☑ 만든이 : 지안에듀 조현준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사

☑ 저서

- TopSpot 정보보호론 이론편/문제편
- 알기쉬운 정보보안기사 필기편/실기편(알기사)
- TopSpot 자료구조론 이론편/쪽집게 기출문제

☑ 무료 동영상 안내

- 지안에듀 홈페이지 이용(www.zianedu.com)
  - [빅데이터 3.2] 조현준 정보보호론 연도별 기출문제 풀이강의(전산 전직렬)
- 유튜브 자투리10분 기출20문항정리
  - 유튜브에서 조현준 정보보호론 검색

2019년 사이버(보안)수사 정보보호론

-2019년 8월 10일 시행

1. ○△× 19.사이버

다음에서 설명하는 정보보호의 목표로 가장 적절한 것은?

보기

정당한 방법으로 권한을 받은 사용자가 자원을 필요로 할 때, 아무런 방해 없이 자원에 접근하고 사용할 수 있음을 보장한다.

① 기밀성(confidentiality)
② 무결성(integrity)
③ 가용성(availability)
④ 신뢰성(reliability)

오답피하기 ③ 가용성(Availability)은 시스템이 지체 없이 동작하도록 하고, 합법적 사용자가 서비스 사용을 거절당하지 않도록 하는 것이다.

정답 ③

2. ○△× 19.사이버

다음 대칭키 암호화에서 키 K값으로 가장 적절한 것은?

보기

- 대칭키 암호화: 8비트 정보 P와 K의 배타적 논리합(XOR) 연산의 결과를 C라 함
- P=00101100
- C=10000110

① 11010010
② 10101010
③ 01010101
④ 10011001

XOR(exclusive or) 연산

0 xor 0 = 0 (짝+ 짝 = 짝)
0 xor 1 = 1 (짝+ 홀 = 홀)
1 xor 0 = 1 (홀+ 짝 = 홀)
1 xor 1 = 0 (홀+ 홀 = 짝)

오답피하기 ② 0010 1100 … P 평문
⊕ ( ) … K Key
1000 0110 … C(P⊕K) 암호문

정답 ②

3. ○△× 19.사이버

복호화 수식이 다음과 같을 때 블록 암호 운영모드로 가장 적절한 것은? (단, P_i: i번째 평문, C_i: i번째 암호문, $D_K(C_i)$: 복호화)

보기

$$P_i = D_K(C_i) \oplus C_{i-1}$$

① CBC(Cipher Block Chaining, 암호블록 연쇄) 모드
② CFB(Cipher FeedBack, 암호 피드백) 모드
③ ECB(Electronic CodeBook, 전자코드북) 모드
④ CTR(Counter, 카운터) 모드

■ 각 모드의 암·복호화 수식 표현

구분	암호화	복호화
ECB	$C_i = E_k(P_i)$ $i = 1,2,...N$	$P_i = D_k(C_i)$ $i = 1,2,...N$
CBC	$C_1 = E_k(P_1 \oplus IV)$ $C_i = E_k(P_i \oplus C_{i-1})$ $i = 2,3,....N$	$P_1 = D_k(C_1) \oplus IV$ $P_i = D_k(C_i) \oplus C_{i-1}$ $i = 2,3,....N$
CFB	$C_i = E_k(C_{i-1}) \oplus P_i$	$P_i = E_k(C_{i-1}) \oplus C_i$ (단, $C_0 = IV$)
OFB	$C_i = P_i \oplus O_i$	$P_i = C_i \oplus O_i$ (단, $O_i = E_k(I_i)$, $I_i = O_{i-1}$, $I_0 = IV$)
CTR	$C_i = P_i \oplus E_k(T_i)$ $i = 1,2,....N-1$	$P_i = C_i \oplus E_k(T_i)$ $i = 1,2,....N-1$

오답피하기 ① CBC 모드를 암호화 수식으로 표현하면 $C_i = E_k(P_i \oplus C_{i-1})$, 복호화 수식으로 표현하면 $P_i = D_k(C_i) \oplus C_{i-1}$ 이 된다.

정답 ①

4. ○△× 19.사이버

하이브리드 암호시스템에 대한 설명으로 가장 적절하지 않은 것은?

① 대칭키 암호시스템과 공개키 암호시스템의 장점을 조합하였다.
② 평문 메시지는 대칭키 암호로 암호화한다.
③ 암호화에서 사용하는 세션키는 의사난수 생성기를 이용하여 생성한다.
④ PGP(Pretty Good Privacy), SSL/TLS(Secure Socket Layer/Transport Layer Security), RSA에서 하이브리드 암호 시스템을 사용한다.

◦ 하이브리드 암호 시스템은 대칭키 암호와 공개키 암호의 장점을 살릴 수 있도록 조합한 방법이다. 일반적으로 서로 다른 2개의 방식을 조합하는 것을 하이브리드라고 한다. 하이브리드 암호 시스템에서는 메시지를 일단 고속의 대칭키 암호로 암호화한다. 그러면 메시지가 암호문으로 변환되기 때문에 메시지의 기밀성을 지킬 수 있게 된다. 다음에 대칭키 암호의 키 기밀성을 지키기 위해서 이 부분에 공개키 암호를 사용한다. 즉, 메시지를 암호화할 때 사용한 대칭키 암호키를 공개키 암호로 암호화한다.
◦ SSL/TLS에서는 대칭키 암호, 공개키 암호, 일방향 해시함수, 메시지 인증코드, 의사난수 생성기, 전자서명을 조합해서 안전한 통신을 수행한다. 또한 SSL/TLS는 암호 스위트를 변경해서 보다 강력한 알고리즘을 사용할 수 있다.

오답피하기 ④ PGP와 SSL/TLS는 하이브리드 암호시스템을 사용하나 RSA는 공개키 암호이다.

정답 ④

5. ○△× 19.사이버

메시지 인증 코드와 전자서명에 대한 설명으로 가장 적절하지 않은 것은?

① 메시지 인증 코드와 전자서명 모두 무결성을 확인할 수 있다.
② 메시지 인증 코드는 부인방지(non-repudiation) 기능을 제공한다.
③ 전자서명은 서명자를 인증하는 기능이 있다.
④ 메시지 인증 코드는 메시지와 비밀키를 사용한다.

◦ 메시지 인증코드는 무결성과 인증을 제공하는 암호 기술이다.
◦ 전자서명은 무결성을 확인하고, 인증과 부인방지를 하기 위한 암호 기술이다.

오답피하기 ② 메시지 인증코드는 부인방지 기능을 제공하지 못하는 반면 전자서명은 제공한다.

정답 ②

6. ○△× 19.사이버

공개키 기반 구조(PKI: Public Key Infrastructure)에 대한 설명으로 가장 적절하지 않은 것은?

① 공개키 기반 구조의 구성요소로는 사용자(user), 등록기관(Registration Authority), 인증기관(Certification Authority), 저장소(repository) 등이 있다.
② 공개키 인증서를 발행하여 무결성, 인증, 부인방지를 보장한다.
③ 등록기관은 인증서와 인증서 취소 목록(Certificate Revocation List)을 발행하고, 공개키 등록 시 본인을 인증한다.
④ 저장소는 인증서를 보관해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 구성된 데이터베이스이다.

오답피하기 ③ 인증서와 인증서 취소 목록(Certificate Revocation List)을 발행하고, 공개키 등록 시 본인을 인증하는 것은 인증기관의 역할이다. 그러나 인증기관이 하는 일 가운데는 「공개키의 등록과 본인에 대한 인증」을 등록기관이나 사람(개체)에게 분담시키는 경우도 있다.

정답 ③

7. ○△× 19.사이버

다음 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

보기

(㉠) 공격은 소스 IP주소와 목적지 IP주소가 동일한 다량의 패킷을 특정 공격 대상 시스템으로 전송하면, 응답이 자기 자신에게 되돌아오도록 하여 시스템의 과부하를 유발한다.

(㉡) 공격은 ICMP Echo 메시지를 큰 패킷으로 만들어, 공격대상 시스템에 분할된 많은 양의 패킷을 도달시켜, 패킷 재결합으로 인한 시스템 과부하를 유발한다.

(㉢) 공격은 ICMP 프로토콜과 브로드캐스팅 개념을 사용한 공격으로 공격대상 호스트의 IP 주소를 source 주소로 갖는 ICMP Echo 요청 패킷을 directed 브로드캐스트 함으로써, 많은 양의 ICMP Echo 응답 패킷을 공격대상 호스트에 전송한다. 이는 공격대상 시스템의 자원을 고갈시킨다.

	㉠	㉡	㉢
①	LAND	ICMP Flooding	Ping of Death
②	LAND	Ping of Death	ICMP Flooding
③	Ping of Death	ICMP Flooding	LAND
④	Ping of Death	LAND	ICMP Flooding

오답피하기 ② Land Attack, Ping of Death, ICMP Flooding 공격에 대한 설명이다. ICMP Flooding 공격은 스머프 공격(Smurf attack)이라고도 부르는데 이 공격은 공공 인터넷 상에서 Flood DoS 공격의 한 변종이다.

정답 ②

8. ○△× 19.사이버

다음 TCP/IP 프로토콜의 계층별 역할에 대한 설명 중 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

보기

(㉠) 계층에서는 송수신지 사이의 패킷을 전달한다. 이를 위해 IP 주소 지정, 패킷화, 단편화가 제공된다.

(㉡) 계층에서는 근거리 통신망(LAN)에서 전송 매체에 데이터(프레임)를 송수신하는 역할을 담당한다.

(㉢) 계층에서는 종단간 통신 서비스 제공을 담당한다. TCP와 UDP가 대표적인 프로토콜이다.

	㉠	㉡	㉢
①	네트워크	데이터링크	전송
②	네트워크	전송	데이터링크
③	전송	데이터링크	네트워크
④	전송	네트워크	데이터링크

OSI 7계층의 기능 설명

OSI 7계층	기능
애플리케이션	네트워크 이용자의 상위 영역으로 화면배치, 파일전송, 전자우편, 디렉터리 서비스 등 하나의 유용한 작업을 할 수 있도록 지원하는 계층
프레젠테이션	데이터를 표준 포맷으로 교환하고, 정확한 데이터를 전송하며 데이터의 압축과 복원, 암호화와 복호화를 수행하는 계층
세션	두 응용프로그램(Application) 간의 연결설정, 이용 및 연결해제 등 대화를 유지하기 위한 구조를 제공하는 계층
트랜스포트	호스트 간의 신뢰성 있는 서비스를 제공하기 위해 논리적 연결을 수행하는 계층
네트워크	두 단말 시스템 간의 논리적 어드레싱과 경로 선택 및 라우팅 제공
데이터링크	MAC 주소를 이용하여 호스트에서 다른 호스트로 또는 라우터 간에 패킷을 전송하며 메시지를 데이터 프레임 형식으로 만드는 계층
물리	단말 시스템 간의 물리적 링크를 가동, 유지, 전달하는 등 전기적, 기계적, 기능적 절차를 정의하는 계층

오답피하기 ① 각각 네트워크 계층, 데이터링크 계층, 전송 계층의 역할 또는 기능에 대한 설명이다.

정답 ①

9. ○△× 19.사이버

다음 사이버 공격 유형에 대한 설명 중 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결한 것은?

보기

(㉠)은 공격자가 도메인을 탈취하여 사용자가 정확한 URL 주소를 입력해도 가짜 사이트로 연결되도록 하는 방법이다.

(㉡)은 이메일 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 신용정보 등의 기밀을 부정하게 얻으려는 사회공학기법을 사용한다.

(㉢)은 문자메시지를 신뢰할 수 있는 사람이 보낸 것처럼 가장하여, 링크 접속을 유도한 뒤 개인정보를 빼내는 방법이다.

	㉠	㉡	㉢
①	스미싱(Smishing)	피싱(Phishing)	파밍(Pharming)
②	스미싱(Smishing)	파밍(Pharming)	피싱(Phishing)

③ 파밍(Pharming) 피싱(Phishing) 스미싱(Smishing)
④ 파밍(Pharming) 스미싱(Smishing) 피싱(Phishing)

오답피하기 ③ 피싱이 금융 기관 등의 웹 사이트에서 보낸 이메일로 위장하여 링크를 유도해 개인의 인증 번호나 신용카드 번호, 계좌 정보 등을 빼내는 반면, 파밍은 아예 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취한다. Smishing은 SMS와 Phishing의 결합어로 휴대폰 문자메시지를 이용하여 피싱하는 기법이다.

정답 ③

10. ○△× 19.사이버

소인수분해의 어려움을 기반으로 한 RSA 암호 알고리즘에서 개인키 d는 7, 합성수 n은 33, 평문 값이 5일 때, 이를 암호화한 암호문의 값으로 가장 적절한 것은?

① 12 ② 13
③ 21 ④ 26

RSA 키 생성 알고리즘

- p와 q라고 하는 두 개의 서로 다른 $(p \neq q)$ 소수를 고른다.
- 두 수를 곱하여 $N = pq$를 찾는다.
- $\phi(N) = (p-1)(q-1)$를 구한다.
- $\phi(N)$보단 작고, $\phi(N)$과 서로소인 정수 e를 찾는다.
- 확장된 유클리드 호제법을 이용하여 $d \times e$를 $\phi(N)$로 나누었을 때 나머지가 1인 정수 d를 구한다. $(de \equiv 1 \pmod{\phi(N)})$

오답피하기 ④ 알고리즘에 적용하여 구하면 다음과 같다.

n이 33이라고 했을 때 조건을 만족하는 소수 p, q를 구하면
$33 = p \times q$에서 직관적으로 3,11을 구할 수 있다.
$\phi(N) = (p-1)(q-1) = (3-1)(11-1) = 20$
$d \times e \bmod \phi(N) = 1$
$7 \times e \bmod 20 = 1$
$\therefore e = 3$
최종적으로 $C = M^e \bmod N$이므로 $5^3 \bmod 33 = 26$이 된다.

정답 ④

11. ○△× 19.사이버

IEEE 802.11i에서 데이터를 보호하기 위해서 AES 알고리즘을 사용한 암호화 운영모드와 메시지 인증기법을 가장 적절하게 짝지은 것은?

① CBC 모드, HMAC 인증
② CBC 모드, CBC-MAC 인증
③ CTR 모드, HMAC 인증
④ CTR 모드, CBC-MAC 인증

- CCMP는 128bit의 대칭키를 사용하고, 48bit의 초기벡터를 사용한다. AES가 제공하는 여러 모드 중 CCMP는 Counter 모드 기반으로 CBC MAC(Cipher Block Chaining Message Authentication Code)을 결합한 CCM을 기반으로 한다.

오답피하기 ④ CCMP는 AES 알고리즘을 사용한 CTR 모드를 사용하고, 인증기법으로 CBC-MAC을 사용한다.

정답 ④

12. ○△× 19.사이버

이메일 보안 S/MIME에 대한 설명 중 가장 적절한 것은?

① 동봉된 데이터(enveloped data)는 암호화된 내용과 서명자의 공개키로 구성된다.
② 서명된 데이터(signed data)는 메시지 다이제스트 값을 서명자의 공개키로 암호화한 후, 그 값을 Base64로 부호화한다.
③ 명문-서명 데이터(clear-signed data)는 내용과 내용에 대한 전자서명으로 구성되며, 전자서명만 Base64로 부호화한다.
④ 서명되고 동봉된 데이터(signed and enveloped data)에서 서명만 되거나 암호화된 개체는 중첩될 수 없다.

- 명문-서명 데이터(Clear-singed data)는 서명된 데이터로서 내용에 대한 디지털 서명을 한다. 그러나 이 경우 오직 디지털 서명만 base64로 부호화하고 내용은 부호화하지 않는다. 결국 S/MIME 기능이 없는 수신자가 비록 서명을 인증할 수는 없지만 메시지 내용을 볼 수는 있다.

오답피하기 ① 동봉된 데이터에는 암호화된 세션키와 수신자 정보(RecipientInfo)가 있다. 수신자 정보에는 수신자의 공개키 인증서 식별자, 세션키 암호에 사용된 알고리즘 식별자가 들어 있다. ② 서명된 데이터는 서명자의 개인키로 암호화해서 디지털 서명을 생성한다. 그리고 base64 부호화를 이용해 내용과 서명을 부호화한다. ④ 서명되고 동봉된 데이터는 서명만 되거나 암호화된 개체는 중첩될 수 있다. 그래서 암호화된 데이터는 서명될 수 있고 서명된 데이터나 명문-서명 데이터는 암호화될 수 있다.

정답 ③

13. ○△× 19.사이버

웹사이트와 브라우저에 대한 공격 유형에 관한 설명 중 ㉠과 ㉡에 들어갈 용어로 가장 적절하게 연결된 것은?

보기

(㉠) 공격법의 한 예로는 URL에 인자 형태로 악성 스크립트를 포함시킨 메일을 사용자에게 보낸 후, 사용자가 URL을 클릭하면 서버로부터 반송된 오류 메시지에 포함된 악성 스크립트가 실행되는 방법이 있다.
(㉡) 공격법의 한 예로는 로그인 상태인 사용자의 세션 쿠키와 다른 인증정보를 취약한 웹 애플리케이션에 자동으로 포함시키고, 공격자가 의도한 HTTP 요청을 사용자가 보낸 것처럼 자동으로 보내는 방법이 있다.

	㉠	㉡
①	Reflected XSS	CSRF
②	SQL 인젝션	Reflected XSS
③	CSRF	SQL 인젝션
④	Reflected XSS	S-HTTP

Reflected XSS(반사형 XSS)

- Reflected XSS 공격은 사용자가 악성 스크립트 코드가 인자 형태로 포함된 URL을 클릭할 때 악성 스크립트 코드가 서버 사이트에 의해 HTML 문서로 반사되어 웹 브라우저에서 실행된다.
- 공격 스크립트가 포함된 URL을 그대로 전달하면 금방 드러날 수 있기 때문에 공격 스크립트 부분은 주로 인코딩을 한 후 전달하여 사용자가 쉽게 눈치 채지 못하도록 만드는 경우가 많다.
- 즉, 반사형 XSS는 외부에 있는 악성 스크립트(외부 사이트 또는 이메일 등에 악성 스크립트가 포함된 링크 등)가 희생자 액션에 의해 취약한 웹 서버로 전달되고, 웹서버의 응답 페이지에 해당 악성 스크립트가 삽입되어(DB에 저장되는 것이 아님) 희생자 측에 전달되어 동작하는 방식이다.
- 희생자 액션이란 공격자에 의해 조작된 사이트에 접근 시 그 서버에서 악성 스크립트를 포함하여 리다이렉트되는 경우나 악성 스크립트가 포함된 링크를 가지고 있는 이메일을 받은 후 이를 클릭하여 취약한 웹서버로 요청 정보를 보내는 행위 등을 말한다.

오답피하기 ① ㉠ XSS 공격유형 중 반사형 XSS에 대한 설명이다. ㉡ 웹 애플리케이션에서 정상적인 경로를 통한 요청과 비정상적인 경로를 통한 요청을 서버가 구분하지 못하는 경우를 악용하는 CSRF 공격에 대한 설명이다.

정답 ①

14. ○△× 19.사이버

다음에서 설명하는 서명기법을 사용하는 응용보안 프로토콜로 가장 적절한 것은?

> 보기
>
> 사용자의 신용카드 번호와 같은 지불정보는 은행의 공개키로 암호화하여 상점에 숨기고, 주문정보는 상점의 공개키로 암호화하여 은행이 알지 못하도록 하는 서명기법

① PGP(Pretty Good Privacy)
② SET(Secure Electronic Transaction)
③ IPsec(IP Security)
④ Bitcoin

- 비트코인(Bitcoin) : 2009년 나카모토 사토시라는 프로그래머가 만든 가상 화폐의 일종으로, 이용자 간의 P2P(파일공유 시스템)를 기반으로 통화의 발행 및 거래가 이루어진다. 비트코인은 다른 가상 화폐와 달리 일반 화폐처럼 오프라인에서 실제 재화나 서비스를 구매할 수 있다. 또한 민간 거래소에서 달러나 유로 등 기존 화폐로 쉽게 바꿀 수도 있다. 보안 측면에서 비트코인에 주목하는 것은 비트코인의 가치가 상승하면서 이를 탈취하기 위한 악성코드도 증가하고 있기 때문이다. 가장 일반적인 형태의 비트코인 악성코드는 비트코인 확인과 전송에 사용되는 암호키를 저장 및 생성하는 소프트웨어 '지갑(Wallets)'을 공격하는 것으로 알려지고 있다.

오답피하기 ② SET은 이중서명을 통해 사용자가 지불정보(신용카드 번호 등)는 상점에게 숨기고 주문정보는 은행에게 숨기는 기능을 제공하여 사용자의 프라이버시가 보호되도록 한다. 즉, 사용자의 주문정보는 상점의 공개키로 암호화하고 지불정보는 은행의 공개키로 암호화하여 전송함으로써 상점은 주문정보만을 은행은 지불정보만을 볼 수 있도록 한다.

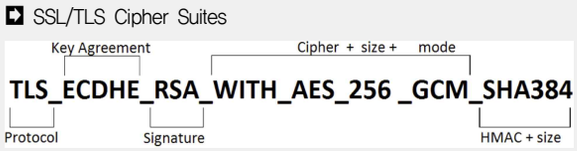
정답 ②

15. ○△× 19.사이버

웹 보안을 위한 TLS 프로토콜의 핸드셰이크 과정에서 클라이언트와 서버가 Cipher Suite로 TLS_RSA_WITH_AES_128_CBC_SHA256을 채택하였다. 다음 설명 중 가장 적절하지 않은 것은?

① RSA 알고리즘을 이용하여 상호 인증을 수행한다.
② 레코드 프로토콜에서 데이터를 암호화할 때, 128비트 키 AES 알고리즘을 CBC 모드로 사용한다.
③ 사용 중인 AES 알고리즘은 암호명세변경(ChangeCipherSpec) 프로토콜을 통해 변경할 수 있다.
④ 레코드 프로토콜에서 메시지 인증 값은 해시함수 SHA256을 CBC-MAC 방식으로 사용하여 만든다.

SSL/TLS Cipher Suites



오답피하기 ④ 키교환 및 인증 알고리즘으로 RSA를 사용하고, 대칭 암호 알고리즘으로 AES를 사용하며 암호키 길이는 256 비트, 블록 암호 모드는 CBC이고, HMAC용 해시 알고리즘은 SHA-256을 사용하는 cipher suite 이다.

정답 ④

16. ○△× 19.사이버

운영체제의 이중 모드에 대한 설명 중 ㉠과 ㉡에 들어갈 용어로 가장 적절하게 연결된 것은?

> 보기
>
> 운영체제의 구조는 이중 모드(dual mode)로 되어 있는데, 이는 사용자 모드(user mode)와 커널 모드(kernel mode)이다. 이 중 사용자 모드에서 하드웨어 자원을 사용하려고 하면 (㉠)가(이) 발생해서 운영체제에 도움을 요청한다.
> 또한, 사용자 모드로 실행 중인 프로그램에서 포인터를 사용하여 커널 주소 영역 메모리를 접근하려 하면 (㉡)를(을) 발생시켜 커널 영역을 보호한다.

㉠	㉡

① 시스템 호출	교착상태
② 예외	스케줄링
③ 시스템 호출	예외
④ 교착상태	시스템 호출

오답피하기 ③ 시스템 호출은 사용자 프로그램이 자신을 대신하여 운영체제가 수행하도록 지정되어 있는 작업들을 운영체제에게 요청할 수 있는 방법을 제공한다. 시스템 호출 중에 비정상적인 상황이 발생 가능한데 이 경우 예외 처리를 통해 대응한다.

정답 ③

17. ○△× 19.사이버

보안 운영체제의 설계 원리와 이에 대한 설명으로 가장 적절하지 않은 것은?

① 최소권한: 각각의 사용자와 프로그램은 가능한 최소한의 권한을 사용하여 시스템 자원을 사용하여야 한다.
② 허용에 근거한 접근: 접근 검토에 대한 기본 값은 접근 허용이며, 설계자는 접근을 차단하여야 하는 항목의 식별에 주의하여야 한다.
③ 완전한 조정: 직접적인 접근 시도와 접근 통제 메커니즘을 우회하려는 접근 시도를 완전히 검사하여야 한다.
④ 권한분리: 객체에 대한 권한은 두 개 이상의 조건에 의존하여야 한다.

보안운영체제 시스템 설계원리
- 최소권한: 사용자와 프로그램이 최소한의 권한만을 사용해야 정보의 손상을 최소화할 수 있다.
- 보호 메커니즘의 경제성: 소규모로 단순하게 보호 메커니즘을 만들어야 한다.(단, 충분한 분석과 시험 그리고 검증을 해야 한다.)
- 개방형 설계: 독립적인 확인이 제공되어야 한다.
- 완전한 조정: 모든 접근 시도는 완전히 검사되어야 한다.
- 허용에 의한 접근: 접근 거부가 원칙이다.
- 권한 분리: 객체에 대한 접근권한은 두 개 이상의 조건에 의존해야만 하나의 보호시스템이 파괴되어도 안전하다.
- 최소 공통 메커니즘: 논리적, 물리적 분리를 채택하면 공유에 의한 위험이 감소한다.(공유 객체는 정보 흐름을 위한 잠재적인 경로를 제공)
- 사용의 용이성: 보안메커니즘은 사용이 용이하여 우회가능성이 적어야 한다.
- 계층적 보안성: 가능한 위협을 여러 단계에서 방어한다.

오답피하기 ② 허용에 근거한 접근은 접근 거부가 원칙이다. 즉 접근 검토에 대한 기본 값은 접근 거부이며, 설계자는 접근을 허용하여야 하는 항목의 식별에 주의하여야 한다.

정답 ②

18. ○△× 19.사이버

BLP(Bell-LaPadula) 보안모델이 가지고 있는 특성과 규칙에 대한 설명으로 가장 적절하지 않은 것은?

① 정보의 불법적인 파괴나 변조를 방지하기보다 비밀정보의 허가없는 접근을 방지하는 것이 목표이다.
② 강제적 정책에 의한 접근통제를 원할 때에 대한 통제 규칙을 정의한다.
③ 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높으면 주체는 객체에 쓰기를 할 수 없다.
④ 주체가 객체를 읽기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 낮아야 한다.

BLP 보안 규칙
- No read up: 주체는 같거나 낮은 보안 수준의 객체만 읽을 수 있다. 단순 보안 속성(ss-property, simple security property)으로 불린다.
- No write down: 주체는 같거나 높은 보안 수준의 객체에만 쓸 수 있다. *속성(*-property, star property)으로 불린다.

오답피하기 ④ 주체가 객체를 읽기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높아야 한다.

정답 ④

19. ○△× 19.사이버

다음과 같은 사례를 방지하기 위한 데이터베이스 보안통제로 가장 적절한 것은?

보기

낮은 비밀 취급 등급자가 레코드 입력 시 오류를 통하여 자신보다 높은 비밀 취급 등급자가 있다는 사실을 알게 되는 사례

① 접근 통제
② 추론 통제
③ 흐름 통제
④ 무결성 통제

다중사례화(Polyinstantiation)
- 낮은 등급자가 레코드 입력 시 높은 등급자가 존재하고 있다는 것을 입력오류를 통해 확인하는 것을 방지하기 위한 방법이다.
- Polyinstantiation은 두 가지 버전의 동일 객체를 생성함으로써 낮은 수준의 주체가 실제 정보를 알지 못하게 하며, 보안 수준을 갖지 않은 엔티티에게 거짓 정보(Cover Story)를 제공하는 방법이다.

오답피하기 ② 보기는 다중사례화에 대한 설명이다. 다중사례화는 추론 공격에 대한 대응책이다.

정답 ②

20. ○△× 19.사이버

소프트웨어 개발과정에서 소스코드에 존재하는 버퍼 오버플로우에 취약한 함수, 하드 코드된 패스워드 등 잠재적인 취약점을 제거하고, 보안을 고려하여 기능을 구현할 때 지켜야 할 보안활동으로 가장 적절한 것은?

① 안전한 코딩(secure coding)
② 위험분석(risk analysis)
③ 모의 침투(penetration test)
④ 디지털 포렌식(digital forensics)

◦ 모의 해킹(침투 테스트, Penetration Testing): 보안이 취약한 부분을 찾아내고 사전 조치 및 개선 방안을 마련하여 보안 사고를 미연에 방지하기 위해 시행하는 선의의 해킹. 사전에 허가된 사람에게 대상 서버나 서비스에 대해 실제 해커와 동일한 방법을 이용하여 침투 가능성을 진단한다.

오답피하기 ① 시큐어 코딩(secure coding, 소프트웨어 개발 보안)은 개발하는 소프트웨어가 복잡해짐으로 인해 보안상 취약점이 발생할 수 있는 부분을 보완하여 프로그래밍하는 것이다. 시큐어 코딩에는 안전한 소프트웨어를 개발하기 위해 지켜야 할 코딩 규칙과 소스 코드 취약 목록이 포함된다.

정답 ①

2020년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

비전공자도 합격 전략 과목으로 만들수 있는 정보보호론!

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2019.09~2019.10	2019.11~2019.12	2020.01~2020.02	2020.03~2020.04	2020.05~2020.06	2020.07~2020.08
전산개발	이론 1.0	기본+심화	용어+요약 1.1 + 1.2	속성이론 1.4			
	기출+적중 3.0		핵심기출 700선 3.1	최고수준 800제 3.3			
	모의고사 5.0				국가직 9급 5.1	지방직 등 9급 5.2	국가직 7급 5.3
정보보호직+경간부 7.0			정보보안기사 필기 7.1				
교재		2020 탑스팟 이론서	핵심기출 700선	·2020 탑스팟 이론서/ 최고수준 800제	프린트물	프린트물	프린트물
문제난이도		중~중상	중~중상	중상~상	중상~상	중상~상	상
비고		·이론서2권-전2권 구성 ·주3회 이론수업 ·매주 복습 퀴즈 진행	·연도별 기출문제 풀이 3.2 -교재프린트 제공, 동영상 진행 ·핵심기출 700선 (문제편/정답·해설편/용어·요약집) -전3권 구성 ·정보보안기사는 11월 개강	·최고 수준 800제 (제본, 수강생 제공)는 고득점 합격을 목표로 함	·모의고사식 실전 훈련	·모의고사식 실전 훈련 ·최신 정보보안기사 기출문제 포함 모의고사 진행	·모의고사식 실전 훈련 ·국회사무처 등 시험대비 겸합 ·최종 마무리 정리

추천과정	
전산개발(9급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2
군무원(9급, 7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2
전산개발(7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3
정보보호직	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1
사이버, 경찰간부	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2 7급 대비 모의고사 5.3

빅데이터 1.0 / 이론

- 1.1 기본+심화 통합이론
- 1.2 핵심 용어 정리 200선(용어집)
- 1.3 핵심 요약집 정리
- 1.4 속성 이론

빅데이터 3.0 / 기출+적중

- 3.1 핵심기출 700선
- 3.2 연도별 기출문제 풀이
- 3.3 최고수준 800제(학원 내부교재)

빅데이터 5.0 / 모의고사

- 5.1 국가직 9급 대비 모의고사
- 5.2 지방직, 교육청, 서울시, 군무원 대비 모의고사
- 5.3 7급 대비 모의고사

빅데이터 7.0 / 정보보호직+경간부

- 7.1 정보보안기사 필기(알기사)

기타 무료 강의

- A 정보보호론 학습 전략
- B 정보보호론 기초 입문 과정
- C 계리직 대비 정보보호론

[전산직 공채 총정리 (3년간)]

시험종류			2017년				2018년				2019년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8~2.22	3.11	90~	3	3.5 ~ 3.15	4.14	70점후	-				컴일,네트워크보안,시스템보안	필기 합격선이 2016년, 2017년 모두 90점이상 공무원기출+정보보안기사필기 문제집에서 다수 출제
해경	전산	7급					1	3.5 ~ 3.15	4.14	-	-				서류전형	
국가직	전산개발	9급	35	2.1 ~ 2.6	4.8	84	50	2.20 ~ 2.23	4.7	73	83	2.20~2.23	4.6	83	국,영,한,컴일,정보	전산개발, 정보보호직 동시 접수 불가
국가직	정보보호	9급	7	2.1 ~ 2.6	4.8	83	5	2.20 ~ 2.23	4.7	69	8	2.20~2.23	4.6	75	국,영,한,네트워크보안,시스템보안	전산개발, 정보보호직 동시 접수 불가
지방직	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.12 ~ 3.16	5.19	시도별	시도별	4.8~4.12	6.15	시도별	국,영,한,컴일,정보	지방직, 교육청 동시 접수 가능, 동시 응시는 불가
교육청	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.26 ~ 3.30	5.19	시도별	시도별	4.15~4.19	6.15	시도별	국,영,한,컴일,정보	거주지 제한 있음, 2019년부터 지방직과 시험지 동일
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12 ~ 3.16	6.23	88	18	3.12~3.18	6.15	76	국,영,한,컴일,정보	거주지 제한 없음, 2019년부터 지방직 시험일자와 동일
군무원	국방부	7급					2	6.7 ~ 6.12	8.11	77	14	4.12~4.17	6.22	74	국,자구,DB,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	국방부	9급	11	4.17~4.21	7.1	72	13	6.7 ~ 6.12	8.11	77.33	8	4.12~4.17	6.22	78.67	국,컴일,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	육군	9급	24	4.24~4.28	7.1	68	18	6.7 ~ 6.12	8.11	74.67	56	4.12~4.17	6.22	77.33	국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7 ~ 6.12	8.11	73.33	19	4.12~4.17	6.22	73.33	국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7 ~ 6.12	8.11	73.33	21	4.12~4.17	6.22	76	국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25	83	3	5.20~5.24	8.24		국,영,한,컴일,정보	객관식 5지 선다형 출제
국가직	전산개발	7급	26	6.5~6.9	8.26	75.83	29	7.14~7.17	8.18	74.16	30	7.14~7.17	8.17		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-	10	7.11~7.30	8.11	-	10	5.24~6.3	7.2		실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격, 경력채용
경찰	사이버(보안)	경장					135	7.20~7.31	9.1	시도별	79	7.12~7.22	8.10		필기(2): 정보보호론,시스템네트워크보안 선택(1): 정보보호관리및법규,디지털포렌식개론, 데이터베이스론	객관식 과목별 20문항, 경력채용 필기시험(50%)→신체,적성,체력(25%)→면접(25%)
지방직(서울)	전산개발	7급					3	3.12~3.16	6.23	80	4	8.6~8.9	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 없음
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13	76.42	2	8.5~8.7	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 있음
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15	312.5(1차) 463.5(2차)	5	8.20~8.29	10.5		필수 : 정보보호론(객), 시스템네트워크보안㈜ 선택 : DB, 통신이론, 소공 중 택1	정보보호론은 전 범위에서 출제 시스템네트워크보안은 해당 범위에서만 서술식으로 출제
국가직(추가)	전산개발	9급	10	8.14~8.17	10.21	80									국,영,한,컴일,정보	2017년 하반기 추가 채용
지방직(추가)	전산개발	9급	시도별	10.20~10.26	12.16	시도별									국,영,한,컴일,정보	2017년 하반기 추가 채용

※ 만든이 : 지안에듀-조현준 선생(정보보호론, 자료구조론, 정보보안기사 담당), 최신 자료는 지안에듀(www.zianedu.com) 조현준 교수방 참조