↑ 목록으로 ← 이전 단원 다음 단원 →

3단원. 보안 기초 개념

> 대상: 전공자 · 정보처리기사 취득자 | 목적: 인프라 직무(네트워크·클라우드·시스템·보안) 기술 면접 대비 중요도: ★★★ 최빈출 · ★★ 자주 출제 · ★ 기본 개념

> **Q1.** 정보보안의 3대 요소(**CIA Triad**)를 설명하고 각각을 위협하는 사례를 드세요. ★★★

답안 정보보안의 핵심 목표는 기밀성(**Confidentiality**), 무결성(**Integrity**), 가용성(**Availability**)의 세 가지로 요약됩니다. 기밀성은 인가된 사용자만 정보에 접근할 수 있도록 하는 것으로, 이를 위협하는 사례는 데이터 유출이나 도청입니다. 무결성은 정보가 인가되지 않은 방식으로 변경·훼손되지 않도록 보장하는 것으로, 위·변조 공격이나 중간자 공격에 의한 데이터 조작이 위협 사례입니다. 가용성은 인가된 사용자가 필요할 때 정상적으로 서비스를 이용할 수 있도록 하는 것으로, **DDoS** 공격이나 랜섬웨어에 의한 서비스 마비가 대표적 위협입니다. 실무에서 보안 정책이나 통제를 설계할 때 이 세 요소 중 무엇을 우선적으로 보호할지 트레이드오프를 고려하는 경우가 많습니다.

관련 개념 기밀성/무결성/가용성, 부인방지(Non-repudiation), 인증(Authenticity), DDoS, 데이터 위변조

> **Q2.** 대칭키 암호화와 비대칭키 암호화의 차이를 설명하고 각각의 장단점을 설명하세요. ★★★

답안 대칭키 암호화는 암호화와 복호화에 동일한 키를 사용하는 방식으로(예: AES), 연산 속도가 빨라 대용량 데이터 암호화에 적합하지만 키를 안전하게 전달·공유하는 문제(키 분배 문제)가 있습니다. 비대칭키 암호화(공개키 암호화)는 공개키와 개인키의 쌍을 사용해, 공개키로 암호화한 데이터는 반드시 대응하는 개인키로만 복호화할 수 있는 방식으로(예: RSA), 키 분배 문제를 해결할 수 있지만 연산이 복잡해 속도가 느립니다. 이 때문에 실무에서는 하이브리드 방식을 주로 사용하는데, 비대칭키로 대칭키(세션키)를 안전하게 교환한 뒤 실제 데이터 통신은 빠른 대칭키로 암호화하는 방식이며, 이는 TLS의 핵심 동작 원리이기도 합니다.

관련 개념 AES, RSA, 키 분배 문제, 하이브리드 암호화, 세션키

> **Q3. TLS/SSL** 핸드셰이크 과정을 개략적으로 설명하세요. ★★★

답안 TLS 핸드셰이크는 클라이언트와 서버가 안전한 통신 채널을 수립하는 과정입니다. 클라이언트가 지원 가능한 암호 방식 목록을 담아 **ClientHello**를 보내면, 서버는 사용할 암호 방식과 자신의 인증서(공개키 포함)를 담아 **ServerHello + Certificate**로 응답합니다. 클라이언트는 인증서를 신뢰할 수 있는 **CA(**인증기관**)**의 서명으로 검증한 뒤, 서버 공개키로 암호화한 세션키(또는 키 교환 값)를 전달합니다. 이후 양측은 이 세션키를 기반으로 대칭키 암호화로 실제 데이터를 주고받습니다. 이 과정에서 인증서 검증은 서버 신원 확인(인증)을, 세션키 교환은 기밀성을 보장하는 역할을 합니다.

관련 개념 인증서(CA, 공개키), ClientHello/ServerHello, 세션키 교환, 서버 신원 검증, TLS 1.3 개선점

Q4. 해시 함수의 특징과 용도를 설명하고, 암호화와 어떻게 다른지 설명하세요. ★★★

답안 해시 함수는 임의 길이의 입력을 고정된 길이의 출력(해시값)으로 변환하는 함수로, 일방향성(입력으로부터 출력은 쉽지만 역산은 사실상 불가능)과 충돌 저항성(서로 다른 입력이 같은 출력을 내기 어려움)이라는 특징을 갖습니다. 암호화는 복호화를 전제로 하지만, 해시는 원래 값으로 되돌릴 수 없다는 점이 결정적 차이입니다. 실무에서는 비밀번호를 원문 그대로 저장하지 않고 해시값(주로 솔트를 추가한 형태)으로 저장해 데이터 유출 시에도 원문 비밀번호가 드러나지 않도록 하며, 파일의 무결성 검증(다운로드 파일의 체크섬 비교)이나 디지털 서명에도 활용됩니다.

관련 개념 일방향성, 충돌 저항성, 솔트(Salt), SHA 계열, 무결성 검증

Q5. 인증(**Authentication**)과 인가(**Authorization**)의 차이를 설명하세요. ★★★

답안 인증은 "당신이 누구인지"를 확인하는 절차로, 아이디/비밀번호, 인증서, 생체정보, OTP 등을 통해 사용자의 신원을 검증하는 것입니다. 인가는 인증이 완료된 사용자에게 "무엇을 할 수 있는지" 권한을 부여하는 절차로, 특정 자원에 대한 읽기/쓰기/실행 권한을 결정합니다. 즉 로그인에 성공했다고 해서 모든 리소스에 접근할 수 있는 것은 아니며, 로그인 이후 역할(Role)이나 정책에 따라 접근 가능한 범위가 인가를 통해 별도로 결정됩니다. 실무에서는 다중 인증(**MFA**)으로 인증을 강화하고, **RBAC(**역할 기반 접근 제어**)**로 인가를 세밀하게 관리하는 것이 일반적인 보안 설계 원칙입니다.

관련 개념 MFA(다중 인증), RBAC/ABAC, 최소 권한 원칙, 세션 관리, SSO

Q6. 방화벽의 종류(패킷 필터링, 상태 기반, 애플리케이션 레벨)를 비교해 설명하세요. ★★★

답안 패킷 필터링 방화벽은 IP 주소, 포트, 프로토콜 등 패킷 헤더 정보만 보고 미리 정의된 규칙(ACL)에 따라 허용/차단을 결정하는 가장 기본적인 방식으로 속도는 빠르지만 세션 상태를 추적하지 못합니다. 상태 기반 방화벽(**Stateful Inspection**)은 연결의 상태(세션 테이블)를 추적해, 예를 들어 내부에서 시작한 연결의 응답 패킷은 별도 규칙 없이도 자동으로 허용하는 등 더 정교한 제어가 가능하며 현재 대부분의 방화벽이 이 방식을 채택합니다. 애플리케이션 레벨 방화벽(프록시/**L7** 방화벽, **WAF** 포함)은 페이로드 내용까지 검사해 특정 애플리케이션 프로토콜의 이상 행위나 SQL 인젝션 같은 공격 패턴까지 탐지할 수 있지만 처리 부하가 큽니다. 실무 네트워크는 보통 이 세 방식을 계층적으로 조합해 운영합니다.

관련 개념 Stateful Inspection, ACL, WAF, 세션 테이블, 프록시 방화벽

Q7. IDS와 **IPS**의 차이를 설명하세요. ★★★

답안 **IDS(Intrusion Detection System)**는 네트워크나 시스템의 트래픽을 모니터링해 공격 시그니처나 이상 행위를 탐지하고 알림(경고)만 발생시키는 시스템으로, 일반적으로 트래픽 경로 밖에서 미러링된 트래픽을 수동적으로 관찰(**Passive**)합니다. **IPS(Intrusion Prevention System)**는 트래픽 경로 상에 직접 위치해(In-line) 탐지된 공격을 실시간으로 차단(**Active**)할 수 있다는 점이 핵심 차이입니다. IPS는 즉각적인 방어가 가능하다는 장점이 있지만, 오탐(**False Positive**)이 발생하면 정상 트래픽까지 차단해 서비스 장애를 유발할 위험이 있어 튜닝이 중요합니다. 탐지 방식으로는 알려진 패턴과 비교하는 시그니처 기반과 정상 행위 패턴에서 벗어남을 감지하는 이상탐지 기반이 있습니다.

관련 개념 시그니처 기반/이상탐지 기반, In-line/Passive, 오탐(False Positive)/미탐(False Negative), NIDS/HIDS, 차단 정책

Q8. 디지털 서명(**Digital Signature**)의 동작 원리와 목적을 설명하세요. ★★

답안 디지털 서명은 송신자가 메시지의 해시값을 자신의 개인키로 암호화해 메시지에 첨부하는 방식으로 동작합니다. 수신자는 송신자의 공개키로 서명을 복호화해 원본 해시값을 얻고, 받은 메시지를 직접 해싱한 값과 비교해 일치하면 메시지가 변조되지 않았고(무결성), 실제로 해당 개인키 소유자가 보냈다는 것(인증, 부인방지)을 동시에 검증할 수 있습니다. 이는 공개키 암호화와 반대 방향으로 키를 사용하는 점이 특징이며, 실무에서는 소프트웨어 배포 시 코드 서명, 전자문서의 서명, 인증서 발급(CA가 인증서에 서명) 등에 활용됩니다.

관련 개념 개인키/공개키, 해시값 서명, 부인방지, 인증서(CA 서명), 전자서명법

Q9. 최소 권한 원칙과 심층 방어(**Defense in Depth**)의 개념을 설명하세요. ★★

답안 최소 권한 원칙(**Principle of Least Privilege**)은 사용자나 프로세스에게 업무 수행에 꼭 필요한 최소한의 권한만 부여해야 한다는 보안 원칙으로, 계정이 탈취되더라도 피해 범위를 최소화하는 데 목적이 있습니다. 심층 방어는 단일 보안 장비나 통제에 의존하지 않고 네트워크, 시스템, 애플리케이션, 데이터 등 여러 계층에 걸쳐 중첩된 보안 통제를 배치하는 전략으로, 하나의 방어선이 뚫려도 다음 계층에서 공격을 저지할 수 있도록 설계합니다. 예를 들어 방화벽 + IPS + 서버 하드닝 + 애플리케이션 인증 + 데이터 암호화를 겹겹이 적용하는 것이 심층 방어의 사례입니다. 두 개념 모두 "완벽한 방어는 없다"는 전제 하에 피해를 최소화하기 위한 설계 철학입니다.

관련 개념 최소 권한, 심층 방어, 계정 권한 관리, 제로 트러스트, 보안 계층화

> **Q10.** 대칭키 암호화 알고리즘 **AES**와 비대칭키 알고리즘 **RSA**를 각각 어디에 사용하는지 실무 관점에서 설명하세요. ★

답안 **AES(Advanced Encryption Standard)**는 빠른 연산 속도 덕분에 대용량 데이터의 실제 암호화에 널리 사용되며, 디스크 암호화, VPN 터널 내 데이터 암호화, TLS 세션 수립 이후의 데이터 전송 구간 암호화 등에 사용됩니다. **RSA**는 연산이 무겁기 때문에 대용량 데이터를 직접 암호화하기보다는 키 교환이나 디지털 서명, 인증서 발급처럼 상대적으로 적은 데이터를 다루는 곳에 사용됩니다. 즉 TLS 통신에서는 초기 핸드셰이크 단계에 RSA(또는 ECDHE 등)로 세션키를 안전하게 교환하고, 이후 실제 데이터 송수신은 AES로 처리하는 조합이 대표적인 실무 활용 사례입니다.

관련 개념 AES, RSA, TLS 핸드셰이크, 키 교환(ECDHE), 디스크 암호화
