2018-국가직-정보보호론-가형-해설

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

1. 전자우편 보안 기술이 목표로 하는 보안 특성이 아닌 것은?
① 익명성
② 기밀성
③ 인증성
④ 무결성
정답 체크 :
(1) 익명성 : 전자우편은 누가 보냈는지 알아야 하므로 익명성이 있으면 안된다.
오답 체크 :
(2) 기밀성 : 전자우편은 중간에 누군가 도청을 해서는 안된다.
(3) 인증성 : 전자우편은 보낸 사람이 누구인지를 알아야 한다.
(4) 무결성 : 전자우편은 메시지의 변조나 위조가 없어야 한다.

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)
정답 체크 :
(4) 백도어 : 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로로 Trapdoor 혹은 Administrative hook이라고도 불린다.
오답 체크 :
(1) 다운로더 : 특정 웹 사이트에서 파일을 내려받고 그 파일이 다시 스파이웨어를 내려받게 한다. 이 스파이웨어는 사용자의 동의를 받지 않고 설치되며 기존 키 워드 검색 프로그램이나 특정 안티스파이웨어 프로그램을 삭제한다.
(2) 키로거 : 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 행위를 말한다. 하드웨어, 소프트웨어를 활용한 방법에서부터 전자적, 음향기술을 활용한 기법까지 다양한 키로깅 방법이 존재한다.
(3) 봇 : 분산 서비스 거부 공격(DDoS)에 사용되는 악성코드를 봇(Bot)이라고 한다.

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
정답 체크 :
(4) 메타모픽(변성) : 감염시킬 때마다 변형, 모양만 변형하는 것이 아니라 행동까지 변화한다. 참고로 다형성(Polymorphic) 또는 갑옷형(Armour) 바이러스는 모양만 변경하고 행동까지 변화하지는 않는다.
오답 체크 :
(1) 암호화 : 바이러스 코드를 쉽게 파악하고 제거할 수 없도록 암호화한 바이러스이다. 바이러스 제작자들은 백신의 진단을 우회하기 위해 자체적으로 코드를 암호화하는 방법을 사용하여 백신 프로그램이 진단하기 힘들게 만들기 시작했다.
(2) 매크로 : 기존의 바이러스는 실행할 수 있는 파일(COM이나 EXE)에 감염된 반면, 매크로 바이러스는 엑셀 또는 워드와 같은 문서 파일의 매크로 기능을 이용하기 때문에 워드나 엑셀 파일을 열 때 감염된다.
(3) 스텔스(은폐형) : 바이러스에 감염된 파일들이 일정 기간의 잠복기를 가지도록 만들어진 바이러스이다. 확산되기도 전에 바이러스가 활동하기 시작하면 다른 시스템으로 전파되기 힘들기 때문에 잠복기를 가진다.

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.
정답 체크 :
(2) 연계보관성 : 해당 설명은 무결성의 원칙이고, 연계보관성의 원칙은 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.
오답 체크 :
(1) 정당성 : 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(3) 신속성 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
(4) 재현 : 법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 한다. 수행할 때마다 다른 결과가 나온다면 증거로 제시할 수 없다.

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
정답 체크 :

(1) 해당 설명은 인젝션 공격(2017 OWASP top 1)에 대한 대비책이 아니라 민감한 데이터 노출(2017 OWASP top 3)에 대한 대비책이다.
오답 체크 :
(2) 기본 옵션은 인터프리터 사용을 피하거나 매개변수화된 인터페이스(PreparedStatement in Java)를 제공하는 안전한 API를 사용한다.
(3) 서버측 "화이트리스트"나 적극적인 입력값 유효성 검증을 한다. 하지만 많은 애플리케이션이 모바일 애플리케이션을 위한 텍스트 영역이나 API와 같은 특수 문자를 필요로 하기에 완벽한 방어책은 아니다.
(4) 남은 동적 쿼리들을 위하여 특정 필터링 구문을 사용하여 인터프리터에 대한 특수 문자를 필터링 처리한다.

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.
정답 체크 :
(4) "개인정보 보호법" 제16조(개인정보의 수집 제한) 상 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.
오답 체크 :
(1) "개인정보 보호법" 제15조(개인정보의 수집·이용) 상 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 1. 정보주체의 동의를 받은 경우, 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, 4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우, 5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
(2) "개인정보 보호법" 제16조(개인정보의 수집 제한) 상 개인정보처리자는 제15조제1항(보기 (1)번) 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
(3) "개인정보 보호법" 제16조(개인정보의 수집 제한) 상 개인정보처리자는 정보주체의 동의를

받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.

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
정답 체크 :
(2)
(ㄱ) : -rwxr-xr-x에서 파일의 소유자는 첫 번째 rwx(읽기/쓰기/실행 가능)를 의미하고, 그룹은 두 번째 r-x(읽기/실행 가능)를 의미하고, 이외 사용자는 마지막 r-x(읽기/실행 가능)를 의미한다. 파일의 소유자의 경우 쓰기가 가능하므로 파일을 수정할 수 있다.
(ㄴ) : 'chmod 777 abc.txt'를 수행하면 -rwxr-xr-x(755)가 -rwxrwxrwx(777)로 바뀐다. 이렇게 되면 모든 사용자가 읽기/쓰기/실행이 가능하다.
오답 체크 :
(1) ㄴ이 없다.
(3), (4)
(ㄷ) : 'chown root abc.txt'라는 명령어는 맞지만, 해당 명령어는 현재의 일반 사용자가 아닌 관리자(root)가 실행해야 한다.

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
정답 체크 :
긴 지문은 허수이고, 진수는 “methodically designed, tested and reviewed”이다.
(3) EAL 4 : methodically designed, tested and reviewed이다.
오답 체크 :
(1) EAL 2 : structurally tested이다.
(2) EAL 3 : methodically tested and checked이다.
(4) EAL 5 : semiformally designed and tested이다.
Tip! : EAL을 테이블로 정리하면 다음과 같다.

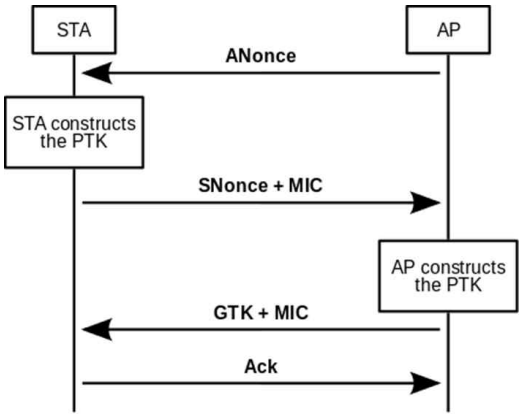
EAL1	functionally tested : 기능 시험
EAL2	structurally tested : 구조 시험
EAL3	methodically tested and checked : 방법론적 시험과 점검
EAL4	methodically designed, tested and reviewed : 방법론적 설계, 시험, 검토
EAL5	semiformally designed and tested : 준정형적 설계 및 시험
EAL6	semiformally verified designed and tested : 준정형적 검증된 설계 및 시험
EAL7	formally verified design and tested : 정형적 검증

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 a^b mod p
④ p, g, a, b, g^{ab} mod p
정답 체크 :
Diffie-Hellman에서 공개되는 정보와 공개되지 않는 정보를 구분하면 다음과 같다.
(1)
공개되지 않는 정보 : a, b는 최종 비밀키를 만들어내는 난수이므로 공개되거나 알려져서는 안된다. 마찬가지로 최종 비밀키 g^{ab} mod p도 알려져서는 안된다. 왜냐하면 알려진 g^a mod p 혹은 g^b mod p와 g^{ab} mod p를 이용하면 a 혹은 b를 알아낼 수 있기 때문이다.
오답 체크 :
(2), (3), (4)
공개되는 정보 : 소수 p와 원시근 g는 공개되어도 무방하다(사용자 A가 만들어서 사용자 B에게 전송하는 것이기 때문에 중간에 도청되어도 상관없다). 그리고 g^a mod p 혹은 g^b mod p는 공개되어 무방하다. 만약, 도청을 해서 g^a mod p 혹은 g^b mod p를 알 수 있다고 하더라도 이산대수 문제에 의해 a 혹은 b를 알아낼 수 없다.

10. IEEE 802.11i에 대한 설명으로 옳지 않은 것은?
① 단말과 AP(Access Point) 간의 쌍별(pairwise) 키와 멀티캐스팅을 위한 그룹키가 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 서버간의 상호 인증을 할 수 있다.
정답 체크 :
(3) 종단간(통신 당사자들)이 아니라 단말과 AP(유무선공유기) 사이의 보안 기법에 해당한다.
오답 체크 :
(1) WPA2는 아래 그림에서 보는 바와 같이 Four-way handshake를 수행한다. AP(유무선공유기)는 단말(STA)에게 난수(ANonce)를 전송한다. 단말은 이를 이용해서 PTK(쌍별키, MIC를 계산하는데 사용)를 만든다. 그리고 단말은 난수(SNonce)와 무결성 코드(MIC)를 전송한다. AP는 이를 이용해서 PTK를 만들고, 단말에게 GTK(멀티캐스팅을 위한 그룹키, 멀티캐스트와 브로드캐스트 패킷을 암호화/복호화하는데 사용)와 무결성 코드(MIC)를 전송한다. 단말은 수신을 잘 받았다는 의미에서 Ack를 보낸다.



(2) WPA2에서는 WPA에서 사용한 TKIP와 새로운 방식은 CCMP를 모두 지원한다.
(4) WPA-Enterprise(기업용)에서는 802.1x와 EAP를 이용하여 무선 단말과 인증 서버(AS) 간의 상호 인증을 수행한다(challeng-response).

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
정답 체크 :
(2) 대칭키 : 암호화(기밀성)을 위해서 사용된다. 대칭키는 의사난수 생성기를 사용하고, 대칭키 공유는 공개키 암호 또는 Diffie-Hellman을 이용한다.
오답 체크 :
(1) MAC : SSL에서 데이터 인증에 사용된다.

(3) 해시 함수 : SSL에서 MAC(데이터 인증)을 생성할 때 사용한다.
(4) 전자서명 : 상대 인증을 위해 사용된다.

12. 메시지 인증에 사용되는 해시 함수의 요건으로 옳지 않은 것은?
① 임의 크기의 메시지에 적용 될 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.
정답 체크 :
(3) 해시는 입력이 1bit 혹은 1Tbit라도 고정된 길이의 출력을 가진다. 이와 같은 특성은 절대 변하지 않는다.
오답 체크 :
(1) 입력 크기에 제한이 있을 수 있지만(SHA-1, SHA-2) 임의 크기의 메시지에 적용될 수 있어야 한다.
(2) 해시를 생성하는 계산이 비교적 쉬워야 한다. 이는 계산 효율이 있어야 하고 구현이 용이해야 함을 의미한다. 아무리 좋은 해시 함수라도 계산이 어렵고 구현이 용이하지 않다면 의미가 없다.
(4) (2)번과 같은 맥락에서 CPU의 특성에 맞게 하드웨어로 구현하든 아니면 소프트웨어로 구현하든 모두 실용적이어야 한다. 실용적이라는 말은 계산의 속도가 현실적이어야 함을 의미한다.

13. 사용자 A가 사용자 B에게 보낼 메시지 M을 공개키 기반의 전자 서명을 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 $M \| E(PR_A, H(M))$
정답 체크 :
(4) 전자서명은 A의 개인키로 메시지 혹은 메시지의 해시값(시간 단축)에 암호화를 수행하는 것이다.
오답 체크 :
(1), (2) 공개키 기반의 전자 서명을 적용하여 메시지의 무결성을 검증하기 위해서는 메시지와 전자 서명을 동시에 보내야 한다. 해당 지문에서는 메시지를 보내지 않는다.
(3) B의 공개키로 암호화를 하는 것은 전자 서명을 적용한 것이 아니라 암호화를 적용한 것이다.

Tip! : 기호가 익숙하지 않은 것을 제외하곤 아주 쉬운 문제에 속한다. 그러므로 암호학에서 기호가 나오면 기호에 익숙해지는 것이 좋다.

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
정답 체크 :
(2)
ECB : 개별적으로 평문 블록을 암호화해서 암호문 블록으로 만든다. 암호화와 복호화가 같은 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 대응하는 블록이 에러가 된다. (오류 전이가 발생하지 않는다.)
OFB : 이전 단계의 출력 블록(평문 블록과 XOR해서 암호문 블록을 만들기 전 단계)을 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 다른 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다. (오류 전이가 발생하지 않는다.)
오답 체크 :
(1), (3), (4)
CFB : 이전 단계의 암호문 블록을 암호화한 후 현재 단계의 평문 블록과 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 다른 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다. (오류 전이가 발생한다.)
CBC : 이전 단계의 암호문 블록과 현재 단계의 평문 블록을 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 다른 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다. (오류 전이가 발생한다.)

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
정답 체크 :
(2) loginlog : 유닉스에서 사용하는 실패한 로그인 시도에 대한 로깅을 수행한다.
오답 체크 :
(1) utmp : 유닉스에서 현재 시스템에 로그인한 사용자의 상태 출력(로깅)한다.
(3) pacct : 유닉스에서 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보 저장하는 로그이다.

(4) btmp : 리눅스에서 실패한 로그인 정보를 담고 있는 로그 파일이다.

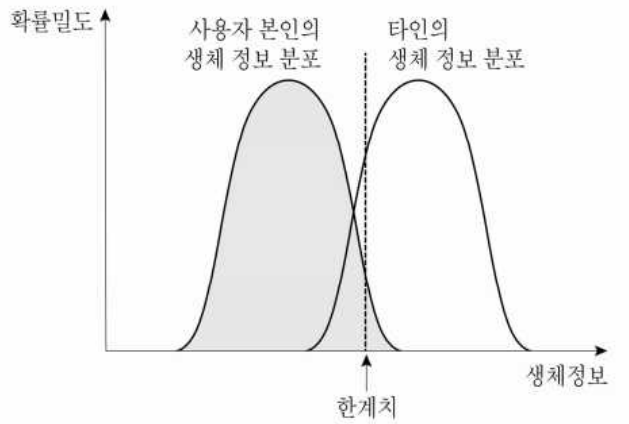
16. 개인정보 보호법 상 개인정보처리자가 개인정보가 유출되었음을 알게 되었을 때에 지체 없이 해당 정보주체에게 알려야할 사항에 해당하지 않는 것은?
① 유출된 개인정보의 항목
② 유출된 시점과 그 경위
③ 조치 결과를 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고한 사실
④ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
정답 체크 :
(3) "개인정보 보호법" 제34조(개인정보 유출 통지 등) 상 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정안전부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정안전부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다. (신고하는 것은 맞는데 이를 정보주체에게 알릴 필요는 없다.)
오답 체크 :
(1), (2), (4)
"개인정보 보호법" 제34조(개인정보 유출 통지 등) 상 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다. 1. 유출된 개인정보의 항목, 2. 유출된 시점과 그 경위, 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, 4. 개인정보처리자의 대응조치 및 피해 구제절차, 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

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 삭제함으로 써 인증서의 폐기 처리를 완료한다.
④ 한 인증기관의 공개키를 다른 인증기관이 검증하는 일이 발생 할 수 있다.
정답 체크 :
(3) 공인인증서의 폐기는 말 그대로 더 이상 사용을 못하게 만드는 것이다. 삭제는 폐기와 별도로 수행되어야 한다.
오답 체크 :
(1) 원래는 사용자가 공개키와 개인키를 만들어 공개키를 인증기관에 전송하는데, 만약 인증기관이 공개키와 개인키를 만들면 개인키를 사용자에게 보내주어야 한다.
(2) 사용자의 공개키에 인증기관의 개인키로 성명을 해서 공인인증서를 생성한다.
(4) 비슷한 일을 수행하는 인증기관끼리 인증 체인을 형성할 수도 있고, 상급 인증기관의 개념을 적용하여 계층 구조를 가질 수도 있다.

18. 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 옳은 것은?
① 생성된 수열의 비트는 정규 분포를 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.
정답 체크 :
(2) 이를 예측 불가능성이라고 한다. 예측 불가능성은 과거에 출력한 의사난수열이 공격자에게 알려져도 다음에 출력하는 의사난수를 공격자는 알아맞힐 수 없다는 성질이다.
오답 체크 :
(1) 생성된 수열의 비트는 정규분포를 따르면 안되고 무작성위성을 가져야 한다. 무작위성이란 의사난수열의 통계적인 성질을 조사해서 치우침이 없도록 하는 성질이다.
(3) 시드라고 불리는 입력 값은 절대로 외부에 알려져서는 안된다. 시드가 알려지면 난수를 그대로 똑같이 만들어 낼 수 있다.
(4) 해당 설명은 난수 생성기의 특성이지 의사 난수 생성기의 특성이 아니다. 의사 난수 생성기는 주기성을 가지며 재현 가능하다.

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 재사용 될 수 없다.
④ 클라이언트가 응용서버에게 제시할 티켓은 AS와 응용서버의 공유 비밀키로 암호화되어 있다.
정답 체크 :
(2) AS는 클라이언트가 TGS에 접속하는데 필요한 세션키와 TGS에 제시할 티켓(TGT)을 사용자 패스워드를 이용한 키로 암호화하여 반송한다.
오답 체크 :
(1) 클라이언트는 AS에게 사용자의 ID를 평문으로 보내지만 패스워드는 보내지 않는다. 이전 버전에서는 패스워드를 평문으로 전송했지만 중간에 도청 문제가 발생하여 더 이상 패스워드를 보내지 않고 서로 사전에 공유한다.
(3) TGS를 통해 발급받은 티켓은 서비스 세션 당 한번 사용하기 때문에 클라이언트가 서버에 접속하기 전에 재사용할 수 있다.
(4) 클라이언트와 서버에게 제시할 티켓은 TGT와 응용서버의 공유 비밀키로 암호화되어 있다.

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

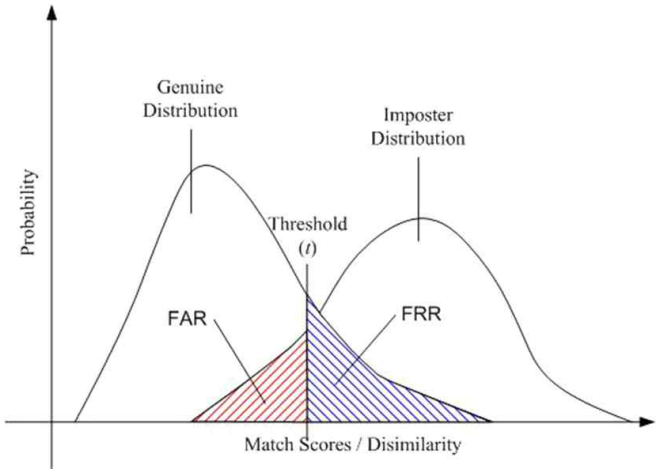


ㄱ. 타인을 본인으로 오인하는 허위일치의 비율(false match rate, false acceptance rate)이 본인을 인식하지 못하고 거부하는 허위불일치의 비율(false non-match rate, false rejection rate)보다 크다. ㄴ. 한계치를 우측으로 이동시키면 보안성은 강화되지만 사용자 편리성은 저하된다. ㄷ. 보안성이 높은 응용 프로그램은 낮은 허위일치비율을 요구한다. ㄹ. 가능한 용의자를 찾는 범죄학 응용 프로그램의 경우 낮은 허위일치비율이 요구된다.

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 체크 :
(1)
(ㄱ) : 한계치가 교차점에서 오른쪽으로 이동했기 때문에 FAR(타인을 본인으로 오인)이 FRR(본인을 인식하지 못하고 거부)보다 크다.
(ㄷ) : 보안성이 높은 응용프로그램은 낮은 FAR(타인을 본인으로 오인)을 요구한다.

오답 체크 :
(2), (3), (4)
(ㄴ) : 한계치를 우측으로 이동하면 FAR(타인을 본인으로 오인)은 커지고 FRR(본인을 인식하지 못하고 거부)은 작아진다. 즉, 보안성은 약화되고 사용자 편리성은 커진다.
(ㄹ) : 가능한 용의자를 찾는 범죄학 응용프로그램의 경우 높은 FAR(타인을 본인으로 오인)이 요구된다.
Tip! : 생체 인식 시스템의 FAR(False Acceptance Rate)과 FRR(False Rejection Rate)을 그림으로 표현하면 다음과 같다.


Genuine
Distribution
Imposter
Distribution
Probability
Threshold
(t)
FAR
FRR
Match Scores / Disimilarity