2020-국가직-정보보호론-가형-해설-곽후근

1. 정보보호 위험관리에 대한 설명으로 옳지 않은 것은?
① 자산은 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설 등이 해당한다.
② 위험은 자산에 손실이 발생할 가능성과 관련되어 있으나 이로 인한 부정적인 영향을 미칠 가능성과는 무관하다.
③ 취약점은 자산이 잠재적으로 가진 약점을 의미한다.
④ 정보보호대책은 위협에 대응하여 자산을 보호하기 위한 관리적, 기술적, 물리적 대책을 의미한다.
정답 체크 :
(2) 위험 : 자산의 취약한 부분에 위협요소가 발생하여 자산에 발생한 손실 또는 손상을 유발할 잠재성(가능성)이다.
오답 체크 :
(1) 자산 : 유형과 무형을 모두 포함한다. 예를 들어, 소프트웨어(software), 하드웨어(hardware), 데이터(data), 인적 요소(personnel), 절차(procedure, 무형임에 유의), 네트워크(network) 등이다.
(3) 취약점 : 위협에 의해 보안에 부정적 영향을 줄 수 있는 정보자산의 속성이나 상태이다.
(4) 정보보호대책 : 위험에 대응하여 자산을 보호하기 위한 관리적, 기술적, 물리적 대책이다.

2. 공개키 암호화에 대한 설명으로 옳지 않은 것은?
① ECC(Elliptic Curve Cryptography)와 Rabin은 공개키 암호 방식이다.
② RSA는 소인수 분해의 어려움에 기초를 둔 알고리즘이다.
③ 전자서명 할 때는 서명하는 사용자의 공개키로 암호화한다.
④ ElGamal은 이산대수 문제의 어려움에 기초를 둔 알고리즘이다.
정답 체크 :
(3) 전자서명 할 때는 서명하는 사용자의 개인키로 암호화한다.
오답 체크 :
(1) 공개키 암호는 RSA, ElGamal, Rabin, ECC 등이 존재한다.
(2) RSA와 Rabin은 소인수 분해의 어려움에 기초한다.
(4) ElGamal과 ECC는 이산대수 문제의 어려움에 기초한다.

3. X.509 인증서 형식 필드에 대한 설명으로 옳은 것은?
① Issuer name – 인증서를 사용하는 주체의 이름과 유효기간 정보
② Subject name – 인증서를 발급한 인증기관의 식별 정보
③ Signature algorithm ID – 인증서 형식의 버전 정보
④ Serial number – 인증서 발급 시 부여된 고유번호 정보
정답 체크 :
(4) Serial number : CA가 할당한 정수로 된 고유 번호
오답 체크 :
(1) Issuer name : 발행자
(2) Subject name : 소유자
(3) Signature algorithm ID : 서명 알고리즘 식별자

4. 일방향 해시함수를 사용하여 비밀번호를 암호화할 때 salt라는 난수를 추가하는 이유는?

① 비밀번호 사전공격(Dictionary attack)에 취약한 문제를 해결할 수 있다.
② 암호화된 비밀번호 해시 값의 길이를 줄일 수 있다.
③ 비밀번호 암호화의 수행 시간을 줄일 수 있다.
④ 비밀번호의 복호화를 빠르게 수행할 수 있다.
정답 체크 :
(1) 비밀번호를 암호화할 때 salt를 추가하면 공격이 수행되는 키 공간(key space)가 증가하게 되어 사전공격을 해결할 수 있다.

5. 윈도우 운영체제에서 TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은?
① TPM의 공개키를 사용하여 플랫폼 설정정보에 서명함으로써 디지털 인증을 생성한다.
② TPM은 신뢰 컴퓨팅 그룹(Trusted Computing Group)에서 표준화된 개념이다.
③ TPM은 키 생성, 난수 발생, 암복호화 기능 등을 포함한 하드웨어 칩 형태로 구현할 수 있다.
④ TPM의 기본 서비스에는 인증된 부트(authenticated boot), 인증, 암호화가 있다.
정답 체크 :
(1) AIK(인증을 위한 키)를 이용하여 PCR(플랫폼 설정정보)에 서명한다.
오답 체크 :
(2) 국제산업표준단체인 TCG(Trusted Computing Group)는 암호화 키 관리와 암호화 처리 등을 하드웨어로 제조된 보안 칩 내부에서만 동작하도록 함으로써 강력한 수준의 보안 환경을 제공하는 보안 칩의 표준 규격을 제공하였다.
(3) 하드웨어 기반의 난수(random number) 생성, 표준 알고리듬(SHA-1, RSA, HMAC 등) 제공, 안전한 키 생성 및 보관, 암호 처리를 위한 프로세서 및 정보 저장을 위한 플랫폼 구성 레지스터(PCR: Platform Configuration Register) 및 비휘발성 메모리 등으로 구성되어 있다.
(4) 일반적으로 개인용 컴퓨터(PC) 주기판에 부착되며, 부팅 단계에서부터 시스템의 무결성 검증에 이용된다.

6. 키 k에 대한 블록 암호 알고리즘 E_k, 평문블록 M_i, Z_0는 초기벡터, $Z_i = E_k(Z_{i-1})$가 주어진 경우, 이때 i= 1, 2, ..., n에 대해 암호블록 C_i를 $C_i = Z \oplus M_i$로 계산하는 운영모드는? (단, $\oplus$는 배타적 논리합이다)
① CBC
② ECB
③ OFB
④ CTR
정답 체크 :
(3) OFB를 나타낸다.
오답 체크 :
(1) CBC : $C_i = E_k(C_{i-1} \oplus M_i)$
(2) ECB : $C_i = E_k(M_i)$
(4) CTR : $C_i = E_k(CTR) \oplus M_i$

7. 정보보호 시스템 평가 기준에 대한 설명으로 옳은 것은?
① ITSEC의 레인보우 시리즈에는 레드 북으로 불리는 TNI(Trusted Network Interpretation)가 있다.
② ITSEC은 None부터 B2까지의 평가 등급으로 나눈다.
③ TCSEC의 EAL2 등급은 기능시험 결과를 의미한다.
④ TCSEC의 같은 등급에서는 뒤에 붙는 숫자가 클수록 보안 수준이 높다.

정답 체크 :

(4) TCSEC의 등급은 다음과 같다 : D 〈 C1 〈 C2 〈 B1 〈 B2 〈 B3 〈 A1

오답 체크 :

(1) TCSEC의 레인보우 시리즈에는 레드 북으로 불리는 TNI가 있다.

(2) ITSEC는 E0부터 E6까지의 평가 등급으로 나눈다.

(3) CC의 EAL2 등급은 구조 시험 결과를 의미한다.

8. SSL(Secure Socket Layer)의 Handshake 프로토콜에서 클라이언트와 서버 간에 논리적 연결 수립을 위해 클라이언트가 최초로 전송하는 ClientHello 메시지에 포함되는 정보가 아닌 것은?

① 세션 ID

② 클라이언트 난수

③ 압축 방법 목록

④ 인증서 목록

정답 체크 :

(4) 인증서 목록은 ServerHello 다음에 서버가 클라이언트에게 보내는 Certificate에 전송되는 정보이다.

오답 체크 :

(1), (2), (3) ClientHello에 전송되는 정보는 버전 번호, 현재 시각, 클라이언트 랜덤(난수), 세션 ID, 사용할 수 있는 암호 스위트 목록, 사용할 수 있는 압축 방법 목록이다.

9. 「개인정보 보호법」상 기본계획에 대한 조항의 일부이다. ㉠, ㉡에 들어갈 내용을 바르게 연결한 것은?

> 제9조(기본계획) ①보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 (㉠)년마다 개인정보 보호 기본계획(이하 “기본계획”이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.
> ②기본계획에는 다음 각 호의 사항이 포함되어야 한다.
> 1. 개인정보 보호의 기본목표와 추진방향
> 2. 개인정보 보호와 관련된 제도 및 법령의 개선
> 3. 개인정보 침해 방지를 위한 대책
> 4. (㉡)
> 5. 개인정보 보호 교육·홍보의 활성화
> 6. 개인정보 보호를 위한 전문인력의 양성
> 7. 그 밖에 개인정보 보호를 위하여 필요한 사항

	㉠	㉡
①	1	개인정보 보호 자율규제의 활성화
②	3	개인정보 보호 자율규제의 활성화
③	1	개인정보 활용·폐지를 위한 계획
④	3	개인정보 활용·폐지를 위한 계획

정답 체크 :

(2) 제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.

② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 개인정보 보호의 기본목표와 추진방향

2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

10. 소수 p = 13, 원시근 g = 2, 사용자 A와 B의 개인키가 각각 3, 2일 때, Diffie-Hellman 키 교환 알고리즘을 사용하여 계산한 공유 비밀키는?
① 6
② 8
③ 12
④ 16
정답 체크 :
(3) $g^{3x2} \bmod p = 2^6 \bmod 13 = 64 \bmod 13 = 12$

11. NIST의 AES(Advanced Encryption Standard) 표준에 따른 암호화 시 암호키(cipher key) 길이가 256비트일 때 필요한 라운드 수는?
① 8
② 10
③ 12
④ 14
정답 체크 :
(4) 256비트일 때 필요한 라운드 수는 14이다.
오답 체크 :
(1) AES에 해당되지 않는다.
(2) 128비트일 때 필요한 라운드 수는 10이다.
(3) 192비트일 때 필요한 라운드 수는 12이다.

12. IPsec의 ESP(Encapsulating Security Payload)에 대한 설명으로 옳지 않은 것은?
① 인증 기능을 포함한다.
② ESP는 암호화를 통해 기밀성을 제공한다.
③ 전송 모드의 ESP는 IP 헤더를 보호하지 않으며, 전송계층으로부터 전달된 정보만을 보호한다.
④ 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 공개키를 사용한다.
정답 체크 :
(4) 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 대칭키를 사용한다.
오답 체크 :
(1), (2) ESP는 인증, 무결성, 기밀성(암호화), 재전송공격 방지를 제공한다.
(3) 전송 모드는 기존 패킷만을 보호하므로 전송계층으로부터 전달된 정보만을 보호한다.

13. 네트워크나 컴퓨터 시스템의 자원 고갈을 통해 시스템 성능을 저하시키는 공격에 해당하는 것만을 모두 고르면?

ㄱ. Ping of Death 공격 ㄴ. Smurf 공격 ㄷ. Heartbleed 공격 ㄹ. Sniffing 공격

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 체크 :
(1) ping of death는 대량의 ping을 보내므로 자원을 고갈하고 Smurf도 대량의 ICMP request/reply를 보내므로 자원을 고갈한다.

오답 체크 :
(2), (3), (4) Heartbleed는 오픈소스 암호화 라이브러리인 OpenSSL에서 발견된 심각한 보안 결함이고, Sniffing은 도청을 의미한다.

14. 다음 설명에 해당하는 위험분석 및 평가 방법을 옳게 짝 지은 것은?

ㄱ. 전문가 집단의 토론을 통해 정보시스템의 취약성과 위협 요소를 추정하여 평가하기 때문에 시간과 비용을 절약할 수 있지만, 정확도가 낮다. ㄴ. 이미 발생한 사건이 앞으로 발생한다는 가정하에 수집된 자료를 통해 위험 발생 가능성을 예측하며, 자료가 많을수록 분석의 정확도가 높아진다. ㄷ. 어떤 사건도 기대하는 대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대해 발생 가능한 결과들을 예측하며, 적은 정보를 가지고 전반적인 가능성을 추론할 수 있다.

	ㄱ	ㄴ	ㄷ
①	순위 결정법	과거자료 분석법	기준선 접근법
②	순위 결정법	점수법	기준선 접근법
③	델파이법	과거자료 분석법	시나리오법
④	델파이법	점수법	시나리오법

정답 체크 :
(3) 델파이법 : 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고, 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.
과거자료 분석법 : 미래 사건의 발생 가능성을 예측하는 방법으로, 과거의 자료를 통해 위험 발생 가능성을 예측한다.
시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여, 일정 조건 하에서 위협에 대한 발생 가능한 결과들을 추정(시나리오)하는 방법이다.

오답 체크 :
(1), (2), (4) 순위 결정법 : 비교 우위 순위 결정표에 위험 항목들의 서술적 순위를 결정하는 방법이다.
기준선 접근법 : 모든 시스템에 대하여 보호의 기본 수준(기준선)을 정하고, 이를 달성하기 위하여 보호대책을 선택한다.

점수법 : 위험 발생 요인에 가중치(점수화)를 두어 위험을 추정하는 방법이다.

15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제19조(국내대리인 지정 대상자의 범위)에 명시된 자가 아닌 것은?

① 전년도(법인인 경우에는 전(前) 사업연도를 말한다) 매출액이 1,000억 원 이상인 자

② 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억 원 이상인 자

③ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상인 자

④ 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송통신위원회로부터 관계 물품·서류 등을 제출하도록 요구받은 자

정답 체크 :

(1) 제19조(국내대리인 지정 대상자의 범위) ① 법 제32조의5제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 전년도[법인인 경우에는 전(前) 사업연도를 말한다] 매출액이 1조원 이상인 자
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
3. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 자
4. 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송통신위원회로부터 관계 물품·서류 등을 제출하도록 요구받은 자

Tip! 제32조의5(국내대리인의 지정)

① 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 다음 각 호의 사항을 대리하는 자(이하 "국내대리인"이라 한다)를 서면으로 지정하여야 한다.

Tip! 제47조(정보보호 관리체계의 인증)

②「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1.「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자

2. 집적정보통신시설 사업자

3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

16. 다음 설명에 해당하는 악성코드 분석도구를 옳게 짝 지은 것은?

> ㄱ. 가상화 기술 기반으로 악성코드의 비정상 행위를 유발하는 실험과정에서 발생할 수 있는 분석시스템으로의 침해를 방지하여 통제된 환경과 분석 기능을 제공한다.
>
> ㄴ. 악성코드의 행위를 추출하기 위해 실제로 해당 코드를 실행함으로써 발생하는 비정상 행위 혹은 시스템 동작 환경의 변화를 살펴볼 수 있는 동적 분석 기능을 제공한다.

	ㄱ	ㄴ
①	Sandbox	Process Explorer
②	Sandbox	Burp Suite

③ Blackbox IDA Pro
④ Blackbox OllyDBG
정답 체크 :
(1) Sandbox : 외부로부터 받은 파일을 바로 실행하지 않고 보호된 영역에서 실행시켜 봄으로써 외부로부터 들어오는 파일과 프로그램이 내부 시스템에 악영향을 주는 것을 미연에 방지하는 기술이다.
Process Explorer : 마이크로소프트 윈도우용 프리웨어 작업 관리자, 시스템 모니터이다.
오답 체크 :
(2) Burp Suite : 웹 프록시 서버이다.
(3) Blackbox : 공격에 사용된다면 내부를 모르고 수행되는 공격을 일컫는다.
IDA Pro : 역공학을 위한 바이너리 검사 툴이다.
(4) OllyDBG : 바이너리 코드 분석을 위한 x86 디버거이다.

17. 윈도우 운영체제의 계정 관리에 대한 설명으로 옳은 것은?
① 'net accounts guest /active:no' 명령은 guest 계정을 비활성화한다.
② 'net user' 명령은 시스템 내 사용자 계정정보를 나열한다.
③ 'net usergroup' 명령은 시스템 내 사용자 그룹정보를 표시한다.
④ 컴퓨터/도메인에 모든 접근권한을 가진 관리자 그룹인 'Admin'이 기본적으로 존재한다.
정답 체크 :
(2) net user : 사용자 계정 정보를 출력한다.
오답 체크 :
(1) net user guest /active:no : guest 계정을 비활성화한다.
(3) net localgroup : 사용자 그룹 정보를 출력한다.
(4) Administrator : 도메인 자원이나 로컬 컴퓨터에 대한 모든 권한이 있다.

18. 커버로스(Kerberos) 프로토콜에 대한 설명으로 옳지 않은 것은?
① 양방향 인증방식의 문제점을 보완하여 신뢰하는 제3자 인증 서비스를 제공한다.
② 사용자의 패스워드를 추측하거나 캡처하지 못하도록 일회용 패스워드를 제공한다.
③ 버전 5에서는 이전 버전과 달리 DES가 아닌 다른 암호 알고리즘을 사용할 수 있다.
④ 클라이언트는 사용자의 식별정보를 평문으로 인증 서버(Authentication Server)에 전송한다.
정답 체크 :
(2) 사용자의 패스워드가 도청되지 않도록 사전에 공유하여 저장한다.
오답 체크 :
(1) 커버로스는 two-party(클라이언트-서버 구조)가 아닌 third-party(인증 서버라는 제3자가 관여)이다.
(3) AES 암호 알고리즘을 사용할 수 있다.
(4) 클라이언트가 AS에 전송하는 정보는 평문이다.

19. 임의적 접근 통제(Discretionary Access Control) 모델에 대한 설명으로 옳은 것은?
① 주체가 소유권을 가진 객체의 접근 권한을 다른 사용자에게 부여할 수 있으며, 사용자 신원에 따라 객체의 접근을 제한한다.
② 주체와 객체가 어떻게 상호 작용하는지를 중앙 관리자가 관리하며, 사용자 역할을 기반으로 객체의 접근을 제한한다.

③ 주체와 객체에 각각 부여된 서로 다른 수준의 계층적인 구조의 보안등급을 비교하여 객체의 접근을 제한한다.
④ 주체가 접근할 수 있는 상위와 하위의 경계를 설정하여 해당 범위 내 임의 객체의 접근을 제한한다.
정답 체크 :
(1) 객체에 대한 소유권(ownership)에 기초해서, 소유권을 가진 주체가 객체에 대한 권한의 전부, 혹은 일부를 다른 주체에게 부여(grant)한다.
오답 체크 :
(2) RBAC를 나타낸다(Role).
(3) MAC를 나타낸다.
(4) LBAC를 나타낸다(Lattice).

20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조(정보통신망의 안정성 확보 등)에 정보보호조치에 관한 지침에 포함되어야 할 보호조치로 명시되지 않은 것은?
① 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
② 사전 정보보호대책 마련 및 보안조치 설계·구현 등을 위한 기술적 보호조치
③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
④ 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치
정답 체크 :
(2) 제45조(정보통신망의 안정성 확보 등)
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.
1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호 시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치
Tip! 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.
1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
5. 정보보호 사전 보안성 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행