网络安全五章考点整理

2026 年 4 月 23 日

目录

1 第 1 章绪论

1.1 核心概念

- 计算机网络：由通信信道连接的主机和网络设备的集合，用于资源共享和相互通信。
- 计算机网络安全：保护网络设备、软件和数据，使其能被合法用户正常使用，同时免受非授权访问。
- 信息安全：保护信息及信息系统免遭泄露、修改、破坏或失去处理能力。
- 网络空间安全：面向网络空间攻防对抗，强调系统的安全、可信、可靠、可控。

1.2 安全属性

- 机密性：防止信息被非授权者获取，主要依靠密码技术。
- 完整性：保证信息真实、未被篡改，主要依靠校验、认证、身份认证等技术。
- 可用性：保证授权用户可正常使用系统，重点防范故障、拥塞、拒绝服务等。
- 不可否认性：发送者不能否认发送过，接收者不能否认接收过，常靠数字签名实现。

1.3 网络安全威胁

- 环境与灾害因素：火灾、水灾、雷电、静电、电磁脉冲等。
- 人为因素：恶意攻击、违纪违法、配置失误、操作疏忽。
- 系统自身因素：硬件故障、软件缺陷、协议漏洞、后门。
- 按攻击影响分类：
  - 被动攻击：窃听、流量分析。
  - 主动攻击：伪装、重放、篡改、拒绝服务。
- Stallings 分类：截获、篡改、伪造、中断。

1.4 安全模型与综合防护

- PDRR 模型：防护、检测、响应、恢复。
- P2DR 模型：策略、保护、检测、响应、恢复。
- IATF 框架：核心是人、技术、操作，体现纵深防御思想。
- 网络通信安全模型三要素：安全变换、秘密信息（密钥）、可信第三方。
- 安全机制：检测、阻止攻击或从攻击中恢复的方法和技术。
- 安全服务：鉴别、访问控制、机密性、完整性、抗抵赖等。

1.5 常考结论

- 单一安全产品不能解决全部网络安全问题，必须采用体系化综合防护。
- 网络安全处理过程是循环过程，通常包括评估、策略制定、实施、培训、审计五个阶段。
- 防火墙、杀毒、访问控制、漏洞扫描等各有作用，也各有局限。

2 第 2 章密码学基础知识

2.1 密码学基础

- 密码系统可表示为：$S = \{M, C, K, E, D\}$。
- 其中 M 是明文空间，C 是密文空间，K 是密钥空间，E 是加密算法，D 是解密算法。
- 密码学由密码编码学和密码分析学组成。
- 现代密码系统强调：系统安全性依赖于密钥，而不依赖于算法保密。

2.2 古典密码

- 隐写术：隐藏消息存在本身。
- 代换密码：用其他字符替换原字符，如凯撒密码。
- 换位密码：改变字符顺序，不改变字符本身。
- 单表代换密码常用统计分析法破解，凯撒密码可用穷举或统计分析破解。

2.3 对称密码体制

- 加密密钥和解密密钥相同，也称单钥密码体制。
- 两种主要形式：
  - 序列密码（流密码）：按比特加密，速度快，错误扩散小，但要求密钥同步。
  - 分组密码：按固定分组加密，适应性强，不需密钥同步。
- 分组密码常见工作模式：ECB、CBC、CFB、OFB、CTR。
- 优点：速度快、效率高、适合大数据加密。
- 缺点：密钥分发困难，用户增多时密钥管理复杂。

2.4 公开密码体制

- 使用一对密钥：公钥公开，私钥保密。
- 特点：加密和解密分离，可实现保密通信和数字签名。
- 优点：密钥管理较简单，适合开放网络。
- 缺点：算法复杂、运算慢，通常不直接加密大数据。
- 实际中常采用混合加密：公钥加密会话密钥，对称密码加密业务数据。

2.5 RSA

- 安全基础：大整数因子分解困难。
- 密钥生成步骤：
  1. 选大素数 p, q；
  2. 计算 $n = pq$；
  3. 计算 $\varphi(n) = (p-1)(q-1)$；
  4. 选取与 $\varphi(n)$ 互素的 e；
  5. 求 d，满足 $ed \equiv 1 \pmod{\varphi(n)}$。
- 公钥：$\{e, n\}$，私钥：$\{d\}$。
- 可用于加密和数字签名。
- 缺点：速度慢，通常只用来交换对称密钥或签名摘要。

2.6 Diffie-Hellman、ElGamal、ECC

- DH：解决密钥交换问题，但不提供身份认证，易受中间人攻击。
- ElGamal：基于离散对数困难问题，可用于加密和签名。
- ECC：基于椭圆曲线离散对数困难问题，优势是密钥短、速度快、安全性高，适合无线和资源受限场景。

2.7 国密算法

- SM2：非对称算法，基于 ECC。
- SM3：杂凑算法。
- SM4：对称分组密码，分组长度和密钥长度均为 128 位。
- ZUC：流密码，常用于移动通信。

2.8 密码分析

- 两条主要思路：穷举破译法和分析破译法。
- 任何密码算法的安全性都与密钥长度、实现方式和攻击成本有关。
- 公开密码不等于一定比对称密码更安全，两者适用场景不同。

3 第 3 章消息认证与身份认证

3.1 认证的基本问题

- 认证用于应对主动攻击，如篡改、删除、添加、重放、伪造源点等。
- 主要解决：
  - 通信实体身份是否真实；
  - 消息内容是否被修改；
  - 消息是否重放；
  - 发送方和接收方是否可否认。
- 认证类型：身份认证、报文认证、顺序认证、发送方认证（数字签名）。

3.2 散列函数

- 定义：$h = H(M)$，输出固定长度散列值。
- 重要特性：唯一性（抗碰撞）和雪崩效应。
- 常见应用：消息认证、文件完整性校验、数字签名、口令文件、入侵检测。
- 常见算法：
  - MD5：128 位摘要，已不安全；
  - SHA-1：160 位摘要，已不推荐继续使用；
  - SHA-2 / SHA-3：更安全；
  - SM3：国产杂凑标准。

3.3 消息认证

- 内容认证：确认消息未被篡改，即完整性检测。
- 顺序认证：确认消息未重放、顺序未被打乱。
- 顺序认证常用机制：序列号、时间戳、挑战/响应。

3.4 MAC 与 HMAC

- MAC：基于共享密钥和消息生成固定长度认证码，用于完整性和源认证。
- 公式：$\mathrm{MAC}_M = F(M, K)$。
- HMAC：以散列函数为基础的消息认证码。
- MAC 能提供：
  - 完整性保护；
  - 消息源认证；
  - 一定程度的抗篡改能力。
- MAC 不能直接提供不可否认性，因为通信双方共享同一密钥。

3.5 数字签名

- 本质：利用私钥对消息或消息摘要签名，接收方用公钥验证。
- 目标：身份认证、完整性、不可否认性。
- 基本要求：
  - 签名不能伪造；
  - 签名不可抵赖；
  - 签名后内容不可改变；
  - 易于验证。
- 实际应用中通常对散列值签名，而不是直接对整份消息签名：
  - 速度更快；
  - 便于验证完整性；
  - 适合长消息。
- 常见实现：RSA、ElGamal、椭圆曲线签名。

3.6 身份认证

- 识别：确认“你是谁”。
- 验证：确认“你真的是你所声称的人”。
- 常见身份认证方式：
  - 所知：口令、密码；
  - 所有：卡、令牌、证件；

  - 所在：地址、位置；
  - 所是：生物特征、行为特征；
  - 密码学认证。

3.7 口令与一次性口令

- 静态口令：实现简单，但容易被窃听、猜测和重放。
- 动态口令：加入时间、事件或挑战等不确定因子。
- OTP：双因子思想，即固定因子 + 动态因子。
- S/KEY：
  - 通过迭代散列生成一次性口令；
  - 能防重放；
  - 但只支持单向认证，不便于分布式认证，且存在进一步攻击风险。

3.8 Needham-Schroeder、Kerberos、EAP

- Needham-Schroeder：基于 KDC 的双向认证协议，引入一次性会话密钥。
- Kerberos：
  - 由可信第三方 KDC 提供认证；
  - 核心票据：TGT 和服务票据；
  - 优点：适合开放网络和分布式环境；
  - 特点：票据有生命周期，避免长期重放。
- EAP：支持多种认证方法的认证框架，常用于 PPP、802.1X、WLAN。

3.9 数字证书

- 数字证书由 CA 签发，用于将用户身份与公钥绑定。
- 最常见格式：X.509。
- 证书内容一般包括主体信息、公钥信息、CA 信息和 CA 的数字签名。
- 证书指纹不是证书内部字段，而是对整个证书计算得到的散列值，浏览器常显示 SHA-1 或 SHA-256 指纹。
- CRL：证书撤销列表。

4 第 5 章无线网络安全

4.1 无线局域网基础

- 无线网络由于频段开放和空间开放，更容易遭受窃听、非法接入、干扰和伪造攻击。
- IEEE 802.11 是无线局域网基础标准。
- 连接 AP 的三个阶段：扫描、认证、关联。

4.2 无线局域网安全风险

- 分组嗅探：攻击者可截获空中传播的数据。
- SSID 风险：SSID 广播会暴露网络信息，隐藏 SSID 只能提高门槛，不能根本防御。
- 假冒 AP：部署同名 AP 诱骗用户连接。
- 寄生者/蹭网：利用开放 AP 或破解密钥接入。
- 直接安全漏洞：WEP 等旧协议脆弱，无法抵御有意攻击。

4.3 风险缓解措施

- 合理设置 SSID，不使用暴露信息的名称。
- 关闭 SSID 广播。
- 调整天线摆放和覆盖范围。
- MAC 过滤：可限制部分接入，但容易被伪造绕过。

4.4 WEP、WPA、WPA2

- WEP：
  - 使用共享静态密钥；
  - 基于 RC4；
  - 容易因 IV 重复和协议设计缺陷被破解；
  - 完整性保护弱，常见被动和主动破解方式。
- WPA：
  - 是 WEP 的改进版；
  - 引入 TKIP；
  - 密钥更长，支持动态密钥；
  - 使用 MIC 增强完整性，使用 TSC 抗重放。

- WPA2：
  - 基于 IEEE 802.11i；
  - 使用 AES；
  - 采用 CCMP；
  - CTR 提供机密性，CBC-MAC 提供认证和完整性保护。

4.5 认证方式

- 802.1X：企业级认证，需要认证服务器参与。
- WPA-PSK：个人用户常见方式，基于预共享密钥。

4.6 常考比较

- WEP 与 WPA：WPA 使用 TKIP、动态密钥和 MIC，安全性明显高于 WEP。
- WPA 与 WPA2：WPA2 用 AES-CCMP 取代 RC4-TKIP，安全性进一步提升。
- MAC 过滤与真正加密认证的区别：前者只是弱接入控制，后者才是核心安全机制。

5 第 6 章数据链路层和网络层安全

5.1 数据链路层风险

- 混杂模式风险：网卡接收所有帧，便于嗅探、会话接管和流量分析。
- 常见工具：tcpdump、Snort、Wireshark。
- 混杂模式检测思路：利用 ARP、ICMP、DNS 异常响应特征。
- 其他风险：负载攻击、MAC 地址伪装、帧外数据利用、DHCP 耗竭、物理层攻击。

5.2 数据链路层安全措施

- 静态地址表、MAC 过滤等硬编码方法。
- CHAP：挑战握手身份认证，优于 PAP。
- PAP：用户名和口令明文传输，安全性弱。
- 高层身份认证和分析工具也可作为辅助手段。

5.3 MAC 与 ARP 风险

- MAC 风险：侦察、伪装、广播/多播负载攻击。
- ARP 风险：
  - ARP 表污染；
  - DoS 攻击；
  - 中间人攻击。
- 缓解措施：
  - 静态 ARP 表；
  - ARP 条目过期；
  - 过滤未经请求的 ARP 应答；
  - 锁定 ARP 表。

5.4 IPv4 风险与缓解

- IPv4 常见风险：地址冲突、IP 欺骗、重放、分组风暴、分段攻击、隧道隐蔽通信。
- 缓解方式：禁用部分协议、私网地址、NAT、反向 NAT、IP 过滤、出口过滤、IPsec。
- NAT 的安全效果：
  - 提供一定匿名性和隐私；
  - 默认阻止外部主动连接内网主机；
  - 只能支持内部主机主动发起的连接。

5.5 IPsec 总体结构

- IPsec 是网络层安全标准，核心目标是提供认证、完整性、机密性和密钥管理。
- 三个重要协议：AH、ESP、IKE。
- 两个核心数据库：
  - SAD：存储安全关联 SA；
  - SPD：存储安全策略 SP。
- SA 是单向的，描述使用何种协议、模式、算法、密钥、生存期等。

5.6 SA、SAD、SPD

- SA 由 SPI、目的地址、安全协议标识等确定。
- SAD 中保存：序列号计数器、抗重放窗口、认证算法、加密算法、运行模式、生存期等。
- SPD 中定义：某类 IP 分组应丢弃、绕过还是受 IPsec 保护。

5.7 IPsec 运行模式

- 传输模式：保护 IP 载荷，主要用于主机到主机。
- 隧道模式：保护整个原始 IP 包，主要用于网关到网关或主机到网关。
- 隧道模式安全功能更强，但带宽开销更大。

5.8 AH 协议

- 功能：完整性、数据源认证、抗重放。
- 不提供保密性。
- 核心机制：HMAC + 序列号 + 滑动窗口。
- AH 会认证整个 IP 包（IP 头中的可变字段置零后参与处理）。
- 因为 NAT 会修改 IP 头，所以 AH 与 NAT 不兼容。

5.9 ESP 协议

- 功能：加密、可选完整性认证、抗重放。
- 传输模式：保护载荷，不保护原 IP 头。
- 隧道模式：对整个原始 IP 包加密和认证，能提供数据流加密。
- ESP 不认证外层 IP 头，因此与 NAT 兼容性好于 AH。

5.10 AH 与 ESP 比较

- AH：重认证、轻保密，不加密，不能与 NAT 共存。
- ESP：强调加密与综合保护，验证范围比 AH 小，但兼容 NAT。
- 若需要公网主机间更强认证，可考虑 AH；若涉及 VPN、NAT、隐私保护，通常优先 ESP。

5.11 IPsec 应用

- 远程安全接入。
- 分支机构之间构建 VPN。
- 企业与合作伙伴建立安全互联。
- 优点：对应用透明，能统一保护各种基于 IP 的上层业务。

6 综合高频简答题

6.1 常见比较题

1. **对称密码与公开密码的比较。**

   对称密码加解密速度快，适合大量数据；公开密码速度较慢，但更便于密钥分发和管理。

2. **流密码与分组密码的比较。**

   流密码按位加密，速度快、实时性好；分组密码按组加密，不需密钥同步，适应性更强。

3. **MAC 与数字签名的比较。**

   MAC 依赖共享密钥，可验证完整性和来源，但不能抗抵赖；数字签名用私钥生成，可抗抵赖。

4. **静态口令、动态口令、一次性口令的比较。**

   静态口令长期不变，易被重放；动态口令会随时间或事件变化；一次性口令每次只能使用一次。

5. **WEP、WPA、WPA2 的比较。**

   WEP 使用静态密钥，安全性最弱；WPA 用 TKIP 改进；WPA2 采用 AES-CCMP，整体安全性最高。

6. **PAP 与 CHAP 的比较。**

   PAP 直接明文传送口令，容易被监听；CHAP 采用挑战响应机制，不直接传输口令，更安全。

7. **IPsec 传输模式与隧道模式的比较。**

   传输模式只保护 IP 载荷，开销较小；隧道模式保护整个原始 IP 包，安全性更强但开销更大。

8. **AH 与 ESP 的比较。**

   AH 提供认证和完整性，不提供加密，且不兼容 NAT；ESP 可提供加密和认证，通常兼容 NAT。

6.2 常见简答题

1. **网络安全的基本属性有哪些，各自如何实现?**

   机密性主要靠加密实现；完整性靠散列、MAC、签名；可用性靠容灾和抗攻击；抗抵赖靠数字签名。

2. **网络攻击按主动/被动如何分类？分别举例。**

   被动攻击只监听而不篡改，如窃听、流量分析；主动攻击会篡改或干扰，如重放、伪装、DoS。

3. **为什么说密码技术是网络安全的核心?**

   因为它不仅能实现保密，还能实现完整性、身份认证和抗抵赖，是多数安全协议的基础。

4. **RSA 的密钥生成过程是什么?**

   先选素数 p, q，计算 n 和 $\varphi(n)$，再选 e 并求逆元 d。公钥为 (e, n)，私钥为 (d, n)。

5. **为什么实际中通常采用混合加密?**

   因为对称加密速度快，适合加密数据；公开密码便于安全传输密钥，所以常组合使用。

6. **散列函数应满足哪些安全要求?**

   应满足单向性、抗碰撞性和雪崩效应，同时要求输入可变长、输出长度固定。

7. **为什么数字签名通常签名消息摘要而不是原文?**

   因为摘要长度固定、签名效率更高，而且只要原文被改动，摘要就会变化，便于验证完整性。

8. **Kerberos 的基本思想和票据机制是什么?**

   Kerberos 由 KDC 统一发放票据。用户先获得 TGT，再换取服务票据，并凭票据访问目标服务器。

9. **WEP 为什么容易被破解?**

   因为 WEP 使用静态密钥和较短的 IV，容易重复，且完整性保护机制较弱，所以易被破解。

10. **WPA2 为什么比 WPA 更安全?**

    因为 WPA2 使用 AES-CCMP，而 WPA 主要使用 TKIP，所以在加密和完整性保护上更安全。

11. **ARP 欺骗如何实现，如何防范?**

    攻击者通过伪造 ARP 应答改写受害主机 ARP 表。防范方法包括静态 ARP、过滤应答和动态检测。

12. **为什么 AH 与 NAT 不兼容，而 ESP 通常可以兼容?**

    AH 会认证 IP 头部，而 NAT 会修改 IP 头，导致校验失败；ESP 主要保护载荷，因此通常可兼容 NAT。

6.3 复习建议

- 先背定义和目标：机密性、完整性、可用性、认证、不可否认性。
- 再背比较题：对称/非对称、MAC/签名、WEP/WPA/WPA2、AH/ESP、传输/隧道。
- 最后掌握流程题：RSA 密钥生成、Kerberos 认证、S/KEY、IPsec 的 SPD/SAD/SA 关系。