

1. 전자 서명의 기능과 가장 관계가 없는 것은?

- ① 인증성 ② 무결성
③ 부인봉쇄 ④ OTP 시간동기

2. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?

- ① 탐지분석 방법에는 오용 탐지 모델과 이상 탐지 모델이 있다.
② 침입탐지시스템의 구성요소로는 스크린 라우터, 베스천 호스트, 프록시 서버 등이 있다.
③ 호스트기반 IDS는 설치되어 있는 호스트 내의 침입 유형을 탐지한다.
④ 긍정오류(false positive)는 정상적인 행위를 침입으로 오인하여 탐지할 때를 말한다.

3. 공개키 암호화 알고리즘이 아닌 것은?

- ① ARIA
② RSA(Rivest, Shamir, Adleman)
③ ElGamal
④ ECC(Elliptic Curve Cryptosystem)

4. OECD 개인정보 보안 8원칙에 대한 내용으로 가장 옳지 않은 것은?

- ① 수집 제한의 원칙 ② 정보 정확성의 원칙
③ 비공개성의 원칙 ④ 책임의 원칙

5. DoS(Denial of Service)는 공격 대상이 수용할 수 있는 능력 이상의 정보나 사용자 또는 네트워크의 용량을 초과시켜 정상적으로 작동하지 못하게 하는 공격이다. DoS공격 중 하나인, SYN Flooding에 대한 설명으로 가장 옳은 것은?

- ① TCP 프로토콜의 3way hand shaking을 이용하여 공격 대상 시스템을 마비시키기 위한 방법으로 클라이언트(공격자)가 SYN+ACK패킷만을 지속적으로 보내는 방법이다.
② 클라이언트(공격자)가 짧은 시간에 많은 수의 SYN 패킷을 서버에 보내 접속을 요청한 후, 클라이언트가 ACK패킷을 보내주지 않는 방법이다.
③ Ping of Death공격으로 클라이언트(공격자)가 ICMP ping을 이용하여 서버에 ACK패킷을 지속적으로 보내는 방법이다.
④ TCP패킷의 시퀀스 번호를 조작하여 서버를 공격하는 방법이다.

6. IPSec(IP Security)에는 전송 모드(transport mode)와 터널 모드(tunnel mode)가 운영된다. IPSec에 대한 설명으로 가장 옳지 않은 것은?

- ① 전송 모드는 보통 호스트-대-호스트 데이터 보호를 필요로 할 때 사용된다.
② 터널 모드에서 IPSec은 가상 터널을 이용하며 새로운 IP패킷은 원래의 IP헤드와 정보를 포함한다.
③ 네트워크 레벨에서 패킷에 대한 보안을 제공하기 위해 IETF에 의해 설계된 프로토콜이다.
④ 전송 모드와 터널 모드에서 IPSec은 전송 계층에서 온 정보 즉, IP헤드를 포함한 IP패킷 전체를 보호한다.

7. 전자우편에 프라이버시, 무결성, 그리고 인증을 제공하기 위해 필 짐머만(Phil Zimmermann)에 의해 고안된 것으로, 안전한 전자우편 메시지를 생성하거나 향후에 검색한 파일을 안전하게 저장하기 위해 사용될 수 있다. 자신이 통신하기 원하는 각각의 사람들에게 대한 공개키가 필요하고, 자신에게 속해 있는 개인키/공개키의 쌍이 필요한 프로토콜은?

- ① POP3 ② SMTP ③ PGP ④ S/MIME

8. 「전자서명법」상 공인인증서에 대한 설명으로 가장 옳지 않은 것은?

- ① 공인인증서에는 공인인증기관의 서명키가 포함되어야 한다.
② 가입자의 사망, 실종선고 또는 해산 사실을 인지한 경우에는 당해 공인인증서를 폐지하여야 한다.
③ 공인인증서의 유효기간이 경과한 경우에는 그 사유가 발생한 때에 그 효력이 소멸된다.
④ 공인인증기관은 공인인증서를 발급받고자 하는 자의 신청이 있는 경우에는 공인인증서의 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다.

9. 「개인정보 보호법」상 <보기> 안의 ㉠에 들어갈 숫자로 옳은 것은?

—<보기>—

개인정보에 관한 분쟁을 조정하는 개인정보 분쟁조정 위원회는 위원장 1명을 포함한 ㉠ 명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.

- ① 10 ② 20 ③ 30 ④ 40

10. KDC(key distribution center) 없이 양쪽 통신 주체가 대칭 세션 키를 생성할 수 있는 프로토콜은?

- ① Otway-Rees 프로토콜
② Needham-Schroeder 프로토콜
③ Diffie-Hellman 프로토콜
④ Kerberos 프로토콜

