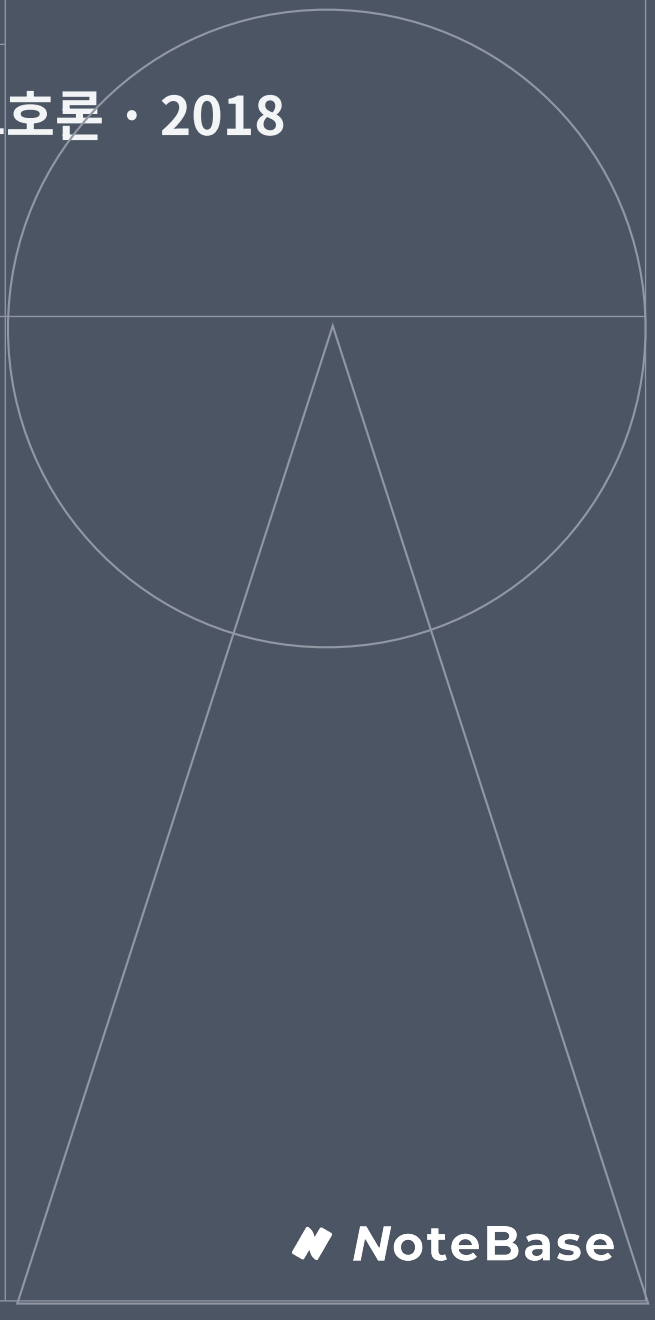
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2018



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2018

공무원/국회직/9급 · 정보보호론 · 2018

1. **정보보호의 침해 유형을 소극적 공격과 적극적 공격으로 구분했을 때 적극적 공격에 해당하는 것은?**

   ① 특정 서버에 대한 접속을 마비시킨다.
   ② 문서들을 분석하여 개인 정보를 추출한다.
   ③ 패스워드 파일로부터 패스워드를 추측한다.
   ④ 특정 사용자의 전자우편 메시지를 분석한다.
   ⑤ 특정 서버와의 트래픽을 선택적으로 감시한다.

정답 1번

출제 포인트

정보보호 침해를 시스템의 동작이나 자원에 직접 영향을 주는 적극적 공격과, 정보를 관찰·수집·분석하는 소극적 공격으로 구분할 수 있는지를 묻는 문제이다.

핵심 개념

적극적 공격: 데이터나 시스템 자원을 변조하거나 정상 동작을 방해하는 공격이다. 키워드는 변조, 위조, 재전송, 서비스 방해이다.
소극적 공격: 시스템의 정상 동작에는 직접 영향을 주지 않은 채 통신 내용이나 트래픽 등에서 정보를 수집·분석하는 공격이다. 키워드는 도청, 내용 분석, 트래픽 분석이다.
두 유형을 가르는 기준은 공격자가 단순히 정보를 알아내는 데 그치는지, 시스템이나 서비스의 상태·동작에 직접 영향을 주는지이다.

NoteBase

선지별 해설

① O — 특정 서버에 대한 접속을 마비시키는 것은 서버의 정상적인 서비스 제공을 방해하는 서비스 거부 공격이므로 적극적 공격이다.
② X — 문서를 분석하여 개인 정보를 추출하는 행위는 정보의 내용을 관찰·분석하는 소극적 공격에 해당한다. 틀린 분류를 바로잡으면 '문서의 내용을 분석하여 개인 정보를 알아내는 것은 소극적 공격이다'가 된다.
③ X — 이미 확보한 패스워드 파일을 바탕으로 패스워드를 추측하는 것은 대상 시스템의 동작을 직접 방해하거나 데이터를 변조하지 않는 오프라인 정보 분석이므로 이 문항의 구분에서는 소극적 공격이다. 틀린 분류를 바로잡으면 '패스워드 파일을 분석하여 패스워드를 추측하는 것은 소극적 공격이다'가 된다.
④ X — 특정 사용자의 전자우편 메시지를 분석하는 것은 메시지 내용을 알아내는 행위로, 소극적 공격에 해당한다. 틀린 분류를 바로잡으면 '전자우편 메시지를 분석하는 것은 소극적 공격이다'가 된다.
⑤ X — 특정 서버와 주고받는 트래픽을 선택적으로 감시하는 것은 통신량·통신 관계 등의 패턴을 관찰하는 트래픽 분석이므로 소극적 공격이다. 틀린 분류를 바로잡으면 '특정 서버와의 트래픽을 감시하는 것은 소극적 공격이다'가 된다.

오답 포인트

③의 '패스워드를 추측한다'는 표현 때문에 적극적 공격처럼 보일 수 있다. 그러나 이 선지는 서버에 직접 로그인을 반복하는 상황이 아니라 확보된 패스워드 파일을 분석하는 상황이므로, 시스템 동작에 직접 영향을 주지 않는 소극적 공격으로 구분한다. ⑤도 감시 대상을 선택했다는 사실보다 행위의 본질이 트래픽 관찰이라는 점이 중요하다.

다시 나오면 이렇게 판단

변조·위조·재전송·서비스 마비처럼 대상의 상태나 정상 동작을 바꾸면 적극적 공격으로 판단한다. 메시지 내용, 저장된 자료, 통신 패턴을 관찰하거나 분석하여 정보만 얻으면 소극적 공격으로 판단한다.

암기 포인트

적극적 공격은 바꾸거나 막고, 소극적 공격은 엿보거나 분석한다.

NoteBase

2. 대칭키 암호에 대한 설명으로 옳지 않은 것은?

① DES, AES는 대칭키 암호 알고리즘에 속한다.

② 대칭키 암호는 두 개의 키 값(비밀키, 공개키)이 서로 대칭적으로 존재해야 한다.

③ AES는 SPN(Substitution-Permutation Network) 기반 대칭키 암호이다.

④ AES는 128비트 라운드 키를 사용한다.

⑤ ARIA, SEED는 우리나라 대칭키 암호이다.

정답 2번

출제 포인트

대칭키 암호의 키 사용 방식과 대표 알고리즘인 DES, AES, ARIA, SEED의 특징을 구별하는 문제이다.

핵심 개념

대칭키 암호는 송신자와 수신자가 동일한 비밀키를 공유하여 암호화와 복호화에 사용하는 방식이다. 반면 공개키 암호는 서로 다른 공개키와 개인키의 쌍을 사용한다. AES는 128비트 블록을 처리하는 SPN 구조의 대칭키 블록 암호이며, 각 라운드에서 사용하는 라운드 키의 크기도 128비트이다.

선지별 해설

① O — DES와 AES는 암호화와 복호화에 공유 비밀키를 사용하는 대표적인 대칭키 암호 알고리즘이다.
② X — 틀린 표현은 '두 개의 키 값(비밀키, 공개키)'이다. 비밀키와 공개키의 쌍을 사용하는 것은 공개키 암호의 특징이다. 대칭키 암호는 송신자와 수신자가 동일한 비밀키를 공유하여 사용한다고 고쳐야 한다.
③ O — AES는 바이트 치환, 행 이동, 열 혼합 등 치환과 순열을 반복하는 SPN 기반의 대칭키 블록 암호이다.
④ O — AES의 블록 크기는 128비트이며, 키 확장으로 생성되어 각 라운드에 적용되는 라운드 키도 128비트이다. 원래 암호키의 길이는 128비트, 192비트 또는 256비트가 될 수 있다는 점과 구별된다.
⑤ O — ARIA와 SEED는 우리나라에서 개발된 대표적인 대칭키 블록 암호이다.

오답 포인트

②는 '대칭적으로 존재한다'는 말로 대칭키 암호처럼 보이게 하지만, 비밀키와 공개키라는 두 종류의 키는 공개키 암호의 구성이다. 또한 ④의 128비트 라운드 키를 AES의 원래 암호키 길이가 항상 128비트라는 뜻으로 오해하기 쉽다.

다시 나오면 이렇게 판단

키의 종류를 먼저 확인한다. 하나의 공유 비밀키를 사용하면 대칭키 암호이고, 공개키와 개인키의 쌍을 사용하면 공개키 암호이다. AES에서는 블록·라운드 키의 128비트와 원래 암호키의 128·192·256비트를 구분한다.

NoteBase

암기 포인트

대칭키는 공유 비밀키 하나, 공개키 암호는 공개키·개인키 한 쌍이다. AES는 SPN, ARIA·SEED는 국산 대칭키 암호이다.

NoteBase

3. 메시지 인증 코드(MAC: Message Authentication Code)가 제공하는 기능들로 짝지어진 것은?

ㄱ. 부인 방지
ㄴ. 상호 인증
ㄷ. 접근 제어
ㄹ. 무결성 보장

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ
⑤ ㄷ, ㄹ

정답 4번

출제 포인트

메시지 인증 코드(MAC)가 제공하는 상호 인증과 무결성 보장 기능을 부인 방지 및 접근 제어와 구별하는 문제이다.

핵심 개념

MAC는 송신자와 수신자가 공유한 비밀키와 메시지를 이용해 짧은 인증값을 만들고 검증하는 기술이다. 메시지가 전송 중 변경되지 않았는지 확인하여 무결성을 보장하며, 공유키를 아는 상대방인지 확인하는 인증 절차에 활용되어 양방향으로 수행하면 상호 인증이 가능하다. 반면 공유키를 양쪽이 함께 알고 있으므로 어느 쪽이 MAC을 생성했는지 제3자에게 입증할 수 없어 부인 방지는 제공하지 않는다. 접근 제어도 자원 이용 권한을 허용하거나 제한하는 별도의 보안 기능이다.

선지별 해설

① X — ㄱ의 '부인 방지'가 틀렸고, ㄹ의 '무결성 보장'이 빠졌다. 올바른 조합은 ㄴ, ㄹ이다.
② X — ㄱ의 '부인 방지'와 ㄷ의 '접근 제어'는 모두 MAC이 직접 제공하는 기능이 아니다. 올바른 조합은 ㄴ, ㄹ이다.
③ X — ㄷ의 '접근 제어'가 틀렸고, 그 자리에 ㄹ의 '무결성 보장'이 들어가야 한다. 올바른 조합은 ㄴ, ㄹ이다.
④ O — MAC은 인증 절차에 활용되어 상호 인증을 가능하게 하고, 메시지의 변경 여부를 검증하여 무결성을 보장한다. 따라서 ㄴ, ㄹ의 조합이 옳다.
⑤ X — ㄹ의 '무결성 보장'은 맞지만 ㄷ의 '접근 제어'가 틀렸고, ㄷ 대신 ㄴ의 '상호 인증'이 들어가야 한다. 올바른 조합은 ㄴ, ㄹ이다.

NoteBase

오답 포인트

‘인증’이라는 말 때문에 부인 방지까지 된다고 오해하기 쉽다. MAC은 대칭키 방식이어서 송신자와 수신자 모두 같은 MAC을 만들 수 있으므로 제3자에게 특정 송신자의 행위를 증명하는 부인 방지 기능은 없다. 또한 접근 제어는 인증된 주체에게 어떤 자원 사용을 허용할지 결정하는 별도 기능이다.

다시 나오면 이렇게 판단

MAC은 ‘공유 비밀키로 상대를 확인하고 메시지 변조를 탐지한다’는 기준으로 판단한다. 따라서 인증과 무결성은 연결하고, 전자서명에 가까운 부인 방지와 권한 관리에 해당하는 접근 제어는 제외한다.

암기 포인트

MAC은 인증·무결성, 전자서명은 부인 방지, 접근 제어는 권한 관리이다.

NoteBase

4. CC(Common Criteria) 인증 제도에 대한 설명으로 옳지 않은 것은?

① CC에서 TOE는 Target of Evaluation의 약자로서 평가 대상을 의미한다.

② CC에서 정보보호시스템은 EAL(Evaluation Assurance Level)로 보안수준을 평가받는다.

③ CC는 미국 NIST FIPS PUB 197 자료를 참고해서 만들어진 제도이다.

④ CC에서 PP는 Protection Profile을 의미하는 것으로 보안 요구 사항을 정의한다.

⑤ CC는 CCRA(Common Criteria Recognition Arrangement)라는 국제상호인정협정을 가지며, CCRA 수준으로 평가를 수행한다.

정답 3번

출제 포인트

이 문제는 CC 인증 제도의 핵심 용어인 TOE, EAL, PP, CCRA의 의미와 CC의 표준화 배경을 구별하는 문제이다.

핵심 개념

CC(Common Criteria)는 정보기술 제품·시스템의 보안 기능과 보증을 공통 기준으로 평가하기 위한 국제 표준이다.
TOE(Target of Evaluation)는 평가 대상 제품 또는 시스템과 그 범위를 뜻한다.
EAL(Evaluation Assurance Level)은 보안 기능이 올바르게 구현되었다는 보증의 수준을 단계화한 것이다.
PP(Protection Profile)는 특정 제품 유형에 필요한 보안 요구사항을 구현 방식과 독립적으로 정의한 문서이다.
CCRA(Common Criteria Recognition Arrangement)는 참여국이 CC 인증서를 상호 인정하기 위한 협정이다.
FIPS PUB 197은 AES 암호 알고리즘을 규정한 미국 연방 표준이며 CC의 제정 근거가 아니다.

NoteBase

선지별 해설

① O — TOE는 Target of Evaluation의 약자로, CC 평가의 대상이 되는 정보기술 제품·시스템과 그 평가 범위를 의미한다.
② O — EAL은 평가 대상의 보증 수준을 나타낸다. 단계가 높아질수록 더 엄격하고 폭넓은 보증 요구사항이 적용된다.
③ X — 틀린 부분은 '미국 NIST FIPS PUB 197 자료를 참고해서 만들어진 제도'라는 표현이다. FIPS PUB 197은 AES를 규정한 표준이다. 올바르게는 CC가 여러 국가의 기존 보안평가 기준을 통합·조화하여 마련된 국제 공통평가기준이라고 해야 한다.
④ O — PP는 특정 유형의 TOE에 요구되는 보안 문제와 보안 요구사항을 구현 방식과 독립적으로 정의한다.
⑤ O — CCRA는 참여국 사이에서 CC 인증 결과를 상호 인정하기 위한 국제 협정이다. 각 참여국의 인증 체계는 CC에 따라 평가를 수행하고, CCRA는 그 인증 결과의 상호 인정 범위를 정한다.

오답 포인트

③은 'NIST'와 'FIPS'라는 보안 분야의 권위 있는 명칭을 제시하여 CC의 근거 문서처럼 보이게 만든다. 그러나 FIPS PUB 197의 대상은 CC 인증 제도가 아니라 AES 암호 알고리즘이다. 또한 ④의 PP는 개별 제품의 구체적 보안 명세인 ST(Security Target)와 구별된다.

다시 나오면 이렇게 판단

약어를 역할별로 대응한다. 평가 대상은 TOE, 보증 수준은 EAL, 제품 유형의 공통 보안 요구사항은 PP, 인증서의 국제 상호 인정은 CCRA이다. FIPS PUB 197이 나오면 CC가 아니라 AES 표준으로 판단한다.

암기 포인트

TOE는 대상, EAL은 보증 단계, PP는 공통 요구사항, CCRA는 상호 인정, FIPS PUB 197은 AES이다.

NoteBase

5. OTP(One Time Password)에 대한 설명으로 옳지 않은 것은?

① OTP는 비밀번호 예측 공격을 막기 위한 방법으로 사용 가능하다.

② 패킷 스니핑을 통한 비밀번호 재사용 공격의 대응책으로 활용 가능하다.

③ 동기화 방식 OTP에서는 시간과 인증 횟수를 기반으로 비밀번호를 동기화 한다.

④ 비동기화 방식 OTP는 인증서버에서 전송된 난수를 기반으로 비밀번호를 생성한다.

⑤ 시간 동기화 방식 OTP는 인증서버와 OTP 생성기의 시간오차범위를 허용하지 않는다.

정답 5번

출제 포인트

OTP의 일회성에 따른 보안 효과와 동기화 방식·비동기화 방식의 생성 원리를 구분하는 문제이다.

핵심 개념

OTP: 한 번의 인증에만 유효한 비밀번호를 생성하여 탈취한 인증값의 재사용을 어렵게 하는 인증 방식이다.
동기화 방식 OTP: 인증서버와 OTP 생성기가 시간 또는 인증 횟수인 카운터를 공유·동기화하여 같은 OTP를 계산한다. 시간 동기화 방식은 양쪽 시계의 차이를 고려한 허용 범위를 둔다.
비동기화 방식 OTP: 서버가 보낸 난수인 도전값에 대해 OTP 생성기가 응답값을 계산하는 질의응답 방식이다.

선지별 해설

① O — OTP는 인증할 때마다 값이 바뀌므로 고정 비밀번호를 반복하여 예측하거나 알아낸 뒤 계속 사용하는 공격을 어렵게 한다.
② O — 패킷 스니핑으로 OTP를 알아내더라도 그 값은 한 번 사용되거나 유효시간이 지나면 무효가 되므로 같은 인증값을 재사용하는 재전송 공격에 대응할 수 있다.
③ O — 동기화 방식은 시간 또는 인증 횟수인 카운터를 기준으로 인증서버와 OTP 생성기가 동일한 값을 계산하도록 동기화한다.
④ O — 비동기화 방식은 인증서버가 전송한 난수인 도전값을 바탕으로 OTP 생성기가 응답 비밀번호를 생성한다.
⑤ X — 틀린 표현은 '시간오차범위를 허용하지 않는다'이다. 시간 동기화 방식은 서버와 OTP 생성기의 시계가 조금 어긋날 수 있으므로 일정한 시간오차범위를 허용하여 검증한다.

NoteBase

오답 포인트

시간 동기화라는 말 때문에 서버와 생성기의 시간이 항상 완전히 같아야 한다고 생각하기 쉽다. 실제 시스템은 시계 오차를 전제로 인접한 시간 구간까지 확인하는 허용 범위를 둔다.

다시 나오면 이렇게 판단

시간·카운터를 양쪽이 공유하면 동기화 방식이고, 서버가 난수를 보내고 생성기가 응답하면 비동기화 방식이다. 시간 기반 OTP에서 '시간오차를 전혀 허용하지 않는다'는 표현은 틀린 것으로 판단한다.

암기 포인트

동기화는 시간·횟수, 비동기화는 난수 질의응답, 시간 OTP는 오차범위를 허용한다.

NoteBase

6. ARP Spoofing이 악용하는 매핑(mapping) 정보로 짝지어진 것은?

① IP 주소 - 도메인 주소
② IP 주소 - MAC 주소
③ MAC 주소 - TCP port 번호
④ MAC 주소 - 도메인 주소
⑤ IP 주소 - TCP port 번호

정답 2번

출제 포인트

ARP 스푸핑이 조작하는 주소 대응 관계가 무엇인지 묻는 문제이다.

핵심 개념

ARP는 같은 네트워크에서 목적지의 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. ARP 스푸핑은 위조된 ARP 응답 등을 보내 IP 주소와 MAC 주소의 대응 정보를 거짓으로 바꾸는 공격이다.
DNS는 도메인 주소와 IP 주소를 대응시키며, TCP 포트 번호는 호스트 내부의 통신 프로세스나 서비스를 식별한다.

선지별 해설

① X — ‘IP 주소 - 도메인 주소’가 틀린 표현이다. 올바르게는 DNS가 도메인 주소와 IP 주소를 대응시키며, ARP가 다루는 대응 관계는 IP 주소와 MAC 주소이다.
② O — ARP는 IP 주소에 대응하는 MAC 주소를 알아내므로, ARP 스푸핑은 이 매핑 정보를 위조한다.
③ X — ‘MAC 주소 - TCP port 번호’가 틀린 표현이다. 올바르게는 ARP가 IP 주소와 MAC 주소를 대응시키며, TCP 포트 번호는 통신 프로세스나 서비스를 식별한다.
④ X — ‘MAC 주소 - 도메인 주소’가 틀린 표현이다. 올바르게는 DNS가 도메인 주소와 IP 주소를 대응시키고, ARP는 IP 주소와 MAC 주소를 대응시킨다.
⑤ X — ‘IP 주소 - TCP port 번호’가 틀린 표현이다. 올바르게는 ARP가 IP 주소와 MAC 주소를 대응시키며, TCP 포트 번호는 ARP 매핑의 대상이 아니다.

오답 포인트

주소나 식별자가 두 개씩 제시되어 모두 네트워크 매핑처럼 보이는 점이 함정이다. 도메인 주소는 DNS, MAC 주소는 ARP, TCP 포트 번호는 프로세스·서비스 식별과 연결해 구분해야 한다.

다시 나오면 이렇게 판단

ARP가 보이면 먼저 ‘IP 주소를 어떤 MAC 주소로 보낼 것인가’를 떠올린다. 따라서 ARP 스푸핑의 조작 대상은 IP 주소와 MAC 주소의 대응 정보로 판단한다.

NoteBase

암기 포인트

DNS는 도메인-IP, ARP는 IP-MAC, TCP 포트는 프로세스·서비스 식별이다.

NoteBase

7. BLP(Bell-La Padula) 모델이 가지고 있는 특성과 규칙에 대한 설명으로 옳지 않은 것은?

① 비밀정보가 허가되지 않은 방식으로 접근되는 것을 방지하고자 하는 것을 목표로 함

② 강제적 접근통제를 하고자 하는 경우 본 모델을 기반으로 통제 규칙을 정의함

③ 단순 보안 규칙은 주체가 객체를 읽기 위해서는 주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함

④ 스타 보안 규칙은 주체가 객체에 쓰기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함

⑤ 강한 스타 보안 규칙은 주체의 읽기/쓰기는 하위 혹은 상위가 아닌 동일한 보안 분류 수준의 객체에 대해서만 가능함

정답 4번

출제 포인트

BLP(Bell-LaPadula) 모델의 기밀성 목표와 단순 보안 규칙, 스타 보안 규칙, 강한 스타 보안 규칙의 접근 조건을 구별하는 문제이다.

핵심 개념

BLP 모델은 정보가 높은 보안 수준에서 낮은 보안 수준으로 유출되는 것을 막는 기밀성 중심의 강제적 접근통제 모델이다.
단순 보안 규칙은 상향 읽기를 금지한다(No Read Up). 주체는 자신의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같을 때 객체를 읽을 수 있다.
스타 보안 규칙은 하향 쓰기를 금지한다(No Write Down). 주체는 자신의 비밀취급 허가 수준과 같거나 더 높은 보안 분류 수준의 객체에만 쓸 수 있다.
강한 스타 보안 규칙은 읽기와 쓰기를 동일한 보안 수준의 객체에 대해서만 허용한다.

NoteBase

선지별 해설

① O — BLP 모델은 허가되지 않은 정보 접근과 낮은 보안 수준으로의 정보 유출을 방지하여 기밀성을 보호하는 것을 목표로 한다.
② O — BLP 모델은 보안 등급과 비밀취급 허가 수준에 따라 접근을 통제하므로 강제적 접근통제 규칙을 정의하는 기반이 된다.
③ O — 단순 보안 규칙은 상향 읽기를 금지하므로, 주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 읽을 수 있다.
④ X — 틀린 표현은 '주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 한다'이다. 이 조건은 낮은 등급의 객체에 쓰는 하향 쓰기를 허용하게 된다. 올바르게는 스타 보안 규칙에 따라 객체의 보안 분류 수준이 주체의 비밀취급 허가 수준보다 높거나 같아야 쓸 수 있다.
⑤ O — 강한 스타 보안 규칙은 정보 흐름을 더 엄격히 제한하여 주체의 읽기와 쓰기를 동일한 보안 분류 수준의 객체에 대해서만 허용한다.

오답 포인트

③의 읽기 조건을 ④의 쓰기 조건에도 그대로 적용하기 쉽다. 읽기는 주체 수준이 객체 수준 이상이어야 하지만, 쓰기는 객체 수준이 주체 수준 이상이어야 한다. ④는 이 방향을 반대로 제시하여 하향 쓰기를 허용한 선지이다.

다시 나오면 이렇게 판단

읽기는 '위로 읽지 못한다'고 판단하여 주체 수준이 객체 수준 이상인지 확인한다. 쓰기는 '아래로 쓰지 못한다'고 판단하여 객체 수준이 주체 수준 이상인지 확인한다. 강한 스타 보안 규칙이면 읽기와 쓰기 모두 동일 수준인지 확인한다.

암기 포인트

BLP는 기밀성, 단순 보안은 No Read Up, 스타 보안은 No Write Down, 강한 스타 보안은 동일 수준에서만 읽기·쓰기이다.

NoteBase

8. 웹 공격의 유형에 대한 설명으로 옳지 않은 것은?

① XSS(Cross-Site Scripting) : 저장 XSS 공격, 반사 XSS 공격, DOM 기반 XSS 공격으로 분류되며, 이에 대응하기 위해서는 웹 어플리케이션의 개발단계에서 XSS에 대비한 입출력값을 검증하고 적절하게 인코딩하는 방법을 선택하는 것이 중요하다.

② SQL injection : 웹에서 사용자가 입력하는 값이 DB 질의어와 연동이 되는 경우에는 클라이언트 측에서만 자바스크립트 등을 통해 사용자의 입력값을 검증하는 것으로 해결된다.

③ CSRF(Cross-Site Request Forgery) : 사용자가 자신의 의도와는 무관하게 공격자가 의도한 웹사이트 사용 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 만드는 공격이다.

④ 쿠키획득 공격 : 로그인된 사용자의 쿠키값을 XSS 등의 공격으로 획득하여 로그인을 할 수 있다.

⑤ 인증우회 공격 : 인증되지 않은 사용자가 접근할 수 없는 페이지를 접근할 수 있는 URL을 획득하여 인증 없이 접근하는 공격방법이다.

정답 2번

출제 포인트

웹 공격의 유형별 공격 원리와 핵심 대응 방법을 구분하는 문제이다. 특히 입력값 검증을 클라이언트 측에만 맡겨서는 안 된다는 점이 핵심이다.

핵심 개념

XSS는 공격자가 삽입한 스크립트가 사용자의 브라우저에서 실행되게 하는 공격이다. 저장 XSS, 반사 XSS, DOM 기반 XSS 등으로 구분하며, 입력값 검증과 출력 위치에 맞는 인코딩이 중요하다.
SQL 삽입은 사용자 입력이 SQL 명령의 일부로 해석되게 하여 데이터베이스 질의를 변조하는 공격이다. 서버 측 검증과 매개변수화 질의(준비된 문장)로 입력값을 SQL 코드와 분리해야 한다.
CSRF는 인증된 사용자의 브라우저가 사용자의 의도와 무관한 요청을 전송하게 만드는 공격이다.
쿠키 획득 공격은 세션 쿠키를 탈취하여 사용자의 인증 세션을 가로채는 공격이고, 인증 우회 공격은 정상 인증 절차 없이 보호된 자원에 접근하는 공격이다.

NoteBase

선지별 해설

① O — XSS는 저장 XSS, 반사 XSS, DOM 기반 XSS 등으로 분류된다. 입력값을 검증하고 출력 위치에 맞게 인코딩하는 것은 대표적인 대응 방법이다.
② X — 틀린 표현은 '클라이언트 측에서만 자바스크립트 등을 통해 사용자의 입력값을 검증하는 것으로 해결된다'이다. 클라이언트 측 검증은 공격자가 우회할 수 있으므로 SQL 삽입을 막을 수 없다. 올바르게는 서버 측에서 입력값을 검증하고 매개변수화 질의 또는 준비된 문장을 사용하여 입력 데이터와 SQL 명령을 분리해야 한다.
③ O — CSRF는 인증된 사용자의 권한을 악용하여 수정·삭제·등록 등 공격자가 의도한 요청을 사용자의 브라우저가 보내게 하는 공격이다.
④ O — XSS 등으로 로그인 사용자의 세션 쿠키를 탈취하면 공격자는 그 세션을 도용하여 해당 사용자로 가장해 서비스에 접근할 수 있다.
⑤ O — 인증되지 않은 사용자가 보호된 페이지의 URL을 알아내어 정상 인증 절차 없이 접근하는 것은 인증 우회 공격에 해당한다.

오답 포인트

②의 함정은 입력값 검증 자체가 아니라 '클라이언트 측에서만'이라는 제한 표현이다. 브라우저에서 수행되는 검증은 요청을 직접 조작하면 우회할 수 있으므로 보안 통제로 충분하지 않다.

다시 나오면 이렇게 판단

공격이 실행되는 위치와 악용 대상을 먼저 구분한다. 브라우저에서 악성 스크립트가 실행되면 XSS, SQL 질의가 변조되면 SQL 삽입, 인증된 사용자가 원치 않는 요청을 보내게 되면 CSRF이다. 입력값 보안 대책에 '클라이언트 측에서만'이라는 표현이 있으면 우회 가능성을 확인한다.

암기 포인트

XSS는 브라우저의 스크립트 실행, SQL 삽입은 DB 질의 변조, CSRF는 인증된 사용자의 요청 위조이다. SQL 삽입 방어는 서버 측 검증과 매개변수화 질의가 핵심이다.

NoteBase

9. Diffie-Hellman 알고리즘은 $(G^a \bmod P)^b \bmod P$와 $(G^b \bmod P)^a \bmod P$를 계산한 값이 같다는 대수적인 성질을 활용한다. 다음 설명 중 옳지 않은 것은?

① a와 b는 비밀값이다.
② P는 소수이다.
③ 두 개의 키를 합성하면 새로운 키가 생성된다.
④ 중간자 공격을 방지한다.
⑤ 암호화와 복호화에 필요한 키를 분배하거나 교환하기 위한 것이다.

정답 4번

출제 포인트

Diffie-Hellman 키 교환의 구성 요소와 용도, 그리고 인증이 없을 때의 중간자 공격 취약성을 구분하는 문제이다.

핵심 개념

Diffie-Hellman은 공개된 소수 P와 생성원 G를 이용하여, 통신 당사자가 자신의 비밀 지수 a, b를 공개하지 않고 같은 공유 비밀값을 계산하는 키 합의 방식이다. 한쪽은 상대방의 공개값과 자신의 비밀값을 결합하여 (G^b P)^a P를 계산하고, 다른 쪽은 (G^a P)^b P를 계산하므로 두 결과가 같다. 다만 상대방의 신원을 인증하는 기능은 자체적으로 제공하지 않는다.

선지별 해설

① O — a와 b는 각 통신 당사자가 임의로 선택하여 외부에 공개하지 않는 비밀 지수이므로 비밀값이다.
② O — 기본적인 Diffie-Hellman에서는 모듈러 연산의 법으로 소수 P를 사용한다.
③ O — 각자의 비밀값과 상대방의 공개값을 결합하여 양쪽이 동일한 새로운 공유 비밀키를 생성한다. 여기서 '두 개의 키를 합성한다'는 것은 자신의 비밀키와 상대방의 공개키를 연산에 함께 사용한다는 뜻이다.
④ X — '중간자 공격을 방지한다'는 부분이 틀렸다. 인증 절차가 없는 Diffie-Hellman은 공격자가 양쪽 사이에서 각각 별도의 키를 합의할 수 있으므로 중간자 공격에 취약하다. 올바르게는 '인증서, 전자서명 등으로 교환되는 공개값과 상대방의 신원을 인증해야 중간자 공격을 방지할 수 있다'이다.
⑤ O — Diffie-Hellman은 암호화·복호화에 사용할 대칭키 자체를 안전하게 합의하거나 그 키를 도출하기 위한 공유 비밀을 만드는 데 사용한다.

NoteBase

오답 포인트

공격자가 비밀 지수 a와 b를 직접 알아내기 어렵다는 성질을 '상대방의 신원까지 확인된다'고 확대 해석하기 쉽다. 그러나 기밀한 공유값의 생성과 통신 상대의 인증은 서로 다른 기능이며, ④의 '중간자 공격을 방지한다'는 표현은 인증 절차가 생략되어 틀린다.

다시 나오면 이렇게 판단

Diffie–Hellman 관련 선지에서는 먼저 '키 합의'와 '인증'을 분리한다. 동일한 공유 비밀값을 만드는 것은 맞지만, 인증서나 전자서명 등 별도의 인증 수단이 제시되지 않았다면 중간자 공격 방지 기능이 있다고 판단할 수 없다.

암기 포인트

DH는 공유키 합의, 인증 없는 DH는 중간자 공격에 취약하다.

NoteBase

10. 「개인정보 보호법」의 개인정보 영향평가에 대한 설명으로 옳지 않은 것은?

① 공공기관의 장은 개인정보 영향평가를 하고 그 결과를 한국인터넷진흥원장에게 제출하여야 한다.

② 개인정보 영향평가는 대통령령으로 정하는 기준에 해당하는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우, 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.

③ 개인정보 영향평가를 하는 경우에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도 등에 대하여 고려하여야 한다.

④ 평가기관의 지정기준 및 지정취소, 평가기준, 평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑤ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 개인정보 영향평가를 하기 위하여 적극 노력하여야 한다.

정답 1번

쟁점

이 문제는 「개인정보 보호법」상 개인정보 영향평가의 실시 주체, 목적, 고려사항, 결과 제출기관을 구별하는 문제이다. 핵심은 영향평가 결과를 한국인터넷진흥원이 아니라 행정안전부장관에게 제출한다는 점이다.

용어 풀이

개인정보 영향평가란 일정한 개인정보파일의 운용으로 개인정보 침해가 우려될 때 위험요인을 분석하고 개선사항을 도출하는 평가이다.

핵심 구분

공공기관의 장은 대통령령상 기준에 해당하는 개인정보파일의 운용으로 개인정보 침해가 우려되면 영향평가를 하고, 그 결과를 행정안전부장관에게 제출하여야 한다. 영향평가에서는 처리하는 개인정보의 수, 제3자 제공 여부, 정보주체의 권리를 해칠 가능성과 위험 정도 등을 고려한다. 공공기관 외의 개인정보처리자에게는 같은 상황에서 영향평가를 위해 적극 노력할 의무가 규정되어 있다.

NoteBase

선지별 해설

① X
공공기관의 장이 영향평가 결과를 제출하는 기관은 한국인터넷진흥원이 아니라 행정안전부장관이다.
틀린 표현: '한국인터넷진흥원장에게 제출'
올바른 표현: '행정안전부장관에게 제출'

② O
개인정보 영향평가는 개인정보파일의 운용으로 개인정보 침해가 우려될 때 위험요인을 분석하고 개선 사항을 도출하기 위한 평가이다.

③ O
영향평가 시에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해칠 가능성과 그 위험 정도 등을 고려한다.

④ O
평가기관의 지정요건과 지정취소의 세부 사유, 영향평가의 기준·방법·절차 등은 법률의 위임에 따라 대통령령에서 구체화한다.

⑤ O
공공기관 외의 개인정보처리자도 개인정보파일 운용으로 정보주체의 개인정보 침해가 우려되는 경우 영향평가를 하기 위하여 적극 노력하여야 한다.

오답 포인트

①의 '한국인터넷진흥원장'은 개인정보보호 관련 전문기관이라는 점을 이용한 함정이다. 영향평가 결과의 법정 제출 상대방은 행정안전부장관이다.

다시 나오면 이렇게 판단

개인정보 영향평가 문제에서는 먼저 실시 주체가 공공기관의 장인지, 결과 제출기관이 행정안전부장관인지 확인한다. 이어 목적은 위험요인 분석과 개선 사항 도출인지, 고려사항은 개인정보의 수·제3자 제공·권리 침해 가능성과 위험 정도인지 구분한다.

암기 포인트

공공기관은 영향평가를 실시하고, 결과는 행정안전부장관에게 제출한다.

NoteBase

11. 전자문서에 대한 인증 및 부인 방지에 활용하는 암호화 방식은?

① SEED
② HIGHT
③ AES
④ RC6
⑤ RSA

정답 5번

출제 포인트

전자문서의 인증과 부인 방지에 사용하는 공개키 암호 기반 전자서명 방식과, 기밀성에 주로 사용하는 대칭키 블록 암호를 구별하는 문제이다.

핵심 개념

전자서명은 서명자의 개인키로 서명값을 만들고 대응하는 공개키로 이를 검증하여 전자문서의 작성자 인증, 무결성 확인, 부인 방지를 제공하는 기술이다.
RSA는 서로 다른 공개키와 개인키를 사용하는 공개키 암호 방식으로 전자서명에 활용할 수 있다. 반면 SEED, HIGHT, AES, RC6은 송신자와 수신자가 같은 비밀키를 사용하는 대칭키 블록 암호이므로 그 자체만으로 전자서명의 부인 방지 기능을 제공하지 않는다.

선지별 해설

① X — SEED는 대칭키 블록 암호이므로 공개키로 서명을 검증하는 전자서명 방식이 아니다. 틀린 선택은 'SEED'이며, 올바르게는 RSA와 같은 공개키 암호 기반 전자서명 방식을 사용한다.
② X — HIGHT는 자원이 제한된 환경을 고려한 경량 대칭키 블록 암호이므로 전자문서의 부인 방지를 위한 전자서명 방식이 아니다. 틀린 선택은 'HIGHT'이며, 올바르게는 RSA와 같은 공개키 암호 기반 전자서명 방식을 사용한다.
③ X — AES는 동일한 비밀키로 암호화와 복호화를 수행하는 대칭키 블록 암호이므로 그 자체로 서명자의 신원을 공개키로 검증할 수 없다. 틀린 선택은 'AES'이며, 올바르게는 RSA와 같은 공개키 암호 기반 전자서명 방식을 사용한다.
④ X — RC6는 대칭키 블록 암호이므로 개인키로 생성한 서명을 공개키로 검증하는 전자서명 방식이 아니다. 틀린 선택은 'RC6'이며, 올바르게는 RSA와 같은 공개키 암호 기반 전자서명 방식을 사용한다.
⑤ O — RSA는 공개키와 개인키의 쌍을 사용하는 공개키 암호 방식이며 전자서명에 활용된다. 개인키로 생성한 서명값을 공개키로 검증함으로써 전자문서의 인증과 부인 방지를 지원한다.

NoteBase

오답 포인트

SEED, HIGHT, AES, RC6도 모두 암호 알고리즘이므로 '암호화 방식'이라는 표현만 보고 고르기 쉽다. 그러나 이 문항의 결정적 단서는 '인증 및 부인 방지'이며, 이는 공개키와 개인키의 역할이 분리된 전자서명의 기능이다.

다시 나오면 이렇게 판단

기밀성만 묻는다면 대칭키 암호도 후보가 되지만, 인증·무결성·부인 방지를 함께 묻는다면 먼저 전자서명과 공개키 암호 방식을 찾는다. 선택지 중 SEED·HIGHT·AES·RC6은 대칭키 블록 암호, RSA는 공개키 암호 방식으로 구분한다.

암기 포인트

SEED·HIGHT·AES·RC6은 대칭키 블록 암호이고, RSA는 공개키 암호이자 전자서명에 활용되는 방식이다.

NoteBase

12. 정보통신망의 안전성 확보를 위해 수립하는 기술적, 물리적, 관리적 보호 조치 등 종합적인 정보보호 관리 체계 인증 제도는?

① PIMS(Personal Information Management System)
② ISMS(Information Security Management System)
③ ITSEC(Information Technology Security Evaluation Criteria)
④ CMVP(Cryptographic Module Validation Program)
⑤ KCMVP(Korea Cryptographic Module Validation Program)

정답 2번

출제 포인트

정보보호 관리체계 인증인 ISMS와 개인정보 관리체계, 보안성 평가 기준, 암호모듈 검증 제도를 구별하는 문제이다.

핵심 개념

ISMS는 조직이 정보통신망의 안전성을 확보하기 위해 기술적·물리적·관리적 보호조치를 종합적으로 수립·운영하는 정보보호 관리체계에 대한 인증 제도이다.
PIMS는 개인정보 보호를 중심으로 한 관리체계이고, ITSEC는 정보기술 제품·시스템의 보안성을 평가하는 기준이며, CMVP와 KCMVP는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다.

선지별 해설

① X — PIMS는 개인정보 보호를 중심으로 한 관리체계이다. 정보통신망의 안전성을 위한 기술적·물리적·관리적 보호조치를 종합적으로 관리하는 정보보호 관리체계 인증 제도라는 표현은 ISMS로 고쳐야 한다.
② O — ISMS는 Information Security Management System의 약자로, 조직의 정보보호 관리체계를 종합적으로 수립·운영하고 그 적합성을 인증하는 제도이므로 문제의 설명과 일치한다.
③ X — ITSEC는 정보기술 제품이나 시스템의 보안성을 평가하기 위한 기준이다. 종합적인 정보보호 관리체계 인증 제도라는 표현은 ISMS로 고쳐야 한다.
④ X — CMVP는 암호모듈이 정해진 보안 기준에 맞게 구현되었는지를 검증하는 제도이다. 조직의 종합적인 정보보호 관리체계 인증 제도라는 표현은 ISMS로 고쳐야 한다.
⑤ X — KCMVP는 국내에서 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다. 조직의 종합적인 정보보호 관리체계 인증 제도라는 표현은 ISMS로 고쳐야 한다.

NoteBase

오답 포인트

① PIMS와 ② ISMS에는 모두 Management System이 들어가지만, 문제의 핵심 표현은 개인정보가 아니라 정보통신망의 안전성과 기술적·물리적·관리적 보호조치의 종합적 관리이다. 또한 ③은 평가 기준, ④와 ⑤는 암호모듈 검증 제도이므로 관리체계 인증과 구별된다.

다시 나오면 이렇게 판단

조직 전체의 기술적·물리적·관리적 정보보호 조치를 종합적으로 관리하는지를 묻으면 ISMS로 판단한다. 개인정보 중심이면 PIMS, 제품·시스템의 보안성 평가 기준이면 ITSEC, 암호모듈 검증이면 CMVP 또는 KCMVP로 구분한다.

암기 포인트

ISMS는 정보보호 관리체계, PIMS는 개인정보 관리체계, ITSEC는 보안성 평가 기준, CMVP·KCMVP는 암호모듈 검증이다.

NoteBase

13. 블록체인(Blockchain) 관련 보안 기술에 대한 설명으로 옳지 않은 것은?

① 블록체인은 해시 함수를 사용하여 데이터에 대한 무결성을 보장한다.

② 블록체인 기술은 데이터의 신뢰성 및 투명성을 제공한다.

③ 공개형 블록체인 기술은 공개키 암호를 사용하기 때문에 권한이 있는 피어(peer)만 참여할 수 있다.

④ 블록체인 기술의 한 예인 하이퍼레저 패브릭(Hyperledger Fabric)에서는 공개키 인증서를 이용하여 피어에 대한 신원(identity) 정보를 제공한다.

⑤ 블록체인 기술에서는 작업 증명이나 지분 증명 등과 같은 합의 알고리즘을 사용한다.

정답 3번

출제 포인트

블록체인의 무결성·신뢰성·투명성, 공개형 블록체인의 참여 방식, 하이퍼레저 패브릭의 신원 관리, 합의 알고리즘을 구분하는 문제이다.

핵심 개념

블록체인은 거래 데이터를 블록으로 묶고 이전 블록과 암호학적으로 연결하여 여러 참여자가 공동으로 검증·공유하는 분산원장 기술이다. 해시 함수는 데이터 변경 여부를 드러내어 무결성을 뒷받침하고, 공개키 암호는 전자서명과 신원 확인 등에 쓰인다. 공개형 블록체인은 원칙적으로 누구나 참여할 수 있는 비허가형 구조이고, 하이퍼레저 패브릭은 인증된 참여자를 전제로 하는 허가형 구조이다. 작업 증명과 지분 증명은 참여 노드들이 원장의 상태에 합의하기 위한 대표적인 합의 방식이다.

NoteBase

선지별 해설

① O — 블록의 데이터가 바뀌면 해시값이 달라지고 이후 블록과의 연결도 어긋나므로 위변조를 탐지할 수 있다. 따라서 해시 함수는 데이터 무결성 보장에 기여한다.
② O — 여러 참여자가 동일한 원장을 공유하고 합의에 따라 거래를 검증하므로 중앙기관에만 의존하지 않고 데이터의 신뢰성을 확보할 수 있으며, 거래 기록의 추적과 검증을 통해 투명성도 제공한다.
③ X — 틀린 표현은 '권한이 있는 피어만 참여할 수 있다'이다. 공개키 암호를 사용한다는 사실은 참여 자격을 제한한다는 뜻이 아니다. 공개형 블록체인은 원칙적으로 별도의 사전 허가 없이 누구나 네트워크에 참여할 수 있다. 권한이 부여된 참여자만 참가하는 구조는 허가형 블록체인에 해당한다.
④ O — 하이퍼레저 패브릭은 인증기관이 발급한 공개키 인증서와 멤버십 서비스 제공자 등을 이용하여 참여자의 신원을 확인하고 권한을 관리한다.
⑤ O — 작업 증명과 지분 증명은 분산된 참여자들이 유효한 블록과 원장 상태를 결정하기 위해 사용하는 대표적인 합의 알고리즘이다.

오답 포인트

③은 '공개키 암호'의 공개라는 말과 '공개형 블록체인'을 연결하면서도 참여는 권한자에게만 제한된다고 뒤집어 놓았다. 암호 기술의 종류와 네트워크 참여 허가 여부는 별개의 판단 기준이다.

다시 나오면 이렇게 판단

선지에서 공개형과 허가형을 먼저 구분한다. 공개형은 누구나 참여할 수 있고, 허가형은 인증·승인된 참여자만 참여한다. 그다음 해시는 무결성, 공개키 인증서는 신원 확인, 작업 증명·지분 증명은 합의라는 기능을 대응시킨다.

암기 포인트

해시=무결성, 공개키 인증서=신원, 작업 증명·지분 증명=합의, 공개형=무허가 참여이다.

NoteBase

14. 파밍(Pharming) 공격에 활용하기 위해 공격자의 웹서버 IP 주소와 매핑해주는 특정 정보로 옳은 것은?

① 정상 사이트의 도메인 주소
② 정상 사이트 서버의 MAC 주소
③ 정상 사이트가 연결되어 있는 스위치의 port 번호
④ 사용자 컴퓨터의 공인 IP주소
⑤ 정상 사이트 서버의 TCP port 번호

정답 1번

출제 포인트

파밍 공격에서 공격자의 위조 웹서버 IP 주소와 연결되는 정보가 정상 사이트의 도메인 주소라는 점을 묻는 문제이다.

핵심 개념

파밍은 DNS 정보나 호스트의 이름 해석 정보를 변조하여 사용자가 정상 도메인 주소를 입력해도 공격자가 만든 위조 사이트로 접속하게 하는 공격이다. 핵심 대응 관계는 '정상 사이트의 도메인 주소 → 공격자의 웹서버 IP 주소'이다. 피싱이 주로 속임수 메시지나 링크로 사용자의 클릭을 유도하는 데 비해, 파밍은 도메인 이름과 IP 주소의 연결을 변조한다.

선지별 해설

① O — 정상 사이트의 도메인 주소를 공격자의 웹서버 IP 주소에 대응시키면, 사용자가 올바른 도메인을 입력해도 위조 사이트로 유도된다.
② X — '정상 사이트 서버의 MAC 주소'는 틀린 표현이다. MAC 주소는 같은 네트워크 구간에서 장치를 식별하는 주소이며 DNS의 도메인-IP 변환 대상이 아니다. 올바르게는 정상 사이트의 도메인 주소를 공격자의 웹서버 IP 주소와 연결한다.
③ X — '정상 사이트가 연결되어 있는 스위치의 port 번호'는 틀린 표현이다. 스위치 포트 번호는 내부 네트워크의 물리적·논리적 연결 위치에 관한 정보로 도메인 이름 해석에 사용되지 않는다. 올바르게는 정상 사이트의 도메인 주소를 공격자의 웹서버 IP 주소와 연결한다.
④ X — '사용자 컴퓨터의 공인 IP 주소'는 틀린 표현이다. 사용자의 공인 IP 주소는 접속 출발지에 관한 정보일 뿐, 특정 도메인을 위조 웹서버로 보내는 매핑 정보가 아니다. 올바르게는 정상 사이트의 도메인 주소를 공격자의 웹서버 IP 주소와 연결한다.
⑤ X — '정상 사이트 서버의 TCP port 번호'는 틀린 표현이다. TCP 포트 번호는 서버에서 실행되는 서비스나 프로세스를 구분하며 도메인과 목적지 IP 주소의 대응을 결정하지 않는다. 올바르게는 정상 사이트의 도메인 주소를 공격자의 웹서버 IP 주소와 연결한다.

NoteBase

오답 포인트

②의 MAC 주소, ③의 스위치 포트, ⑤의 TCP 포트는 모두 통신에 쓰이는 식별 정보이므로 혼동하기 쉽다. 그러나 파밍의 핵심은 DNS 등 이름 해석 정보를 조작하여 정상 도메인이 공격자의 IP 주소를 가리키게 만드는 데 있다.

다시 나오면 이렇게 판단

문제에 '파밍'과 '웹서버 IP 주소의 매핑'이 함께 나오면 도메인 이름을 IP 주소로 바꾸는 DNS 대응 관계를 먼저 확인한다. 정상 도메인 주소가 공격자의 IP 주소를 가리키면 파밍에 해당한다.

암기 포인트

파밍은 정상 도메인과 공격자 IP의 거짓 매핑이다.

NoteBase

15. 해시 함수에 대한 설명으로 옳지 않은 것은?

① 해시 함수를 사용하면 임의 길이의 메시지에 대해 특정 길이를 갖는 출력값을 얻을 수 있다.
② 해시 함수는 일방향 함수에 해당한다.
③ 동일한 출력값을 갖는 임의의 두 입력 메시지를 찾기 어렵다는 것을 강한 충돌 저항성(strong collision resistance)이라고 한다.
④ 해시 함수는 블록체인에서 체인 형태로 사용되어 데이터의 신뢰성을 보장한다.
⑤ 해시 함수는 대칭키 암호와 달리 키 값을 적용할 수 없기 때문에 MAC(Message Authentication Code)로 사용할 수 없다.

정답 5번

출제 포인트

해시 함수의 고정 길이 출력, 일방향성, 강한 충돌 저항성, 무결성 보장 기능과 키를 결합한 MAC 구성을 구별하는 문제이다.

핵심 개념

해시 함수: 임의 길이의 메시지를 고정 길이의 해시값으로 변환하는 함수이다. 역으로 원문을 구하기 어렵다는 일방향성과 같은 해시값을 만드는 서로 다른 두 메시지를 찾기 어렵다는 충돌 저항성을 보안 성질로 삼는다.
MAC: 송신자와 수신자가 공유한 비밀키를 이용하여 메시지의 무결성과 출처 인증을 확인하는 값이다. 일반 해시 함수 자체는 키를 입력받지 않지만, HMAC처럼 비밀키와 해시 함수를 결합하면 MAC을 구성할 수 있다.

선지별 해설

① O — 해시 함수는 입력 메시지의 길이와 관계없이 알고리즘이 정한 고정 길이의 해시값을 출력한다.
② O — 해시값으로부터 원래 입력 메시지를 현실적으로 복원하기 어려우므로 일방향 함수에 해당한다.
③ O — 강한 충돌 저항성은 같은 해시값을 갖는 서로 다른 두 입력 메시지를 찾아내기 어려운 성질이다.
④ O — 블록체인은 각 블록에 이전 블록과 연결되는 해시값을 포함하므로 데이터가 변조되면 연결된 해시 관계가 달라져 무결성을 검증할 수 있다.
⑤ X — 틀린 표현은 '키 값을 적용할 수 없기 때문에 MAC으로 사용할 수 없다'이다. 일반 해시 함수 자체는 키가 없지만, 비밀키를 해시 함수와 정해진 방식으로 결합한 HMAC을 사용하면 MAC을 구성할 수 있다.

오답 포인트

'해시 함수 자체는 키를 입력받지 않는다'는 사실을 '해시 함수를 이용한 MAC 구성은 불가능하다'로 확대하면 ⑤를 맞는 설명으로 오인하게 된다. HMAC은 비밀키와 해시 함수를 결합한다는 점이 핵심이다.

NoteBase

다시 나오면 이렇게 판단

해시 함수의 기본 성질과 활용 방식을 나누어 판단한다. 고정 길이 출력·일방향성·충돌 저항성은 기본 성질이고, 무결성 검증은 대표 활용이다. 키가 필요한 인증 기능이 나오면 해시 함수 단독이 아니라 HMAC처럼 비밀키를 결합한 구조인지 확인한다.

암기 포인트

해시는 고정 길이·일방향·충돌 저항, HMAC은 해시와 비밀키의 결합이다.

NoteBase

16. 공개키 기반 구조(PKI: Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?

① 공개키 인증서는 특정 사용자의 신원과 그 사용자의 공개키를 바인딩시키는 기술이다.

② 공개키 인증서를 생성할 때는 인증기관(CA: Certificate Authority)의 공개키를 사용하여 서명할 수 있다.

③ CA간에는 인증 체인을 형성할 수 있기 때문에 특정 CA에 의해 서명된 인증서는 인증 체인상의 다른 CA에 의해서도 보장될 수 있다.

④ 공개키 인증서 서명에는 RSA나 ECDSA를 사용할 수 있다.

⑤ PKI에서 RA(Registration Authority)는 인증서 발급을 요청한 사용자의 신원을 검증하는 역할을 한다.

정답 2번

출제 포인트

공개키 기반 구조(PKI)에서 인증서, 인증기관(CA), 등록기관(RA)의 역할과 전자서명에 사용되는 키를 구별하는 문제이다.

핵심 개념

공개키 인증서는 특정 사용자의 신원과 공개키를 연결하고, 인증기관(CA)의 전자서명으로 그 연결의 신뢰성을 보증하는 전자 문서이다. CA는 자신의 개인키로 인증서에 서명하고, 인증서 이용자는 CA의 공개키로 그 서명을 검증한다. 등록기관(RA)은 인증서 발급 신청자의 신원을 확인하여 CA의 발급 업무를 지원한다.

NoteBase

선지별 해설

① O — 공개키 인증서는 인증서 주체의 신원 정보와 그 주체의 공개키를 결합하여 공개키의 소유자를 확인할 수 있게 한다.

② X — 틀린 표현은 '인증기관(CA)의 공개키를 사용하여 서명'한다는 부분이다. 전자서명은 서명자의 개인키로 생성하므로, CA는 자신의 개인키로 인증서에 서명하고 이용자는 CA의 공개키로 서명을 검증한다.

③ O — 서로 다른 CA가 상대 CA의 공개키 인증서에 서명하는 교차 인증을 통해 CA 간 인증 경로를 만들 수 있다. 따라서 한 CA가 발급한 인증서도 인증 체인상의 다른 CA를 신뢰 기준으로 하여 검증될 수 있다.

④ O — RSA와 ECDSA는 모두 전자서명 알고리즘으로 사용할 수 있으므로 공개키 인증서의 서명 알고리즘으로 사용될 수 있다.

⑤ O — RA는 인증서 발급을 신청한 사용자의 신원과 등록 정보를 확인하고, 확인 결과를 CA에 전달하는 역할을 한다.

오답 포인트

②는 CA의 키를 사용한다는 사실 자체는 맞지만 공개키와 개인키의 용도를 바꾸어 놓았다. 서명 생성에는 개인키를 사용하고 서명 검증에는 공개키를 사용한다.

다시 나오면 이렇게 판단

'누가 서명하는가'를 먼저 확인한 뒤 그 주체의 개인키는 서명 생성, 공개키는 서명 검증에 대응시킨다. 이어 CA는 인증서 발급·서명, RA는 신청자 신원 확인이라는 역할로 구분한다.

암기 포인트

CA 개인키로 서명하고 CA 공개키로 검증한다. RA는 신원 확인을 담당한다.

NoteBase

17. 다음 중 <보기>에서 설명하는 것은?

<보 기>

IETF의 작업 그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반으로 개발한 전자우편 보안 기술이며, RFC 3850, 3851 등에서 정의되어 있다. 전자우편에 대한 암호화 및 전자서명을 통하여 메시지 기밀성, 메시지 무결성, 사용자 인증, 송신 사실 부인 방지, 프라이버시 보호 등의 보안 기능을 제공한다.

① MIME(Multipurpose Internet Mail Extensions)
② SMTP(Simple Mail Transfer Protocol)
③ PGP(Pretty Good Privacy)
④ PEM(Privacy Enhanced Mail)
⑤ S/MIME(Secure/Multipurpose Internet Mail Extensions)

정답 5번

출제 포인트

전자우편 관련 기술인 MIME, SMTP, PGP, PEM, S/MIME의 역할과 표준화 배경을 구별하는 문제이다. RSADSI 기술, RFC 3850·3851, 암호화와 전자서명을 함께 제시한 설명은 S/MIME을 가리킨다.

핵심 개념

S/MIME은 MIME 형식의 전자우편에 공개키 기반의 암호화와 전자서명 기능을 결합한 보안 표준이다. 암호화는 메시지 기밀성을 제공하고, 전자서명은 메시지 무결성, 사용자 인증, 송신 사실 부인 방지를 지원한다.
MIME은 전자우편의 콘텐츠 형식을 확장하고, SMTP는 전자우편을 전송하며, PGP·PEM·S/MIME은 전자우편 보안과 관련되지만 개발 배경과 표준이 서로 다르다.

NoteBase

선지별 해설

① X — MIME은 문자 집합, 첨부 파일, 이미지 등 다양한 콘텐츠를 전자우편으로 표현할 수 있게 하는 형식 확장 규격이다. 틀린 부분은 제시문을 MIME 자체의 설명으로 본 것이다. 올바르게는 '전자우편 콘텐츠 형식을 확장하는 규격'이다.
② X — SMTP는 전자우편을 송신하고 중계하는 전송 프로토콜이며, 그 자체가 암호화와 전자서명을 제공하는 보안 기술은 아니다. 틀린 부분은 보안 기능을 SMTP의 기능으로 본 것이다. 올바르게는 '전자우편 전송 프로토콜'이다.
③ X — PGP는 전자우편과 파일을 암호화하고 서명할 수 있는 보안 기술이지만, 제시문의 RSADSI 기반 IETF 작업 그룹 기술과 RFC 3850·3851에 해당하지 않는다. 틀린 부분은 해당 표준화 배경을 PGP와 연결한 것이다. 올바르게는 제시된 특징이 S/MIME에 해당한다.
④ X — PEM은 Privacy Enhanced Mail로, 전자우편의 기밀성과 인증을 위한 초기 보안 규격이지만 제시된 RFC 3850·3851의 S/MIME 규격은 아니다. 틀린 부분은 RFC 3850·3851을 PEM과 연결한 것이다. 올바르게는 해당 RFC들이 S/MIME 관련 규격이다.
⑤ O — S/MIME은 RSADSI의 기술을 바탕으로 개발되었으며, MIME 전자우편에 암호화와 전자서명을 적용하여 기밀성, 무결성, 사용자 인증, 송신 사실 부인 방지 등의 보안 기능을 제공한다. 제시문의 설명과 일치한다.

오답 포인트

MIME과 S/MIME의 이름이 비슷하고 PGP·PEM도 전자우편 보안 기술이어서 혼동하기 쉽다. 이 문항의 결정적 단서는 'RSADSI', 'RFC 3850·3851', 'MIME 전자우편의 암호화 및 전자서명'이다.

다시 나오면 이렇게 판단

전자우편 형식 확장이면 MIME, 전송이면 SMTP, MIME 기반 암호화·전자서명과 인증서 처리가 함께 나오면 S/MIME으로 판단한다. PGP와 PEM이 함께 제시되면 개발 주체와 RFC 번호까지 확인하여 구별한다.

암기 포인트

MIME은 형식, SMTP는 전송, S/MIME은 MIME에 보안을 더한 표준이다.

NoteBase

18. 무선 네트워크 보안 기술에 대한 설명으로 옳지 않은 것은?

① WEP는 보안 취약성이 있다고 알려져 있다.
② WPA2 기술은 AES-CCMP를 사용한다.
③ 무선네트워크 환경에서 인증/인가를 위해 RADIUS 프로토콜을 사용하여 연결한다.
④ Diameter 프로토콜은 RADIUS보다 세션관리, 보안 측면에서 개선 및 확장된 프로토콜이다.
⑤ WPA-PSK 방식은 공개키 인증서 공유 방식으로 확장성이 좋다.

정답 5번

출제 포인트

이 문제는 무선 네트워크 보안 기술인 WEP, WPA2, RADIUS, Diameter, WPA-PSK의 보안 방식과 용도를 구별하는 문제이다.

핵심 개념

WEP는 초기 무선 암호화 방식으로 보안 취약성이 크다.
WPA2는 강한 무선 보안을 위해 AES 기반의 CCMP를 사용한다.
RADIUS는 원격 사용자의 인증·인가·계정 관리를 제공하며, 무선 기업 환경에서는 802.1X/EAP와 함께 사용된다.
Diameter는 RADIUS의 후속 프로토콜로서 신뢰성, 보안, 세션 관리 및 확장성을 개선하였다.
WPA-PSK는 사용자나 단말이 미리 공유한 하나의 비밀키를 사용하는 방식으로, 인증서를 공유하는 공개키 방식이 아니다.

선지별 해설

① O — WEP는 짧은 초기화 벡터와 취약한 키 처리 등으로 공격에 약해 보안 취약성이 있는 방식으로 알려져 있다.
② O — WPA2는 데이터 기밀성과 무결성 보호에 AES 기반의 CCMP를 사용한다.
③ O — RADIUS는 무선 네트워크에서 사용자의 인증·인가·계정 관리를 중앙에서 처리하기 위해 인증 서버와 연동하는 프로토콜이다.
④ O — Diameter는 RADIUS의 한계를 보완한 후속 프로토콜로, 세션 관리와 보안 및 확장성 측면이 개선되었다.
⑤ X — 틀린 표현은 '공개키 인증서 공유 방식으로 확장성이 좋다'이다. WPA-PSK는 공개키 인증서를 공유하는 방식이 아니라 모든 참여자가 사전에 설정한 비밀키를 공유하는 방식이다. 참여자가 많아질수록 키 배포·변경·회수와 사용자별 통제가 어려워 확장성이 좋다고 보기 어렵다.

NoteBase

오답 포인트

⑤의 PSK를 인증서 기반의 공개키 인증과 혼동하기 쉽다. PSK의 P는 Public이 아니라 Pre-Shared를 뜻하며, 다수 사용자를 개별 인증하는 기업형 방식과 구별된다.

다시 나오면 이렇게 판단

PSK가 보이면 '사전에 공유한 하나의 비밀키'를 먼저 떠올린다. 인증서나 사용자별 중앙 인증, RADIUS 연동이 제시되면 WPA-Enterprise 계열의 특징으로 판단한다.

암기 포인트

WEP는 취약, WPA2는 AES-CCMP, RADIUS는 중앙 인증, Diameter는 RADIUS 개선, PSK는 사전 공유 비밀키이다.

NoteBase

19. 전송 계층 보안(TLS: Transport Layer Security) 프로토콜에 대한 설명으로 옳지 않은 것은?

① TLS는 TCP 프로토콜상에서 사용되며, DTLS는 UDP 프로토콜상에서 사용된다.
② TLS 프로토콜에서는 레코드 프로토콜 단계에서 공개키 인증서를 사용한다.
③ TLS는 SSL을 기초로 개발되었다.
④ FTPS에서는 FTP 파일 전송 프로토콜에서 안전한 전송을 위해 TLS를 사용한다.
⑤ TLS 프로토콜에서 대칭키 암호인 ARIA를 사용할 수 있다.

정답 2번

출제 포인트

TLS와 DTLS의 전송 계층 기반, TLS 내부 하위 프로토콜의 역할, TLS의 활용 사례와 암호 알고리즘을 구분하는 문제이다.

핵심 개념

TLS: 신뢰성 있는 전송을 제공하는 TCP 위에서 통신의 기밀성·무결성·인증을 제공하는 보안 프로토콜이다.
DTLS: 데이터그램의 순서 변경·손실 가능성을 고려하여 UDP 위에서 TLS와 유사한 보안 기능을 제공하는 프로토콜이다.
TLS 핸드셰이크 프로토콜은 통신 상대 인증, 암호 스위트 협상, 키 설정을 담당하며 이 과정에서 공개키 인증서를 사용할 수 있다. TLS 레코드 프로토콜은 상위 프로토콜의 데이터를 레코드로 나누어 보호하고 전송한다.

선지별 해설

① O — TLS는 일반적으로 TCP 위에서 사용되고, DTLS는 UDP 데이터그램 환경에 맞게 설계되어 UDP 위에서 사용된다.
② X — 틀린 부분은 '레코드 프로토콜 단계에서 공개키 인증서를 사용한다'이다. 공개키 인증서를 이용한 서버 또는 클라이언트 인증은 TLS 핸드셰이크 프로토콜에서 이루어진다. 레코드 프로토콜은 핸드셰이크 메시지와 응용 데이터를 레코드 단위로 보호하여 운반한다.
③ O — TLS는 SSL의 후속 표준으로 개발되었으므로 SSL을 기초로 발전한 프로토콜이라는 설명은 옳다.
④ O — FTPS는 FTP 통신에 TLS를 적용하여 제어 연결과 데이터 연결을 안전하게 보호하는 방식이다.
⑤ O — ARIA를 사용하는 TLS 암호 스위트가 정의되어 있으므로 TLS에서 대칭키 암호 알고리즘으로 ARIA를 사용할 수 있다.

NoteBase

오답 포인트

②는 TLS 전체가 인증서를 활용한다는 사실을 이용해 그 담당 계층을 바꾼 선지이다. 인증서 기반 인증과 키 협상은 핸드셰이크 프로토콜의 역할이고, 레코드 프로토콜의 핵심은 데이터를 레코드 단위로 보호하여 전송하는 것이다.

다시 나오면 이렇게 판단

TLS의 기능을 묻는 선지는 '협상·인증·키 설정'이면 핸드셰이크 프로토콜, '분할·보호·전송'이면 레코드 프로토콜로 구분한다. 전송 기반은 TLS-TCP, DTLS-UDP로 연결한다.

암기 포인트

TLS는 TCP, DTLS는 UDP이며, 인증서·키 협상은 핸드셰이크, 데이터 보호·운반은 레코드이다.

NoteBase

20. 「개인정보 보호법 시행령」에서 정한 고유식별정보의 범위에 포함되지 않는 것은?

① 「주민등록법」 제7조의2 제1항에 따른 주민등록번호
② 「여권법」 제7조 제1항 제1호에 따른 여권번호
③ 「도로교통법」 제80조에 따른 운전면허의 면허번호
④ 「국가연구개발사업의 관리 등에 관한 규정」 제25조 제11항에 따른 과학기술인 등록번호
⑤ 「출입국관리법」 제31조 제4항에 따른 외국인등록번호

정답 4번

쟁점

이 문제는 「개인정보 보호법 시행령」상 고유식별정보의 범위에 관한 문제이다. 핵심은 시행령이 열거한 네 가지 식별번호와 그 밖의 등록번호를 구별하는 것이다.

용어 풀이

고유식별정보는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보 중 「개인정보 보호법 시행령」이 정한 정보를 말한다.

핵심 구분

「개인정보 보호법 시행령」 제19조는 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 고유식별정보로 열거한다. 과학기술인 등록번호는 이 네 가지에 포함되지 않는다.

NoteBase

선지별 해설

① O
주민등록번호는 시행령 제19조가 정한 고유식별정보에 포함된다.

② O
여권번호는 시행령 제19조가 정한 고유식별정보에 포함된다.

③ O
운전면허의 면허번호는 시행령 제19조가 정한 고유식별정보에 포함된다.

④ X
과학기술인 등록번호는 시행령 제19조가 열거한 고유식별정보가 아니다.
틀린 표현: 과학기술인 등록번호가 고유식별정보의 범위에 포함된다는 취지
올바른 표현: 과학기술인 등록번호는 「개인정보 보호법 시행령」 제19조의 고유식별정보 범위에 포함되지 않는다.

⑤ O
외국인등록번호는 시행령 제19조가 정한 고유식별정보에 포함된다.

오답 포인트

법령에 따라 부여되는 모든 개인 식별번호가 곧 「개인정보 보호법 시행령」상 고유식별정보라고 생각하면 ④를 놓치기 쉽다. 이 시행령의 고유식별정보는 네 가지 번호로 한정하여 판단한다.

다시 나오면 이렇게 판단

선지의 번호가 주민등록번호·여권번호·운전면허의 면허번호·외국인등록번호 중 하나인지 확인한다. 이 네 가지가 아닌 별도의 등록번호라면 시행령 제19조의 고유식별정보에 포함되지 않는 것으로 판단한다.

암기 포인트

고유식별정보 네 가지는 주민·여권·운전면허·외국인등록 번호이다.

NoteBase