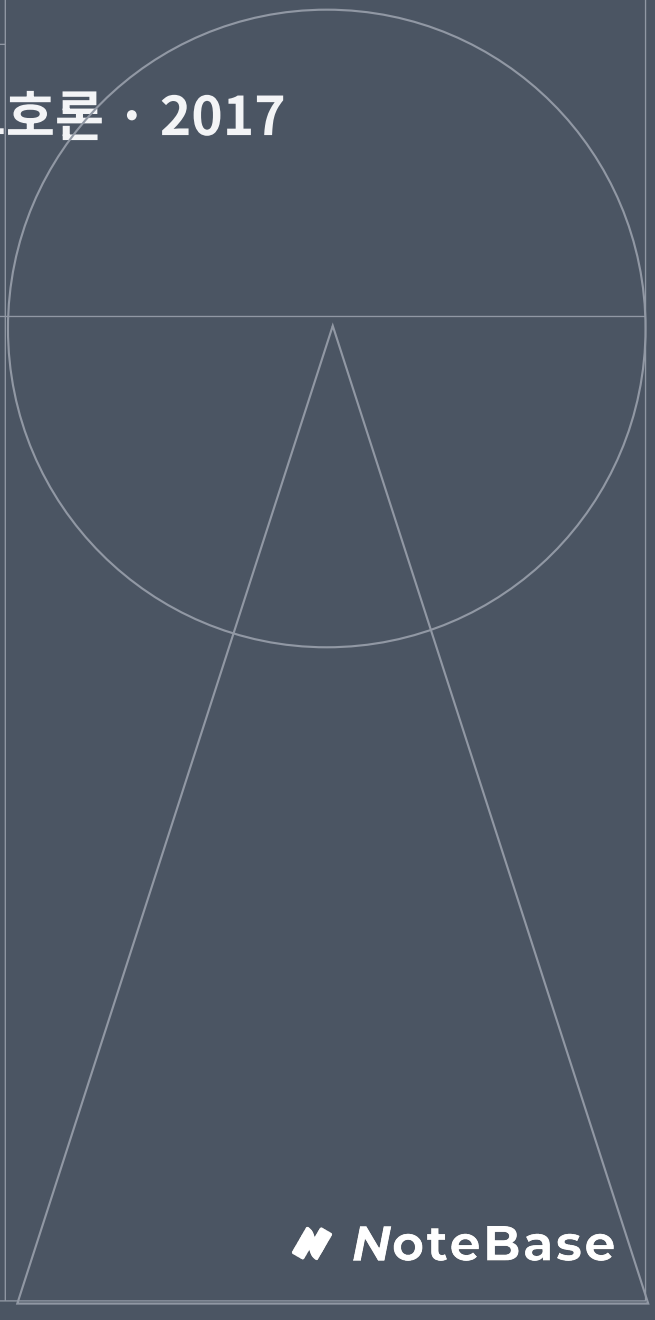
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2017



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2017

공무원/국회직/9급 · 정보보호론 · 2017

1. 다음 중 정보 보안 시스템을 설계하거나 운영할 때의 목표로 옳지 않은 것은?

① 기밀성 보장
② 무결성 보장
③ 가용성 보장
④ 책임회피성 보장
⑤ 사용자 인증

정답 4번

출제 포인트

정보 보안의 기본 목표와 보안이 지향하지 않는 개념을 구별하는 문제이다.

핵심 개념

기밀성은 허가받지 않은 정보 공개를 막는 속성이고, 무결성은 정보가 허가 없이 변경·삭제되지 않도록 정확성과 완전성을 지키는 속성이며, 가용성은 정당한 사용자가 필요할 때 정보와 시스템을 이용할 수 있게 하는 속성이다. 사용자 인증은 접근 주체가 주장하는 신원이 맞는지 확인하는 기능이다. 또한 보안은 행위의 주체와 책임을 추적할 수 있게 해야 하므로 책임 회피를 보장하는 것이 아니라 책임추적성과 부인방지성을 확보하는 방향으로 설계한다.

선지별 해설

① O — 기밀성 보장은 권한 없는 자에게 정보가 노출되는 것을 막는 정보 보안의 기본 목표이다.
② O — 무결성 보장은 정보가 무단으로 변경되거나 삭제되지 않도록 정확성과 완전성을 유지하는 기본 목표이다.
③ O — 가용성 보장은 정당한 사용자가 필요한 시점에 정보와 시스템을 정상적으로 이용할 수 있게 하는 기본 목표이다.
④ X — 틀린 표현은 '책임회피성 보장'이다. 보안 시스템은 사용자가 자신의 행위에 대한 책임을 피하게 하는 것이 아니라 행위 주체를 식별하고 추적할 수 있도록 책임추적성을 보장해야 한다.
⑤ O — 사용자 인증은 사용자가 주장하는 신원이 맞는지 검증하여 비인가자의 접근을 차단하는 보안상의 목표이자 핵심 기능이다.

NoteBase

오답 포인트

④의 '책임회피성'을 익숙한 보안 용어인 '책임추적성'으로 잘못 읽기 쉽다. 정보 보안은 책임 회피를 허용하는 것이 아니라 누가 어떤 행위를 했는지 확인할 수 있게 한다.

다시 나오면 이렇게 판단

각 선지가 정보의 비밀·정확성·이용 가능성·사용자 신원 확인·행위 책임 확인을 강화하는지 판단한다.
행위자의 책임을 숨기거나 회피하게 하는 표현은 보안 목표에 반한다.

암기 포인트

보안은 기밀성·무결성·가용성을 지키고 사용자를 인증하며 책임을 추적한다. 책임을 회피하게 하지는 않는다.

NoteBase

2. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은?

① 공개된 채널을 통하여 서로 정보를 교환하는 것만으로 공통의 비밀키를 만들어 낼 수 있다.
② 부인방지를 제공하는 전자서명이 가능하다.
③ 인수분해 문제에 기반한 알고리즘이다.
④ 중간자 공격을 수행하는 것이 불가능하다.
⑤ 키 생성 시 사용된 난수가 노출되어도 비밀키는 안전하다.

정답 1번

출제 포인트

Diffie-Hellman 키 교환의 기능, 수학적 기반, 인증 제공 여부, 중간자 공격 가능성, 비밀 지수 노출의 영향을 구별하는 문제이다.

핵심 개념

Diffie-Hellman 키 교환은 각 참여자가 자신의 비밀값은 공개하지 않고 공개값만 교환하여 동일한 공유 비밀을 계산하는 방식이다. 이 방식의 안전성은 이산대수 문제의 어려움과 관련되지만, 기본 방식 자체는 상대방의 신원을 인증하지 않으므로 중간자 공격에 취약하다. 키 생성에 사용한 비밀 난수인 개인 지수가 노출되면 공격자가 공유 비밀을 계산할 수 있다.

선지별 해설

① O — 공개 채널에서는 각자의 공개값만 교환하고, 각자는 자신의 비밀값과 상대방의 공개값을 이용해 같은 공유 비밀을 계산할 수 있다. 공통 비밀 자체를 공개 채널로 보내지 않는다는 점이 핵심이다.
② X — 틀린 표현은 '부인방지를 제공하는 전자서명이 가능하다'이다. 기본 Diffie-Hellman은 키 합의 기능만 제공하며 전자서명이나 부인방지 기능을 제공하지 않는다. 올바르게는 전자서명 등 별도의 인증 기법을 결합해야 상대 인증과 부인방지 기능을 확보할 수 있다.
③ X — 틀린 표현은 '인수분해 문제에 기반'이다. Diffie-Hellman의 안전성은 인수분해 문제가 아니라 유한군에서의 이산대수 문제 및 관련 계산 문제의 어려움에 기반한다. 올바르게는 '이산대수 문제에 기반한 알고리즘이다'라고 해야 한다.
④ X — 틀린 표현은 '중간자 공격을 수행하는 것이 불가능하다'이다. 기본 Diffie-Hellman은 통신 상대를 인증하지 않으므로 공격자가 양쪽과 각각 키 교환을 수행하는 중간자 공격이 가능하다. 올바르게는 인증서, 전자서명, 사전 공유키 등으로 교환 메시지를 인증해야 중간자 공격을 방지할 수 있다.
⑤ X — 틀린 표현은 '난수가 노출되어도 비밀키는 안전하다'이다. 키 생성에 쓰인 비밀 난수, 즉 개인 지수가 노출되면 공개된 상대방의 값과 결합하여 공유 비밀을 계산할 수 있다. 올바르게는 키 생성용 비밀 난수를 안전하게 보호해야 한다.

NoteBase

오답 포인트

공개 채널을 사용한다는 사실을 '아무 값이나 공개되어도 안전하다'는 뜻으로 오해하기 쉽다. 공개되는 것은 교환용 공개값이고, 개인 지수로 쓰이는 난수는 비밀이어야 한다. 또한 Diffie-Hellman은 키 합의 방식일 뿐 상대 인증이나 전자서명 기능까지 자동으로 제공하지 않는다.

다시 나오면 이렇게 판단

Diffie-Hellman 선지는 세 기준으로 판단한다. 공개값을 교환해 공유 비밀을 만든다는 설명은 맞고, 수학적 기반은 이산대수이며, 기본 방식에 인증 기능이 없으므로 중간자 공격이 가능하다. 개인 지수나 그 생성에 사용한 비밀 난수가 노출되면 안전하지 않다.

암기 포인트

DH는 '공개값 교환·이산대수 기반·인증 없음'이며, 인증이 없으면 중간자 공격에 취약하다.

NoteBase

3. OWASP(The Open Web Application Security Project)에서 2013년에 발표한 10대 웹 취약점에 속하지 않는 것은?

① 인젝션
② 크로스 사이트 요청 변조
③ 인증 및 세션 관리 취약점
④ 취약한 간접 객체 참조
⑤ 검증되지 않은 리다이렉트 및 포워드

정답 4번

출제 포인트

OWASP가 2013년에 발표한 10대 웹 애플리케이션 보안 취약점의 구성 항목을 정확히 구별하는 문제이다.

핵심 개념

OWASP Top 10은 웹 애플리케이션에서 중요하게 다루어야 할 보안 위험을 10개 범주로 정리한 목록이다. 2013년 목록에는 인젝션, 크로스 사이트 요청 변조, 인증 및 세션 관리 취약점, 안전하지 않은 직접 객체 참조, 검증되지 않은 리다이렉트 및 포워드 등이 포함된다. 핵심 구별어는 객체 참조 항목의 '직접'이다.

선지별 해설

① O — 인젝션은 OWASP Top 10 2013에 포함된다. 명령이나 질의의 일부로 신뢰할 수 없는 데이터가 삽입되어 의도하지 않은 동작을 일으키는 취약점이다.
② O — 크로스 사이트 요청 변조(CSRF)는 OWASP Top 10 2013에 포함된다. 인증된 사용자가 원하지 않는 요청을 보내도록 유도하는 공격이다.
③ O — 인증 및 세션 관리 취약점은 OWASP Top 10 2013에 포함된다. 인증 정보나 세션 식별자의 관리 실패로 계정이나 세션이 탈취될 수 있는 취약점이다.
④ X — 틀린 표현은 '취약한 간접 객체 참조'이다. 2013년 목록의 실제 항목은 '안전하지 않은 직접 객체 참조(Insecure Direct Object References)'이며, 사용자가 입력한 객체 식별자로 내부 객체에 직접 접근할 때 권한 검사가 미흡한 위험을 말한다.
⑤ O — 검증되지 않은 리다이렉트 및 포워드는 OWASP Top 10 2013에 포함된다. 목적지를 충분히 검증하지 않아 사용자가 악성 사이트로 이동하거나 부적절한 내부 경로로 전달될 수 있는 취약점이다.

오답 포인트

④는 '객체 참조'라는 익숙한 표현을 유지하면서 '직접'을 '간접'으로 바꾼 함정이다. 문항이 '속하지 않는 것'을 묻는 부정형이라는 점도 함께 확인해야 한다.

NoteBase

다시 나오면 이렇게 판단

OWASP Top 10의 항목명은 핵심 명사를 기준으로 대조한다. 객체 참조가 나오면 2013년 항목의 정확한 표현이 ‘안전하지 않은 직접 객체 참조’인지 확인하고, 문두의 ‘속하지 않는’이라는 부정 조건을 마지막에 적용한다.

암기 포인트

2013년 객체 참조 항목은 ‘간접’이 아니라 ‘직접’이다.

NoteBase

4. 다음 중 TCP 세션 하이재킹에 대한 설명으로 옳은 것은?

① 서버와 클라이언트의 통신에서 TCP의 송신 포트 제어에 문제가 발생하도록 공격한다.
② 서버와 클라이언트의 통신에서 TCP의 ACK 넘버 제어에 문제가 발생하도록 공격한다.
③ 서버와 클라이언트의 통신에서 TCP의 시퀀스 넘버 제어에 문제가 발생하도록 공격한다.
④ 서버와 클라이언트의 통신에서 TCP의 수신 포트 제어에 문제가 발생하도록 공격한다.
⑤ 서버와 클라이언트의 통신에서 TCP의 체크섬 제어에 문제가 발생하도록 공격한다.

정답 3번

출제 포인트

TCP 세션 하이재킹이 이미 성립된 연결을 가로채기 위해 악용하는 TCP 헤더의 핵심 제어값을 묻는 문제이다.

핵심 개념

TCP 세션 하이재킹은 공격자가 정상 통신 당사자인 것처럼 패킷을 주입하여 이미 설정된 TCP 연결을 탈취하는 공격이다. TCP는 수신한 바이트의 순서를 시퀀스 넘버로 확인하므로, 공격자는 정상 세그먼트로 받아들여질 시퀀스 넘버를 예측하거나 통신 흐름을 교란한다.
시퀀스 넘버는 전송 데이터의 순서와 수신 가능 범위를 판단하는 값이고, ACK 넘버는 상대에게 다음에 받을 바이트의 번호를 알리는 확인 응답값이다. 포트 번호는 통신 종단의 응용 프로세스를 식별하며, 체크섬은 전송 중 오류를 검출한다.

선지별 해설

① X — 송신 포트 제어가 공격의 핵심이라는 표현이 틀리다. 송신 포트는 통신 종단의 응용 프로세스를 식별하는 값이며, 올바르게는 TCP의 시퀀스 넘버 제어에 문제가 발생하도록 공격한다고 해야 한다.
② X — ACK 넘버 제어가 공격의 핵심이라는 표현이 틀리다. ACK 넘버는 상대에게 다음에 받을 바이트 번호를 알리는 확인 응답값이며, 올바르게는 TCP의 시퀀스 넘버를 예측·조작하여 정상 패킷처럼 받아들여지게 한다고 해야 한다.
③ O — TCP 세션 하이재킹은 정상 연결의 시퀀스 넘버를 예측하거나 통신 흐름을 교란하여 공격 패킷을 정상 세그먼트처럼 수용하게 만드는 공격이다.
④ X — 수신 포트 제어가 공격의 핵심이라는 표현이 틀리다. 수신 포트 역시 통신 종단의 서비스를 식별하는 값이며, 올바르게는 TCP의 시퀀스 넘버 제어에 문제를 일으키는 공격이라고 해야 한다.
⑤ X — 체크섬 제어가 공격의 핵심이라는 표현이 틀리다. 체크섬은 세그먼트의 전송 오류를 검출하는 값이며, 올바르게는 유효한 체크섬을 갖춘 패킷에 적절한 시퀀스 넘버를 사용하여 세션을 가로챈다고 해야 한다.

NoteBase

오답 포인트

TCP 헤더의 모든 필드가 공격에 쓰일 수 있을 것처럼 보이지만, 이 문항의 핵심은 연결의 데이터 순서를 동기화하는 시퀀스 넘버이다. ACK 넘버는 시퀀스 넘버와 함께 흐름에 관여하므로 특히 혼동하기 쉽지만, 세션 하이재킹의 대표적인 공격 지점은 시퀀스 넘버의 예측과 조작이다.

다시 나오면 이렇게 판단

이미 성립된 TCP 연결에 공격 패킷을 정상 데이터처럼 끼워 넣는 상황이면 수신 측이 패킷의 순서를 인정하는 기준인 시퀀스 넘버를 먼저 판단한다. 포트는 프로세스 식별, ACK 넘버는 수신 확인, 체크섬은 오류 검출로 구분한다.

암기 포인트

TCP 세션 하이재킹의 핵심은 시퀀스 넘버 예측·조작이다.

NoteBase

5. <보기>는 XSS(Cross-site Scripting) 공격을 수행하기 위한 각 단계들을 나타낸다. ㄱ~ㅁ을 순서에 맞게 나열한 것으로 옳은 것은?

<보 기>

ㄱ. 사용자 시스템에서 XSS 코드가 실행된다.

ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.

ㄷ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.

ㄹ. 결과가 공격자에게 전달된다.

ㅁ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.

① ㄴ-ㄱ-ㄷ-ㄹ-ㅁ

② ㄴ-ㄱ-ㄹ-ㄷ-ㅁ

③ ㄴ-ㄷ-ㅁ-ㄱ-ㄹ

④ ㄷ-ㄴ-ㄱ-ㅁ-ㄹ

⑤ ㄷ-ㄴ-ㅁ-ㄱ-ㄹ

정답 5번

출제 포인트

이 문제는 저장형 XSS 공격에서 공격자가 악성 스크립트를 게시판에 저장한 뒤 사용자의 브라우저에서 실행되어 결과가 공격자에게 전달되기까지의 순서를 묻는 문제이다.

올바른 순서

ㄷ → ㄴ → ㅁ → ㄱ → ㄹ

1. ㄷ — 공격자가 XSS 코드를 포함한 게시판 글을 웹 서버에 저장한다.
2. ㄴ — 웹 사용자가 공격자가 작성한 게시판 글에 접근한다.
3. ㅁ — 웹 서버가 XSS 코드를 포함한 게시판 글을 사용자에게 전달한다.
4. ㄱ — 전달된 글에 포함된 XSS 코드가 사용자 시스템의 브라우저에서 실행된다.
5. ㄹ — 실행 결과가 공격자에게 전달된다.

왜 이 순서인가: 공격 글이 먼저 서버에 저장되어야 사용자가 접근할 수 있고, 서버가 해당 글을 사용자에게 전달해야 사용자 측에서 코드가 실행될 수 있기 때문이다. 결과 전달은 코드 실행 뒤에 일어난다.

NoteBase

선지별 해설

① X — ㄴ → ㄱ에서 사용자가 글에 접근하자마자 코드가 실행되는 것으로 배열했으나, 그 전에 공격 글의 서버 저장(ㄷ)과 서버에서 사용자로의 전달(ㅁ)이 필요하다. 틀린 순서 ㄴ → ㄱ → ㄷ → ㄹ → ㅁ은 올바르게 ㄷ → ㄴ → ㅁ → ㄱ → ㄹ로 고쳐야 한다.
② X — 코드 실행(ㄱ)과 결과 전달(ㄹ)을 공격 글의 서버 저장(ㄷ) 및 사용자 전달(ㅁ)보다 앞에 두었다. 실행할 코드가 담긴 글이 먼저 저장되고 전달되어야 하므로, ㄴ → ㄱ → ㄹ → ㄷ → ㅁ은 올바르게 ㄷ → ㄴ → ㅁ → ㄱ → ㄹ로 고쳐야 한다.
③ X — 사용자 접근(ㄴ)을 공격 글의 서버 저장(ㄷ)보다 앞에 두었다. 저장형 XSS에서는 공격자가 악성 코드를 포함한 글을 서버에 먼저 저장한 다음 사용자가 그 글에 접근하므로, ㄴ → ㄷ → ㅁ → ㄱ → ㄹ은 올바르게 ㄷ → ㄴ → ㅁ → ㄱ → ㄹ로 고쳐야 한다.
④ X — 코드 실행(ㄱ)을 웹 서버가 게시판 글을 사용자에게 전달하는 단계(ㅁ)보다 앞에 두었다. 사용자 브라우저가 글을 전달받아야 그 안의 코드가 실행되므로, ㄷ → ㄴ → ㄱ → ㅁ → ㄹ은 올바르게 ㄷ → ㄴ → ㅁ → ㄱ → ㄹ로 고쳐야 한다.
⑤ O — 공격 글 저장(ㄷ), 사용자 접근(ㄴ), 서버의 글 전달(ㅁ), 사용자 측 코드 실행(ㄱ), 결과의 공격자 전달(ㄹ) 순서로 선후관계가 모두 맞는다.

오답 포인트

사용자의 글 접근(ㄴ)과 웹 서버의 글 전달(ㅁ)을 같은 단계처럼 보는 것이 함정이다. 사용자가 글을 요청하여 접근한 뒤 웹 서버가 응답으로 글을 전달하고, 그 다음 사용자 브라우저에서 XSS 코드가 실행된다. 또한 저장형 XSS이므로 사용자 접근보다 공격 글의 서버 저장이 먼저이다.

다시 나오면 이렇게 판단

저장형 XSS의 순서는 공격자의 서버 저장 → 사용자의 요청·접근 → 서버의 악성 콘텐츠 전달 → 사용자 브라우저의 스크립트 실행 → 정보나 실행 결과의 공격자 전달이라는 원인과 결과의 흐름으로 판단한다.

암기 포인트

저장형 XSS는 저장 → 접근 → 전달 → 실행 → 유출 순서이다.

NoteBase

6. ECC(Elliptic Curve Cryptography) 암호시스템에 대한 설명으로 옳지 않은 것은?

① 타원곡선 상의 이산대수 문제에 기반을 둔다.
② 키 교환, 암호화, 전자서명에 모두 사용 가능하다.
③ RSA보다 짧은 공개키를 이용하여 비슷한 수준의 보안레벨을 제공한다.
④ 임베디드 플랫폼 등과 같은 경량 응용분야에는 적합하지 않다.
⑤ 비슷한 수준의 보안레벨에서는 RSA보다 전자서명 생성 속도가 빠르다.

정답 4번

출제 포인트

이 문제는 ECC의 안전성 기반, 활용 범위, 키 길이와 연산 효율의 특징을 묻는 문제이다.

핵심 개념

ECC는 타원곡선 위의 이산로그 문제를 이용하는 공개키 암호 방식이다. RSA와 비슷한 보안 수준을 더 짧은 키로 구현할 수 있어 저장 공간, 통신량, 전력과 연산 자원이 제한된 임베디드·모바일 환경에 적합하다. 타원곡선 기반 방식은 키 교환, 암호화, 전자서명에 활용된다.

선지별 해설

① O — ECC의 안전성은 타원곡선 군에서의 이산로그 문제를 풀기 어렵다는 점에 기반한다.
② O — 타원곡선 기반 알고리즘은 키 교환, 공개키 암호화, 전자서명에 각각 활용될 수 있다.
③ O — ECC는 RSA보다 훨씬 짧은 키로 비슷한 수준의 보안성을 제공하므로 키 저장 공간과 전송량을 줄일 수 있다.
④ X — 틀린 표현은 '경량 응용분야에는 적합하지 않다'이다. 올바르게는 ECC가 짧은 키와 비교적 작은 자원 요구량을 가지므로 임베디드 플랫폼과 같은 경량 응용분야에 적합하다고 해야 한다.
⑤ O — 비슷한 보안 수준에서 ECC 계열 전자서명은 일반적으로 RSA보다 서명 생성이 빠르고 짧은 키와 서명을 사용할 수 있다. 다만 검증 속도까지 항상 ECC가 더 빠르다는 뜻은 아니다.

오답 포인트

③의 '짧은 공개키'라는 특징을 보안성이 낮다는 의미로 오해하면 ④를 놓치기 쉽다. ECC의 짧은 키는 같은 보안 수준을 더 적은 자원으로 달성한다는 장점이므로 경량 환경에 오히려 유리하다.

NoteBase

다시 나오면 이렇게 판단

ECC 관련 선지는 ‘타원곡선 이산로그 문제’, ‘RSA 대비 짧은 키’, ‘경량 환경에 적합’, ‘키 교환·암호화·전자서명에 활용’이라는 기준으로 판단한다. 같은 보안 수준에서 키가 짧다는 표현은 장점으로 본다.

암기 포인트

ECC는 짧은 키로 높은 보안성을 제공하므로 경량·임베디드 환경에 적합하다.

NoteBase

7. <보기>에서 설명하는 해시함수(H)의 특성으로 옳은 것은?

<보 기>

주어진 메시지 x에 대해, H(x)=H(y)인 x≠y를 만족하는 두 개의 메시지 x, y를 찾는 것이 어려울 때, 해시함수가 이 성질을 가지고 있다고 한다.

① Second Pre-image Resistance
② Collision Resistance
③ Integrity
④ Onewayness
⑤ Uniform Distribution

정답 1번

출제 포인트

이 문제는 주어진 메시지와 같은 해시값을 갖는 다른 메시지를 찾기 어려운 성질이 제2 역상 저항성임을 구별하는 문제이다.

핵심 개념

제2 역상 저항성(Second Pre-image Resistance): 주어진 메시지 x에 대하여 $H(x) = H(y)$이면서 $x \neq y$인 다른 메시지 y를 찾기 어려운 성질이다. / 키워드: 주어진 메시지와 같은 해시값
충돌 저항성(Collision Resistance): 특정 메시지를 미리 주지 않은 상태에서 해시값이 같은 임의의 서로 다른 두 메시지를 찾기 어려운 성질이다. / 키워드: 임의의 두 메시지
역상 저항성·일방향성(Pre-image Resistance·Onewayness): 주어진 해시값으로부터 그 해시값을 만드는 입력 메시지를 찾기 어려운 성질이다. / 키워드: 해시값에서 입력 찾기

NoteBase

선지별 해설

① O — 주어진 메시지 x와 같은 해시값을 갖는 다른 메시지 y를 찾기 어렵다는 설명은 제2 역상 저항성(Second Pre-image Resistance)의 정의와 일치한다.
② X — 틀린 표현은 Collision Resistance이다. 충돌 저항성은 주어진 x를 기준으로 삼는 것이 아니라, $H(x) = H(y)$를 만족하는 임의의 서로 다른 두 메시지 x, y를 찾기 어려운 성질이다.
③ X — 틀린 표현은 Integrity이다. 무결성은 정보가 허가 없이 변경되거나 훼손되지 않았음을 뜻하며, 제시된 해시함수의 계산적 난이도 성질은 제2 역상 저항성이다.
④ X — 틀린 표현은 Onewayness이다. 일방향성은 주어진 해시값 h에 대해 $H(x) = h$인 입력 x를 찾기 어려운 성질이고, 주어진 입력과 같은 해시값을 갖는 다른 입력을 찾기 어려운 성질은 제2 역상 저항성이다.
⑤ X — 틀린 표현은 Uniform Distribution이다. 균등 분포는 해시 출력값이 가능한 범위에 고르게 분포하는 성질이고, 제시된 성질은 주어진 메시지의 다른 충돌 상대를 찾기 어려운 제2 역상 저항성이다.

오답 포인트

②의 충돌 저항성과 ①의 제2 역상 저항성은 모두 서로 다른 두 메시지의 해시값이 같다는 조건을 사용한다. 그러나 문제에서 한 메시지 x가 먼저 주어진다는 표현이 제2 역상 저항성을 결정한다.

다시 나오면 이렇게 판단

입력 하나가 먼저 주어지고 같은 해시값의 다른 입력을 찾는 문제이면 제2 역상 저항성, 아무 입력도 정해지지 않은 채 같은 해시값의 임의의 두 입력을 찾는 문제이면 충돌 저항성, 해시값에서 원래 입력을 찾는 문제이면 역상 저항성으로 판단한다.

암기 포인트

주어진 입력의 짝 찾기는 제2 역상, 임의의 한 쌍 찾기는 충돌, 해시값에서 입력 찾기는 역상이다.

NoteBase

8. 시스템 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM (Trusted Platform Module)이 있다. TPM이 지원하지 않는 기능은?

① 암호키 생성 및 저장
② 인증된 부트(Authenticated Boot)
③ 디바이스 및 플랫폼 인증
④ 원격 검증(Remote Attestation)
⑤ 감사(Audit)

정답 5번

출제 포인트

TPM이 하드웨어 신뢰 기반으로 제공하는 암호키 보호·플랫폼 무결성 검증·인증 기능과 일반적인 보안 감사 기능을 구별하는 문제이다.

핵심 개념

TPM은 암호키를 안전하게 생성·보관하고, 부팅 구성요소의 측정값을 저장하며, 그 측정값과 TPM이 보호하는 키를 이용해 장치·플랫폼의 상태와 신원을 증명하는 보안 모듈이다.
감사는 시스템에서 발생한 보안 관련 사건을 기록하고 사후에 추적·검토하는 기능으로, TPM의 고유 기능이 아니라 주로 운영체제나 보안 소프트웨어가 담당한다.

선지별 해설

① O — TPM은 난수 생성과 암호 연산을 지원하며 암호키를 TPM 내부에 안전하게 생성·저장할 수 있다.
② O — TPM은 부팅 과정의 구성요소를 측정하여 플랫폼 구성 레지스터에 누적하고, 이 값을 바탕으로 부팅 무결성을 확인하는 인증된 부팅을 지원한다.
③ O — TPM이 보호하는 고유 키와 자격 증명은 장치의 신원을 증명하고 플랫폼이 신뢰할 수 있는 상태인지 인증하는 데 사용된다.
④ O — 원격 검증은 TPM에 저장된 플랫폼 측정값을 서명하여 원격 상대방에게 플랫폼 상태를 증명하는 대표적 기능이다.
⑤ X — 틀린 표현은 '감사(Audit)를 TPM이 지원하는 기능'이라고 본 부분이다. 올바르게는 감사는 보안 사건을 기록하고 사후 검토하는 운영체제·응용 보안 기능이며, TPM은 그 과정에 필요한 키 보호나 무결성 증명 정보를 제공할 수 있을 뿐 감사 자체를 수행하지 않는다.

오답 포인트

TPM이 보안 전반을 담당한다고 생각하면 ⑤도 기능으로 오인하기 쉽다. TPM의 핵심은 키 보호, 부팅 상태 측정, 장치·플랫폼 인증, 원격 검증이며 보안 로그의 기록·분석인 감사와는 역할이 다르다.

NoteBase

다시 나오면 이렇게 판단

선지가 키의 생성·보호, 부팅 무결성 측정, 플랫폼 신원 인증, 측정값을 이용한 원격 증명에 관한 것이면 TPM 기능으로 판단한다. 사건 로그의 기록·추적·사후 검토에 관한 것이면 감사 시스템의 기능으로 판단한다.

암기 포인트

TPM은 키 보호·측정·인증·원격 증명, 감사는 로그 기록·사후 검토이다.

NoteBase

9. 네트워크에서 서비스를 제공하는 서버 혹은 시스템은 동시 접속할 수 있는 사용자 수를 제한한다. 이러한 특성을 이용하여 다수의 존재하지 않는 사용자가 시스템에 접속한 것처럼 속여 다른 사용자가 서비스를 받지 못하게 하는 공격으로 옳은 것은?

① Ping of Death
② SYN Flooding
③ Boink
④ TearDrop
⑤ Smurf

정답 2번

출제 포인트

서버가 유지할 수 있는 동시 접속 자원을 고갈시켜 정상 사용자의 접속을 막는 서비스 거부 공격이 무엇인지 묻는 문제이다.

핵심 개념

SYN Flooding은 공격자가 출발지 주소를 위조한 SYN 패킷을 대량 전송하고 연결을 완성하지 않아, 서버에 다수의 반개방 연결을 쌓이게 하는 서비스 거부 공격이다. 서버의 연결 대기 큐와 같은 자원이 소진되면 정상 사용자의 새 연결이 거부된다.
Ping of Death·Boink·TearDrop은 비정상적인 패킷이나 조각 처리를 악용하는 공격이고, Smurf는 브로드캐스트와 위조된 출발지 주소를 이용해 ICMP 응답을 피해자에게 증폭·집중시키는 공격이다.

NoteBase

선지별 해설

① X — Ping of Death는 허용 크기를 넘거나 비정상적으로 조작된 ICMP 패킷의 처리 과정에서 시스템 장애를 유발하는 공격이다. 틀린 표현은 '동시 접속 수 제한을 이용한다'는 대응 관계이며, 올바르게는 비정상적인 대형 ICMP 패킷 처리를 악용하는 공격이다.
② O — SYN Flooding은 위조한 출발지 주소로 SYN 패킷을 대량 전송하여 TCP 3-way handshake를 완료하지 않고 반개방 연결을 누적시킨다. 그 결과 서버의 연결 대기 자원이 고갈되어 정상 사용자가 접속하지 못하므로 지문에 해당한다.
③ X — Boink는 비정상적으로 조작된 분할 UDP 패킷의 처리 문제를 악용해 시스템 장애를 일으키는 공격이다. 틀린 표현은 '다수의 존재하지 않는 사용자가 접속한 것처럼 속인다'는 대응 관계이며, 올바르게는 비정상적인 분할 패킷 처리를 악용하는 공격이다.
④ X — TearDrop은 서로 겹치거나 잘못된 오프셋을 가진 IP 조각을 보내 재조립 과정의 오류를 유발하는 공격이다. 틀린 표현은 '동시 접속 자원을 소진한다'는 대응 관계이며, 올바르게는 IP 단편 재조립 취약점을 악용하는 공격이다.
⑤ X — Smurf는 피해자의 IP 주소를 출발지로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 응답이 피해자에게 집중되게 하는 증폭 공격이다. 틀린 표현은 '서버의 접속 대기 큐를 고갈시킨다'는 대응 관계이며, 올바르게는 브로드캐스트를 이용해 ICMP 트래픽을 증폭·반사하는 공격이다.

오답 포인트

문제의 핵심 표현은 '동시 접속할 수 있는 사용자 수'와 '존재하지 않는 사용자가 접속한 것처럼 속인다'이다. 이는 TCP 연결을 시작하는 SYN만 보내 반개방 상태를 쌓는 공격을 가리킨다. 출발지 주소 위조가 등장한다는 이유만으로 Smurf를 고르면 안 된다. Smurf는 위조된 주소와 브로드캐스트를 이용한 ICMP 증폭 공격이다.

다시 나오면 이렇게 판단

반개방 연결·접속 대기 큐·3-way handshake 미완료·SYN 대량 전송이 보이면 SYN Flooding으로 판단한다. 비정상 대형 ICMP 패킷은 Ping of Death, 겹치는 IP 조각은 TearDrop, 브로드캐스트를 통한 ICMP 증폭은 Smurf로 구분한다.

암기 포인트

SYN Flooding은 SYN만 보내 연결 자리를 차지하는 공격이다.

NoteBase

10. 메시지 인증 코드(MAC: Message Authentication Code)에 대한 설명으로 옳지 않은 것은?

① MAC 검증을 통하여 메시지의 위조 여부를 판별할 수 있다.
② MAC을 이용하여 송신자 인증이 가능하다.
③ MAC 검증을 위해서는 메시지와 공개키가 필요하다.
④ 해시함수를 이용하여 MAC을 생성할 수 있다.
⑤ MAC 생성자와 검증자는 동일한 키를 사용한다.

정답 3번

출제 포인트

메시지 인증 코드(MAC)의 기능과 생성·검증에 사용하는 키의 성격을 묻는 문제이다.

핵심 개념

MAC은 메시지와 송신자·수신자가 공유한 비밀키를 함께 사용해 만든 짧은 인증값이다. 수신자는 같은 비밀키로 MAC을 검증하여 메시지의 무결성과 송신자 인증을 확인할 수 있다. 일반적인 MAC은 공개키가 아니라 대칭키인 공유 비밀키를 사용하며, 해시함수에 비밀키를 결합한 HMAC도 MAC의 한 방식이다.

선지별 해설

① O — 메시지가 변조되거나 비밀키 없이 거짓 MAC이 붙으면 수신자가 계산한 MAC과 일치하지 않으므로 위조 여부를 판별할 수 있다.
② O — 올바른 MAC을 생성하려면 공유 비밀키를 알아야 하므로, MAC 검증을 통해 그 키를 공유한 송신자가 보낸 메시지인지 인증할 수 있다.
③ X — 틀린 표현은 '공개키가 필요하다'이다. 올바르게는 MAC 검증에 송신자와 수신자가 공유한 비밀키가 필요하다.
④ O — 해시함수에 비밀키를 결합하는 HMAC과 같이 해시함수를 이용해 MAC을 생성할 수 있다.
⑤ O — 일반적인 MAC은 대칭키 방식이므로 MAC 생성자와 검증자가 동일한 공유 비밀키를 사용한다.

오답 포인트

③의 '공개키'를 전자서명과 혼동하기 쉽다. MAC은 공유 비밀키를 사용하는 대칭키 기반 인증 방식이고, 전자서명은 개인키로 서명하고 공개키로 검증한다.

다시 나오면 이렇게 판단

생성자와 검증자가 같은 비밀키를 공유하면 MAC, 서로 다른 개인키와 공개키를 사용하면 전자서명으로 구분한다. MAC 문항에서는 무결성·송신자 인증·공유 비밀키를 핵심 기준으로 판단한다.

NoteBase

암기 포인트

MAC은 메시지와 공유 비밀키로 생성하며, 같은 비밀키로 무결성과 송신자를 검증한다.

NoteBase

11. 수동적 보안 공격에 해당하는 것을 <보기>에서 모두 고르면?

<보 기>

ㄱ. 신분 위장 ㄴ. 메시지 변경 ㄷ. 도청
ㄹ. 트래픽 분석 ㅁ. 서비스 거부

① ㄱ, ㄴ
② ㄴ, ㅁ
③ ㄷ, ㄹ
④ ㄱ, ㄷ, ㄹ
⑤ ㄷ, ㄹ, ㅁ

정답 3번

출제 포인트

수동적 보안 공격과 능동적 보안 공격을 공격자가 시스템이나 데이터에 변화를 일으키는지에 따라 구분하는 문제이다.

핵심 개념

수동적 공격은 정보를 몰래 관찰하거나 수집하지만 데이터와 시스템 상태를 변경하지 않는 공격이다. 도청과 트래픽 분석이 이에 해당한다.
능동적 공격은 데이터나 통신 상태를 변경하거나 정상적인 서비스를 방해하는 공격이다. 신분 위장, 메시지 변경, 서비스 거부가 이에 해당한다.

선지별 해설

① X — ㄱ 신분 위장과 ㄴ 메시지 변경은 모두 공격자가 통신 내용이나 행위에 개입하는 능동적 공격이다. 틀린 조합 'ㄱ, ㄴ'은 'ㄷ, ㄹ'로 고쳐야 한다.
② X — ㄴ 메시지 변경은 데이터를 변조하고, ㅁ 서비스 거부는 정상적인 서비스 이용을 방해하므로 모두 능동적 공격이다. 틀린 조합 'ㄴ, ㅁ'은 'ㄷ, ㄹ'로 고쳐야 한다.
③ O — ㄷ 도청은 통신 내용을 몰래 관찰하는 공격이고, ㄹ 트래픽 분석은 통신량·빈도·상대 등의 패턴을 수집하는 공격이다. 둘 다 데이터를 변경하지 않으므로 수동적 공격이다.
④ X — ㄷ 도청과 ㄹ 트래픽 분석은 수동적 공격이지만, ㄱ 신분 위장은 다른 주체인 것처럼 가장하여 통신에 개입하는 능동적 공격이다. 틀린 조합 'ㄱ, ㄷ, ㄹ'은 'ㄷ, ㄹ'로 고쳐야 한다.
⑤ X — ㄷ 도청과 ㄹ 트래픽 분석은 수동적 공격이지만, ㅁ 서비스 거부는 시스템의 가용성을 훼손하는 능동적 공격이다. 틀린 조합 'ㄷ, ㄹ, ㅁ'은 'ㄷ, ㄹ'로 고쳐야 한다.

NoteBase

오답 포인트

공격자가 몰래 수행한다는 일상적 의미만으로 수동적 공격을 판단하면 신분 위장을 잘못 포함하기 쉽다.
보안에서의 구분 기준은 은밀성 자체가 아니라 데이터·시스템 상태의 변경 또는 서비스 방해 여부이다.

다시 나오면 이렇게 판단

내용이나 통신 패턴을 관찰·수집하기만 하면 수동적 공격으로, 위장·변조·서비스 방해처럼 통신이나 시스템 상태에 변화를 일으키면 능동적 공격으로 판단한다.

암기 포인트

수동은 엿보기인 도청·트래픽 분석, 능동은 개입하기인 위장·변경·서비스 거부이다.

NoteBase

12. 디지털 포렌식(Digital Forensic)을 통해 획득된 증거가 법적인 효력을 갖기 위해서는 증거를 발견(Discovery), 기록(Recording), 획득(Collection), 보관(Preservation)하는 절차가 적절해야 한다. 이를 만족하기 위해 지켜야 하는 기본 원칙으로 옳지 않은 것은?

① 최량 증거의 원칙
② 재현의 원칙
③ 정당성의 원칙
④ 신속성의 원칙
⑤ 연계보관성의 원칙

정답 1번

출제 포인트

디지털 증거의 법적 효력을 확보하기 위해 수집·분석 과정에서 지켜야 하는 기본 원칙과, 법정에서 증거를 평가하는 원칙을 구별하는 문제이다.

핵심 개념

디지털 포렌식의 기본 원칙은 증거 취급 과정의 적법성과 신뢰성을 확보하는 기준이다. 재현성은 같은 조건과 절차에서 같은 분석 결과가 나와야 한다는 원칙이고, 정당성은 적법하고 정당한 절차와 방법으로 증거를 다루어야 한다는 원칙이다. 신속성은 변조·소실 가능성이 큰 디지털 증거를 적시에 확보·처리해야 한다는 원칙이며, 연계보관성은 발견부터 법정 제출까지 증거의 취급자·시점·방법·이동 내역이 끊김 없이 추적되어야 한다는 원칙이다. 반면 최량 증거의 원칙은 원본 등 가장 신뢰할 수 있는 증거를 우선한다는 증거법상의 관념으로, 이 문항에서 묻는 디지털 포렌식 수행의 기본 원칙에 해당하지 않는다.

NoteBase

선지별 해설

① X — '최량 증거의 원칙'은 원본 등 가장 신뢰할 수 있는 증거를 우선하는 증거법상의 관념이지, 디지털 포렌식 수행 과정의 기본 원칙은 아니다. 올바르게는 재현성·정당성·신속성·연계보관성과 같은 절차적 원칙을 기본 원칙으로 보아야 한다.
② O — 재현의 원칙은 동일한 조건과 방법으로 검증했을 때 동일한 결과가 나와야 한다는 원칙으로, 분석 결과의 신뢰성을 뒷받침한다.
③ O — 정당성의 원칙은 디지털 증거의 발견·수집·분석이 적법하고 정당한 절차와 방법에 따라 이루어져야 한다는 원칙이다.
④ O — 신속성의 원칙은 휘발되거나 변경되기 쉬운 디지털 증거를 소실 전에 신속하게 확보하고 처리해야 한다는 원칙이다.
⑤ O — 연계보관성의 원칙은 증거의 발견부터 수집·이송·보관·분석·법정 제출까지 모든 취급 내역을 기록하여 증거의 동일성과 무결성을 설명할 수 있어야 한다는 원칙이다.

오답 포인트

①의 '최량 증거'도 증거의 신뢰성과 관련된 표현이어서 포렌식 원칙처럼 보이는 것이 함정이다. 그러나 ②~⑤는 디지털 증거를 실제로 발견·수집·보관·분석하는 과정의 원칙이고, ①은 법정에서 어떤 증거를 우선할 것인지에 관한 증거법상의 관념이라는 차이가 있다.

다시 나오면 이렇게 판단

선지가 포렌식 작업의 방법과 이력 관리에 관한 것인지 확인한다. 적법한 방법, 같은 결과의 재현, 신속한 확보, 끊김 없는 취급 기록은 포렌식 수행 원칙이고, 원본·최량 증거의 우선은 법정의 증거 평가 관념으로 구별한다.

암기 포인트

포렌식 수행은 정당·재현·신속·연계보관, 최량 증거는 증거법상의 관념이다.

NoteBase

13. 와이파이(Wi-Fi) 보안 기술에 대한 설명으로 옳지 않은 것은?

① IEEE 802.11 표준 기반의 무선 랜 기술이다.
② WEP 방식은 현재 보안상 취약점이 발견되었다.
③ WEP 방식은 MAC(Media Access Control) 주소 인증 프로토콜을 사용한다.
④ WPA 방식은 TKIP(Temporal Key Integrity Protocol)를 사용한다.
⑤ WPA2 방식은 AES-CCMP(Counter Mode CBC-MAC Protocol)를 사용한다.

정답 3번

출제 포인트

Wi-Fi의 기반 표준과 WEP·WPA·WPA2가 사용하는 인증·암호화 기술의 차이를 묻는 문제이다.

핵심 개념

Wi-Fi는 IEEE 802.11 계열 표준에 기반한 무선 LAN 기술이다.
WEP는 초기 무선 보안 방식으로 RC4 기반 암호화를 사용하지만 여러 구조적 취약점 때문에 안전하지 않다.
WPA는 WEP를 보완하기 위해 TKIP를 사용하고, WPA2는 더 강한 AES-CCMP를 사용한다.
MAC 주소 인증은 단말의 MAC 주소를 허용 목록과 대조하는 접근 통제 방식이며 WEP 자체의 인증 프로토콜이 아니다.

선지별 해설

① O — Wi-Fi는 IEEE 802.11 표준 계열에 기반한 무선 LAN 기술이다.
② O — WEP는 키 관리와 암호화 방식 등에 구조적 취약점이 발견되어 현재 안전한 보안 방식으로 보지 않는다.
③ X — 틀린 표현은 'WEP 방식은 MAC 주소 인증 프로토콜을 사용한다'이다. 올바르게는 WEP는 공유키를 이용해 무선 구간의 인증과 암호화를 제공하는 초기 보안 방식이며, MAC 주소 인증은 WEP와 별개의 접근 통제 방식이다.
④ O — WPA는 WEP의 취약점을 보완하기 위해 TKIP를 사용하는 방식이다.
⑤ O — WPA2는 강한 기밀성과 무결성 보호를 제공하는 AES-CCMP를 사용한다.

오답 포인트

③은 무선 공유기에서 WEP 설정과 MAC 주소 필터링을 함께 사용할 수 있다는 점을 이용해 두 기능을 하나의 프로토콜처럼 섞은 선지이다. 함께 설정할 수 있다는 사실과 WEP가 MAC 주소 인증 프로토콜을 사용한다는 주장은 다르다.

NoteBase

다시 나오면 이렇게 판단

Wi-Fi 보안 방식은 ‘WEP－초기 방식·취약’, ‘WPA－TKIP’, ‘WPA2－AES-CCMP’로 연결하고, MAC 주소 필터링은 이 암호화 방식들과 별개의 접근 통제로 구분한다.

암기 포인트

WEP는 취약, WPA는 TKIP, WPA2는 AES-CCMP이며 MAC 주소 인증은 WEP와 별개이다.

NoteBase

14. 접근 제어 모델에 대한 설명으로 옳지 않은 것은?

① DAC(Discretionary Access Control)는 정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

② MAC(Mandatory Access Control)는 사용자 계정에 기반하며, 자원의 소유자가 다른 사용자의 보안 레벨을 수정할 수 있다.

③ BLP(Bell-LaPadula) 모델은 자신보다 높은 보안 레벨의 문서에 쓰기는 가능하지만, 보안 레벨이 낮은 문서에는 쓰기 권한이 없다.

④ BLP의 보안 목적은 기밀성이지만, Biba 모델은 정보의 무결성을 높이는 데 있다.

⑤ RBAC(Role Based Access Control)는 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

정답 2번

출제 포인트

이 문제는 DAC·MAC·RBAC의 권한 결정 기준과 BLP·Biba 모델의 보안 목적 및 정보 흐름 규칙을 구별하는 문제이다.

핵심 개념

DAC는 자원 소유자의 재량에 따라 접근 권한을 정하는 모델이다.
MAC는 주체의 보안 인가와 객체의 보안 등급을 비교하여 중앙 정책에 따라 접근을 강제하는 모델이다.
RBAC는 사용자의 개인 신분이 아니라 조직에서 맡은 역할에 권한을 부여하는 모델이다.
BLP는 기밀성 보호 모델로서 상위 등급 읽기 금지와 하위 등급 쓰기 금지를 적용한다. Biba는 무결성 보호 모델로서 하위 무결성 등급 읽기 금지와 상위 무결성 등급 쓰기 금지를 적용한다.

선지별 해설

① O — DAC에서는 정보 소유자가 자원의 보안 등급과 접근 권한을 재량적으로 정할 수 있으므로 옳다.
② X — 틀린 표현은 '사용자 계정에 기반'하고 '자원의 소유자가 다른 사용자의 보안 레벨을 수정할 수 있다'는 부분이다. MAC는 주체의 보안 인가와 객체의 보안 등급에 기반하며, 중앙에서 정한 강제 정책을 적용하므로 자원 소유자가 보안 레벨을 임의로 수정할 수 없다.
③ O — BLP의 별표 속성은 하위 보안 등급으로 쓰는 것을 금지한다. 따라서 자신보다 높은 등급에는 쓸 수 있지만 낮은 등급에는 쓸 수 없다는 설명은 옳다.
④ O — BLP는 정보가 낮은 등급으로 유출되지 않도록 기밀성을 보호하고, Biba는 신뢰도가 낮은 정보가 높은 무결성 영역을 오염시키지 않도록 무결성을 보호하므로 옳다.
⑤ O — RBAC는 사용자에게 직접 권한을 하나씩 부여하는 대신 조직 내 역할에 권한을 부여하고 사용자를 그 역할에 배정하므로 옳다.

NoteBase

오답 포인트

②는 MAC의 M을 '계정 중심 관리'로 오해하게 만든다. MAC의 핵심은 계정이나 소유자의 재량이 아니라 보안 인가·보안 등급과 중앙의 강제 정책이다. 또한 ③에서는 BLP의 쓰기 방향을 반대로 기억하기 쉽지만, 기밀성 보호를 위해 정보가 아래 등급으로 내려가는 쓰기를 막는다는 점이 핵심이다.

다시 나오면 이렇게 판단

권한 결정자가 소유자이면 DAC, 중앙 보안 정책과 등급 비교이면 MAC, 조직의 직무·역할이면 RBAC로 판단한다. 정보 흐름 모델은 BLP가 기밀성 때문에 하향 쓰기를 막고, Biba가 무결성 때문에 상향 쓰기를 막는다는 기준으로 구별한다.

암기 포인트

DAC는 소유자 재량, MAC는 등급에 따른 강제, RBAC는 역할 중심이다. BLP는 기밀성·하향 쓰기 금지, Biba는 무결성·상향 쓰기 금지이다.

NoteBase

15. <보기>에서 설명하는 블록암호 운영모드로 옳은 것은?

<보 기>

- '한 단계 앞의 암호 알고리즘의 출력을 암호화한 값'과 '평문 블록'을 XOR 연산하여 암호문 블록을 생성하는 운영모드이다.
- 암호화와 복호화가 같은 구조를 가지고 있다.
- 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트에만 에러가 발생한다.

① ECB
② CBC
③ CFB
④ OFB
⑤ CTR

정답 4번

출제 포인트

이 문제는 블록암호 운영모드 가운데 OFB의 출력 피드백 방식, 암·복호 구조, 전송 오류의 영향을 구별하는 문제이다.

핵심 개념

OFB(Output Feedback)는 블록암호의 이전 출력값을 다시 암호화하여 키 스트림을 만들고, 이를 평문 또는 암호문과 XOR하는 운영모드이다. 암호화와 복호화 모두 같은 키 스트림을 XOR하므로 구조가 같고, 암호문의 한 비트 오류는 복호화된 평문의 같은 위치 한 비트에만 영향을 준다.
ECB는 각 평문 블록을 독립적으로 암호화하고, CBC는 앞 암호문 블록을 다음 평문 블록에 연쇄하며, CFB는 앞 암호문을 피드백한다. CTR은 카운터 값을 암호화해 키 스트림을 만든다.

NoteBase

선지별 해설

① X — ECB는 각 블록을 서로 독립적으로 암호화하므로 이전 암호 알고리즘의 출력을 다시 암호화하는 피드백 과정이 없다. 또한 암호문 한 비트의 오류는 복호화 시 해당 평문 블록 전체에 불규칙하게 영향을 줄 수 있다. ‘ECB’가 아니라 ‘OFB’가 올바른 표현이다.
② X — CBC는 앞 암호문 블록과 현재 평문 블록을 XOR한 뒤 암호화한다. 암호문 비트 오류는 현재 평문 블록에 불규칙한 오류를 만들고 다음 평문 블록의 대응 비트에도 영향을 준다. ‘CBC’가 아니라 ‘OFB’가 올바른 표현이다.
③ X — CFB는 앞 암호문을 암호 알고리즘에 입력해 얻은 값과 평문을 XOR하며, 암호문 오류가 이후 구간에도 전파될 수 있다. 보기처럼 평문의 대응 비트에만 오류가 한정되는 모드는 CFB가 아니라 OFB이다.
④ O — OFB는 이전 출력값을 다시 암호화해 생성한 키 스트림과 평문을 XOR한다. 암·복호가 모두 같은 키 스트림과 XOR하는 구조이고, 암호문 한 비트 오류가 평문의 대응 비트에만 나타나므로 보기의 세 설명과 모두 일치한다.
⑤ X — CTR은 이전 출력을 피드백하지 않고 서로 다른 카운터 값을 암호화하여 키 스트림을 만든다. 암·복호 구조가 같고 오류가 대응 비트에만 생긴다는 특징은 비슷하지만, 보기의 ‘한 단계 앞의 암호 알고리즘의 출력’을 사용하는 모드는 CTR이 아니라 OFB이다.

오답 포인트

CTR도 암·복호 구조가 같고 비트 오류가 대응 비트에만 제한되므로 ⑤와 혼동하기 쉽다. 구별점은 키 스트림의 입력이다. 이전 암호 출력값을 되먹임하면 OFB이고, 증가하는 카운터 값을 넣으면 CTR이다.

다시 나오면 이렇게 판단

운영모드는 피드백 대상과 오류 전파 범위를 함께 확인한다. 이전 출력값을 피드백하고 암·복호에 같은 XOR 구조를 사용하며 오류가 대응 비트에만 머물면 OFB로 판단한다. 카운터를 암호화하면 CTR, 앞 암호문을 피드백하면서 오류가 뒤에도 전파되면 CFB로 구별한다.

암기 포인트

OFB는 출력(Output)을 피드백하고, CTR은 카운터(Counter)를 암호화한다. OFB의 암호문 비트 오류는 평문의 같은 비트에만 남는다.

NoteBase

16. 다음 중 캐싱(Caching) 장비가 응답하지 않도록 설정된 다수의 HTTP GET 패킷을 특정 시스템에 전송하여 서비스를 마비시키는 공격으로 옳은 것은?

① Slowloris 공격
② HTTP GET Flooding 공격
③ ARP Spoofing 공격
④ DNS Spoofing 공격
⑤ HTTP CC(Cache-control) 공격

정답 5번

출제 포인트

캐시 서버를 우회하도록 HTTP 요청을 구성해 원본 웹 서버의 자원을 고갈시키는 HTTP CC 공격을 다른 네트워크 공격과 구별하는 문제이다.

핵심 개념

HTTP CC(Cache-Control) 공격은 다수의 HTTP GET 요청에 캐시를 사용하지 않게 하는 설정을 넣어 캐싱 장비가 대신 응답하지 못하게 하고, 요청이 원본 웹 서버까지 전달되도록 하여 서버 부하를 높이는 애플리케이션 계층 서비스 거부 공격이다. 결정적 키워드는 '캐싱 장비가 응답하지 않도록 설정된 다수의 HTTP GET'이다.

선지별 해설

① X — Slowloris 공격은 HTTP 요청 헤더를 매우 느리게 또는 불완전하게 보내 연결을 장시간 점유하는 공격이다. '캐시를 우회하는 다수의 완성된 GET 요청'이 아니라 '느린 전송으로 연결 유지'가 올바른 특징이다.
② X — HTTP GET Flooding 공격은 다수의 GET 요청 자체로 웹 서버 자원을 소모시키는 공격이다. '캐싱 장비가 응답하지 않도록 설정한다'는 특징까지 포함하는 명칭은 HTTP CC 공격이다.
③ X — ARP Spoofing 공격은 위조된 ARP 정보를 보내 동일 네트워크 안에서 IP 주소와 MAC 주소의 대응 관계를 변조하는 공격이다. HTTP GET과 캐시 제어를 이용하는 공격이 아니라 ARP 캐시를 오염시키는 공격이다.
④ X — DNS Spoofing 공격은 위조된 DNS 응답 등으로 도메인 이름이 공격자가 의도한 IP 주소로 해석되게 하는 공격이다. 캐시 우회 HTTP GET으로 웹 서버를 마비시키는 공격이 아니라 이름 해석 결과를 변조하는 공격이다.
⑤ O — HTTP CC(Cache-Control) 공격은 캐싱 장비가 응답하지 못하도록 한 다수의 HTTP GET 요청을 원본 서버로 보내 부하를 집중시키므로 문제의 설명과 일치한다.

NoteBase

출제자가 노린 함정

②의 HTTP GET Flooding도 다수의 GET 요청을 이용하므로 가장 헷갈리기 쉽다. 그러나 문제의 핵심 문구인 ‘캐싱 장비가 응답하지 않도록 설정’은 단순 GET 폭주가 아니라 캐시 우회를 이용하는 ⑤ HTTP CC 공격을 가리킨다.

다시 나오면 이렇게 판단

요청을 천천히 보내 연결을 붙잡으면 Slowloris, 다수의 GET 요청 자체를 강조하면 HTTP GET Flooding, 캐시를 우회해 원본 서버까지 요청을 보내는 점을 강조하면 HTTP CC로 판단한다. ARP 주소 대응 변조와 DNS 이름 해석 변조는 HTTP 기반 서비스 거부 공격과 구분한다.

암기 포인트

CC는 Cache-Control, 캐시를 건너뛰고 원본 서버를 직접 압박하는 공격이다.

NoteBase

17. 다음 지문의 ㉠에 들어갈 말로 옳은 것은?

> 리눅스 시스템에서 관리자(root) 권한이 필요 없는 프로그램에 소유자가 관리자로 되어 있으면서 (㉠)가 설정된 경우에는 시스템의 보안에 허점을 초래할 수 있다. 실제로 이것이 설정된 파일은 백도어 및 버퍼 오버플로우 등 여러 공격에 이용된다.

① SetUID
② SetGID
③ Sticky Bit
④ Finger
⑤ Shadow

정답 1번

출제 포인트

root가 소유한 실행 파일을 일반 사용자가 실행할 때 파일 소유자의 권한으로 동작하게 만드는 특수 권한이 무엇인지 묻는 문제이다.

핵심 개념

SetUID는 실행 파일을 실행한 프로세스의 유효 사용자 ID를 파일 소유자의 ID로 바꾸는 특수 권한이다. 따라서 root 소유 실행 파일에 SetUID가 설정되면 일반 사용자도 그 프로그램이 실행되는 동안 root 권한을 사용할 수 있다.
SetGID는 유효 그룹 ID를 파일의 소유 그룹 ID로 바꾸며, Sticky Bit는 주로 공유 디렉터리에서 다른 사용자의 파일 삭제·이름 변경을 제한한다. Finger는 사용자 정보 조회 기능이고, Shadow는 암호 해시를 일반 계정 정보와 분리하여 보호하는 방식이다.

NoteBase

선지별 해설

① O — SetUID가 설정된 실행 파일은 실행 시 프로세스의 유효 사용자 ID가 파일 소유자의 ID가 된다. root 소유 파일이라면 root 권한으로 동작하므로 취약점이 있을 때 백도어 설치나 버퍼 오버플로 공격에 악용될 수 있다.
② X — SetGID는 사용자 ID가 아니라 유효 그룹 ID를 파일의 소유 그룹 ID로 바꾸는 권한이다. 틀린 대응은 '관리자(root) 소유 파일을 관리자 사용자 권한으로 실행'한 부분이며, 올바르게는 SetUID이다.
③ X — Sticky Bit는 주로 여러 사용자가 함께 쓰는 디렉터리에서 파일 소유자·디렉터리 소유자·root만 해당 파일을 삭제하거나 이름을 바꿀 수 있게 한다. 틀린 대응은 '파일 소유자의 권한으로 실행'한 부분이며, 올바르게는 SetUID이다.
④ X — Finger는 시스템 사용자 정보나 로그인 정보를 조회하는 명령·서비스로, 특수 실행 권한 비트가 아니다. 틀린 대응은 '실행 시 파일 소유자 권한을 부여하는 기능'으로 본 부분이며, 올바르게는 SetUID이다.
⑤ X — Shadow는 암호 해시를 접근이 제한된 별도 파일에 저장하여 보호하는 방식으로, 실행 파일의 권한 상승 기능이 아니다. 틀린 대응은 'root 권한으로 실행되게 하는 설정'으로 본 부분이며, 올바르게는 SetUID이다.

오답 포인트

SetUID와 SetGID는 모두 실행 시 신원을 바꾸는 특수 권한이지만, SetUID는 사용자 ID를, SetGID는 그룹 ID를 바꾼다. 지문의 '소유자가 관리자(root)'와 '관리자 권한이 필요 없는 프로그램이 root 권한으로 동작'한다는 표현이 SetUID를 가리킨다.

다시 나오면 이렇게 판단

실행 파일의 소유자 권한으로 동작하면 SetUID, 소유 그룹 권한으로 동작하면 SetGID, 공유 디렉터리에서 타인의 파일 삭제를 제한하면 Sticky Bit로 판단한다.

암기 포인트

SetUID는 소유자 사용자 권한, SetGID는 소유 그룹 권한, Sticky Bit는 공유 디렉터리 삭제 제한이다.

NoteBase

18. 다음 중 버퍼 오버플로우(Buffer Overflow)에 취약한 C언어 함수로 옳지 않은 것은?

① int scanf (const char *format, ...);
② char *gets (char *buf);
③ int strcmp (const char *str1, const char *str2);
④ char *realpath (const char *path, char *resolved_path);
⑤ char *strcat (char *dest, const char *src);

정답 3번

출제 포인트

버퍼의 크기를 확인하지 않은 채 데이터를 쓰거나 이어 붙일 수 있는 C 함수와, 데이터를 쓰지 않고 비교만 하는 함수를 구별하는 문제이다.

핵심 개념

버퍼 오버플로우는 확보된 버퍼의 경계를 넘어 데이터를 기록할 때 발생한다. scanf, gets, realpath, strcat은 사용 방법이나 전달된 버퍼 크기에 따라 경계를 넘겨 쓸 위험이 있지만, strcmp는 두 문자열을 읽어 비교할 뿐 대상 버퍼에 문자열을 기록하지 않는다.

선지별 해설

① O — scanf에서 %s와 같은 변환에 최대 필드 폭을 지정하지 않으면 입력 길이를 제한하지 못해 목적지 문자 배열을 넘겨 쓸 수 있다. 안전하게는 버퍼 크기에 맞는 필드 폭을 지정하거나 길이를 제한하는 입력 방식을 사용한다.
② O — gets는 입력을 저장할 버퍼의 크기를 전달받지 않고 줄 전체를 읽으므로 긴 입력이 들어오면 버퍼 경계를 넘길 수 있다. 안전하게는 크기를 인수로 받는 fgets를 사용한다.
③ X — strcmp는 str1과 str2가 가리키는 문자열을 읽어 사전식으로 비교하며 목적지 버퍼에 데이터를 쓰지 않으므로, 제시된 함수들 가운데 버퍼 오버플로우를 일으키는 쓰기 함수로 보는 것은 옳지 않다. 틀린 표현은 '버퍼 오버플로우에 취약한 함수'이며, 올바르게는 '널 문자로 끝나는 두 문자열을 비교하는 함수'이다. 다만 유효한 널 종료 문자열을 전달해야 한다.
④ O — realpath는 정규화된 절대 경로를 resolved_path에 기록하므로, 호출자가 충분한 크기의 출력 버퍼를 마련하지 않은 사용 방식에서는 경계를 넘겨 쓸 위험이 있다. 안전하게는 구현이 지원하는 경우 출력 버퍼를 함수가 할당하게 하거나 충분한 크기를 보장한다.
⑤ O — strcat은 dest 뒤에 src를 붙이면서 dest의 남은 공간을 확인하지 않으므로 결합 결과가 dest의 크기를 넘으면 버퍼 오버플로우가 발생한다. 안전하게는 붙이기 전에 필요한 전체 길이와 목적지 용량을 확인한다.

NoteBase

오답 포인트

③의 strcmp도 포인터를 받는 문자열 함수라는 이유만으로 위험한 쓰기 함수라고 판단하기 쉽다. 그러나 이 문항의 구별점은 포인터 사용 자체가 아니라 버퍼에 데이터를 기록하는가이다. strcmp는 비교를 위해 읽기만 한다.

다시 나오면 이렇게 판단

각 함수가 목적지 버퍼에 입력·변환 결과·문자열을 기록하는지 먼저 확인한다. 기록한다면 버퍼 크기나 최대 길이를 인수로 받아 경계를 보장하는지 살피고, 읽어서 비교만 하는 함수는 별도로 구분한다.

암기 포인트

gets는 무제한 입력, strcat은 무제한 이어 붙이기, strcmp는 쓰기가 아닌 비교이다.

NoteBase

19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공하는 경우, 이용자에게 알리고 동의를 받아야 하는 내용으로 옳지 않은 것은?

① 개인정보를 제공 받는 자
② 제공하는 개인정보의 항목
③ 개인정보를 제공 받는 자의 개인정보 이용 목적
④ 개인정보를 제공 받는 자의 개인정보 보호책임자
⑤ 개인정보를 제공 받는 자의 개인정보 보유 및 이용기간

정답 4번

쟁점

이 문제는 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공하기 전에 알려야 하는 사항에 관한 문제이다. 핵심은 제3자 제공의 대상·목적·항목·기간과 개인정보 보호책임자를 구별하는 것이다.

용어 풀이

제3자 제공 동의 = 개인정보를 보유한 사업자가 이용자 외의 다른 자에게 개인정보를 넘기기 전에 제공 내용을 알리고 이용자의 의사를 확인하는 절차이다.

핵심 구분

문항이 근거로 삼은 정보통신망법 제24조의2 제1항은 개인정보를 제공받는 자, 그 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 그 자의 개인정보 보유 및 이용 기간을 이용자에게 알리고 동의를 받도록 규정하였다. 개인정보 보호책임자는 이 네 가지 제3자 제공 고지사항에 포함되지 않는다.

선지별 해설

① O — '개인정보를 제공받는 자'는 개인정보가 누구에게 넘어가는지를 나타내므로 고지사항에 포함된다.
② O — '제공하는 개인정보의 항목'은 어떤 개인정보가 넘어가는지를 나타내므로 고지사항에 포함된다.
③ O — '개인정보를 제공받는 자의 개인정보 이용 목적'은 제3자가 개인정보를 왜 이용하는지를 나타내므로 고지사항에 포함된다.
④ X — '개인정보를 제공받는 자의 개인정보 보호책임자'는 제3자 제공 동의를 받을 때의 고지사항이 아니다. 틀린 표현: 개인정보를 제공받는 자의 개인정보 보호책임자. 올바른 표현: 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간.
⑤ O — '개인정보를 제공받는 자의 개인정보 보유 및 이용 기간'은 제3자가 개인정보를 언제까지 보유하고 이용하는지를 나타내므로 고지사항에 포함된다.

NoteBase

오답 포인트

개인정보 보호책임자가 개인정보 보호 제도에서 중요한 역할을 한다는 이유만으로 모든 동의 절차의 필수 고지사항이라고 판단하기 쉽다. 이 문항은 조직의 담당자 정보가 아니라 제3자 제공의 구체적 내용인 누구에게·왜·무엇을·언제까지를 묻는다.

다시 나오면 이렇게 판단

제3자 제공 동의 문제에서는 제공받는 자, 이용 목적, 제공 항목, 보유·이용 기간을 먼저 묶어 확인한다. 담당자나 개인정보 보호책임자처럼 제공 내용 자체가 아닌 항목은 이 기본 묶음과 구별한다.

암기 포인트

제3자 제공의 기본 네 항목은 '누구에게·왜·무엇을·언제까지'이다.

NoteBase

20. <보기>에서 설명하는 SSL 프로토콜로 옳은 것은?

<보 기>

이 프로토콜을 이용하여 서버와 클라이언트가 서로를 인증하고, 암호와 MAC 알고리즘, 그리고 SSL 레코드 안에 보낼 데이터를 보호하는 데 사용할 암호키를 협상할 수 있다.

① Alert Protocol
② Handshake Protocol
③ Record Protocol
④ Change Cipher Spec Protocol
⑤ Encapsulating Security Payload Protocol

정답 2번

출제 포인트

SSL을 구성하는 하위 프로토콜의 역할을 구분하고, 인증과 보안 매개변수 협상을 담당하는 프로토콜을 찾는 문제이다.

핵심 개념

Handshake Protocol은 서버와 클라이언트가 통신을 시작하기 전에 상대를 인증하고 암호 스위트, MAC 알고리즘, 키 생성에 필요한 값 등 보안 매개변수를 협상하는 프로토콜이다.
Alert Protocol은 오류나 경고를 알리고, Record Protocol은 협상된 보안 매개변수에 따라 데이터를 보호하며, Change Cipher Spec Protocol은 이후 레코드부터 협상된 설정을 적용한다는 사실을 알린다. ESP는 SSL이 아니라 IPsec의 보안 프로토콜이다.

NoteBase

선지별 해설

① X — Alert Protocol은 SSL 통신 중 발생한 경고·오류와 연결 종료 사실을 전달한다. 틀린 표현은 인증과 암호 알고리즘·키를 협상하는 프로토콜로 본 부분이며, 올바르게는 Handshake Protocol이다.
② O — Handshake Protocol은 서버 인증과 선택적인 클라이언트 인증을 수행할 수 있고, 암호 스위트와 키 생성에 필요한 정보를 협상한다. 보기의 설명과 일치한다.
③ X — Record Protocol은 상위 계층 데이터를 조각화하고, 협상된 알고리즘과 키를 이용해 무결성과 기밀성을 제공한다. 틀린 표현은 통신 전에 인증과 보안 매개변수를 협상한다고 본 부분이며, 올바르게는 Handshake Protocol의 역할이다.
④ X — Change Cipher Spec Protocol은 이후 전송되는 레코드부터 협상된 암호 스위트와 키를 사용한다는 전환 신호를 보낸다. 틀린 표현은 이 프로토콜 자체가 인증과 알고리즘·키 협상을 수행한다고 본 부분이며, 협상은 Handshake Protocol이 수행한다.
⑤ X — Encapsulating Security Payload Protocol은 IPsec에서 IP 패킷의 기밀성·무결성·인증 등을 제공하는 프로토콜로, SSL 하위 프로토콜이 아니다. 틀린 표현은 SSL의 인증·협상 프로토콜로 본 부분이며, 올바르게는 Handshake Protocol이다.

오답 포인트

‘데이터를 보호한다’는 표현만 보고 Record Protocol을 고르기 쉽다. 그러나 보기의 중심 동사는 실제 데이터 보호가 아니라 통신 전의 ‘인증’과 암호 알고리즘·키 ‘협상’이므로 Handshake Protocol을 선택해야 한다.

다시 나오면 이렇게 판단

인증·알고리즘·키 협상은 Handshake, 실제 데이터 보호는 Record, 경고·오류 통지는 Alert, 협상된 설정으로의 전환 신호는 Change Cipher Spec으로 구분한다. ESP가 나오면 SSL이 아니라 IPsec 계열인지 먼저 확인한다.

암기 포인트

Handshake는 협상, Record는 보호, Alert는 통지, Change Cipher Spec은 전환, ESP는 IPsec이다.

NoteBase