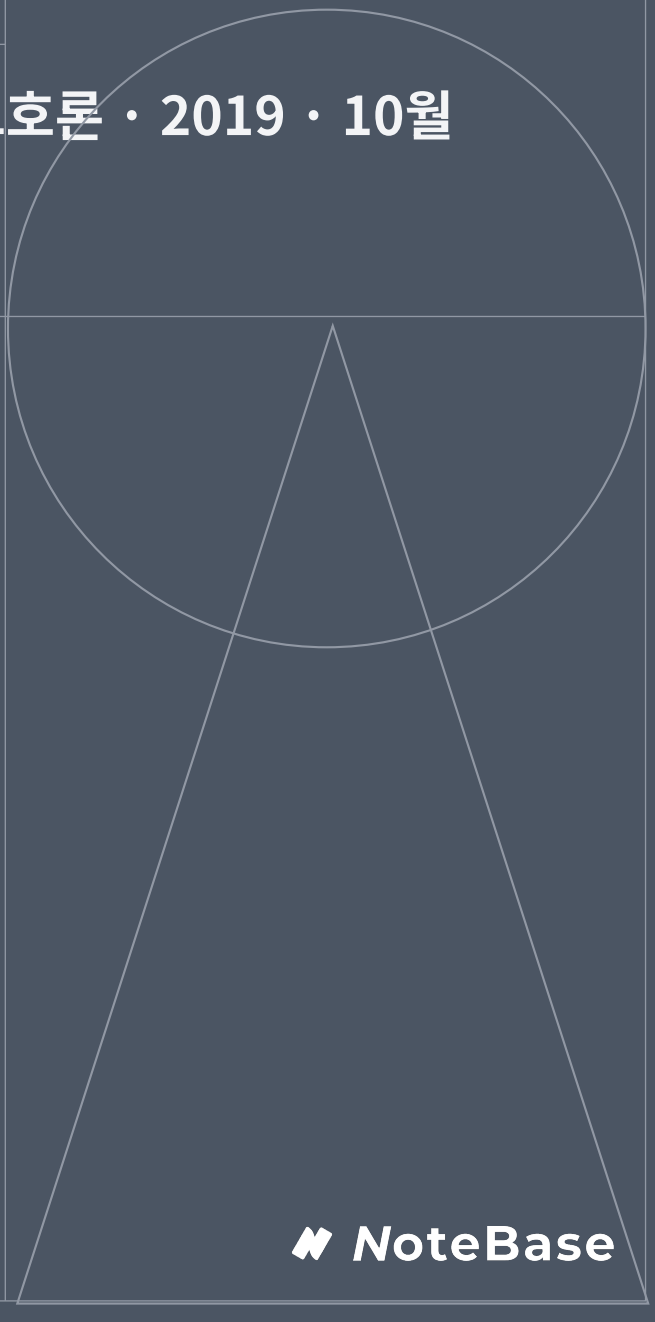
기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2019 · 10월



NoteBase

기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2019 · 10월

공무원/서울시/7급 · 정보보호론 · 2019 · 10월

문 1. 전자 서명의 기능과 가장 관계가 없는 것은?

① 인증성

② 무결성

③ 부인봉쇄

④ OTP 시간동기

정답 4번

출제 포인트

전자 서명이 보장하는 보안 기능과 OTP처럼 인증에 쓰이는 별도 기술을 구분하는 문제이다.

핵심 개념

전자 서명은 서명자의 신원을 확인하고, 메시지 변조 여부를 검증하며, 서명 사실의 부인을 어렵게 하는 기술이다.
인증성은 서명자가 누구인지 확인하는 성질이고, 무결성은 서명 후 내용이 바뀌지 않았음을 확인하는 성질이며, 부인봉쇄는 서명자가 사후에 서명 사실을 부인하기 어렵게 하는 성질이다.
OTP 시간동기는 현재 시간 값을 기준으로 일회용 비밀번호를 생성하는 방식으로, 전자 서명의 기능이 아니라 별도의 사용자 인증 기술이다.

선지별 해설

① O: 인증성은 전자 서명이 제공하는 대표적 기능이다. 전자 서명은 공개키 기반으로 서명자를 확인할 수 있으므로 인증성과 관계가 있다.
② O: 무결성은 전자 서명 후 메시지가 변경되었는지 확인하는 기능이다. 서명 검증이 실패하면 내용이 변조되었음을 알 수 있으므로 전자 서명과 직접 관계가 있다.
③ O: 부인봉쇄는 서명자가 나중에 자신이 서명하지 않았다고 주장하기 어렵게 하는 성질이다. 전자 서명의 핵심 기능 중 하나이다.
④ X: 틀린 부분은 "OTP 시간동기"이다. 실제로는 OTP 시간동기는 일회용 비밀번호를 생성하는 인증 방식이지 전자 서명의 기능이 아니다. 올바르게는 "전자 서명의 기능은 인증성, 무결성, 부인봉쇄이다"라고 정리한다.

NoteBase

오답 포인트

인증성과 OTP가 모두 '인증'과 관련되어 보여 같은 범주로 오해하기 쉽다. 그러나 인증성은 전자 서명이 보장하는 보안 성질이고, OTP 시간동기는 사용자를 확인하는 구현 방식이라는 점에서 층위가 다르다.

다시 나오면 이렇게 판단

선지가 보안이 무엇을 보장하는 성질인지 묻는지, 아니면 인증을 수행하는 수단이나 방식인지 먼저 구분한다. 인증성·무결성·부인봉쇄처럼 보장 성질이면 전자 서명 기능에 가깝고, OTP·토큰·생체정보처럼 인증 수단이면 별도 인증 기술로 본다.

암기 포인트

전자 서명은 인증성·무결성·부인봉쇄를 보장하고, OTP는 일회용 비밀번호 인증 방식이다.

NoteBase

문 2. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?

① 탐지분석 방법에는 오용 탐지 모델과 이상 탐지 모델이 있다.

② 침입탐지시스템의 구성요소로는 스크린 라우터, 베스천 호스트, 프록시 서버 등이 있다.

③ 호스트기반 IDS는 설치되어 있는 호스트 내의 침입 유형을 탐지한다.

④ 긍정오류(false positive)는 정상적인 행위를 침입으로 오인하여 탐지할 때를 말한다.

정답 2번

출제 포인트

이 문제는 침입탐지시스템의 탐지 방식, 구성요소, 적용 위치, 오탐 개념을 구별할 수 있는지를 묻는 문제이다.

핵심 개념

오용 탐지는 이미 알려진 공격 패턴이나 시그니처와 일치하는지를 보는 방식이다. 이상 탐지는 정상 행위 기준선에서 벗어나는 비정상 행위를 찾는 방식이다. IDS의 핵심 구성은 센서, 분석기, 관리 서버, 데이터베이스, 콘솔처럼 탐지와 분석을 수행하는 요소이며, 스크린 라우터·베스천 호스트·프록시 서버는 전형적인 방화벽 구조나 중계 보안 요소에 가깝다.

선지별 해설

1번: O. IDS의 탐지 방식은 크게 오용 탐지와 이상 탐지로 나뉜다. 오용 탐지는 알려진 공격 패턴을, 이상 탐지는 정상 기준에서 벗어난 행위를 찾는 방식이므로 설명이 맞다.
2번: X. 틀린 부분은 "스크린 라우터, 베스천 호스트, 프록시 서버"를 IDS의 구성요소라고 본 점이다. 실제로는 IDS의 구성요소를 센서, 분석 엔진, 관리 콘솔, 이벤트 저장소 등으로 보는 것이 맞고, 제시된 용어들은 방화벽 또는 프록시 기반 보안 구조에서 주로 쓰인다.
3번: O. 호스트기반 IDS는 설치된 개별 호스트 내부에서 로그, 파일 무결성, 시스템 호출, 프로세스 활동 등을 감시하여 침입 징후를 탐지한다. 따라서 설치된 호스트 내의 침입 유형을 탐지한다는 설명은 타당하다.
4번: O. 공정오류는 false positive를 뜻하며, 실제로는 정상인 행위를 침입이나 공격으로 잘못 판단하는 경우이다. 제시된 설명은 공정오류의 정의와 일치한다.

오답 포인트

2번은 IDS와 방화벽 관련 용어를 섞어 놓은 선지이다. 탐지 방식이나 오탐 개념은 익숙해도, 보안 장비의 구성요소와 배치 구조를 구분하지 못하면 방화벽 용어를 IDS 용어로 오인하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

보안 시스템 문제는 먼저 탐지 방식인지, 장비 구성인지, 배치 위치인지, 오탐 개념인지를 나눈다. 그다음 특정 용어가 탐지 엔진·센서 계열인지, 아니면 방화벽·프록시 구조 용어인지를 구분하면 정답을 빠르게 걸러낼 수 있다.

암기 포인트

IDS는 센서와 분석으로 탐지하고, 스크린 라우터·베스천 호스트·프록시는 방화벽 구조로 기억한다.

NoteBase

문 3. 공개키 암호화 알고리즘이 아닌 것은?

① ARIA

② RSA(Rivest, Shamir, Adleman)

③ ElGamal

④ ECC(Elliptic Curve Cryptosystem)

정답 1번

출제 포인트

대칭키 블록 암호와 공개키 암호를 구분하는 문제이다.

핵심 개념

ARIA는 하나의 비밀키로 암호화와 복호화를 처리하는 대칭키 블록 암호이다.
RSA는 큰 정수의 소인수분해 난이도에 기반한 대표적 공개키 암호이다.
ElGamal은 이산대수 문제에 기반한 공개키 암호이다.
ECC는 타원곡선 이산대수 문제에 기반한 공개키 암호 체계이다.

선지별 해설

① O
ARIA는 공개키 암호가 아니라 대칭키 블록 암호이다. 같은 비밀키로 암호화와 복호화를 수행하므로 발문에 맞는 정답이다.

② X
틀린 판단은 RSA를 공개키 암호가 아닌 것으로 보는 점이다. 올바르게는 RSA는 대표적인 공개키 암호화 알고리즘이다.

③ X
틀린 판단은 ElGamal을 공개키 암호가 아닌 것으로 보는 점이다. 올바르게는 ElGamal은 이산대수 문제 기반의 공개키 암호이다.

④ X
틀린 판단은 ECC를 공개키 암호가 아닌 것으로 보는 점이다. 올바르게는 ECC는 타원곡선 기반 공개키 암호 체계이다.

NoteBase

오답 포인트

알고리즘 이름만 보고 공개키 여부를 감으로 고르면 틀리기 쉽다. 이 문항은 명칭 암기가 아니라 대칭키와 공개키의 분류 기준을 정확히 묻는다.

다시 나오면 이렇게 판단

선지 이름을 보자마자 먼저 대칭키인지 공개키인지 분류하면 된다. RSA·ElGamal·ECC는 공개키로, ARIA·AES·DES·SEED는 대칭키로 판단한다.

암기 포인트

ARIA는 대칭키이고 RSA·ElGamal·ECC는 공개키이다.

NoteBase

문 4. OECD 개인정보 보안 8원칙에 대한 내용으로 가장 옳지 않은 것은?

① 수집 제한의 원칙

② 정보 정확성의 원칙

③ 비공개의 원칙

④ 책임의 원칙

정답 3번

출제 포인트

이 문제는 OECD 개인정보 보호 8원칙의 정확한 명칭을 구별할 수 있는지를 묻는 문제이다.

핵심 개념

수집 제한의 원칙은 개인정보를 적법하고 공정한 수단으로, 필요한 범위에서 수집해야 한다는 원칙이다.
정보 정확성의 원칙은 개인정보가 이용 목적에 맞게 정확하고 완전하며 최신 상태로 유지되어야 한다는 원칙이다.
공개의 원칙은 개인정보 처리방침과 운영 내용을 공개해 정보주체가 알 수 있게 해야 한다는 원칙이다.
책임의 원칙은 개인정보처리자가 위 원칙들을 지킬 책임을 진다는 원칙이다.

선지별 해설

1번 O: OECD 8원칙에는 수집 제한의 원칙이 포함된다. 개인정보는 무제한 수집이 아니라 목적에 필요한 범위에서 공정하게 수집해야 한다는 취지이다.
2번 O: OECD 8원칙에는 정보 정확성의 원칙이 포함된다. 수집된 정보는 목적에 맞게 정확성, 완전성, 최신성이 유지되어야 한다.
3번 X: 틀린 부분은 '비공개'이다. OECD 8원칙의 해당 명칭은 비공개의 원칙이 아니라 공개의 원칙이며, 개인정보 처리방침과 운영 내용을 공개해 투명성을 확보해야 한다.
4번 O: OECD 8원칙에는 책임의 원칙이 포함된다. 개인정보를 처리하는 자가 각 원칙 준수에 대해 책임을 진다는 내용이다.

오답 포인트

공개의 원칙과 보안성 확보 원칙을 혼동하면 3번을 맞는 말처럼 보기 쉽다. 보안은 무조건 숨기는 것이 아니라, 필요한 보호조치를 하면서도 처리방침과 운영의 투명성은 공개한다는 점이 함정이다.

다시 나오면 이렇게 판단

OECD 8원칙 문제는 각 원칙의 한글 명칭부터 확인하면 풀린다. 수집 제한, 정보 정확성, 목적 명확화, 이용 제한, 안전 보호, 공개, 개인 참여, 책임처럼 정식 명칭에 없는 단어가 끼어들면 오답으로 판단할 수 있다.

NoteBase

암기 포인트

OECD 8원칙은 비공개가 아니라 공개이고, 숨김은 보안 원칙의 영역이다.

NoteBase

문 5. DoS(Denial of Service)는 공격 대상이 수용할 수 있는 능력 이상의 정보나 사용자 또는 네트워크의 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격이다. DoS공격 중 하나인, SYN Flooding에 대한 설명으로 가장 옳은 것은?

① TCP 프로토콜의 3way hand shaking을 이용하여 공격 대상 시스템을 마비시키기 위한 방법으로 클라이언트(공격자)가 SYN+ACK패킷만을 지속적으로 보내는 방법이다.

② 클라이언트(공격자)가 짧은 시간에 많은 수의 SYN패킷을 서버에 보내 접속을 요청한 후, 클라이언트가 ACK패킷을 보내주지 않는 방법이다.

③ Ping of Death공격으로 클라이언트(공격자)가 ICMP ping을 이용하여 서버에 ACK패킷을 지속적으로 보내는 방법이다.

④ TCP패킷의 시퀀스 번호를 조작하여 서버를 공격하는 방법이다.

정답 2번

출제 포인트

이 문제는 TCP 3-way handshaking을 악용하는 SYN Flooding의 동작 원리와 다른 DoS 기법을 구분하는지를 묻는 문제이다.

핵심 개념

SYN Flooding은 공격자가 짧은 시간에 많은 SYN 패킷을 보내 연결을 요청한 뒤 마지막 ACK를 완료하지 않아 서버에 반개방 연결을 누적시키는 공격이다. 핵심 구분점은 사용하는 패킷이 SYN이며, 서버의 자원을 소모시키는 원인이 미완료 연결 상태라는 점이다.

1번

X이다. 틀린 표현은 "클라이언트(공격자)가 SYN+ACK패킷만을 지속적으로 보내는 방법"이다. SYN Flooding은 공격자가 SYN 패킷을 대량으로 보내고 서버가 돌려준 SYN+ACK에 대해 최종 ACK를 보내지 않아 반개방 연결을 쌓는 공격이다. SYN+ACK는 일반적으로 서버가 응답으로 보내는 패킷이다.

2번

O이다. 공격자가 짧은 시간에 많은 SYN 패킷을 보내 접속을 요청한 뒤 최종 ACK를 보내지 않으면 서버는 연결 대기 상태를 유지하게 된다. 이 반개방 연결이 누적되면 백로그 큐와 자원이 소진되어 정상 사용자의 접속이 어려워진다.

NoteBase

3번

X이다. 틀린 표현은 "Ping of Death공격으로"와 "ICMP ping을 이용하여 서버에 ACK패킷을 지속적으로 보내는 방법"이다. Ping of Death는 비정상적으로 크거나 잘못 조합된 ICMP 패킷으로 시스템 오류를 유발하는 공격이다. ACK 패킷을 지속적으로 보내는 설명도 SYN Flooding이나 Ping of Death의 핵심 원리가 아니다.

4번

X이다. 틀린 표현은 "TCP패킷의 시퀀스 번호를 조작하여 서버를 공격하는 방법"이다. TCP 시퀀스 번호 조작은 세션 하이재킹이나 TCP 스푸핑 계열의 설명에 가깝다. SYN Flooding은 시퀀스 번호 조작이 아니라 대량의 SYN 요청과 미완료 핸드셰이크를 이용한다.

오답 포인트

이 문항의 함정은 패킷 이름과 공격 기법 이름을 뒤섞는 데 있다. 1번은 SYN과 SYN+ACK의 송신 주체를 바꾸었고, 3번은 Ping of Death와 ACK Flood 성격의 표현을 섞었으며, 4번은 세션 하이재킹 계열 개념을 SYN Flooding에 끼워 넣었다.

다시 나오면 이렇게 판단

SYN Flooding이 보이면 먼저 TCP 3-way handshaking의 순서를 떠올리면 된다. 공격자가 보내는 것은 SYN이고, 서버가 기다리게 되는 것은 최종 ACK이므로 반개방 연결이 누적된다는 설명이면 정답 방향이다.

암기 포인트

SYN Flooding은 SYN 요청 다수 전송 후 최종 ACK 부재로 반개방 연결을 쌓는 공격이다.

NoteBase

문 6. IPSec (IP Security)에는 전송 모드(transport mode)와 터널 모드(tunnel mode)가 운영된다. IPSec에 대한 설명으로 가장 옳지 않은 것은?

① 전송 모드는 보통 호스트-대-호스트 데이터 보호를 필요로 할 때 사용된다.

② 터널 모드에서 IPSec은 가상 터널을 이용하며 새로운 IP패킷은 원래의 IP헤드와 정보를 포함한다.

③ 네트워크 레벨에서 패킷에 대한 보안을 제공하기 위해 IETF에 의해 설계된 프로토콜이다.

④ 전송 모드와 터널 모드에서 IPSec은 전송 계층에서 온 정보 즉, IP헤드를 포함한 IP패킷 전체를 보호한다.

정답 4번

출제 포인트

이 문제는 IPSec의 전송 모드와 터널 모드가 무엇을 보호하는지, 그리고 IPSec이 어느 계층에서 동작하는지를 구분하는 문제이다.

핵심 개념

전송 모드는 종단 호스트 사이에서 기존 IP 헤더는 유지하고 상위 계층 데이터 중심으로 보호하는 방식이다. 결정 차이축은 보호 범위이며 키워드는 호스트-대-호스트, 기존 IP 헤더 유지이다.
터널 모드는 원래 IP 패킷 전체를 새 IP 패킷 안에 캡슐화하여 보호하는 방식이다. 결정 차이축은 보호 범위이며 키워드는 새 IP 헤더, 원본 IP 패킷 전체 캡슐화이다.
IPSec은 네트워크 계층에서 IP 패킷 보안을 제공하는 IETF 표준 프로토콜 집합이다. 결정 차이축은 동작 계층이며 키워드는 네트워크 계층, AH, ESP이다.

NoteBase

선지별 해설

① O
전송 모드는 보통 종단 호스트 간 통신에서 사용되며 호스트-대-호스트 데이터 보호에 적합하다.
기존 IP 헤더를 그대로 두고 상위 계층 데이터 중심으로 보호하므로 전송 모드 설명에 맞다.
② O
터널 모드는 새 외부 IP 헤더를 붙이고 그 안에 원래 IP 패킷 전체를 넣는다.
따라서 새 패킷 내부에는 원래의 IP 헤더와 데이터가 함께 포함된다.
③ O
IPSec은 네트워크 계층에서 인증과 기밀성 등을 제공하도록 IETF가 표준화한 프로토콜 집합이다.
전송 계층 보안인 TLS와 달리 IP 패킷 수준에서 동작한다.
④ X
틀린 부분은 "전송 모드와 터널 모드에서"와 "IP헤더를 포함한 IP패킷 전체를 보호한다"이다.
실제로는 터널 모드가 원래 IP 패킷 전체를 새 패킷 안에 캡슐화해 보호하고, 전송 모드는 기존 IP 헤더를 유지한 채 상위 계층 데이터 중심으로 보호한다.
또한 IPSec은 전송 계층이 아니라 네트워크 계층에서 동작한다.

오답 포인트

"IP 패킷을 보호한다"는 표현만 보고 두 모드가 모두 같은 범위를 보호한다고 착각하기 쉽다. 이 문항은 보호 대상이 상위 계층 데이터 중심인지, 원래 IP 패킷 전체인지의 차이를 바꿔 놓은 점이 함정이다.

다시 나오면 이렇게 판단

IPSec 문제는 먼저 동작 계층이 네트워크 계층인지 확인하고, 다음으로 전송 모드는 기존 IP 헤더 유지, 터널 모드는 원래 IP 패킷 전체 캡슐화라는 축으로 판단하면 된다.

암기 포인트

전송 모드는 헤더 유지와 데이터 보호, 터널 모드는 패킷 전체 캡슐화와 보호이다.

NoteBase

문 7. 전자우편에 프라이버시, 무결성, 그리고 인증을 제공하기 위해 필 짐머만(Phil Zimmermann)에 의해 고안된 것으로, 안전한 전자우편 메시지를 생성하거나 향후에 검색한 파일을 안전하게 저장하기 위해 사용될 수 있다. 자신이 통신하기 원하는 각각의 사람들에 대한 공개키가 필요하고, 자신에게 속해 있는 개인키/공개키의 링이 필요한 프로토콜은?

① POP3

② SMTP

③ PGP

④ S/MIME

정답 3번

출제 포인트

이 문제는 PGP와 POP3, SMTP, S/MIME의 기능 차이를 구분하고, 특히 필 짐머만과 공개키 링·개인키 링이라는 단서로 PGP를 식별하는지를 묻는 문제이다.

핵심 개념

PGP는 필 짐머만이 고안한 전자우편 보안 체계로, 공개키 암호와 전자서명을 이용해 프라이버시, 무결성, 인증을 제공하며 공개키 링과 개인키 링을 사용한다.
POP3는 메일 서버에서 전자우편을 내려받는 수신 프로토콜이다.
SMTP는 전자우편을 서버로 보내는 전송 프로토콜이다.
S/MIME는 MIME 기반 전자우편 보안 표준이지만, 문제의 핵심 단서인 필 짐머만과 키 링 구조를 직접 가리키지는 않는다.

NoteBase

선지별 해설

① X
POP3는 전자우편을 수신하기 위한 프로토콜이다. 틀린 부분은 보안 전자우편 생성과 키 링 사용 주체를 POP3로 본 점이다. 실제로는 공개키 링과 개인키 링을 사용하여 전자우편 보안을 제공하는 PGP이다.

② X
SMTP는 전자우편을 전송하는 프로토콜이다. 틀린 부분은 프라이버시, 무결성, 인증을 제공하는 보안 프로토콜로 본 점이다. 실제로는 메일 전송 기능은 SMTP가 맡고, 문제의 보안 기능과 키 링 구조는 PGP가 맡는다.

③ O
PGP는 필 짐머만이 만든 전자우편 보안 프로토콜로, 사용자가 통신 상대의 공개키를 보유하고 자신의 공개키 링과 개인키 링을 관리한다. 지문의 설명과 정확히 일치한다.

④ X
S/MIME도 전자우편 보안을 제공하지만, 문제의 단서인 필 짐머만이 고안했다는 점과 공개키 링·개인키 링 구조에는 맞지 않는다. 틀린 부분은 지문의 PGP 특징을 S/MIME에 대응시킨 점이다. 실제로는 해당 설명의 대상은 PGP이다.

오답 포인트

전자우편 관련 프로토콜이라는 공통점 때문에 POP3, SMTP, S/MIME를 함께 떠올리기 쉽다. 그러나 POP3는 수신, SMTP는 전송 기능이고, 보안 전자우편과 필 짐머만, 공개키 링·개인키 링이라는 단서가 붙으면 PGP로 바로 좁혀진다.

다시 나오면 이렇게 판단

전자우편 문제에서는 먼저 기능을 나눠 본다. 수신이면 POP3, 전송이면 SMTP, MIME 기반 인증서 보안이면 S/MIME, 필 짐머만과 키 링 관리가 나오면 PGP로 판단된다.

암기 포인트

PGP는 필 짐머만, 키 링, 전자우편 보안이다. POP3는 받기, SMTP는 보내기, S/MIME는 인증서 기반 메일 보안이다.

NoteBase

문 8. 「전자서명법」상 공인인증서에 대한 설명으로 가장 옳지 않은 것은?

① 공인인증서에는 공인인증기관의 서명키가 포함되어야 한다.

② 가입자의 사망, 실종선고 또는 해산 사실을 인지한 경우에는 당해 공인인증서를 폐지하여야 한다.

③ 공인인증서의 유효기간이 경과한 경우에는 그 사유가 발생한 때에 그 효력이 소멸된다.

④ 공인인증기관은 공인인증서를 발급받고자 하는 자의 신청이 있는 경우에는 공인인증서의 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다.

정답 1번

쟁점

이 문제는 구 전자서명법상 공인인증서의 필수 기재사항, 폐지 사유, 효력 소멸 사유, 제한 공인인증서 발급 가능 여부를 구별하는 문제이다.
핵심은 공인인증서에 들어가는 것은 가입자의 전자서명검증정보와 인증기관 식별정보이지 공인인증기관의 서명키 자체가 아니라는 점이다.

용어 풀이

공인인증서 = 구 전자서명법상 공인인증기관이 가입자의 신원을 확인한 뒤 발급하는 인증서이다.
전자서명검증정보 = 전자서명이 진정한지 확인하는 공개 정보이다.

핵심 구분

공인인증서에는 가입자의 전자서명검증정보, 공인인증기관의 명칭 등 인증기관임을 확인할 수 있는 정보, 유효기간 등이 포함된다. 반면 공인인증기관의 서명키 같은 전자서명생성정보는 포함 대상이 아니다.
또한 공인인증서의 유효기간이 지나면 효력이 소멸하고, 가입자의 사망·실종선고·해산 등을 인지하면 공인인증기관은 해당 인증서를 폐지하여야 한다.
신청이 있으면 이용범위 또는 용도를 제한하는 공인인증서도 발급할 수 있다.

NoteBase

기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2019 · 10월

선지별 해설

① X
- 틀린 이유는 "공인인증기관의 서명키"라는 표현 때문이다. 구 전자서명법상 공인인증서의 포함사항은 가입자의 전자서명검증정보, 공인인증기관의 명칭 등 인증기관임을 확인할 수 있는 정보, 유효기간 등이지 공인인증기관의 서명키 자체가 아니다.
- 틀린 표현: 공인인증기관의 서명키가 포함되어야 한다.
- 올바른 표현: 가입자의 전자서명검증정보와 공인인증기관임을 확인할 수 있는 정보 등이 포함되어야 한다.

② O
- 가입자의 사망, 실종선고 또는 해산 사실을 공인인증기관이 인지한 경우는 법정 폐지 사유이다. 따라서 당해 공인인증서를 폐지하여야 한다.
- 핵심은 "할 수 있다"가 아니라 "폐지하여야 한다"는 의무 규정이라는 점이다.

③ O
- 공인인증서의 유효기간이 경과한 경우는 효력 소멸 사유이다. 별도의 추가 조치가 있어야만 효력이 없어지는 구조가 아니라 그 사유가 발생하면 효력이 소멸된다.
- 핵심은 폐지 사유와 효력 소멸 사유를 구별하는 것이다.

④ O
- 구 전자서명법은 공인인증서를 발급받고자 하는 자의 신청이 있으면 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다고 규정하였다.
- 제한 인증서의 발급 가능 여부를 묻는 선지로서 조문 내용과 일치한다.

오답 포인트

①의 함정은 인증기관이 인증서를 발급할 때 서명행위를 한다는 사실과 인증서 안에 서명키 자체가 들어간다는 주장을 혼동하게 만드는 점이다. 인증기관은 인증서에 관여하지만 그 서명키 자체를 인증서에 넣는 것은 아니다. 또한 ②의 폐지 사유와 ③의 효력 소멸 사유를 같은 범주로 섞어서 보면 헷갈리기 쉽다.

다시 나오면 이렇게 판단

전자서명법형 선지는 먼저 "무엇이 인증서에 기재되는가"와 "어떤 경우에 효력이 없어지는가"를 나누어 본다. 그 다음 표현이 검증정보인지 서명키인지, 임의 규정인지 의무 규정인지, 폐지 사유인지 효력 소멸 사유인지를 구분하면 정답을 빠르게 고를 수 있다.

암기 포인트

공인인증서에는 검증정보가 들어가고 서명키는 들어가지 않는다. 사망·실종선고·해산은 폐지, 유효기간 경과는 효력 소멸이다.

NoteBase

문 9. 「개인정보 보호법」 상 <보기> 안의 ㉠에 들어갈 숫자로 옳은 것은?

<보기>
개인정보에 관한 분쟁을 조정하는 개인정보 분쟁조정위원회는 위원장 1명을 포함한 ㉠ 명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.

① 10
② 20
③ 30
④ 40

정답 2번

쟁점

이 문제는 2019년 10월 출제 당시 개인정보 분쟁조정위원회의 법정 구성 인원에 관한 문제이다.
핵심은 "위원장 1명을 포함한 20명 이내"라는 숫자를 정확히 구별하는 것이다.

용어 풀이

개인정보 분쟁조정위원회는 개인정보에 관한 분쟁을 조정하는 법정 조정기구이다.

핵심 구분

2019년 10월 출제 당시 시행 중인 개인정보 보호법은 개인정보 분쟁조정위원회를 위원장 1명을 포함한 20명 이내의 위원으로 구성한다고 정하였다.
따라서 10명, 30명, 40명은 모두 숫자만 바꿔 놓은 오답이다.

NoteBase

기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2019 · 10월

선지별 해설

① X
- 숫자 10명이 틀렸다. 출제 당시 법은 위원장 1명을 포함한 20명 이내라고 규정하였다.
- 틀린 표현: 10명
- 올바른 표현: 20명

② O
- 출제 당시 법정 위원 수는 위원장 1명을 포함한 20명 이내였다. 따라서 빈칸에는 20이 들어간다.

③ X
- 숫자 30명이 틀렸다. 출제 당시 기준으로는 30명이 아니라 20명 이내였다.
- 틀린 표현: 30명
- 올바른 표현: 20명

④ X
- 숫자 40명이 틀렸다. 위원 수를 과장한 선택지이며 법정 상한과 맞지 않는다.
- 틀린 표현: 40명
- 올바른 표현: 20명

오답 포인트

이 문제는 위원회의 기능이나 절차가 아니라 법정 인원수만 정확히 기억하는지를 묻는다.
숫자형 법령 문제에서 비슷한 위원회 숫자나 개정 후 숫자를 섞어 기억하면 오답이 된다.

다시 나오면 이렇게 판단

법령형 숫자 문제는 기관명과 숫자를 한 묶음으로 확인하면 된다.
선택지가 숫자만 달라질 때에는 조문 속 핵심 수치 하나만 정확히 대조해도 정답을 고를 수 있다.

암기 포인트

개인정보 분쟁조정위원회는 출제 당시 위원장 포함 20명 이내이다.

NoteBase

문 10. KDC(key distribution center) 없이 양쪽 통신 주체가 대칭 세션 키를 생성할 수 있는 프로토콜은?

① Otway–Rees 프로토콜

② Needham–Schroeder 프로토콜

③ Diffie–Hellman 프로토콜

④ Kerberos 프로토콜

정답 3번

출제 포인트

이 문제는 KDC를 두는 대칭키 분배 방식과, 제3자 없이 당사자끼리 공유 비밀을 만드는 Diffie-Hellman의 차이를 묻는 문제이다.

핵심 개념

Otway-Rees는 신뢰된 서버(KDC)의 도움으로 통신 당사자에게 세션 키를 분배하는 대칭키 인증 프로토콜이다.
Needham-Schroeder는 이 문맥에서는 KDC를 이용해 세션 키를 나누는 대칭키 버전을 가리킨다.
Diffie-Hellman은 양측이 공개값을 교환해 제3자 없이 같은 공유 비밀을 계산하는 키 합의 프로토콜이다.
Kerberos는 AS/TGS로 대표되는 KDC 기반 인증 체계로, 티켓과 세션 키를 중앙 서버가 발급한다.

선지별 해설

① X: Otway-Rees는 신뢰된 서버가 개입해 세션 키를 전달하는 구조이다. 틀린 부분은 'KDC 없이'라는 조건에 맞지 않는다는 점이다. 올바르게는 'Otway-Rees는 KDC를 이용해 세션 키를 분배한다'이다.
② X: Needham-Schroeder는 이 문항 맥락에서 대칭키 기반의 KDC 이용 프로토콜을 뜻한다. 틀린 부분은 '양측만으로 세션 키를 만든다'고 볼 수 없다는 점이다. 올바르게는 'Needham-Schroeder 대칭키 방식은 KDC를 통해 세션 키를 분배받는다'이다.
③ O: Diffie-Hellman은 양측이 각자 비밀값과 공개값을 사용해 동일한 공유 비밀을 계산하므로 KDC가 없어도 대칭 세션 키의 재료를 만들 수 있다. 인증 기능은 약하지만, 키 합의 자체는 제3자 없이 가능하다.
④ X: Kerberos는 대표적인 KDC 기반 인증 프로토콜이다. 틀린 부분은 '중앙 분배자 없이 동작한다'고 볼 수 없다는 점이다. 올바르게는 'Kerberos는 KDC가 티켓과 세션 키를 발급해 인증을 수행한다'이다.

오답 포인트

Needham-Schroeder와 Diffie-Hellman을 모두 '키 교환'으로만 외우면 헷갈리기 쉽다. 이 문제의 함정은 '키를 만든다'와 '키를 중앙에서 받아 분배받는다'를 구분하지 못하게 하는 데 있다.

NoteBase

다시 나오면 이렇게 판단

발문에 'KDC 없이', '제3자 없이', '양측이 직접 공유 비밀 생성'이 나오면 Diffie-Hellman 계열을 먼저 떠올리면 된다. 반대로 서버가 세션 키를 나눠 주거나 티켓을 발급하면 KDC 기반 프로토콜로 판단한다.

암기 포인트

Diffie-Hellman은 당사자끼리 합의, Kerberos·Otway-Rees·Needham-Schroeder는 KDC가 개입하는 분배 방식이다.

NoteBase

문 11. 난수에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 옳게 짝지은 것은?

<보기>
난수(random number)는 암호기술에서 중요한 역할을 담당하고 있다. 특히, 암호기술에 사용 가능한 난수는 다음의 두 가지 성질을 가져야 한다. _____㉠_____은 과거의 수열로부터 다음 수를 예측할 수 없다는 성질이고, _____㉡_____은 같은 수열을 재현할 수 없다는 성질이다.

① ㉠: 무작위성, ㉡: 예측 불가능성
② ㉠: 예측 불가능성, ㉡: 재현 불가능성
③ ㉠: 재현 불가능성, ㉡: 예측 불가능성
④ ㉠: 무작위성, ㉡: 재현 불가능성

정답 2번

출제 포인트

이 문제는 암호용 난수의 핵심 성질인 예측 불가능성과 재현 불가능성을 정의 문장에 맞춰 구분하는 문제이다.

핵심 개념

예측 불가능성은 과거에 나온 수열을 알아도 다음 값을 미리 맞힐 수 없는 성질이다. 재현 불가능성은 같은 난수열을 다시 만들어 내거나 동일한 수열을 반복 재생할 수 없는 성질이다. 무작위성은 전체 분포가 치우치지 않고 불규칙하게 보이는 성질이지만, 이 문장의 직접 정의는 예측 여부와 재현 여부를 묻는다.

선지별 해설

① X: ㄱ의 "무작위성"이 틀린 표현이다. 과거 수열로부터 다음 수를 예측할 수 없다는 설명은 무작위성이 아니라 예측 불가능성이다. ㄴ의 "예측 불가능성"도 틀린 표현이다. 같은 수열을 다시 만들 수 없다는 뜻이므로 올바르게는 재현 불가능성이다.
② O: ㄱ을 예측 불가능성, ㄴ을 재현 불가능성으로 짝지은 것이 보기의 정의와 정확히 일치한다.
③ X: ㄱ의 "재현 불가능성"과 ㄴ의 "예측 불가능성"이 서로 뒤바뀌었다. 올바르게는 ㄱ이 예측 불가능성이고 ㄴ이 재현 불가능성이다.
④ X: ㄱ의 "무작위성"이 틀린 표현이다. 보기의 첫 번째 설명은 분포의 불규칙성보다 다음 값의 예측 가능성을 묻는다. 올바르게는 예측 불가능성이다. ㄴ의 재현 불가능성은 맞는 방향이지만 ㄱ이 틀려 전체 선택지는 오답이다.

오답 포인트

무작위성과 예측 불가능성을 같은 말처럼 섞어 쓰면 ①이나 ④로 흔들리기 쉽다. 이 문항은 성질 이름을 외우는 문제가 아니라 문장 속 핵심 동사인 "예측할 수 없다"와 "재현할 수 없다"를 각각 대응시키는지가 함정이다.

NoteBase

다시 나오면 이렇게 판단

선지에 난수 성질이 섞여 나오면 먼저 문장에 "다음 값을 맞출 수 없다"가 있는지, "같은 수열을 다시 만들 수 없다"가 있는지를 본다. 전자는 예측 불가능성, 후자는 재현 불가능성으로 바로 연결하면 된다.

암기 포인트

예측 불가능성은 다음 값 차단이고, 재현 불가능성은 같은 수열 반복 차단이다.

NoteBase

문 12. 일방향 해시함수의 성질로 가장 옳지 않은 것은?

① 정해진 길이의 입력 값을 받아 정해진 길이의 결과 값을 출력한다.

② 일반적으로 빠른 시간 내에 결과 값을 계산할 수 있다.

③ 일반적으로 입력 값이 다르면 결과 값도 다르다.

④ 결과 값으로부터 입력 값을 역산할 수 없다.

정답 1번

출제 포인트

이 문제는 일방향 해시함수의 기본 성질인 가변 길이 입력, 고정 길이 출력, 계산 효율성, 일방향성을 구별할 수 있는지를 묻는다.

핵심 개념

일방향 해시함수는 임의 길이의 입력을 받아 고정 길이의 해시값으로 압축하는 함수이다.
핵심 성질은 입력으로부터 해시값을 빠르게 계산할 수 있다는 점과, 해시값만으로 원래 입력을 실질적으로 복원할 수 없다는 점이다.
서로 다른 입력이 항상 다른 해시값을 내는 것은 아니지만, 좋은 해시함수는 서로 다른 입력이 같은 값을 내는 충돌이 드물도록 설계된다.

선지별 해설

1번: X. 틀린 부분은 "정해진 길이의 입력 값"이다. 해시함수는 보통 정해진 길이 입력만 받는 것이 아니라 임의 길이의 입력을 받아 고정 길이의 결과 값을 출력한다.
2번: O. 해시함수는 무결성 검증, 비밀번호 저장, 전자서명 등에서 반복 사용되므로 입력으로부터 해시값을 효율적으로 계산할 수 있어야 한다.
3번: O. 절대적으로 항상 다른 결과가 나오는 것은 아니지만, 일반적인 성질로는 서로 다른 입력이 같은 해시값을 내기 어렵도록 설계된다. 선지의 "일반적으로"라는 표현 때문에 옳은 설명으로 본다.
4번: O. 일방향성은 결과 값만 보고 원래 입력 값을 역산하기 매우 어렵다는 뜻이다. 따라서 해시값으로부터 입력을 복원할 수 없다는 설명은 맞다.

오답 포인트

1번은 출력 길이가 고정이라는 성질을 입력 길이에도 그대로 옮겨 붙인 함정이다. 3번은 충돌 가능성을 떠올리면 흔들리기 쉬운데, 선지에 "항상"이 아니라 "일반적으로"가 들어 있어 충돌 저항성을 설명한 문장으로 처리해야 한다.

NoteBase

다시 나오면 이렇게 판단

해시함수 선지는 먼저 입력 길이가 가변인지, 출력 길이가 고정인지 확인한다. 그다음 계산은 빠르게 가능하지만 역산은 어렵다는 두 축으로 보면 대부분의 오답을 걸러낼 수 있다.

암기 포인트

해시는 가변 입력, 고정 출력, 빠른 계산, 어려운 역산이다.

NoteBase

문 13. 「정보통신기반 보호법」 및 동법 시행령에서 규정한 정보통신기반보호위원회에 대한 설명으로 가장 옳지 않은 것은?

① 위원회의 위원장은 행정안전부장관이다.

② 위원회의 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다.

③ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.

④ 위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

정답 1번

쟁점

이 문제는 정보통신기반보호위원회의 구성과 운영에 관한 법령 내용을 정확히 구별하는 문제이다.
핵심은 위원장, 위원 자격, 실무위원회 설치, 의결정족수를 각각 따로 구분하는 것이다.

용어 풀이

차관급 공무원은 중앙행정기관에서 차관에 준하는 지위의 공무원을 말한다.
실무위원회는 위원회의 심의를 지원하고 위임된 사항을 검토·심의하는 하위 위원회이다.

핵심 구분

정보통신기반보호위원회 위원장은 국무조정실장이다. 행정안전부는 관련 위원이나 소관 업무와 연결될 수 있으나 위원장을 맡는 주체는 아니다.
위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 구성된다.
위원회 아래에는 공공분야 실무위원회와 민간분야 실무위원회가 두어지며, 의결은 재적위원 과반수 출석과 출석위원 과반수 찬성으로 한다.

NoteBase

선지별 해설

① X: 위원회의 위원장은 행정안전부장관이 아니라 국무조정실장이다. 위원장 주체를 잘못 적은 선지이므로 옳지 않다.
틀린 표현: 위원회의 위원장은 행정안전부장관이다.
올바른 표현: 위원회의 위원장은 국무조정실장이다.

② O: 법은 위원회의 위원을 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 정한다. 위원 구성에 관한 조문 내용을 그대로 반영한 선지이다.

③ O: 법은 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 두도록 한다. 실무위원회의 존재와 분야 구분을 맞게 적은 선지이다.

④ O: 시행령은 위원회가 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다고 정한다.
출석정족수와 의결정족수를 모두 정확히 적은 선지이다.

오답 포인트

이 문제를 틀렸다면 위원회 위원장과 실무위원회 또는 관계 부처의 직위를 혼동했을 가능성이 높다. 특히 행정안전부가 정보통신기반시설 보호 체계의 관련 기관으로 등장하므로 위원장까지 행정안전부장관으로 착각하기 쉽다.

다시 나오면 이렇게 판단

위원회 관련 조문 문제는 먼저 위원장이 누구인지, 다음으로 위원 자격이 무엇인지, 그 아래 실무위원회가 어떻게 나뉘는지, 마지막으로 정족수가 어떻게 되는지를 순서대로 나누어 판단한다. 장관, 차관, 국무조정실장처럼 직위가 섞여 나오면 위원장인지 위원인지부터 구별하면 정답이 빨라진다.

암기 포인트

위원장은 국무조정실장이고, 위원은 차관급 공무원과 위촉위원이며, 실무위원회는 공공·민간으로 나뉘고, 의결은 재적 과반 출석과 출석 과반 찬성이다.

NoteBase

문 14. 접근통제 보안 모델에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 옳게 짝지은 것은?

<보기>

_____㉠_____은 데이터 무결성에 초점을 둔 상업용 모델로서, 비인가자들의 데이터 변형 방지를 목적으로 한다. 주체는 보다 낮은 무결성 수준의 정보를 읽을 수 없고, 보다 높은 무결성 수준의 객체를 수정할 수 없다.

_____㉡_____도 무결성 모델의 하나로서, 허가받은 사용자가 허가받지 않고 데이터를 수정하는 것을 방지한다. 주체는 단지 허가된 프로그램을 통하여 객체에 접근할 수 있다.

① ㉠: Bell-LaPadula Model, ㉡: Biba Model

② ㉠: Biba Model, ㉡: Bell-LaPadula Model

③ ㉠: Biba Model, ㉡: Clark-Wilson Model

④ ㉠: Clark-Wilson Model, ㉡: Biba Model

정답 3번

출제 포인트

이 문제는 무결성 보안 모델인 Biba와 Clark-Wilson의 핵심 통제 원리를 구분할 수 있는지를 묻는 문제이다.

핵심 개념

Biba 모델은 데이터 무결성을 보호하기 위한 계층형 모델로서 'No Read Down, No Write Up'이 핵심이다.
Clark-Wilson 모델은 상업 환경의 무결성 모델로서 허가된 사용자라도 허가된 프로그램을 통해서만 데이터를 다루게 하는 것이 핵심이다.
Bell-LaPadula 모델은 기밀성 모델로서 'No Read Up, No Write Down'이 핵심이므로 무결성 모델과 구별해야 한다.

NoteBase

선지별 해설

① X: ㄱ을 Bell-LaPadula로 둔 부분이 틀리다. ㄱ의 '낮은 무결성 읽기 금지, 높은 무결성 쓰기 금지'는 Biba의 규칙이다. ㄴ도 Biba가 아니라 허가된 프로그램을 통해서만 접근하는 Clark-Wilson이어야 한다. 틀린 표현은 'ㄱ = Bell-LaPadula, ㄴ = Biba'이다. 올바르게는 'ㄱ = Biba, ㄴ = Clark-Wilson'이다.
② X: ㄱ은 Biba라는 점은 맞지만 ㄴ을 Bell-LaPadula로 둔 부분이 틀리다. Bell-LaPadula는 기밀성 모델이라 비인가 수정 방지와 허가된 프로그램을 통한 접근 통제를 설명하지 않는다. 틀린 표현은 'ㄴ = Bell-LaPadula'이다. 올바르게는 'ㄴ = Clark-Wilson'이다.
③ O: ㄱ의 무결성 수준 기반 읽기·쓰기 제한은 Biba 모델의 설명과 일치한다. ㄴ의 '허가된 프로그램을 통해서만 객체 접근'은 Clark-Wilson 모델의 well-formed transaction 통제와 일치하므로 옳다.
④ X: ㄱ을 Clark-Wilson으로, ㄴ을 Biba로 둔 부분이 모두 틀리다. Clark-Wilson은 무결성 수준의 상하 읽기·쓰기 규칙으로 설명되지 않고, Biba는 허가된 프로그램을 통한 접근만을 전면에 둔 모델이 아니다. 틀린 표현은 'ㄱ = Clark-Wilson, ㄴ = Biba'이다. 올바르게는 'ㄱ = Biba, ㄴ = Clark-Wilson'이다.

오답 포인트

ㄱ 문장의 '상업용'이라는 표현만 보고 Clark-Wilson을 먼저 떠올리면 함정에 걸리기 쉽다. 이 문항의 결정 단서는 뒤에 붙은 '낮은 무결성 읽기 금지, 높은 무결성 수정 금지'이며, 이 규칙 조합이 Biba를 확정한다. ㄴ에서는 '허가된 프로그램'이라는 표현이 Clark-Wilson의 핵심 단서이다.

다시 나오면 이렇게 판단

먼저 기밀성 모델인지 무결성 모델인지 구분한 뒤, 규칙 문구를 대입하면 된다. 낮은 무결성 읽기 금지와 높은 무결성 쓰기 금지가 나오면 Biba이고, 높은 기밀성 읽기 금지와 낮은 기밀성 쓰기 금지가 나오면 Bell-LaPadula이다. 허가된 프로그램이나 정형화된 트랜잭션이 나오면 Clark-Wilson으로 판단할 수 있다.

암기 포인트

Biba는 무결성의 상하 수준 통제, Clark-Wilson은 상업용 무결성과 허가된 프로그램, Bell-LaPadula는 기밀성 통제이다.

NoteBase

문 15. 데이터를 도청, 수집해서 데이터를 분석하는 것으로 직접적인 피해를 발생시키지 않는 공격에 해당하는 것은?

① 스니핑
② 스미싱
③ ARP 스푸핑
④ DDoS

정답 1번

출제 포인트

이 문제는 직접적인 피해를 주는 능동적 공격과, 통신 내용을 엿듣고 수집하는 수동적 공격을 구별하는 문제이다.

핵심 개념

스니핑은 네트워크를 지나가는 패킷을 도청하여 정보를 수집하는 수동적 공격이다. 스미싱은 문자메시지로 악성 링크 클릭이나 앱 설치를 유도해 정보를 탈취하는 사회공학 기반 공격이다. ARP 스푸핑은 위조된 ARP 정보로 통신 경로를 속여 트래픽을 가로채는 능동적 공격이다. DDoS는 다수의 요청으로 서비스를 마비시키는 가용성 침해 공격이다.

선지별 해설

① O: 스니핑은 데이터를 도청, 수집, 분석하지만 시스템에 직접 변조나 파괴를 가하지 않는 대표적인 수동적 공격이다.
② X: 틀린 부분은 스미싱을 수동적 도청 공격으로 보는 점이다. 스미싱은 문자메시지로 사용자를 속여 악성 행위를 유도하는 공격이므로 올바르게는 사회공학적 피싱 공격이다.
③ X: 틀린 부분은 ARP 스푸핑을 직접 피해를 발생시키지 않는 공격으로 보는 점이다. ARP 스푸핑은 ARP 테이블을 변조해 통신 흐름을 바꾸므로 올바르게는 능동적으로 개입하는 스푸핑 공격이다.
④ X: 틀린 부분은 DDoS를 데이터 수집형 공격으로 보는 점이다. DDoS는 대량 트래픽으로 정상 서비스를 방해하므로 올바르게는 직접적인 서비스 거부를 일으키는 가용성 공격이다.

오답 포인트

ARP 스푸핑도 결과적으로 패킷을 가로채 볼 수 있어서 스니핑과 비슷하게 느껴질 수 있다. 그러나 문제의 기준은 결과가 아니라 공격 방식이며, 도청만 하면 수동적 공격이고 주소 정보나 트래픽 흐름을 바꾸면 능동적 공격이 된다.

NoteBase

다시 나오면 이렇게 판단

발문에 도청, 수집, 분석, 직접 피해 없음이 나오면 먼저 수동적 공격을 떠올리면 된다. 반대로 위조, 변조, 유도, 마비처럼 대상 시스템이나 사용자의 상태를 바꾸는 표현이 나오면 능동적 공격으로 판단할 수 있다.

암기 포인트

스니핑은 듣기, 스푸핑은 속이기, DDoS는 막기, 스미싱은 문자로 낚기이다.

NoteBase

문 16. <보기>에서 설명하는 블록 암호(Block Cipher) 알고리즘은?

<보기>
• 2010년대 국내에서 개발한 경량 고속 블록 암호 알고리즘이다.
• 스마트폰, 사물인터넷 등 저전력 암호화에 널리 쓸 수 있다.
• AES를 개발한 벨기에 루벤대학 COSIC연구소에서 안전성을 검증받았다.

① SEED
② HIGHT
③ LEA
④ IDEA

정답 3번

출제 포인트

이 문제는 국내 블록 암호 알고리즘들의 개발 시기, 경량성, 활용 환경을 구분하여 LEA의 특징을 식별하는 문제이다.

핵심 개념

LEA는 2010년대 국내에서 개발된 경량 고속 블록 암호로, 저전력 소프트웨어 환경과 IoT 기기 적용을 강하게 의식한 알고리즘이다.
SEED는 국내 표준 대칭키 블록 암호이지만 1990년대 말 개발된 범용 블록 암호이다.
HIGHT는 국내 경량 블록 암호이지만 2000년대 중반에 나온 64비트 블록 암호이다.
IDEA는 국내 알고리즘이 아니라 스위스에서 개발된 블록 암호이다.

NoteBase

선지별 해설

① X: SEED는 국내에서 개발된 블록 암호라는 점은 맞지만, 보기의 핵심인 2010년대 개발 경량 고속 블록 암호와는 다르다.
틀린 표현은 '2010년대 국내 개발 경량 고속 블록 암호'이다. 올바르게는 'SEED는 1990년대 말 개발된 국내 표준 블록 암호'이다.
② X: HIGHT는 저전력 환경을 고려한 국내 경량 블록 암호이지만, 개발 시기가 2010년대가 아니라 2000년대 중반이므로 보기와 완전히 일치하지 않는다.
틀린 표현은 '2010년대 국내 개발'이다. 올바르게는 'HIGHT는 2000년대 중반 개발된 국내 경량 블록 암호'이다.
③ O: LEA는 2010년대 국내에서 개발된 경량 고속 블록 암호이며, 스마트폰과 사물인터넷 같은 저전력 소프트웨어 환경을 목표로 한다. 또한 AES를 만든 벨기에 루벤대학 COSIC 연구소에서 안전성 검증을 받은 것으로 알려져 보기의 설명과 일치한다.
④ X: IDEA는 블록 암호이지만 국내 개발 알고리즘이 아니고, 보기의 국내 경량 고속 암호 설명과도 맞지 않는다.
틀린 표현은 '국내에서 개발한 경량 고속 블록 암호'이다. 올바르게는 'IDEA는 해외에서 개발된 범용 블록 암호'이다.

오답 포인트

국내 알고리즘이라는 단서만 보고 SEED나 HIGHT로 가기 쉽다. 이 문항의 분기점은 '2010년대', '경량 고속', 'IoT 저전력', 'COSIC 검증'이라는 묶음 단서이며, 이 조합은 LEA에 집중된다.

다시 나오면 이렇게 판단

국내 블록 암호 문제에서는 먼저 개발 시기로 후보를 줄이고, 다음으로 경량 암호인지 범용 표준 암호인지를 구분하면 된다. 2010년대 국내 경량 고속 소프트웨어 블록 암호라는 단서가 나오면 LEA를 우선 판단한다.

암기 포인트

LEA는 2010년대 국내 경량 고속 IoT 블록 암호, SEED는 1990년대 국내 표준 블록 암호, HIGHT는 2000년대 국내 경량 블록 암호이다.

NoteBase

문 17. 블록 암호 운용 모드인 CTR 모드에 대한 설명으로 가장 옳지 않은 것은?

① 블록을 암호화할 때마다 1씩 증가해 가는 카운터를 암호화해서 키 스트림을 만들어 낸다.

② 암호화와 복호화가 완전히 같은 구조가 되므로, 프로그램 구현이 간단하다.

③ 블록을 임의의 순서로 처리할 수 있다.

④ 암호화에서는 병렬처리를 할 수 없지만, 복호화에서는 병렬처리가 가능하다.

정답 4번

출제 포인트

이 문제는 CTR 모드의 핵심 구조인 카운터 기반 키스트림 생성과 병렬 처리 가능 여부를 묻는 문제이다.

핵심 개념

CTR 모드는 카운터 값을 블록 암호의 암호화 함수에 넣어 키스트림 블록을 만든 뒤, 이를 평문 또는 암호문과 XOR하는 방식이다. 각 블록은 이전 블록 결과에 의존하지 않으므로 암호화와 복호화 모두 같은 구조로 동작하고 병렬 처리도 가능하다.

선지별 해설

① O. CTR은 매 블록마다 증가하는 카운터를 암호화해 키스트림을 만든다. 평문 자체를 직접 블록 암호에 넣는 것이 아니라 카운터를 암호화한 결과를 XOR에 사용한다.
② O. CTR의 복호화도 암호화와 동일하게 카운터를 암호화해 키스트림을 만든 뒤 XOR하므로 구조가 사실상 같다. 블록 암호의 복호화 함수가 별도로 필요하지 않아 구현이 단순하다.
③ O. 각 블록의 키스트림이 해당 카운터 값만으로 독립적으로 결정되므로 블록을 순차적으로만 처리할 필요가 없다. 따라서 임의 순서 처리와 사전 계산이 가능하다.
④ X. 틀린 부분은 '암호화에서는 병렬처리를 할 수 없지만, 복호화에서는 병렬처리가 가능하다'는 표현이다. CTR은 암호화와 복호화 모두 각 블록이 독립적이므로 둘 다 병렬처리가 가능하다.

오답 포인트

CTR을 CBC와 혼동하면 병렬 처리 성질을 거꾸로 기억하기 쉽다. CBC는 암호화가 이전 암호문 블록에 의존하지만, CTR은 카운터만 알면 각 블록 키스트림을 바로 만들 수 있다는 점이 함정이다.

다시 나오면 이렇게 판단

카운터를 먼저 암호화해 키스트림을 만들고 각 블록이 서로 독립이면 CTR로 판단한다. 독립 구조가 보이면 암호화·복호화 모두 같은 방식이고 둘 다 병렬 처리 가능하다고 정리된다.

NoteBase

암기 포인트

CTR은 카운터 암호화, XOR 결합, 양방향 동일 구조, 양방향 병렬 처리이다.

NoteBase

문 18. 메시지 인증 코드(MAC)에 대한 설명으로 가장 옳지 않은 것은?

① 일방향 해시 함수를 이용하여 MAC을 만들 수 있다.

② 블록 암호를 이용하여 MAC을 만들 수 있다.

③ 재전송 공격에 대응하기 위해서 순서번호, 타임스탬프, 임의의 비표(nonce) 등을 포함하여 MAC을 만들 수 있다.

④ MAC에는 부인방지 기능이 포함되어 있으나, 제3자에게 증명하는 기능은 포함되어 있지 않다.

정답 4번

출제 포인트

이 문제는 MAC의 구현 방식과 보안 기능을 전자서명과 구별할 수 있는지를 묻는 문제이다.

핵심 개념

MAC는 송신자와 수신자가 공유한 비밀키로 메시지 무결성과 인증을 확인하는 값이다.
해시 기반 MAC는 HMAC처럼 일방향 해시 함수와 비밀키를 결합해 만들 수 있고, 블록 암호 기반 MAC는 CBC-MAC처럼 만들 수 있다.
전자서명은 제3자 검증과 부인방지를 제공하지만, MAC는 공유키 방식이므로 제3자에게 송신 사실을 증명하는 부인방지 기능을 제공하지 않는다.

선지별 해설

① O: 일방향 해시 함수를 이용한 대표적 MAC가 HMAC이다. 단순 해시값만 붙이는 것은 MAC가 아니지만, 비밀키와 해시 함수를 결합하면 MAC를 만들 수 있다.
② O: 블록 암호를 이용한 대표적 MAC가 CBC-MAC이다. 따라서 블록 암호를 이용하여 MAC를 만들 수 있다는 설명은 옳다.
③ O: MAC 자체만으로는 재전송 공격을 막기 어려우므로 순서번호, 타임스탬프, nonce 같은 신선도 정보를 메시지에 포함해 함께 검증한다. 이 설명은 옳다.
④ X: 틀린 부분은 'MAC에는 부인방지 기능이 포함되어 있으나'이다. MAC는 공유 비밀키를 쓰므로 송신자와 수신자 모두 MAC를 생성할 수 있어 누가 만들었는지 제3자에게 증명할 수 없고, 따라서 부인방지 기능도 제공하지 않는다. 올바르게는 'MAC에는 무결성과 메시지 인증 기능은 있으나, 부인방지 기능과 제3자 증명 기능은 없다'이다.

오답 포인트

MAC의 인증 기능을 전자서명의 부인방지 기능과 같은 것으로 혼동하면 ④를 맞는 설명으로 착각하기 쉽다.
공유키 기반 인증과 공개키 기반 서명의 차이를 구분하지 못하도록 만든 함정이다.

NoteBase

다시 나오면 이렇게 판단

문장에서 '공유 비밀키'가 보이면 무결성과 인증은 가능하지만 부인방지와 제3자 증명은 불가능하다고 판단한다. 반대로 '제3자 검증'이나 '부인방지'가 나오면 전자서명 계열 개념인지 먼저 본다.

암기 포인트

MAC는 공유키 인증, 전자서명은 공개검증과 부인방지이다.

NoteBase

문 19. 싱글 사인 온(SSO)에 대한 설명으로 가장 옳지 않은 것은?

① 하나의 시스템에서 인증을 받으면, 다른 시스템에 대한 접근 권한도 얻게 되는 편리한 인증 시스템이다.

② 기업에서는 회원에 대한 통합관리가 가능해 마케팅을 극대화시킬 수 있다는 장점이 있다.

③ 적절한 권한관리시스템과 함께 사용할 경우, 보안성과 효율성을 갖춘 통합인증시스템으로 활용할 수 있다.

④ 해킹을 통해서 한 번의 인증과정만 통과하면, 모든 시스템에 접속할 수 있다는 단점이 존재하기 때문에 국내에는 도입되지 않고 있다.

정답 4번

출제 포인트

이 문제는 SSO의 기본 개념, 운영상 장점, 그리고 보안상 한계를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

SSO는 한 번의 인증으로 여러 연계 시스템을 다시 로그인하지 않고 이용하게 하는 통합 인증 방식이다.
권한관리는 로그인 여부와 별개로 각 시스템에서 무엇을 할 수 있는지를 통제하는 체계이므로, SSO는 권한관리와 함께 설계되어야 안전하다.
SSO의 대표적 위험은 인증정보가 탈취되면 피해 범위가 여러 시스템으로 확산될 수 있다는 점이지, 그 위험 때문에 SSO 자체가 도입되지 않는다는 뜻은 아니다.

선지별 해설

① O: SSO의 핵심은 한 번 인증한 사용자가 연계된 다른 시스템을 추가 로그인 없이 이용하게 하는 데 있다. 문장의 "하나의 시스템에서 인증을 받으면, 다른 시스템에 대한 접근 권한도 얻게 된다"는 취지는 SSO의 기본 설명에 해당한다.
② O: 기업 입장에서는 회원 계정을 통합 관리할 수 있어 사용자 관리 효율이 높아지고, 서비스 연계와 고객 분석에도 유리하다. 문장의 "통합관리가 가능해 마케팅을 극대화"한다는 설명은 SSO의 활용상 장점을 말한 것으로 볼 수 있다.
③ O: SSO는 권한관리시스템과 결합될 때 편의성과 관리 효율을 높일 수 있다. 인증 통합만 하고 권한통제가 부실하면 위험하지만, 적절한 권한관리와 함께 운영하면 통합인증체계로 활용할 수 있다는 점에서 옳다.
④ X: 틀린 부분은 "국내에는 도입되지 않고 있다"는 표현이다. SSO는 국내에서도 기업 내부 시스템, 포털, 그룹웨어, 대학, 클라우드 서비스 등에서 널리 도입되어 있다. 올바르게는 "한 번의 인증정보가 탈취되면 여러 시스템으로 피해가 확산될 수 있으므로 강한 인증과 세션 보호가 중요하다"이다.

NoteBase

오답 포인트

4번은 SSO의 실제 단점인 "단일 인증 실패 시 피해 확산 가능성"을 먼저 제시한 뒤, 마지막에 "국내에는 도입되지 않고 있다"를 붙여 문장을 틀리게 만든 선지이다. 수험생은 앞부분이 맞는 설명이라서 뒷부분의 단정이 틀렸다는 점을 놓치기 쉽다.

다시 나오면 이렇게 판단

SSO 문제는 먼저 "한 번 인증으로 여러 시스템 이용"이라는 정의가 맞는지 확인하고, 다음으로 장점은 편의성과 통합관리, 단점은 인증정보 탈취 시 피해 확산으로 정리해 판단하면 된다. 마지막에 "도입되지 않는다", "사용할 수 없다"처럼 과도하게 단정하는 표현이 붙으면 오답일 가능성이 크다.

암기 포인트

SSO는 로그인은 한 번, 이용은 여러 곳, 위험은 한 번 뚫리면 여러 곳이다.

NoteBase

문 20. <보기>에서 DoS 공격에 해당하는 것을 모두 고른 것은?

<보기>
ㄱ. Land Attack
ㄴ. 패킷 필터링
ㄷ. SMURF Attack

① ㄴ
② ㄱ, ㄴ
③ ㄱ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 3번

출제 포인트

이 문제는 DoS 공격 기법과 보안 방어 기법을 구분할 수 있는지를 묻는다.

핵심 개념

DoS 공격은 시스템 자원이나 네트워크 대역폭을 소모시켜 정상 서비스를 불가능하게 만드는 공격이다.
Land Attack은 출발지 IP와 목적지 IP, 출발지 포트와 목적지 포트를 같게 조작한 패킷으로 대상 시스템에 혼란을 주는 DoS 공격이다.
Smurf Attack은 출발지 IP를 피해자로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수의 응답이 피해자에게 집중되게 하는 DoS 공격이다.
패킷 필터링은 패킷 헤더의 주소·포트·프로토콜 정보를 기준으로 허용 또는 차단을 수행하는 방어 기술이다.

선지별 해설

1번(X): ㄴ의 패킷 필터링은 공격이 아니라 트래픽을 걸러내는 방어 기법이다. 틀린 표현은 'DoS 공격에 해당한다'이며, 올바르게는 'DoS 방어를 위해 사용할 수 있는 필터링 기술이다'이다.
2번(X): ㄱ은 Land Attack으로 DoS 공격이 맞지만, ㄴ은 패킷 필터링으로 공격이 아니다. 틀린 부분은 ㄴ을 공격 목록에 포함한 점이며, 올바르게는 'ㄱ만 해당하고 ㄴ은 해당하지 않는다'이다.
3번(O): ㄱ의 Land Attack과 ㄷ의 Smurf Attack은 모두 서비스 거부를 유발하는 대표적인 DoS 공격이다. 보기의 두 항목 모두 공격 유형이므로 옳다.
4번(X): ㄱ과 ㄷ은 DoS 공격이지만 ㄴ의 패킷 필터링은 방어 기술이다. 틀린 부분은 ㄴ까지 함께 묶은 점이며, 올바르게는 'ㄱ, ㄷ'만 고른 3번이다.

NoteBase

오답 포인트

공격 이름과 방어 기술 이름을 함께 제시해 분류를 흔드는 유형이다. 패킷 필터링은 보안 장비에서 수행하는 차단 방식이라는 점을 놓치면 2번이나 4번으로 흐르기 쉽다.

다시 나오면 이렇게 판단

각 보기 항목을 먼저 '공격 기법인지, 방어 기법인지'로 분류한 뒤 답지를 고르면 된다. 공격을 묻는 문제에서 필터링, 차단, 탐지 같은 용어가 보이면 우선 방어 기술인지부터 확인한다.

암기 포인트

Land와 Smurf는 DoS 공격이고, 패킷 필터링은 DoS 대응 기술이다.

NoteBase