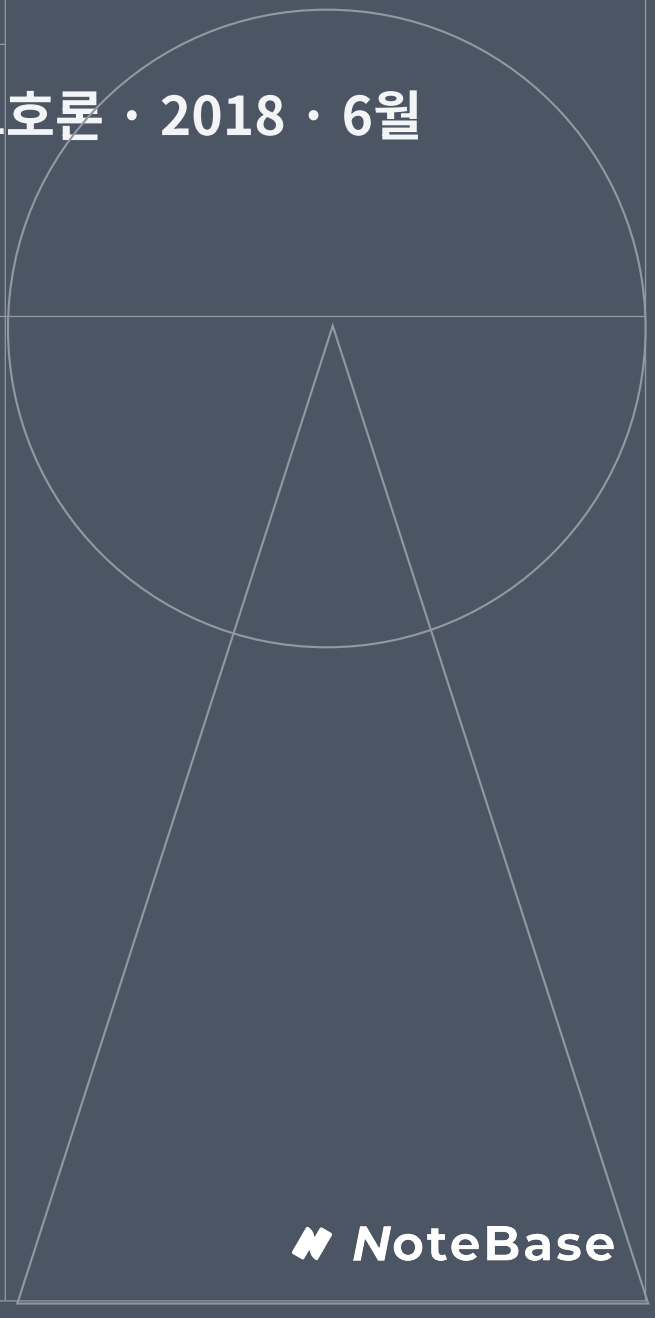
기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2018 · 6월



NoteBase

기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2018 · 6월

공무원/서울시/9급 · 정보보호론 · 2018 · 6월

문 1. 2009년 Moxie Marlinspike가 제안한 공격 방식이며, 중간자 공격을 통해 사용자와 서버 사이의 HTTPS 통신을 HTTP로 변경해서 비밀번호 등을 탈취하는 공격 방식으로 가장 옳은 것은?

① SSL stripping

② BEAST attack

③ CRIME attack

④ Heartbleed

정답 1번

간단한 해설

SSL stripping은 중간자가 HTTPS로의 전환을 가로막아 사용자 쪽 통신을 **암호화되지 않은 HTTP**로 유지하고, 이를 통해 비밀번호 등을 탈취하는 공격이다.

공통 해설

SSL stripping은 사용자와 서버 사이에 끼어든 공격자가 HTTPS 연결로 유도하는 링크나 리다이렉트를 HTTP로 바꾸어, **사용자와 공격자 사이의 통신을 평문으로 유지**하는 공격이다. 2009년 Moxie Marlinspike가 공개한 방식으로, 문제의 'HTTPS 통신을 HTTP로 변경하여 비밀번호 등을 탈취한다'는 설명에 해당한다.

예를 들어 사용자가 HTTP 페이지에서 로그인 링크를 누를 때, 중간자가 그 링크를 HTTP로 바꾸면 사용자는 비밀번호를 암호화되지 않은 상태로 전송하게 된다. 공격자는 사용자와는 HTTP로, 실제 서버와는 HTTPS로 통신을 중계하면서 비밀번호를 읽을 수 있다. 핵심은 이미 성립한 TLS 연결의 암호를 해독하는 것이 아니라 **사용자 쪽의 HTTPS 연결 성립을 막는 것**이다.

NoteBase

문 2. XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?

① 게시판 등의 웹페이지에 악의적인 코드 삽입이 가능하다는 취약점이 있다.

② 공격 코드를 삽입하는 부분에 따라 저장 XSS 방식과 반사 XSS 방식이 있다.

③ 악성코드가 실행되면서 서버의 정보를 유출하게 된다.

④ Javascript, VBScript, HTML 등이 사용될 수 있다.

정답 3번

간단한 해설

XSS의 악성 스크립트는 **사용자의 브라우저에서 실행**된다. 서버 내부 정보를 직접 유출하는 공격으로 설명한 것이 잘못이며, 대표적인 피해는 브라우저가 접근할 수 있는 쿠키·세션 정보 등의 탈취이다.

선지별 해설

① O: 사용자 입력을 안전하게 처리하지 않고 웹페이지에 출력하면, 공격자가 게시글이나 댓글 등에 넣은 코드가 페이지의 일부로 전달될 수 있다. 다른 사용자가 이를 열었을 때 브라우저가 **단순한 글이 아닌 실행할 코드로 해석**하면서 XSS가 발생한다.

② O: 저장 XSS는 공격 코드가 게시판이나 데이터베이스 등에 **저장된 뒤** 해당 내용을 조회하는 사용자에게 전달되는 방식이다. 반사 XSS는 공격 코드가 포함된 요청 값이 검색 결과나 오류 메시지 등의 **응답에 반영**되어 사용자에게 돌아오는 방식이다. 두 방식 모두 최종적으로 사용자의 브라우저에서 코드가 실행된다.

③ X: XSS의 실행 위치와 주된 피해 대상을 잘못 설명했다. 악성 스크립트는 서버 내부가 아니라 **피해자의 브라우저에서 해당 웹사이트의 권한으로 실행**된다. 따라서 '서버의 정보를 유출'한다는 설명은 '사용자의 브라우저에서 접근 가능한 쿠키·세션 정보 등을 탈취할 수 있다'로 고쳐야 한다. 모든 쿠키를 읽을 수 있는 것은 아니며, 스크립트의 접근이 허용된 정보가 대상이 된다.

④ O: XSS에는 JavaScript가 주로 사용되며, HTML의 태그나 이벤트 속성도 악성 스크립트를 실행하는 통로가 될 수 있다. VBScript 역시 이를 지원하던 Internet Explorer 등의 환경에서 사용될 수 있었다. 사용 가능한 코드는 **브라우저가 해석·실행하는 기능**에 따라 달라진다.

NoteBase

문 3. <보기>에서 설명하는 보안 목적으로 가장 옳은 것은?

<보기>
정보가 허가되지 않은 방식으로 바뀌지 않는 성질

① 무결성 (Integrity)
② 가용성 (Availability)
③ 인가(Authorization)
④ 기밀성 (Confidentiality)

정답 1번

간단한 해설

정보가 허가되지 않은 방식으로 변경되지 않도록 보장하는 성질은 **무결성**이다. 핵심은 정보 내용이 부당하게 바뀌지 않는다는 데 있다.

공통 해설

무결성(Integrity)은 **허가되지 않은 변경으로부터 정보를 보호**하는 성질이다. 보기의 '정보가 허가되지 않은 방식으로 바뀌지 않는 성질'은 이 정의에 해당한다. 여기서 변경을 막는다는 것은 모든 수정을 금지한다는 뜻이 아니라, 허용된 절차와 권한을 벗어난 수정을 막는다는 뜻이다. 예를 들어 성적 자료를 권한 없는 사람이 임의로 고쳐 점수를 바꾸었다면 무결성이 침해된 것이다.

NoteBase

문 4. 「개인정보 보호법」상 용어 정의로 가장 옳지 않은 것은?

① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

② 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람

③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위

④ 개인정보관리자: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

정답 4번

간단한 해설

④가 설명하는 법정 용어는 '개인정보관리자'가 아니라 **'개인정보처리자'**이다. 업무 목적으로 개인정보파일을 운용하기 위해 개인정보를 직접 처리하거나 다른 사람을 통해 처리하는 주체를 뜻한다.

선지별 해설

① O: 「개인정보 보호법」 제2조제1호에 따르면, 살아 있는 사람의 성명·주민등록번호·영상 등으로 그 사람을 식별할 수 있으면 개인정보에 해당한다. 핵심은 **살아 있는 개인을 알아볼 수 있는 정보**라는 점이다. 그 정보만으로 식별하기 어려워도 다른 정보와 쉽게 결합하여 식별할 수 있는 경우 역시 포함된다.

② O: 제2조제3호의 정보주체는 **처리되는 정보가 누구에 관한 것인지**를 기준으로 정해진다. 예를 들어 회사가 보유한 고객정보에서 식별되는 고객이 정보주체이다. 정보를 수집하거나 보관하는 회사 자체를 가리키는 말이 아니다.

③ O: 제2조제2호의 처리는 개인정보를 수집하거나 이용하는 행위뿐 아니라 **저장·보유·파기 등도 포함**하는 넓은 개념이다. 다른 정보와 연계하거나 연동하는 행위, 잘못된 내용을 정정하거나 정보를 복구하는 행위도 처리에 해당하므로 선지의 열거는 법의 정의에 부합한다.

④ X: 제2조제5호에서 이러한 주체를 부르는 용어는 **'개인정보처리자'**이다. 따라서 '개인정보관리자'를 '개인정보처리자'로 고쳐야 한다. 업무상 개인정보파일을 운용하려고 개인정보를 직접 다루거나 타인을 통해 다루는 주체가 이에 해당하며, 공공기관·법인·단체뿐 아니라 개인도 포함될 수 있다.

NoteBase

문 5. Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?

① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.

② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.

③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.

④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

정답 3번

간단한 해설

AES는 Feistel 구조가 아니라 치환과 순열을 반복하는 **SPN 구조**를 사용한다. Feistel 구조를 사용하는 대표적인 대칭키 블록 암호는 DES이다.

선지별 해설

① O: 평문 블록의 길이, 키의 길이, 라운드 수는 Feistel 암호의 보안 강도를 좌우하는 주요 설계 요소이다. 키가 길면 전수조사할 키 후보가 많아지고, 충분한 라운드를 거치면 평문과 키의 영향이 블록 전체로 퍼져 분석이 어려워진다. 블록 길이는 같은 키로 많은 데이터를 처리할 때 블록의 반복 등에 영향을 준다. 다만 **이 세 요소만으로 안전성이 보장되는 것은 아니며**, 라운드 함수와 라운드 키 생성 방식도 중요하다.

② O: Feistel 구조에서는 암호화와 복호화에 **같은 연산 구조를 사용하되 라운드 키를 역순으로 적용**한다. 한쪽 절반에 라운드 함수를 적용한 결과를 다른 쪽 절반과 XOR하는데, 같은 값으로 XOR를 다시 하면 원래 값이 복원된다. 이 성질 때문에 복호화할 때 라운드 함수 자체의 역함수를 구할 필요가 없다. 따라서 '동일하다'는 키의 적용 순서까지 같다는 뜻이 아니다.

③ X: AES는 **SPN(Substitution-Permutation Network) 구조**를 사용한다. 블록 전체를 바이트 배열로 다루면서 바이트 치환, 행 이동, 열 혼합, 라운드 키 결합 등의 변환을 수행한다. 블록을 좌우로 나누고 한쪽의 라운드 함수 결과를 다른 쪽과 결합하는 Feistel 구조와 구별된다. 'AES는 Feistel 암호 방식을 사용한다'는 'AES는 SPN 구조를 사용한다'로 고쳐야 한다.

④ O: Feistel 구조는 DES와 같은 **대칭키 블록 암호**를 구성하는 데 사용된다. 대칭키 암호에서는 송신자와 수신자가 같은 비밀키를 공유하며, 이 비밀키에서 생성한 라운드 키를 암호화와 복호화에 사용한다. Feistel은 이러한 블록 암호의 내부 연산을 구성하는 방식이다.

NoteBase

문 6. 디지털 서명에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

<보기>
ㄱ. 디지털 서명은 부인방지를 위해 사용할 수 있다.
ㄴ. 디지털 서명 생성에는 개인키를 사용하고 디지털 서명 검증에는 공개키를 사용한다.
ㄷ. 해시 함수와 공개키 암호를 사용하여 생성된 디지털 서명은 기밀성, 인증, 무결성을 위해 사용할 수 있다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 1번

간단한 해설

디지털 서명은 서명자의 확인과 내용 변경의 탐지를 통해 인증·무결성·부인방지를 지원한다. 하지만 **메시지 내용을 숨기는 기밀성은 제공하지 않으므로**, 기밀성이 필요하면 별도의 암호화를 적용해야 한다.

보기별 해설

ㄱ. O: 부인방지는 서명자가 나중에 자신이 서명했다는 사실을 부정하지 못하도록 하는 것이다. 서명자의 개인키로 생성한 서명은 대응하는 공개키로 검증할 수 있어 **서명 사실을 입증하는 근거**가 된다. 이를 위해서는 개인키가 안전하게 관리되고 공개키가 실제 서명자의 것인지 확인되어야 한다.

ㄴ. O: 디지털 서명은 **개인키로 생성하고 대응하는 공개키로 검증**한다. 개인키는 서명자만 보유하도록 비밀로 관리하며, 검증자는 서명자의 개인키를 전달받지 않고도 공개키로 서명을 확인할 수 있다.

ㄷ. X: 해시 함수와 공개키 암호 기술을 이용한 디지털 서명은 서명자의 확인을 통한 인증과 메시지 변경 여부를 확인하는 무결성을 제공한다. 그러나 서명을 붙였다고 메시지 자체가 암호문으로 바뀌는 것은 아니므로 **기밀성은 제공하지 않는다**. 따라서 제공 기능은 인증·무결성·부인방지로 고쳐야 하며, 내용을 숨기려면 별도의 암호화가 필요하다.

옳은 보기는 ㄱ, ㄴ이며, 이 조합은 ①에 해당한다.

NoteBase

문 7. 분산반사 서비스 거부(DRDoS) 공격의 특징으로 가장 옳지 않은 것은?

① TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한다.

② 공격자의 추적이 매우 어려운 공격이다.

③ 악성 봇의 감염을 통한 공격이다.

④ 출발지 IP 주소를 위조하는 공격이다.

정답 3번

간단한 해설

DRDoS는 **악성 봇 감염을 전제로 하지 않고**, 정상 서버를 반사체로 이용해 공격 대상에 응답 트래픽을 집중시키는 공격이다. 요청의 출발지 IP 주소를 공격 대상의 주소로 위조하면 반사체의 응답이 공격 대상에게 향한다.

선지별 해설

분산반사 서비스 거부(DRDoS)는 여러 서버를 반사체로 이용하여 그 응답 트래픽을 공격 대상에 집중시키고, 네트워크나 시스템 자원을 소모시켜 서비스를 방해하는 공격이다.

① O: TCP를 이용한 반사 공격에서는 출발지 주소가 위조된 SYN 요청에 서버가 SYN/ACK로 응답하는 동작을 악용한다. 라우터가 **출발지 주소의 정당성을 검증하지 않고** 패킷을 전달하면 위조 요청이 반사체에 도달할 수 있다. 선지의 라우팅 테이블 운영상 취약성은 이러한 전달·검증상의 허점을 뜻한다.

② O: 피해자가 직접 받는 패킷의 출발지는 실제 공격자가 아니라 **여러 반사체의 주소**이다. 반사체가 받은 요청의 출발지 주소도 피해자의 주소로 위조되어 있으므로 실제 공격자를 추적하기 어렵다.

③ X: DRDoS는 **정상 서버를 감염시키지 않고도 반사체로 이용**할 수 있다. 악성 봇에 감염된 여러 기기가 직접 공격 트래픽을 보내는 전형적인 봇넷 기반 DDoS와 달리, DRDoS의 핵심은 위조 요청에 대한 정상 서버의 응답을 피해자에게 보내게 하는 것이다. 봇넷이 공격 요청을 보낼 수는 있지만, 봇 감염 자체가 DRDoS의 필수 조건은 아니다.

④ O: 요청 패킷의 **출발지 IP 주소를 공격 대상의 IP 주소로 위조**한다. 반사체는 그 주소를 요청자의 주소로 보고 응답하므로 응답 트래픽이 공격자 대신 공격 대상에게 전달된다.

NoteBase

문 8. 침입탐지시스템의 비정상행위 탐지 방법에 대한 설명으로 가장 옳지 않은 것은?

① 정상적인 행동을 기준으로 하여 여기서 벗어나는 것을 비정상으로 판단한다.

② 정량적인 분석, 통계적인 분석 등을 사용한다.

③ 오탐률이 높으며 수집된 다양한 정보를 분석하는 데 많은 학습 시간이 소요된다.

④ 알려진 공격에 대한 정보 수집이 어려우며, 새로운 취약성 정보를 패턴화하여 지식데이터베이스로 유지 및 관리하기가 쉽지 않다.

정답 4번

간단한 해설

④의 공격 정보를 패턴화하여 지식데이터베이스로 관리하는 부담은 **오용탐지(서명 기반 탐지)**의 한계이다. 비정상행위 탐지는 **정상행위에서 벗어나는 정도**를 이용하므로, 사전에 공격 패턴이 등록되지 않은 새로운 공격도 탐지할 수 있다.

선지별 해설

① O: 비정상행위 탐지는 사용자나 시스템의 정상적인 행동을 나타내는 프로파일을 만들고, 관측된 행동이 **정상 기준에서 크게 벗어나는지**를 판단한다. 알려진 공격 패턴과 일치하는지를 검사하는 방식과 구별된다.

② O: 접속 횟수나 트래픽 양처럼 행동 특성을 수치화하는 **정량적·통계적 분석**을 사용한다. 예를 들어 평소의 트래픽 양과 현재의 트래픽 양을 비교하여 정상 범위를 크게 벗어났는지 판단할 수 있다.

③ O: 정상적인 행동도 평소와 크게 달라지면 공격으로 판단할 수 있어 **오탐률이 높아질 수 있다**. 오탐은 정상행위를 공격으로 잘못 판단하는 것이다. 또한 정상행위의 다양한 양상을 반영하는 프로파일을 구축하려면 충분한 정보를 수집하고 분석하는 관찰·학습 시간이 필요하다.

④ X: 공격 정보를 수집하고 새로운 공격·취약성에 맞추어 패턴과 지식데이터베이스를 갱신하는 부담은 **오용탐지(서명 기반 탐지)**의 한계이다. 오용탐지는 저장된 공격 패턴과 관측된 행위를 대조한다. 비정상행위 탐지는 공격 패턴 대신 정상행위 프로파일과의 차이를 이용하므로, 사전에 패턴이 등록되지 않은 새로운 공격도 탐지할 수 있다.

NoteBase

문 9. 메모리 변조 공격을 방지하기 위한 기술 중 하나로, 프로세스의 중요 데이터 영역의 주소를 임의로 재배치하여 공격자가 공격 대상 주소를 예측하기 어렵게 하는 방식으로 가장 옳은 것은?

① canary

② ASLR

③ no-execute

④ Buffer overflow

정답 2번

간단한 해설

프로세스의 메모리 주소 배치를 무작위로 바꾸어 공격 대상의 위치를 예측하기 어렵게 하는 기술은 **ASLR(주소 공간 배치 무작위화)**이다.

공통 해설

ASLR(Address Space Layout Randomization)은 프로세스의 가상 주소 공간에서 스택·힙·공유 라이브러리 등의 **배치 주소를 무작위화**하는 기술이다. 공격자가 메모리를 변조해 실행 흐름을 바꾸려면 공격 코드나 이용하려는 함수 등의 위치를 알아야 하는 경우가 있는데, 주소 배치가 달라지면 미리 예상한 주소를 그대로 이용하기 어려워진다. 따라서 문항의 '주소를 임의로 재배치하여 공격 대상 주소를 예측하기 어렵게 한다'는 설명은 ASLR의 작동 원리에 해당한다. 이는 주소 예측을 어렵게 하여 공격 성공 가능성을 낮추는 방식이며, 버퍼 오버플로 같은 **메모리 오류 자체를 제거하는 것은 아니다**.

NoteBase

문 10. 퍼징(fuzzing)에 대한 설명으로 가장 옳은 것은?

① 사용자를 속여서 사용자의 비밀정보를 획득하는 방법이다.

② 실행코드를 난독화하여 안전하게 보호하는 방법이다.

③ 소프트웨어 테스팅 방법 중 하나로 난수를 발생시켜서 대상 시스템에 대한 결함이 발생하는 입력을 주입하는 방법이다.

④ 소스 코드를 분석하는 정적 분석 방법이다.

정답 3번

간단한 해설

퍼징은 **무작위·비정상 입력을 자동으로 주입**하여 프로그램의 오류나 취약점을 찾는 소프트웨어 테스트 기법이다. 프로그램을 실제로 실행하며 반응을 관찰하는 동적 테스트에 해당한다.

선지별 해설

① X: 사용자를 속여 비밀정보를 얻는 것은 **사회공학적 공격**에 해당한다. 퍼징은 사람을 속이는 대신 프로그램에 다양한 입력을 넣어 결함을 찾는다.

② X: 실행코드를 이해하거나 분석하기 어렵게 바꾸는 것은 **코드 난독화**이다. 퍼징은 코드를 보호하도록 변형하는 기법이 아니라 입력에 대한 실행 결과를 검사하는 테스트 기법이다.

③ O: 퍼징은 난수 등을 이용해 입력을 생성하거나 기존 입력을 변형한 뒤 대상 프로그램에 주입한다. 이때 비정상 종료나 오류 같은 반응을 관찰하여 **입력 처리 과정에 숨어 있는 결함**을 찾아낸다. 모든 입력에서 반드시 결함이 발생하는 것은 아니며, 결함을 드러내는 입력을 탐색하는 것이다.

④ X: 정적 분석은 프로그램을 실행하지 않고 소스 코드 등의 구조와 내용을 분석한다. 퍼징은 입력을 주입한 뒤 **프로그램을 실행하여 동작을 관찰**하므로 동적 테스트에 해당한다.

NoteBase

문 11. 보안 측면에서 민감한 암호 연산을 하드웨어로 이동함으로써 시스템 보안을 향상시키고자 나온 개념으로, TCG 컨소시엄에 의해 작성된 표준은?

① TPM

② TLS

③ TTP

④ TGT

정답 1번

간단한 해설

TPM은 TCG가 표준화한 신뢰 플랫폼 모듈로, **민감한 암호 연산과 암호키 보호를 하드웨어에서 수행**하여 시스템의 보안을 높인다.

공통 해설

TPM(Trusted Platform Module)은 TCG(Trusted Computing Group)가 표준화한 신뢰 플랫폼 모듈이다. 암호키를 생성·보호하고 암호 연산을 수행하는 보안 기능을 제공한다. 문제의 핵심 조건인 **하드웨어를 통한 민감한 암호 연산의 보호**에 대응하는 명칭이 TPM이다.

예를 들어 TPM에서 외부로 내보낼 수 없도록 생성한 개인키로 전자서명을 수행하면, 응용 프로그램은 TPM에 서명을 요청하고 서명 결과를 받는다. 이때 **개인키 자체를 응용 프로그램에 전달하지 않고** 연산할 수 있으므로, 소프트웨어에서 키가 노출될 위험을 줄인다.

NoteBase

문 12. 사회 공학적 공격 방법에 해당하지 않는 것은?

① 피싱
② 파밍
③ 스미싱
④ 생일 공격

정답 4번

간단한 해설

생일 공격은 **생일 역설에 따른 충돌 확률**을 이용하는 암호학적 공격이다. 사람을 속여 정보 제공이나 특정 행동을 유도하는 사회 공학적 공격과 구별된다.

공통 해설

사회 공학적 공격은 **사람의 신뢰와 심리를 악용**하여 민감한 정보를 내놓거나 공격자에게 유리한 행동을 하도록 유도하는 방식이다. 공격에 기술적 수단이 쓰이더라도, 사용자가 속아서 정보를 제공하게 만드는 부분은 사회 공학적 요소이다.

피싱은 신뢰할 만한 기관 등을 사칭한 메시지나 가짜 웹사이트로 사용자를 속이고, 스미싱은 문자 메시지를 이용해 같은 방식으로 정보 제공이나 악성 앱 설치 등을 유도한다. 파밍은 접속 경로를 조작해 사용자를 가짜 웹사이트로 보내며, 사용자가 그곳을 정상 사이트로 믿고 개인정보를 입력하도록 속인다. 세 방법은 전달·접속 방식에는 차이가 있지만, 사용자의 신뢰를 악용해 정보를 빼내거나 행동을 유도한다는 공통점이 있다.

생일 공격은 생일 역설을 이용하여 서로 다른 입력에서 **같은 해시값이 나오는 충돌** 등을 찾는 암호학적 공격이다. 여러 사람 중 생일이 같은 두 사람이 있을 확률처럼, 여러 입력의 출력값 중 같은 값이 나타날 확률을 이용한다. 사람의 생일 정보를 알아내거나 심리를 조종하는 공격이 아니므로 사회 공학적 공격에 해당하지 않는다.

NoteBase

문 13. 접근 제어 방식 중, 주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산 시스템 환경에서 많이 사용되는 방식은?

① 접근 제어 행렬(Access Control Matrix)

② 접근 가능 목록(Capability List)

③ 접근 제어 목록(Access Control List)

④ 방화벽(Firewall)

정답 2번

간단한 해설

접근 가능 목록(Capability List)은 한 주체를 기준으로 접근할 수 있는 객체와 각 객체에 허용된 권한을 묶은 목록이다. 객체를 기준으로 접근할 주체들을 나열하는 접근 제어 목록과 관점이 다르다.

공통 해설

접근 가능 목록(Capability List)은 **주체별로 객체와 접근 권한을 나열**하는 방식이다. 주체는 사용자나 프로세스처럼 접근을 요청하는 쪽이고, 객체는 파일처럼 접근 대상이 되는 자원이다. 목록의 각 항목에는 대상 객체와 그 객체에 허용된 읽기·쓰기 등의 연산이 함께 들어간다.

예를 들어 프로세스 P의 목록에 '파일 A: 읽기', '파일 B: 읽기·쓰기'가 있다면, P는 A를 읽을 수 있고 B를 읽거나 쓸 수 있다. 이처럼 '이 주체가 어떤 객체에 어떤 연산을 할 수 있는가'를 나타내는 목록이 문제에서 설명한 접근 가능 목록이다.

접근 제어 행렬에서 행을 주체, 열을 객체로 두면 접근 가능 목록은 **한 주체에 해당하는 행**의 권한 정보를 목록으로 표현한 것이다. 반면 접근 제어 목록(Access Control List)은 한 객체에 해당하는 열을 기준으로, 그 객체에 접근할 수 있는 주체와 권한을 묶는다.

NoteBase

문 14. WPA2를 공격하기 위한 방식으로, WPA2의 4-way 핸드셰이크(handshake) 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격 방식으로 가장 옳은 것은?

① KRACK
② Ping of Death
③ Smurf
④ Slowloris

정답 1번

간단한 해설

KRACK은 WPA2 핸드셰이크 메시지를 조작·재전송하여 이미 사용 중인 암호화 키의 **재설치**를 유도하는 공격이다. 키 재설치로 암호화에 쓰이는 값이 재사용되면 무선 통신 내용이 노출될 수 있다.

공통 해설

KRACK(Key Reinstallation Attack)은 WPA2의 키 설치 절차를 악용하는 '키 재설치 공격'이다. 4-way 핸드셰이크는 무선 단말과 액세스 포인트가 통신에 사용할 키를 확인하고 설치하는 절차이다. 취약한 단말은 이 과정의 세 번째 메시지를 다시 받으면 **이미 설치한 키를 다시 설치**할 수 있다. 공격자는 핸드셰이크 메시지를 조작·재전송하여 이 동작을 유도한다.

키를 재설치할 때 패킷 암호화에 사용하는 번호인 nonce와 수신 재전송 검사용 카운터가 초기화되면, 같은 키 아래에서 nonce가 재사용될 수 있다. 이는 암호화의 안전성을 훼손하여 통신 내용의 복호화·노출로 이어질 수 있다. 따라서 문항의 식별 기준은 **WPA2 핸드셰이크를 이용한 키 재설치**이며, 이 작동 방식을 가리키는 명칭이 KRACK이다.

NoteBase

문 15. 오일러 함수 $\phi()$를 이용해 정수 $n = 15$에 대한 $\phi(n)$을 구한 값으로 옳은 것은? (단, 여기서 오일러 함수 $\phi()$는 RSA 암호 알고리즘에 사용되는 함수이다.)

① 1

② 5

③ 8

④ 14

정답 3번

간단한 해설

$15 = 3 \times 5$이므로 15와 **서로소인 수**는 3과 5 어느 쪽의 배수도 아닌 수이다. 1부터 15까지에서 이 조건을 만족하는 자연수는 8개이므로 $\phi(15) = 8$이다.

계산 과정

오일러 함수 $\phi(n)$은 1부터 n까지의 자연수 중 **n과 서로소인 수의 개수**이다. 서로소란 두 수의 최대공약수가 1이라는 뜻이다. 15의 소인수는 3과 5이므로, 15와 서로소이려면 3의 배수도 5의 배수도 아니어야 한다.

1부터 15까지 총 15개 중 3의 배수는 3, 6, 9, 12, 15로 5개이고, 5의 배수는 5, 10, 15로 3개이다. 두 개수를 각각 빼면 **공통 배수인 15를 두 번 제외**하므로 1개를 다시 더한다. 따라서 서로소인 수의 개수는 $15 - 5 - 3 + 1 = 8$개이다.

따라서 $\phi(15) = 8$이며, 이는 ③의 8에 해당한다.

NoteBase

문 16. 능동적 공격으로 가장 옳지 않은 것은?

① 재전송

② 트래픽 분석

③ 신분위장

④ 메시지 변조

정답 2번

간단한 해설

트래픽 분석은 통신 내용이나 흐름을 바꾸지 않고 통신량·빈도·송수신 관계 등을 관찰하여 정보를 추론하는 **수동적 공격**이다. 능동적 공격은 데이터나 시스템 동작에 개입한다.

공통 해설

능동적 공격과 수동적 공격을 가르는 기준은 **데이터나 시스템 동작에 개입하는가**이다. 능동적 공격은 데이터를 삽입·변조하거나 정상적인 동작에 영향을 주려는 공격이고, 수동적 공격은 대상의 데이터나 동작을 바꾸지 않은 채 정보를 얻으려는 공격이다.

재전송은 이전에 전송된 유효한 데이터를 다시 보내 수신자가 이를 처리하도록 시도하고, 신분위장은 정당한 사용자나 통신 주체인 것처럼 가장하여 시스템을 속인다. 메시지 변조는 전달되는 데이터의 내용을 바꾼다. 이들은 모두 통신이나 시스템 동작에 개입하므로 능동적 공격에 해당한다. 반면 트래픽 분석은 **통신 흐름을 관찰하여 정보를 추론**하므로 수동적 공격에 해당한다. 메시지 내용이 암호화되어 있어도 통신량·빈도·송수신 관계 등 관찰 가능한 특성을 분석할 수 있다.

NoteBase

문 17. 무선랜 보안에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

<보기>
ㄱ. WEP는 RC4 암호 알고리즘을 사용한다.
ㄴ. WPA는 AES 암호 알고리즘을 사용한다.
ㄷ. WPA2는 EAP 인증 프로토콜을 사용한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 2번

간단한 해설

WPA의 기본 암호화 방식은 AES가 아니라 **RC4 기반 TKIP**이다. WPA2의 EAP 사용은 **기업용 인증 모드**에 관한 설명이다.

보기별 해설

ㄱ. O: WEP는 **RC4 스트림 암호**를 사용하여 무선으로 전송하는 데이터의 내용을 암호화한다. 따라서 WEP의 암호 알고리즘을 RC4로 설명한 것은 옳다.

ㄴ. X: WPA의 기본 암호화 방식은 **RC4 기반의 TKIP**이다. TKIP는 WEP의 취약한 키 사용 방식 등을 보완한 프로토콜이며, 내부 암호 알고리즘으로 RC4를 사용한다. AES 기반 CCMP를 기본 암호화 방식으로 사용하는 것은 WPA2이다.

ㄷ. O: WPA2는 **기업용 모드에서 IEEE 802.1X/EAP**를 이용하여 사용자를 인증한다. EAP는 여러 인증 방식을 수용하는 인증 프레임워크로, 데이터 암호화에 쓰이는 AES와 역할이 다르다. 다만 WPA2의 모든 모드에서 EAP를 쓰는 것은 아니며, 개인용 모드는 사전 공유 키인 PSK를 사용한다.

옳은 보기는 ㄱ, ㄷ이므로 두 보기를 함께 고른 ②에 해당한다.

NoteBase

문 18. BLP(Bell & La Padula) 모델에 대한 설명으로 가장 옳지 않은 것은?

① 다단계 등급 보안(Multi Level Security) 정책에 근간을 둔 모델이다.

② 기밀성을 강조한 모델이다.

③ 수학적 모델이다.

④ 상업용 보안구조 요구사항을 충족하는 범용 모델이다.

정답 4번

간단한 해설

BLP는 군사·정부 환경의 다단계 보안정책을 바탕으로 **기밀성**을 보호하는 모델이다. 상업 환경에서 중요한 데이터의 정확성과 정당한 변경 같은 **무결성 요구까지 포괄하는 범용 모델은 아니다**.

선지별 해설

① O: BLP는 **다단계 등급 보안정책**을 형식화한 모델이다. 사용자나 프로세스인 주체에는 인가 수준을, 파일 등 객체에는 보안등급을 부여하고, 이들 사이의 등급 관계에 따라 접근을 통제한다.

② O: BLP의 주된 보호 목표는 허가받지 않은 주체에게 정보가 공개되지 않도록 하는 **기밀성**이다. 기본 규칙인 '상위 등급 읽기 금지(No Read Up)'는 낮은 등급의 주체가 높은 등급의 정보를 읽는 것을 막고, '하위 등급 쓰기 금지(No Write Down)'는 높은 등급의 정보가 낮은 등급의 객체로 흘러가는 것을 막는다.

③ O: BLP는 시스템의 상태와 상태 전이, 보안조건을 수학적으로 정의하는 **정형적 보안 모델**이다. 초기 상태가 안전하고 허용된 모든 상태 전이가 보안조건을 유지한다면 이후에도 안전한 상태가 유지됨을 논증한다. 여기서 안전하다는 것은 모델이 정한 기밀성 조건을 만족한다는 뜻이다.

④ X: BLP는 **군사·정부 환경의 기밀성 보호를 중심으로 한 모델**이다. 상업 환경에서는 거래 기록의 정확성 유지나 부당한 변경 방지 같은 무결성 요구도 중요하지만, BLP의 등급별 정보흐름 통제만으로 이러한 요구를 모두 보장할 수는 없다. 따라서 '상업용 보안구조 요구사항을 충족하는 범용 모델'이라는 설명은 부적절하다.

NoteBase

문 19. <보기>와 관련된 데이터베이스 보안 요구 사항으로 가장 옳은 것은?

<보기>
서로 다른 트랜잭션이 동일한 데이터 항목에 동시적으로 접근하여도 데이터의 일관성이 손상되지 않도록 하기 위해서는 로킹(locking) 기법 등과 같은 병행 수행 제어 기법 등이 사용되어야 한다.

① 데이터 기밀성
② 추론 방지
③ 의미적 무결성
④ 운영적 무결성

정답 4번

간단한 해설

서로 다른 트랜잭션이 같은 데이터에 동시에 접근하더라도 **데이터의 일관성을 유지**해야 한다는 요구가 운영적 무결성이다. 로킹은 충돌하는 접근을 제어하여 이를 보장하는 기법이다.

공통 해설

운영적 무결성은 여러 트랜잭션이 동시에 수행될 때 서로의 처리에 부당하게 영향을 주어 데이터의 일관성이 깨지는 것을 방지하는 요구 사항이다. 보기의 핵심은 **동일한 데이터 항목에 대한 동시 접근**으로 발생할 수 있는 충돌을 제어한다는 데 있다. 이처럼 병행 수행 과정의 일관성을 보호하는 요구는 운영적 무결성에 해당한다.

예를 들어 두 트랜잭션이 같은 값을 읽고 각자 수정한 뒤 저장하면, 나중에 저장한 결과가 앞선 수정 내용을 덮어써 갱신이 유실될 수 있다. 로킹은 데이터 항목에 잠금을 설정하여 **서로 충돌하는 접근을 제한**함으로써 이러한 문제를 방지한다.

NoteBase

문 20. RSA에 대한 설명으로 가장 옳지 않은 것은?

① AES에 비하여 암, 복호화 속도가 느리다.

② 키 길이가 길어지면 암호화 및 복호화 속도도 느려진다.

③ 키 생성에 사용되는 서로 다른 두 소수(p, q)의 길이가 길어질수록 개인키의 안전성은 향상된다.

④ 중간자(man-in-the-middle) 공격으로부터 안전하기 위해서는 2,048비트 이상의 공개키를 사용하면 된다.

정답 4번

간단한 해설

2,048비트 이상의 RSA 키를 사용해도 **공개키가 실제 통신 상대방의 것인지** 확인하지 않으면 중간자 공격을 막을 수 없다. 키 길이를 늘리는 것은 소인수분해 공격을 어렵게 하는 것이며, 중간자 공격을 막으려면 인증서 검증 등으로 **공개키와 소유자의 신원을 확인**해야 한다.

선지별 해설

① O: RSA는 공개키와 개인키를 사용하는 비대칭키 암호이고, AES는 같은 비밀키로 암호화와 복호화를 수행하는 대칭키 암호이다. RSA는 큰 정수의 모듈러 거듭제곱 연산을 수행하므로 일반적으로 AES보다 **암호화·복호화 속도가 느리다**. 따라서 대량의 데이터를 암호화할 때는 AES 같은 대칭키 암호를 주로 사용한다.

② O: RSA의 키 길이는 보통 모듈러스 n의 비트 길이를 뜻한다. 같은 구현과 연산 조건에서 키가 길어지면 **연산할 정수의 크기가 커져** 암호화와 복호화에 필요한 계산량이 증가한다. 따라서 일반적으로 처리 속도가 느려진다.

③ O: 일반적인 두 소수 기반 RSA에서 모듈러스 n은 서로 다른 소수 p와 q의 곱이다. 공격자가 n을 소인수분해하여 p와 q를 알아내면 공개키 정보와 함께 개인키를 계산할 수 있다. 적절히 생성한 p와 q의 비트 길이를 늘리면 n도 커져 **소인수분해가 더 어려워지므로**, 이러한 공격에 대한 개인키의 안전성이 높아진다.

④ X: 중간자 공격은 공격자가 통신 사이에 끼어들어 상대방을 사칭하는 공격이다. 예를 들어 공격자가 수신자의 공개키 대신 자신의 공개키를 전달하고 송신자가 이를 믿으면, 송신자는 공격자의 공개키로 암호화하게 된다. 공격자는 자신의 개인키로 내용을 복호화할 수 있으므로 수신자의 RSA 키가 2,048비트 이상이어도 이 공격은 막히지 않는다. 필요한 대책은 단순한 키 길이 증가가 아니라 **공개키 소유자 인증**이다. 신뢰할 수 있는 인증기관의 인증서를 검증하는 등의 방법으로 그 공개키가 실제 상대방의 것인지 확인해야 한다.

NoteBase