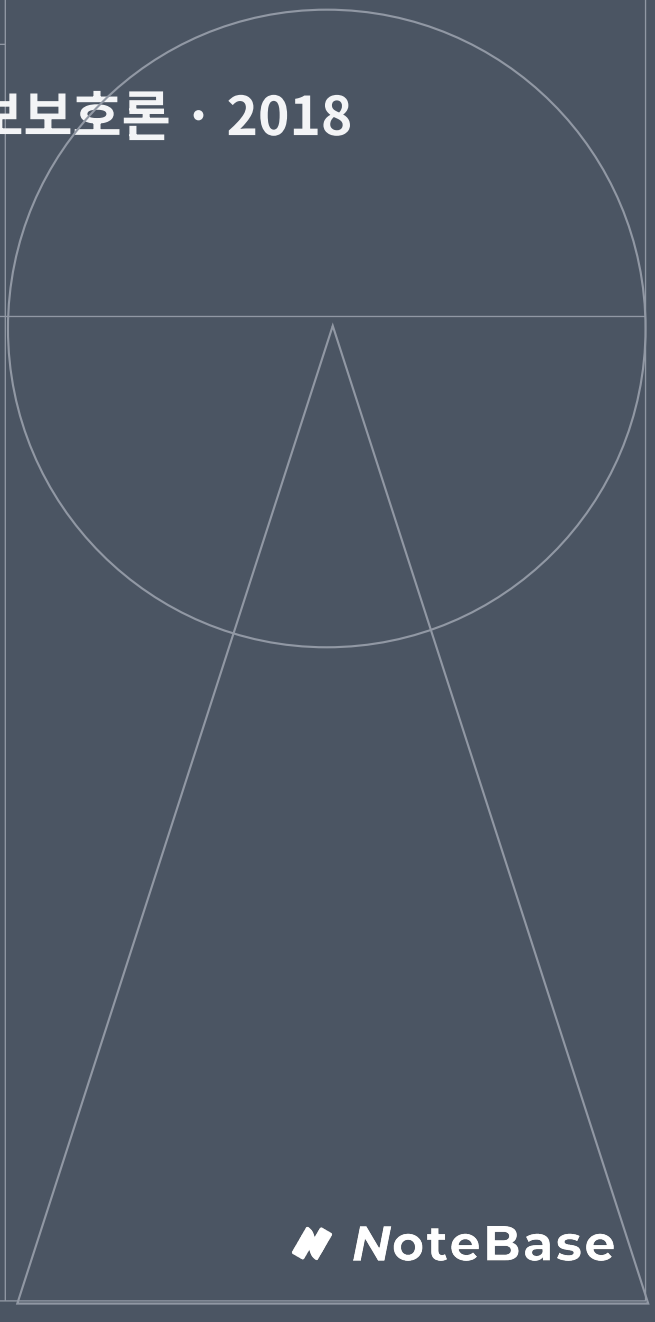
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2018



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2018

공무원/경찰/경력채용 · 정보보호론 · 2018

문 1. 정보보호의 주요 목적(3원칙)으로 가장 적절하지 않은 것은?

① 무결성(Integrity)

② 기밀성(Confidentiality)

③ 신뢰성(Reliability)

④ 가용성(Availability)

정답 3번

간단한 해설

신뢰성은 시스템의 일관된 기능 수행과 관련되지만, 통상적인 **정보보호의 3원칙에는 포함되지 않는다**. 3원칙은 기밀성·무결성·가용성이다.

개념 구분

무결성(Integrity): 정보가 **허가 없이 변경되거나 훼손되지 않도록** 하여 정확성과 완전성을 유지하는 성질이다. 정보보호의 3원칙에 포함된다.

기밀성(Confidentiality): 정보가 **인가되지 않은 대상에게 공개되지 않도록** 하는 성질이다. 접근 권한이 없는 사람이 정보를 열람하거나 유출하는 것을 막으며, 정보보호의 3원칙에 포함된다.

신뢰성(Reliability): 시스템이 의도한 기능을 일관되게 수행하는 성질이다. 정보보호와 관련된 속성일 수 있지만, 통상적인 **정보보호의 3원칙에는 포함되지 않는다**.

가용성(Availability): 인가된 사용자가 **필요할 때 정보와 서비스를 이용할 수 있도록** 하는 성질이다. 장애나 서비스 거부로 이용이 중단되는 것을 막으며, 정보보호의 3원칙에 포함된다.

정보보호의 3원칙은 기밀성·무결성·가용성이므로, 이에 해당하지 않는 신뢰성을 제시한 ③이 발문의 요구에 맞는다.

NoteBase

문 2. OECD 개인정보보호 8개 원칙 중 개인정보의 유출, 권한, 접근금지 등 합리적인 보안장치 설정과 개인정보의 물리적·조직적·기술적 안전 조치 확보와 관련한 원칙으로 가장 적절한 것은?

① 수집제한의 원칙(Collection Limitation Principle)

② 목적명시의 원칙(Purpose Specification Principle)

③ 이용제한의 원칙(Use Limitation Principle)

④ 안전성 확보의 원칙(Security Safeguards Principle)

정답 4번

간단한 해설

개인정보의 유출이나 무단 접근 같은 위험에 대비하여 **합리적인 보안조치로 보호**하는 것이 안전성 확보의 원칙이다. 물리적·조직적·기술적 안전 조치를 마련한다는 설명이 이 원칙을 가리킨다.

개념 구분

수집제한의 원칙: 개인정보의 수집 범위를 제한하고 적법하고 공정한 방법으로 수집하며, 적절한 경우 정보주체의 인지나 동의를 얻도록 한다. **수집 단계의 범위와 방법**에 관한 원칙이다.

목적명시의 원칙: 개인정보를 수집하는 목적을 **늦어도 수집 시점까지 명시**하고, 이후에는 그 목적이나 그 목적과 양립하면서 변경 시 명시한 목적에 맞게 이용하도록 한다.

이용제한의 원칙: 정보주체의 동의나 법적 근거가 있는 경우를 제외하고, 명시된 목적 외로 개인정보를 공개·제공·이용하지 않도록 한다. **수집 후 목적 외 이용을 제한**하는 원칙이다.

안전성 확보의 원칙: 개인정보의 분실, 무단 접근, 파괴, 부정 이용, 변경, 유출 등의 위험에 대비하여 **합리적인 보안조치로 개인정보를 보호**하도록 한다. 문제에서 제시한 보안장치 설정과 물리적·조직적·기술적 안전 조치 확보가 여기에 해당한다.

따라서 문제의 설명에 해당하는 것은 ④ 안전성 확보의 원칙이다.

NoteBase

문 3. 사용자 인증 방법 중에서 신분증, 주민등록증 등을 이용하여 인증하는 방법으로 가장 적절한 것은?

① 지식 기반 인증(What you know)

② 소유 기반 인증(What you have)

③ 커버로스 인증(Kerberos)

④ 생체 기반 인증(What you are)

정답 2번

간단한 해설

신분증과 주민등록증을 제시하는 방법은 사용자가 **소유한 증표**를 이용하는 인증이다. 알고 있는 비밀정보나 신체적 특징을 기준으로 하는 인증과 구별된다.

개념 구분

지식 기반 인증: 비밀번호나 PIN처럼 **사용자가 알고 있는 정보**를 확인한다. 신분증이라는 물건을 제시하는 것은 지식 기반 인증의 분류 기준에 해당하지 않는다.

소유 기반 인증: 신분증, 출입증, 보안 토큰처럼 **사용자가 가지고 있는 물건**을 이용한다. 이 문제의 신분증과 주민등록증은 소지한 증표를 제시한다는 점에서 소유 기반 인증으로 분류한다.

커버로스 인증: 신뢰하는 인증 서버가 발급한 **티켓을 이용하는 네트워크 인증 프로토콜**이다. 신분증을 소지·제시하는 인증 요인의 명칭을 묻는 이 문제와 구별된다.

생체 기반 인증: 지문, 홍채, 얼굴처럼 **사용자의 신체적 특징**을 이용한다. 신분증이라는 증표의 소유와 신체적 특징의 확인은 구별해야 한다.

따라서 신분증과 주민등록증을 이용하는 인증은 ② 소유 기반 인증에 해당한다.

NoteBase

문 4. 각 주체가 각 객체에 접근할 때마다 관리자에 의해 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 주체에게만 접근 권한을 부여하는 접근 통제 정책으로 가장 적절한 것은?

① 강제적 접근 통제(Mandatory Access Control)

② 임의적 접근 통제(Discretionary Access Control)

③ 역할기반 접근 통제(Role Based Access Control)

④ 최소 권한 정책(Least Privilege Policy)

정답 1번

간단한 해설

관리자가 사전에 정한 규칙을 시스템이 강제하고, 그 규칙을 충족한 주체에게만 접근을 허용하는 방식은 **강제적 접근 통제(MAC)**이다. 객체 소유자의 재량보다 **중앙에서 정한 보안 정책**이 접근 허용 여부를 결정한다.

개념 구분

강제적 접근 통제(MAC): 중앙 관리자가 정한 보안 정책을 시스템이 강제하여 주체의 객체 접근을 허용하거나 거부한다. 주체는 접근을 요청하는 사용자·프로세스이고, 객체는 파일 같은 접근 대상이다. 문제의 '관리자에 의해 사전에 규정된 규칙'을 매번 적용한다는 단서는 **소유자나 사용자가 임의로 바꿀 수 없는 정책**에 따른 통제를 가리킨다. 대표적으로 주체의 보안 인가와 객체의 보안 등급을 비교한다.

임의적 접근 통제(DAC): **객체의 소유자 등 권한을 가진 주체가 재량으로** 접근 대상자와 허용 권한을 정한다. 관리자가 사전에 정한 정책을 일반 사용자가 변경할 수 없도록 강제하는 방식과 구별된다.

역할기반 접근 통제(RBAC): 권한을 조직의 직무에 따른 역할에 부여하고, 사용자에게 역할을 할당하여 접근을 통제한다. 판단의 핵심은 **사용자가 맡은 역할에 연결된 권한**이다. 문제에는 역할의 할당이나 직무에 따른 권한 묶음이 제시되어 있지 않다.

최소 권한 정책: 사용자나 프로세스에 **업무 수행에 필요한 최소한의 권한만** 부여한다는 원칙이다. 권한의 범위를 제한하는 원칙이므로, 문제에서 설명한 접근 통제 방식의 명칭에 해당하지 않는다.

따라서 제시된 설명에 가장 적절한 정책은 ① 강제적 접근 통제이다.

NoteBase

문 5. 정보의 안전한 정도를 평가하는 TCSEC(Trusted Computer System Evaluation Criteria)의 보안등급 중에서 “검증된 설계(Verified Design)”를 의미하는 보안등급으로 가장 적절한 것은?

① A등급

② B등급

③ C등급

④ D등급

정답 1번

간단한 해설

TCSEC에서 '검증된 설계(Verified Design)'는 **A등급에 속하는 A1**의 명칭이다. A1은 형식적 설계 명세와 검증을 통해 보안 구현의 신뢰성을 높인다.

개념 구분

A등급: '검증된 보호'에 해당하며, 이 범주에 속하는 **A1의 명칭이 '검증된 설계(Verified Design)'**이다. A1은 B3와 보안 기능 면에서는 동등하지만, 형식적 설계 명세와 검증 기법을 통해 보안 기능이 올바르게 구현되었다는 보증을 강화한다.

B등급: **강제적 보호**에 해당한다. 주체와 객체의 보안등급 등을 바탕으로 강제적 접근통제를 수행하며, B1·B2·B3으로 구분된다. 따라서 '검증된 설계'라는 등급 명칭에 해당하지 않는다.

C등급: **임의적 보호**에 해당한다. 사용자나 사용자 그룹의 신원과 접근 권한을 바탕으로 임의적 접근통제를 제공하며, C1·C2로 구분된다. 형식적 설계 검증을 특징으로 하는 A1과 구별된다.

D등급: '최소한의 보호'에 해당한다. 평가를 받았으나 **더 높은 등급의 요구사항을 충족하지 못한** 시스템을 분류하는 범주이다.

'검증된 설계'는 A등급의 A1을 뜻하므로 제시된 선택지 중 ① A등급에 대응한다.

NoteBase

문 6. 윈도우즈(Windows) 운영체제에서 지원하는 네트워크 관련 명령어와 주요 기능에 대한 설명으로 가장 적절하지 않은 것은?

① route : 라우팅 테이블의 정보 확인

② netstat : 연결 포트 등의 네트워크 상태 정보 확인

③ nslookup : 사용자 계정 정보 확인

④ ipconfig : 컴퓨터에 설치되어 있는 랜 카드에 대한 구성 상태를 확인

정답 3번

간단한 해설

nslookup은 **DNS 이름·주소 정보를 조회**하는 명령어이다. 사용자 계정 정보를 확인하는 기능으로 설명한 부분이 잘못됐다.

선지별 해설

① O: route는 로컬 IP 라우팅 테이블의 경로 정보를 확인하거나 변경하는 명령어이다. **route print**를 사용하면 목적지 네트워크, 게이트웨이, 인터페이스 등의 경로 정보를 확인할 수 있다.

② O: netstat는 활성 TCP 연결, 수신 대기 포트, 프로토콜 통계 등 **네트워크 연결 상태**를 확인하는 명령어이다. 예를 들어 netstat -a는 활성 TCP 연결과 TCP·UDP 수신 대기 포트를 표시한다.

③ X: nslookup은 사용자 계정 정보가 아니라 **DNS 서버에 질의하여 도메인 이름과 IP 주소 등의 정보**를 확인하는 명령어이다. 따라서 '사용자 계정 정보 확인'을 'DNS 이름·주소 정보 조회'로 고쳐야 한다.

④ O: ipconfig는 네트워크 어댑터의 **TCP/IP 구성 상태**를 확인하는 명령어이다. 기본 실행으로 IP 주소, 서브넷 마스크, 기본 게이트웨이 등을 표시하고, ipconfig /all로 더 자세한 구성을 확인할 수 있다.

NoteBase

문 7. 다음 중 블록 암호 알고리즘으로 가장 적절하지 않은 것은?

① RC5

② RC4

③ Blowfish

④ SEED

정답 2번

간단한 해설

RC4는 키 스트림을 평문과 결합하여 암호화하는 **스트림 암호**이다. 일정 길이의 블록을 변환하는 블록 암호로 분류하지 않는다.

개념 구분

블록 암호는 평문을 정해진 길이의 블록으로 나누어 암호화한다. 스트림 암호는 키 스트림을 생성하고 평문과 결합하여 순차적으로 암호화한다.

RC5: **블록 암호**이다. 블록 크기, 키 길이, 라운드 수를 매개변수로 정하며, 선택한 설정에서 일정한 크기의 평문 블록을 암호문 블록으로 변환한다.

RC4: **스트림 암호**이다. 생성한 키 스트림을 평문과 XOR하여 암호화하므로 블록 암호로 분류하지 않는다. 이름이 비슷한 RC5와 암호 처리 방식이 다르다.

Blowfish: **64비트 블록**을 처리하는 대칭키 블록 암호이다. 입력을 두 부분으로 나누어 라운드 연산을 반복하는 Feistel 구조를 사용한다.

SEED: **128비트 블록**을 처리하는 대칭키 블록 암호이다. 128비트 키와 16라운드 Feistel 구조를 사용한다.

따라서 블록 암호에 해당하지 않는 알고리즘은 ② RC4이다.

NoteBase

문 8. 다음 중 CFB(Cipher-FeedBack mode)의 복호화 수식으로 가장 적절한 것은? (단, P_i: i번째 평문, C_i: i번째 암호문, $E_K(P_i)$: 암호화, $D_K(C_i)$: 복호화)

① $P_i = D_K(C_i)$

② $P_i = D_K(C_i) \oplus C_{i-1}$

③ $P_i = C_i \oplus E_K(C_{i-1})$

④ $P_i = D_K(C_i \oplus C_{i-1})$

정답 3번

간단한 해설

CFB는 **복호화에도 암호화 함수**를 사용한다. 이전 암호문을 암호화한 출력과 현재 암호문을 XOR하면 평문이 복원되므로, 복호화식은 $P_i = C_i \oplus E_K(C_{i-1})$이다.

핵심 풀이

CFB는 이전 암호문을 암호화 함수의 입력으로 되먹임하여 만든 출력과 데이터를 XOR하는 방식이다. 이 문항은 이전 암호문 블록 전체를 되먹임하는 형태이며, 첫 블록에서는 $C_0 = IV$로 두어 초기화 벡터를 사용한다.

CFB의 암호화는 $C_i = P_i \oplus E_K(C_{i-1})$이다. XOR은 같은 값을 두 번 적용하면 원래 값으로 돌아오므로, 양변에 $E_K(C_{i-1})$를 XOR하면 $P_i = C_i \oplus E_K(C_{i-1})$를 얻는다. 따라서 **복호화할 때에도 암호화 함수**를 사용하며, 현재 암호문과 이전 암호문을 암호화한 출력을 XOR한다.

①의 $P_i = D_K(C_i)$는 각 암호문 블록을 독립적으로 복호화하는 ECB의 식이다. 이전 암호문을 되먹임하는 과정이 없어 CFB의 복호화식이 아니다.

②의 $P_i = D_K(C_i) \oplus C_{i-1}$는 CBC의 복호화식이다. CBC는 현재 암호문을 먼저 복호화한 뒤 이전 암호문과 XOR하지만, CFB는 **이전 암호문을 암호화한 출력**을 현재 암호문과 XOR한다.

④의 $P_i = D_K(C_i \oplus C_{i-1})$는 XOR 결과를 복호화 함수에 넣으므로 CFB의 처리 구조와 다르다. CFB에서는 복호화 함수 안에서 XOR하는 것이 아니라, 암호화 함수의 출력을 얻은 뒤 현재 암호문과 XOR해야 한다.

도출한 복호화식 $P_i = C_i \oplus E_K(C_{i-1})$는 ③과 일치한다.

NoteBase

문 9. 사용자 A와 B가 Diffie-Hellman 키 교환 알고리즘을 이용하여 비밀키를 공유하고자 한다. A는 3을, B는 2를 각각의 개인 키로 선택하고, A는 B에게 $21(=7^3 \bmod 23)$을, B는 A에게 $3(=7^2 \bmod 23)$을 전송한다면, A와 B가 공유하게 되는 비밀키 값으로 가장 적절한 것은?(단, 사용자 A와 B는 소수 23과 그 소수의 원시근 7을 공유하여 사용한다.)

① 3

② 4

③ 5

④ 6

정답 2번

간단한 해설

상대방의 공개값에 자신의 개인 키를 지수로 적용하고 23으로 나눈 나머지를 구한다. A는 3^323=4, B는 21^223=4를 얻으므로 같은 비밀키를 공유한다.

계산 과정

주어진 값은 공통 소수 p = 23, 원시근 g = 7, A의 개인 키 a = 3, B의 개인 키 b = 2이다. A가 보낸 공개값은 21이고 B가 보낸 공개값은 3이다. 구할 값은 두 사용자가 각각 계산하여 얻는 공통 비밀값 K이다.

Diffie-Hellman에서는 **상대방에게 받은 공개값을 자신의 개인 키만큼 거듭제곱**한 뒤 p로 나눈 나머지를 구한다. 공개값을 각각 Y_A=g^a p, Y_B=g^b p라고 하면 두 사람의 계산은 K=Y_B^a p=Y_A^b p=g^ab p로 같은 값이 된다.

A는 B에게 받은 3에 자신의 개인 키 3을 적용한다. K=3^323=2723=4이다. 27 = 23 × 1 + 4이므로 나머지는 4이다.

B는 A에게 받은 21에 자신의 개인 키 2를 적용한다. K=21^223=44123=4이다. 441 = 23 × 19 + 4이므로 A와 같은 값을 얻는다.

두 사용자가 공유하는 비밀키 값은 4이므로 ②와 일치한다.

NoteBase

문 10. 다음 중 공개키 암호 알고리즘에 대한 설명으로 가장 적절한 것은?

① ElGamal은 소인수 분해의 어려움을 이용한다.

② Diffie-Hellman의 알고리즘은 이산대수의 어려움을 이용한다.

③ RSA는 정보의 비밀성 보장을 위한 암호화에만 사용된다.

④ Rabin 암호 알고리즘은 이산대수의 어려움을 이용한다.

정답 2번

간단한 해설

Diffie-Hellman은 **이산대수의 어려움**을 이용해 공개된 통신 경로에서도 두 참여자가 공유 비밀값을 합의하도록 하는 방식이다.

선지별 해설

① X: ElGamal은 **이산대수의 어려움**을 이용하는 공개키 암호 방식이다. 유한한 수학적 구조에서 거듭제곱의 결과를 구하는 것은 쉽지만, 그 결과로부터 비밀 지수를 역으로 알아내기는 어렵다는 성질을 이용하므로 '소인수 분해'를 '이산대수'로 고쳐야 한다.

② O: Diffie-Hellman은 **이산대수를 구하기 어려운 구조**를 이용하는 키 합의 방식이다. 두 참여자는 각자의 비밀값을 공개하지 않고 계산 결과를 교환하여 같은 공유 비밀값을 얻는다. 도청자가 공개된 계산 결과에서 비밀 지수를 쉽게 역산할 수 없도록 하는 것이 핵심이다.

③ X: RSA는 비밀성을 위한 암호화뿐 아니라 **전자서명에도 사용된다**. 암호화에서는 수신자의 공개키로 암호화하고 수신자의 개인키로 복호화한다. 전자서명에서는 서명자의 개인키로 서명을 생성하고 그 공개키로 검증하므로, 사용 목적을 암호화에만 한정할 수 없다.

④ X: Rabin 암호 알고리즘은 **큰 합성수의 소인수 분해가 어렵다는 성질**을 이용한다. 두 큰 소수의 곱을 공개하고 그 소인수를 비밀로 유지하며, 합성수를 법으로 한 제곱 연산을 역으로 푸는 문제를 이용한다. 따라서 '이산대수'를 '소인수 분해'로 고쳐야 한다.

따라서 공개키 알고리즘의 수학적 기반을 적절하게 설명한 선지는 ②이다.

NoteBase

문 11. 암호학적 해시 함수가 가져야 할 특성으로 가장 적절하지 않은 것은?

① 서로 다른 두 입력 메시지에 대해 같은 해시 값이 나올 가능성은 있으나, 계산적으로 같은 해시 값을 갖는 서로 다른 두 입력 메시지를 찾는 것은 불가능해야 한다.

② 해시 값을 이용하여 원래의 입력 메시지를 찾는 것은 계산상으로 불가능해야 한다.

③ 입력 메시지의 길이에 따라 출력되는 해시 값의 길이는 비례해야 한다.

④ 입력 메시지와 그 해시 값이 주어졌을 때, 이와 동일한 해시 값을 갖는 다른 메시지를 찾는 것은 계산상으로 불가능해야 한다.

정답 3번

간단한 해설

암호학적 해시 함수의 출력 길이는 **입력 메시지 길이에 비례하지 않고 고정**된다. 입력이 길어져도 같은 해시 함수를 사용하면 출력 비트 수는 일정하다.

선지별 해설

① O: '충돌 저항성'에 관한 설명이다. 서로 다른 입력이 같은 해시 값을 갖는 충돌은 존재할 수 있지만, 공격자가 **충돌하는 임의의 두 입력**을 찾아내는 것은 계산적으로 어려워야 한다. 충돌 저항성은 충돌이 전혀 존재하지 않는다는 뜻이 아니다.

② O: '역상 저항성' 또는 '일방향성'에 관한 설명이다. **주어진 해시 값으로부터 그 값을 만드는 입력**을 찾아내는 것이 계산적으로 어려워야 한다. 해시 값만으로 원래 메시지를 쉽게 복원할 수 없어야 한다는 취지이다.

③ X: 일반적인 암호학적 해시 함수의 출력 길이는 입력 메시지의 길이에 비례하지 않고, **사용하는 해시 함수에 따라 고정**된다. 입력이 길어지더라도 같은 해시 함수를 사용하면 출력 비트 수가 함께 늘어나는 것은 아니다.

④ O: '제2역상 저항성'에 관한 설명이다. **특정 입력 메시지가 먼저 주어진 상태**에서 그 메시지와 같은 해시 값을 갖는 다른 메시지를 찾는 것이 계산적으로 어려워야 한다. 어떤 두 입력이든 찾아도 되는 ①의 충돌 저항성과 구별된다.

NoteBase

문 12. 다음 중 TCP/IP 프로토콜 계층과 각 계층에서 구현되는 보안 기술의 연결이 가장 적절한 것은?

① 응용 계층 - Kerberos

② 전송 계층 - IPSec

③ 네트워크 계층 - SSL/TLS

④ 데이터링크 계층 - SET

정답 1번

간단한 해설

Kerberos는 티켓을 이용해 응용 서비스의 이용자를 인증하는 **응용 계층 보안 기술**이다. 네트워크의 패킷이나 링크의 프레임 자체를 보호하는 기술과 구별된다.

선지별 해설

① O: Kerberos는 신뢰하는 인증 서버가 발급한 티켓을 이용하여 **사용자와 응용 서비스 사이의 인증**을 제공한다. TCP 또는 UDP를 통해 인증 메시지를 주고받는 응용 계층 보안 기술이므로 연결이 맞다.

② X: IPsec은 **네트워크 계층의 IP 패킷**을 보호하는 보안 기술이다. AH와 ESP 등을 사용하여 인증·무결성 또는 기밀성 서비스를 제공한다. 전송 모드라는 운영 방식이 있어도 전송 계층의 프로토콜로 바뀌는 것은 아니므로, 네트워크 계층과 연결해야 한다.

③ X: SSL/TLS는 **TCP 위에서 응용 데이터를 보호**하는 보안 프로토콜이다. 계층별 보안 기술의 일반적인 분류에서는 전송 계층 보안으로 다루며, 네트워크 계층에서 IP 패킷을 직접 보호하는 IPsec과 구별된다.

④ X: SET는 인터넷상의 카드 결제에서 거래 정보의 기밀성·무결성과 거래 참여자의 인증을 제공하는 **응용 계층의 전자결제 보안 기술**이다. 데이터링크 계층의 프레임을 보호하는 기술이 아니므로, 응용 계층과 연결해야 한다.

따라서 계층과 보안 기술의 연결이 적절한 것은 ①이다.

NoteBase

문 13. 다음 중 TCP와 UDP에 대한 설명으로 가장 적절하지 않은 것은?

① 서비스: 신뢰성, TCP: 패킷이 그들의 목적지에 도달했는지 확인하며, 패킷이 도달할 때, ACK를 수신하기 때문에, 신뢰성 있는 프로토콜이다., UDP: 패킷이 목적지에 도달되는 것을 보장하지 않기 때문에, 신뢰성이 없는 프로토콜이다.

② 서비스: 패킷 순서, TCP: 패킷 내에 순서번호를 사용하지 않는다., UDP: 패킷 내에 순서번호를 사용하여, 각 패킷들이 순차적으로 수신되도록 한다.

③ 서비스: 혼잡 제어, TCP: 목적지 컴퓨터는 데이터의 처리가 어렵거나, 전송속도가 느려질 경우 이를 송신지 컴퓨터에 통보한다., UDP: 목적지 컴퓨터는 송신지 컴퓨터로 흐름제어에 대한 통보를 하지 않는다.

④ 서비스: 속도, TCP: UDP보다 느리다., UDP: TCP보다 빠르다.

정답 2번

간단한 해설

순서번호로 수신 데이터의 순서를 복원하는 것은 TCP이다. UDP 자체에는 순서번호를 이용한 순서 보장 기능이 없으므로, 두 프로토콜의 기능을 바꾸어 설명한 부분이 핵심 오류이다.

NoteBase

선지별 해설

① O: TCP는 순서번호와 확인응답(ACK), 필요한 재전송을 이용하여 수신 측에 신뢰성 있게 데이터를 전달한다. UDP 자체에는 이런 확인응답·재전송 절차가 없어 **전달 성공을 보장하지 않는다**.

② X: 두 프로토콜의 기능을 반대로 설명했다. **TCP가 순서번호를 사용**하여 수신 데이터를 원래 순서로 재조립하고 응용프로그램에 순서대로 전달한다. UDP 헤더에는 순서번호가 없으며, UDP 자체는 데이터그램의 도착 순서를 보장하지 않는다.

③ X: 서비스 표제의 '혼잡 제어'는 본문에 적힌 기능과 일치하지 않는다. 수신 컴퓨터의 처리능력에 맞춰 송신량을 조절하는 것은 **흐름 제어**이다. TCP는 수신자가 광고하는 수신 윈도를 이용해 이를 수행하고 UDP 자체에는 같은 기능이 없다는 대비는 맞다. 혼잡 제어는 수신자 처리능력이 아니라 네트워크의 혼잡에 맞춰 전송량을 조절하므로, 이 설명의 표제는 '흐름 제어'로 구별해야 한다.

④ O: 신뢰성 보장에 필요한 처리 부담을 비교하는 일반적인 설명이다. TCP에는 연결 설정, 확인응답, 재전송 등의 절차가 있지만 UDP는 이를 기본적으로 제공하지 않아 **프로토콜 처리 부담이 작다**. 다만 실제 전송 속도는 통신 환경과 구현에 따라 달라지므로 UDP가 모든 상황에서 더 빠르다는 보장은 아니다.

③에는 제어 기능의 명칭을 혼동한 표현이 있지만 TCP와 UDP의 흐름 제어 기능 대비 자체는 맞다. 반면 ②는 순서번호 사용과 순서 보장 기능을 완전히 반대로 연결했으므로, '가장 적절하지 않은' 것을 고르는 이 문항의 인정 정답은 ②이다.

NoteBase

문 14. 다음은 SSL 프로토콜에 대한 내용이다. 이에 대해 가장 적절한 것은?

상위계층에서 수신된 메시지를 전달하는 역할을 담당
데이터 분할, 압축, 메시지 인증 및 암호화 기능을 수행

① Alert Protocol
② Handshake Protocol
③ Record Protocol
④ Change Cipher Spec Protocol

정답 3번

간단한 해설

SSL에서 상위계층 메시지를 분할하고 압축·메시지 인증·암호화를 거쳐 전달하는 것은 **Record Protocol**이다. 보안 매개변수를 협상하는 절차와 실제 메시지를 보호하여 운반하는 기능을 구별한다.

핵심 풀이

Record Protocol은 상위계층의 메시지를 받아 **분할 → 압축 → 메시지 인증 코드(MAC) 부가 → 암호화**를 거쳐 전송한다. 분할은 데이터를 처리 가능한 크기로 나누고, MAC은 메시지의 무결성과 인증을, 암호화는 기밀성을 제공한다. 압축은 협상된 방식에 따르며 압축하지 않는 방식도 가능하다. 수신 측은 역순으로 복호화·MAC 검증·압축 해제·재조립한다.

Alert Protocol은 **오류·경고나 연결 종료**를 상대방에게 알린다. 실제 데이터 보호 처리를 담당하는 계층과 구별된다.

Handshake Protocol은 통신 상대의 인증, 암호 알고리즘의 협상, 키 설정을 수행하여 **통신에 사용할 보안 매개변수**를 정한다.

Change Cipher Spec Protocol은 이후의 레코드부터 **협상한 암호 명세와 키를 적용**함을 알린다. 알고리즘 자체를 협상하는 Handshake와도 구별된다.

따라서 지문에 제시된 메시지 전달과 보호 기능을 담당하는 것은 ③ Record Protocol이다.

NoteBase

문 15. ㉠, ㉡, ㉢에 들어갈 내용이 바르게 연결된 것은?

(㉠)은(는) 메시지 압축과 변조된 종단 간 연결로를 제공하고, 인증서를 이용해 서버와 클라이언트의 인증을 하는데 사용된다.
(㉡)은(는) 인터넷과 같은 공개된 통신망에서 전자상거래를 하기 위한 “지불시스템에 대한 기술표준”으로 S/W와 H/W를 포함한다.
(㉢)은(는) 인터넷상에서 VPN(Virtual Private Network)을 구현하는데 사용될 수 있도록 개발된 Protocol이다.

① ㉠: SSL, ㉡: SET, ㉢: IPSec
② ㉠: SET, ㉡: SSL, ㉢: IPSec
③ ㉠: SET, ㉡: IPSec, ㉢: SSL
④ ㉠: SSL, ㉡: IPSec, ㉢: SET

정답 1번

간단한 해설

인증서 기반 통신 상대 인증은 **SSL**, 전자상거래 지불 표준은 **SET**, IP 계층의 VPN 보호는 **IPSec**에 연결된다. 원문의 '변조된 종단 간 연결로'는 SSL 기능에 맞지 않는 표현이며, SSL은 변조를 탐지하여 통신을 보호한다.

빈칸별 해설

㉠: SSL이다. **인증서를 이용한 서버·클라이언트 인증**이 SSL을 가리키는 단서이다. SSL은 핸드셰이크에서 인증과 암호화 방식 등을 협상하고, 레코드 처리에서 압축을 선택적으로 수행하며 암호화와 메시지 무결성 검사를 통해 통신을 보호한다. 클라이언트 인증서 인증은 선택적으로 수행될 수 있다. 다만 원문의 '변조된 종단 간 연결로를 제공'라는 표현은 SSL의 기능에 맞지 않는다. SSL이 제공하려는 것은 **변조를 탐지하고 통신을 보호하는 기능**이며, 변조된 연결 자체를 제공하는 것이 아니다.

㉡: SET이다. SET은 공개된 통신망에서 이루어지는 전자상거래의 **안전한 카드 결제**를 위한 기술 규격이다. 카드 소지자·가맹점·결제 게이트웨이 등이 결제 정보를 안전하게 주고받도록 하는 데 초점이 있으므로, 지문의 '지불시스템에 대한 기술표준'과 연결된다.

㉢: IPSec이다. IPSec은 **IP 계층에서 패킷을 보호**하는 프로토콜 체계이다. 인증·무결성·기밀성 등의 보안 서비스를 제공하고, 터널 모드 등을 이용해 공중망을 통과하는 사설망 통신을 보호하므로 VPN 구현에 사용된다.

인증서 기반 인증, 전자상거래 지불 표준, VPN이라는 단서를 각각 연결하면 ㉠ SSL, ㉡ SET, ㉢ IPSec이며, 이 조합은 ①에 해당한다.

NoteBase

문 16. 다음 중 PGP(Pretty Good Privacy)에 대한 설명으로 가장 적절하지 않은 것은?

① E-mail의 보안과 파일 암호화에 사용된다.

② 전자 서명, 기밀성, 압축, 단편화와 재조립 등의 기능이 있다.

③ E-mail 응용 프로그램에 플러그인도 가능하다.

④ 자신의 공개키를 전달하려면 인증기관의 서명이 필요하다.

정답 4번

간단한 해설

PGP는 사용자 간의 키 인증과 신뢰 관계를 활용하는 '신뢰망' 방식을 사용할 수 있으므로, 공개키 전달에 **인증기관의 서명이 반드시 필요한 것은 아니다**.

선지별 해설

① O: PGP는 **전자우편과 파일의 암호화·전자 서명**에 활용된다. 메시지 내용을 암호화하여 제3자의 열람을 막거나, 전자 서명으로 서명자와 내용의 무결성을 확인할 수 있다.

② O: 전자 서명은 서명자 확인과 변경 탐지에, 암호화는 기밀성 보호에 쓰인다. 또한 메시지 압축과 **긴 메시지를 여러 부분으로 나누어 전송한 뒤 재조립**하는 기능을 지원하므로 열거한 기능들이 PGP의 설명에 해당한다.

③ O: PGP 기능을 전자우편 프로그램에 **플러그인 형태로 연동**할 수 있다. 이를 통해 메일 프로그램 안에서 암호화·복호화 및 전자 서명·검증을 수행할 수 있다.

④ X: PGP에서 공개키를 전달하는 데 **인증기관의 서명이 반드시 필요한 것은 아니다**. 전통적인 PGP는 사용자가 공개키의 지문을 직접 확인하거나 다른 사용자의 키 인증 서명과 신뢰 관계를 이용하는 '신뢰망' 방식을 사용할 수 있다. 중앙 인증기관의 인증서가 필수인 방식으로 설명하면 안 된다.

NoteBase

문 17. 다음 설명에 해당하는 블루투스(Bluetooth) 공격 방법으로 가장 적절한 것은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격 방법은 블루투스 장치끼리 인증없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여, 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나, 취약한 장치의 파일에 접근하는 공격 방법이다.

① 블루스나프(BlueSnarf)
② 블루프린팅(BluePrinting)
③ 블루버그(BlueBug)
④ 블루재킹(BlueJacking)

정답 1번

간단한 해설

OPP의 취약한 구현을 악용해 **주소록·달력 같은 저장 정보를 무단으로 열람**하는 것은 블루스나프의 특징이다. 메시지를 보내거나 장치의 명령 기능을 제어하는 공격과 구별된다.

핵심 풀이

블루스나프: 블루투스의 객체 교환 기능을 잘못 구현한 장치에서 **주소록·달력 등의 데이터를 무단으로 읽어 오는 공격**이다. 제시문의 OPP 기능과 파일 접근은 이 공격의 단서이다. OPP가 인증 없이 객체 교환을 허용한다는 사실만으로 항상 취약한 것은 아니며, 장치가 허용되지 않은 파일 요청까지 받아들이는 구현상 취약점이 악용된다.

블루프린팅: 장치가 공개하는 주소나 서비스 정보 등의 특징을 조합하여 **제조사·모델·펌웨어 등의 정보를 식별**하는 기법이다. 취약한 장치를 찾는 사전 정보 수집에 활용할 수 있지만, 제시문처럼 저장된 주소록과 달력을 가져오는 행위 자체를 뜻하지 않는다.

블루버그: 취약한 블루투스 장치의 명령 기능에 접근하여 **통화·메시지 전송 등 장치 기능을 무단으로 제어**하는 공격이다. 데이터 접근이 수반될 수 있지만, 제시문은 명령 제어보다 객체 교환 기능을 통한 파일 열람을 설명한다.

블루재킹: 주변 블루투스 장치에 **원하지 않는 메시지나 명함을 보내는** 행위이다. 정보를 상대 장치로 보내는 점에서, 상대 장치의 저장 정보를 빼내는 블루스나프와 구별된다.

따라서 제시문에 해당하는 공격 방법은 ① 블루스나프이다.

NoteBase

문 18. 다음 설명에 해당하는 공격 방법으로 가장 적절한 것은?

웹 사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로, 사용자로 위장한 공격자가 웹 사이트에 프로그램 코드를 삽입하여, 나중에 이 사이트를 방문하는 다른 사용자의 웹 브라우저에서 해당 코드가 실행되도록 한다.

① 세션 탈취(Session Hijacking)
② 제로 데이(Zero-Day) 공격
③ 패킷 스니핑(Packet Sniffing) 공격
④ XSS(Cross-Site Scripting)

정답 4번

간단한 해설

웹 사이트에 삽입한 코드가 **다른 사용자의 웹 브라우저에서 실행**되도록 하는 공격은 XSS이다. 코드를 사이트에 남겨 두고 이후 방문자에게 실행시키는 설명은 **저장형 XSS**에 해당한다.

핵심 풀이

XSS는 웹 페이지에 삽입된 악성 스크립트가 **다른 사용자의 브라우저에서 실행**되게 하는 공격이다. 지문에서는 검증이 불충분한 입력에 코드가 포함되고, 그 내용이 나중에 방문한 사용자에게 전달되어 실행된다. 특히 사이트에 삽입해 둔 코드가 후속 방문자에게 실행되는 흐름은 **저장형 XSS**의 전형적인 형태이다.

세션 탈취는 이미 성립한 정상 사용자의 세션을 가로채 그 사용자로 가장하는 공격이다. XSS가 세션 탈취의 수단이 될 수는 있지만, 지문은 세션을 넘겨받는 결과보다 **웹 페이지에 코드를 삽입하여 브라우저에서 실행**시키는 방법을 직접 설명한다.

제로 데이 공격은 **아직 알려지지 않은 취약점**을 악용하는 공격이다. 취약점의 공개·인지 시점이 핵심이며, 지문에는 그 취약점이 새로 발견되었거나 알려지지 않았다는 조건이 없다.

패킷 스니핑 공격은 네트워크에서 오가는 패킷을 가로채 관찰하여 정보를 수집하는 공격이다. **전송 중인 통신을 엿듣는 것**과 웹 페이지에 코드를 삽입하는 것은 공격 방식이 다르다.

따라서 제시된 공격 방법은 ④ XSS이다.

NoteBase

문 19. 버퍼에 할당된 메모리의 경계를 침범해서 데이터 오류를 발생하게 하는 공격으로 가장 적절한 것은?

① 스푸핑(Spoofing)

② 스니핑(Sniffing)

③ 버퍼 오버플로(Buffer Overflow)

④ 스캐닝(Scanning)

정답 3번

간단한 해설

버퍼에 허용된 범위를 넘어 데이터를 쓰면 **인접한 메모리의 데이터가 손상**될 수 있다. 이러한 경계 초과 쓰기를 악용하는 것이 버퍼 오버플로 공격이다.

핵심 풀이

버퍼 오버플로: 버퍼는 데이터를 임시로 저장하기 위해 할당한 메모리 영역이다. 프로그램이 입력 크기나 저장 범위를 제대로 검사하지 않아 **버퍼의 경계 밖에 데이터를 쓰면** 인접한 데이터가 손상되거나 프로그램이 비정상 종료될 수 있다. 제시문의 메모리 경계 침범과 데이터 오류가 이 특징에 해당한다.

스푸핑: 사용자나 통신 상대의 신원·주소 등을 속여 **정상적인 대상인 것처럼 위장**하는 기법이다. 신뢰 대상을 속이는 것이 핵심이며, 버퍼의 저장 경계를 넘는 현상과는 다르다.

스니핑: 네트워크에서 오가는 **통신 데이터를 수집·관찰**하는 기법이다. 공격에 악용되면 노출된 정보를 엿볼 수 있지만, 메모리 경계를 넘어 데이터를 덮어쓰는 방식은 아니다.

스캐닝: 대상 시스템의 존재, 열린 포트나 제공 서비스 등을 **탐색하여 정보를 수집**하는 기법이다. 취약점 탐색이나 공격 준비에 이용될 수 있으나, 그 자체가 버퍼의 메모리 경계를 침범하는 공격을 뜻하지는 않는다.

따라서 설명에 해당하는 공격은 ③ 버퍼 오버플로이다.

NoteBase

문 20. 다음 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 ㉠, ㉡에 들어갈 용어로 가장 적절한 것은?

제23조의2(주민등록번호의 사용 제한)
① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.
1. 제23조의3에 따라 (㉠)으로 지정받은 경우
2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우
3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 (㉡)가 고시하는 경우

① ㉠: 개인정보처리기관, ㉡: 방송통신위원회
② ㉠: 개인정보처리기관, ㉡: 개인정보보호위원회
③ ㉠: 본인확인기관, ㉡: 개인정보보호위원회
④ ㉠: 본인확인기관, ㉡: 방송통신위원회

정답 4번

간단한 해설

제23조의3에 따라 본인확인 대체수단 업무를 수행하도록 지정되는 기관은 **본인확인기관**이다. 제시된 당시 조문에서 영업상 불가피한 수집·이용의 고시 주체는 **방송통신위원회**이다.

빈칸별 해설

문제에 제시된 당시 조문은 정보통신서비스 제공자의 주민등록번호 수집·이용을 원칙적으로 금지하고, 본인확인기관 지정·법령상 허용·고시 대상 해당 등의 예외를 정한다. 단순히 개인정보를 처리한다는 이유만으로 예외가 되는 것은 아니다.

㉠: **본인확인기관**이다. 제23조의3에 따라 주민등록번호를 사용하지 않고 본인을 확인하는 대체수단의 개발·제공·관리 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되어 지정된 기관을 뜻한다. 빈칸 앞의 '제23조의3에 따라 지정받은 경우'가 단서이므로 '개인정보처리기관'과 구별된다.

㉡: **방송통신위원회**이다. 제시된 당시 제23조의2 제1항 제3호는 영업상 목적의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자를 고시하는 주체를 방송통신위원회로 정한다. 영업상 필요성만으로 허용되는 것이 아니라 **해당 고시 대상에 해당해야** 하며, 이 빈칸의 주체를 개인정보보호위원회로 바꾸면 안 된다.

따라서 ㉠ 본인확인기관, ㉡ 방송통신위원회의 조합인 ④와 일치한다.

NoteBase