2016-국회직-정보보호론-가형-해설

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

1. 정보보호시스템이 제공하는 보안서비스 개념과 그에 대한 설명으로 옳은 것은?

ㄱ . 기밀성(Confidentiality) : 데이터가 위·변조 되지 않아야 함
ㄴ . 무결성(Integrity) : 권한이 있는 자는 서비스를 사용 하여야 함
ㄷ . 인증(Authentication) : 정당한 자임을 상대방에게 입증하여야 함
ㄹ . 부인방지(Nonrepudiation) : 거래사실을 부인할 수 없어야 함
ㅁ . 가용성(Availability) : 비 인가자에게는 메시지를 숨겨야 함

① ㄱ, ㄴ
② ㄱ, ㅁ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
⑤ ㄹ, ㅁ

해설)

정답 체크 :

(4)

ㄷ : 상대방의 신원을 확인시켜 준다. 사용자 인증(시스템 접근 통제)과 데이터 출처 인증(MAC)이 있다.

ㄹ : 송신부인방지(어떤 메시지가 송신되었을 때 수신자는 그 메시지가 실제로 송신자라고 주장하는 주체에 의해 송신되었음을 확인한다). 수신부인방지(어떤 메시지가 수신되었을 때 송신자는 그 메시지가 실제로 수신자라고 주장하는 주체에 의해 수신되었음을 확인한다).

오답 체크 :

(1), (2), (3), (5)

ㄱ : 비인가자에게는 메시지를 숨겨야 함

ㄴ : 데이터가 위·변조되지 않아야 함

ㅁ : 권한이 있는 자는 서비스를 사용하여야 함

2. 서버 관리자가 해커의 공격이 발생하고 있음을 감지하고 tcpdump 프로그램으로 네트워크 패킷을 캡처하였다. 다음의 요약된 캡처 정보가 나타내는 공격으로 옳은 것은?

```
13:07:13. 639870 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 670484 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 685593 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 693481 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 712833 192.168.1.73.2321 > 192.168.1.73.http ...
```

① Smudge 공격
② LAND 공격
③ Ping of Death 공격
④ Smurf 공격

⑤ Port Scan 공격
해설)
정답 체크 :
tcpdump(명령 줄에서 실행하는 일반적인 패킷 가로채기 소프트웨어)의 출력을 분석하면 다음과 같다.
13:07:13.639870 // 패킷 수집 시간을 나타낸다.
192.168.1.73.2321 > 192.168.1.73.http // 출발지 IP.포트번호 > 목적지 IP.포트번호(또는 서비스 이름), 포트번호가 /etc/services 파일에 등록이 되어 있는 경우라면 서비스 이름으로 표시된다.
(2) tcpdump를 분석하면 출발지 IP와 목적지 IP가 같음을 알 수 있고, Land 공격은 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소를 똑같이 만들어서 공격 대상에게 보내는 공격이므로 해당 문제의 답임을 알 수 있다.
오답 체크 :
(1) 스마트폰 혹은 태블릿 PC의 터치스크린에 묻어 있는 손가락의 자국(얼룩)을 이용해서 패스워드를 알아내는 수법이다. 일반적으로 자주 사용하는 패스워드에만 자국이 집중적으로 묻어 있을 것이기 때문에 해당 수법으로 공격하는 것이 가능하다.
(3) 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
(4) 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부(DDoS) 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.
(5) 공격을 수행하기 위한 전단계로 포트를 스캔하다. 포트 스캔이란 공격 대상의 컴퓨터에서는 어떤 포트들이 열려있는지 확인하는 작업이다. 포트 스캔 후에 열려져 있는 포트를 대상으로 공격을 수행한다.
Tip! : 네트워크 장비에서 패킷을 분석할 때 사용하는 굉장히 유명한 툴이다. 일반적으로 리눅스에서 사용되나, 윈도우 버전도 존재한다. 해당 내용을 외우지 말고 설치 후 꼭 한번 사용해보자.

3. 메시지 인증 코드와 전자서명에 대한 설명으로 옳은 것은?
① 전자서명은 대칭키가 사전에 교환 되어야 사용 할 수 있다.
② 메시지 인증 코드와 전자서명 모두 무결성과 부인 방지 기능을 제공 한다.
③ 전자서명은 서명 생성자를 인증하는 기능이 있다.
④ 메시지 인증 코드 값을 검증 하는데 공개키가 필요하다.
⑤ 전자서명은 서명-후-해시(Sign-then-Hash) 방식이다.
해설)
정답 체크 :
(3) 전자서명은 개인키를 이용하여 서명하므로 서명 생성자를 인증할 수 있다. 즉, 해당 개인

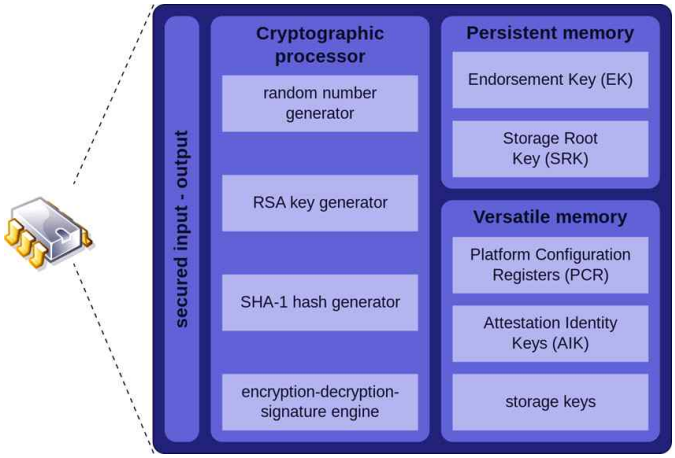
키는 서명 생성자만이 소유하고 있다.
오답 체크 :
(1) 전자서명은 공개키를 사용한다.
(2) 메시지 인증 코드는 인증/무결성 기능을 제공하고, 전자서명은 인증/무결성/부인방지 기능을 제공한다.
(4) 메시지 인증 코드는 대칭키(비밀키)가 필요하다.
(5) 전자서명은 해시-후-서명(Hash-then-Sign) 방식이다.

4. 아래 그림은 TLS(Transport Layer Security)를 통해 쇼핑몰에 로그인하는 화면이다. 이에 대한 설명으로 옳지 않은 것은?

① TLS는 현재 1.1 버전까지 발표되었다.
② TLS는 SSL을 기반으로한 IETF 인터넷 표준이다.
③ 서버 인증서를 통해 서버를 인증하고 키 교환을 한다.
④ 상호 교환된 키로 사용자의 패스워드는 암호화 된다.
⑤ 주소 창에 있는 자물쇠를 클릭하면 서버 인증서를 볼 수 있다.
해설)
정답 체크 :
(1) 현재 1.3버전까지 발표되었다.
오답 체크 :
(2) SSL 3.0을 기초로 해서 IETF가 만든 프로토콜이다. 1999년에 RFC2246으로서 발표된 TLS 1.0은 SSL 3.1이다.
(3) 인증서를 통해 서버와 클라이언트가 상호 인증하고 키교환을 한다.
(4) 상호 교환된 키는 데이터(패스워드와 같은 데이터)를 암호화하는데 사용된다.
(5) 자물쇠를 클릭하면 인증서에 대한 상세 정보(버전, 일련 번호, 서명 알고리즘 등)를 알 수 있다.

5. TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은?
① 하드웨어 기반으로 안전한 저장 공간과 실행영역을 제공한다.
② 난수발생기, 암·복호화 엔진, RSA 키 생성기 등을 포함한다.
③ 비휘발성 메모리 영역에 최상위 루트키가 탑재된 다.
④ 단계적으로 인증된 절차로 운영체제가 부팅되도록 한다.
⑤ 국내 공인인증서 저장시 서명키를 저장하는 표준방식이다.
해설)
정답 체크 :
(5) 공인인증서가 저장되는 것은 맞지만 공인인증서를 서명한 개인키(서명키)는 저장되지 않는다.

오답 체크 :
TPM은 그림으로 나타내면 다음과 같다.



(1) 암호화된 키, 패스워드, 디지털 인증서 등을 저장하는 안전한 저장 공간을 제공하는 보안 모듈이다.
(2) 그림에서 보는 바와 같이 random number generator(난수발생기), encryption-decryption signature engine(암·복호화 엔진), RSA key generator(RSA 키 생성기) 등을 포함한다.
(3) 그림에서 보는 바와 같이 persistent memory(비휘발성 메모리)에 storage root key(최상위 루트 키)가 탑재된다.
(4) 일반적으로 개인용 컴퓨터(PC) 주기판에 부착되며, 부팅 단계에서부터 시스템의 무결성 검증에 이용된다.

6. CPU의 NX(No-Execute) 비트 기술을 활용하여 효과적으로 차단할 수 있는 공격 유형으로 옳은 것은?
① Cross-Site Scripting 공격
② Denial of Service 공격
③ ARP Spoofing 공격
④ SQL Injection 공격
⑤ Buffer Overflow 공격
해설)
정답 체크 :
(5) 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드(eggshell)가 실행된다. NX 비트 기술을 이용하면 스택에서 프로그램(eggshell)을 실행할 수 없게 하여 버퍼 오버플로우 문제를 해결할 수 있다.
오답 체크 :
(1) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자

동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다. 사용자의 입력 값 등을 검사해서 방어한다.
(2) DoS(서버를 서비스 거부 상태로 만듦)의 공격 유형에는 취약점 공격형과 자원 고갈형이 존재한다. 취약점 공격형은 teardrop, land attack이 해당되고, 자원 고갈형은 flooding 공격이 해당된다. 네트워크 보안 장비(방화벽 등)에서 land attack을 차단할 수 있고, flooding은 ratio를 조정해서 차단할 수 있다(초당 100개 이상의 패킷은 받지 않는다).
(3) 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다. 상대방의 MAC을 고정해서 방어한다.
(4) 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다. 사용자의 입력 값 등을 검사해서 방어한다.

7. IPsec에 대한 설명으로 옳지 않은 것은?
① IPsec 정책 설정 과정에서 송·수신자의 IP 주소를 입력한다.
② AH(Authentication Header) 프로토콜은 무결성을 제공한다.
③ 트랜스포트(Transport) 모드에서는 IP 헤더도 암호화된다.
④ 재전송 공격을 막기 위해 IP 패킷별로 순서번호를 부여한다.
⑤ IKE(Internet Key Exchange) 프로토콜로 세션키를 교환한다.
해설)
정답 체크 :
(3) 터널 모드에서는 IP헤더도 암호화되지만, 트랜스포트(전송) 모드에서는 IP헤더가 암호화되지 않는다. 트랜스포트 모드는 네트워크(IP) 계층 상위 계층인 전송(port), 응용(payload) 계층의 데이터에 대한 보호를 목적으로 하며, IP 패킷의 원본(payload)에 필드를 추가함으로서 구현되기 때문이다.
오답 체크 :
(1) IPSec 정책(policy)은 어떤 IP 트래픽을 보호하고, 어떤 IP 트래픽을 보호하지 않을 것인지를 결정하는 것이다. 이때 IP 필터를 사용하는데 해당 필터에 송수신지 IP가 들어가게 된다.
(2) AH는 인증과 무결성을 제공한다.
(4) AH, ESP에서 순서번호(sequence number)를 이용해서 재전송 공격을 막는다.
(5) 인터넷 표준 암호키 교환 프로토콜이다. 송신 측에서 수신 측이 생성한 암호키(세션키)를 상대방에게 안전하게 송신하기 위한 방법이다.

8. 정보통신망 이용촉진 및 정보보호 등에 관한 법률이 규정하는 정보보호 관리체계의 인증권자와 개인정보보호 관리체계의 인증권자를 순서대로 나열한 것으로 옳은 것은?
① 미래창조과학부장관, 방송통신위원회
② 미래창조과학부장관, 한국인터넷진흥원
③ 방송통신위원회, 방송통신위원회

④ 방송통신위원회, 한국인터넷진흥원
⑤ 한국인터넷진흥원, 한국인터넷진흥원
해설)
정답 체크 :
(1) 해당 문제처럼 년도에 따라 답이 바뀔 수 있는 것은 매년 해당 답의 갱신 여부를 체크해 보아야 한다. 일단 현재(2019년도)를 기점으로 ISMS의 인증권자는 “과학기술정보통신부”이고, PIMS의 인증권자는 “행정안전부”와 “방송통신위원회”이다. 그리고 ISMS와 PIMS는 ISMS-P로 통합되었다. 인증기관인 “한국인터넷진흥원(KISA)”이다.

9. 해커가 리눅스 서버에 침입 후 백도어를 설치하였다. 백도어와 연관된 포트가 열려 있는지 확인하기 위해 사용할 수 있는 프로그램으로 옳은 것은?
① ps
② nmap
③ nslookup
④ traceroute
⑤ ping
해설)
정답 체크 :
(2) 가장 대표적인 포트 또는 IP 스캔 프로그램으로서 로컬 및 네트워크 시스템에 대한 스캔을 통해 자신이 관리하는 시스템에 자신도 알지 못하는 포트가 열려 있는지를 확인할 수 있는 도구다.
오답 체크 :
(1) 대부분의 유닉스 계통 운영 체제에서 현재 실행되고 있는 프로세스들을 표시한다(process status).
(3) 인터넷 서버 관리자나 사용자가 호스트 이름을 입력하면 그 IP 주소를 알려 주는 프로그램이고, 그 반대의 경우에도 가능하다.
(4) 리눅스에서 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답속도를 표시해 준다. 윈도우에서는 tracert를 사용한다.
(5) IP 네트워크를 통해 특정한 호스트가 도달할 수 있는지의 여부를 테스트하는 데 쓰이는 컴퓨터 네트워크 도구의 하나이다.

10. 암호학적 해시함수에 대한 설명으로 옳지 않은 것은?
① MD5나 SHA-1은 취약점이 발견되어 더 이상 사용하지 않는 것이 바람직하다.
② 해시함수는 출력값에 대응하는 입력값을 구하기 어렵다.
③ 해시함수의 내부 알고리즘에 관계없이 충돌저항성을 분석하는 방법으로 생일 공격(Birthday Attack)이 있다.
④ 패스워드와 난수를 해시한 값을 전송할 때, 난수가 노출되어도 사전 공격(Dictionary Attack)에 안전하다.
⑤ 최근에는 가상화폐인 비트 코인(Bitcoin)을 채굴하는 알고리즘에 사용된다.
해설)
정답 체크 :

(4) 난수는 salt이고 사전공격을 막는데 사용한다. 그러므로 난수가 노출되면 사전공격에 안전하지 않다.
오답 체크 :
(1) MD5는 내부 구조 일부에 대한 몇 가지 공격 방법이 발견되었고, SHA-1은 강한 충돌 내성(출력이 같은 서로 다른 입력이 존재)이 침해되었다.
(2) 해시의 일방향성을 의미한다.
(3) 생일 공격(Birth Day)이란 어떤 모임에서 사람이 수가 증가할수록 생일이 같을 확률이 증가함을 의미한다. 그러므로 해시의 입력값을 증가하면 같은 출력값을 가지는 입력값을 가지는 확률이 증가하게 된다. 해당 방법은 내부 알고리즘에 관계없이 충돌저항성(같은 출력을 같은 입력을 찾는 것)을 분석할 수 있다.
(5) 비트코인에 SHA-255과 RIPEMD-160이 사용된다.
Tip! : 비트코인(최근 출제 경향)에 사용하는 해시 함수(SHA-256, RIPEMD-160)는 중요하므로 꼭 기억하기 바란다.

11. 공개키 암호와 대칭키 암호에 대한 설명으로 옳은 것은?
① 공개키를 교환하기 위해 대칭키 암호를 이용한다.
② 128비트 RSA 공개키와 2048비트 대칭키는 안전도가 비슷하다.
③ 두 암호 모두 기밀성과 무결성을 동시에 보장한다.
④ 긴 메시지 암호화에는 하이브리드 방식의 암호가 효율적이다.
⑤ 공개키 암호는 대칭키 암호에 비해 처리속도가 빠르다.
해설)
정답 체크 :
(4) 긴 메시지는 속도가 빠른 대칭키로 암호화하고, 대칭키는 속도가 느린 공개키로 암호화한다.
오답 체크 :
(1) 대칭키 암호를 교환하기 위해 공개키를 이용한다.
(2) 128비트 대칭키와 2048비트 공개키는 안전도가 비슷하다.
(3) 기밀성과 무결성을 동시에 보장하지 않는다. 예를 들어, 대칭키를 이용해서 암호화를 수행하면 기밀성을 보장하고, 대칭키를 이용해서 MAC(메시지 인증 코드)을 하면 인증과 무결성을 보장한다. 동시에 보장하려면 암호화와 MAC을 동시에 수행하여야 한다.
(5) 공개키 암호는 수학적 계산으로 인해 대칭키 암호에 비해 처리속도가 느리다.
Tip! : 기밀성과 무결성을 동시에 보장하지 않는다는 지문은 정말 중요한 지문으로 꼭 기억해두는 것이 좋다. 그리고 구체적인 숫자는 외우지 못하더라도 비슷한 안전도를 구현하기 위해 대칭키의 비트수가 더 작다는 것에 유념하기 바란다.

12. 사용자 인증 방식에 대한 설명으로 옳지 않은 것은?
① 패스워드 인증은 서버 측에서 인증 시스템 구축이 용이하다는 장점 이 있다.
② 시각 동기화 OTP(One Time Password)는 두 사용자가 사전에 대칭키를 공유해야 한다.
③ 전자서명 방식은 도전-응답(Challenge-Response) 프로토콜과 결합하여 사용자를 인증한다.
④ 생체인증은 생체 정보를 인식할 때 마다 발생할 수 있는 에러 처리가 중요하다.

⑤ I-PIN은 주민등록번호 대신 사용할 수 있는 일회용 사용자 식별번호이다.
해설)
정답 체크 :
(5) I-PIN(인터넷 가상 주민등록번호)은 주민등록번호 대신 사용할 수는 있지만 일회용은 아니다.
오답 체크 :
(1) 패스워드 인증 방식은 보편화된 인증 방식(데이터베이스)으로 인증시스템 구축이 용이하다.
(2) 시각 동기화 OTP에서는 서로 동기화한 시각을 대칭키로 암호화해서 보낸다.
(3) 전자서명을 이용한 도전-응답 프로토콜의 동작 과정은 다음과 같다. 처음에 사용자가 서버에게 자신이 인증 받기를 원한다고 요청한다. 두 번째는 서버가 도전(challenge)를 생성해서 사용자에게 보낸다. 세 번째는 사용자가 도전(challenge)에 사용자의 개인키로 서명해서 서버에게 응답(response)을 보낸다. 마지막 네 번째는 서버가 사용자의 공개키로 응답(response)을 검증하고 사용자의 접근을 허락한다.
(4) 생체인식은 아직까지는 오인식률이 높기 때문에 이를 처리하는 것이 중요하다. 예를 들어, 지문 인식은 지문에 물만 묻어도 잘 인식되지 않는다.

13. DNS(Domain Name System)의 보안 위협과 DNSSEC(Domain Name System Security Extensions) 대응에 대한 설명으로 옳지 않은 것은?
① Cache Poisoning 공격은 DNS 캐시에 저장된 정보를 오염시켜 공격자가 지정한 주소로 유도한다.
② DNS Spoofing은 서버에서 응답하는 IP 주소를 변조하여 의도하지 않은 주소로 유도한다.
③ DNSSEC는 서버의 응답에 전자서명을 부가함으로써 서버 인증 및 무결성을 제공 한다.
④ DNSSEC는 인증 체인 형태로 확장되어 계층적 구조의 DNS 서버에도 적용될 수 있다.
⑤ DNSSEC는 서버의 응답을 숨기지는 않지만, 서비스 거부 공격을 막는 효과가 있다.
해설)
정답 체크 :
(5) DNSSEC은 cache poisoning은 막을 수 있지만, 피싱, DoS(DDoS) 등은 막을 수 없다.
오답 체크 :
(1) DNS의 캐시의 데이터를 조작해서 공격자가 원하는 주소로 가게끔 하는 것이다.
(2) 실제 DNS보다 가짜 DNS가 먼저 응답하여 공격자가 원하는 주소로 가게끔 하는 것이다.
(3) DNS 서버가 응답에 서명을 해서 보내면 사용자는 검증을 함으로써 인증과 무결성을 보장한다.
(4) 계층적 구조의 DNS 서버에서 서로 간에 전자서명을 이용해서 인증과 무결성을 보장한다.

14. TCSEC(Trusted Computer System Evaluation Criteria)에 따라 보안 등급을 평가할 때 보안 수준이 높은 순서대로 나열한 것으로 옳은 것은?
① Structured Protection > Labeled Security Protection > Controlled Access Protection
② Discretionary Security Protection > Controlled Access Protection > Minimal Protection

③ Minimal Protection > Structured Protection > Labeled Security Protection
④ Discretionary Security Protection > Labeled Security Protection > Minimal Protection
⑤ Controlled Access Protection > Discretionary Security Protection > Structured Protection
해설)
정답 체크 :
(1) TCSEC에서 보안 수준이 높은 순서대로 나열하면 다음과 같다.
A1(Verified Design) > B3(Security Domains) > B2(Structured Protection) > B1(Labeled Security) > C2(Controlled Access Protection) > C1(Discretionary Security Protection) > D(Minimal Protection)
Tip! : 다른 보안 등급에서는 비슷한 용어를 사용하므로 중요 용어(structured, labeled, controlled, discretionary)들을 기억해두는 것이 좋다.

15. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?
① 이메일 보안이나 파일 암호화에 사용된 다.
② 공개키 인증을 위해 PGP 인증서를 사용한다.
③ 자신의 공개키를 전달하는 데 인증기관의 서명이 필요하다.
④ 이메일에 서명 할 때, 서명자의 패스워드를 요구한다.
⑤ 이메일 관리 프로그램에 플러그인도 가능하다.
해설)
정답 체크 :
(3) 공개키를 전달할 때 인증기관이 없는 사용자들끼리의 신뢰망(web of trust)를 사용한다. 즉, 인증기관이 공개키를 인증하는 것이 아니라 사용자간의 서로의 신뢰도를 이용해서 공개키를 인증한다.
오답 체크 :
(1) 처음에 파일 암호화 규격으로 개발되었고, 이후 이메일 보안에 적용되었다.
(2) PGP에서는 OpenPGP에서 정해진 형식의 인증서와 X.509 호환용 인증서를 사용한다.
(4) 암호화되어 있는 개인키(서명을 위해 필요한 키)를 복호화하는데 필요한 키를 만들기 위해 사용자의 패스워드(패스 프레이즈)가 사용된다.
(5) 워드프레스(wordpress) 등에서 사용할 수 있는 플러그인(기존 소프트웨어에 별도로 장착해서 사용할 수 있는 소프트웨어 모듈)이 존재한다.

16. 자원의 접근 제어 방법 중 강제적 접근 제어(Mandatory Access Control)에 해당하는 것으로 옳은 것은?
① 자원마다 보안 등급이 부여 된 다.
② 사용자별로 접근 권리를 이전할 수 있다.
③ UNIX 운영체제의 기본 접근 제어 방식 이다.
④ 조직의 역할에 따라 접근 권한을 부여하는 방식 이다.
⑤ 자원의 소유자가 자원에 대한 접근 권한을 설정한다.
해설)

정답 체크 :
(1) 자원마다 보안등급이 부여되고, 보안등급을 비교함으로써 접근 허용 여부를 결정한다.
오답 체크 :
(2) ACL에 해당된다.
(3) DAC에 해당된다.
(4) RBAC에 해당된다.
(5) DAC에 해당된다.

17. 다음 용어에 대한 설명으로 옳지 않은 것은?
① Rootkit : 시스템 침입 후의 공격을 도와주는 프로그램들의 집합
② Obfuscation : 코드를 분석하기 어렵도록 변조하는 행위
③ Ransomware : 복호화를 조건으로 금전을 요구하기 위해 피해자의 데이터를 암호화하는 악성코드
④ Cross-Site Scripting: 웹 애플리케이션의 데이터를 악성 스크립트 코드로 변조하는 공격
⑤ Sandbox: 악성코드가 시스템 자원에 쉽게 접근하도록 만든 백도어
해설)
정답 체크 :
(5) 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태이다. iOS의 경우 앱에 대한 샌드박스를 제공해 다른 앱과의 통신을 통제하고 있다.
오답 체크 :
(1) 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입을 위한 백도어, 트로이목마 설치, 원격 접근, 내부 사용 흔적 삭제, 관리자 권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램의 모음이다.
(2) 프로그래밍 언어로 작성된 코드에 대해 읽기 어렵게 만드는 작업이다(쓰레기 코드를 집어넣거나 코드의 순서를 바꿈). 대표적인 사용 예로는 프로그램에서 사용된 아이디어나 알고리즘 등을 숨기는 것 등이 있다.
(3) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.
(4) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

18. 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 정한 개인 정보의 보호 조치로 옳지 않은 것은?
① 개인정보를 안전하게 저 장할 수 있는 암호화 기술 등을 이용
② 개인정보에 대한 불법적인 접근을 차단하기 위한 접근 통제 장치의 설치

③ 접속기록의 변조 방지를 위한 조치
④ 개인정보를 안전하게 취급하기 위한 내부관리계획의 공개
⑤ 컴퓨터 바이러스에 의한 침해 방지 조치
해설)
정답 체크 :
(4) “정보통신망법” 제28조(개인정보의 보호조치) 상 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립ㆍ시행은 맞지만 공개는 보호조치에 해당되지 않는다.
오답 체크 :
(1), (2), (3), (5) “정보통신망법” 제28조(개인정보의 보호조치) 상 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실ㆍ도난ㆍ유출ㆍ위조ㆍ변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적ㆍ관리적 조치를 하여야 한다. 1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립ㆍ시행, 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치ㆍ운영, 3. 접속기록의 위조ㆍ변조 방지를 위한 조치, 4. 개인정보를 안전하게 저장ㆍ전송할 수 있는 암호화기술 등을 이용한 보안조치, 5. 백신 소프트웨어의 설치ㆍ운영 등 컴퓨터바이러스에 의한 침해 방지조치, 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

19. 국내 정보보호 관리체계(ISMS) 인증에 관한 평가 기준 중 시스템 개발 보안에 대한 통제사항으로 옳지 않은 것은?
① 정보시스템 설계시 사용자 인증에 관한 보안 요구사항을 고려하여야 한다.
② 알려진 기술적 보안 취약성에 대한 노출 여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.
③ 소스 프로그램은 운영 환경에 보관하는 것을 원칙으로 하고, 인가된 사용자만 소스 프로그램에 접근하여야 한다.
④ 개발 및 시험 시스템은 운영 시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.
⑤ 운영 환경으로의 이관은 통제된 절차에 따라 이루어져야 하고, 실행 코드는 시험과 사용자 인수 후 실행하여야 한다.
해설)
정답 체크 :
(3) 소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하며, 소스 프로그램 관리자는 각 운영시스템 별로 지정하여야 한다. 또한 소스 프로그램 접근에 대한 통제절차를 수립하고 이행하여야 한다.
오답 체크 :
(1) 응용시스템 설계시 반드시 사용자 인증에 대한 보안 요구사항을 고려하여야 한다. 중요한 메시지의 경우 무결성이 요구될 때 메시지 인증기법을 적용하고 비밀성이 요구될 시 암호화를 적용하여야 한다.
(2) 보안사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경을 하여야 한다.

(4) 원칙적으로 개발, 시험, 운영 환경을 분리하여야 한다. 또한 응용프로그램을 개발환경으로부터 운영환경으로 이전하는 절차를 저의하고 문서화하여야 한다.
(5) 운영 프로그램의 수정은 적절한 권한을 지닌 사람만이 시행하여야 하고, 운영시스템은 실행코드만 보유하여야 한다. 실행코드는 성공적인 시험과 사용자 인수 후에 실행하여야 한다.

20. ISO/IEC 17799와 같은 정보보호 관리체계 표준에서 나열된 보안 통제 사항들을 근거로 시스템에 대한 보안 위험을 분석하는 방법으로 옳은 것은?
① 비정형화된 접근법(Informal Approach)
② 기준 접근법(Baseline Approach)
③ 상세위험 분석 (Detailed Risk Analysis)
④ 통합 접근법(Combined Approach)
⑤ 시나리오 접근법(Scenario Approach)
해설)
정답 체크 :
(2) 보안 통제사항들은 체크리스트(정보보호대책)를 의미하므로 기준 접근법에 해당된다.
오답 체크 :
(1) 모든 정보자산에 기업이외의 전문가 지식 및 경험을 활용하는 방법이다.
(3) 모든 정보자산에 대해 상세 위험 분석(자산가치, 위협, 취약점의 평가에 기초한 위험을 산정)을 하는 방법이다.
(4) 기준선 접근법과 상세 위험 분석 접근법을 조합하여 분석하는 방법이다.
(5) 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여, 일정 조건 하에서 위협에 대한 발생 가능한 결과들을 추정(시나리오)하는 방법이다.