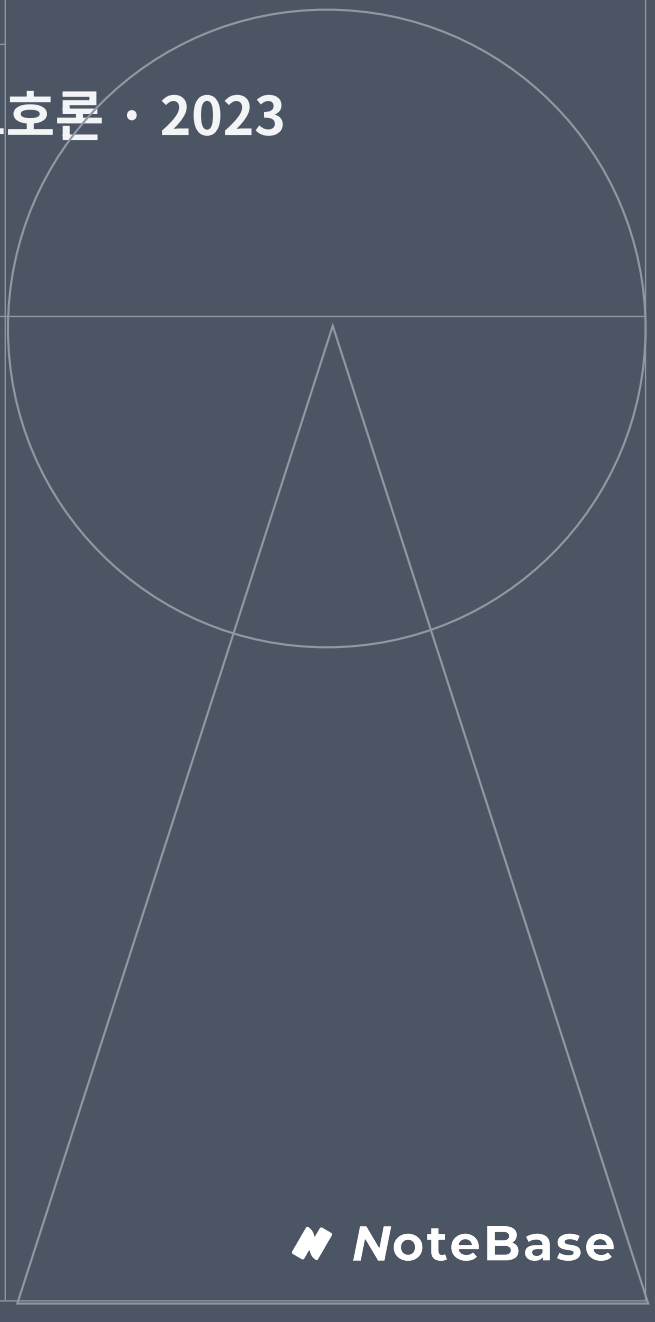
기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2023



NoteBase

기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2023

공무원/군무원/9급 · 정보보호론 · 2023

1. 정보보호의 기본 목표 중 아래에 대한 설명으로 가장 적절한 것은?

> - 허락된 사용자는 자산, 서비스를 적절하고 신뢰성 있게 이용할 수 있어야 한다.
> - 이것을 보존하기 위해 행해지는 활동으로는 백업, 시스템 및 네트워크 용량 증설, 침입 탐지 시스템 운용 등이 있다.

① 기밀성　② 무결성
③ 가용성　④ 인증성

정답 3번

출제 포인트

허락된 사용자가 필요할 때 자산과 서비스를 신뢰성 있게 이용하도록 보장하는 정보보호 목표가 가용성임을 판별하는 문제이다.

핵심 개념

기밀성: 허가되지 않은 주체에게 정보가 공개되지 않도록 보호하는 성질이다. 키워드는 비인가 공개 방지이다.
무결성: 정보와 시스템이 허가되지 않게 변경되거나 훼손되지 않도록 정확성과 완전성을 유지하는 성질이다. 키워드는 변조 방지이다.
가용성: 허락된 사용자가 필요할 때 자산과 서비스를 적절하고 신뢰성 있게 이용할 수 있도록 보장하는 성질이다. 키워드는 중단 없는 이용이다.
인증성: 사용자나 시스템의 신원 및 정보의 출처가 진짜임을 확인할 수 있는 성질이다. 키워드는 신원·출처 확인이다.

NoteBase

선지별 해설

① X — 기밀성은 비인가자에게 정보가 노출되지 않도록 하는 목표이다. 제시문은 정보의 비인가 공개 방지가 아니라 허락된 사용자의 신뢰성 있는 이용을 설명하므로 틀리다. '기밀성'이 아니라 '가용성'이 올바른 표현이다.
② X — 무결성은 정보나 시스템의 허가되지 않은 변경·훼손을 막아 정확성과 완전성을 유지하는 목표이다. 제시문의 백업, 용량 증설, 침입 탐지 시스템 운영은 서비스 이용 가능 상태를 유지하기 위한 활동이므로 '무결성'이 아니라 '가용성'이 올바른 표현이다.
③ O — 가용성은 허락된 사용자가 필요할 때 자산과 서비스를 적절하고 신뢰성 있게 이용할 수 있도록 보장하는 목표이다. 백업, 시스템·네트워크 용량 증설, 침입 탐지 시스템 운영은 장애나 공격으로 인한 서비스 중단을 줄여 가용성을 보존한다.
④ X — 인증성은 사용자나 시스템의 신원 또는 정보의 출처가 진짜인지 확인하는 성질이다. 제시문은 신원·출처 확인이 아니라 자산과 서비스의 지속적인 이용을 설명하므로 '인증성'이 아니라 '가용성'이 올바른 표현이다.

오답 포인트

백업과 침입 탐지 시스템을 데이터 보호나 사용자 확인 수단으로만 보고 기밀성·무결성·인증성과 혼동하기 쉽다. 이 문항에서는 활동의 명칭보다 '허락된 사용자가 신뢰성 있게 이용한다'와 '용량 증설'이라는 문구가 가용성을 직접 가리킨다.

다시 나오면 이렇게 판단

공개 여부는 기밀성, 변경·훼손 여부는 무결성, 필요할 때 이용 가능한지는 가용성, 신원·출처의 진위 확인은 인증성으로 구분한다. 특히 백업, 이중화, 용량 증설, 장애 복구처럼 서비스 중단을 예방하거나 복구하는 활동은 가용성으로 판단한다.

암기 포인트

기밀성은 못 보게, 무결성은 못 바꾸게, 가용성은 필요할 때 쓰게, 인증성은 진짜인지 확인하게 하는 목표이다.

NoteBase

2. 다음 중 자체적으로 실행되면서 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성코드는?
① 루트킷 ② 바이러스
③ 웜 ④ 트로이목마

정답 3번

출제 포인트

악성코드가 숙주 프로그램 없이 자율적으로 실행되면서 네트워크를 통해 자신을 복제·전파하는지를 구별하는 문제이다.

핵심 개념

웜은 독립적으로 실행되며 네트워크의 취약점 등을 이용해 자기 자신을 다른 시스템으로 복제·전파하는 악성코드이다.
바이러스는 파일이나 부트 영역 같은 숙주에 기생하여 복제되고, 트로이목마는 정상 프로그램으로 위장하지만 스스로 복제하지 않으며, 루트킷은 침입 흔적이나 악성 활동을 숨기는 데 초점이 있다.

선지별 해설

① X — 루트킷은 공격자가 획득한 권한이나 악성 프로세스·파일 등의 흔적을 숨겨 탐지를 어렵게 하는 도구이다. 틀린 표현은 '자체적으로 실행되면서 네트워크를 통해 자신을 복제하고 전파한다'는 성질을 루트킷에 대응시킨 부분이며, 올바르게는 이러한 악성코드는 웜이다.
② X — 바이러스는 일반적으로 숙주 파일이나 프로그램에 자신을 삽입하고 감염된 숙주가 실행될 때 복제된다. 틀린 표현은 '독립적으로 실행되어 네트워크로 자기 복제·전파한다'는 부분이며, 올바르게는 이는 웜의 특징이다.
③ O — 웜은 숙주 프로그램 없이 자율적으로 실행되며 네트워크를 통해 다른 시스템으로 자기 자신을 복제하고 전파하므로 문제의 설명과 일치한다.
④ X — 트로이목마는 정상적이거나 유용한 프로그램처럼 위장하여 사용자의 실행을 유도한 뒤 악성 기능을 수행하며, 자기 복제 기능은 없다. 틀린 표현은 '자신을 복제하고 전파한다'는 부분이며, 올바르게는 자기 복제 없이 위장하여 침투하는 악성코드가 트로이목마이다.

오답 포인트

② 바이러스도 복제된다는 점 때문에 웜과 혼동하기 쉽다. 그러나 이 문항의 결정적 표현은 '자체적으로 실행'과 '네트워크를 통해 전파'이며, 이는 숙주에 기생하는 바이러스가 아니라 웜을 가리킨다.

NoteBase

다시 나오면 이렇게 판단

숙주 없이 독립 실행하고 네트워크를 따라 자동으로 자기 복제하면 웜, 숙주 파일에 기생하면 바이러스, 정상 프로그램으로 위장하지만 자기 복제를 하지 않으면 트로이목마, 침입 흔적과 악성 활동을 숨기면 루트킷으로 판단한다.

암기 포인트

웜은 독립·네트워크·자기 복제, 바이러스는 숙주 감염, 트로이목마는 위장, 루트킷은 은닉이다.

3. 다음 중 강제적 접근 제어 모델에 대한 설명으로 가장 적절하지 않은 것은?
① 접근 권한이 시스템의 전체적인 보안 정책 및 관련 규칙에 따라 결정된다.
② 주체와 객체의 수가 증가함에 따라 규칙의 수도 기하급수적으로 증가하는 문제가 있다.
③ 시스템의 모든 주체와 객체가 보안 레이블을 반드시 갖는다.
④ 기밀문서가 엄격히 다루어지는 군이나 정보기관 등에 적합하다.

정답 2번

출제 포인트

강제적 접근 제어(MAC)의 권한 결정 방식, 보안 레이블, 적용 분야를 정확히 구별하는 문제이다.

핵심 개념

강제적 접근 제어는 시스템이 정한 보안 정책에 따라 주체의 인가 수준과 객체의 보안 등급을 비교하여 접근을 통제하는 방식이다. 개별 사용자가 임의로 권한을 부여하거나 변경할 수 없으며, 주체와 객체에 부여된 보안 레이블이 접근 판단의 핵심 기준이 된다.

선지별 해설

① O — 접근 권한은 사용자의 자율적 판단이 아니라 시스템 전체의 보안 정책과 관련 규칙에 따라 중앙에서 결정된다.
② X — 틀린 표현은 '주체와 객체의 수가 증가함에 따라 규칙의 수도 기하급수적으로 증가한다'이다. 강제적 접근 제어는 주체와 객체의 보안 레이블을 비교하는 공통 정책으로 접근 여부를 판단하므로, 개별 주체·객체 쌍마다 규칙을 반드시 추가하여 규칙 수가 기하급수적으로 늘어나는 모델이라고 볼 수 없다. 올바르게는 '주체와 객체가 증가해도 보안 레이블과 공통 정책에 따라 접근을 통제한다'이다.
③ O — 강제적 접근 제어에서는 모든 주체와 객체에 보안 레이블을 부여하고, 이 레이블의 관계에 따라 접근 허용 여부를 판단한다.
④ O — 기밀문서의 등급과 사용자의 인가 수준을 엄격히 비교해야 하는 군이나 정보기관과 같은 환경에 적합하다.

오답 포인트

②의 '수가 늘면 규칙도 기하급수적으로 증가한다'는 표현을 접근 제어의 일반적 관리 부담과 혼동하기 쉽다. 강제적 접근 제어의 핵심은 개별 관계마다 임의로 권한을 정하는 것이 아니라 보안 레이블과 중앙 정책으로 일관되게 판정하는 데 있다.

NoteBase

다시 나오면 이렇게 판단

선지에서 중앙 보안 정책, 주체·객체의 보안 레이블, 엄격한 기밀성 통제를 말하면 강제적 접근 제어의 특징으로 판단한다. 개별 사용자나 개별 주체·객체 쌍 중심의 임의적 권한 설정을 핵심 특징으로 제시하면 강제적 접근 제어와 맞지 않는다고 판단한다.

암기 포인트

MAC는 중앙 정책과 보안 레이블로 강제 통제하며, 군·정보기관처럼 기밀성이 중요한 환경에 적합하다.

NoteBase

4. 다음 중 정상적인 프로그램으로 위장하여 사용자로 하여금 실행을 유도하는 악성 프로그램은?
① 트로이목마 ② 백도어
③ 루트킷 ④ 셸코드

정답 1번

출제 포인트

정상적인 프로그램처럼 위장하여 사용자가 직접 실행하도록 유도하는 악성코드가 트로이목마임을 구별하는 문제이다.

핵심 개념

트로이목마는 유용하거나 정상적인 프로그램으로 가장해 설치·실행을 유도한 뒤 악성 기능을 수행한다.
백도어는 정상 인증 절차를 우회하여 시스템에 다시 접근할 수 있는 통로이고, 루트킷은 공격자의 존재나 악성 활동을 숨기면서 높은 권한을 유지하는 도구 집합이며, 셸코드는 취약점 공격 뒤 명령 실행 권한 등을 얻기 위해 사용되는 작은 코드 조각이다.

선지별 해설

① O — 트로이목마는 정상·유용한 프로그램처럼 위장하여 사용자의 설치나 실행을 유도하므로 문제의 설명과 일치한다.
② X — 틀린 부분은 '정상적인 프로그램으로 위장하여 사용자 실행을 유도하는 프로그램'을 백도어로 본 점이다. 백도어는 정상적인 인증이나 접근 통제를 우회해 시스템에 접근할 수 있도록 만든 비밀 통로이다.
③ X — 틀린 부분은 해당 위장·실행 유도형 악성코드를 루트킷으로 본 점이다. 루트킷은 공격자의 프로세스·파일·접속 흔적 등을 숨기고 높은 권한을 은밀하게 유지하는 도구 집합이다.
④ X — 틀린 부분은 해당 악성 프로그램을 셸코드로 본 점이다. 셸코드는 주로 취약점 공격의 페이로드로 실행되어 셸 획득이나 임의 명령 실행을 가능하게 하는 작은 코드 조각이다.

오답 포인트

트로이목마가 실행된 뒤 백도어를 설치하거나 루트킷으로 흔적을 숨길 수 있어 용어를 혼동하기 쉽다. 그러나 이 문항의 결정적 표현은 '정상적인 프로그램으로 위장'과 '사용자로 하여금 실행을 유도'이다.

다시 나오면 이렇게 판단

정상 프로그램으로 위장해 사용자의 자발적 실행을 유도하면 트로이목마, 인증 우회 접근 통로이면 백도어, 은폐와 권한 유지가 핵심이면 루트킷, 취약점 공격에서 실행되는 코드 조각이면 셸코드로 판단한다.

NoteBase

암기 포인트

위장·실행 유도는 트로이목마, 우회 통로는 백도어, 은폐는 루트킷, 공격용 코드 조각은 셸코드이다.

NoteBase

5. 다음 중 이산대수 문제를 효율적으로 풀 수 있다면 깨지는 알고리즘은?
① AES ② RSA
③ Diffie-Hellman ④ SHA

정답 3번

출제 포인트

이산대수 문제를 효율적으로 풀 수 있을 때 직접 안전성이 무너지는 공개키 암호 기술을 구별하는 문제이다.

핵심 개념

이산대수 문제는 밑과 거듭제곱 결과가 주어졌을 때 그 지수를 구하는 문제이다. Diffie–Hellman에서는 공개값으로부터 비밀 지수를 알아내기 어렵다는 성질이 핵심 안전성의 기반이므로, 이산대수를 효율적으로 계산하면 공유 비밀값을 복원할 수 있다.
AES는 대칭키 블록 암호이고, RSA는 큰 정수의 소인수분해 난이도에 기반하며, SHA는 해시 함수이다.

선지별 해설

① AES — X
AES의 안전성은 이산대수 문제가 아니라 비밀키 탐색의 어려움과 알려진 암호해독 공격에 대한 내성에 기반한다. 틀린 연결은 '이산대수 문제를 효율적으로 풀면 AES가 깨진다'이며, 올바르게는 AES의 키를 효율적으로 탐색하거나 AES 자체에 대한 실용적 암호해독법이 발견되면 안전성이 무너진다.

② RSA — X
RSA의 대표적인 안전성 기반은 큰 합성수를 소인수분해하기 어렵다는 점이다. 틀린 연결은 '이산대수 문제를 효율적으로 풀면 RSA가 깨진다'이며, 올바르게는 RSA 모듈러스를 효율적으로 소인수분해하면 개인키를 계산할 수 있다.

③ Diffie–Hellman — O
Diffie–Hellman은 공개값에서 비밀 지수를 구하기 어려운 이산대수 문제에 의존한다. 이산대수를 효율적으로 풀면 각 참여자의 비밀 지수를 알아내 공유 비밀값을 계산할 수 있으므로 키 교환의 기밀성이 깨진다.

④ SHA — X
SHA 계열은 입력을 고정 길이 해시값으로 바꾸는 해시 함수이며 이산대수 문제에 기반하지 않는다. 틀린 연결은 '이산대수 문제를 효율적으로 풀면 SHA가 깨진다'이며, 올바르게는 효율적인 역상 공격이나 제2역상 공격 또는 충돌 공격이 가능해지면 해당 보안 성질이 무너진다.

NoteBase

오답 포인트

RSA와 Diffie–Hellman이 모두 공개키 암호 기술이라는 이유만으로 같은 수학 문제에 기반한다고 혼동하기 쉽다. RSA는 소인수분해, Diffie–Hellman은 이산대수라는 기반 문제의 차이가 핵심 함정이다.

다시 나오면 이렇게 판단

알고리즘 이름을 수학적 난제와 연결해 판단한다. 이산대수는 Diffie–Hellman, 소인수분해는 RSA, 비밀키 탐색은 AES, 역상·제2역상·충돌은 SHA와 연결된다.

암기 포인트

DH는 이산대수, RSA는 소인수분해, AES는 대칭키, SHA는 해시이다.

NoteBase

6. 다음 중 인터넷과 같은 공중망에 터널을 형성하고 이를 통해 패킷을 캡슐화하여 전달함으로써 사설망과 같은 전용 회선처럼 사용할 수 있게 하는 기술에 해당하지 않는 것은?

① PPTP ② L2TP
③ ICMP ④ IPSec

정답 3번

출제 포인트

공중망에서 사설망처럼 통신하도록 패킷을 캡슐화하는 터널링 기술과, 네트워크 제어·오류 보고용 프로토콜을 구별하는 문제이다.

핵심 개념

터널링은 원래 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 공중망을 통해 전달하는 방식이다. PPTP와 L2TP는 터널을 구성하는 프로토콜이고, IPSec는 IP 계층에서 인증·무결성·기밀성을 제공하며 터널 모드로 VPN을 구현할 수 있다. 반면 ICMP는 IP 통신 과정의 오류 보고와 진단·제어 메시지 전달에 사용되며 VPN 터널링 기술이 아니다.

선지별 해설

① X — PPTP는 PPP 프레임을 캡슐화하여 IP망에 터널을 형성하는 VPN 터널링 프로토콜이다. 틀린 판단은 'PPTP가 터널링 기술에 해당하지 않는다'이며, 올바르게는 'PPTP는 터널링 기술에 해당한다'이다.
② X — L2TP는 2계층 프레임을 공중 IP망 등으로 운반하기 위한 터널을 구성하는 프로토콜이다. 틀린 판단은 'L2TP가 터널링 기술에 해당하지 않는다'이며, 올바르게는 'L2TP는 터널링 기술에 해당한다'이다.
③ O — ICMP는 IP 패킷 전달 중 발생한 오류를 알리고 네트워크 상태를 진단·제어하는 메시지 프로토콜이므로, 제시된 VPN 터널링 기술에 해당하지 않는다.
④ X — IPSec는 IP 계층 보안 프로토콜 집합이며, 터널 모드에서는 원래 IP 패킷 전체를 보호·캡슐화하여 VPN 터널을 구성한다. 틀린 판단은 'IPSec가 터널링 기술에 해당하지 않는다'이며, 올바르게는 'IPSec는 터널 모드로 VPN 터널링에 사용된다'이다.

오답 포인트

③ ICMP도 IP 계층과 관련된 프로토콜이라는 이유만으로 IPSec와 같은 터널링 기술로 오인하기 쉽다. 그러나 ICMP의 핵심 기능은 오류 보고와 진단이며, IPSec의 터널 모드는 원래 IP 패킷 전체를 보호·캡슐화한다. 또한 문제의 '해당하지 않는'이라는 부정형을 놓치면 터널링 기술인 PPTP·L2TP·IPSec를 고르기 쉽다.

NoteBase

다시 나오면 이렇게 판단

각 프로토콜의 주된 목적을 먼저 구분한다. PPTP·L2TP는 터널 형성, IPSec 터널 모드는 IP 패킷 보호와 캡슐화, ICMP는 오류 보고와 진단으로 판단한다.

암기 포인트

PPTP·L2TP·IPSec는 VPN 터널, ICMP는 오류 보고·진단이다.

NoteBase

7. 다음 위험 분석 중 가장 기본적이고 일반적인 수준에서 보안 통제 항목의 구현 여부를 조사하는 접근법은?
① 상세 접근법(Detailed Risk Analysis)
② 기준 접근법(Baseline Approach)
③ 비정형 접근법(Informal Approach)
④ 통합 접근법(Combined Approach)

정답 2번

출제 포인트

위험 분석 접근법 가운데 조직에 공통으로 적용할 보안 통제 기준을 정해 두고 그 구현 여부를 점검하는 가장 기본적이고 일반적인 방법을 구별하는 문제이다.

핵심 개념

기준 접근법(Baseline Approach)은 표준화된 보안 통제의 기준선(baseline)을 설정하고 각 통제 항목의 구현 여부를 점검하는 방법이다. 자산별 위험을 일일이 정밀 분석하지 않아도 공통적인 최소 보호 수준을 신속하게 확보할 수 있다.
상세 접근법은 자산 가치, 위협, 취약점, 발생 가능성 및 영향을 개별적으로 정밀 분석한다. 비정형 접근법은 정형화된 절차보다 전문가의 경험과 판단에 의존한다. 통합 접근법은 자산의 중요도와 위험 수준에 따라 상세 접근법과 기준 접근법 등을 함께 사용한다.

선지별 해설

① X — 상세 접근법(Detailed Risk Analysis)은 자산별 위협·취약점·발생 가능성·영향을 구체적으로 분석하는 정밀한 방법이므로, 공통 보안 통제의 구현 여부를 기본 수준에서 조사하는 방법이 아니다. 틀린 표현은 '상세 접근법'이며, 올바르게는 '기준 접근법'이다.
② O — 기준 접근법(Baseline Approach)은 공통적인 보안 통제의 기준선을 마련하고 통제 항목이 구현되었는지를 확인하는 기본적이고 일반적인 접근법이다.
③ X — 비정형 접근법(Informal Approach)은 정형화된 기준선에 따라 통제 구현 여부를 조사하는 방식이 아니라 전문가의 지식·경험·판단을 활용하는 방식이다. 틀린 표현은 '비정형 접근법'이며, 올바르게는 '기준 접근법'이다.
④ X — 통합 접근법(Combined Approach)은 모든 대상을 하나의 기본 기준으로만 조사하는 방식이 아니라 중요 자산에는 상세 분석을 적용하고 나머지에는 기준 접근법 등을 적용하는 혼합 방식이다. 틀린 표현은 '통합 접근법'이며, 올바르게는 '기준 접근법'이다.

NoteBase

오답 포인트

‘가장 기본적이고 일반적인 수준’이라는 표현 때문에 절차가 덜 정형적인 비정형 접근법을 고르기 쉽다. 그러나 이 문항의 결정적 단서는 ‘보안 통제 항목의 구현 여부를 조사’한다는 부분이다. 공통 통제 목록과 기준선을 바탕으로 점검하는 방법은 기준 접근법이다.

다시 나오면 이렇게 판단

공통 통제, 최소 보호 수준, 체크리스트, 구현 여부가 제시되면 기준 접근법으로 판단한다. 자산별 정밀 산정이면 상세 접근법, 전문가 경험 중심이면 비정형 접근법, 중요도에 따라 여러 방법을 나누어 적용하면 통합 접근법이다.

암기 포인트

기준은 공통 통제 점검, 상세는 자산별 정밀 분석, 비정형은 경험과 판단, 통합은 위험 수준별 혼합 적용이다.

NoteBase

8. 다음 대칭키 운영 모드 중 보안성이 가장 높은 방법으로, 각 블록은 이전 암호문과 XOR 연산 후에 암호화되며 한 블록에서 발생한 에러가 다음 블록들에 영향을 주기 때문에 병렬 처리가 불가능한 특징을 갖는 것은?

① ECB ② CBC
③ CFB ④ CTR

정답 2번

출제 포인트

블록 암호 운용 모드별 블록 결합 방식과 오류 전파·병렬 처리 특성을 구별하는 문제이다.

핵심 개념

ECB는 각 평문 블록을 서로 독립적으로 암호화한다. CBC는 현재 평문 블록을 이전 암호문 블록과 XOR한 뒤 암호화하므로 블록들이 연쇄적으로 연결된다. CFB는 이전 암호문을 암호화한 출력과 현재 평문을 XOR하여 암호문을 만든다. CTR은 연속된 카운터 값을 암호화한 출력과 평문을 XOR하므로 각 블록을 독립적으로 처리할 수 있다.

NoteBase

선지별 해설

① ECB — X
각 블록을 독립적으로 암호화하므로 이전 암호문과 XOR하지 않으며, 동일한 평문 블록이 동일한 암호문 블록으로 나타날 수 있다. 틀린 표현은 문제의 연쇄 처리 특성을 ECB로 본 부분이며, 올바르게는 CBC이다.

② CBC — O
현재 평문 블록을 이전 암호문 블록과 XOR한 후 블록 암호로 암호화한다. 이전 블록의 결과가 다음 블록의 입력에 필요하므로 암호화의 병렬 처리가 어렵고, 암호문 블록의 오류가 복호화 과정에서 현재 평문 블록과 다음 평문 블록에 영향을 준다.

③ CFB — X
CFB는 이전 암호문 블록을 암호화한 값과 현재 평문을 XOR하는 피드백 방식이다. 문제처럼 현재 평문을 이전 암호문과 먼저 XOR한 뒤 암호화하는 구조가 아니다. 틀린 표현은 해당 구조를 CFB로 본 부분이며, 올바르게는 CBC이다.

④ CTR — X
CTR은 이전 암호문이 아니라 서로 다른 카운터 값을 암호화한 출력과 평문을 XOR한다. 블록별 카운터를 미리 계산할 수 있어 병렬 처리가 가능하고 오류도 다른 블록으로 전파되지 않는다. 틀린 표현은 연쇄적 오류 전파와 병렬 처리 불가를 CTR의 특성으로 본 부분이며, 올바르게는 CBC이다.

오답 포인트

CBC와 CFB는 모두 이전 암호문을 이용하지만 연산 순서가 다르다. CBC는 '평문 XOR 이전 암호문 → 블록 암호화'이고, CFB는 '이전 암호문을 블록 암호화 → 평문과 XOR'이다. 또한 보안성이 높다는 표현만으로 고르기보다 문제에 제시된 결합 구조와 오류 전파 특성을 기준으로 판단해야 한다.

다시 나오면 이렇게 판단

현재 평문과 이전 암호문을 먼저 XOR한 뒤 암호화하면 CBC로 판단한다. 블록이 서로 독립적이면 ECB, 이전 암호문을 암호화한 뒤 평문과 XOR하면 CFB, 카운터를 암호화한 뒤 평문과 XOR하면 CTR이다.

암기 포인트

CBC는 이전 암호문과 먼저 XOR한 뒤 암호화하는 연쇄 모드이다.

NoteBase

9. RSA 암호 시스템에서 밥이 앨리스의 공개키 (e, N) = (7, 143)을 취득하여 앨리스에게 평문 9를 암호화하여 보내고자 한다. 이때 전송되는 암호문은?

① $9^7 \mod 143$ ② $7^9 \mod 143$

③ $143^7 \mod 9$ ④ $7^{143} \mod 9$

정답 1번

출제 포인트

RSA에서 공개키의 지수와 모듈러스를 올바른 자리에 대입하여 평문을 암호화하는 식을 고르는 문제이다.

조건 정리

주어진 공개키: e, N = 7,143

평문: $M = 9$

구해야 할 값: 암호문 C

주의할 조건: 평문 M을 밑으로, 공개 지수 e를 지수로 두고, N으로 나눈 나머지를 구한다.

사용할 공식

C=M^e N

이 공식을 쓰는 이유: RSA 암호화는 수신자의 공개키 e, N를 사용하여 평문 M을 e제곱한 뒤 N으로 나눈 나머지를 암호문으로 만드는 연산이기 때문이다.

계산 과정

1. $M = 9$, $e = 7$, $N = 143$을 공식에 대입하면 C=9^7 143이다.
2. 9^2 143=81, 9^4 143=126이다.
3. $9^7 = 9^4 \cdot 9^2 \cdot 9$이므로 C=(126·81·9) 143=48이다. 따라서 전송되는 암호문을 나타내는 식은 9^7 143이다.

선지 판단

① O — 9^7 143은 평문 9를 공개 지수 7만큼 거듭제곱하고 공개키의 모듈러스 143으로 나눈 나머지를 구하므로 RSA 암호화식과 일치한다. 계산값은 48이다.

② X — 7^9 143은 평문 9와 공개 지수 7의 자리를 서로 바꾼 식이다. 올바르게는 9^7 143이다.

③ X — 143^7 9는 모듈러스 143을 밑으로, 평문 9를 나누는 수로 잘못 배치한 식이다. 올바르게는 평문 9를 밑으로 하고 143을 모듈러스로 하는 9^7 143이다.

④ X — 7^143 9는 공개 지수 7을 밑으로, 모듈러스 143을 지수로, 평문 9를 나누는 수로 잘못 배치한 식이다. 올바르게는 9^7 143이다.

NoteBase

오답 포인트

이 문제의 함정은 공개키를 *e*, *N* 순서로 제시한 것을 거듭제곱식의 밑과 지수 순서로 오해하는 데 있다. *e*는 밑이 아니라 지수이고, *N*은 지수가 아니라 나누는 수이며, 평문 *M*이 밑이다.

다시 나오면 이렇게 판단

RSA 암호화 문제에서는 먼저 평문 *M*, 공개 지수 *e*, 모듈러스 *N*을 구분한 뒤 C=M^e N의 자리에 차례로 대입하여 판단한다.

암기 포인트

RSA 암호화는 '평문을 공개 지수만큼 거듭제곱하고 공개키의 *N*으로 나눈 나머지', 즉 C=M^e N이다.

NoteBase

10. SSL/TLS 프로토콜이 보안을 제공하는 계층은?
① 물리 계층 ② 데이터링크 계층
③ 네트워크 계층 ④ 전송 계층

정답 4번

출제 포인트

SSL/TLS가 통신 계층 중 어디에서 보안 기능을 제공하는지 묻는 문제이다.

핵심 개념

SSL/TLS는 응용 프로토콜과 TCP 사이에서 동작하며, 전송되는 데이터를 암호화하고 통신 상대를 인증하며 무결성을 보호하는 전송 계층 보안 프로토콜이다.
계층 구분의 핵심은 보호 대상이다. 물리 계층은 실제 전송 매체와 신호, 데이터링크 계층은 같은 링크의 프레임, 네트워크 계층은 패킷의 주소 지정과 경로 선택, 전송 계층은 종단 간 데이터 전달을 담당한다.

선지별 해설

① X — '물리 계층'은 틀린 표현이다. 물리 계층은 케이블·전파와 같은 매체를 통해 비트를 신호로 전달하는 계층이다. 올바르게는 SSL/TLS가 전송 계층에서 보안을 제공한다고 해야 한다.
② X — '데이터링크 계층'은 틀린 표현이다. 데이터링크 계층은 동일한 링크에서 프레임을 전달하고 물리 주소를 처리하는 계층이다. 올바르게는 SSL/TLS가 전송 계층에서 보안을 제공한다고 해야 한다.
③ X — '네트워크 계층'은 틀린 표현이다. 네트워크 계층은 IP 주소를 바탕으로 패킷의 전달 경로를 정하는 계층이다. 올바르게는 SSL/TLS가 전송 계층에서 보안을 제공한다고 해야 한다.
④ O — SSL/TLS는 TCP를 기반으로 종단 간 통신 데이터의 기밀성·무결성과 상대 인증을 제공하므로 전송 계층 보안 프로토콜로 분류한다.

오답 포인트

HTTPS처럼 응용 계층 프로토콜이 TLS를 사용하므로 응용 서비스 자체와 TLS의 계층을 혼동하기 쉽다. 이 문항에서는 TCP 위에서 안전한 종단 간 통신을 제공한다는 점을 기준으로 전송 계층을 고른다.

다시 나오면 이렇게 판단

프로토콜 이름과 보호 단위를 연결한다. SSL/TLS는 TCP 기반 종단 간 데이터 보호이므로 전송 계층, IP 패킷 자체의 보호는 네트워크 계층 보안으로 구분한다.

암기 포인트

SSL/TLS는 TCP 위에서 동작하는 전송 계층 보안이다.

NoteBase

11. 다음 중 커버로스(Kerberos)에 대한 설명으로 가장 적절하지 않은 것은?
① 신뢰받는 제3자인 키 배포 기관이 개입하여 각 구성원을 인증하고 구성원들 사이에 세션키를 발급한다.
② 세션키는 공개키 알고리즘을 통해 구현된다.
③ 커버로스는 세션키를 기반으로 티켓 기반 인증 기법을 제공한다.
④ 티켓 발급 서버가 사용자에게 서비스를 받는 데 필요한 티켓을 발급한다.

정답 2번

출제 포인트

커버로스의 티켓 기반 인증 구조와 세션키에 사용되는 암호 방식이 대칭키 방식이라는 점을 묻는 문제이다.

핵심 개념

커버로스는 신뢰할 수 있는 제3자인 키 배포 센터(KDC)가 관여하여 사용자를 인증하고, 티켓과 세션키를 이용해 네트워크 서비스를 안전하게 사용하도록 하는 인증 프로토콜이다. KDC는 인증 서버(AS)와 티켓 발급 서버(TGS)의 기능으로 구성되며, 커버로스의 세션키는 공개키 알고리즘이 아니라 대칭키 알고리즘을 기반으로 한다.

선지별 해설

① O — 커버로스에서는 신뢰받는 제3자인 KDC가 인증 과정에 관여하고 통신 주체가 사용할 세션키를 제공한다.
② X — 틀린 표현은 '세션키는 공개키 알고리즘을 통해 구현된다'이다. 올바르게는 커버로스의 세션키는 대칭키 알고리즘을 통해 구현된다고 해야 한다.
③ O — 커버로스는 세션키를 사용하며, 서버 접근 권한을 증명하는 티켓을 기반으로 인증을 수행한다.
④ O — TGS는 사용자가 특정 응용 서버의 서비스를 이용할 때 필요한 서비스 티켓을 발급한다.

오답 포인트

②의 '공개키'가 함정이다. 커버로스가 네트워크 환경에서 안전한 인증을 제공한다는 사실을 공개키 암호 방식과 연결하기 쉽지만, 커버로스의 핵심은 KDC가 발급하는 티켓과 대칭키 기반 세션키이다.

다시 나오면 이렇게 판단

커버로스 선지는 KDC, AS, TGS, 티켓, 세션키의 역할을 먼저 확인한다. 암호 방식이 제시되면 '공개키'가 아니라 '대칭키'인지 판단한다.

NoteBase

암기 포인트

커버로스는 신뢰받는 KDC, 티켓 인증, 대칭키 기반 세션키이다.

NoteBase

12. 윈도우를 비롯한 시스템 내 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM에 대한 설명으로 가장 적절하지 않은 것은?
① 난수 발생, 키 생성 및 저장, 해시값 생성, 암호화 및 전자서명을 한다.
② TPM은 인증 키를 내장한 상태로 공장에서 출고된다.
③ 운영체제 부팅 과정에서 인증을 통해 신뢰성을 확보한다.
④ 명령어 처리 과정에서 운영체제에 의존한다.

정답 4번

출제 포인트

이 문제는 TPM의 보안 기능과 운영체제로부터 독립된 하드웨어 보안 모듈이라는 특성을 구별하는 문제이다.

핵심 개념

TPM(Trusted Platform Module)은 암호 키와 플랫폼 무결성 정보를 안전하게 생성·보관·처리하는 하드웨어 기반 보안 모듈이다. 난수·키 생성, 암호 연산, 해시, 전자서명, 부팅 무결성 측정과 검증 등을 지원한다. 핵심 구분은 보안 연산이 일반 운영체제의 소프트웨어 처리에 의존하는 것이 아니라 격리된 TPM 내부에서 수행된다는 점이다.

선지별 해설

① O — TPM은 난수를 발생시키고 암호 키를 생성·저장하며, 해시값 생성과 암호화·전자서명에 필요한 보안 연산을 수행할 수 있다.

② O — TPM에는 장치를 식별하고 신뢰성을 증명하는 데 쓰이는 고유한 인증 키(EK, Endorsement Key)가 제조 과정에서 생성되어 안전하게 내장될 수 있다.

③ O — TPM은 부팅 과정에서 측정된 구성 요소의 해시값을 안전하게 기록하고 검증·증명함으로써 플랫폼과 운영체제의 부팅 무결성 및 신뢰성 확보를 지원한다.

④ X — 틀린 표현은 '명령어 처리 과정에서 운영체제에 의존한다'이다. TPM은 운영체제에서 명령을 전달받을 수 있지만, 키 보호와 주요 보안 명령의 처리는 운영체제에 의존하지 않고 격리된 TPM 하드웨어 내부에서 수행된다.

NoteBase

오답 포인트

TPM을 운영체제가 호출한다는 사실과 TPM의 보안 처리가 운영체제에 의존한다는 주장을 혼동하기 쉽다. 운영체제는 TPM에 명령을 요청하는 주체일 수 있지만, 보호 대상 키와 핵심 연산은 운영체제와 분리된 TPM 내부에 머문다.

다시 나오면 이렇게 판단

TPM 관련 선지는 '하드웨어 격리', '키의 안전한 보관', '부팅 무결성 측정·검증'이면 옳은 방향이고, 핵심 보안 처리가 운영체제나 일반 소프트웨어에 의존한다고 하면 틀린 방향으로 판단한다.

암기 포인트

TPM은 운영체제에 종속된 보안 프로그램이 아니라, 키와 무결성 정보를 하드웨어 안에서 지키는 신뢰의 뿌리이다.

NoteBase

13. ARP 스푸핑 공격으로 인한 피해를 막기 위한 방안으로 가장 적절하지 않은 것은?
① MAC 주소를 정적으로 바꾼다.
② ARP 캐시의 내용이 바뀌면 관리자에게 경고 메시지를 보낸다.
③ Snort와 같은 침입 탐지 시스템을 활용한다.
④ 방화벽을 이용하여 ARP 패킷에 대해 임계값을 설정한다.

정답 4번

출제 포인트

ARP 스푸핑 방어는 IP 주소와 MAC 주소의 거짓 대응 관계가 ARP 캐시에 들어오는 것을 막거나 그 변조를 탐지하는 방식이어야 한다.

핵심 개념

ARP 스푸핑은 공격자가 위조 ARP 메시지를 보내 피해 호스트의 ARP 캐시에 잘못된 IP-MAC 대응 관계를 저장하게 하는 공격이다. 정적 ARP 매핑은 대응 관계의 임의 변경을 막고, ARP 캐시 변경 감시와 침입 탐지 시스템은 위조·변조 징후를 탐지한다. 단순한 패킷 수 임계값은 대응 관계의 진위를 확인하지 못한다.

선지별 해설

① O — MAC 주소를 정적으로 운용한다는 것은 방어 관점에서 신뢰하는 IP-MAC 대응 관계를 정적 ARP 항목으로 고정하는 방식이다. 공격자가 보낸 위조 ARP 응답으로 해당 대응 관계가 쉽게 바뀌지 않게 하므로 적절하다.
② O — ARP 캐시 내용의 변경을 감시하고 관리자에게 경고하면 비정상적인 IP-MAC 대응 관계 변조를 빠르게 발견할 수 있으므로 적절하다.
③ O — Snort와 같은 침입 탐지 시스템은 중복 IP, 비정상 ARP 응답, MAC 주소 대응 관계의 급격한 변경 등 ARP 스푸핑 징후를 탐지하는 데 활용할 수 있으므로 적절하다.
④ X — 틀린 부분은 '방화벽에서 ARP 패킷 수에 임계값을 설정하면 ARP 스푸핑 피해를 막을 수 있다'는 취지이다. ARP 스푸핑은 많은 패킷을 보내지 않아도 성공할 수 있고, 패킷 수만으로는 IP-MAC 대응 관계가 진짜인지 판별할 수 없다. 올바르게는 정적 ARP 매핑, ARP 캐시 변경 감시, 동적 ARP 검사와 같이 대응 관계의 위조 여부를 검증하거나 탐지해야 한다.

오답 포인트

④의 '임계값'은 대량 트래픽을 제한하는 방어와 ARP 정보의 진위를 검증하는 방어를 혼동하게 만든다. 공격 패킷의 개수가 적더라도 거짓 ARP 정보 한 번으로 캐시가 오염될 수 있다는 점이 핵심 함정이다.

NoteBase

다시 나오면 이렇게 판단

각 방안이 IP-MAC 대응 관계의 변조를 막거나 그 변조 사실을 탐지하는지 확인한다. 단순히 ARP 패킷의 양만 제한하고 대응 관계의 진위를 확인하지 않는 방안은 직접적인 ARP 스푸핑 대책으로 보기 어렵다.

암기 포인트

ARP 스푸핑 방어의 핵심은 패킷 수 제한이 아니라 IP-MAC 매핑의 고정·검증·변경 탐지이다.

NoteBase

14. 다음 중 802.11 무선 랜 보안이 제공하지 않는 것은?

① 전자서명 ② 인증

③ 키 교환 ④ 보호 데이터 전송

정답 1번

출제 포인트

802.11 무선 LAN 보안이 제공하는 기능과 전자서명 기능을 구별하는 문제이다.

핵심 개념

802.11 무선 LAN 보안은 무선 단말과 접근점 사이에서 상대를 인증하고, 암호화에 사용할 키를 설정·교환하며, 무선 구간의 데이터를 보호하여 전송하는 체계이다. 전자서명은 개인키로 서명을 생성하고 공개키로 서명자를 확인하는 기능으로, 여기서 묻는 802.11 무선 LAN 보안의 제공 기능에 해당하지 않는다.

선지별 해설

① O — 전자서명은 802.11 무선 LAN 보안이 제공하는 기능이 아니므로 '제공하지 않는 것'을 묻는 문제의 정답이다. 전자서명은 공개키 기반의 별도 서명 기능이다.

② X — 인증은 접속 주체가 정당한 단말이나 사용자인지를 확인하는 무선 LAN 보안 기능이다. 틀린 판단은 '인증을 제공하지 않는다'는 것이며, 올바르게는 '802.11 무선 LAN 보안은 인증을 제공한다'이다.

③ X — 키 교환은 통신 당사자가 보호 통신에 사용할 암호 키를 설정·공유하는 과정으로 무선 LAN 보안 기능에 포함된다. 틀린 판단은 '키 교환을 제공하지 않는다'는 것이며, 올바르게는 '802.11 무선 LAN 보안은 키 교환을 제공한다'이다.

④ X — 보호 데이터 전송은 무선 프레임을 암호화하고 무결성을 보호하여 도청이나 변조 위험을 줄이는 기능이다. 틀린 판단은 '보호 데이터 전송을 제공하지 않는다'는 것이며, 올바르게는 '802.11 무선 LAN 보안은 보호 데이터 전송을 제공한다'이다.

오답 포인트

문제의 부정형 표현인 '제공하지 않는 것'을 놓치거나, 전자서명을 데이터 무결성 보호와 같은 기능으로 보아 ④와 혼동하기 쉽다. 프레임의 무결성 보호와 공개키 기반 전자서명은 서로 다른 기능이다.

다시 나오면 이렇게 판단

802.11 무선 LAN 보안의 기능은 '접속 주체 확인(인증) → 보호 통신용 키 설정·교환 → 데이터 보호 전송'의 흐름으로 판단한다. 개인키로 서명하고 공개키로 검증하는 전자서명은 이 흐름과 구별한다.

NoteBase

암기 포인트

802.11 무선 LAN 보안은 인증·키 교환·보호 전송을 제공하고, 전자서명은 제공하지 않는다.

NoteBase

15. 다음 중 리버스 엔지니어링이 사용되는 분야에 해당하지 않는 것은?
① 취약점 분석 ② 악성코드 분석
③ 버그 수정 ④ 컴파일

정답 4번

출제 포인트

리버스 엔지니어링의 개념을 이해하고 실제 적용 분야와 정방향 소프트웨어 개발 작업을 구별하는 문제이다.

핵심 개념

리버스 엔지니어링은 완성된 프로그램이나 시스템의 구조와 동작을 역으로 분석하여 설계 원리, 기능, 취약점 등을 파악하는 활동이다.
리버스 엔지니어링의 대표적 적용 분야에는 취약점 분석, 악성코드 분석, 원인을 찾기 위한 버그 분석·수정 등이 있다. 반면 컴파일은 소스 코드를 목적 코드나 실행 가능한 기계어 형태로 변환하는 정방향 작업이다.

선지별 해설

① O — 취약점 분석은 프로그램의 내부 구조와 실행 동작을 분석하여 보안상 약점을 찾아내므로 리버스 엔지니어링이 사용되는 분야이다.
② O — 악성코드 분석은 실행 파일의 코드와 행위를 역으로 추적하여 기능과 공격 방식을 파악하므로 대표적인 리버스 엔지니어링 분야이다.
③ O — 버그 수정 과정에서는 원본 설계나 소스 코드가 충분하지 않을 때 프로그램의 동작과 바이너리를 역으로 분석하여 오류 원인을 찾을 수 있으므로 리버스 엔지니어링이 활용될 수 있다.
④ X — 틀린 표현은 '컴파일'이다. 컴파일은 소스 코드를 기계가 실행할 수 있는 목적 코드로 변환하는 정방향 작업이므로 리버스 엔지니어링의 적용 분야에 해당하지 않는다. 올바르게는 '리버스 엔지니어링이 사용되는 분야에 해당하지 않는 것은 컴파일이다'라고 해야 한다.

오답 포인트

프로그램의 코드 형태를 바꾼다는 공통점만 보고 컴파일도 역공학이라고 판단하기 쉽다. 그러나 컴파일은 소스 코드에서 실행 코드로 진행하는 정방향 변환이고, 리버스 엔지니어링은 완성된 결과물에서 내부 구조와 동작을 거꾸로 파악하는 분석이다.

다시 나오면 이렇게 판단

완성된 실행 파일이나 시스템에서 내부 구조·기능·원인을 역으로 파악하는 작업이면 리버스 엔지니어링으로 판단한다. 소스 코드를 실행 코드로 만드는 작업이면 컴파일로 판단한다.

NoteBase

암기 포인트

역공학은 결과물에서 구조를 거슬러 올라가는 분석이고, 컴파일은 소스 코드에서 실행 코드로 내려가는 변환이다.

NoteBase

16. 다음 중 XSS 공격이 수행되는 순서를 옳게 나열한 것은?

가. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.
나. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.
다. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.
라. 사용자 시스템에서 XSS 코드가 실행된다.
마. 공격 결과가 공격자에게 전달된다.

① 가-나-다-라-마
② 가-다-나-라-마
③ 가-나-라-다-마
④ 가-라-나-다-마

정답 1번

출제 포인트

이 문제는 게시판에 저장된 악성 스크립트가 사용자의 접근을 계기로 전달·실행되는 저장형 XSS 공격의 수행 순서를 묻는 문제이다.

올바른 순서

가 → 나 → 다 → 라 → 마

1. 가 — 공격자가 XSS 코드를 포함한 게시글을 웹 서버에 저장한다.
2. 나 — 웹 사용자가 해당 게시글에 접근한다.
3. 다 — 웹 서버가 XSS 코드가 포함된 게시글을 사용자에게 전달한다.
4. 라 — 전달된 XSS 코드가 사용자 시스템의 브라우저에서 실행된다.
5. 마 — 실행에 따른 공격 결과가 공격자에게 전달된다.

왜 이 순서인가: 사용자의 게시글 접근이 있어야 서버가 악성 코드가 포함된 응답을 보내며, 코드가 사용자 측에 전달되어야 브라우저에서 실행될 수 있기 때문이다.

NoteBase

선지별 해설

① O — 가에서 악성 게시글을 저장한 뒤, 나의 사용자 접근을 계기로 다의 서버 응답이 전달되고, 라에서 코드가 실행된 후 마의 공격 결과가 전송되므로 올바른 순서이다.
② X — '가 → 다 → 나'는 사용자가 게시글에 접근하기 전에 서버가 해당 게시글을 사용자에게 전달하는 순서로 되어 있어 잘못이다. 올바르게는 가 → 나 → 다 → 라 → 마이다.
③ X — '나 → 라 → 다'는 XSS 코드가 사용자에게 전달되기 전에 실행되는 순서로 되어 있어 잘못이다. 올바르게는 나 → 다 → 라이며, 전체 순서는 가 → 나 → 다 → 라 → 마이다.
④ X — '가 → 라 → 나 → 다'는 사용자의 접근과 서버의 코드 전달보다 사용자 시스템에서의 실행을 앞세워 잘못이다. 올바르게는 가 → 나 → 다 → 라 → 마이다.

오답 포인트

나의 '게시글 접근'과 다의 '게시글 전달'을 혼동하기 쉽다. 사용자가 먼저 게시글을 요청해야 서버가 그 내용을 응답으로 전달할 수 있으므로 나가 다보다 앞선다. 또한 사용자 측 실행인 라는 코드 전달인 다 이후에만 가능하다.

다시 나오면 이렇게 판단

저장형 XSS의 순서는 공격자의 악성 코드 저장 → 사용자의 페이지 접근 → 서버의 악성 코드 전달 → 사용자 브라우저의 코드 실행 → 공격 결과의 공격자 전송이라는 의존관계로 판단한다.

암기 포인트

저장형 XSS는 '저장 → 접근 → 전달 → 실행 → 결과 전송' 순서이다.

NoteBase

17. 두 사용자가 사전에 대칭키를 교환하지 않았다고 가정할 때, 다음 중 인증 및 키 교환 과정을 수행할 수 있는 방법으로 가장 적절하지 않은 것은?
① 공개키 암호
② 전자서명과 Diffie-Hellman의 조합
③ 공개키 암호와 Diffie-Hellman의 조합
④ 전자서명과 해시함수의 조합

정답 4번

출제 포인트

사전에 대칭키를 공유하지 않은 두 사용자가 상대를 인증하면서 새로운 공유 비밀키를 설정할 수 있는 방법인지 판단하는 문제이다.

핵심 개념

공개키 암호는 수신자의 공개키로 세션키 등을 암호화해 전달할 수 있고, 전자서명은 송신자 인증과 메시지 무결성을 제공한다. Diffie-Hellman은 사전 공유 비밀 없이 공유 비밀값을 만드는 키 합의 방식이다. 해시함수는 입력을 고정 길이 값으로 변환할 뿐, 그 자체로 두 사용자의 공유 비밀키를 생성하거나 전달하지 않는다.

선지별 해설

① O — 공개키 암호를 이용하면 상대방의 공개키로 새 세션키나 키 설정에 필요한 값을 보호하여 전달할 수 있으며, 공개키 기반의 질의·응답 절차로 인증도 구성할 수 있다.
② O — 전자서명은 상대방과 교환값을 인증하고 변조를 검출하며, Diffie-Hellman은 그 인증된 교환값을 바탕으로 공유 비밀키를 합의한다.
③ O — Diffie-Hellman으로 공유 비밀키를 합의하고 공개키 암호로 교환 메시지의 주체 확인이나 보호를 구성할 수 있으므로 인증과 키 교환 절차를 수행할 수 있다.
④ X — 전자서명은 인증과 무결성을 제공하고 해시함수는 메시지 요약값을 만들지만, 둘 다 공유 비밀키를 생성하거나 전달하는 기능은 없다. 틀린 표현은 '전자서명과 해시함수의 조합으로 인증 및 키 교환을 수행할 수 있다'는 취지이며, 올바르게는 '전자서명과 해시함수의 조합으로 인증과 무결성 검증은 가능하지만 별도의 키 교환 또는 키 전송 수단이 필요하다'이다.

오답 포인트

④에서 전자서명 과정에 해시함수가 사용된다는 사실 때문에 키 교환까지 가능하다고 착각하기 쉽다. 그러나 인증 기능과 공유 비밀키 설정 기능은 서로 다르다.

NoteBase

다시 나오면 이렇게 판단

각 조합을 '상대방의 신원을 확인하는 기능'과 '두 사용자가 같은 비밀키를 갖게 하는 기능'으로 나누어 확인한다. 전자서명·해시는 전자에 기여하지만, 키 합의나 안전한 키 전송 수단이 없으면 후자를 충족하지 못한다.

암기 포인트

서명은 인증, Diffie-Hellman은 키 합의, 해시는 요약이다. 서명과 해시만으로는 공유키가 생기지 않는다.

NoteBase

18. 다음 중 대칭키 암호 알고리즘인 AES(Advanced Encryption Standard)에 대한 설명으로 가장 적절하지 않은 것은?
① 운영모드 중 CTR 모드로는 사용이 쉽지만 CBC 모드로는 사용이 어렵다.
② 메시지를 128비트열의 블록들로 나누는 메시지 패딩이 필요하다.
③ 보안 강도에 따라 128, 192, 256비트열의 키를 사용할 수 있다.
④ 각 보안 강도에 따라 AES 내부 라운드 함수의 동작 수가 달라진다.

정답 1번

출제 포인트

AES의 고정 블록 크기, 지원 키 길이, 키 길이에 따른 라운드 수와 운영 모드 적용 가능성을 구별하는 문제이다.

핵심 개념

AES는 128비트 블록을 암호화하는 대칭키 블록 암호이며, 128·192·256비트 키를 지원한다. 키 길이에 따라 라운드 수는 각각 10·12·14회이다. CBC와 CTR은 AES에 모두 적용할 수 있는 운영 모드이다. CBC는 평문의 마지막 블록이 128비트에 못 미치면 일반적으로 패딩이 필요하지만, CTR은 블록 암호를 스트림 암호처럼 사용하므로 패딩이 필요하지 않다.

선지별 해설

① X — 틀린 표현은 'CTR 모드로는 사용이 쉽지만 CBC 모드로는 사용이 어렵다'이다. AES는 CTR 모드와 CBC 모드에 모두 사용할 수 있다. 올바르게는 'AES는 CTR과 CBC를 비롯한 여러 운영 모드에 적용할 수 있으며, CTR은 병렬 처리와 임의 접근이 쉽고 CBC는 암호화 시 앞 암호문 블록에 의존한다'이다.
② O — AES의 블록 크기는 키 길이와 관계없이 128비트이다. 따라서 평문을 128비트 블록 단위로 처리하며, CBC처럼 완전한 블록을 요구하는 모드에서는 마지막 블록이 부족할 때 패딩으로 채운다.
③ O — AES는 보안 강도에 따라 128비트, 192비트, 256비트 키를 사용할 수 있다.
④ O — 키 길이가 길어지면 내부 라운드 수도 달라져 128비트 키는 10회, 192비트 키는 12회, 256비트 키는 14회의 라운드를 수행한다.

오답 포인트

①은 CTR이 병렬 처리와 임의 접근에 유리하다는 사실을 'AES는 CBC로 사용하기 어렵다'는 주장으로 바꾼 함정이다. 운영 모드별 처리 특성이 다르다는 것과 AES에 그 모드를 적용할 수 있는지는 별개의 판단이다.

NoteBase

다시 나오면 이렇게 판단

AES 문항에서는 블록 크기는 항상 128비트인지, 키 길이는 128·192·256비트인지, 라운드 수는 10·12·14회인지 먼저 확인한다. 운영 모드는 적용 가능 여부와 병렬 처리·패딩 같은 성질을 분리해 판단한다.

암기 포인트

AES는 블록 128, 키 128·192·256, 라운드 10·12·14이며 CBC와 CTR 모두 사용 가능하다.

NoteBase

19. 다음 중 이 권한이 설정되어 있는 파일을 사용자가 실행하면 일시적으로 사용자의 권한이 아닌 파일 소유자(특히 관리자)의 권한으로 실행되기 때문에 공격에 많이 사용되는 것은?

① SetUID ② SetGID
③ Sticky bit ④ UID

정답 1번

출제 포인트

이 문제는 실행 파일에 설정되는 SetUID의 효과와 SetGID, Sticky bit, UID의 차이를 묻는 문제이다.

핵심 개념

SetUID: 실행 파일을 실행한 사용자가 실행 중에는 파일 소유자의 유효 사용자 ID와 권한으로 동작하게 하는 특수 권한이다. 파일 소유자가 root이면 권한 상승 공격에 악용될 수 있다.
SetGID: 실행 파일을 파일 소유 그룹의 유효 그룹 ID로 실행하게 하는 특수 권한이다.
Sticky bit: 주로 공유 디렉터리에서 파일 삭제·이름 변경을 해당 파일 소유자, 디렉터리 소유자 또는 root로 제한하는 특수 권한이다.
UID: 운영체제가 사용자를 식별하기 위해 부여하는 사용자 식별 번호이다.

선지별 해설

① O — SetUID가 설정된 실행 파일은 실행한 사용자의 원래 권한이 아니라 파일 소유자의 유효 사용자 ID로 동작한다. 특히 root 소유의 SetUID 프로그램에 취약점이나 잘못된 설정이 있으면 일반 사용자가 높은 권한을 얻는 공격에 악용될 수 있다.
② X — 틀린 부분은 '파일 소유자의 권한으로 실행'되는 기능을 SetGID로 본 것이다. 올바르게는 SetGID가 실행 파일을 파일 소유 그룹의 유효 그룹 ID로 실행하게 한다. 파일 소유자의 유효 사용자 ID로 실행하게 하는 것은 SetUID이다.
③ X — 틀린 부분은 Sticky bit가 실행 시 파일 소유자의 권한을 부여한다고 본 것이다. 올바르게는 Sticky bit가 주로 공유 디렉터리에서 다른 사용자의 파일을 함부로 삭제하거나 이름을 변경하지 못하게 제한한다.
④ X — 틀린 부분은 UID를 실행 권한을 바꾸는 설정으로 본 것이다. 올바르게는 UID가 사용자를 구별하는 식별 번호이며, 실행 파일을 파일 소유자의 권한으로 동작하게 하는 특수 권한은 SetUID이다.

오답 포인트

SetUID와 SetGID는 모두 실행 시 유효 ID를 바꾸므로 혼동하기 쉽다. 문제의 핵심 표현은 '파일 소유자의 권한'이다. 사용자 소유자 기준이면 SetUID이고, 소유 그룹 기준이면 SetGID이다.

NoteBase

다시 나오면 이렇게 판단

실행 시 누구의 ID를 따르는지 확인한다. 파일 소유자의 사용자 ID를 따르면 SetUID, 파일 소유 그룹의 그룹 ID를 따르면 SetGID, 공유 디렉터리의 삭제를 제한하면 Sticky bit, 단순히 사용자를 식별하는 번호이면 UID이다.

암기 포인트

SetUID는 소유자(User), SetGID는 소유 그룹(Group), Sticky bit는 공유 디렉터리의 삭제 제한, UID는 사용자 식별 번호이다.

NoteBase

20. 다음 중 '정보보호시스템 공통평가기준'에 대한 설명으로 가장 적절하지 않은 것은?

① 보안목표명세서는 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.

② 보호프로파일은 평가대상 범주를 위한 특정 소비자의 요구에 부합하는 구현에 독립적인 보안요구사항의 집합을 말한다.

③ 평가보증등급은 공통평가기준에서 미리 정의된 보증수준을 가지는 보증 컴포넌트로 이루어진 패키지를 말한다.

④ 클래스는 보호프로파일, 보안목표명세서에 포함될 수 있는 보안요구사항의 가장 작은 선택 단위로서 엘리먼트의 모음을 말한다.

정답 4번

출제 포인트

정보보호시스템 공통평가기준에서 보안목표명세서, 보호프로파일, 평가보증등급과 보안요구사항의 계층인 클래스·패밀리·컴포넌트·엘리먼트를 정확히 구별하는 문제이다.

핵심 개념

보안목표명세서(ST): 식별된 평가대상의 평가 근거가 되는 보안요구사항과 구현 명세의 집합이다.
보호프로파일(PP): 특정 소비자 요구를 충족하는 평가대상 범주에 대해 구현과 독립적으로 작성한 보안요구사항의 집합이다.
평가보증등급(EAL): 공통평가기준이 미리 정의한 보증수준을 나타내는 보증 컴포넌트의 패키지이다.
보안요구사항 계층: 클래스는 공통 초점을 가진 패밀리의 모음이고, 패밀리는 공통 목적을 가진 컴포넌트의 모음이며, 컴포넌트는 엘리먼트의 모음이자 보호프로파일이나 보안목표명세서에서 선택할 수 있는 최소 단위이다. 엘리먼트는 더 나눌 수 없는 개별 보안요구사항이다.

NoteBase

선지별 해설

① O — 보안목표명세서는 식별된 평가대상을 실제로 평가할 때 근거로 사용하는 보안요구사항과 구현 명세를 제시하므로 적절하다.
② O — 보호프로파일은 특정 소비자의 요구를 만족시키는 평가대상 범주의 보안요구사항을 특정 구현과 독립적으로 기술하므로 적절하다.
③ O — 평가보증등급은 공통평가기준에서 미리 정의된 보증수준을 가지며, 이를 구성하는 보증 컴포넌트들의 패키지이므로 적절하다.
④ X — 틀린 표현은 '클래스는 … 가장 작은 선택 단위로서 엘리먼트의 모음'이다. 올바르게는 컴포넌트가 보호프로파일과 보안목표명세서에서 선택할 수 있는 가장 작은 단위이자 엘리먼트의 모음이며, 클래스는 공통된 초점을 가진 패밀리의 모음이다.

오답 포인트

④는 컴포넌트의 정의를 클래스에 바꾸어 붙인 선지이다. '엘리먼트의 모음'과 '가장 작은 선택 단위'라는 표현은 클래스가 아니라 컴포넌트를 가리킨다.

다시 나오면 이렇게 판단

보안요구사항의 계층을 클래스 → 패밀리 → 컴포넌트 → 엘리먼트 순서로 확인한다. 선택 가능한 최소 단위를 물으면 컴포넌트이고, 더 나눌 수 없는 개별 요구사항을 물으면 엘리먼트이다.

암기 포인트

클래스는 패밀리의 모음, 패밀리는 컴포넌트의 모음, 컴포넌트는 엘리먼트의 모음이며 선택의 최소 단위이다.

NoteBase

21. 다음 중 클라이언트-서버 간 동작하는 TLS (Transport Layer Security) v1.2 프로토콜에 대한 설명 중 가장 적절하지 않은 것은?
① 서버는 암호 조합들(cipher suites)을 ClientHello 메시지로 전송한다.
② 서버인증 및 키 교환을 위해 Handshake 프로토콜을 수행한다.
③ 애플리케이션 층(Layer)의 데이터는 Record 프로토콜을 이용해서 암호화된다.
④ 서버가 전송한 인증서를 통해 클라이언트는 서버를 인증한다.

정답 1번

출제 포인트

TLS 1.2에서 Handshake 프로토콜과 Record 프로토콜의 역할, 그리고 ClientHello와 ServerHello의 송신 주체를 구분하는 문제이다.

핵심 개념

Handshake 프로토콜: 클라이언트와 서버가 보안 매개변수를 협상하고 서버 인증 및 키 교환을 수행하여 통신에 사용할 키를 정하는 절차이다.
Record 프로토콜: 상위 계층의 데이터를 조각화하고 무결성 보호와 암호화를 적용하여 전송하는 프로토콜이다.
메시지 주체 구분: 클라이언트는 ClientHello에 자신이 지원하는 암호 조합 목록을 담아 보내고, 서버는 그중 하나를 선택하여 ServerHello로 알린다.

선지별 해설

① X — 틀린 표현은 '서버는 암호 조합들을 ClientHello 메시지로 전송한다'이다. ClientHello는 클라이언트가 보내며, 클라이언트가 지원하는 암호 조합 목록을 제시한다. 올바르게는 서버가 제시된 목록에서 암호 조합 하나를 선택하여 ServerHello 메시지로 전송한다고 해야 한다.
② O — TLS Handshake 프로토콜에서는 서버 인증에 필요한 인증서 교환과 키 교환이 이루어지고, 이후 사용할 보안 매개변수와 키가 설정된다.
③ O — 애플리케이션 계층의 데이터는 TLS Record 프로토콜에서 무결성 보호와 암호화가 적용된 레코드로 만들어져 전송된다.
④ O — 클라이언트는 서버가 전송한 인증서의 유효성과 신뢰 관계 등을 검증하여 서버의 신원을 인증한다.

NoteBase

오답 포인트

①은 암호 조합이 오가는 사실 자체는 맞지만 ClientHello의 송신 주체를 서버로 바꾼 함정이다. 또한 클라이언트는 여러 지원 조합을 제시하지만 서버는 그중 선택한 하나를 ServerHello로 알린다는 차이를 구분해야 한다.

다시 나오면 이렇게 판단

메시지 이름의 주체부터 확인한다. ClientHello는 클라이언트의 지원 목록 제시, ServerHello는 서버의 선택 결과 통지, Handshake는 협상·인증·키 교환, Record는 실제 데이터의 보호와 전송으로 판단한다.

암기 포인트

ClientHello는 목록 제시, ServerHello는 하나 선택, Handshake는 인증·키 교환, Record는 데이터 보호이다.

NoteBase

22. 다음 중 이메일 보안을 위한 PGP(Pretty Good Privacy)에 대한 설명으로 가장 적절하지 않은 것은?
① PGP는 Web of Trust 개념으로 신뢰된 인증기관 없이 인증한다.
② PGP의 공개키 암호 및 전자서명 기법은 X.509 형식을 따라야 한다.
③ 별도의 PGP 프로그램을 설치하고 기존의 이메일 시스템과 함께 사용한다.
④ 이메일 본문뿐만 아니라 첨부파일까지 비밀성 및 무결성을 보장할 수 있다.

정답 2번

출제 포인트

PGP의 신뢰 모델, 키·서명 형식, 이메일 연동 방식, 보호 범위를 구분하는 문제이다.

핵심 개념

PGP는 이메일의 기밀성, 무결성, 인증, 부인 방지를 제공하는 보안 방식이다. 공개키 암호로 키를 안전하게 전달하고 전자서명으로 발신자와 메시지 무결성을 확인한다.
신뢰 모델: 중앙 인증기관의 계층적 보증에 반드시 의존하지 않고, 사용자들이 서로의 공개키에 서명하여 신뢰를 연결하는 Web of Trust를 사용한다.
형식 구분: PGP의 키와 전자서명은 OpenPGP 계열의 독자적인 패킷·인증서 형식을 사용하므로 X.509 형식을 반드시 따라야 하는 것은 아니다.

선지별 해설

① O — PGP는 사용자들이 서로의 공개키에 서명하여 신뢰를 확장하는 Web of Trust를 사용하므로 중앙의 신뢰된 인증기관이 반드시 필요하지 않다.
② X — 틀린 표현은 'X.509 형식을 따라야 한다'이다. PGP의 공개키 암호와 전자서명은 OpenPGP 계열의 키·서명 형식을 사용하며, X.509 형식을 따라야 하는 것은 아니다. 올바르게는 'PGP는 공개키 암호와 전자서명 기법을 사용하지만 그 키·서명 형식이 X.509를 반드시 따르지는 않는다'이다.
③ O — PGP는 별도의 프로그램이나 기능을 설치하여 기존 이메일 시스템과 연동해 사용할 수 있다. 이메일 시스템 전체를 새로 구축해야 하는 방식이 아니다.
④ O — PGP는 이메일 본문뿐 아니라 이메일에 포함된 첨부파일도 암호화하거나 전자서명하여 기밀성과 무결성을 보호할 수 있다.

NoteBase

오답 포인트

공개키 암호와 전자서명을 사용한다는 사실만 보고 모든 공개키 기반 방식이 X.509 인증서 형식을 따른다고 생각하기 쉽다. 그러나 암호 기술의 종류와 키·인증서의 표현 형식은 별개의 문제이며, PGP는 Web of Trust와 OpenPGP 형식을 중심으로 동작한다.

다시 나오면 이렇게 판단

PGP 관련 선지는 '신뢰 구조는 Web of Trust인가', '키·서명 형식을 X.509로 단정하는가', '본문과 첨부파일을 모두 보호할 수 있는가'를 차례로 확인한다. '반드시 X.509를 따른다'는 표현은 PGP의 형식과 맞지 않는다.

암기 포인트

PGP는 Web of Trust, OpenPGP 형식, 본문·첨부파일 보호이다. X.509 필수는 아니다.

NoteBase

23. 다음 중 사용자 인증서를 이용하여 인증서버에 로그인하는 경우에 대한 설명 중 가장 적절하지 않은 것은?

① 사용자 인증서는 인증서버도 신뢰하는 인증기관에서 발급받은 것이어야 한다.
② 인증서버는 사용자와 도전-응답 프로토콜을 수행해서 사용자를 인증한다.
③ 사용자 인증서에 대응하는 개인키는 인증서버에 보관하고 인증할 때마다 요청한다.
④ 사용자는 키보드 보안 및 개인 방화벽에 필요한 파일을 추가적으로 설치할 수 있다.

정답 3번

출제 포인트

사용자 인증서를 이용한 로그인에서 인증기관의 신뢰 관계, 도전–응답 절차, 개인키의 보관 주체를 구별하는 문제이다.

핵심 개념

인증서 기반 사용자 인증은 인증서의 공개키가 특정 사용자에게 속한다는 사실을 신뢰할 수 있는 인증기관이 보증하고, 사용자가 자신의 개인키로 도전값에 대한 응답을 생성함으로써 개인키의 소유를 증명하는 방식이다. 인증서와 공개키는 인증서버에 제시할 수 있지만, 개인키는 사용자 측에서 안전하게 보관해야 한다. 인증서버는 개인키 자체를 전달받지 않고 공개키로 응답의 유효성을 검증한다.

선지별 해설

① O — 인증서버가 사용자의 인증서를 신뢰하려면 그 인증서가 서버가 신뢰하는 인증기관에서 발급되었거나 신뢰 경로를 통해 검증될 수 있어야 한다.
② O — 인증서버는 임의의 도전값을 보내고, 사용자가 개인키로 생성한 응답을 인증서의 공개키로 검증하는 도전–응답 절차를 통해 사용자를 인증할 수 있다.
③ X — 틀린 표현은 '개인키는 인증서버에 보관하고 인증할 때마다 요청한다'이다. 개인키를 서버에 맡기면 개인키의 비밀성과 소유자 통제가 훼손된다. 올바르게는 개인키를 사용자 측의 안전한 저장소에 보관하고, 사용자가 인증 시 그 개인키로 도전값에 대한 응답을 생성한다.
④ O — 인증 과정과 별도로 입력 정보 보호나 단말 보안을 강화하기 위해 키보드 보안 또는 개인 방화벽에 필요한 파일을 추가로 설치할 수 있다. 이는 개인키를 인증서버에 보관한다는 의미가 아니다.

NoteBase

오답 포인트

③은 인증서버가 사용자의 공개키가 포함된 인증서를 확인한다는 사실을 개인키까지 보관한다는 것으로 바꾼 함정이다. 공개키는 검증에 사용되지만 개인키는 사용자만 통제해야 한다.

다시 나오면 이렇게 판단

인증서 로그인 문항에서는 '서버는 공개키로 검증하고, 사용자는 개인키로 응답을 생성한다'는 역할 분담을 먼저 확인한다. 서버가 사용자의 개인키를 보관하거나 매번 제공한다는 표현은 부적절한 것으로 판단한다.

암기 포인트

공개키는 서버가 검증하고, 개인키는 사용자가 보관한다.

NoteBase

24. 다음 중 메시지 인증 코드(MAC: Message Authentication Code)와 전자서명을 비교한 설명으로 가장 적절하지 않은 것은?
① MAC와 전자서명 모두 메시지의 무결성을 보장하려는 경우 사용할 수 있다.
② MAC은 대칭키 환경에서 사용하고, 전자서명은 공개키 환경에서 사용한다.
③ 전자서명과는 다르게 MAC은 부인방지(Non-repudiation) 기능을 제공한다.
④ 대표적인 MAC 기법으로 CBC-MAC과 HMAC이 사용된다.

정답 3번

출제 포인트

이 문제는 MAC과 전자서명이 제공하는 보안 기능과 사용되는 키 구조의 차이를 묻는 문제이다.

핵심 개념

MAC: 송신자와 수신자가 공유한 대칭키로 메시지의 무결성과 인증을 확인하는 값이다. 공유키를 함께 알고 있으므로 제3자에게 어느 당사자가 생성했는지를 증명하는 부인방지는 제공하지 못한다.
전자서명: 서명자가 자신의 개인키로 서명하고 검증자가 공개키로 확인하는 방식이다. 메시지의 무결성과 서명자 인증을 제공하며 부인방지를 지원한다.
핵심 차이는 MAC은 공유 대칭키, 전자서명은 개인키·공개키 쌍을 사용한다는 점이다.

선지별 해설

① O — MAC은 메시지가 변조되면 검증값이 달라지고, 전자서명도 서명 대상 메시지가 바뀌면 검증에 실패하므로 둘 다 메시지의 무결성을 보장하는 데 사용할 수 있다.
② O — MAC은 송신자와 수신자가 같은 비밀키를 공유하는 대칭키 환경에서 사용하고, 전자서명은 개인키로 서명하고 공개키로 검증하는 공개키 환경에서 사용한다.
③ X — 틀린 표현은 'MAC은 부인방지 기능을 제공한다'이다. 공유키를 가진 어느 당사자도 MAC을 생성할 수 있으므로 특정 당사자가 생성했다는 사실을 제3자에게 입증하기 어렵다. 올바르게는 '전자서명은 부인방지를 제공하지만 MAC은 부인방지를 제공하지 못한다'이다.
④ O — CBC-MAC은 블록 암호 기반의 대표적인 MAC이고, HMAC은 해시 함수와 비밀키를 결합한 대표적인 MAC이다.

NoteBase

오답 포인트

③은 MAC도 송신자 인증에 활용된다는 점을 부인방지와 혼동하게 만든다. 공유키 기반의 인증은 통신 당사자 사이에서 유효하지만, 누가 MAC을 생성했는지를 제3자에게 증명하는 부인방지와는 다르다.

다시 나오면 이렇게 판단

키를 공유하면 MAC, 개인키로 서명하고 공개키로 검증하면 전자서명으로 구분한다. 이어서 부인방지가 제시되면 공유키를 쓰는 MAC이 아니라 개인키의 소유자를 특정할 수 있는 전자서명의 기능으로 판단한다.

암기 포인트

MAC은 대칭키·무결성·인증, 전자서명은 공개키 방식·무결성·인증·부인방지이다.

NoteBase

25. 다음 중 대칭키 암호에 대한 공격 모델 설명으로 가장 바르게 연결된 것은?
① Ciphertext-Only Attack: 선택한 암호문에 대응하는 평문을 획득하여 공격
② Known-Plaintext Attack: 전송되는 암호문만을 획득하여 공격
③ Chosen-Plaintext Attack: 선택한 평문에 대응하는 암호문을 획득하여 공격
④ Chosen-Ciphertext Attack: 알려진 평문에 대응하는 암호문을 획득하여 공격

정답 3번

출제 포인트

대칭키 암호 공격 모델을 공격자가 확보하거나 선택할 수 있는 정보와 그에 대응하여 얻는 정보의 방향으로 구분하는 문제이다.

핵심 개념

Ciphertext-Only Attack(암호문 단독 공격): 공격자가 암호문만 확보한 상태에서 평문이나 키를 추정하는 공격이다.
Known-Plaintext Attack(기지 평문 공격): 공격자가 이미 알고 있는 평문과 그에 대응하는 암호문의 쌍을 이용하는 공격이다.
Chosen-Plaintext Attack(선택 평문 공격): 공격자가 원하는 평문을 선택하고 그 평문에 대응하는 암호문을 얻어 분석하는 공격이다.
Chosen-Ciphertext Attack(선택 암호문 공격): 공격자가 원하는 암호문을 선택하고 그 암호문에 대응하는 평문을 얻어 분석하는 공격이다.
핵심 차이는 '선택한 평문 → 대응 암호문'이면 선택 평문 공격이고, '선택한 암호문 → 대응 평문'이면 선택 암호문 공격이라는 점이다.

NoteBase

선지별 해설

① X — '선택한 암호문에 대응하는 평문을 획득'한다는 설명은 Ciphertext-Only Attack이 아니라 Chosen-Ciphertext Attack이다. 올바르게는 Ciphertext-Only Attack은 공격자가 암호문만 획득하여 평문이나 키를 추정하는 공격이다.
② X — '전송되는 암호문만을 획득'한다는 설명은 Known-Plaintext Attack이 아니라 Ciphertext-Only Attack이다. 올바르게는 Known-Plaintext Attack은 이미 알려진 평문과 그에 대응하는 암호문을 획득하여 분석하는 공격이다.
③ O — 공격자가 평문을 선택하고 그 평문에 대응하는 암호문을 획득하여 분석하므로 Chosen-Plaintext Attack의 설명과 정확히 일치한다.
④ X — '알려진 평문에 대응하는 암호문을 획득'하는 것은 Chosen-Ciphertext Attack의 핵심 방향이 아니다. 올바르게는 Chosen-Ciphertext Attack은 공격자가 선택한 암호문에 대응하는 평문을 획득하여 분석하는 공격이다.

오답 포인트

①과 ④는 평문과 암호문의 대응 방향을 뒤바꾼 함정이고, ②는 '암호문만'이라는 표현을 Known-Plaintext Attack에 붙인 함정이다. 공격 모델의 이름보다 공격자가 무엇을 선택하거나 알고 있으며 무엇을 얻는지를 확인해야 한다.

다시 나오면 이렇게 판단

선지에서 공격자의 출발 정보와 획득 정보를 화살표로 정리한다. 암호문만 보유하면 Ciphertext-Only, 알려진 평문·암호문 쌍이면 Known-Plaintext, 선택 평문 → 암호문이면 Chosen-Plaintext, 선택 암호문 → 평문이면 Chosen-Ciphertext로 판단한다.

암기 포인트

평문을 고르면 CPA: 평문 → 암호문, 암호문을 고르면 CCA: 암호문 → 평문이다.

NoteBase