정보보호론

문 1. 전자우편 보안 기술이 목표로 하는 보안 특성이 아닌 것은?
① 익명성
② 기밀성
③ 인증성
④ 무결성

문 2. 프로그램이나 손상된 시스템에 허가되지 않는 접근을 할 수 있도록 정상적인 보안 절차를 우회하는 악성 소프트웨어는?
① 다운로더(downloader)
② 키 로거(key logger)
③ 봇(bot)
④ 백도어(backdoor)

문 3. 프로그램을 감염시킬 때마다 자신의 형태뿐만 아니라 행동 패턴까지 변화를 시도하기도 하는 유형의 바이러스는?
① 암호화된(encrypted) 바이러스
② 매크로(macro) 바이러스
③ 스텔스(stealth) 바이러스
④ 메타모픽(metamorphic) 바이러스

문 4. 증거의 수집 및 분석을 위한 디지털 포렌식의 원칙에 대한 설명으로 옳지 않은 것은?
① 정당성의 원칙 – 증거 수집의 절차가 적법해야 한다.
② 연계 보관성의 원칙 – 획득한 증거물은 변조가 불가능한 매체에 저장해야 한다.
③ 신속성의 원칙 – 휘발성 정보 수집을 위해 신속히 진행해야 한다.
④ 재현의 원칙 – 동일한 조건에서 현장 검증을 실시하면 피해 당시와 동일한 결과가 나와야 한다.

문 5. 웹 애플리케이션의 대표적인 보안 위협의 하나인 인젝션 공격에 대한 대비책으로 옳지 않은 것은?
① 보안 프로토콜 및 암호 키 사용 여부 확인
② 매개변수화된 인터페이스를 제공하는 안전한 API 사용
③ 입력 값에 대한 적극적인 유효성 검증
④ 인터프리터에 대한 특수 문자 필터링 처리

문 6. 「개인정보 보호법」상의 개인정보의 수집·이용 및 수집 제한에 대한 설명으로 옳지 않은 것은?
① 개인정보처리자는 정보주체의 동의를 받은 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
② 개인정보처리자는 「개인정보 보호법」에 따라 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
③ 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.
④ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니하는 경우 정보주체에게 재화 또는 서비스의 제공을 거부할 수 있다.

문 7. <보기 1>은 리눅스에서 일반 사용자(hello)가 'ls -al'을 수행한 결과의 일부분이다. <보기 2>의 설명에서 옳은 것만을 모두 고른 것은?

<보기 1>

-rwxr-xr-x 1 hello world 4096 Nov 21 15:12 abc.txt
ⓐ ⓑ

<보기 2>

ㄱ. ⓐ는 파일의 소유자, 그룹, 이외 사용자 모두가 파일을 읽고 실행할 수 있지만, 파일의 소유자만이 파일을 수정할 수 있음을 나타낸다.
ㄴ. ⓑ가 모든 사용자(파일 소유자, 그룹, 이외 사용자)에게 읽기, 쓰기, 실행 권한을 부여하려면 'chmod 777 abc.txt'의 명령을 입력하면 된다.
ㄷ. ⓑ가 해당 파일의 소유자를 root로 변경하려면 'chown root abc.txt'의 명령을 입력하면 된다.

① ㄱ
② ㄱ, ㄴ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

문 8. 다음은 CC(Common Criteria)의 7가지 보증 등급 중 하나에 대한 설명이다. 시스템이 체계적으로 설계되고, 테스트되고, 재검토되도록(methodically designed, tested and reviewed) 요구하는 것은?

낮은 수준과 높은 수준의 설계 명세를 요구한다. 인터페이스 명세가 완벽할 것을 요구한다. 제품의 보안을 명시적으로 정의한 추상화 모델을 요구한다. 독립적인 취약점 분석을 요구한다. 개발자 또는 사용자가 일반적인 TOE의 중간 수준부터 높은 수준까지의 독립적으로 보증된 보안을 요구하는 곳에 적용 가능하다. 또한 추가적인 보안 관련 비용을 감수할 수 있는 곳에 적용 가능하다.

① EAL 2
② EAL 3
③ EAL 4
④ EAL 5

문 9. 다음에 설명한 Diffie-Hellman 키 교환 프로토콜의 동작 과정에서 공격자가 알지 못하도록 반드시 비밀로 유지해야 할 정보만을 모두 고른 것은?

소수 p와 p의 원시근 g에 대하여, 사용자 A는 p보다 작은 양수 a를 선택하고, $x = g^a \bmod p$를 계산하여 x를 B에게 전달한다. 마찬가지로 사용자 B는 p보다 작은 양수 b를 선택하고, $y = g^b \bmod p$를 계산하여 y를 A에게 전달한다. 그러면 A와 B는 $g^{ab} \bmod p$를 공유하게 된다.

① a, b
② p, g, a, b
③ a, b, $g^{ab} \bmod p$
④ p, g, a, b, $g^{ab} \bmod p$

문 10. IEEE 802.11i에 대한 설명으로 옳지 않은 것은?
① 단말과 AP(Access Point) 간의 쌍별(pairwise) 키와 멀티캐스팅을 위한 그룹 키가 정의되어 있다.
② 전송되는 데이터를 보호하기 위해 TKIP(Temporal Key Integrity Protocol)와 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol) 방식을 지원한다.
③ 서로 다른 유무선랜 영역에 속한 단말들의 종단간(end-to-end) 보안 기법에 해당한다.
④ 802.1X 표준에서 정의된 방법을 이용하여 무선 단말과 인증 서버 간의 상호 인증을 할 수 있다.

문 11. SSL(Secure Socket Layer)에서 메시지에 대한 기밀성을 제공하기 위해 사용되는 것은?
① MAC(Message Authentication Code)
② 대칭키 암호 알고리즘
③ 해시 함수
④ 전자서명

문 12. 메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?
① 임의 크기의 메시지에 적용될 수 있어야 한다.
② 해시를 생성하는 계산이 비교적 쉬워야 한다.
③ 다양한 길이의 출력을 생성할 수 있어야 한다.
④ 하드웨어 및 소프트웨어에 모두 실용적이어야 한다.

문 13. 사용자 A가 사용자 B에게 보낼 메시지 M을 공개키 기반의 전자서명을 적용하여 메시지의 무결성을 검증하도록 하였다. A가 보낸 서명이 포함된 전송 메시지를 다음 표기법에 따라 바르게 표현한 것은?

PUx: X의 공개키 PRx: X의 개인키 E(K,M): 메시지 M을 키 K로 암호화 H(M): 메시지 M의 해시 ‖: 두 메시지의 연결

① $E(PU_B, M)$ ② $E(PR_A, M)$
③ $M \| E(PU_B, H(M))$ ④ $M \| E(PR_A, H(M))$

문 14. 대칭키 블록 암호 알고리즘의 운영 모드 중에서 한 평문 블록의 오류가 다른 평문 블록의 암호 결과에 영향을 미치는 오류 전이(error propagation)가 발생하지 않는 모드만을 묶은 것은? (단, ECB: Electronic Code Book, CBC: Cipher Block Chaining, CFB: Cipher Feedback, OFB: Output Feedback)
① CFB, OFB ② ECB, OFB
③ CBC, CFB ④ ECB, CBC

문 15. 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 옳지 않은 것은?
① utmp – 로그인, 로그아웃 등 현재 시스템 사용자의 계정 정보
② loginlog – 성공한 로그인에 대한 내용
③ pacct – 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보
④ btmp – 실패한 로그인 시도

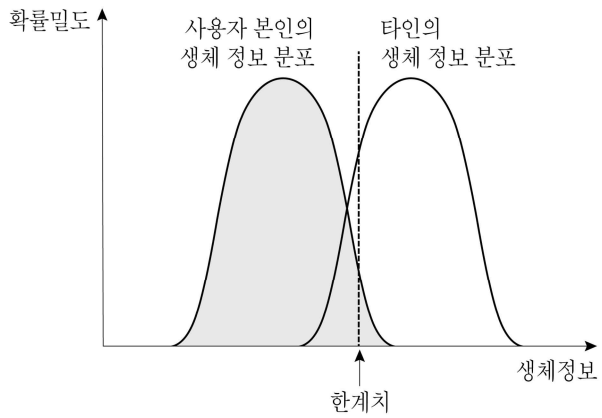
문 16. 「개인정보 보호법」상 개인정보처리자가 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 알려야 할 사항에 해당하지 않는 것은?
① 유출된 개인정보의 항목
② 유출된 시점과 그 경위
③ 조치 결과를 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고한 사실
④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

문 17. 인증서를 발행하는 인증기관, 인증서를 보관하고 있는 저장소, 공개키를 등록하거나 등록된 키를 다운받는 사용자로 구성되는 PKI(Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?
① 인증기관이 사용자의 키 쌍을 생성할 경우, 인증기관은 사용자의 개인키를 사용자에게 안전하게 보내는 일을 할 필요가 있다.
② 사용자의 공개키에 대해 인증기관이 전자서명을 해서 인증서를 생성한다.
③ 사용자의 인증서 폐기 요청에 대하여 인증기관은 해당 인증서를 저장소에서 삭제함으로써 인증서의 폐기 처리를 완료한다.
④ 한 인증기관의 공개키를 다른 인증기관이 검증하는 일이 발생할 수 있다.

문 18. 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?
① 생성된 수열의 비트는 정규분포를 따라야 한다.
② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 없어야 한다.
③ 시드(seed)라고 불리는 입력 값은 외부에 알려져도 무방하다.
④ 비결정적(non-deterministic) 알고리즘을 사용하여 재현 불가능한 수열을 생성해야 한다.

문 19. 사용자 워크스테이션의 클라이언트, 인증서버(AS), 티켓발행서버(TGS), 응용서버로 구성되는 Kerberos에 대한 설명으로 옳은 것은? (단, Kerberos 버전 4를 기준으로 한다)
① 클라이언트는 AS에게 사용자의 ID와 패스워드를 평문으로 보내어 인증을 요청한다.
② AS는 클라이언트가 TGS에 접속하는 데 필요한 세션키와 TGS에 제시할 티켓을 암호화하여 반송한다.
③ 클라이언트가 응용서버에 접속하기 전에 TGS를 통해 발급받은 티켓은 재사용될 수 없다.
④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.

문 20. 생체 인식 시스템은 저장되어 있는 개인의 물리적 특성을 나타내는 생체 정보 집합과 입력된 생체 정보를 비교하여 일치 정도를 판단한다. 다음 그림은 사용자 본인의 생체 정보 분포와 공격자를 포함한 타인의 생체 정보 분포, 그리고 본인 여부를 판정하기 위한 한계치를 나타낸 것이다. 그림 및 생체 인식 응용에 대한 설명으로 옳은 것만을 고른 것은?



ㄱ. 타인을 본인으로 오인하는 허위 일치의 비율(false match rate, false acceptance rate)이 본인을 인식하지 못하고 거부하는 허위 불일치의 비율(false non-match rate, false rejection rate)보다 크다.
ㄴ. 한계치를 우측으로 이동시키면 보안성은 강화되지만 사용자 편리성은 저하된다.
ㄷ. 보안성이 높은 응용프로그램은 낮은 허위 일치 비율을 요구한다.
ㄹ. 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 낮은 허위 일치 비율이 요구된다.

① ㄱ, ㄷ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄴ, ㄹ