<정보보호론>

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 답 ①	<국가직 동형모의고사 2회 1번> 1. 능동적 공격(active attack)에 해당하지 않는 것은? ① 메시지 내용 공개(release of message contents) ② 재전송(replay) ③ 메시지 수정(modification of message) ④ 신분위장(masquerade) 답 ①

2. 전자서명이 제공하는 보안 요소가 아닌 것은? ① 메시지 무결성 ② 서명자 인증 ③ 서명 부인 방지 ④ 메시지 기밀성 답 ④	<진도별 모의고사 - 무결성&인증 27번> 27. 전자서명(digital signature)에 대한 설명으로 옳지 않은 것은? ① 메시지의 기밀성을 보장한다. ② 메시지 또는 메시지의 해시값에 대한 서명을 생성한다. ③ 송신자의 키 쌍을 사용한다. ④ 서명과 함께 메시지를 함께 전송해야 한다. 답 ①

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 답 ④	<진도별 모의고사 - 정보보호관리체제> 23. TCSEC에 대한 설명으로 옳지 않은 것은? ① 기밀성과 가용성에 대한 요구사항을 골고루 다룬다. ② 가장 높은 평가 수준은 A이다. ③ 높은 등급으로 갈수록 보안 기능 요구사항과 보안 보증 요구사항이 체계적으로 증가한다. ④ 평가시 운영체제에 구분을 둔다. 답 ①

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 답 ③	<동형모의고사 11회 2번> 2. 클락-윌슨(Clark-Wilson) 보안 모델에 대한 설명으로 옳지 않은 것은? ① 비인가자들의 데이터 변형 방지, 내/외부의 일관성 유지, 합법적인 사용자에 의한 불법적인 수정 방지를 목표로 한다. ② 비즈니스 입장에서 직무분리 개념을 적용하여 이해가 충돌하는 회사 간의 정보 흐름이 일어나지 않도록 통제한다. ③ 정보의 입력, 처리, 확인은 여러 사람이 나누어 관리한다. ④ 사용자가 직접 객체에 접근하는 것을 금지하며 응용 프로그램의 사용을 강제한다. 답 ②

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

답 ②

<동형모의고사 1회 6번>

6. 정보보호의 목표의 연결로 옳은 것은?

<보기1>
ㄱ. 전송 도중 데이터가 위변조되지 않아야 한다. ㄴ. 정당한 자임을 상대방에게 입증해야 한다. ㄷ. 인가된 사용자만이 데이터를 읽을 수 있다. ㄹ. 인가된 사용자가 조직의 정보자산에 적시에 접근하여 업무를 수행할 수 있도록 한다.

<보기2>	
A. 기밀성	B. 무결성
C. 가용성	D. 인증성

	ㄱ	ㄴ	ㄷ	ㄹ
①	A	B	C	D
②	A	C	D	B
③	B	C	A	D
④	B	D	A	C

답 ④

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 답 ④	<진도별 모의고사 - 정보보호관련법 8번> 8.「개인정보보호법」상 "개인정보"에 관한 내용으로 옳지 않은 것은? ① 살아 있는 개인에 관한 정보이다. ② 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보이다. ③ 해당 정보만으로는 특정 개인을 알아볼 수 없으며 다른 정보와 결합하여도 알아볼 수 없는 정보이다. ④ 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)도 개인정보에 해당된다. 답 ③

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 답 ③	<동형모의고사 5회 7번> 7. NAT(Network Address Translation)는 고갈되는 공인 IP주소를 효과적으로 사용하려는 목적과 내부 시스템의 네트워크 구조를 노출하지 않는 보안성을 제공한다. 다음 중 NAT 구현 방법에 해당하지 않는 것은? ① Normal NAT ② Reverse NAT ③ Direct NAT ④ Exclude NAT 답 ③

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

답 ②

<진도별 모의고사 - 암호시스템 127번>
127. 다음 <보기>의 특성을 갖는 공격은 무엇인가?

<보기>
◦ 암호화된 통신 또는 키 교환 프로토콜과 관계있는 공격이다.
◦ A와 B가 안전한 통신을 위해 키를 교환할 경우 공격자는 자기 자신을 통신 라인에서 A와 B 사이에 위치하여 A 또는 B에게 자기 자신의 키를 주고, 자기 자신은 A 또는 B의 키를 가로챈다. A가 B에게 보내는 메시지를 공격자가 해독해서 보고, 자기 자신의 키로 암호화해서 보내면 B가 다시 메시지를 복호화한다.
◦ A와 B는 안전하게 통신을 하고 있다고 생각하지만 공격자가 모든 것을 알아내고 있는 공격이다.

① 재전송 공격(replay attack)
② 중간자 공격(man in the middle attack)
③ 전수 공격(brute force attack)
④ 알려진 평문 공격(known-plaintext attack)

답 ②

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.

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

답 ④

<진도별 모의고사 - 암호시스템 94번>

94. 공개키 암호 방식을 사용할 경우 다음 <보기>의 상황에서 사용해야 할 키(key)로 옳은 것은?

<보기>
ㄱ. 철수가 영희에게 보내는 메시지를 제3자가 볼 수 없도록 암호화하여 전송하려 한다. ㄴ. 철수가 영희에게 철수가 만든 문서이면서 문서가 변경되지 않았음을 확신시켜주는 정보를 함께 보내고자 한다.

	ㄱ	ㄴ
①	철수의 개인키	영희의 공개키
②	철수의 공개키	영희의 개인키
③	영희의 공개키	철수의 개인키
④	영희의 개인키	철수의 공개키

답 ③

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. 답 ①	<동형모의고사 14회 7번> 7.「개인정보 보호법」 3조 개인정보 보호 원칙으로 옳은 것은? ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최대한의 개인정보만을 적법하고 정당하게 수집하여야 한다. ② 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다. ③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 부인방지성이 보장되도록 하여야 한다. ④ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 처리하지 않는다. 답 ②

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. 답 ②	<동형모의고사 4회 13번> 13. 다음 중에서 버퍼 오버플로우(Buffer Overflow)에 대한 설명으로 옳지 않은 것은? ① 스택 오버플로우(Stack Overflow)는 복귀주소를 변조하여 악성 모듈을 실행하여 공격할 수 있다. ② 스택 상에 있는 공격자의 코드가 실행되지 못하도록 한다. ③ 스택 스매싱(stack smashing)을 이용하여 복귀주소 변경을 미리 확인할 수 있다. ④ rtl(return to libc) 공격은 스택에 있는 복귀주소를 실행 가능한 libc 영역의 주소와 같은 임의의 주소로 돌려 원하는 함수를 수행하게 한다. 답 ③

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

답 ③

<정보보호론 이론서 p.410>

	2.4.7 업무환경 보안
2.5. 인증 및 권한 관리	2.5.1 사용자 계정 관리 2.5.2 사용자 식별 2.5.3 사용자 인증 2.5.4 비밀번호 관리 2.5.5 특수 계정 및 권한관리 2.5.6 접근권한 검토

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

답 ②

<진도별 모의고사 - 정보보호관련법 11번>
11. 「개인정보보호법」 상 다음의 내용을 갖고 있는 조직은 무엇인가?

> ◦개인정보 보호에 관한 사무를 독립적으로 수행하기 위한 조직으로「정부조직법」 제2조에 따른 중앙행정기관으로 본다.
> ◦국무총리 소속이다.
> ◦상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.

① 개인정보 보호책임자　② 개인정보 보호위원회
③ 한국 인터넷 진흥원　④ 정보보호 최고 책임자

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.

	(가)	(나)
①	GET	XSS
②	GET	CSRF
③	POST	XSS
④	POST	CSRF

답 ④

<동형모의고사 5회 16번>

16. 다음 중 HTTP(HyperText Transfer Protocol)에 대한 설명으로 옳지 않은 것은?

① 서버는 클라이언트로부터 요청이 없으면 응답을 보낼 수 없다.

② GET 요청 메소드는 웹 페이지 등의 자원을 전송해줄 것을 요청한다.

③ POST 요청 메소드를 사용할 경우 요청 메시지에는 요청 바디(Body)가 포함되어 클라이언트가 서버로 보내는 데이터를 추가할 수 있다.

④ 상태 코드는 요청 메소드에 포함된다.

답 ④

<진도별 모의고사 - 웹보안 34번>

34. 다음 설명에 해당하는 공격은 무엇인가?

<보기>
◦ 로그온 된 피해자의 취약한 웹 애플리케이션에 피해자의 세션 쿠키와 기타 다른 인증정보를 자동으로 포함하여 위조된 HTTP 요청을 강제로 보내도록 하는 것이다. ◦ 공격자가 취약한 애플리케이션이 피해자로부터의 정당한 요청이라고 오해할 수 있는 요청들을 강제로 만들 수 있다. ◦ 예방을 위해 각각의 HTTP 요청에서 예측 불가능한 토큰을 포함해야 한다.

① 크로스사이트 스크립트(XSS)

② 크로스사이트 요청 위조(CSRF)

③ Format String 공격

④ 리버스 엔지니어링(reverse engineering) 공격

답 ②

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 답 ②	<동형모의고사 13회 18번> 18. 다음 <보기>의 내용은 어느 S/MIME 유형에 해당하는가? ㄱ. 특정 대칭암호 알고리즘에서 사용할 의사랜덤 세션키를 생성한다. ㄴ. 각 수신자를 위해 수신자의 공개키로 세션키를 암호화한다. ㄷ. 각 수신자를 위해 수신자정보라고 알려진 블록을 준비한다. 수신자 정보 블록에는 수신자의 공개키 인증서 식별자, 세션키 암호에 사용된 알고리즘 식별자, 암호화된 세션키가 들어있다. ㄹ. 세션키로 메시지 내용을 암호화한다. ① 봉함 데이터 ② 서명 데이터 ③ 명문 서명 데이터 ④ 서명과 봉함 데이터 답 ①

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 답 ③	<동형모의고사 5회 15번> 15. 리눅스의 shadow 파일을 이용하여 알 수 있는 정보가 아닌 것은? ① 사용자 계정 이름 ② 암호화된 패스워드 ③ UID와 GID ④ 암호 변경 최소 기간 답 ③

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

답 ④

<진도별 모의고사 － 무결성&인증 36번>

36. <보기>를 참고하여 DSS(Digital Signature Standard)에 대한 내용으로 옳지 않은 것은?

<보기>

송신측은 소수 p를 512비트에서 1024비트 사이의 길이가 되도록 선정한다.

송신측은 160비트 소수 q를 선택한다. q는 p-1의 약수이다.

$e_1 = e_0^{(p-1)/q} \bmod p$, e_0는 원시근이다.

$e_2 = e_1{}^d \bmod p$,

공개키는 {e_1, e_2, p, q}이다. 개인키는 {d}이다.

① Schnorr 구조에서 빌려온 아이디어를 ElGamal에 더하여 수립한 DSA(Digital Signature Algorithm)를 사용한다.

② 서명 생성 과정에서 두 개의 서명을 생성하며 이 중 첫 번째 서명 값은 메시지 M과 무관하다.

③ 서명 검증 과정에서 출력된 결과는 메시지와 비교하여 검증한다.

④ 동일한 소수 p를 사용할 경우 RSA 알고리즘보다 빠르다.

답 ③

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

답 ①

<진도별 모의고사 - 웹보안 8번>

8. 웹 브라우저와 웹 서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법의 프로토콜 중 다음 <보기>의 설명에 해당하는 것은?

<보기>
◦ 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유키를 결정한다. ◦ 인증서를 이용한 서버와 클라이언트 간 인증을 수행한다.

① 핸드셰이크 프로토콜
② 암호사양 변경 프로토콜
③ 경고 프로토콜
④ 레코드 프로토콜

답 ①

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, 해시함수에 입력되는 블록의 크기와 같다.

답 ③

<진도별 모의고사 - 무결성&인증 23번>

23. 다음 수식에 의해 출력되는 정보는 무엇인가?

H[(K$^+$⊕opad) ‖ H[(K$^+$⊕ipad) ‖ M]]
마지막 암호화 후 왼쪽에서 n비트를 출력한다.
H : 해시함수
K$^+$: 대칭키 K에 0을 패딩한 값
⊕ : XOR
‖ : 연결
ipad, opad : 특정 상수

① HMAC ② SHA-512
③ CMAC ④ MD

답 ①

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

Pi : 평문 블록 Ci : 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.

답 ①

<진도별 모의고사 - 암호시스템 79번, 80번>

79. DES의 블록 운용 모드 중 암호 피드백 모드(CFB : Cipher FeedBack)에 해당하는 설명은?

① 동일한 키에 의한 동일한 평문 입력은 항상 동일한 암호문을 출력한다.

② 버퍼에 남아있는 암호문과 다음의 평문을 XOR 연산 후 암호화한다.

③ 각 평문블록별로 증가하는 서로 다른 카운터값을 키로 암호화한 후 평문 블록과 XOR 연산을 수행한다.

④ 이전 암호문 블록을 암호화하여 평문 블록과 XOR 연산을 수행한다.

답 ④

80. 다음 중 CFB 모드의 암호화로 옳은 것은?(단, P는 평문 블록, C는 암호문 블록이다)

① $C_j = E_k(C_{j-1} \oplus P_j)$ ② $C_j = E_k(C_{j-1}) \oplus P_j$

③ $C_j = E_k(C_{j-1} \oplus P_{j-1})$ ④ $C_j = E_k(C_{j-1}) \oplus P_{j-1}$

답 ②