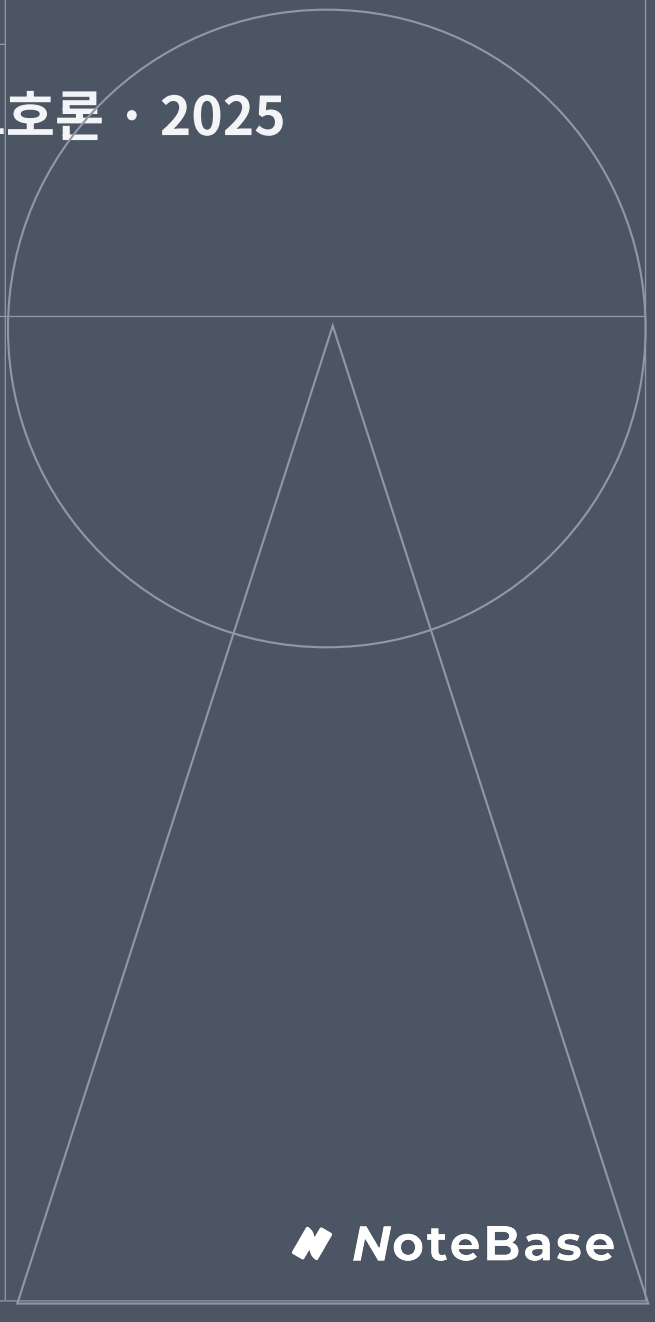
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2025

공무원/국가직/9급 · 정보보호론 · 2025

문 1. 적극적(active) 공격에 해당하는 것만을 모두 고르면?

ㄱ. 위장(masquerade)
ㄴ. 변조(modification)
ㄷ. 도청(eavesdropping)
ㄹ. 트래픽 분석(traffic analysis)

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

정답 1번

간단한 해설

위장은 **다른 주체를 사칭해 통신에 개입**하고, 변조는 **메시지 내용을 변경**하므로 단순한 정보 관찰을 넘어서는 적극적 공격이다.

NoteBase

보기별 해설

적극적 공격은 데이터를 변경하거나 허위 통신을 하는 등 통신·시스템 동작에 개입하는 공격이다. 소극적 공격은 통신 내용을 바꾸지 않고 정보나 통신 특성을 관찰하여 알아내는 공격이다.

ㄱ. 위장(masquerade): 적극적 공격이다. 공격자가 **다른 주체의 신분을 사칭**하여 정당한 사용자나 통신 상대인 것처럼 행동한다. 허위 신분으로 통신에 개입한다는 점에서 단순한 관찰과 구별된다.

ㄴ. 변조(modification): 적극적 공격이다. 전송되는 메시지의 내용을 무단으로 바꾸는 공격으로, **데이터의 무결성**을 침해한다.

ㄷ. 도청(eavesdropping): 소극적 공격이다. 통신 내용을 몰래 읽거나 듣는 공격으로, **내용을 변경하지 않고 정보를 얻는다**. 따라서 정보의 기밀성을 침해하지만 적극적 공격에는 해당하지 않는다.

ㄹ. 트래픽 분석(traffic analysis): 소극적 공격이다. 메시지 내용 자체를 해독하지 못하더라도 **통신량·시점·빈도·송수신 관계** 등을 관찰하여 정보를 추론한다. 통신 내용을 변경하거나 통신 동작을 방해하는 방식이 아니므로 적극적 공격과 구별된다.

적극적 공격에 해당하는 보기는 ㄱ과 ㄴ이므로 ①의 조합과 일치한다.

NoteBase

문 2. 전자서명이 제공하는 보안 요소가 아닌 것은?

① 메시지 무결성

② 서명자 인증

③ 서명 부인 방지

④ 메시지 기밀성

정답 4번

간단한 해설

전자서명은 메시지의 변경 여부와 서명자를 확인하게 하지만, **메시지 내용을 숨기지는 않는다**. 메시지 기밀성을 확보하려면 **별도의 암호화**가 필요하다.

선지별 해설

전자서명은 서명자의 개인키로 생성하고, 그에 대응하는 공개키로 검증한다.

① O: 메시지 무결성은 메시지가 서명된 뒤 변경되지 않았는지를 확인하는 성질이다. 서명은 특정 메시지에 연결되므로 메시지가 바뀌면 기존 서명으로 정상적으로 검증되지 않는다. 이를 통해 **메시지의 변조를 탐지**할 수 있다.

② O: 서명자 인증은 누가 메시지에 서명했는지를 확인하는 것이다. **공개키가 해당 서명자의 것임이 확인된 경우**, 그 공개키로 서명을 검증하여 대응하는 개인키로 서명이 생성되었음을 확인할 수 있다.

③ O: 서명 부인 방지는 서명자가 나중에 자신이 서명했다는 사실을 부당하게 부인하지 못하도록 하는 성질이다. 개인키가 서명자만 사용할 수 있도록 안전하게 관리되었다면, 검증 가능한 서명은 **서명 사실을 제삼자에게 입증하는 증거**가 된다.

④ X: 메시지 기밀성은 허가받지 않은 사람이 메시지 내용을 알 수 없도록 하는 성질이다. 전자서명 자체는 메시지 내용을 암호화하지 않으므로, 서명만 붙인 메시지는 다른 사람이 내용을 읽을 수 있다. 따라서 기밀성은 전자서명만으로 제공되지 않으며, **메시지를 별도로 암호화**해야 한다.

NoteBase

문 3. 흔히 ‘Orange Book’으로 불리며, 미국에서 제정된 보안 표준으로 효과적인 정보보호 시스템 평가의 기준 개발과 이러한 기준에 맞게 개발된 제품들을 평가하는 데 초점을 두고 있는 정보 보안 평가 기준은?

① CC

② PIMS

③ ITSEC

④ TCSEC

정답 4번

간단한 해설

'Orange Book'은 미국 국방부가 제정한 **TCSEC(신뢰 컴퓨터 시스템 평가 기준)**의 별칭이다. 정보보호 시스템의 평가 기준을 제시하고, 제품이 그 기준을 충족하는지 평가하는 데 사용한다.

공통 해설

TCSEC는 Trusted Computer System Evaluation Criteria의 약자로, 미국 국방부가 제정한 '신뢰 컴퓨터 시스템 평가 기준'이다. 이 기준을 담은 문서인 DoD 5200.28-STD가 'Orange Book'으로 불린다.

TCSEC는 **제품 개발과 평가에 공통으로 적용할 보안 요구사항**을 제시한다. 개발자는 이 기준에 맞추어 정보보호 시스템을 설계하고, 평가자는 개발된 제품이 해당 요구사항을 충족하는지 판단한다. 따라서 발문의 '미국에서 제정', 'Orange Book', '기준에 맞게 개발된 제품 평가'라는 단서는 TCSEC에 대응한다.

NoteBase

문 4. 다음에서 설명하는 보안 모델은?

◯ 상업 환경에서의 데이터의 무결성에 중점을 둔 것이다.
◯ 정형화된 트랜잭션의 처리 과정에서 직무를 분리하도록 한다.
◯ 제약을 받는(constrained) 데이터 항목에 대해 무결성 검증 절차를 거치도록 한다.

① Bell-LaPadula
② Biba
③ Clark-Wilson
④ Lattice

정답 3번

간단한 해설

정형화된 트랜잭션과 직무 분리로 상업 환경의 데이터 무결성을 유지하는 것이 Clark-Wilson 모델의 특징이다. 제약 데이터 항목이 무결성 조건을 만족하는지는 무결성 검증 절차로 확인한다.

공통 해설

Clark-Wilson 모델은 상업 환경에서 오류나 부정한 변경으로부터 데이터의 무결성을 보호하는 모델이다. 보호 대상인 제약 데이터 항목(CDI)은 사용자가 임의로 변경할 수 없으며, **인증된 변환 절차(TP)를 통해서만 변경**한다. 정형화된 트랜잭션은 무결성 조건을 만족하는 유효한 상태의 데이터를 변경한 뒤에도 유효한 상태가 유지되도록 하는 처리이다.

직무 분리는 한 사람이 중요한 업무를 모두 처리하지 못하도록 역할과 권한을 나누는 것이다. 예를 들어 거래를 승인하는 사람과 실행하는 사람을 분리하여 한 사람의 부정행위를 어렵게 한다. 무결성 검증 절차(IVP)는 제약 데이터 항목이 정해진 무결성 조건을 만족하는지 확인한다. 즉, 변환 절차는 유효한 상태를 유지하며 데이터를 바꾸고, 검증 절차는 데이터의 상태가 유효한지 점검한다.

지문에서 상업 환경의 무결성 보호, 정형화된 트랜잭션과 직무 분리, 제약 데이터 항목의 무결성 검증을 함께 제시한 것은 이러한 Clark-Wilson 모델의 통제 방식을 설명한 것이다.

NoteBase

문 5. 다음에서 설명하는 정보보호의 목표에 해당하는 것은?

◯ 정당한 사용자가 정보시스템의 데이터 또는 자원을 필요로 하는 시점에 사용할 수 있는 성질이다.
◯ 확보 방법으로 데이터 백업, 중복성 유지 등이 있다.
◯ 위협 요소로는 서비스 거부 공격, 지진, 홍수 등이 있다.

① 기밀성
② 가용성
③ 무결성
④ 책임추적성

정답 2번

간단한 해설

정당한 사용자가 데이터나 자원을 **필요한 시점에 사용할 수 있게 하는** 것이 가용성이다. 백업과 중복성 유지는 이용 중단에 대비하는 수단이고, 서비스 거부 공격과 재해는 이를 위협한다.

공통 해설

가용성은 정당한 사용자가 필요할 때 정보시스템의 데이터나 자원에 접근하여 사용할 수 있는 성질이다. 제시된 설명에서 개념을 식별하는 기준은 **필요한 시점의 사용 가능성**이다.

데이터 백업은 데이터가 손실되었을 때 복구할 수 있게 하고, 중복성 유지는 일부 자원에 장애가 생겨도 다른 자원으로 서비스를 이어 갈 수 있게 한다. 둘 다 장애로 인한 이용 중단에 대비하여 가용성을 확보하는 방법이다. 반대로 서비스 거부 공격은 정당한 사용자의 서비스 이용을 방해하고, 지진이나 홍수는 설비를 손상시키거나 가동을 중단시켜 데이터와 자원을 사용할 수 없게 할 수 있다. 따라서 정의, 확보 방법, 위협 요소가 모두 가용성이라는 하나의 목표로 연결된다.

NoteBase

문 6. 「개인정보 보호법」에서 규정하고 있는 개인정보에 해당하지 않는 것은?

① 성명
② 주민등록번호
③ 영상 등을 통하여 개인을 알아볼 수 있는 정보
④ 사망자에 대한 정보

정답 4번

①
살아 있는 개인의 성명은 **그 개인을 알아볼 수 있는 정보**로서 개인정보에 해당한다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

②
주민등록번호는 **살아 있는 특정 개인을 식별하는 정보**이므로 개인정보에 해당한다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

③
영상 등을 통하여 **살아 있는 개인을 알아볼 수 있다면 개인정보**에 해당한다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

NoteBase

④

개인정보는 **살아 있는 개인에 관한 정보**를 대상으로 하므로, 사망자 본인에 관한 정보는 이에 해당하지 않는다.

개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용 · 결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

NoteBase

문 7. 다음에서 설명하는 기술은?

◯ 공인 IP 주소가 내부 사설 IP 주소보다 부족한 경우에 적용 가능한 방식이다.
◯ 내부 사설 IP 주소나 내부 네트워크 대역을 공인 IP로 자동 매핑하는 기능을 제공한다.
◯ 내부 IP 주소를 외부로부터 보호해 주는 기능을 제공하기도 한다.

① ARP
② IPS
③ NAT
④ VLAN

정답 3번

간단한 해설

NAT(네트워크 주소 변환)는 내부 사설 IP 주소를 외부 통신에 사용할 공인 IP 주소로 변환한다. 포트 번호까지 변환하는 방식을 사용하면 여러 내부 기기가 공인 IP 주소를 공유할 수 있어 주소 부족을 완화한다.

공통 해설

NAT(Network Address Translation)는 네트워크 경계에서 패킷의 IP 주소를 변환하는 기술이다. 내부 기기가 외부로 통신할 때 사설 IP 주소를 공인 IP 주소로 바꾸고, 돌아오는 응답은 저장된 변환 정보를 이용해 해당 내부 기기로 전달한다. 지문의 사설 주소와 공인 주소 간 매핑은 이러한 주소 변환을 뜻한다.

공인 IP 주소가 내부 기기 수보다 적을 때는 NAT의 한 방식인 NAPT 또는 PAT를 사용할 수 있다. 이는 **IP 주소와 포트 번호를 함께 변환**하여 여러 내부 기기의 통신을 구별한다. 예를 들어 두 내부 기기가 하나의 공인 IP 주소를 사용하더라도 외부에 사용하는 포트 번호를 다르게 매핑하면 응답을 각 기기에 돌려보낼 수 있다. 따라서 내부 기기마다 별도의 공인 IP 주소를 할당할 필요가 줄어든다.

외부와 주고받는 패킷에는 변환된 공인 IP 주소가 나타나므로 내부 사설 IP 주소를 외부에 직접 드러내지 않는 효과도 있다. 사설 주소의 공인 주소 매핑, 공인 주소 부족 완화, 내부 주소 은닉이라는 지문의 특징은 NAT의 작동으로 설명된다.

NoteBase

문 8. 다음과 같은 과정으로 진행되는 공격은?

1. 공개키 암호 방법을 사용하는 A와 B의 통신에 C가 개입한다.
2. C는 A의 공개키를 가로채어 B에게 C의 공개키를 A의 공개키처럼 전송한다.
3. B는 C의 공개키로 메시지를 암호화하여 A에게 전송한다.
4. C는 B가 보낸 메시지를 가로채어 C의 개인키로 복호화한다.
5. C는 복호화한 메시지를 단계 2에서 가로챈 A의 공개키로 암호화하여 A에게 B가 보낸 것처럼 전송한다.
6. A는 자신의 개인키로 메시지를 복호화한다.

① Smurf
② 중간자(MITM)
③ Sniffing
④ Slowloris

정답 2번

간단한 해설

C가 자신의 공개키를 A의 공개키로 속여 전달했으므로, B가 암호화한 메시지를 C의 개인키로 읽을 수 있다. 이후 A의 공개키로 다시 암호화해 전달하는 것은 통신 당사자 사이에 끼어드는 **중간자(MITM) 공격**이다.

공통 해설

중간자(MITM) 공격은 공격자가 통신 당사자 사이에 개입하여 상대방인 것처럼 행세하면서 메시지를 가로채거나 조작하고 전달하는 공격이다. 이 사례의 식별 기준은 **공개키를 바꿔치기하여 상대방을 사칭하고 통신을 중계한다**는 점이다.

단계 2에서 C는 자신의 공개키를 A의 공개키처럼 B에게 전달한다. B는 이를 믿고 단계 3에서 C의 공개키로 메시지를 암호화한다. 공개키로 암호화한 메시지는 그에 대응하는 개인키로 복호화하므로, 단계 4에서 해당 개인키를 가진 C가 메시지를 읽을 수 있다. 이는 A의 개인키를 알아내거나 암호 자체를 깨서 복호화한 것이 아니라, **B가 사용한 공개키의 실제 소유자가 C**이기 때문에 가능한 일이다.

단계 5에서 C는 읽은 메시지를 원래의 A 공개키로 다시 암호화하여 B가 보낸 것처럼 전달한다. 따라서 단계 6에서 A도 자신의 개인키로 메시지를 복호화할 수 있다. 이처럼 통신 내용을 엿듣는 데 그치지 않고 공개키 전달에 개입하여 메시지를 가로채고 재암호화해 전달하는 전체 과정이 중간자 공격에 해당한다.

NoteBase

문 9. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

공개키 암호 방식으로 송신자가 수신자에게 보낼 평문을 암호화할 때는 (가)를 사용하고, 송신자가 평문을 전자서명하여 수신자에게 보낼 때는 (나)를 사용한다.

① (가): 송신자의 공개키, (나): 송신자의 공개키
② (가): 수신자의 공개키, (나): 송신자의 공개키
③ (가): 송신자의 공개키, (나): 송신자의 개인키
④ (가): 수신자의 공개키, (나): 송신자의 개인키

정답 4번

간단한 해설

내용을 수신자만 읽게 하려면 **수신자의 공개키**로 암호화한다. 전자서명은 송신자가 작성했음을 확인하는 수단이므로 **송신자의 개인키**로 생성한다.

빈칸별 해설

(가) 수신자의 공개키: 공개키 암호 방식은 서로 짝을 이루는 공개키와 개인키를 사용한다. 수신자의 공개키로 암호화하면 그에 대응하는 **수신자의 개인키로 복호화**하므로, 개인키를 비밀로 보관한 수신자만 내용을 읽을 수 있다. 송신자의 공개키로 암호화하면 송신자의 개인키가 필요하므로 수신자에게 비밀 내용을 전달하려는 목적에 맞지 않는다.

(나) 송신자의 개인키: 전자서명은 메시지의 작성자를 확인하고 내용의 변경 여부를 검증하기 위한 것이다. 송신자는 자신의 개인키로 서명을 생성하고, 수신자는 **송신자의 공개키로 서명을 검증**한다. 일반적으로 메시지의 해시값에 서명 연산을 수행하며, 메시지를 비밀로 만드는 암호화와는 목적이 다르다. 누구나 알 수 있는 공개키로 서명을 생성한다면 송신자만이 작성했다는 근거가 될 수 없다.

(가)는 수신자의 공개키, (나)는 송신자의 개인키이므로 ④의 조합과 일치한다.

NoteBase

문 10. 「개인정보 보호법」 제3조(개인정보 보호 원칙)상 개인정보 보호 원칙으로 옳지 않은 것은?

① 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 가명처리가 가능한 경우에는 가명에 의하여, 가명처리로 목적을 달성할 수 없는 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

정답 1번

①

익명 또는 가명 처리로 수집목적을 달성할 수 있다면 **익명처리가 가능할 때에는 익명으로, 익명처리로 목적을 달성할 수 없을 때에는 가명으로** 처리해야 한다. 선지는 익명과 가명의 우선순위를 뒤바꾸었다.

개인정보 보호법 제3조(개인정보 보호 원칙)
⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020.2.4>

②

개인정보의 처리 목적을 명확히 하고, 그 목적에 필요한 **최소한의 개인정보만 적법하고 정당하게 수집**해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

③

처리 목적에 필요한 범위에서 개인정보의 **정확성·완전성·최신성**이 보장되도록 해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

NoteBase

④

개인정보는 **정보주체의 사생활 침해를 최소화하는 방법**으로 처리해야 한다.

개인정보 보호법 제3조(개인정보 보호 원칙)
⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

NoteBase

문 11. 스택 오버플로(stack overflow) 공격에 대응하는 방법으로 옳지 않은 것은?

① 스택에 저장할 수 있는 데이터의 최대 길이를 지정해야 하는 함수를 사용한다.

② 스택에서 코드가 실행되는 것을 허용한다.

③ 스택 영역을 임의의 메모리 주소에 할당하여 스택 영역의 주소에 대한 추측을 어렵게 한다.

④ 함수의 종료 연산을 수행하기 전에 카나리(canary) 값의 변경 여부를 검사한다.

정답 2번

간단한 해설

스택에서 코드 실행을 허용하면 공격자가 스택에 넣은 악성 코드가 실행될 수 있다. 대응하려면 **스택의 코드 실행을 금지**하는 실행 방지 기법을 적용해야 한다.

선지별 해설

이 문항의 스택 오버플로 공격은 스택에 있는 버퍼의 경계를 넘어 데이터를 써서 복귀 주소 등 인접한 정보를 변조하는 공격을 뜻한다.

① O: 입력이나 복사 길이의 상한을 지정할 수 있는 함수를 사용하고, 그 상한을 **대상 버퍼의 용량 이내**로 설정하면 버퍼 경계를 넘는 쓰기를 방지할 수 있다. 단순히 길이를 지정하는 데 그치지 않고 실제 저장 공간에 맞게 제한해야 한다.

② X: 스택에서 코드 실행을 허용하면 공격자가 스택에 주입한 악성 코드가 실행될 수 있어 공격에 이용된다. 스택을 **실행 불가능한 영역**으로 설정하는 NX 또는 데이터 실행 방지(DEP)를 적용하여 스택에 저장된 데이터를 명령어로 실행하지 못하게 해야 한다.

③ O: 주소 공간 배치 무작위화(ASLR)는 스택 등 메모리 영역이 배치되는 주소를 무작위화한다. 공격자가 악성 코드의 위치나 실행 흐름을 돌릴 대상 주소를 **미리 예측하기 어렵게** 하여 공격의 성공 가능성을 낮춘다.

④ O: 카나리는 스택의 버퍼 오버플로로 인한 손상을 탐지하기 위해 두는 검사값이다. 함수가 복귀하기 전에 **카나리 값이 원래 값과 같은지** 검사하고, 변경되었다면 프로그램을 중단하여 변조된 복귀 주소에 따라 실행되는 것을 막는다.

NoteBase

문 12. ISMS-P 인증을 위한 정보보호 보호대책 요구사항 중 '인증 및 권한관리' 항목에 해당하지 않는 것은?

① 비밀번호 관리

② 접근권한 검토

③ 정보시스템 보호

④ 특수 계정 및 권한관리

정답 3번

간단한 해설

'정보시스템 보호'는 장비의 배치와 통신·전력 케이블의 보호 등을 다루는 **'2.4 물리 보안'**의 세부 항목이다. 사용자 인증과 계정·권한을 관리하는 '2.5 인증 및 권한관리'에 속하지 않는다.

선지별 해설

① O: 비밀번호 관리는 '2.5.4 비밀번호 관리'에 해당한다. 법적 요구사항과 외부 위협요인을 고려하여 사용자와 이용자의 비밀번호 관리절차를 수립·이행하는 항목이다. 비밀번호는 사용자 인증에 쓰이는 수단이므로 **인증수단의 안전한 관리**를 다룬다.

② O: 접근권한 검토는 '2.5.6 접근권한 검토'에 해당한다. 사용자 계정의 등록·이용·삭제와 접근권한의 부여·변경·삭제 이력을 남기고 **주기적으로 적정성을 점검**하는 항목이다. 권한을 처음 부여하는 데 그치지 않고 계속 보유할 필요가 있는지도 확인한다.

③ X: 정보시스템 보호는 **'2.4 물리 보안'의 '2.4.3 정보시스템 보호'**에 해당한다. 환경적 위험과 유해요소, 비인가 접근 가능성을 줄이도록 시스템의 중요도와 특성을 고려해 장비를 배치하고 통신·전력 케이블을 손상으로부터 보호하는 항목이다. 따라서 분류를 '인증 및 권한관리'가 아니라 '물리 보안'으로 고쳐야 한다.

④ O: 특수 계정 및 권한관리는 '2.5.5 특수 계정 및 권한 관리'에 해당한다. 시스템 관리나 중요정보 관리 등 특수 목적에 쓰이는 계정과 권한을 **최소한으로 부여하고 별도로 식별·통제**하는 항목이다. 관리자 권한처럼 영향이 큰 권한이 불필요하게 부여되거나 남용되는 것을 방지한다.

NoteBase

문 13. 정보보호 관련 법률과 소관 부처를 잘못 짝지은 것은?

① 「개인정보 보호법」 ―개인정보보호위원회
② 「위치정보의 보호 및 이용 등에 관한 법률」 ―과학기술정보통신부
③ 「공공기관의 정보공개에 관한 법률」 ―행정안전부
④ 「전자서명법」 ―과학기술정보통신부

정답 2번

①

개인정보 보호에 관한 사무는 **개인정보 보호위원회**가 독립적으로 수행한다.

개인정보 보호법 제7조(개인정보 보호위원회)
① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. <개정 2020.2.4>

②

위치정보의 보호 및 이용에 관한 시책을 마련하는 소관 기관은 **방송미디어통신위원회**이다.

위치정보의 보호 및 이용 등에 관한 법률 제3조(위치정보의 보호 및 이용 등을 위한 시책의 강구)
방송미디어통신위원회는 관계중앙행정기관의 장과 협의를 거쳐 위치정보의 안전한 보호와 건전한 이용 등을 위하여 다음 각호의 사항이 포함되는 시책을 마련하여야 한다. <개정 2008.2.29, 2018.12.24, 2025.10.1>
1. 위치정보의 보호 및 이용 등을 위한 시책의 기본방향
2. 위치정보의 보호에 관한 사항(위치정보 처리에 따른 위험성 및 결과, 개인위치정보주체의 권리 등을 명확하게 인지하지 못할 수 있는 14세 미만의 아동의 위치정보 보호에 관한 사항을 포함한다)
3. 공공목적을 위한 위치정보의 이용에 관한 사항
4. 위치정보사업 및 위치기반서비스사업과 관련된 기술개발 및 표준화에 관한 사항
5. 위치정보사업 및 위치기반서비스사업의 안전성 및 신뢰성 향상에 관한 사항
6. 위치정보사업 및 위치기반서비스사업의 품질개선 및 품질평가 등에 관한 사항
7. 그 밖에 위치정보의 보호 및 이용 등을 위하여 필요한 사항

NoteBase

③

정보공개제도의 정책 수립과 제도 개선에 관한 기획·총괄 업무는 **행정안전부장관**이 관장한다.

공공기관의 정보공개에 관한 법률 제24조(제도 총괄 등)
① 행정안전부장관은 이 법에 따른 정보공개제도의 정책 수립 및 제도 개선 사항 등에 관한 기획 · 총괄 업무를 관장한다. <개정 2014.11.19, 2017.7.26>

④

전자서명 이용 촉진을 위한 행정적·재정적·기술적 지원은 **과학기술정보통신부장관**이 담당한다.

전자서명법 제5조(전자서명의 이용 촉진을 위한 지원) 과학기술정보통신부장관은 전자서명의 이용을 촉진하기 위하여 다음 각 호의 사항에 대한 행정적 · 재정적 · 기술적 지원을 할 수 있다.
1. 전자서명 관련 기술의 연구 · 개발 · 활용 및 표준화
2. 전자서명 관련 전문인력의 양성
3. 다양한 전자서명수단의 이용 확산을 위한 시범사업 추진
4. 전자서명의 상호연동 촉진을 위한 기술지원 및 연동설비 등의 운영
5. 제9조에 따른 인정기관 및 제10조에 따른 평가기관의 업무 수행 및 운영
6. 그 밖에 전자서명의 이용 촉진을 위하여 필요한 사항

NoteBase

문 14. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

공격자는 웹사이트에서 인증 과정을 거쳐 활성 세션을 가지고 있는 사용자로 하여금 공격자가 만든 악의적인 링크에 접근하게 유도한다. 이 링크를 클릭한 사용자는 자신도 인지하지 못한 채 공격자가 의도한 데이터를 HTTP 몸체(body)에 첨부하여 페이지 내용을 변경하도록 하는 HTTP (가) 요청을 웹사이트로 보낸다. 이와 같은 방식의 공격을 (나)라고 한다.

① (가): GET, (나): XSS

② (가): GET, (나): CSRF

③ (가): POST, (나): XSS

④ (가): POST, (나): CSRF

정답 4번

간단한 해설

변경할 데이터를 **HTTP 몸체에 담아 전송**하는 방식은 POST이다. 이미 인증된 사용자의 세션을 이용해 본인이 의도하지 않은 요청을 보내도록 유도하는 공격은 **CSRF**이다.

빈칸별 해설

(가) POST: POST는 요청 몸체에 담긴 데이터를 서버가 처리하도록 요청하는 메서드이다. 지문에서는 공격자가 의도한 데이터를 **HTTP 몸체에 첨부하여 페이지 내용을 변경**하므로 POST에 해당한다. GET은 주로 자원을 조회하는 메서드이며, 일반적인 GET 방식의 폼 전송에서는 입력값을 URL의 쿼리 문자열에 담는다.

(나) CSRF: CSRF(사이트 간 요청 위조)는 인증된 사용자의 브라우저가 사용자의 의도와 다른 요청을 웹사이트에 보내도록 유도하는 공격이다. 세션 쿠키 등 인증 정보가 요청에 함께 전달되면, 서버는 이를 해당 사용자의 요청으로 받아들일 수 있다. 지문의 '활성 세션'과 '자신도 인지하지 못한 채 페이지 내용을 변경하는 요청'은 **기존 인증 상태를 악용한 요청 위조**를 가리킨다. XSS는 웹사이트에 삽입된 악성 스크립트가 사용자의 브라우저에서 실행되는 공격으로, 구별의 핵심은 악성 스크립트의 삽입과 실행이다.

따라서 (가)는 POST, (나)는 CSRF이며, 이 조합은 ④와 일치한다.

NoteBase

문 15. S/MIME(RFC 8551)의 데이터 콘텐트 유형(data content type) 중 데이터의 기밀성만을 제공하는 것은?

① Signed-Data

② Enveloped-Data

③ Auth-Enveloped-Data

④ Compressed-Data

정답 2번

간단한 해설

Enveloped-Data는 메시지를 암호화하여 **기밀성만** 제공한다. Auth-Enveloped-Data는 기밀성에 무결성까지 제공하므로 '기밀성만'이라는 조건과 구별된다.

공통 해설

기밀성은 허가받지 않은 사람이 데이터 내용을 알 수 없도록 하는 성질이고, 무결성은 데이터의 무단 변경을 탐지할 수 있도록 하는 성질이다. 이 문항은 각 데이터 콘텐트 유형 자체가 제공하는 기능 중 **기밀성만 제공하는 유형**을 묻는다.

Enveloped-Data는 메시지 내용을 암호화하여 기밀성을 제공하지만, 그 자체로 메시지 무결성을 제공하지는 않는다. Auth-Enveloped-Data는 **기밀성과 무결성을 함께 제공**하므로, 단순히 암호화 여부만 보면 두 유형을 구별할 수 없다. 따라서 '기밀성만'에 대응하는 유형은 Enveloped-Data이다.

같은 기준에서 Signed-Data의 전자서명은 인증·메시지 무결성·출처 부인방지를 제공하며, 메시지 내용을 숨기는 기능은 아니다. Compressed-Data의 압축도 메시지 크기를 줄이는 기능으로, 그 자체로 기밀성을 제공하지 않는다.

NoteBase

문 16. 리눅스 /etc/shadow 파일에 포함되지 않는 것은?

① 사용자 계정명

② 솔트(salt)

③ 대칭키 암호 알고리즘의 종류

④ 기준일(epoch)부터 패스워드가 최종 수정된 날까지의 일수

정답 3번

간단한 해설

/etc/shadow의 패스워드 정보는 **복호화가 아니라 해시값 비교**에 사용된다. 패스워드 필드에 들어갈 수 있는 알고리즘 식별자는 대칭키 암호 알고리즘의 종류가 아니라 **패스워드 해시 방식**을 나타낸다.

선지별 해설

① O: 사용자 계정명은 /etc/shadow의 첫 번째 필드에 저장된다. 해당 계정의 패스워드 정보와 유효기간 정보를 어느 사용자에게 적용할지 식별하는 값이다.

② O: 솔트(salt)는 패스워드 해시를 계산할 때 함께 사용하는 값이며, **패스워드 필드의 저장 문자열에 포함**된다. 로그인할 때도 같은 솔트를 사용해야 저장된 해시와 비교할 수 있다. 솔트를 다르게 사용하면 같은 패스워드라도 저장되는 해시가 달라지도록 할 수 있다.

③ X: /etc/shadow에는 대칭키 암호 알고리즘의 종류를 저장하는 항목이 없다. 패스워드를 대칭키로 복호화하여 확인하는 대신, 입력한 패스워드와 저장된 솔트로 해시를 계산하여 저장 값과 비교한다. 패스워드 필드에 기록될 수 있는 알고리즘 식별자는 **패스워드 해시 방식의 식별자**로 구분해야 한다.

④ O: 세 번째 필드에는 **1970년 1월 1일 00:00:00 UTC**를 기준으로 패스워드가 마지막으로 변경된 날까지의 일수가 저장된다. 이는 마지막 변경일부터 오늘까지 지난 일수가 아니라, 고정된 기준일부터 마지막 변경일까지의 일수이다.

NoteBase

문 17. 소수 p를 선택하고, 위수가 p−1인 원시근을 사용하는 대신에 p−1의 소인수인 q를 위수로 갖는 원소를 이용해서 서명과 검증에 사용할 키를 생성하는 전자서명 구조는?

① RSA

② ElGamal

③ ECDSA

④ Schnorr

정답 4번

간단한 해설

Schnorr 서명은 소수 p에 대해 p−1의 소인수 q를 택하고, **위수가 q인 부분군**에서 키를 생성한다. 전체 곱셈군을 생성하는 원시근 대신 이 부분군의 생성원을 쓴다는 것이 핵심이다.

공통 해설

소수 p를 법으로 하는 0이 아닌 나머지들은 곱셈에 대해 p−1개의 원소를 가진 군을 이룬다. 원소 g의 위수는 g^t ≡ 1 ±od p을 만족하는 가장 작은 양의 정수 t이다. 원시근의 위수는 p−1이므로, 그 거듭제곱으로 전체 곱셈군의 원소를 생성할 수 있다.

Schnorr 서명은 p−1의 소인수 q를 정하고, **위수가 q인 원소 g**를 선택한다. g의 거듭제곱들이 이루는 부분군에는 q개의 원소가 있으며, g^q ≡ 1 ±od p이 성립한다. 이 부분군에서 비밀키 x를 정하고, g의 거듭제곱을 법 p로 계산하여 공개키를 만든다. 즉, 문제의 조건은 전체 군 대신 소수 위수의 부분군을 이용하는 Schnorr의 키 생성 구조를 가리킨다.

기본 ElGamal 서명은 위수가 p−1인 원시근을 사용한다. 따라서 이 문항에서는 단순히 소수 p를 이용한다는 사실보다, 생성원의 위수를 **p−1에서 그 소인수 q로 제한한다**는 조건으로 구별한다.

NoteBase

문 18. TLS 핸드셰이크 프로토콜의 목적에 해당하는 것만을 모두 고르면?

ㄱ. 인증서 확인
ㄴ. 세션을 활성 상태로 유지
ㄷ. 세션키 생성 및 교환
ㄹ. 응용 데이터 전송

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 1번

간단한 해설

TLS 핸드셰이크는 안전한 통신을 준비하면서 **인증서를 통한 상대 인증**과 **세션키 설정**을 수행한다. 응용 데이터는 이렇게 마련한 키를 이용하여 레코드 프로토콜로 보호해 전송한다.

보기별 해설

ㄱ. O: 인증서 기반 인증에서는 인증서의 서명, 유효기간, 신뢰 경로 등을 확인하여 **통신 상대의 신원을 검증**한다. 이는 핸드셰이크에서 수행하는 상대 인증에 해당한다.

ㄴ. X: 세션을 활성 상태로 유지하는 것은 연결 유지·관리의 문제이다. 핸드셰이크의 목적은 **보안 통신에 필요한 인증과 암호 매개변수·키 설정**이며, 세션을 계속 활성 상태로 유지하기 위한 주기적 확인 절차는 여기에 해당하지 않는다.

ㄷ. O: 핸드셰이크에서는 키 교환에 필요한 정보를 주고받아 공유 비밀값을 마련하고, 이를 바탕으로 양쪽이 사용할 **세션키를 도출**한다. 이 키는 이후 응용 데이터의 암호화 등 데이터 보호에 사용된다.

ㄹ. X: 응용 데이터 전송은 **레코드 프로토콜**을 통해 이루어진다. 레코드 프로토콜은 설정된 키와 암호 알고리즘을 이용하여 데이터를 보호해 전달하며, 핸드셰이크는 이러한 전송에 필요한 보안 조건을 마련한다.

핸드셰이크의 목적에 해당하는 보기는 ㄱ과 ㄷ이며, ①의 조합과 일치한다.

NoteBase

문 19. 다음 수식으로 표현된 HMAC에 대한 설명으로 옳지 않은 것은? (단, K는 키, M은 메시지, H는 해시 함수, ⊕는 XOR, ||는 연결(concatenation)이다)

HMAC(K,M)=H((K^+opad)\|H((K^+ipad)\|M))

① HMAC 구조는 해시 함수 H로 MD5, SHA-1, SHA-512 등 가용한 것을 선택할 수 있도록 되어 있다.

② K는 HMAC를 주고받는 사용자가 공유하는 비밀키이다.

③ K^+는 K의 왼쪽에 0을 패딩해서 전체 비트 수가 해시 함수 출력의 크기와 같게 되도록 한 것이다.

④ ipad와 opad는 각각 16진수 36과 5C가 반복된 것으로, 해시 함수에 입력되는 블록의 크기와 같다.

정답 3번

간단한 해설

HMAC의 키 패딩은 키의 **오른쪽에 0을 채워 입력 블록 크기**에 맞추는 과정이다. 왼쪽에 채우거나 해시 출력 크기에 맞추는 것이 아니다.

선지별 해설

① O: HMAC은 **기반 해시 함수를 바꿀 수 있는 구조**이다. H에 MD5, SHA-1, SHA-512 등을 적용할 수 있으며, 선택한 해시 함수에 따라 입력 블록 크기와 해시 출력 크기가 정해진다.

② O: K는 송신자와 수신자가 **공유하는 비밀키**이다. 송신자는 이 키와 메시지로 HMAC 값을 만들고, 수신자는 같은 키와 수신한 메시지로 값을 다시 계산하여 전달받은 값과 비교한다. 이를 통해 메시지의 무결성과 인증을 확인한다.

③ X: K^+는 키의 **오른쪽에 0을 채워 해시 함수의 입력 블록 크기**에 맞춘 값이다. 키가 입력 블록보다 길면 먼저 H로 해시한 뒤, 그 결과의 오른쪽에 0을 채운다. 키가 입력 블록 크기와 같으면 0을 추가하지 않는다. 따라서 '왼쪽'은 '오른쪽'으로, '해시 함수 출력의 크기'는 '해시 함수 입력 블록의 크기'로 고쳐야 한다. 예를 들어 SHA-1은 입력 블록이 64바이트이고 출력이 20바이트이므로, 패딩된 키의 길이는 20바이트가 아니라 64바이트이다.

④ O: ipad는 1바이트 값 0x36을, opad는 1바이트 값 0x5C를 **입력 블록 크기만큼 반복**한 값이다. 두 값은 K^+와 길이가 같아 비트별 XOR을 할 수 있다. 수식에서 ipad는 메시지와 함께 내부 해시에 사용되고, opad는 내부 해시 결과와 함께 외부 해시에 사용된다.

NoteBase

문 20. 다음 수식으로 나타낸 블록 암호 운용 모드에 대한 설명으로 옳은 것은?

P_i: 평문 블록 C_i: 암호문 블록 E_K: 암호화 함수 K: 키 IV: 초기벡터	$C_1 = E_K(P_1 \oplus IV)$ $C_i = E_K(P_i \oplus C_{i-1}),\ i = 2, 3, ..., N$

① 복호화 함수를 D_K이라고 하면, 평문 블록 $P_1 = D_K(C_1) \oplus IV$이고, $P_i = D_K(C_i) \oplus C_{i-1},\ i = 2, 3, ..., N$이다.

② 송신자와 수신자가 공유하는 IV는 반드시 제3자에게 비밀로 해야 한다.

③ 암호문 블록 C_j ($j = 1, 2, ..., N$)의 전송 도중에 비트 오류가 발생하면, 복호화된 P_j부터 P_N까지의 모든 평문 블록에 영향을 미친다.

④ 여러 평문 블록에 대한 암호화 과정의 병렬처리가 가능하다.

정답 1번

간단한 해설

제시된 수식은 이전 암호문 블록을 평문과 XOR한 뒤 암호화하는 **CBC 모드**이다. 복호화할 때는 암호문에 복호화 함수를 적용한 결과를 **이전 암호문 블록과 다시 XOR**하며, 첫 블록에는 이전 암호문 대신 초기벡터를 사용한다.

NoteBase

선지별 해설

① O: CBC에서는 암호화 전에 평문과 이전 암호문을 XOR한다. 따라서 암호문에 복호화 함수 D_K를 적용하면 두 값이 XOR된 상태로 돌아온다. 여기에 **이전 암호문을 다시 XOR하면** 같은 값이 상쇄되어 평문이 복원된다. 첫 블록은 $P_1 = D_K(C_1) \oplus IV$이고, 두 번째부터 N번째 블록까지는 $P_i = D_K(C_i) \oplus C_{i-1}$이다.

② X: 초기벡터 IV는 첫 평문 블록과 XOR하는 값이며, 비밀키와 달리 **제3자에게 공개되어도 된다**. 다만 CBC의 초기벡터는 암호화 전에 예측할 수 없도록 생성해야 한다. 비밀로 유지해야 하는 암호키 K와 초기벡터의 요구사항을 구별해야 한다.

③ X: 암호문 블록 C_j에 전송 중 비트 오류가 생기면, P_j에서는 복호화 함수의 입력이 바뀌어 비트 오류가 불규칙하게 발생한다. 다음 블록 P_{j+1}에서는 오류가 난 C_j를 XOR하므로 같은 위치의 비트가 뒤집힌다. 영향은 **해당 평문 블록과 바로 다음 평문 블록에 한정**되며, 그 뒤의 블록은 오류가 없는 암호문들로 복호화하므로 영향을 받지 않는다. C_N에 오류가 생긴 경우에는 다음 블록이 없으므로 P_N만 영향을 받는다.

④ X: 하나의 메시지를 CBC로 암호화할 때는 현재 블록을 처리하려면 **이전 블록의 암호화 결과가 먼저 필요**하므로 블록 간 병렬처리가 불가능하다. 반면 복호화에서는 수신된 각 암호문 블록에 복호화 함수를 독립적으로 적용한 뒤 이전 암호문과 XOR할 수 있으므로 병렬처리가 가능하다.

NoteBase