# 复习提纲

第一章

1.1

* 信息安全的ISO定义、信息安全的目的（p1）。
* 信息安全的几个要素的涵义，具体包括：机密性、完整性、可用性、可控性、不可否认性。（p2）
* 信息保障的三要素：人、技术和管理。（p2）
* 信息保障的四个方面：保护、检测、反应和恢复。（p2)

1.2

* 信息安全威胁的基本类型：信息泄露、伪造、完整性破坏、业务否决或拒绝服务、未经授权访问（p3~4)

1.3

* 社会工程学攻击的概念 （教材p9）

1.4

* 信息安全的三个基本目标 ，CIA三元组，DAD三元组（教材p9）
* 信息系统的三个基本要素：人、信息、系统（p10）
* 信息系统的五个安全层次：物理安全、运行安全、数据安全、内容安全、管理安全（p10-11）

第二章

2.1

* 密码学（Cryptography）的作用：是信息安全的核心基础。
* 密码学的构成：（1）密码编码学；（2）密码分析学；
* 密码编码学、密码分析学的定义（p15，2.1.1）
* 现代密码学的理论基础：香农在1949年发表的《秘密体制的通信理论》使密码学真正成为了一门科学。（p15）
* 加密通信模型（p16 ，图2.1）
* 密码体制的五要素：M、C、K、E、D（p16）
* 依据密码体制的特点及出现的时间，可以将密码大致划分为三个类别：古典替换密码、对称密钥密码和公开密钥密码。
* 古典替换密码主要包括：单表代替密码、多表代替密码等。（p17）
* 对称密钥密码通常分为两类：分组密码（Block Cipher）和序列密码（Stream Cipher，流密码）

2.2 古典替换密码

* 移位密码原理，凯撒密码是一种移位密码。
* 乘数密码原理.
* 仿射密码原理
* 多表替代密码原理

2.3 对称密钥密码

* DES加密算法主要特点：分组长度，有效密钥长度，运算轮数…
* 分组密码的工作模式：ECB模式，CBC模式,……（p27，2.3.3）
* 三重DES基本原理（p30）
* AES加密算法主要特点：分组长度、密钥长度、计算轮数…（p31）
* （补充）对称密钥体制的加密过程中，混淆（confusion）和扩散（diffusion）两种操作的作用（参见ppt）.

2.4 公开密钥密码

* 公钥密码提出的标志：1976年的Diffie-Hellman密钥交换算法（p33）
* 公开密钥密码与对称密钥密码的不同：不是基于代替和置换，而是基于数学函数；非对称/双密钥； 六要素；支持不可抵赖性（不可否认性）（p32）
* 公开密钥密码与对称密钥密码相比，其优缺点：
  + 优点：解决了密钥分发到的难题，密钥管理简单容易，便于实现数字签名。
  + 缺点：计算开销大、加密和解密速度慢、要求密钥位数更多、密文长度往往大于明文长度。
* 公钥密码通信的安全性保障：私钥的保密性
* 公钥密码体系的特点：公、私钥成对生成，公钥和算法对外公开，私钥保密。
* 公钥密码体系的应用场合：（1）加密信息（机密性）；（2）身份认证（可认证性）；
* 公钥密码的核心思想：单向陷门函数的三个条件、单向性、陷门性、陷门信息（p33）；
* Diffie-Hellman密钥交换算法：原根、离散对数、算法过程（p34）
* 公开密钥算法数学基础：欧拉函数的概念、欧拉定理的使用、算法时间复杂度的表示方式（p35）
* RSA密码算法：大整数因子分解问题、分组密码、密钥生成步骤、辗转相除法求逆元（p35-36）
* 椭圆曲线密码体制（Elliptic Curve Cryptosystems，ECC）相比RSA的优势（p37）

2.5 消息认证

* 认证的目的：（1）验证收发双方；（2）验证消息的完整性；（p38）
* 认证的手段：消息认证、数字签名、实体认证、摘要函数（Hash 函数）（p38）
* 消息认证的目的：证明消息的信源、信宿真实性；消息内容没有受到篡改、消息序号和时间性正确。
* 消息认证的手段：消息加密；消息认证码（MAC）； （p38）
* 主要的消息摘要算法：MD5， SHA-1， SHA-256等
* 散列函数的健壮性：弱无碰撞、强无碰撞、单向性（p40-41）
* 散列函数的安全长度：生日悖论、生日攻击、消息摘要长度下限…(p41)
* 数字签名作用：防止抵赖
* 数字签名原理：用私钥对散列值进行加密，用公钥做验证。（p45）

第四章

4.1

* 身份认证的依据：三个方面：用户所知道的、所拥有的、所具有的…（p57）
* 身份认证的技术：口令认证、密码学认证、生物特征认证，各自的优缺点（p57）
* （补充）基于令牌的认证：用户持有的用于进行认证的一种物品，比如：银行卡（磁条卡、智能卡，……）、电子身份证；
* 单因子认证与双因子认证；

4.2 认证协议

* 基于挑战-应答方式的认证协议基本原理（p58）
* Needham-Schroeder认证协议：理解认证过程；
* Kerberos认证协议：基于对称密钥系统为C/S应用提供的第三方认证服务；由AS和TGS构成；理解其认证过程（三阶段、六步骤）。（p59）
* Windows系统安全认证：主域控制器的作用、交互过程不在网络上传递口令及其散列值（哈希值）。
* Needham-Schroeder公钥认证协议：协议交互过程；(p62)
* 公钥交换存在的问题： 双方直接交换公钥容易受到中间人攻击，由此提出了基于数字证书、利用PKI解决公钥交换的问题。(见ppt)
* 数字证书的结构（X.509 v3）（p62 图4.4）；
* 数字证书的可信性验证方法： 获取证书、生成摘要、与CA签名比较……
* 基于CA数字证书的认证协议：数字证书的概念、主要内容，身份认证过程（图4.5）；（p62-63）

4.3 PKI

* 公钥基础设施（PKI）的组成结构及各个组件的功能（图4.6， p63-64）
* PKI涉及的标准： 证书格式遵循X.509，访问协议遵循LDAP . （p64-66）
* 根证书、证书链的概念（p64）
* 用户查询证书库的目的：获取公钥、验证证书有效性（p64）
* PKI的密钥备份与恢复功能（p64）
* 证书申请撤销的原因（p64）
* PKI的典型功能（p66）

第五章

5.1

* 访问控制的基本组成元素： 主体、客体、访问控制策略（p67）
* 主要的三种访问控制模型（p68）
* 自主访问控制模型（DAC Model）的原理、权限的三种存储方式（ACL/ACCL/ACM）， 优缺点； （p68-70）
* 强制访问控制模型（MAC Model）的原理，优缺点（p70）
* Bell-LaPadula (BLP)模型与Biba模型的比较（p70）
* 基于角色的访问控制模型（RBAC Model）原理，优缺点；
* 制定访问控制策略需遵守的三个原则（p72）

5.3 Windows 系统的安全管理

* Windows系统的访问控制的构成（两大组件）（p74）
* 访问令牌和安全描述符的主要功能（p74-76）

第六章

6.2

* 计算机病毒根据工作原理和传播方式划分为三类（p82）
* CIH病毒属于传统病毒，其主要由三个模块构成，包括： …（p82-83）
* CIH病毒的攻击对象：PE格式的exe文件（p83）
* CIH病毒发作的方式：启动模块驻留内存，传染模块和破坏模块均为条件触发。（p83）
* CIH病毒的主要传播方式是文件复制（p83）
* CIH病毒的查杀方式：手工检测、杀毒软件。（p83）
* 蠕虫病毒的特征：传染性、网络传播、利用漏洞…
* 尼姆达（Nimda）是典型的蠕虫病毒，能够通过网页、邮件和本地共享区传播（p85）
* Nimda病毒的攻击对象：本地PE格式文件（p86）
* 木马病毒的特点：以控制计算机为目的（87）
* 木马的构成：控制端（客户端）、木马程序（服务器端）、木马配置程序（p87）
* 病毒防治的四个方面：检测、清除、预防、免疫（p89-92）

6.3 网络入侵

* 拒绝服务攻击（DoS）的攻击方式：发送非法的协议分组，或构造大量网络流量，使系统或网络无法响应正常的服务（p93）

第七章

7.2

* 防火墙的定义（p107）
* 防火墙的主要功能：主要用于隔离内网与外网，控制和过滤内外网之间的网络数据流量（p107-108）
* 防火墙的主要局限性：无法检测不经过防火墙的流量，不能防范内部人员的恶意攻击，不能阻止被病毒感染和有害程序或文件的传递（比如：木马），不能阻止数据驱动式攻击（比如：缓冲区溢出）。
* 入侵检测系统（IDS）主要功能：对网络传输实时监测，并及时发出警报。（p116）

---End---