

## 정보보호론

문 1. 인가된 사용자가 조직의 정보자산에 적시에 접근하여 업무를 수행할 수 있도록 유지하는 것을 목표로 하는 정보 보호 요소는?

- ① 기밀성(confidentiality)      ② 무결성(integrity)  
③ 가용성(availability)      ④ 인증성(authentication)

문 2. 발신지 IP 주소가 공격대상의 IP 주소로 위조된 ICMP 패킷을 특정 브로드캐스트 주소로 보내어 공격대상이 다량의 ICMP reply 패킷을 받도록 하는 공격기법은?

- ① SYN flooding      ② Smurf attack  
③ Land attack      ④ Teardrop

문 3. 중간자(man-in-the-middle) 공격에 대한 설명으로 옳은 것은?

- ① Diffie-Hellman 키 교환 프로토콜은 중간자 공격에 대비하도록 설계된 것이다.  
② 공격대상이 신뢰하고 있는 시스템을 불능상태로 만들고 공격자가 신뢰시스템인 것처럼 동작한다.  
③ 공격자가 송·수신자 사이에 개입하여 송신자가 보낸 정보를 가로채고, 조작된 정보를 정상적인 송신자가 보낸 것처럼 수신자에게 전달한다.  
④ 여러 시스템으로부터 한 시스템에 집중적으로 많은 접속 요청이 발생하여, 해당 시스템이 정상적인 동작을 못하게 된다.

문 4. 다중수준 보안(multi-level security) 시스템을 대상으로 다음 사항을 준수하는 보안 모델은?

- 주체는 자신과 같거나 자신보다 낮은 보안 수준의 객체만 읽을 수 있음(no read up)  
○ 주체는 자신과 같거나 자신보다 높은 보안 수준의 객체에만 쓸 수 있음(no write down)

- ① 벨라파둘라(Bell-Lapadula)      ② 비바(Biba)  
③ 클락윌슨(Clark-Wilson)      ④ 중국인벽(Chinese wall)

문 5. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거하여 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 일정 기준에 적합한지에 관하여 인증하는 것은?

- ① CC 인증      ② ITSEC 인증  
③ PIMS 인증      ④ ISMS 인증

문 6. 버퍼 오버플로우 공격의 대응수단으로 적절하지 않은 것은?

- ① 스택상에 있는 공격자의 코드가 실행되지 못하도록 한다.  
② 프로세스 주소 공간에 있는 중요 데이터 구조의 위치가 변경되지 않도록 적재 주소를 고정시킨다.  
③ 함수의 진입(entry)과 종료(exit) 코드를 조사하고 함수의 스택 프레임에 대해 손상이 있는지를 검사한다.  
④ 변수 타입과 그 타입에 허용되는 연산들에 대해 강력한 표기법을 제공하는 고급수준의 프로그래밍 언어를 사용한다.

문 7. 네트워크상에서 교환되는 인증 정보에 대한 재전송 공격(replay attack)을 막기 위한 방법으로 적절하지 않은 것은?

- ① 시도-응답(challenge-response) 인증 방식을 사용한다.  
② 메시지에 사전에 동기화된 현재 시각에 해당하는 타임스탬프(timestamp)를 포함하여 전송한다.  
③ 메시지에 송신자의 개인키로 서명한 전자서명(digital signature)을 포함하여 전송한다.  
④ 메시지에 수신자로부터 받은 일회용 랜덤 값에 해당하는 nonce를 포함하여 전송한다.

문 8. AES(Advanced Encryption Standard) 알고리즘을 구성하는 변환 과정 중, 상태 배열의 열 단위의 행렬 곱셈과 같은 형태로 표현되는 것은?

- ① 바이트 치환(substitute bytes)  
② 행 이동(shift row)  
③ 열 혼합(mix columns)  
④ 라운드 키 더하기(add round key)

문 9. 「정보통신기반 보호법」상 정보통신기반시설과 관련된 사항으로 옳지 않은 것은?

- ① 미래창조과학부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.  
② 누구든지 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위를 하여서는 아니된다.  
③ 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설의 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관이나 수사기관에 그 사실을 통지할 수 있다.  
④ 정부는 정보통신기반시설의 보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다.

문 10. 무선 LAN 보안에 관한 설명 중 ㉠ ~ ㉣에 들어갈 용어를 바르게 나열한 것은?

강도 높은 프라이버시 및 인증 기능을 포함하는 무선 LAN 보안 표준인 IEEE ( ㉠ )가 진화하는 과정에서 Wi-Fi 연합이 WPA/WPA2를 공표하였다. WPA는 WEP 암호의 약점을 보완한 ( ㉡ )를 사용한다. 위 표준과 유사한 WPA2는 ( ㉢ )를 채택하여 보다 강력한 보안을 제공한다. ( ㉣ )는 엄격한 보안이 요구되는 네트워크에서 확장된 인증 과정을 수행하는 인증 프로토콜이다.

- |   | ㉠       | ㉡    | ㉢    | ㉣      |
|---|---------|------|------|--------|
| ① | 802.11i | TKIP | AES  | EAP    |
| ② | 802.11i | DES  | TKIP | RADIUS |
| ③ | 802.1x  | DES  | TKIP | EAP    |
| ④ | 802.1x  | TKIP | AES  | RADIUS |

문 11. 「개인정보 보호법」에서 규정하고 있는 개인정보 중 민감정보에 해당하지 않는 것은?

- ① 주민등록번호
- ② 노동조합·정당의 가입·탈퇴에 관한 정보
- ③ 건강에 관한 정보
- ④ 사상·신념에 관한 정보

문 12. 메시지의 무결성 보장과 송신자에 대한 인증을 목적으로 공유 비밀키와 메시지에서부터 만들어지는 것은?

- ① 의사 난수
- ② 메시지 인증 코드
- ③ 해시
- ④ 인증서

문 13. 사용자 인증을 위한 접근방법으로 사용자가 알고 있는 것, 사용자가 가지고 있는 것, 사용자 자신의 특성을 이용하는 것 등이 있다. 최근 사용이 증가하고 있는 OTP(One Time Password)에 대한 설명으로 옳은 것은?

- ① 어떤 패스워드가 일정유형으로 반복해서 생성된다.
- ② 사용자가 알고 있는 정보에 의한 인증 기법이다.
- ③ 일반적으로 사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다.
- ④ 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

문 14. 위험 분석 방법 중 델파이법에 대한 설명으로 옳은 것은?

- ① 위험 발생 빈도를 추정하는 계산식을 통해 위험을 계량하여 분석한다.
- ② 미지의 사건을 추정하는 데 사용되는 방법으로 확률적 편차를 이용해 최저, 보통, 최고의 위험도를 분석한다.
- ③ 전문가 집단으로 구성된 위험 분석팀의 위험 분석 및 평가를 통해 여러 가능성을 전제로 위험과 취약성에 대한 의견수렴을 통한 분석 방법이다.
- ④ 어떤 사건이 예상대로 발생하지 않는다는 사실에 근거하여 주어진 조건하에 발생 가능한 위험에 따른 결과를 예측하는 방법이다.

문 15. ARP(Address Resolution Protocol) 스푸핑(spoofing) 기법을 이용한 스니핑(sniffing) 공격의 대응책으로 적절하지 않은 것은?

- ① 데이터를 암호화하여 전송한다.
- ② 라우터에 패킷 필터를 설정하여 서로 다른 LAN 간에 전송되는 패킷들을 검열하고 차단한다.
- ③ ARP 테이블 내의 MAC 주소 값을 정적(static)으로 설정한다.
- ④ 주기적으로 프러미스큐어스(promiscuous) 모드에서 동작하는 기기들이 존재하는지 검사함으로써 스니핑 중인 공격자를 탐지한다.

문 16. 커beros(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은?

- ① 커beros는 클라이언트와 응용서버 간의 상호 인증을 중재하는 제3자 인증 서비스를 제공한다.
- ② 커beros 서버는 AS(Authentication Server)와 TGS(Ticket Granting Server)로 구성된다.
- ③ TGS가 발급하는 티켓은 응용서버의 공개키로 암호화된다.
- ④ 한번 인증을 받은 클라이언트는 TGS에 여러 차례 접속할 수 있고 여러 응용서버에 접속할 때 사용할 티켓들을 획득할 수 있다.

문 17. IPSec 프로토콜과 이를 이용한 두 가지 운용 모드에 대한 설명으로 옳지 않은 것은?

- ① AH(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷의 페이로드의 무결성을 제공한다.
- ② 전송 모드에서 IPSec은 본래의 IPv4 패킷 헤더를 암호화하지 않는다.
- ③ ESP(Encapsulating Security Payload) 프로토콜은 발신지 인증과 페이로드의 무결성 및 기밀성을 제공한다.
- ④ 터널 모드는 송신자와 수신자가 모두 호스트인 경우에 사용되어 네트워크 전 구간에서 전체 IP 패킷을 암호화한다.

문 18. ElGamal 공개키 암호 방식의 기본 원리인 이산 대수(discrete logarithm) 문제를 바르게 설명한 것은? (단,  $p$ ,  $q$ 는 소수,  $a$ 는  $p$ 의 원시원소이고,  $\phi(\ )$ 는 Euler's totient 함수이다)

- ①  $a$ ,  $p$ ,  $y$ 가 주어졌을 때,  $y = a^x \bmod p$ 를 만족하는  $x$ 를 구하는 문제
- ②  $a, p, x, Y$ 가 주어졌을 때,  $Y = a^y \bmod p$ 를 만족하는  $a^{xy} \bmod p$ 를 구하는 문제
- ③  $n$ 이 주어졌을 때,  $n = pq$ 를 만족하는  $\phi(n)$ 을 구하는 문제
- ④  $n$ 과  $\phi(n)$ 과 서로소인  $e$ 가 주어졌을 때,  $n = pq$ 이면서  $ed \bmod \phi(n) = 1$ 을 만족하는  $d$ 를 구하는 문제

문 19. 「개인정보 보호법」상 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하도록 명시하고 있다. 개인정보 보호책임자의 업무에 해당하지 않는 것은?

- ① 개인정보 처리방침의 수립 및 공개
- ② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- ③ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
- ④ 개인정보 보호 교육 계획의 수립 및 시행

문 20. 사전에 A와 B가 공유하는 비밀키가 존재하지 않을 때, A가 B에게 전달할 메시지 M의 기밀성을 제공할 목적으로 공개키와 대칭키 암호화 기법을 모두 활용하여 암호화한 전송 메시지를 아래의 표기 기호를 사용하여 바르게 표현한 것은?

$PU_X$ : X의 공개키  
 $PR_X$ : X의 개인키  
 $K_{AB}$ : A에 의해 임의 생성된 A와 B 간의 공유 비밀키  
 $E(k, m)$ : 메시지 m을 암호키 k로 암호화하는 함수  
 $\parallel$ : 두 메시지의 연결

- ①  $E(K_{AB}, M) \parallel E(PU_A, K_{AB})$
- ②  $E(PR_A, (E(K_{AB}, M) \parallel K_{AB}))$
- ③  $E(K_{AB}, M) \parallel E(PR_A, K_{AB})$
- ④  $E(K_{AB}, M) \parallel E(PU_B, K_{AB})$