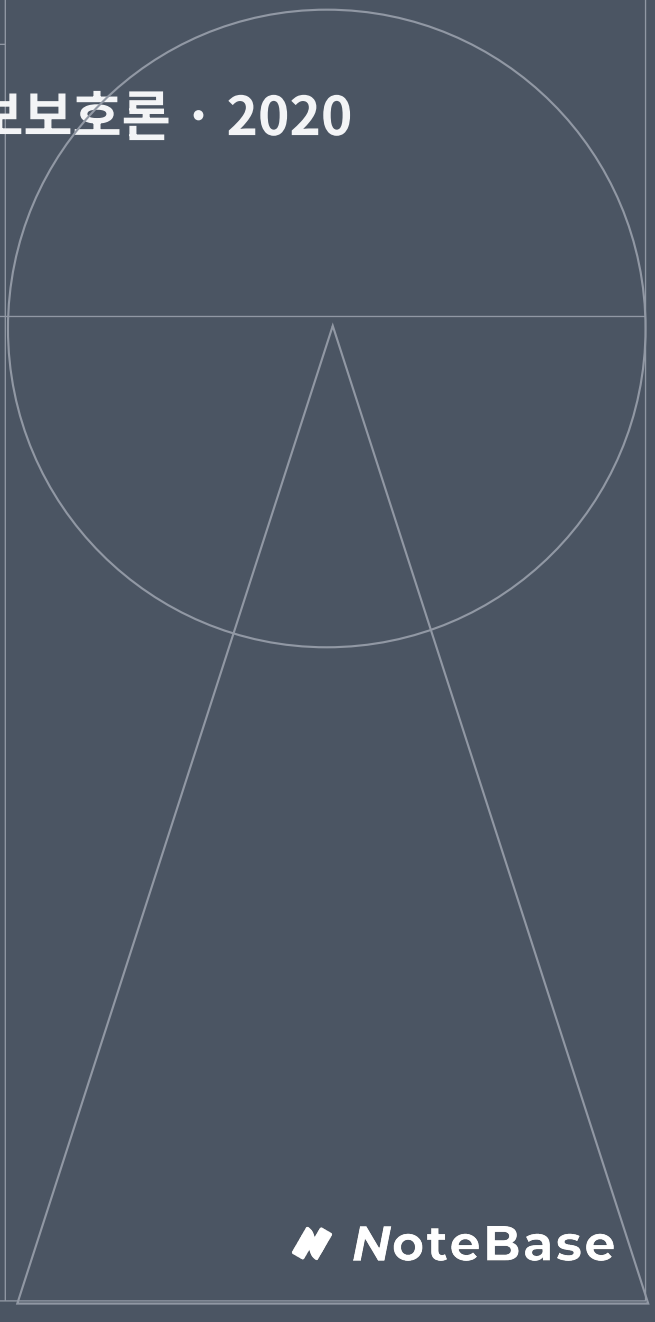
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2020



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2020

공무원/경찰/경력채용 · 정보보호론 · 2020

문 1. 다음에서 설명하는 정보보호의 보안 서비스로 가장 적절한 것은?

기관 내부의 중요 데이터를 외부로 전송하는 행위가 탐지된 경우, 전송자가 전송하지 않았음을 주장하지 못하도록 확실한 증거를 제시할 수 있는 보안 서비스이다.

① 무결성(Integrity)
② 가용성(Availability)
③ 기밀성(Confidentiality)
④ 부인방지(non-Repudiation)

정답 4번

간단한 해설

전송 사실을 뒷받침하는 증거로 전송자의 부인을 막는 서비스는 **부인방지**이다. 중요 데이터가 외부로 나갔다는 상황보다, 전송 행위를 나중에 부정하지 못하게 한다는 요구가 판단의 핵심이다.

개념 구분

부인방지: 특정인이 수행한 행위를 나중에 부인하지 못하도록 검증 가능한 증거를 제공하는 서비스이다.
제시문은 데이터 유출 자체의 차단보다 '전송자가 전송 사실을 부인하지 못하게 하는 증거'에 초점을 두므로 ④ 부인방지에 해당한다.

무결성: 데이터가 허가 없이 변경되거나 훼손되지 않았음을 보장하는 성질이다. 데이터의 변경 여부가 아니라 전송 행위의 부인 가능성을 묻는 이 사례의 핵심 서비스와는 다르다.

가용성: 인가된 사용자가 필요한 때 정보와 서비스를 이용할 수 있도록 하는 성질이다. 전송자가 한 행위를 입증하는 기능을 뜻하지 않는다.

기밀성: 허가되지 않은 사람에게 정보가 공개되지 않도록 하는 성질이다. 중요 데이터의 외부 유출은 기밀성을 침해할 수 있지만, 유출자의 전송 사실을 증명하는 서비스는 부인방지이다.

NoteBase

문 2. 암호분석 중 암호기에 접근할 수 있어, 평문 P를 선택하여 이에 대응하는 암호문 C를 얻어 키 K나 평문 P를 추정하여 암호를 해독하는 방법으로 가장 적절한 것은?

① 암호문 단독 공격(COA, Ciphertext Only Attack)

② 기지 평문 공격(KPA, Known Plaintext Attack)

③ 선택 평문 공격(CPA, Chosen Plaintext Attack)

④ 선택 암호문 공격(CCA, Chosen Ciphertext Attack)

정답 3번

간단한 해설

공격자가 **평문을 직접 선택하고 대응하는 암호문을 얻는** 조건이므로 선택 평문 공격이다. 이미 확보한 평문·암호문 쌍만 이용하는 기지 평문 공격과 구별한다.

개념 구분

선택 평문 공격(CPA): 공격자가 평문을 직접 정하고 암호기에 입력하여 대응하는 암호문을 얻은 뒤, 그 관계를 분석한다. 발문의 결정적 단서는 단순히 평문을 알고 있다는 것이 아니라 **평문을 선택할 수 있다**는 점이므로 ③에 해당한다.

암호문 단독 공격(COA): 수집한 암호문을 이용해 암호를 분석한다. 평문을 직접 선택하여 암호화 결과를 얻는 능력은 전제하지 않는다.

기지 평문 공격(KPA): 이미 알고 있는 평문과 그에 대응하는 암호문 쌍을 이용한다. 주어진 쌍을 아는 것과 원하는 평문을 골라 새 암호문을 얻는 것은 다르다.

선택 암호문 공격(CCA): 공격자가 암호문을 선택하고 복호화 결과인 평문을 얻어 분석한다. 선택하는 입력이 평문인 CPA와 반대이다.

NoteBase

문 3. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(Error Propagation)가 발생하는 모드만을 묶은 것으로 가장 적절한 것은? (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher FeedBack, OFB: Output FeedBack)

① CBC, CFB

② CFB, OFB

③ CBC, ECB

④ OFB, ECB

정답 1번

간단한 해설

CBC와 CFB는 **앞서 생성된 암호문을 후속 암호화에 사용**하므로 평문 오류의 영향이 다른 블록으로 이어진다. 두 모드를 묶은 ①이 정답이다.

핵심 풀이

이 문항은 **평문 블록의 오류가 암호화 결과에 미치는 영향**을 묻는다. 키와 초기화 벡터 등 나머지 조건이 같을 때, 변경된 평문에서 나온 암호문이 뒤의 암호화 과정에 다시 입력되는지 확인한다.

CBC: 현재 평문과 직전 암호문을 XOR한 뒤 암호화한다. 평문 오류로 현재 암호문이 달라지면 그 값이 다음 블록의 입력에 사용되므로 **암호문 연결을 따라 오류가 전이**된다.

CFB: 앞서 생성한 암호문을 피드백하여 암호 함수의 입력을 만들고, 그 출력과 현재 평문을 XOR하여 암호문을 생성한다. 평문 오류로 바뀐 암호문이 다시 입력되므로 **암호문 피드백을 통해 후속 암호화에 영향**을 준다.

ECB: 각 평문 블록을 **서로 독립적으로 암호화**한다. 한 블록이 바뀌어도 다른 블록의 암호화 입력은 바뀌지 않으므로 블록 사이 오류 전이가 없다.

OFB: 키와 초기화 벡터로부터 암호 함수의 출력들을 연속 생성하고 이를 평문과 XOR한다. 피드백하는 것은 **평문과 결합하기 전의 출력**이므로, 평문 오류가 뒤의 키스트림을 바꾸지 않아 다른 블록으로 전이되지 않는다.

따라서 해당 모드만 묶은 것은 ① CBC, CFB이다.

NoteBase

문 4. 블록 암호 모드의 암호화 수식은 다음과 같다. 이 모드들의 복호화 수식으로 가장 적절한 것은? (단, P_i: i번째 평문, C_i: i번째 암호문, $E_K(P_i)$: 암호화, $D_K(C_i)$: 복호화, ⊕: XOR, K: 키)

블록 암호 모드	암호화 수식
CBC(Cipher Block Chaining)	$C_i = E_K(C_{i-1} \oplus P_i)$
CFB(Cipher FeedBack)	$C_i = E_K(C_{i-1}) \oplus P_i$
CTR(CounTeR mode)	$C_i = E_K(counter) \oplus P_i$

① CBC: $P_i = E_K(C_{i-1}) \oplus C_i$, CFB: $P_i = D_K(C_i) \oplus C_{i-1}$, CTR: $P_i = D_K((counter) \oplus C_i)$

② CBC: $P_i = D_K(C_i) \oplus C_{i-1}$, CFB: $P_i = E_K(C_{i-1}) \oplus C_i$, CTR: $P_i = E_K(counter) \oplus C_i$

③ CBC: $P_i = C_i \oplus E_K(C_{i-1})$, CFB: $P_i = E_K(C_{i-1}) \oplus C_i$, CTR: $P_i = E_K(counter) \oplus C_i$

④ CBC: $P_i = D_K(C_i) \oplus C_{i-1}$, CFB: $P_i = D_K(C_i) \oplus C_{i-1}$, CTR: $P_i = D_K((counter) \oplus C_i)$

정답 2번

간단한 해설

CBC는 **암호화 함수의 역연산**을 먼저 수행해야 한다. CFB와 CTR은 **암호화 함수로 만든 동일한 비트열을 다시 XOR**하여 평문을 복원한다.

NoteBase

대응 관계 해설

같은 비트열을 두 번 XOR하면 원래 값으로 돌아오므로 $(A \oplus B) \oplus B = A$이다. 또한 같은 키를 사용하는 암호화 함수 E_K와 복호화 함수 D_K는 서로 역함수이다. 이 두 성질로 각 암호화식을 평문 P_i에 대해 정리한다.

CBC: 주어진 식은 $C_i = E_K(C_{i-1} \oplus P_i)$이다. 양변에 복호화 함수를 적용하면 $D_K(C_i) = C_{i-1} \oplus P_i$이고, 이전 암호문을 다시 XOR하면 $P_i = D_K(C_i) \oplus C_{i-1}$이다. 즉 **현재 암호문을 복호화한 뒤 이전 암호문과 XOR**한다. 첫 블록에서는 이전 암호문 대신 초기화 벡터를 사용한다.

CFB: 주어진 식은 $C_i = E_K(C_{i-1}) \oplus P_i$이다. 이전 암호문을 암호화한 동일한 값을 양변에 XOR하면 $P_i = E_K(C_{i-1}) \oplus C_i$이다. 평문에 암호화 함수를 직접 적용한 구조가 아니므로 **복호화할 때도 암호화 함수**로 같은 XOR용 비트열을 만든다.

CTR: 주어진 식은 $C_i = E_K(\text{counter}) \oplus P_i$이다. **암호화 때와 같은 카운터 값을 암호화**하여 암호문과 XOR하므로 $P_i = E_K(\text{counter}) \oplus C_i$이다. 카운터와 암호문을 먼저 XOR하여 복호화 함수에 넣는 방식이 아니다.

CBC에는 복호화 함수가, CFB와 CTR에는 암호화 함수가 쓰이는 위 세 복호화식의 조합은 ②이다.

NoteBase

문 5. Triple-DES(Data Encryption Standard)에서는 DES 암호화와 복호화를 섞어서 암호화한다. 다음 중 순서를 가장 적절하게 나열한 것은?

① 암호화 → 암호화 → 복호화

② 암호화 → 복호화 → 암호화

③ 복호화 → 암호화 → 복호화

④ 암호화 → 복호화 → 복호화

정답 2번

간단한 해설

Triple-DES의 암호화는 DES 연산을 세 번 결합하며, **가운데 단계에 복호화 연산**을 사용한다. 이때 복호화는 평문을 최종 복원하는 것이 아니라 전체 암호화를 구성하는 중간 변환이다.

올바른 순서

암호화 → 복호화 → 암호화

첫 번째 암호화: 평문 블록 P에 첫 번째 키 K_1을 사용한 DES 암호화 연산 E를 적용하여 중간값 $X = E_{K_1}(P)$를 만든다. 이 결과가 **다음 단계의 입력**이 된다.

두 번째 복호화: 첫 단계의 결과 X에 두 번째 키 K_2를 사용한 DES 복호화 연산 D를 적용하여 $Y = D_{K_2}(X)$를 만든다. 여기서 복호화는 **중간 변환에 쓰이는 연산**이다. 첫 단계와 다른 키를 사용하므로 앞의 암호화를 그대로 취소하여 원래 평문으로 돌아가는 과정이 아니다.

세 번째 암호화: 두 번째 단계의 결과 Y에 세 번째 키 K_3를 사용한 DES 암호화 연산을 적용하여 최종 암호문 $C = E_{K_3}(Y)$를 얻는다. 각 단계는 **직전 단계가 만든 결과를 이어받아** 처리하므로, 이 세 연산이 합쳐져 하나의 Triple-DES 암호화 변환을 이룬다.

NoteBase

문 6. DES(Data Encryption Standard)에서 입력값 $101111_{(2)}$이 다음과 같은 S-Box를 통과할 때 출력값으로 가장 적절한 것은?

S-Box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	07	02	12	05	10	14	01
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

① $0001_{(2)}$

② $0011_{(2)}$

③ $0111_{(2)}$

④ $1110_{(2)}$

정답 3번

간단한 해설

입력의 **양 끝 2비트는 행 번호, 가운데 4비트는 열 번호**를 정한다. 행 번호 3과 열 번호 7의 값은 십진수 7이므로, 출력은 4비트 이진수 0111이다.

NoteBase

계산 과정

1. 행 번호 결정: DES의 S-Box는 입력 6비트 중 첫째 비트와 마지막 비트를 이어 붙여 행 번호를 정한다. 입력 101111의 양 끝은 1과 1이므로 행 번호는 다음과 같다.
$11_{(2)} = 3_{(10)}$

2. 열 번호 결정: 가운데 네 비트를 순서대로 읽어 열 번호를 정한다. 입력 101111의 가운데 네 비트는 0111이므로 열 번호는 다음과 같다.
$0111_{(2)} = 7_{(10)}$

3. 표 조회: 제시된 S-Box에서 행 번호 3과 열 번호 7이 만나는 칸의 값은 07, 즉 십진수 7이다. 행과 열은 0부터 표시되어 있으므로 표에 적힌 번호를 그대로 사용한다.

4. 출력 변환: S-Box의 출력은 4비트이므로 십진수 7을 앞의 0을 포함한 이진수 0111로 나타낸다.
$7_{(10)} = 0111_{(2)}$

따라서 출력값은 ③이다.

NoteBase

문 7. 전자서명이 제공하는 기능 중 가장 적절하지 않은 것은?

① 서명자만이 서명문을 생성할 수 있다.

② 서명자가 전자 서명한 후에는 서명한 사실을 부인할 수 없다.

③ 서명문의 서명자를 확인할 수 있다.

④ 해시값이 포함된 전자서명을 다른 문서에 반복 서명할 수 있다.

정답 4번

간단한 해설

전자서명은 **특정 문서의 내용과 서명자를 함께 연결**하므로, 기존 서명값을 내용이 다른 문서에 그대로 재사용할 수 없다. 다른 문서에는 해당 문서에 대한 새 서명이 필요하다.

선지별 해설

① O — 전자서명의 **위조 불가성**에 관한 설명이다. 서명은 서명자의 개인키로 생성하므로, 안전한 알고리즘을 사용하고 개인키가 보호된다는 전제에서 다른 사람이 유효한 서명을 위조하기 어렵다.

② O — 전자서명은 **부인 방지** 기능을 제공한다. 수신자는 서명을 검증하고 제3자에게 서명 사실을 입증할 근거로 제시할 수 있으므로, 서명자가 나중에 자신이 서명했다는 사실을 부인하는 것을 방지한다.

③ O — 전자서명의 **서명자 인증** 기능이다. 서명자와 연결된 공개키로 서명을 검증하여 해당 개인키의 소유자가 서명했는지 확인한다. 공개키가 실제 누구에게 속하는지도 신뢰할 수 있게 확인되어야 한다.

④ X — 전자서명은 **서명한 문서의 내용에 결합**된다. 문서의 해시값을 이용한 서명을 내용이 다른 문서에 그대로 붙이면, 새 문서에서 계산한 해시값과 서명이 대응하지 않아 검증에 실패한다. 따라서 다른 문서에는 그 문서에 대한 새 서명을 생성해야 한다. 같은 개인키를 다시 사용하는 것과 기존 서명값을 다른 문서에 재사용하는 것은 다르다.

NoteBase

문 8. 메시지 인증 코드(MAC)에 대한 설명 중 가장 적절하지 않은 것은?

① 메시지와 송·수신자만이 공유하는 비밀키를 입력받아 생성된다.

② 메시지 무결성 검증이 가능하다.

③ 부인방지(non-Repudiation)를 위해 사용한다.

④ 인증(Authentication)이 가능하다.

정답 3번

간단한 해설

MAC은 송신자뿐 아니라 **비밀키를 공유한 수신자도 생성**할 수 있다. 따라서 메시지 무결성과 출처 인증은 가능하지만 **부인방지는 제공하지 않는다**.

선지별 해설

① O: MAC은 **메시지와 공유 비밀키**를 입력으로 계산하는 인증값이다. 송신자는 이 값을 메시지와 함께 보내고, 수신자는 같은 비밀키로 인증값을 계산하여 검증한다.

② O: 수신자가 받은 메시지로 다시 계산한 MAC을 수신한 MAC과 비교하여 **전송 중 메시지의 변경 여부**를 검증할 수 있다. 공격자는 비밀키 없이 변경된 메시지에 맞는 유효한 MAC을 만들기 어렵다.

③ X: **송신자와 수신자 모두 같은 비밀키로 MAC을 생성**할 수 있으므로, 제3자에게 어느 쪽이 만들었는지를 MAC만으로 입증할 수 없다. 따라서 MAC은 부인방지를 제공하지 않으며, 부인방지에는 일반적으로 서명자만 보유한 개인키로 생성하는 전자서명을 활용한다.

④ O: 공유키를 안전하게 송·수신자만 보유한다는 전제에서, 수신자는 유효한 MAC을 통해 **비밀키를 아는 상대가 만든 메시지**임을 확인하는 데이터 출처 인증을 할 수 있다. 이는 제3자에게 작성자를 입증하는 부인방지와는 다른 성질이다.

따라서 MAC의 기능으로 적절하지 않은 설명은 부인방지를 제시한 ③이다.

NoteBase

문 9. 다음 중 사용자 인증(User Authentication)에 대한 설명으로 가장 적절하지 않은 것은?

① 지식기반 인증의 가장 큰 문제는 오인식(False Acceptance), 오거부(False Rejection)가 존재한다는 것이다.

② 패스워드를 저장할 때 해시를 이용하는데, 안전도를 높이기 위해 솔트(Salt)를 사용한다.

③ 비밀번호로 사용되는 PIN(Personal Identification Number)은 지식기반 인증이다.

④ OTP(One Time Password)는 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

정답 1번

간단한 해설

오인식과 오거부는 **생체인증의 대표적인 인식 오류**이다. 이를 지식기반 인증의 가장 큰 문제로 제시한 ①이 적절하지 않다.

선지별 해설

① X: 타인을 정당한 사용자로 받아들이는 오인식과 정당한 사용자를 거부하는 오거부는 **생체인증의 확률적 특징 비교**에서 대표적으로 다루는 문제이다. 지식기반 인증은 입력한 비밀값의 일치 여부를 확인하며, 주요 위험은 비밀번호의 추측·유출·도용 등이다. 따라서 생체인증의 문제를 지식기반 인증의 가장 큰 문제로 제시한 부분을 고쳐야 한다.

② O: 솔트는 비밀번호를 해시 처리할 때 함께 넣는 값이다. 비밀번호별로 서로 다른 솔트를 사용하면 동일한 비밀번호에도 다른 해시가 생성되어 **미리 계산한 해시 목록의 재사용**과 여러 계정에 대한 일괄 추측을 어렵게 한다. 솔트만으로 약한 비밀번호가 안전해지는 것은 아니므로 적절한 비밀번호 해싱 방식도 필요하다.

③ O: PIN은 사용자가 기억하고 입력하는 숫자 형태의 비밀값이므로 **사용자가 아는 것**에 근거한 지식기반 인증이다. PIN을 입력하는 기기 자체를 소지한다는 사실과 PIN이라는 인증 요소의 분류는 구별한다.

④ O: OTP는 일회성 인증값을 생성하고 검증하는 데 필요한 관리가 있다. 예를 들어 **이벤트 방식은 카운터, 시간 방식은 시계의 동기화**를 관리해야 하며, 사용자별 비밀키 보호와 생성기 분실 대응도 필요할 수 있다. 따라서 생성 방식에 따라 사용자나 서버의 관리 부담이 생길 수 있다.

따라서 가장 적절하지 않은 설명은 ①이다.

NoteBase

문 10. 주체가 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로, 객체의 소유자가 접근 여부를 결정하는 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 문맥 의존성 접근 통제(Context-dependent Access Control)

정답 2번

간단한 해설

주체나 그룹의 신원을 기준으로 하면서 **객체 소유자가 접근 권한을 결정**하는 방식은 임의적 접근 통제(DAC)이다. 그룹이 등장하더라도 역할에 권한을 부여한다는 조건이 없다면 역할기반 접근 통제로 판단하지 않는다.

개념 구분

강제적 접근 통제(MAC): **중앙에서 정한 보안 정책을 강제**하여 접근을 결정한다. 대표적으로 주체의 보안 등급과 객체의 보안 표지를 비교하며, 객체 소유자가 자신의 재량만으로 이 정책을 바꿀 수 없다.

임의적 접근 통제(DAC): 주체 또는 그 주체가 속한 그룹의 신원을 바탕으로 권한을 확인하고, **객체 소유자가 접근 권한을 부여·변경**할 수 있는 방식이다. 예를 들어 파일 소유자가 특정 사용자나 그룹에 읽기·쓰기 권한을 주는 경우가 해당한다. 발문의 그룹 신원과 소유자의 결정권이라는 두 단서가 이 방식에 부합한다.

역할기반 접근 통제(RBAC): **직무에 따른 역할에 권한을 연결**하고 사용자에게 역할을 부여하여 접근을 관리한다. 그룹이 언급되었다는 이유만으로 이 방식이라고 판단할 수 없으며, 역할과 권한의 연결이 핵심이다.

문맥 의존성 접근 통제: **접근 시점의 시간·위치 등 상황 조건**을 고려하여 허용 여부를 결정한다. 같은 사용자라도 근무시간이나 접속 위치가 달라지면 접근 결과가 달라질 수 있다. 소유자의 권한 부여가 아니라 접근 요청의 상황을 기준으로 한다는 점에서 구별된다.

따라서 정답은 ② 임의적 접근 통제이다.

NoteBase

문 11. 다음에서 설명하는 것으로 가장 적절한 것은?

· Brewer-Nash 모델이라고도 한다.
· 이익충돌을 방지하기 위한 모델이다.
· 서로 대립 관계에 있는 객체 간의 정보 접근을 통제하는 모델이다.

① 벨라파듈라(Bell-Lapadula) 모델
② 비바(Biba) 모델
③ 클락 윌슨(Clark-Wilson) 모델
④ 만리장성(Chinese Wall) 모델

정답 4번

간단한 해설

Brewer-Nash라는 이름과 **이해충돌 방지**는 만리장성 모델의 핵심 단서이다. 한 주체가 경쟁 회사들의 비공개 정보를 함께 접하지 못하도록 이전 접근 이력에 따라 권한을 제한한다.

핵심 풀이

만리장성 모델은 Brewer와 Nash가 제안한 접근통제 모델로, 서로 경쟁하는 조직 사이에서 이해충돌을 일으킬 수 있는 정보 흐름을 제한한다. 따라서 제시된 세 단서에 해당하는 것은 ④ 만리장성(Chinese Wall) 모델이다.

접근통제의 기준은 이전의 정보 접근 이력이다. 예를 들어 동일한 이해충돌 집합에 속한 경쟁 회사 A와 B가 있을 때, 한 주체가 A의 비공개 정보에 접근했다면 B의 비공개 정보에는 접근하지 못하도록 제한한다. 모든 회사의 정보를 일괄 차단하는 방식은 아니다.

벨라파듈라 모델은 보안등급에 따른 정보 흐름 통제로 기밀성을 보호한다. 비바 모델은 무결성 등급에 따른 접근통제로 데이터의 오염을 막고, 클락 윌슨 모델은 정당한 거래 절차와 직무 분리 등을 통해 무결성을 보호한다. 이들보다 '경쟁 관계의 정보에 대한 접근 이력과 이해충돌 방지'가 만리장성 모델을 특정하는 단서이다.

NoteBase

문 12. 난수의 성질을 분류하는 데 사용되는 항목 중 가장 적절하지 않은 것은?

① 무작위성

② 예측 불가능성

③ 재현 불가능성

④ 주기성

정답 4번

간단한 해설

난수의 성질은 무작위성, 예측 불가능성, 재현 불가능성의 충족 여부로 구분할 수 있다. **주기성은 같은 수열이 규칙적으로 반복되는 성질**이므로 이 분류의 성질로 가장 적절하지 않다.

선지별 해설

① O: 무작위성은 수열이 **통계적으로 편향이나 규칙성을 드러내지 않는 성질**이다. 예를 들어 비트 난수에서는 0과 1의 출현 빈도와 비트 사이의 관계 등을 살펴본다. 통계적 무작위성이 있다고 해서 다음 값을 예측하기도 어렵다는 결론이 자동으로 성립하는 것은 아니다.

② O: 예측 불가능성은 이미 얻은 출력 등을 알아도 **아직 생성되지 않은 값을 현실적인 계산량으로 알아내기 어려운 성질**이다. 암호학적으로 안전한 난수에는 단순한 통계적 무작위성을 넘어 이러한 성질이 중요하다.

③ O: 재현 불가능성은 같은 생성 절차를 다시 실행해도 **동일한 수열을 의도적으로 다시 만들어 낼 수 없는 성질**이다. 물리적 잡음 등 비결정적 현상에서 얻는 진정한 난수와, 같은 초기 상태와 입력으로 동일한 수열을 재현하는 의사난수를 구별하는 기준이다. 모든 의사난수가 이 성질을 갖는다는 뜻은 아니다.

④ X: 주기성은 일정한 간격으로 같은 수열이 반복되는 성질이므로, 앞의 세 가지와 같은 난수의 성질 분류 항목으로 제시하기에는 적절하지 않다. 의사난수 생성기에서 주기가 나타날 수는 있지만, 이는 구현의 특성이며 **반복 규칙이 있다는 사실이 난수성을 보장하지는 않는다**. 따라서 난수에 주기성이 요구된다고 이해해서는 안 된다.

NoteBase

문 13. 대칭키 암호화 알고리즘으로만 묶은 것으로 가장 적절한 것은?

① RC4, SKIPJACK, DSA

② DES, Blowfish, LEA

③ DES, ECC, Rabin

④ IDEA, ElGamal, HIGHT

정답 2번

간단한 해설

DES, Blowfish, LEA는 모두 **대칭키 블록 암호**이다. 나머지 묶음에는 공개키 방식이나 전자서명 알고리즘이 포함되어 있으므로 정답은 ②이다.

개념 구분

대칭키 암호는 암호화와 복호화에 **같은 비밀키를 공유**하는 방식이다. 공개키 방식은 공개키와 개인키를 구별하므로, 각 묶음에 공개키 알고리즘이나 전자서명 알고리즘이 섞여 있는지 확인한다.

②의 DES, Blowfish, LEA는 모두 **대칭키 블록 암호**이다. 데이터를 정해진 크기의 블록 단위로 처리하며, 세 알고리즘 모두 대칭키 암호화라는 조건을 만족한다.

①의 RC4는 대칭키 스트림 암호이고 SKIPJACK은 대칭키 블록 암호이다. 그러나 **DSA는 공개키 기반 전자서명 알고리즘**이므로 대칭키 암호화 알고리즘만으로 구성된 묶음이 아니다.

③의 DES는 대칭키 암호이지만, **ECC와 Rabin은 공개키 방식**에 속한다. ECC는 타원곡선을 이용하는 공개키 암호 기술이고, Rabin은 공개키와 개인키를 구분하는 암호 방식이다.

④의 IDEA와 HIGHT는 대칭키 블록 암호이지만 **ElGamal은 공개키 암호 방식**이다. 따라서 이 묶음에도 대칭키가 아닌 알고리즘이 포함되어 있다.

따라서 대칭키 암호화 알고리즘으로만 묶인 것은 ② DES, Blowfish, LEA이다.

NoteBase

문 14. 두 소수 p는 3, q는 11이고, 공개키 e는 3, 암호문 C는 3일 때, RSA 암호 알고리즘을 사용하여 평문 P의 값을 구한 것으로 가장 적절한 것은? (단, 개인키 d의 값은 계산될 수 있는 최소의 자연수로 한다.)

① 7

② 8

③ 9

④ 10

정답 3번

간단한 해설

개인 지수는 **공개 지수의 모듈러 역수**로 구하면 $d = 7$이다. 암호문을 이 지수만큼 거듭제곱한 뒤 $n = 33$으로 나눈 나머지를 구하므로 P=3^733=9이다.

계산 과정

모듈러스 계산: 서로 다른 두 소수 $p = 3$, $q = 11$로부터 $n = pq = 33$이다. 개인 지수를 구할 때 사용하는 오일러 함수 값은 $\varphi(n) = (p-1)(q-1) = 2 \times 10 = 20$이다. **개인 지수 계산과 평문 복원의 나머지 기준을 구별**해야 한다. 전자는 $\varphi(n) = 20$, 후자는 $n = 33$을 사용한다.

개인 지수 계산: 공개 지수 $e = 3$의 역수를 $\varphi(n) = 20$을 기준으로 구한다. 즉 ed≡1±od20이므로 $3d = 20k + 1$을 만족하는 정수를 찾는다. $k = 0$에서는 자연수 해가 없고, $k = 1$일 때 $3d = 21$이므로 **최소 자연수 개인 지수**는 $d = 7$이다.

평문 복원: RSA 복호화식 P=C^d n에 $C = 3$, $d = 7$, $n = 33$을 넣는다. $3^7 = 2187 = 33 \times 66 + 9$이므로 **33으로 나눈 나머지**인 $P = 9$를 얻는다. 검산하면 $9^3 = 729 = 33 \times 22 + 3$으로 원래 암호문 3이 복원된다.

평문을 나타내는 정수는 9이므로 정답은 ③이다.

NoteBase

문 15. 다음에서 설명하는 것으로 가장 적절한 것은?

· 인터넷상에서 신용카드를 이용한 상품구매 시 안전한 대금결제 과정 처리를 위해 RSA 암호화와 인증기술을 이용한다.
· 전자봉투와 이중서명을 사용한다.

① SET(Secure Electronic Transaction)
② PGP(Pretty Good Privacy)
③ OTP(One Time Password)
④ SSO(Single Sign On)

정답 1번

간단한 해설

신용카드 결제와 이중서명의 결합이 SET을 식별하는 핵심 단서이다. 전자봉투로 기밀성을 보호하고, 이중서명으로 주문정보와 지불정보를 연결한다.

핵심 풀이

SET은 인터넷에서 신용카드 결제를 안전하게 처리하기 위한 프로토콜이다. 거래 정보의 기밀성·무결성과 참여자 인증을 위해 암호화와 인증기술을 사용한다. 신용카드 대금결제에 전자봉투와 이중서명을 결합한다는 설명은 ①에 해당한다.

전자봉투는 거래 데이터를 대칭키로 암호화하고, 그 대칭키를 수신자의 공개키로 보호하여 전달하는 방식이다. SET에서는 RSA로 대칭키를 보호하여 안전하게 전달한다.

이중서명은 주문정보와 지불정보의 해시값을 결합해 하나의 서명으로 연결한다. 판매자에게 지불정보의 세부 내용을, 결제기관에게 주문정보의 세부 내용을 모두 공개하지 않고도 두 정보가 같은 거래에 속함을 검증하도록 한다.

다른 개념과의 구별: PGP는 전자우편 등 데이터의 암호화·서명에 쓰이는 보안 기술이고, OTP는 한 번 사용하는 비밀번호를 통한 인증 방식이다. SSO는 한 번의 로그인으로 연결된 여러 서비스에서 인증을 이용하는 방식이다. 이들은 전자봉투와 이중서명으로 신용카드 결제 정보를 보호하는 SET의 설명과 구별된다.

NoteBase

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

① 공개키의 정당성을 확인하는 방법이다.

② 전자우편에서 프라이버시(Privacy), 무결성(Integrity), 그리고 인증(Authentication)을 제공한다.

③ 인증기관의 인증서가 필요하지 않다.

④ 계층적인 신뢰 구조에 따라 X.509 인증서는 사용할 수 없다.

정답 4번

간단한 해설

PGP는 대표적으로 **사용자 간 신뢰망**을 이용하며, 중앙 인증기관의 계층 구조를 필수 전제로 하지 않는다. X.509 인증서도 PGP 제품의 지원 여부에 따라 사용할 수 있으므로, 신뢰 구조를 이유로 사용 불가라고 단정할 수 없다.

선지별 해설

① O: PGP는 공개키가 주장하는 소유자의 것인지 확인하는 기능을 제공한다. 공개키와 사용자 신원의 결합에 대한 서명, 신뢰하는 사용자의 보증, 지문 확인 등을 통해 공개키의 정당성을 판단한다.

② O: 전자우편 내용을 암호화하여 기밀성을 제공하고, 전자서명을 검증하여 메시지의 변경 여부와 서명자의 진위를 확인한다. 이에 따라 프라이버시, 무결성, 인증을 제공할 수 있다.

③ O: PGP의 전형적인 신뢰망에서는 사용자가 서로의 공개키를 인증하므로 중앙 인증기관이 발급한 인증서를 필수로 요구하지 않는다. 이는 공개키와 신원을 연결하는 인증 정보 자체가 없다는 뜻은 아니다.

④ X: PGP의 대표적인 신뢰 방식은 중앙 인증기관의 계층 구조가 아니라 **사용자 간 신뢰망(Web of Trust)**이다. 또한 X.509 인증서 지원은 제품의 구현과 기능에 따라 달라지며, 이를 지원하는 PGP 제품도 있다. 따라서 ‘계층적인 신뢰 구조에 따라 X.509 인증서를 사용할 수 없다’는 설명은 적절하지 않다.

NoteBase

문 17. 다음에서 설명하는 SSL 프로토콜로 가장 적절한 것은?

· 연결을 위해 기밀성과 메시지 무결성 서비스를 제공한다.
· 신뢰하는 전송서비스를 필요로 하므로 TCP 프로토콜을 사용한다.
· 수신된 데이터는 복호화를 하고, MAC을 확인하고, 압축을 풀고, 재조립하여 상위 계층으로 전달한다.

① Handshake 프로토콜
② ChangeCipherSpec 프로토콜
③ Alert 프로토콜
④ Record 프로토콜

정답 4번

간단한 해설

SSL에서 **암호화와 MAC을 통해 데이터를 보호**하고, 수신한 데이터를 복호화·검증하여 상위 계층에 전달하는 것은 Record 프로토콜이다. TCP 위에서 동작한다는 설명도 이에 부합한다.

NoteBase

핵심 풀이

기밀성과 무결성: SSL Record 프로토콜은 상위 계층에서 받은 데이터를 레코드로 처리하며, 협상된 방식에 따라 **암호화로 기밀성, MAC으로 무결성**을 제공한다. 메시지 자체를 보호하는 기능이라는 점이 핵심 단서이다.

TCP 사용: SSL Record 계층은 **신뢰성 있는 전송 계층 위에서** 동작하며, 대표적으로 TCP를 이용한다. 여기서 신뢰성은 데이터의 전달과 순서 보장을 뜻하며, TCP 자체가 암호화나 보안 인증을 제공한다는 뜻은 아니다.

수신 데이터 처리: Record 계층은 송신 측이 적용한 보호 처리를 되돌려 복호화하고 MAC을 검증한 뒤, 압축을 사용했다면 압축을 풀고 조각을 재조립하여 상위 계층에 전달한다. 지문의 **복호화·MAC 확인·압축 해제·재조립**은 이 레코드 처리 기능을 직접 설명한다.

Handshake 프로토콜: 통신 상대의 인증, 암호 알고리즘의 협상, 키 설정을 담당한다. 데이터를 보호하는 데 필요한 **보안 조건을 합의**하는 역할이므로 실제 레코드 처리와 구별된다.

ChangeCipherSpec 프로토콜: 이후 전송되는 레코드에 **새로 합의한 암호 명세와 키를 적용**하도록 암호 상태의 전환을 알린다.

Alert 프로토콜: 오류나 경고, 연결 종료 통지 등 **연결 상태에 관한 알림**을 전달한다.

따라서 세 가지 설명에 해당하는 것은 ④ Record 프로토콜이다.

NoteBase

문 18. 다음에서 ㉠, ㉡, ㉢에 들어갈 용어로 가장 적절하게 연결한 것은?

· (㉠) 공격은 패킷 헤더 정보를 조작하여, 올바른 재조합을 불가능하게 만드는 것을 이용한다.
· (㉡) 공격 사례로 Trinoo, TFN, Stacheldraht 공격 등이 있다.
· (㉢) 공격은 IP 위장과 ICMP의 특성을 이용한다.

① ㉠: Teardrop, ㉡: DDoS, ㉢: Smurf

② ㉠: Land, ㉡: DDoS, ㉢: SYN flooding

③ ㉠: Boink, ㉡: SYN flooding, ㉢: Teardrop

④ ㉠: Teardrop, ㉡: SYN flooding, ㉢: Land

정답 1번

간단한 해설

단편 재조립 정보 조작은 Teardrop, Trinoo·TFN·Stacheldraht가 속하는 공격 분류는 DDoS이다. **IP 위장과 ICMP 응답의 반사·증폭**은 Smurf를 가리킨다.

빈칸별 해설

㉠ Teardrop: IP 단편의 위치를 나타내는 오프셋 등 **재조립 정보를 조작**하여 단편이 서로 겹치도록 만드는 공격이다. 취약한 시스템이 이 단편을 재조립하는 과정에서 오류나 장애가 발생하므로, 정상적인 재조합을 방해한다는 설명에 해당한다. 출발지와 목적지 주소를 같게 만드는 Land와 구별된다.

㉡ DDoS: Trinoo, TFN, Stacheldraht는 **여러 시스템을 동원하는 분산 서비스 거부** 공격 도구들이다. 여러 공격 에이전트가 특정 대상에 트래픽을 집중시키는 것이 공통 특징이다. SYN flooding은 TCP의 연결 설정 과정에 부담을 주는 구체적 공격 방식이므로 이 도구들을 포괄하는 분류는 DDoS이다.

㉢ Smurf: 피해자의 주소로 **출발지 IP를 위장한 ICMP 요청**을 브로드캐스트하여 여러 호스트의 응답이 피해자에게 집중되게 하는 반사·증폭 공격이다. 따라서 IP 위장과 ICMP를 함께 이용한다는 단서에 맞는다. TCP 연결 설정을 이용하는 SYN flooding이나 주소를 같게 만드는 Land와 구별된다.

따라서 ㉠ Teardrop, ㉡ DDoS, ㉢ Smurf로 연결한 ①이다.

NoteBase

문 19. 리눅스의 /etc/shadow 파일에서 확인할 수 있는 정보로 가장 적절하지 않은 것은?

① 사용자의 UID

② 사용자 계정이 만료되는 날짜

③ 암호를 사용할 수 있는 최대 기간

④ 암호가 마지막으로 변경된 날짜

정답 1번

간단한 해설

UID는 /etc/passwd에 저장된다. /etc/shadow는 비밀번호 정보와 최종 변경일·최대 사용 기간·계정 만료일 등의 수명 관리 정보를 담는다.

선지별 해설

① X — **사용자의 UID는 /etc/passwd**의 세 번째 필드에 저장된다. /etc/shadow에는 로그인 이름이 있지만 숫자형 사용자 식별자인 UID를 저장하는 필드는 없다.

② O — /etc/shadow의 여덟 번째 필드는 **계정 만료일**이다. 날짜 자체를 문자열로 쓰는 대신 1970년 1월 1일부터 지난 일수로 나타낸다. 계정의 만료일과 비밀번호의 사용 기간은 별도 항목이다.

③ O — /etc/shadow의 다섯 번째 필드는 **비밀번호 최대 사용 기간**이다. 마지막 변경일로부터 비밀번호를 다시 변경해야 할 때까지의 기간을 일수로 지정한다.

④ O — /etc/shadow의 세 번째 필드는 **비밀번호 최종 변경일**이다. 마지막으로 비밀번호를 변경한 날짜를 1970년 1월 1일부터 지난 일수로 저장한다.

NoteBase

문 20. 침입탐지시스템(Intrusion Detection System)에서 가장 적절하지 않은 것은?

① 합법적 사용자를 침입자로 판단하게 되는 긍정오류(False Positive)가 발생할 수 있다.

② 침입자를 합법적 사용자로 판단하게 되는 부정오류(False Negative)가 발생할 수 있다.

③ 침입탐지시스템은 데이터 수집원에 따라 네트워크 기반과 호스트 기반 등으로 분류한다.

④ 침입탐지시스템은 패킷을 차단하며, DMZ(DeMilitarized Zone)에서만 설치가 가능하다.

정답 4번

간단한 해설

IDS는 침입 징후를 탐지하고 알리는 시스템이며, **DMZ에서만 설치할 수 있는 것은 아니다**. 직접 차단 기능과 설치 위치를 잘못 설명한 ④가 정답이다.

선지별 해설

① O: 침입탐지에서 긍정(Positive)은 침입이 있다고 판단했다는 뜻이다. 실제로는 정상인데 침입으로 경보를 내면 **정상을 침입으로 오탐**한 긍정오류이다. 합법적인 활동도 탐지 규칙에 걸리면 이러한 오류가 발생할 수 있다.

② O: 부정(Negative)은 침입이 없다고 판단했다는 뜻이다. 실제 침입을 정상으로 판단하여 놓치면 **침입을 정상으로 미탐**한 부정오류이다. 탐지 규칙이나 분석 범위가 공격을 포착하지 못할 때 발생할 수 있다.

③ O: 네트워크 기반 IDS는 패킷 등 네트워크 트래픽을, 호스트 기반 IDS는 운영체제·응용프로그램 로그나 파일 변경 등 개별 호스트의 정보를 분석한다. 이는 **탐지에 사용하는 데이터의 수집원**에 따른 분류이다.

④ X: IDS의 기본 기능은 침입 징후의 **탐지·기록·경보**이며, 패킷을 직접 차단하는 방지 기능은 일반적으로 IPS와 구별하여 설명한다. IDS의 탐지 결과를 방화벽 등과 연계할 수는 있다. 또한 설치 위치는 **DMZ로 제한되지 않는다**. 감시 목적에 따라 내부망의 주요 구간이나 개별 호스트에도 배치할 수 있다.

따라서 가장 적절하지 않은 설명은 ④이다.

NoteBase