2020-지방직-정보보호론-B형-해설-곽후근

1. 전자 서명(digital signature) 보안 메커니즘이 제공하는 보안 서비스가 아닌 것은?
① 근원 인증
② 메시지 기밀성
③ 메시지 무결성
④ 부인 방지
정답 체크 :
(2) 전자 서명은 기밀성을 제공하지 않는다. 기밀성을 제공하기 위해서는 별도의 암호화를 수행해야 한다.
오답 체크 :
(1) 전자 서명은 서명자 인증을 제공한다.
(3) 전자 서명은 무결성을 제공한다.
(4) 전자 서명은 부인 방지를 제공한다.

2. AES(Advanced Encryption Standard)에 대한 설명으로 옳은 것은?
① DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘이다.
② Feistel 구조로 구성된다.
③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.
④ 2001년에 국제표준화기구인 IEEE가 공표하였다.
정답 체크 :
(1) DES의 약한 보안을 대체하기 위해 만들어진 새로운 표준이다.
오답 체크 :
(2) SPN 구조로 구성된다.
(3) AES의 평가 기준은 안전성(선형/차분 공격), 비용(속도 및 메모리 요구량), 알고리즘 및 구현 특성(유연성과 단순성)이다. 그러므로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 만들어진 알고리즘은 AES 후보에서 제외되었다.
(4) 2001년에 NIST(미국 표준 기술 연구소)가 공표하였다.

3. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?
① 호스트 기반 IDS와 네트워크 기반 IDS로 구분한다.
② 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단한다.
③ 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.
④ IDS는 방화벽처럼 내부와 외부 네트워크 경계에 위치해야 한다.
정답 체크 :
(4) 네트워크 기반 IDS는 내부와 외부 네트워크 경계에 위치하나, 호스트 기반 IDS는 내부 네트워크 안의 호스트에 위치한다.
오답 체크 :
(1) 호스트, 네트워크 그리고 하이브리드로 구분한다.
(2) 오용 탐지는 오용을 탐지하기 위해 패턴 또는 지식 정보(실행 절차 및 특징 정보)를 이용한다.
(3) 비정상 행위 탐지는 비정상 행위를 탐지하기 위해 프로파일이나 통계적 임계치, 인공지능 등을 이용한다.

4. RSA 암호 알고리즘에서 두 소수, p = 17, q = 23과 키 값 e = 3을 선택한 경우, 평문 m = 8에 대한 암호문 c로 옳은 것은?

① 121

② 160

③ 391

④ 512

정답 체크 :

(1) n = p x q = 17 x 23 = 391

$8^e \bmod n = 8^3 \bmod 391 = 512 \bmod 391 = 121$

5. IEEE 802.11i RSN(Robust Security Network)에 대한 설명으로 옳은 것은?

① TKIP는 확장형 인증 프레임워크이다.

② CCMP는 데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드로 이용한다.

③ EAP는 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용한다.

④ 802.1X는 무결성 보장을 위해 CBC—MAC를 이용한다.

정답 체크 :

(2) CCMP는 데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드를 사용하고, 무결성 보장을 위해 CBC-MAC을 이용한다.

오답 체크 :

(1) 해당 설명은 EAP이고, TKIP는 데이터 기밀성을 보장한다.

(3) EAP는 WPA2-Enterprise에서 인증을 위해 사용한다.

(4) 해당 설명은 CCMP이고, 802.1x는 WAP2-Enterprise에서 별도의 인증 서버를 사용한다.

6. CC(Common Criteria) 인증 평가 단계를 순서대로 바르게 나열한 것은?

가. PP(Protection Profile) 평가
나. ST(Security Target) 평가
다. TOE(Target Of Evaluation) 평가

① 가→나→다

② 가→다→나

③ 나→가→다

④ 다→나→가

정답 체크 :

(1) PP(Protection Profile) : 사용자 또는 개발자의 요구사항을 정의한다(전체 제품). 기술적인 구현 가능성을 고려하지 않는다.

ST(Security Target) : 개발자가 작성하며 제품 평가를 위한 상세 기능을 정의한다(개별 제품). 기술적 구현 가능성을 고려한다.

TOE : 획득하고자 하는 보안 수준을 의미한다(EAL)

7. SQL 삽입 공격에 대한 설명으로 옳지 않은 것은?

① 사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생한

다.
② 공격이 성공하면 데이터베이스에 무단 접근하여 자료를 유출하거나 변조시키는 결과가 초래될 수 있다.
③ 사용자의 입력값으로 웹 사이트의 SQL 질의가 완성되는 약점을 이용한 것이다.
④ 자바스크립트와 같은 CSS(Client Side Script) 기반 언어로 사용자 입력을 필터링하는 방법으로 공격에 대응하는 것이 바람직하다.
정답 체크 :
(4) 클라이언트와 서버 양측에서 입력값에 대해 안전한 값만 사용될 수 있도록 검증작업을 수행한다.
오답 체크 :
(1) 데이터베이스에 요청하는 query를 true로 만든다.
(2) 공격이 성공하면 계정이 뚫리게 되므로 데이터베이스에 무단 접근이 가능하다.
(3) SQL 질의 중에 select를 사용한다.

8. 유닉스/리눅스의 파일 접근 제어에 대한 설명으로 옳지 않은 것은?
① 접근 권한 유형으로 읽기, 쓰기, 실행이 있다.
② 파일에 대한 접근 권한은 소유자, 그룹, 다른 모든 사용자에 대해 각각 지정할 수 있다.
③ 파일 접근 권한 변경은 파일에 대한 쓰기 권한이 있으면 가능하다.
④ SetUID가 설정된 파일은 실행 시간 동안 그 파일의 소유자의 권한으로 실행된다.
정답 체크 :
(3) 파일 접근 권한 변경은 파일 소유자나 슈퍼 유저만 가능하다(chmod 명령을 사용).
오답 체크 :
(1) 접근 권한 유형은 rwx이다.
(2) 접근 권한은 소유자, 그룹, 다른 사용자에 대해 개별적으로 지정할 수 있다.
(4) SetUID를 사용하면 effective UID가 그 파일의 소유자 권한으로 바뀐다.

9. IPSec에 대한 설명으로 옳지 않은 것은?
① 전송(transport) 모드에서는 전송 계층에서 온 데이터만을 보호하고 IP 헤더는 보호하지 않는다.
② 인증 헤더(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.
③ 보안상 안전한 채널을 만들기 위한 보안 연관(Security Association)은 양방향으로 통신하는 호스트 쌍에 하나만 존재한다.
④ 일반적으로 호스트는 보안 연관 매개변수들을 보안 연관 데이터베이스에 저장하여 사용한다.
정답 체크 :
(3) SA는 양방향으로 통신하는 호스트 쌍에 여러개가 존재한다.
오답 체크 :
(1) 전송 모드는 기존 패킷에 적용하므로 IP 헤더는 보호하지 않는다.
(2) AH는 인증과 무결성을 제공한다.
(4) 일반적으로 SA를 위해 SPI를 사용한다.

10.「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 명시된 것으로 옳지 않은 것은?
① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야

한다.
② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
③ 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.
④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기할 수 있다.
정답 체크 :
(4) 제27조(이용자 정보의 보호) ③ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.
오답 체크 :
(1) 제25조(침해사고 등의 통지 등) ② 클라우드컴퓨팅서비스 제공자는 제1항제2호(이용자 정보가 유출된 때)에 해당하는 경우에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.
(2) 제26조(이용자 보호 등을 위한 정보 공개) ① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
(3) 제27조(이용자 정보의 보호) ① 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.

11. 인증기관이 사용자의 공개키에 대한 인증을 수행하기 위해 X.509 형식의 인증서를 생성할 때 서명에 사용하는 키는?
① 인증기관의 공개키
② 인증기관의 개인키
③ 사용자의 개인키
④ 인증기관과 사용자 간의 세션키
정답 체크 :
(2) 인증서를 생성할 때 서명에 사용하는 키는 인증기관의 개인키이다.

12. 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?
① 메시지는 대칭 암호 방식으로 암호화한다.
② 일반적으로 대칭 암호에 사용하는 세션키는 의사 난수 생성기로 생성한다.
③ 생성된 세션키는 무결성 보장을 위하여 공개키 암호 방식으로 암호화한다.
④ 메시지 송신자와 수신자가 사전에 공유하고 있는 비밀키가 없어도 사용할 수 있다.
정답 체크 :
(3) 생성된 세션키는 기밀성 보장을 위하여 공개키 암호 방식으로 암호화한다.
오답 체크 :
(1) 메시지는 속도를 위해 대칭 암호 방식으로 암호화한다.
(2) 세션키는 의사 난수 생성기(소프트웨어)로 생성한다.

(4) 세션키를 공개키로 암호화하기 때문에 비밀키를 사전에 공유할 필요가 없다.

13. 해시함수의 충돌저항성을 위협하는 공격 방법은?
① 생일 공격
② 사전 공격
③ 레인보우 테이블 공격
④ 선택 평문 공격
정답 체크 :
(1) 입력의 개수를 늘리면 충돌이 발생하는 원리를 이용하는 해시함수 공격 방법이다.
오답 체크 :
(2) 사전 공격 : 사전 파일을 이용하여 패스워드를 크래킹한다.
(3) 레인보우 테이블 공격 : 패스워드의 해시값과 reduction 함수를 사용하여 패스워드를 크래킹한다.
(4) 선택 평문 공격 : 암호화기를 사용할 수 있다는 가정하에 블록 암호문을 해독하기 위해 공격한다.

14. 블록 암호 운용 모드에 대한 설명으로 옳지 않은 것은?
① CFB는 블록 암호화를 병렬로 처리할 수 없다.
② ECB는 IV(Initialization Vector)를 사용하지 않는다.
③ CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록만 영향을 받는다.
④ CTR는 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.
정답 체크 :
(3) CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록과 다음 블록에 영향을 받는다(에러 전파).
오답 체크 :
(1) CFB는 암호화를 병렬 처리할 수 없고, 복호화를 병렬 처리할 수 있다.
(2) ECB는 블록을 개별적으로 처리하는 구조이므로 IV를 사용하지 않는다.
(4) CTR은 블록마다 서로 다른 카운터 값(+1)을 사용한다.

15. 「개인정보 보호법」상 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은?
① 범죄의 예방 및 수사를 위하여 필요한 경우
② 공공기관의 장이 허가한 경우
③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
④ 시설안전 및 화재 예방을 위하여 필요한 경우
정답 체크 :
(2) 제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

16. SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는 데 악용될 수 있는

명령어는?
① HELO
② MAIL FROM
③ RCPT TO
④ VRFY
정답 체크 :
(4) VRFY : 수신자의 주소를 조회하려고 사용한다.
오답 체크 :
(1) HELO : SMTP 세션을 시작하며, 송신자의 호스트 이름을 전송하여 서버에 자신의 신분을 알려준다.
(2) MAIL FROM : 송신자의 메일 주소를 통지한다.
(3) RCPT TO : 수신자의 메일 주소를 통지한다.

17. 다음 법 조문의 출처는?

> 제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

① 국가정보화 기본법
② 개인정보 보호법
③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률
④ 정보통신산업진흥법
정답 체크 :
(3) 정보통신망법 : 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.
오답 체크 :
(1) 국가정보화 기본법 : 이 법은 국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정함으로써 지속가능한 지식정보사회의 실현에 이바지하고 국민의 삶의 질을 높이는 것을 목적으로 한다.
(2) 개인정보 보호법 : 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.
(4) 정보통신산업진흥법 : 이 법은 정보통신산업의 진흥을 위한 기반을 조성함으로써 정보통신산업의 경쟁력을 강화하고 국민경제의 발전에 이바지함을 목적으로 한다.

18. 위조된 출발지 주소에서 과도한 양의 TCP SYN 패킷을 공격 대상 시스템으로 전송하는 서비스 거부 공격에 대응하기 위한 방안의 하나인, SYN 쿠키 기법에 대한 설명으로 옳은 것은?
① SYN 패킷이 오면 세부 정보를 TCP 연결 테이블에 기록한다.
② 요청된 연결의 중요 정보를 암호화하고 이를 SYN—ACK 패킷의 응답(acknowledgment) 번호로 하여 클라이언트에게 전송한다.

③ 클라이언트가 SYN 쿠키가 포함된 ACK 패킷을 보내오면 서버는 세션을 다시 열고 통신을 시작한다.
④ TCP 연결 테이블에서 연결이 완성되지 않은 엔트리를 삭제하는 데까지의 대기 시간을 결정한다.
정답 체크 :
(3) ACK이 올 경우 쿠키값을 검증하여 제대로 된 값인 경우 연결을 형성한다.
오답 체크 :
(1) SYN 쿠키가 포함된 ACK 패킷을 보내오면 TCP 연결 테이블에 기록한다(메모리를 할당한다).
(2) 클라이언트에서 연결요청이 있을 경우 SYN-ACK 패킷에 특별한 쿠키값을 담아 보낸다.
(4) 연결이 완성되지 않은 엔트리는 TCP 연결 테이블에 존재하지 않는다. 그러므로 대기 시간을 결정할 필요가 없다.

19. ISO/IEC 27001:2013 보안관리 항목을 PDCA 모델에 적용할 때, 점검(check)에 해당하는 항목은?
① 성과평가(performance evaluation)
② 개선(improvement)
③ 운영(operation)
④ 지원(support)
정답 체크 :
(1) 성과 평가 : Check에 해당한다.
오답 체크 :
(2) 개선 : Act에 해당한다.
(3) 운영 : Do에 해당한다.
(4) 지원 : Plan에 해당한다.

20. 다음에서 설명하는 블록체인 합의 알고리즘은?

○ 비트코인에서 사용하는 방식이 채굴 경쟁으로 과도한 자원 소비를 발생 시킨다는 문제를 해결하기 위한 대안으로 등장하였다. ○ 채굴 성공 기회를 참여자에 따라 차등적으로 부여한다. ○ 다수결로 의사 결정을 해서 블록을 추가하는 방식이 아니므로 불특정 다수가 참여하는 환경에서 유효하다.

① Paxos
② PoW(Proof of Work)
③ PoS(Proof of Stake)
④ PBFT(Practical Byzantine Fault Tolerance)
정답 체크 :
(3) PoS : 지분증명이라 부르기도 하며 채굴기 없이 본인이 소유한 코인의 지분으로 채굴되는 방식이다. 해당 코인을 가지고 있는 소유자가 현재 보유하고 있는 자산(stake) 양에 비례하여 블록을 생성할 권한을 더 많이 부여되는 방식이다. 참여에 대한 보상은 이자와 같은 방식으로 코인이 지급되며, 일정 수 이상의 코인을 보관하고 있는 지갑을 블록체인 네트워크에 연결시켜놓기만 하면 보상을 받을 수 있다. 단점은 퀀텀의 51% 지분을 갖고 있는 A라는 사람이 데이터 업데이트의 권한을 쥐고 흔들 수 있다고 볼 수 있다. 따라서 맘에 안드는 사람 B의 자산을 A가 악의적으로 기록을 삭제하여 0원으로 만들 수도 있다. PoS를 사용하는 대표 코인에는 퀀텀, 네오, 스트라티스 등이 존재한다.
오답 체크 :

(1) Paxos : 신뢰할 수 없는 프로세서들의 네트워크 에서 합의 문제(분산 컴퓨팅과 다중 에이전트 시스템에서 프로세스들이 사용할 값을 하나로 결정하는 문제)를 해결하기 위한 프로토콜 그룹이다. 합의 문제는 구성원이나 구성원 간의 통신 매체에 장애가 발생할 수 있늘 경우 어려워진다.
(2) PoW : 작업증명으로 부르기도 하며 해시연산을 처리하는 하드웨어(GPU, ASIC채굴기) 등을 사용해서 증명하는 방식이다. 간단하게 말해 하드웨어 장비를 사용해 코인을 채굴하는 것이다. 해시함수에서 나온 출력값을 채굴자들이 하드웨어 장비(GPU, CPU와 같은 컴퓨팅 파워)를 통해 결과를 도출하는 것이다. 이러한 방식으로 문제를 해결하면 가장 빨리 채굴된 블록만 인정을 받고 나머지는 버려지게 되기 때문에 이중지불 문제가 해결 되게 된다. PoW를 사용하는 대표 코인에는 비트코인, 라이트코인, 제트캐시, 모네로 등이 존재한다.
(4) PBFT : 네오, 질리카, 하이퍼레저, R3, ITC, 텐더민트 등에서 사용하는 합의 알고리즘(다수의 참여자들이 통일된 의사결정을 하기 위해 사용하는 알고리즘)이다. 블록체인 네트워크 상에 새로운 블록들이 생성되는 과정에서 기존의 악의적인 공격으로 잘못된 블록이 생성될 수 있다.