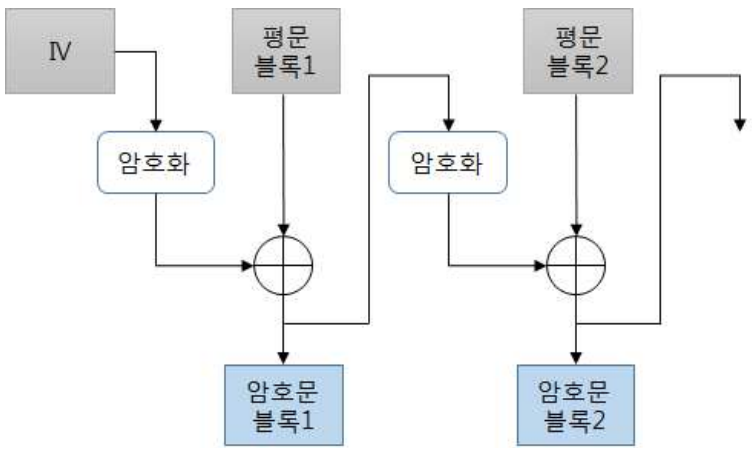
정보보호론

1. AES 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① Rijndael 알고리즘이 AES로 선정되었다.
② 블록 길이가 128비트인 대칭 블록 암호이다.
③ 키의 길이에 따라 10, 12, 14라운드를 가진다.
④ 키의 길이는 128, 192, 256비트를 지원한다.
⑤ 페이스텔(Feistel) 구조를 기반으로 작성되었다.

2. 다음 그림이 나타내는 블록암호 운용 모드는?



① ECB
② CBC
③ CFB
④ OFB
⑤ CTR

3. 키 분배 문제를 해결하기 위한 방법으로 옳지 않은 것은?

① 키를 사전에 공유
② 공개키 암호를 사용
③ Diffie-Hellman 알고리즘을 이용
④ 키 배포 센터(KDC)를 이용
⑤ SEED 암호 알고리즘을 이용

4. TCP/IP 프로토콜 계층과 각 계층에서 구현되는 보안 기술의 연결로 옳은 것은?

① 응용 계층 - Kerberos
② 전송 계층 - IPSec
③ 네트워크 계층 - TLS
④ 데이터링크 계층 - SSL
⑤ 물리 계층 - SET

5. 다음 중 충돌 저항성(Collision Resistance)과 관련이 높은 알고리즘은?

① AES
② DES
③ SHA-1
④ RSA
⑤ ECC

6. 특정한 목표를 겨냥해서 사전에 치밀하게 계획한 다음 장기적으로 집중적이고 은밀하게 공격하는 수법은?

① DDoS 공격
② 리버스 엔지니어링 공격
③ 레이스 컨디션 공격
④ 세션 하이재킹 공격
⑤ APT 공격

7. XSS(Cross Site Scripting)에 대한 설명으로 옳지 않은 것은?

① 웹페이지가 사용자에게 입력받은 데이터를 필터링하지 않고 그대로 동적으로 생성된 웹페이지에 포함하여 사용자에게 재전송할 때 발생한다.
② 해킹을 통해 시스템 권한을 획득한 후 시스템에 직접 명령을 입력할 수 있는 쉘을 실행한다.
③ 쿠키를 통해 웹페이지 사용자의 정보 추출을 할 수 있다.
④ 클라이언트에서 실행되는 언어로 작성된 악성 스크립트 코드를 게시판, 이메일 등에 포함시켜 전달한다.
⑤ 웹사이트에 방문하는 사용자를 악성 코드가 포함되어 있는 사이트로 리다이렉션 시킬 수도 있다.

8. 다음에서 설명하는 보안 공격은?

> 피싱(phishing)보다 한 단계 진화된 수법으로 진짜 사이트 주소를 입력하더라도 가짜 사이트로 접속을 유도해 개인정보를 훔치는 수법이다. 즉, 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인 네임 시스템(DNS) 또는 프락시 서버의 주소를 변조함으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤에 개인정보를 훔치는 공격기법이다.

① 파밍(Pharming) 공격
② 스미싱(Smishing) 공격
③ ARP 스푸핑(Spoofing) 공격
④ 세션 하이재킹(Session Hijacking) 공격
⑤ 중간자 개입(Man-in-the-middle) 공격

9. 암호화가 필요한 정보들 중에서 정보주체를 제외하고 정보를 다루는 관리자조차 암호화된 정보의 원래 정보가 무엇인지 알 수 없어야 하는 정보는?

① 은행계좌번호
② 주민등록번호
③ 신용카드번호
④ 비밀번호
⑤ 여권번호

10. 소프트웨어 보안 약점의 유형과 그러한 약점을 이용한 공격의 예로 옳지 않은 것은?

① DB와 연동된 웹어플리케이션에서 입력값에 대한 유효성 검증 누락 - SQL 삽입 공격
② 검증되지 않은 외부 입력이 웹서버의 동적 웹페이지 생성에 사용 - XSS 공격
③ 사용자 입력값을 외부사이트 주소로 사용하여 자동 연결 - 피싱(Phishing) 공격
④ XQuery를 사용하여 XML 데이터에 대한 동적 쿼리 생성 시 외부 입력에 대한 유효성 검증 누락 - 인증우회 공격
⑤ 검증되지 않은 외부 입력이 XPath 쿼리문 생성 시 문자열로 사용 - 리버스 엔지니어링 공격

11. 디바이스 인증수단으로 옳지 않은 것은?

① One Time Password
② MAC 주소값
③ 802.1x, WPA 표준 암호프로토콜
④ X.homesec-2
⑤ SSID

12. 해시함수의 설명으로 옳지 않은 것은?

① 양방향성을 가진다.
② 메시지가 다르면 매우 높은 확률로 해시값도 다르다.
③ 임의의 길이 메시지로부터 고정길이의 해시값을 계산한다.
④ 해시값을 고속으로 계산할 수 있다.
⑤ MD5, RIPEMD-160, SHA-512 등이 있다.

13. 공개키 암호인 RSA의 특징에 대한 설명으로 옳지 않은 것은?

① 매우 큰 소수를 사용하여 키를 만든다.
② 암·복호화 과정에 계산량이 많다.
③ 개인 인증서에도 사용한다.
④ 키를 교환해야 하는 불편함이 있다.
⑤ 디지털 서명에도 사용한다.

14. 시스템의 보안 취약점이 발견된 뒤 이를 막을 수 있는 패치가 발표되기 전에 그 취약점을 이용한 악성코드나 해킹공격을 감행하는 수법은?

① APT 공격
② 스턱스넷 공격
③ DDoS 공격
④ 제로데이 공격
⑤ XSS 공격

15. TLS 서브 프로토콜 중에서 데이터를 분할, 압축, 암호 등의 기능을 수행하는 프로토콜은?

① Handshake Protocol
② Change Cipher Spec Protocol
③ Alert Protocol
④ Record Protocol
⑤ Heartbeat Protocol

16. 다음 중 「개인정보보호법」에 대한 설명으로 옳지 않은 것은?

① 제3조 '개인정보 보호 원칙'에 따르면, 개인정보는 목적 외의 용도로 활용해서는 안된다.
② 제4조 '정보주체의 권리'에 따르면, 정보주체는 자신의 개인정보의 처리에 관한 동의여부, 동의범위 등을 선택하고 결정할 수 있다.
③ 제15조 '개인정보의 수집·이용'에 따르면, 모든 개인정보의 수집은 정보주체의 동의를 받아야 한다.
④ 제21조 '개인정보의 파기'에 따르면, 개인정보의 보유기간이 경과하거나, 더이상 불필요한 경우 지체 없이 그 개인정보를 파기해야한다. 단, 다른 법령에 따라 보존해야하는 경우도 있다.
⑤ 제34조 '개인정보 유출 통지 등'에 따르면, 개인정보 유출이 확인된 경우 지체 없이 정보주체에게 유출된 항목과 시점, 경위 등을 통보해야 한다.

17. IPSec에 대한 설명으로 옳지 않은 것은?

① Tunnel Mode는 IP 헤더를 포함한 모든 Payload를 암호화 한다.
② Transport Mode에서 송·수신자의 IP 주소는 바뀌게 된다.
③ ESP 프로토콜은 인증을 사용하지 않을 수도 있다.
④ ESP 프로토콜의 경우 암호화 알고리즘으로 DES, 3DES, AES등을 사용할 수 있다.
⑤ AH 프로토콜의 경우 기밀성을 보장하지 못한다.

18. IT시스템에 발생할 수 있는 다음의 보안 이슈들과 밀접한 관계를 가진 정보보호 요소는?

> ○ IT 시스템의 저장된 데이터 변경
> ○ IT 시스템 메모리 변경
> ○ IT 시스템 간 메시지 전송 중 내용 변경

① 기밀성(Confidentiality)
② 무결성(Integrity)
③ 가용성(Availability)
④ 신뢰성(Reliability)
⑤ 책임추적성(Accountability)

19. 다음 중 이산 대수 문제의 어려움에 기초한 암호 알고리즘은?

① DES
② AES
③ Diffie-Hellman
④ RSA
⑤ SHA-2

20. 다음 지문의 괄호 안에 들어갈 말로 옳은 것은?

> ( )은/는 HTTP 기반의 통신 서비스에서 보안 기능을 제공하기 위한 한 방안의 오픈 소스 라이브러리이다. C언어로 작성되어 있는 중심 라이브러리 안에는, 기본적인 암호화 기능 및 여러 유틸리티 함수들이 구현되어 있다.

① IPSec
② OpenSSL
③ Kerberos
④ MySQL
⑤ PGP