名词解释列举

A. 引言 & 安全框架

A.1 被动攻击 (Passive Attack)

- 定义：攻击者对传输中的信息进行侦听或监视，但不修改数据流。
- 特征：包括信息内容泄露和流量分析。其特点是难以检测（不改变数据），重点在于预防（如使用加密）。

A.2 主动攻击 (Active Attack)

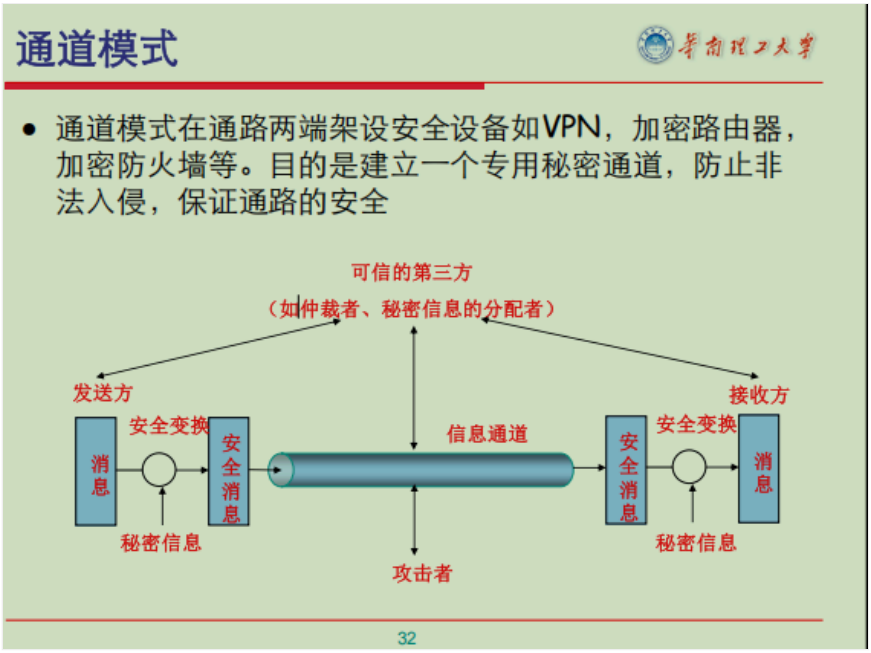
- 定义：攻击者主动对数据流进行篡改、伪造或中断。
- 特征：包括伪造（插入伪造信息）、重放（拦截后重新发送）、修改（篡改内容）和拒绝服务（DoS）。其特点是容易检测，但难防范。

A.3 CIA 三要素

- 机密性 **(Confidentiality)**：确保信息不泄露给非授权方（防侦听）。
- 完整性 **(Integrity)**：确保数据在传输过程中未被修改、插入、删除或重放（防篡改）。
- 可用性 **(Availability)**：确保授权用户能按需正常使用系统资源（防中断）。

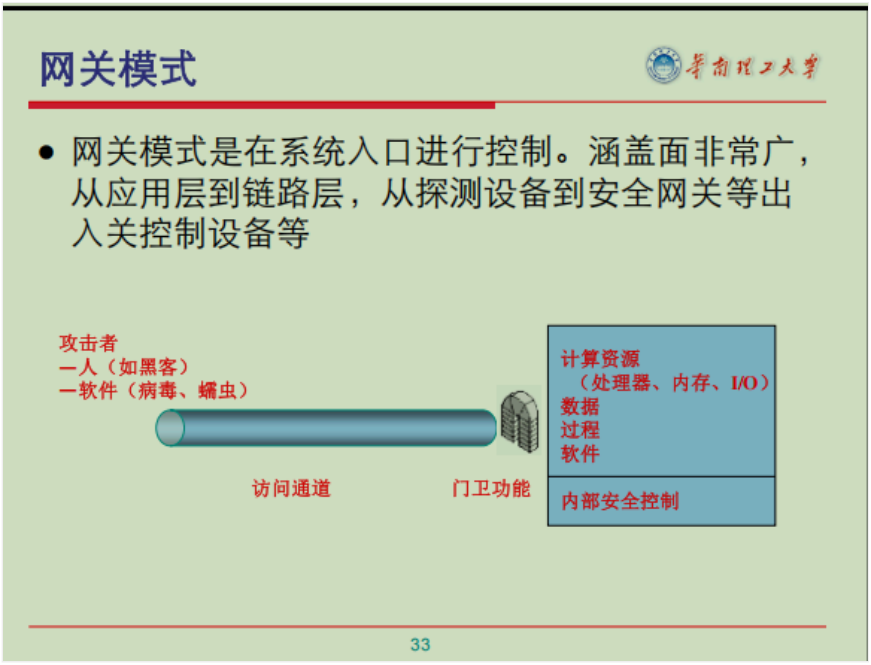
A.4 通道模式 (Channel Mode)

- 定义：在通道的两端架设安全设备，建立专用的秘密通道，防止非法入侵，保证通信安全。
- 实现方式：通过加密实现。



A.5 网关模式 (Gateway Mode)

- 定义：在系统入口进行控制，涵盖面广。
- 范围：从应用层到链路层，从探测设备到安全网关等出入控制设备等。



A.6 系统模式 (System Mode)

- 特征：

- 应用层是人机交互的地方，控制机制实现很灵活。
- 控制粒度更细，可以到用户级（个人）或文件级，实现用户认证和数据认证。

A.7 内核模式 (Kernel Mode)

- 定义：操作系统中的安全内核是信息系统安全可靠的最基本要素。
- 特征：
  - 安全内核是多用户操作系统必备的内部控制系统。
  - 只有在可靠的安全内核的基础上才能实现可靠的多级控制。

B. 传统加密技术

B.1 扩散 (Diffusion) [重点标记：定义 2.2.2]

- 定义：将明文的统计结构扩散到密文的长程统计特性中，使明文和密文的统计关系尽量复杂。
- 目的：隐藏原始消息的统计性质，使攻击者无法利用语言的统计特征（如字母频率）破译。

B.2 混乱 (Confusion) [重点标记：定义 2.2.3]

- 定义：使密文的统计特性和密钥的取值之间的关系尽量复杂。
- 目的：增加从密文推导密钥的难度。

B.3 雪崩效应 (Avalanche Effect) [重点标记：考/定义 2.2.5]

- 定义：指明文或密钥的某一位发生微小变换（如改变1 bit），会导致输出密文发生巨大变化（理想约为50%的位改变）。
- 意义：是衡量加密算法（特别是 S 盒）优劣的重要指标。

B.4 计算安全 (Computational Security)

- 定义：若破译密码的代价超出密文价值，或破译所需时间超出信息有效生命期，则称算法是计算安全的。

D. 现代对称加密 & 工作模式

D.1 分组密码工作模式 (Modes of Operation) [重点标记：考]

- **ECB (电子密码本模式)**：将明文分成块，独立加密。缺点是相同的明文块产生相同的密文块，无法隐藏模式信息。
- **CBC (密码分组链接模式)**：当前明文块与前一密文块（或初始向量 IV）异或后再加密。优点是能隐藏明文模式，缺点是无法并行处理。
- **CTR (计数器模式)**：将计数器值加密后与明文异或（流密码模式）。优点是可并行处理，效率高。

D.2 中间相遇攻击 (Meet-in-the-Middle Attack)

- 定义：针对多重加密（如双重 DES）的一种已知明文攻击。
- 原理：攻击者从明文侧加密和从密文侧解密，通过查找中间结果的匹配来缩减搜索空间，使得双重 DES 的安全性并不比单重 DES 高多少。

E. 传输层安全性 & 密钥分配

E.1 KDC (Key Distribution Center)

- 定义：密钥分发中心。一个可信的第三方机构，负责在通信双方之间分配会话密钥（Session Key）。

E.2 会话密钥 (Session Key) vs. 主密钥 (Master Key)

- 主密钥：
    - 用户与 KDC 共享的长期密钥；
    - 仅用于加密临时密钥的传输。
- 会话密钥：
    - 用于加密具体通信数据的临时密钥。
    - 在线创建
    - 只用在一个逻辑会话中加密数据
    - 经常改变

E.3 Nonce (随机数) [重点标记：E.III]

- 定义：仅使用一次的随机数值。随机性、不可预测性。
- 作用：用于认证协议中，通过挑战-应答机制来防止重放攻击。

F. 公钥密码学

F.1 单向陷门函数 (Trapdoor One-way Function) [重点标记：定义 6.1.1]

- 定义：一个函数 f，正向计算容易（$y = f(x)$）；在不知道陷门信息的情况下求逆极其困难；但若知道陷门信息（私钥），求逆则变得容易。它是公钥密码的数学基础。

F.2 离散对数问题 (Discrete Logarithm Problem) [重点标记：定义 6.1.5]

- 定义：已知质数 p 和原根 α，给定 y，在计算上难以求出 x 使得 $y \equiv \alpha^x \mod p$。这是 Diffie-Hellman 和 ElGamal 算法的安全性基础。

G. 消息认证

G.1 MAC (消息认证码)

- 定义：利用密钥和消息生成的一个固定长度的短数据块。
- 作用：同时验证消息的来源（认证）和完整性。与 Hash 不同，它依赖于共享密钥。

G.2 散列函数 (Collision Resistance) [重点标记：考]

- 定义：任意长度的输入消息 M，映射为一个固定长度的散列值（或称消息摘要）的密码学函数。该输出是输入所有消息位的函数。
- 性质：
    - 抗碰撞
        - 弱抗冲突：给定 x，难以找到 $y \neq x$ 使得 $H(x) = H(y)$。
        - 强抗冲突：难以找到任意一对 $x \neq y$ 使得 $H(x) = H(y)$。

- 单向性：给定h，不容易找到x使得 H(x)=h
- 易于计算：
  - 给出 x，容易计算 H(x)
  - 比密钥加密快

H. 数字签名 & 认证

H.1 数字签名 (Digital Signature) [补充重点]

- 定义：一种对数字消息进行签名的机制，通常使用发送者的私钥进行加密变换。
- 特征：
  - 不可否认性：发送方不能抵赖（因为只有他有私钥）。
  - 完整性：验证内容未被篡改。
  - 身份认证：确认消息是由声称的发送方发出的。

H.2 重放攻击 (Replay Attack) [重点标记：问]

- 定义：攻击者截获有效的认证信息（如加密后的凭证），并在稍后重新发送，试图冒充合法身份。
- 对策：使用时间戳、序列号或随机挑战值（Nonce）。

H.3 数字证书 (Digital Certificate/X.509) [重点标记：考]

- 定义：由可信证书授权机构 (CA) 签发的电子文档，将用户的公钥与用户身份（ID）绑定。
- 作用：解决公钥分发中的信任问题（防中间人伪造公钥），包含 CA 的签名以防篡改。

J. IPSec

J.1 隧道模式 (Tunnel Mode) vs. 传输模式 (Transport Mode) [重点标记：考]

- 传输模式：仅加密 IP 数据载荷（TCP/UDP 头 + 数据），保留原 IP 头。用于端到端通信。
- 隧道模式：加密整个 IP 数据包（包括原 IP 头），并封装在新的 IP 头中。用于 VPN 网关之间的通信，可防止流量分析。

J.2 安全关联 (SA, Security Association)

- 定义：通信双方关于安全参数（如算法、密钥、SPI）的单向逻辑连接协定。双向通信需要建立两个 SA。

K. Web 安全 (SET)

K.1 双向签名 (Dual Signature) [重点标记：问]

- 定义：在 SET 协议中使用的概念。将两份不同信息（如 OI 订单信息和 PI 支付信息）的摘要连接后再次哈希，并用发送者私钥签名。
- 作用：将订单信息和支付信息链接起来，但又保持隔离。使得商家只能看到订单信息（不知道信用卡号），银行只能看到支付信息（不知道买了什么），但双方都能验证两者的关联性。