脚本攻击），DOM-based XSS（基于文档对象模型的跨站脚本攻击）：从效果上来说属于反射型XSS

跨站点请求伪造攻击（CSRF）：伪造客户顿请求；防范：使用验证码，在用户会话验证信息中添加随机数

点击劫持攻击

**4.2.8远程控制**

木马：

具有远程控制、信息偷取、隐藏传输功能的恶意程序；通过诱骗的方式安装；一般没有病毒的的感染功能；特点：伪装性，隐藏性，窃密性，破坏性；

连接方式：C/S结构；最初的网络连接方法；反弹端口技术：服务器端主动的发起连接请求，客户端被动的等待连接；木马隐藏技术：线程插入技术、DLL动态劫持技术、RootKit（内核隐藏技术）

Wwbshell：用Web脚本写的木马后门，用于远程控制网站服务器；以ASP、PHP、ASPX、JSP等网页文件的形式存在；被网站管理员可利用进行网站管理、服务器管理等

4.3网络安全防护技术

4.3.1防火墙

一般部署在网络边界，也可部署在内网中某些需要重点防护的部门子网的网络边界

功能：在内外网之间进行数据过滤；对网络传输和访问的数据进行记录和审计；防范内外网之间的异常网络行为；通过配置NAT提高网络地址转换功能

分类：硬件防火墙：X86架构的防火墙（中小企业），ASIC、NP架构的防火墙（电信运营商）；软件防火墙（个人计算机防护）

防火墙技术：

包过滤技术：默认规则；主要在网络层和传输层进行过滤拦截，不能阻止应用层攻击，也不支持对用户的连接认证，不能防止IP地址欺骗

状态检测技术（动态包过滤技术）：增加了对数据包连接状态变化的额外考虑，有效阻止Dos攻击

地址翻译技术：静态NAT，NAT池，端口地址转换PAT

应用级网关（代理服务器）：在应用层对数据进行安全规则过滤

体系结构：

双重宿主主机体系结构：至少有两个网络接口，在双重宿主主机上运行多种代理服务器，有强大的身份认证系统

屏蔽主机体系结构：防火墙由一台包过滤路由器和一台堡垒主机组成，通过包过滤实现了网络层传输安全的同时，还通过代理服务器实现了应用层的安全

屏蔽子网体系结构：由两个包过滤路由器和一台堡垒主机组成；最安全，支持网络层、传输层、应用层的防护功能；添加了额外的保护体系，周边网络（非军事区，DMZ）通常放置堡垒主机和对外开放的应用服务器；堡垒主机运行应用级网关

防火墙的安全策略

4.3.2入侵检测系统和入侵防御系统

入侵检测系统（IDS）：

控制台：在内网中，探测器：连接交换机的网络端口

分类：根据数据采集方式：基于网络的入侵检测系统（NIDS）、基于主机的入侵检测系统（HIDS）；根据检测原理：误用检测型入侵检测系统、异常检测型入侵检测系统

技术：误用检测技术：专家系统、模型推理、状态转换分析；异常检测技术：统计分析、神经网络；其他入侵检测技术：模式匹配、文件完整性检验、数据挖掘、计算机免疫方法

体系结构：集中式结构：单一的中央控制台；分布式结构：建立树形分层结构

部署：一个控制台可以管理多个探测器，控制台可以分层部署，主动控制台和被动控制台

入侵防御系统（IPS）：

部署：网络设备：网络中需要保护的关键子网或者设备的网络入口处，控制台

不足：可能造成单点故障，可能造成性能瓶颈，漏报和无保的影响

4.3.3PKI

公共密钥基础设施是创建、管理、存储、分布和作废数字证书的一场系列软件、硬件、人员、策略和过程的集合

组成：数字证书是PKI的核心；安全策略；证书认证机构（CA）；证书注册机构；证书分发机构；基于PKI的应用接口

数字证书

信任模式：单证书认证机构信任模式，层次信任模型，桥证书认证机构信任模型

4.3.4VPN

利用开放的物理链路和专用的安全协议实现逻辑上网络安全连接的技术

网络连接类型：远程访问型VPN（Client-LAN）客户机和服务器都安装VPN软件；网络到网关类型的VPN（LAN-LAN）客户端和服务器各自在自己的网络边界部署硬件VPN网关设备

VPN协议分类：网络隧道技术

第二层隧道协：封装数据链路层数据包；介于二、三层之间的隧道协议；第三层隧道协议IPSec，通用路由封装协议（GRE）；传输层的SSL VPN协议：SSL协议工作在TCP/IP和应用层之间

4.3.5网络安全协议

Internet安全协议（IPSec）：引入加密算法、数据完整性验证和身份认证；网络安全协议：认证协议头（AH）、安全载荷封装（ESP，传输模式、隧道模式），密钥协商协议：互联网密钥交换协议（IKE）

传输层安全协议（SSL）：解决点到点数据安全传输和传输双方身份认证的网络安全传输协议；记录协议和握手协议

应用层安全协议：

Kerberos协议；SSH协议：加密所有传输的数据，能防止DNS欺骗和IP欺骗；安全超文本传输协议（SHTTP）；安全多用途网际邮件扩充协议（S/MIME）；安全电子交易协议SET）

Windows操作系统核心组件中，Kernel属于Windows核心系统DLL组件；NTdll.dll属于windows内部函数组件；Win32k.sys属于windows子系统的内核模式部分组件；HAL.dll属于windows硬件抽象层组件。

利用Wireshark捕获的前面10个数据包是ISAKMP协议数据包

网络嗅探工具通过获取数据包中的明文数据来窃取敏感信息，VPN.SSL.SSH等加密的设备和技术可有效防范网络嗅探工具对数据的嗅探和分析

静态包过滤防火墙技术对数据包进行过滤的协议层为：网络层和传输层。

SSL为传输层上的应用层提供加密，身份认证，完整性验证的保护

信息系统安全保障涵盖三个方面：生命周期，保障要素和安全特征

P2DR安全模型：策略，防护，检测，响应。

IDS的异常检测技术主要是通过统计分析方法和神经网络方法实现

我国专家在1999年提出了更为完善的“保护-预警-检测-应急-恢复-反击模型。

Inetd是unix最重要的网络服务进程，是监听网络请求的守护进程。Xinetd可以替换其功能。

Whois是internet上提供的查找相关域名，ip地址，E-mail信箱，联系电话等信息的一种服务。

限制内存堆栈区的代码为不可执行状态的技术是DEP

信息安全管理工作的基础是风险评估，核心是风险处置。

信任根是系统可信的基点。TCG定义可信计算平台的信任根包括3个根：可信测量根，可信存储根，可信报告根。

CC评估等级每一级均需评估七个功能类，分别是配置管理，分发和操作，开发过程，指导文献，生命期的技术支持，测试和脆弱性评估。

CC将评估过程划分为过程和保证两部分。

中国信息安全测评中心英文简称CNITSEC

属于网络层协议的是ospf，rip，snmp，icmp

Land攻击是较早使用的一种攻击方法，他利用TCP协议的握手过程，将攻击数据包的源地址和目标地址都设置成目标主机的Ip地址。

Script Flood攻击属于应用层协议的攻击。

SSl协议建立在TCP/IP协议之上，在HTTP等应用层协议之下，对基于TCP/IP协议的应用服务是完全透明的。

系统维护的注意事项：维护和更改记录，更改的清楚，错误报告的处理，老版本的的备份和清理。

访问控制管理的重要组成部分包括：用户账户管理，操作跟踪，访问权力和许可证的管理。

修改了目录文件的存放目录后，日志还是可以被清空的，下面通过修改日志文件访问权限，防止这种事情发生，前提是Windows系统采用NTFS文件系统格式。

MITRE公司建立的通用漏洞列表CVE相当于软件漏洞的一个行业标准。

信息安全管理体系审核是为了获得审核证据，对体系进行客观的评价。

对于用户创建的默认权限，可以使用umask命令来设置。

IKE协议属于混合型协议，由OAKLEY,SKEME,ISAKMP

RADIUS运行在UDP协议上，并且没有定义重传机制，而Diameter运行在可靠的的TCP之上

BitBlaze平台由三个部分组成：Vine，静态分析组件，TEMU,动态分析组件，Rudder，结合动态和静态分析进行具体和符号化的组件。Nessus是目前全世界使用人数最多的系统漏洞扫描与分析软件。Metaspoit是一个免费的可下载的框架

代码混淆技术：词法转换，控制流转换，数据流转换。

PKI是创建，管理，存储，分布和作废数字证书的一系列软件，硬件，人员，策略和过程的集合。

GS技术是一项缓冲区溢出的检测防护技术，使用该技术的编译器针对函数调用和返回时添加保护和检查功能的代码，在函数被调用时，在缓冲区和函数返回地址增加一个32位的随机数security\_cookie的值是否变化。

成立于1984年的全国信息技术安全标准化技术委员会CITS，是目前国内最大的标准化技术委员会。

通过对日志进行进行分析，发现所需事件信息和规律是安全审计的根本目的。

中国信息安全评测中心英文简称CNITSEC.

我国专家在1999年提出更为完善的保护-预警-检测-应急-恢复-反击模型。

针对恶意程序检测或者查杀的主要技术包括：特征码查杀，启发式查杀，基于虚拟机技术的行为判断以及主动防御等。

定义一个用户的数据库存取权限，就是要定义这个用户在那些数据库对象上进行哪些类型的操作。

限制内存堆栈区的代码为不可执行的状态，从而防范溢出后代码的执行，这种技术称为数据

TCG可信计算系统结构可划分为三个层次，分别为可信平台模块，可信软件栈和可信平台应用软件。

数据流测试技术是一项基于代码的白盒的测试技术，他能提供充分的代码覆盖，通过分析代码软件代码中变量的取值变化和语句的执行情况，来分析数据处理逻辑和程序的控制流关系。

软件漏洞等级分为注意，警告，重要，紧急。

数据库事务处理的四大特性：原子性，一致性，分离性，持久性。

Netstat命令的作用是可以用来查看进程，并能查看发起程序。NTsd命令的作用是用来终止进程；taskkill命令的作用是终止进程命令。

信息资产的最重要的三个属性是：机密性，完整性，有效性。

电子认证服务提供者应当妥善保存与相关的信息，信息保存期限至少为电子签名认证证书失效后5年。

Exploit的含义是漏洞利用。

定义ISMS的范围就是在组织机构内选定架构ISMS的范围。

软件产品的攻击面包括一个软件可能遭受外来攻击的所有攻击点，包括代码，网络接口，服务和协议。、