2019-지방직-정보보호론-A형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

해설에 대한 모든 권리는 곽후근(대방고시, 하이클래스)에 있습니다.

1번부터 10번 해설동영상은 https://www.youtube.com/watch?v=CHRCLjeJyoI&t=2167s,
11번부터 20번 해설동영상은 https://www.youtube.com/watch?v=emEriI9n9eU&t=148s
을 참고하기 바랍니다.

1. 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직은?

① CISO
② CERT
③ CPPG
④ CPO

정답 체크 :

(2) CERT : 1988년 11월 22일 저녁, 미국 전역의 컴퓨터가 모리스 웜에 의해 멎어버린 사건이 이후 미 정부가 적극적으로 적절한 침해 사고의 대응책을 마련했다. DARPA(The Defense Advanced Research Projects Agency)은 컴퓨터와 관련한 침해 사고에 적절히 대응하고자, 피치버그의 카네기 멜론 대학 내의 소프트웨어공학 연구소에 CERT(Computer Emergency Response Team) 팀을 만들었다.

오답 체크 :

(1) CISO : 최고정보보안임원(Chief Information Security Officer)은 조직의 정보 및 데이터 보안을 책임지는 임원이다. (CSO)

(3) CPPG : 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 갖춘 인력 또는 향후 기업 또는 기관의 개인정보 관리를 희망하는 자(비공인 민간 자격, Certified Privacy Protection General)

(4) CPO : 개인정보 보호책임자(Chief Privacy Officer), 홈페이지에 공개

2. OECD 개인정보보호 8개 원칙 중 다음에서 설명하는 것은?

개인정보 침해, 누설, 도용을 방지하기 위한 물리적.조직적. 기술적인 안전조치를 확보해야 한다.

① 수집 제한의 원칙(Collection Limitation Principle)
② 이용 제한의 원칙(Use Limitation Principle)
③ 정보 정확성의 원칙(Data Quality Principle)
④ 안전성 확보의 원칙(Security Safeguards Principle)

정답 체크 :

(4) 안정성 확보의 원칙

개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호장치를 마련해야 한다.

오답 체크 :

(1) 수집 제한의 원칙 : 모든 개인정보는 적법하고, 공정한 수단에 의해 수집되어야 하며, 정

보주체에게 알리거나 동의를 얻은 후 수집되어야 한다.
(2) 이용 제한의 원칙 : 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안된다.
(3) 정보 정확성의 원칙 : 개인정보는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지하여야 한다.

3. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은?
① DoS 공격
② 취약한 인증 및 세션 공격
③ SQL 삽입 공격
④ CSRF 공격
정답 체크 :
(4) CSRF : 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격
오답 체크 :
(1) DoS : flooding 공격 등을 통해 서버를 무력화시킴
(2) 취약한 인증 및 세션 공격 :
URL에 세션 정보가 노출 되도록 코딩하는 경우
공공장소의 컴퓨터에서 사용되는 어플리케이션에서 세션 타임아웃이 없고, 로그아웃을 하지 않고 단순히 브라우저만 닫아서 세션이 유지되는 경우
쿠키 변조 : 쿠키를 사용하는 웹페이지의 경우 쿠키를 암호화할 때 취약한 암호를 사용하는 경우
(3) SQL 삽입 : 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점

4. 스테가노그래피에 대한 설명으로 옳지 않은 것은?
① 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.
② 원문 데이터에 비해 더 많은 정보의 은닉이 가능하므로 암호화보다 공간효율성이 높다.
③ 텍스트.이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.
④ 고해상도 이미지 내 각 픽셀의 최하위 비트들을 변형하여 원본의 큰 손상 없이 정보를 은닉하는 방법이 있다.
정답 체크 :
(2) 스테가노그래피는 원본과 부가정보가 들어가야 하므로 공간효율성이 좋지 않다. 암호화는 원본을 암호문으로 바꾼 것이므로 공간효율성이 좋다.
오답 체크 :
(1) 메시지의 내용을 읽지 못하게 하는 것이 아니라, 메시지의 존재 자체를 숨기는 기법이다. 메시지를 숨겨 넣는 방법을 알게 되면 메시지의 내용은 금방 노출된다.
(3) 전체 데이터에 일부분의 정보를 숨긴다. (디지털 데이터 - 2진 데이터)

(4) 고해상도 이미지의 경우 픽셀당 32비트를 사용하므로 최하위 비트들을 변형해도 원본에 큰 손상이 발생하지 않는다.

5. 다음 중 OSI 7계층 모델에서 동작하는 계층이 다른 것은?
① L2TP
② SYN 플러딩
③ PPTP
④ ARP 스푸핑
정답 체크 :
(2) 4계층 : SYN 플러딩 → 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다. (syn cookie를 이용해서 막을 수 있다.)
오답 체크 :
(1), (3) 2계층 : L2TP(PPTP+L2F), PPTP(1:1 연결) → VPN에서 사용하는 터널링 프로토콜, L2F(1:N 연결)도 존재한다.
(4) 2계층 : ARP 스푸핑 → 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다. (3계층과 경계가 애매하나 가장 틀린 답은 아님)

6. 해시 함수의 충돌에 대한 설명으로 옳은 것은?
① 해시 함수의 입력 메시지가 길어짐에 따라 생성되는 해시 값이 길어지는 것을 의미한다.
② 서로 다른 해시 함수가 서로 다른 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
③ 동일한 해시 함수가 서로 다른 두 개의 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
④ 동일한 해시 함수가 동일한 입력 값에 대해 다른 출력 값을 내는 것을 의미한다.
정답 체크 :
(3)
약한 충돌 내성 : 어느 메시지의 해시 값이 주어졌을 때, 그 해시 값과 같은 해시 값을 갖는 다른 메시지를 발견해 내는 것이 매우 곤란한 성질
강한 충돌 내성 : 해시 값이 일치할 것 같은, 다른 2개의 메시지를 발견해 내는 것이 매우 곤란한 성질
오답 체크 :
(1) 입력 메시지의 길이에 무관하게 해시 값을 일정하고 이는 충돌과 무관하다.
(2) 서로 다른 해시 함수가 아니라 동일한 해시 함수가 서로 다른 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
(4) 동일한 해시 함수는 동일한 입력 값에 동일한 출력 값을 내야 한다. 만약, 다른 출력 값을 가지면 이는 해시 함수로 사용할 수 없다.

7. 암호화 기법들에 대한 설명으로 옳지 않은 것은?

① Feistel 암호는 전치(Permutation)와 대치(Substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.

② Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.

③ AES는 암호키의 길이를 64비트, 128비트, 256비트 중에서 선택한다.

④ 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과 밖에 얻지 못한다.

정답 체크 :

(3) AES : 키의 비트 길이 → 128, 192, 256비트

오답 체크 :

(1) Feistel : 전치와 환자(대치)를 반복한다.

전치(Transposition) : 평문 문자의 순서를 특정 방식으로 섞어서 재배치 (Permutation과 비슷한 용어이다)

환자(Substitution) : 평문 문자를 특정한 다른 문자로 대치한다.

(2) Kerckhoff : 키 이외에 암호 시스템의 모든 것이 공개되어도 안전해야 한다

(4) Double DES : P -> E_{k1}(P) -> M -> E_{k2}(M) -> C

중간 일치 공격은 다음과 같이 P에 2^{56}개의 키를 전사 공격(암호화)해보고, C에 2^{56}개의 키를 전사 공격(복호화)해봐서 같은 것(M)을 찾는 공격이다.

$E_{k1}(P) = M = D_{k2}(C)$

해당 공격을 수행하면 원래 기대했던 2^{112}의 비용이 들지 않고(112=56+56), 2^{57}의 비용이 든다(57=56+1).

8. 디지털 포렌 식에 대한 설명에서 ㉠ , ㉡ 에 들어 갈 용어는?

(㉠) 공간은 물리적으로 파일에 할 당 된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또 한, 이전에 저장되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파 편 조사에 활용할 수 있다. 이 때, 디지털 포렌 식의 파일 (㉡) 과정을 통해 디스크 내 비구조화된 데이터 스트림을 식 별하고 의미 있는 내용을 추출할 수 있다.

㉠	㉡
① 실린더(Cylinder)	역어셈블링(Disassembling)
② MBR(Master Boot Record)	리버싱(Reversing)
③ 클러스터(Cluster)	역컴파일(Decompiling)
④ 슬랙(Slack)	카빙(Carving)

정답 체크 :

(4)

슬랙(느슨한, 늘어진) : 파일의 크기(물리 구조)가 데이터 단위 크기의 배수(논리 구조)가 되지 않아, 저장매체에서 파일이 저장되고 남은 공간을 말한다. 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간을 말한다. 정보를 은닉할 수 있고, 파일의 복구 및 삭제된 파일의 파편 조사시 유용하게 사용될 수 있으므로 포렌식 분석 시 고려해야 한다.

카빙(조각품, 새긴 무늬) : 데이터 영역에 존재하는 파일 자체 정보(시그니처, 논리구조, 파일

형식, 고유 특성)를 이용하는 방법으로 디스크의 비할당 영역을 처음부터 끝까지 스캔하여 삭제된 파일을 찾아 복원하는 방식이다. (시그니처 - 고유한 포맷 식별)
오답 체크 :
(1) 실린더(HDD), 역어셈블링(실행파일 → 어셈블리어)
(2) MBR(부팅 정보), 리버싱(리버스 엔지니어링, 실행파일 → 소스코드)
(3) 클러스터(저가의 PC들을 하나의 PC로 만듦)
(3) 역컴파일(실행파일 → 소스코드)

9. 버퍼 오버플로우 공격 대응 방법 중 ASLR(Address Space Layout Randomization)에 대한 설명으로 옳은 것은?
① 함수의 복귀 주소 위조 시, 공격자가 원하는 메모리 공간의 주소를 지정하기 어렵게 한다.
② 함수의 복귀 주소와 버퍼 사이에 랜덤(Random) 값을 저장하여 해당 주소의 변조 여부를 탐지한다.
③ 스택에 있는 함수 복귀 주소를 실행 가능한 임의의 libc 영역 내 주소로 지정하여 공격자가 원하는 함수의 실행을 방해한다.
④ 함수 호출 시 복귀 주소를 특수 스택에 저장하고 종료 시 해당 스택에 저장된 값과 비교하여 공격을 탐지한다.
정답 체크 :
(1) : ASLR - 메모리 공격을 방어하기 위해 주소 공간배치를 난수화하는 기법이다.
오답 체크 :
(2) : Stack Guard에 대한 설명으로 Canary(밀고자)로 Random, Null, Terminator를 사용한다.
(3) : RTL에 대한 설명으로 해당 방법은 버퍼 오버플로우에 대한 방어가 아니라 NX-bit 방어(스택에서 실행을 금지함)에 대한 우회 공격 기법이다.
(4) : Stack Shield에 대한 설명으로 Global RET Stack이라는 특수 스택에 복귀 주소를 저장한다.

10. 국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도는?
① PIPL - P
② ISMS - I
③ PIMS - I
④ ISMS - P
정답 체크 :
(4) ISMS → PIMS(PIPL과 PIMS 통합) → ISMS-P(ISMS와 PIMS 통합)

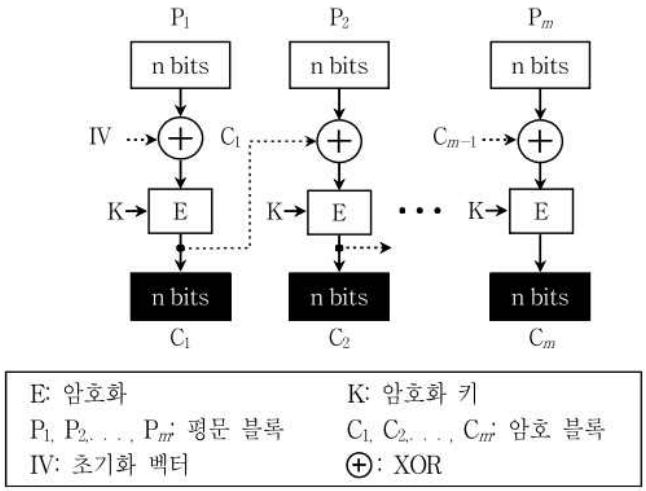
오답 체크 :

(1) PIPL : 공공기관이나 민간기업이 개인정보 유출사고 등을 예방하기 위해 추진 중인 개인정보보호 활동들이 체계적이고 지속적으로 이행될 수 있도록 촉진하는 지원체계로서, 개인정보보호 활동에 대해 객관적이고 공신력 있는 검증을 통해 개선 및 보완이 이루어질 수 있도록 자율적인 환경을 조성하는데 그 목적을 두고 있다.

(2) ISMS : 정보통신망의 안전성 및 정보의 신뢰성을 확보하고, 조직의 정보보호 수준 제고를 위하여 관리적·기술적·물리적 보호조치를 종합한 것으로, 조직의 관리체계를 효과적으로 수립하도록 2001년 모델을 개발하여 국내 표준으로 제정되었으며 관리체계의 기본 틀이자 공통 프레임워크로 활용되고 있다.

(3) PIMS : 국민들에게는 개인정보를 안전하게 관리하는 조직에게 객관적으로 식별할 수 있는 기준을 제시하여 조직 스스로 개인정보 유·노출 및 개인정보의 수집·보관·이용 등 취급 절차상에서 발생할 수 있는 침해 요인을 파악하고 이를 미연에 방지하도록 하는 체계적이고 종합적인 관리체계이다.

11. 다음의 블록 암호 운용 모드는?



① 전자 코드북 모드(Electronic Code Book Mode)

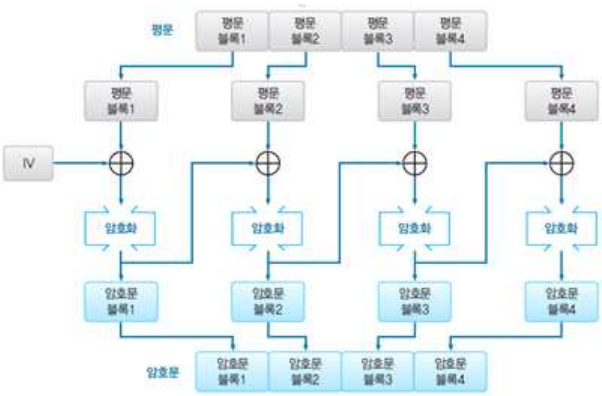
② 암호 블록 연결 모드(Cipher Block Chaining Mode)

③ 암호 피드백 모드(Cipher Feedback Mode)

④ 출력 피드백 모드(Output Feedback Mode)

정답 체크 :

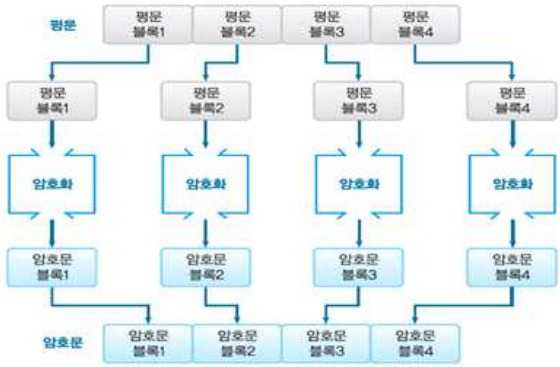
(2)



(a) CBC 모드에 의한 암호화

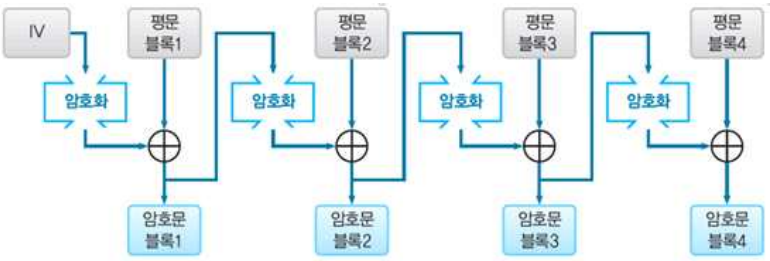
오답 체크 :

(1)



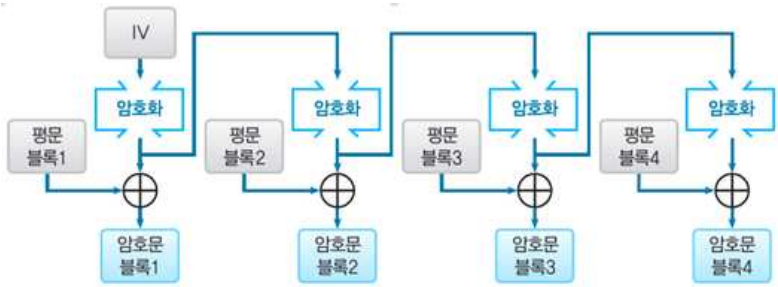
(a) ECB 모드에 의한 암호화

(3)



(a) CFB 모드에 의한 암호화

(4)



(a) OFB 모드에 의한 암호화

12. 무결성을 위협하는 공격이 아닌 것은?
① 스누핑 공격(Snooping Attack)
② 메시지 변조 공격(Message Modification Attack)
③ 위장 공격(Masquerading Attack)
④ 재전송 공격(Replay Attack)
정답 체크 :
(1) 스누핑 : 기밀성

Attacks	*Passive/Active*	*Threatening*
Snooping (Sniffing) Traffic analysis	Passive	Confidentiality
Modification Masquerading (Spoofing) Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

오답 체크 :
(2) 메시지 변조 : 무결성
(3) 위장 : 무결성
(4) 재전송 : 무결성

13. 다음에서 설명하는 접근 제어 모델은?
군사용 보안구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델로 알려져 있다. 불법적 파괴나 변조보다는 정보의 기밀성 유지에 초점을 두고 있다. '상위 레벨 읽기 금지 정책(No-Read-Up Policy)'을 통해 인가받은 비밀 등급이 낮은 주체는 높은 보안 등급의 정보를 열람 할 수 없다. 또한, 인가 받은 비밀 등급 이하의 정보 수정을 금지하는 '하위 레벨 쓰기 금지 정책(No-Write-Down Policy)'을 통해 비밀 정보의 유출을 차단 한다.
① DAC(Discretionary Access Control) 모델
② Bell-LaPadula 모델
③ Biba 모델
④ RBAC(Role-Based Access Control) 모델
정답 체크 :
(2) BLP : 기밀성을 보장하는 최초의 수학적 모델(No Read Up, No Write Down)
오답 체크 :
(1) DAC : 자신의 권한을 다른 사람에게 이양, 유닉스
(3) Biba : 무결성을 보장하는 최초의 모델, BLP(Bell-LaPadula) 속성과 반대이다(No Write Up, No Read Down)
(4) RBAC : 사람이 아닌 역할에 권한 할당

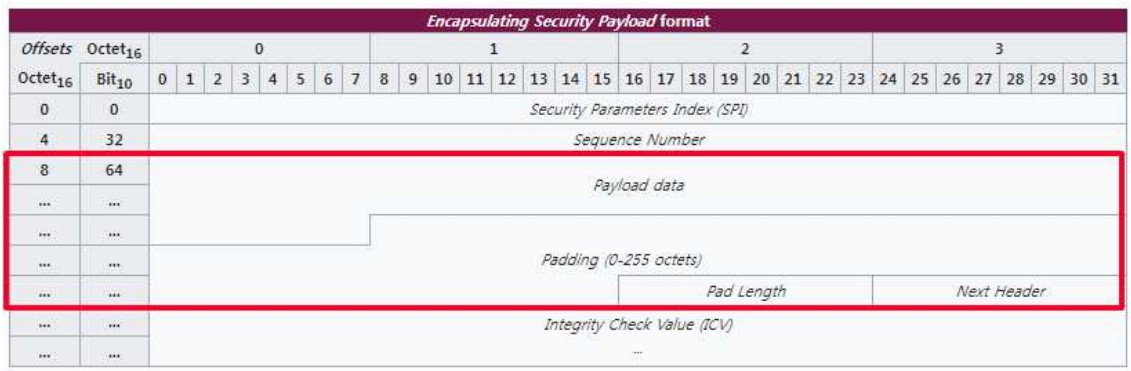
14. 유럽의 일반개인정보보호법(GDPR)에 대한 설명으로 옳은 것은?

① EU 회원국들 간 개인정보의 자유로운 이동을 금지하기 위한 목적을 갖는다.
② 그 자체로는 EU의 모든 회원국에게 직접적인 법적 구속력을 갖지 않는다.
③ 중요한 사항 위반 시 직전 회계 연도의 전 세계 매출액 4% 또는 2 천만 유로 중 높은 금액이 최대한도 부과 금액이다.
④ 만 19세 미만 미성년자의 개인정보 수집 시 친권자의 동의를 얻어야 한다.
정답 체크 :
(3)

일반적 위반 사항 (대리인 미지정 위반 등)	중요한 위반 사항 (국외 이전 규정 위반 등)
전 세계 매출액 2% 또는 1천만 유로(약 125억원) 중 높은 금액	전 세계 매출액 4% 또는 2천만 유로(약 250억원) 중 높은 금액

오답 체크 :
(1) 정보주체의 권리와 기업의 책임성 강화, 개인정보의 EU역외이전 요건 명확화 등을 주요 내용
(2) EU GDPR은 28개 모든 유럽 회원국에 공통적으로 적용되는 법률 : 법적 구속력을 가짐
(4) '만16세 미만의 아동'에게 온라인 서비스 제공 시 '아동의 친권을 보유하는 자'의 동의를 얻어야 함
Tip! : GDPR(https://www.privacy.go.kr/gdpr)를 참고하기 바란다.

15. IPsec의 캡슐화 보안 페이로드(ESP) 헤더에서 암호화되는 필드가 아닌 것은?
① SPI(Security Parameter Index)
② Payload Data
③ Padding
④ Next Header
정답 체크 :
(1) SPI : 암호화 방법 및 키의 비트 길이 등의 정보 이므로 굳이 암호화할 필요가 없다. (커크호프의 원리)



오답 체크 :
(2) Payload : 원본 IP 패킷의 내용이므로 암호화해야 한다.
(3) Padding : Payload를 암호화하기 위해(블록 길이) 들어가는 패딩이므로 암호화한다.
(4) Next Header : 다음 패킷의 유형(IP 프로토콜 번호)이므로 암호화한다.

16. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?
① 서버와 클라이언트 간 양방향 통신에 동일한 암호화 키를 사용한다.
② 웹 서비스 이외에 다른 응용 프로그램에도 적용할 수 있다.
③ 단편화, 압축, MAC 추가, 암호화, SSL 레코드 헤더 추가의 과정으로 이루어진다.
④ 암호화 기능을 사용하면 주고 받는 데이터가 인터넷 상에서 도청되는 위험성을 줄일 수 있다.
정답 체크 :
(1) 서로 다른 키를 사용한다.

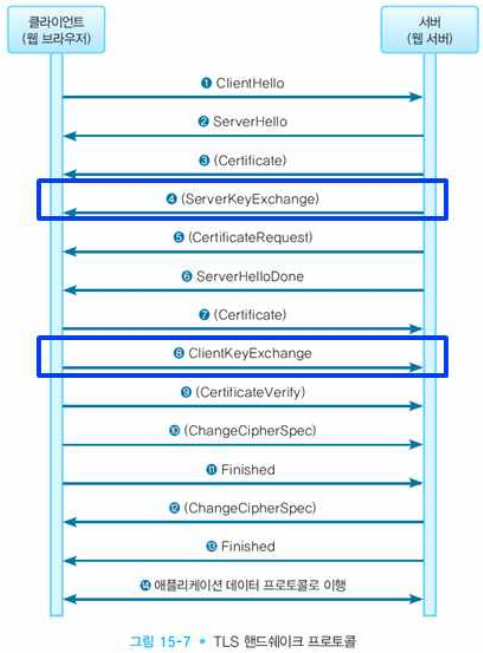


그림 15-7 • TLS 핸드쉐이크 프로토콜

오답 체크 :
(2) SMTP, POP3 등에도 적용할 수 있다.
(3) 단편화, 압축, MAC 추가, 암호화, SSL 레코드 헤더 추가를 수행한다.

그림 15-6 • TLS 레코드 프로토콜의 처리

(4) https(SSL)로 되어 있으면 패스워드를 암호화할 수 있다.

17. KCMVP에 대한 설명으로 옳은 것은?

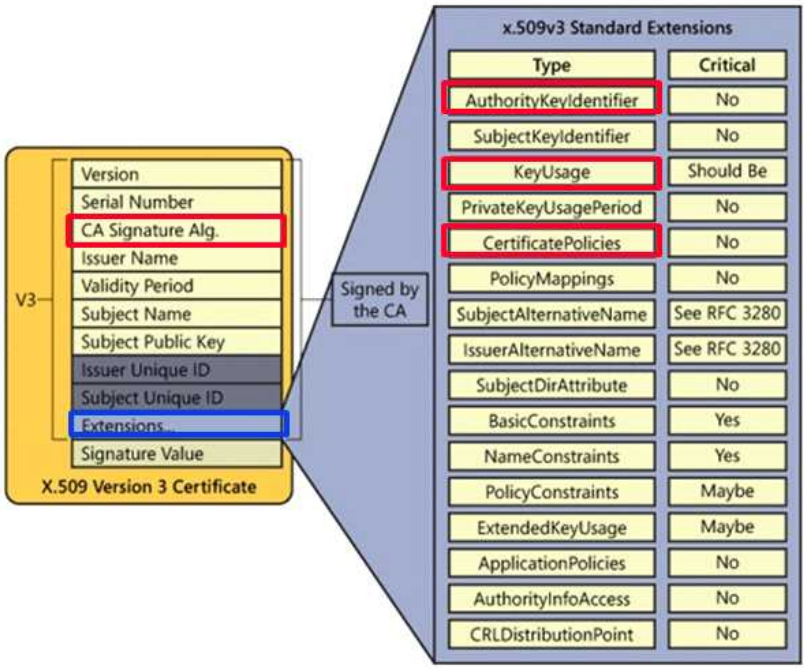
① 보안 기능을 만족하는 신뢰도 인증 기준으로 EAL1부터 EAL7까지의 등급이 있다.
② 암호 알고리즘이 구현된 프로그램 모듈의 안전성과 구현 적합성을 검증하는 제도이다.
③ 개인정보보호활동을 체계적·지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가한다.
④ 조직의 정보자산을 효과적으로 보호하고 있는지 평가하여 일정 수준 이상의 기업에 인증을 부여한다.
정답 체크 :
(2) : KCMVP - 국산 알고리즘을 탑재한 암호모듈에 대한 구현의 적합성, 안전성 등을 검증하는 제도(vs. CMVP는 비슷한 일을 하는 국제 제도이다.)
오답 체크 :
(1) : CC - IT 제품이나 특정 사이트의 정보 시스템에 대해 정보 보안평가 인증을 위한 평가기준
(3) : PIMS에 대한 설명이다.
(4) : ISMS에 대한 설명이다.

18. 개인정보 보호법 상 개인정보 분쟁조정위원회에 대한 설명으로 옳지 않은 것은?
① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다.
② 위원장은 행정안전부·방송통신위원회·금융위원회 및 개인정보보호위원회의 고위공무원 단에 속하는 일반직공무원 중에서 위촉한다.
③ 분쟁 조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
④ 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니 한다.
정답 체크 :
(2) “개인정보 보호법” 제40조(설치 및 구성) 상 ④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다. : 권한 분리(Separation of Duty)의 원칙에 의해 해당 권한을 공무원이 아닌 사람에게 위촉한다.
오답 체크 :
(1) “개인정보 보호법” 제40조(설치 및 구성) 상 ② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다. : 숫자에 민감해야 한다.
(3) “개인정보 보호법” 제40조(설치 및 구성) 상 ⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다. : 다른 법령에서도 통용되는 일반적인 내용이다.
(4) “개인정보 보호법” 제41조(위원의 신분보장) 상 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다. : 다른 법령에서도 통용되는 일반적인 내용이다.

19. 전자화폐 및 가상화폐에 대한 설명으로 옳지 않은 것은?
① 전자화폐는 전자적 매체에 화폐의 가치를 저장한 후 물품 및 서비스 구매시 활용하는 결제수단이며, 가상화폐는 전자화폐의 일종으로 볼 수 있다.

② 전자화폐는 발행, 사용, 교환 등의 절차에 관하여 법률에서 규정하고 있으나, 가상화폐는 별도로 규정하고 있지 않다.
③ 가상화폐인 비트 코인은 분산 원장 기술로 알려진 블록체인을 이용한다.
④ 가상화폐인 비트 코인은 전자화폐와 마찬가지로 이중 지불(Double Spending)문제가 발생하지 않는다.
정답 체크 :
(4) 이중 지불(Double Spending)
100만원의 잔고에서 100만원을 꺼내 썼을 때 잔고가 0원으로 갱신되기 전에 100만원을 또 쓰는 시간차 공격이다.
예 : 인터넷 창을 두 개 띄워놓고 동시에 버튼을 누르면 두 개의 지불 요청이 동시에 날아간다.
전자화폐 : 금융 기관이 관여하므로 이중 지불 문제가 발생하지 않는다.
가상화폐 : 분산 구조로 인해 이중 지불 문제 발생한다. -> 이를 해결하기 위해 비트코인에서는 PoW(Proof of Work)를 수행한다.
오답 체크 :
(1) 전자화폐(IC 카드 혹은 네트워크), 가상화폐(전자화폐의 일종, 비트코인)
(2) 전자화폐(금융결제원), 가상화폐(분산원장, 아직 정해진바 없음)
(3) 가상화폐 : 분산원장기술(2019 국가직 시험 문제 참조), 블록체인
Tip! : 잘 알겠지만 공무원 시험의 특성상 가장 최근 시험의 문제를 참조해서 내는 경향이 존재한다(아니면 비슷한 문제들을 출제하고 분리해서 내는지?). 그러므로 만약, 지방직을 보려고 한다면 해당 년도에 선행한 국가직은 무조건 모든 선지를 숙지하고 시험장에 가야한다.

20. X.509 인증서(버전 3)의 확장(Extensions) 영역에 포함되지 않는 항목은?
① 인증서 정책(Certificate Policies)
② 기관키 식별자(Authority Key Identifier)
③ 키 용도(Key Usage)
④ 서명 알고리즘 식별자(Signature Algorithm Identifier)
정답 체크 :
(4) 서명 알고리즘 식별자 : CA Signature Alg.



오답 체크 :

(1) 인증서 정책 : CertificatePolicies

(2) 기관 키 식별자 : AuthorityKeyIdentifier

(3) 키 용도 : KeyUsage

Tip! : 해당 문제를 모르는 상태에서 문제를 풀 수 있는 방법은 한 가지 방법밖에 존재하지 않는다. 즉, 중요 정보와 중요 정보가 아닌 것을 구분하는 것이다. 아무래도 중요하지 않은 정보는 확장 영역에 포함될 것이다. 지문에서 서명 알고리즘 식별자는 아주 중요한 정보이다. 왜냐하면 서명 알고리즘 식별자는 서명할 때 사용한 알고리즘에 대한 정보이므로 이것을 모른다면 서명을 검증할 수 없기 때문이다.