第一章 概述

**1. 信息安全的ISO定义，信息安全目的。**

ISO给出的定义：“在技术上和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露”。

信息安全的目的：“确保以电磁信号为主要形式的、在计算机网络化系统中进行获取、处理、存储、传输和应用的信息内容在各个物理及逻辑区域中的安全存在，并不发生任何侵害行为”。

1. **信息安全的三个基本目标是什么？其含义分别是什么？**

CIA三元组是信息安全的三个最基本的目标

机密性Confidentiality：指信息在存储、传输、使用过程中，不会泄漏给非授权用户或实体；

完整性Integrity：指信息在存储、使用、传输过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；

可用性Availability：指确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源。

1. **信息系统的三个基本要素是什么？信息系统的五个层次是什么？含义是什么？**

人员、信息、系统

物理安全：指对网络及信息系统物理装备的保护。

运行安全：指对网络及信息系统的运行过程和运行状态的保护。

数据安全：指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。

内容安全：指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。

管理安全：指通过针对人的信息行为的规范和约束，提供对信息的机密性、完整性、可用性以及可控性的保护

**4. 信息安全保障体系包含哪四部分内容？**

信息安全保障体系包括四个部分内容，即PDRR。

保护（Protect）

检测（Detect）

反应（React）

恢复（Restore）

**第二章 密码学**

**1. 对称密码、非对称密码定义**

对称加密（symmetric）：K

加密与解密的密钥相同，P=D(K, E(K,P))

非对称加密（asymmetric）：（KE, KD)

加密与解密的密钥不同，P=D(KD, E(KE,P))，

解密密钥KD是加密密钥KE的逆运算

1. **对称密码算法DES，公钥密码算法RSA、公钥密码算法的密钥生成方式**
2. **数字签名的特性**

不可伪造：如果P用S(P,M)签署了报文M，其他任何人不可能生成相同的签名S(P,M)

真实性：接收者R可以验证签名S(P,M)是否真的来自声称者P，并且签名严格附属于M不可变：签名时刻的内容M不可变

不可重用：如果对新的内容M’重用以前的签名S(P,M)，接收者R可以立即察觉任何人都可以验证签名

**4. 什么是哈希函数**

是一种典型的消息认证函数，提供消息的完整性保护

**第四章 身份认证**

**1. 什么是身份认证**

身份认证是证实用户的真实身份与其所声称的身份是否相符的过程。

1. **身份认证的三种方式：**口令认证、令牌认证、生物特征认证
2. **身份认证根据认证条件的数目分类、根据认证数据状态分类**

根据认证条件的数目分类

仅通过一个条件的相符合来证明一个人的身份，称之为单因子认证；

通过两种不同条件来证明一个人的身份，称之为双因子认证；

通过组合多种不同条件来证明一个人的身份，称之为多因子认证。

根据认证数据的状态来看，

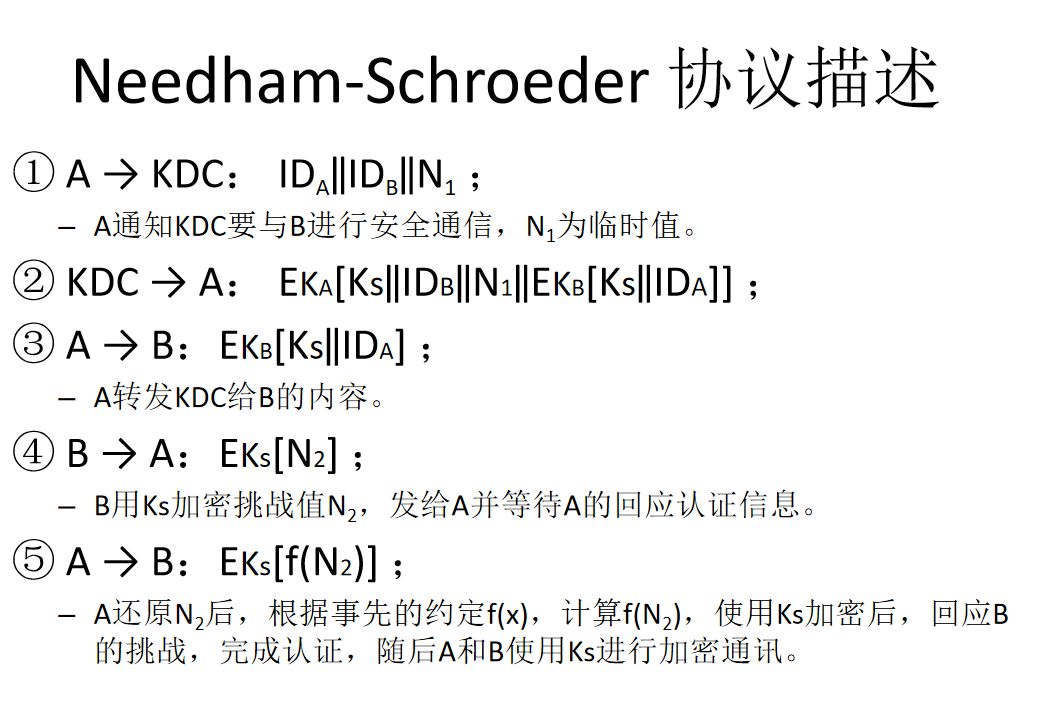
静态数据认证:指用于识别用户身份的认证数据事先已产生并保存在特定的存储介质上；

动态数据认证:指用于识别用户身份的认证数据不断动态变化，每次认证使用不同的认证数据，即动态密码。

1. **认证协议基于对称密码、非对称密码实现**

基于对称密码

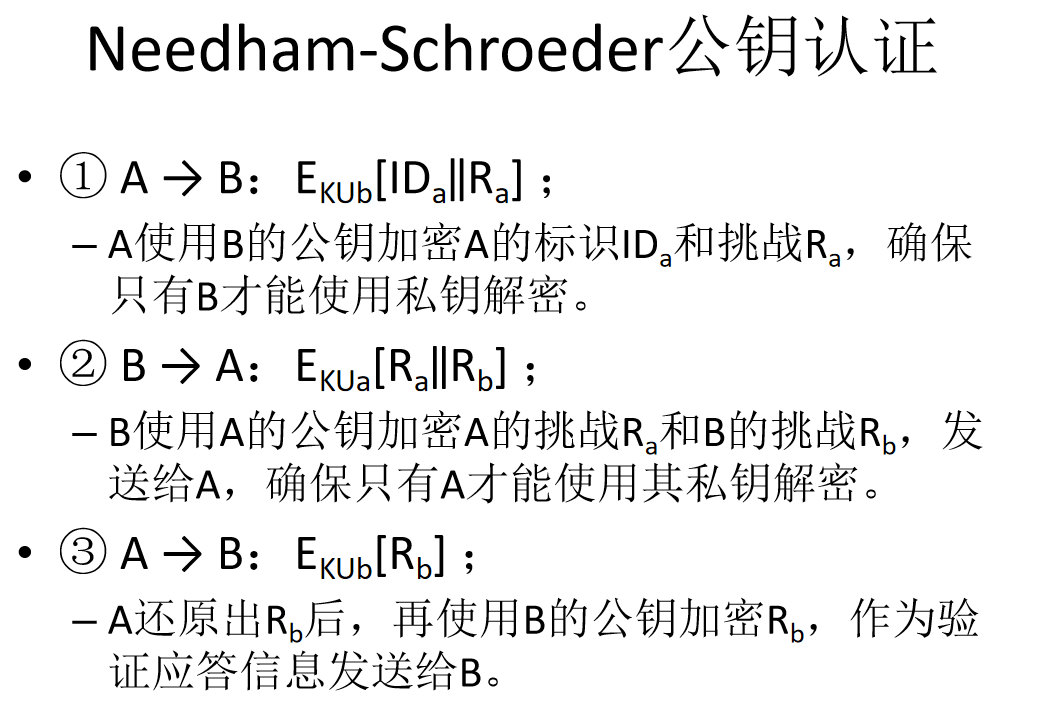
在只有少量用户的封闭式网络系统中，各用户之间的双人共享密钥的数量有限，可以采用挑战-应答方式来实现认证；

对于规模较大的网络系统，一般采用密钥服务器的方式来实现认证，即依靠可信的第三方完成认证。（Needham-Schroeder认证协议）****

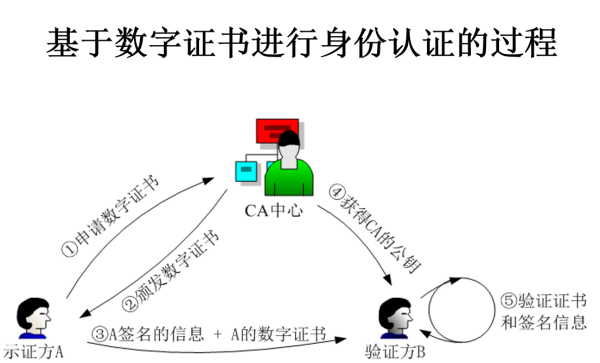
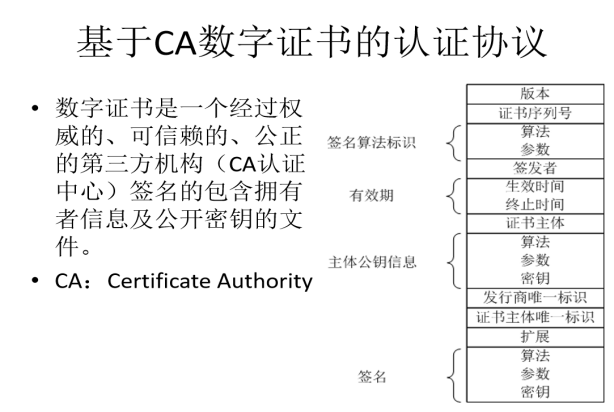
基于非对称（公钥）

方式一是实体A需要认证实体B，A发送一个明文挑战消息（也称挑战因子，通常是随机数）给B，B接收到挑战后，用自己的私钥对挑战明文消息加密，称为签名；B将签名信息发送给A，A使用B的公钥来解密签名消息，称为验证签名，以此来确定B是否具有合法身份。

方式二是实体A将挑战因子用实体B的公钥加密后发送给B，B收到后是用自己的私钥解密还原出挑战因子，并将挑战因子明文发还给A，A可以根据挑战因子内容的真伪来核实B的身份。

****

**5. 基于数字证书实现身份认证的过程**

****

**第五章 访问控制**

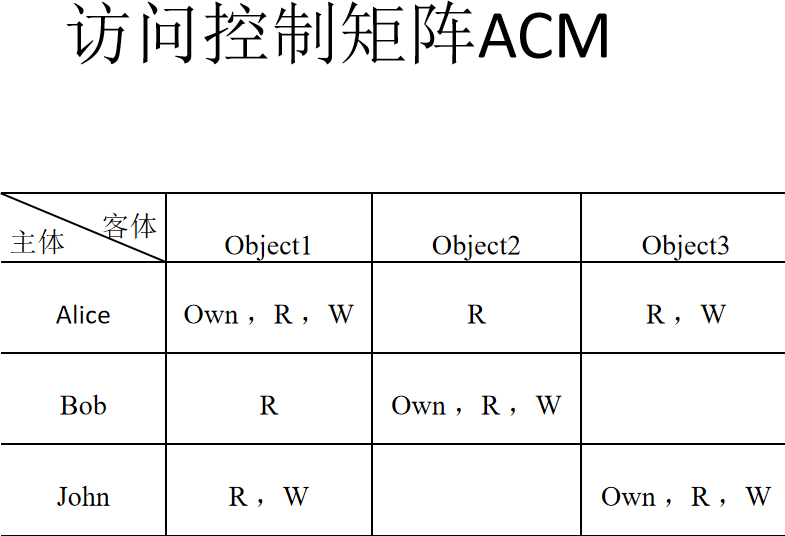
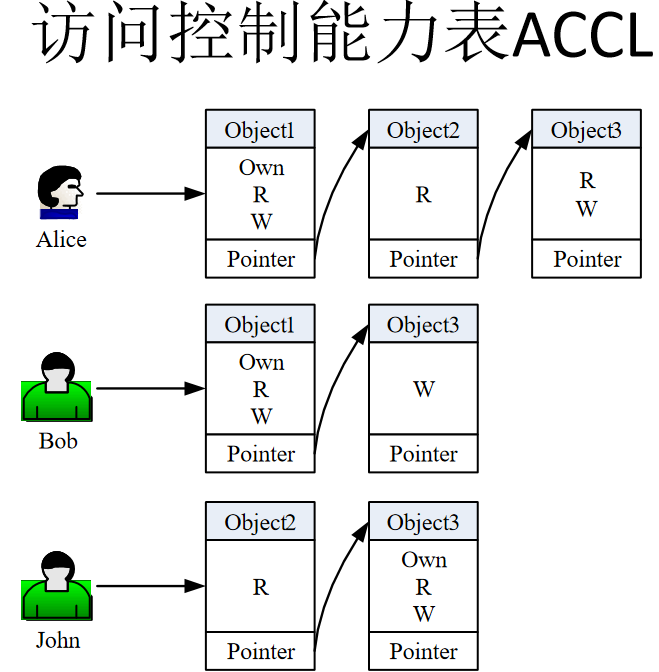
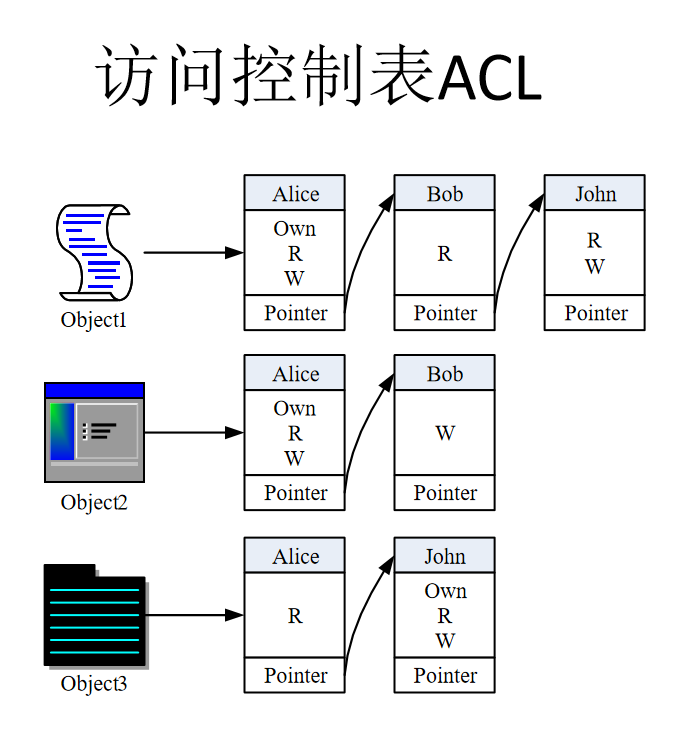
**1. 访问控制的三个元素：**

主体，客体，访问控制策略

1. **访问控制三种模型的定义：**

自主访问控制、强制访问控制、基于角色的访问控制

1. **访问控制列表、访问能力表、访问控制矩阵**

****

1. **强制访问控制的四种形式，并举例说明**

**向下读（RD，Read Down）：**

主体安全级别高于客体信息资源的安全级别时，即SC(s)≥SC(o)，允许读操作； Bell-LaPadula（BLP）

向上读（RU，Read Up）：

主体安全级别低于客体信息资源的安全级别时，即SC(s)≤SC(o)，允许读操作； Biba

向下写（WD，Write Down）：

SC(s)≥SC(o)时，允许写操作； Biba

向上写（WU，Write Up）：

SC(s)≤SC(o)时，允许写操作。 Bell-LaPadula（BLP）

1. **Windows系统中的四类安全主体**

用户是Windows系统中操作计算机资源的主体，每个用户必须先行加入Windows系统，并被指定唯一的账户，

组是用户账户集合的一种容器，同时组也被赋予了一定的访问权限，放到一个组中的所有账户都会继承这些权限；

计算机是指一台独立计算机的全部主体和客体资源的集合，也是Windows系统管理的独立单元；

域是使用域控制器(DC, Domain Controller)进行集中管理的网络，域控制器是共享的域信息的安全存储仓库，同时也作为域用户认证的中央控制机构。

1. **Windows系统访问控制模块的组成**

访问令牌（Access Token）和安全描述符（Security Descriptor），它们分别被访问者和被访问者持有。通过访问令牌和安全描述符的内容，Windows可以确定持有令牌的访问者能否访问持有安全描述符的对象。

**7. Windows系统中的安全标识符 SID**

Windows中的每个账户或账户组都有一个安全标识符SID（Security Identity）

Administrator、Users等账户或者账户组在Windows内部均使用SID来标识的。

每个SID在同一个系统中都是唯一的。

**第六章 网络威胁（恶意软件）**

**1. 什么是恶意软件**

利用计算机系统漏洞来对计算机系统造成威胁的程序

1. **病毒的定义**

编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或程序代码

1. **病毒、蠕虫的特点**

病毒可通过任何介质进行传播，蠕虫通过网络

病毒的自身拷贝必须嵌入到其他程序中来传播，蠕虫的自身拷贝都是以独立程序的形式传播

1. **病毒的四个阶段**

潜伏阶段：病毒处于休眠状态

传播阶段：病毒将自身的拷贝插入其他程序或硬盘上某个与系统相关的区域。病毒拷贝时会变异来逃避检测。

触发阶段：病毒被激活以执行预先设定的功能

执行阶段：执行病毒功能

**5. 特洛伊木马**

特洛伊木马是一个有用的或表面上看起来有用的程序或命令过程，内部隐藏着恶意代码。

**第七章 网络防御（防火墙）**

**1. 防火墙定义**

一种用来加强网络之间访问控制、防止外部网络用户以非法手段通过外部网络进入内部网络、访问内部网络资源，保护内部网络操作环境的特殊网络互连设备。

1. **防火墙的三个设计目标**

所有入站和出站的网络流量都必须通过防火墙。

只有经过授权的网络流量才允许通过防火墙。

防火墙本身不能被渗透，应该运行在有安全操作系统的可信系统上。

**3. 简单了解工作原理**