정보보호론

1. 정보보호의 침해 유형을 소극적 공격과 적극적 공격으로 구분했을 때 적극적 공격에 해당하는 것은?

① 특정 서버에 대한 접속을 마비시킨다.
② 문서들을 분석하여 개인 정보를 추출한다.
③ 패스워드 파일로부터 패스워드를 추측한다.
④ 특정 사용자의 전자우편 메시지를 분석한다.
⑤ 특정 서버와의 트래픽을 선택적으로 감시한다.

2. 대칭키 암호에 대한 설명으로 옳지 않은 것은?

① DES, AES는 대칭키 암호 알고리즘에 속한다.
② 대칭키 암호는 두 개의 키 값(비밀키, 공개키)이 서로 대칭적으로 존재해야 한다.
③ AES는 SPN(Substitution-Permutation Network) 기반 대칭키 암호이다.
④ AES는 128비트 라운드 키를 사용한다.
⑤ ARIA, SEED는 우리나라 대칭키 암호이다.

3. 메시지 인증 코드(MAC: Message Authentication Code)가 제공하는 기능들로 짝지어진 것은?

ㄱ. 부인 방지
ㄴ. 상호 인증
ㄷ. 접근 제어
ㄹ. 무결성 보장

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ
⑤ ㄷ, ㄹ

4. CC(Common Criteria) 인증 제도에 대한 설명으로 옳지 않은 것은?

① CC에서 TOE는 Target of Evaluation의 약자로서 평가 대상을 의미한다.
② CC에서 정보보호시스템은 EAL(Evaluation Assurance Level)로 보안수준을 평가받는다.
③ CC는 미국 NIST FIPS PUB 197 자료를 참고해서 만들어진 제도이다.
④ CC에서 PP는 Protection Profile을 의미하는 것으로 보안 요구 사항을 정의한다.
⑤ CC는 CCRA(Common Criteria Recognition Arrangement)라는 국제상호인정협정을 가지며, CCRA 수준으로 평가를 수행한다.

5. OTP(One Time Password)에 대한 설명으로 옳지 않은 것은?

① OTP는 비밀번호 예측 공격을 막기 위한 방법으로 사용 가능하다.
② 패킷 스니핑을 통한 비밀번호 재사용 공격의 대응책으로 활용 가능하다.
③ 동기화 방식 OTP에서는 시간과 인증 횟수를 기반으로 비밀번호를 동기화 한다.
④ 비동기화 방식 OTP는 인증서버에서 전송된 난수를 기반으로 비밀번호를 생성한다.
⑤ 시간 동기화 방식 OTP는 인증서버와 OTP 생성기의 시간오차범위를 허용하지 않는다.

6. ARP Spoofing이 악용하는 매핑(mapping) 정보로 짝지어진 것은?

① IP 주소 - 도메인 주소
② IP 주소 - MAC 주소
③ MAC 주소 - TCP port 번호
④ MAC 주소 - 도메인 주소
⑤ IP 주소 - TCP port 번호

7. BLP(Bell-La Padula) 모델이 가지고 있는 특성과 규칙에 대한 설명으로 옳지 않은 것은?

① 비밀정보가 허가되지 않은 방식으로 접근되는 것을 방지하고자 하는 것을 목표로 함
② 강제적 접근통제를 하고자 하는 경우 본 모델을 기반으로 통제 규칙을 정의함
③ 단순 보안 규칙은 주체가 객체를 읽기 위해서는 주체의 비밀취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함
④ 스타 보안 규칙은 주체가 객체에 쓰기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높거나 같아야 함
⑤ 강한 스타 보안 규칙은 주체의 읽기/쓰기는 하위 혹은 상위가 아닌 동일한 보안 분류 수준의 객체에 대해서만 가능함

8. 웹 공격의 유형에 대한 설명으로 옳지 않은 것은?

① XSS(Cross-Site Scripting) : 저장 XSS 공격, 반사 XSS 공격, DOM 기반 XSS 공격으로 분류되며, 이에 대응하기 위해서는 웹 어플리케이션의 개발단계에서 XSS에 대비한 입출력값을 검증하고 적절하게 인코딩하는 방법을 선택하는 것이 중요하다.

② SQL injection : 웹에서 사용자가 입력하는 값이 DB 질의어와 연동이 되는 경우에는 클라이언트 측에서만 자바스크립트 등을 통해 사용자의 입력값을 검증하는 것으로 해결된다.

③ CSRF(Cross-Site Request Forgery) : 사용자가 자신의 의도와는 무관하게 공격자가 의도한 웹사이트 사용 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 만드는 공격이다.

④ 쿠키획득 공격 : 로그인된 사용자의 쿠키값을 XSS 등의 공격으로 획득하여 로그인을 할 수 있다.

⑤ 인증우회 공격 : 인증되지 않은 사용자가 접근할 수 없는 페이지를 접근할 수 있는 URL을 획득하여 인증 없이 접근하는 공격방법이다.

9. Diffie-Hellman 알고리즘은 $(G^a \bmod P)^b \bmod P$와 $(G^b \bmod P)^a \bmod P$를 계산한 값이 같다는 대수적인 성질을 활용한다. 다음 설명 중 옳지 않은 것은?

① a와 b는 비밀값이다.

② P는 소수이다.

③ 두 개의 키를 합성하면 새로운 키가 생성된다.

④ 중간자 공격을 방지한다.

⑤ 암호화와 복호화에 필요한 키를 분배하거나 교환하기 위한 것이다.

10. 「개인정보 보호법」의 개인정보 영향평가에 대한 설명으로 옳지 않은 것은?

① 공공기관의 장은 개인정보 영향평가를 하고 그 결과를 한국인터넷진흥원장에게 제출하여야 한다.

② 개인정보 영향평가는 대통령령으로 정하는 기준에 해당하는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우, 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.

③ 개인정보 영향평가를 하는 경우에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도 등에 대하여 고려하여야 한다.

④ 평가기관의 지정기준 및 지정취소, 평가기준, 평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑤ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 개인정보 영향평가를 하기 위하여 적극 노력하여야 한다.

11. 전자문서에 대한 인증 및 부인 방지에 활용하는 암호화 방식은?

① SEED

② HIGHT

③ AES

④ RC6

⑤ RSA

12. 정보통신망의 안전성 확보를 위해 수립하는 기술적, 물리적, 관리적 보호 조치 등 종합적인 정보보호 관리 체계 인증 제도는?

① PIMS(Personal Information Management System)

② ISMS(Information Security Management System)

③ ITSEC(Information Technology Security Evaluation Criteria)

④ CMVP(Cryptographic Module Validation Program)

⑤ KCMVP(Korea Cryptographic Module Validation Program)

13. 블록체인(Blockchain) 관련 보안 기술에 대한 설명으로 옳지 않은 것은?

① 블록체인은 해시 함수를 사용하여 데이터에 대한 무결성을 보장한다.

② 블록체인 기술은 데이터의 신뢰성 및 투명성을 제공한다.

③ 공개형 블록체인 기술은 공개키 암호를 사용하기 때문에 권한이 있는 피어(peer)만 참여할 수 있다.

④ 블록체인 기술의 한 예인 하이퍼레저 패브릭(Hyperledger Fabric)에서는 공개키 인증서를 이용하여 피어에 대한 신원(identity) 정보를 제공한다.

⑤ 블록체인 기술에서는 작업 증명이나 지분 증명 등과 같은 합의 알고리즘을 사용한다.

14. 파밍(Pharming) 공격에 활용하기 위해 공격자의 웹서버 IP 주소와 매핑해주는 특정 정보로 옳은 것은?

① 정상 사이트의 도메인 주소

② 정상 사이트 서버의 MAC 주소

③ 정상 사이트가 연결되어 있는 스위치의 port 번호

④ 사용자 컴퓨터의 공인 IP주소

⑤ 정상 사이트 서버의 TCP port 번호

15. 해시 함수에 대한 설명으로 옳지 않은 것은?

① 해시 함수를 사용하면 임의 길이의 메시지에 대해 특정 길이를 갖는 출력값을 얻을 수 있다.

② 해시 함수는 일방향 함수에 해당한다.

③ 동일한 출력값을 갖는 임의의 두 입력 메시지를 찾기 어렵다는 것을 강한 충돌 저항성(strong collision resistance)이라고 한다.

④ 해시 함수는 블록체인에서 체인 형태로 사용되어 데이터의 신뢰성을 보장한다.

⑤ 해시 함수는 대칭키 암호와 달리 키 값을 적용할 수 없기 때문에 MAC(Message Authentication Code)로 사용할 수 없다.

16. 공개키 기반 구조(PKI: Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?

① 공개키 인증서는 특정 사용자의 신원과 그 사용자의 공개키를 바인딩시키는 기술이다.

② 공개키 인증서를 생성할 때는 인증기관(CA: Certificate Authority)의 공개키를 사용하여 서명할 수 있다.

③ CA간에는 인증 체인을 형성할 수 있기 때문에 특정 CA에 의해 서명된 인증서는 인증 체인상의 다른 CA에 의해서도 보장될 수 있다.

④ 공개키 인증서 서명에는 RSA나 ECDSA를 사용할 수 있다.

⑤ PKI에서 RA(Registration Authority)는 인증서 발급을 요청한 사용자의 신원을 검증하는 역할을 한다.

17. 다음 중 <보기>에서 설명하는 것은?

<보 기>

IETF의 작업 그룹에서 RSADSI(RSA Data Security Incorporation)의 기술을 기반으로 개발한 전자우편 보안 기술이며, RFC 3850, 3851 등에서 정의되어 있다. 전자우편에 대한 암호화 및 전자서명을 통하여 메시지 기밀성, 메시지 무결성, 사용자 인증, 송신 사실 부인 방지, 프라이버시 보호 등의 보안 기능을 제공한다.

① MIME(Multipurpose Internet Mail Extensions)

② SMTP(Simple Mail Transfer Protocol)

③ PGP(Pretty Good Privacy)

④ PEM(Privacy Enhanced Mail)

⑤ S/MIME(Secure/Multipurpose Internet Mail Extensions)

18. 무선 네트워크 보안 기술에 대한 설명으로 옳지 않은 것은?

① WEP는 보안 취약성이 있다고 알려져 있다.

② WPA2 기술은 AES-CCMP를 사용한다.

③ 무선네트워크 환경에서 인증/인가를 위해 RADIUS 프로토콜을 사용하여 연결한다.

④ Diameter 프로토콜은 RADIUS보다 세션관리, 보안 측면에서 개선 및 확장된 프로토콜이다.

⑤ WPA-PSK 방식은 공개키 인증서 공유 방식으로 확장성이 좋다.

19. 전송 계층 보안(TLS: Transport Layer Security) 프로토콜에 대한 설명으로 옳지 않은 것은?

① TLS는 TCP 프로토콜상에서 사용되며, DTLS는 UDP 프로토콜상에서 사용된다.

② TLS 프로토콜에서는 레코드 프로토콜 단계에서 공개키 인증서를 사용한다.

③ TLS는 SSL을 기초로 개발되었다.

④ FTPS에서는 FTP 파일 전송 프로토콜에서 안전한 전송을 위해 TLS를 사용한다.

⑤ TLS 프로토콜에서 대칭키 암호인 ARIA를 사용할 수 있다.

20. 「개인정보 보호법 시행령」에서 정한 고유식별정보의 범위에 포함되지 않는 것은?

①「주민등록법」 제7조의2 제1항에 따른 주민등록번호

②「여권법」 제7조 제1항 제1호에 따른 여권번호

③「도로교통법」 제80조에 따른 운전면허의 면허번호

④「국가연구개발사업의 관리 등에 관한 규정」 제25조 제11항에 따른 과학기술인 등록번호

⑤「출입국관리법」 제31조 제4항에 따른 외국인등록번호