

信息安全 (Information Security)

一、基本术语 (Basic Terms)

英文术语	中文释义
Vulnerability	脆弱点：系统中可能被利用并造成损害的薄弱点
Threat	威胁：可能导致系统或资产损失的潜在条件
Attack	攻击：利用脆弱点以实现威胁的具体行为
Countermeasure / Control	对策 / 控制措施：防止威胁造成危害的方法

二、信息安全目标：CIA三元组 (C-I-A Triad)

英文术语	中文释义
Confidentiality	保密性：确保资源只被授权人访问
Integrity	完整性：确保信息只能被授权人修改
Availability	可用性：确保授权用户能随时使用资源
Authentication	认证：确认信息或资源身份的机制
Nonrepudiation	不可否认性：防止事后否认已发送的信息

三、密码学 (Cryptography)

英文术语	中文释义
Encryption	加密：将明文转换为密文防止未授权访问
Decryption	解密：将密文还原为明文的过程
RC4	一种流密码算法 (WEP使用)
AES	高级加密标准，比RC4安全得多

四、访问控制 (Access Control)

英文术语	中文释义
Subject	主体：如用户、进程，发起访问请求
Object	客体：如文件、数据库，被访问的资源
Access Type	访问类型：如读 (read)、写 (write)、执行 (execute)
Policy	策略：规定主体对客体的授权方式

英文术语	中文释义
Buffer Overflows	缓冲区溢出：攻击者通过写入超过分配内存边界的数据来覆盖执行代码

五、恶意软件 (Malware)

英文术语	中文释义
Virus	病毒：能自我复制并感染其他程序
Worm	蠕虫：通过网络传播自己
Trojan Horse	特洛伊木马：伪装成正常程序的恶意代码
Ransomware	勒索软件：加密数据并要求赎金解锁（如WannaCry）

六、安全边界与防护 (Security Perimeters)

英文术语	中文释义
Security Perimeter	安全边界：可信区域与非可信区域之间的边界
Firewall	防火墙：过滤内外网之间通信的数据包
Reference Monitor	参考监控器：具备不可规避、不可篡改、可验证三要素
Intrusion Detection System (IDS)	入侵检测系统：监控并识别系统中的恶意行为

七、缓冲区溢出 (Buffer Overflow)

英文术语	中文释义
Buffer Overflow	缓冲区溢出：写入数据超过分配内存边界导致覆盖执行代码
Executable Memory	可执行内存：攻击者尝试用数据覆盖指令区域并执行

八、无线安全 (WEP vs WPA)

英文术语	中文释义
WEP	有线等效保密：早期Wi-Fi加密协议，存在严重漏洞
WPA	Wi-Fi保护访问：使用AES等更强加密算法提升安全
IV (Initialization Vector)	初始化向量：影响密钥强度，WEP中长度仅24位，易被预测

九、拒绝服务攻击 (Denial of Service, DoS)

英文术语	中文释义
DoS Attack	拒绝服务攻击：使服务无法为合法用户正常提供

英文术语	中文释义
Volumetric Attack	容量耗尽攻击：制造海量流量瘫痪网络
Application-based Attack	应用层攻击：针对服务逻辑耗尽系统资源
Protocol Exploitation	协议漏洞攻击：伪造协议数据干扰通信

十、隐私 (Privacy)

英文术语	中文释义
Privacy	隐私：对个人信息的控制权
Personally Identifiable Information (PII)	可识别个人身份信息：如身份、位置、健康、通信记录等
Owner / Subject	所有者 / 对象：拥有或被描述的数据实体