

정보보호론

1. 정보보안 목표와 그 목표에 대한 위협 요소를 바르게 연결한 것만을 모두 고르면?

ㄱ. 기밀성 - 재전송(replaying)
ㄴ. 무결성 - 가장(masquerading)
ㄷ. 가용성 - 서비스 거부(DoS)

- ① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

2. CA(Certification Authority)가 사용자 A에게 발급한 X.509 버전 3 형식의 인증서에 포함되는 정보가 아닌 것은?

- ① A의 공개키
② A의 개인키
③ 인증서의 유효 기간
④ CA가 사용한 서명 알고리즘

3. 다음 설명에 해당하는 암호학적 해시함수 h의 특성은?

주어진 x와 h(x)에 대해 $h(x) = h(y)$ 를 만족하는 $y(y \neq x)$ 를 찾는 것이 계산적으로 불가능해야 한다.

- ① 무결성(integrity)
② 일방향성(one-way property)
③ 강한 충돌 저항성(strong collision resistance)
④ 약한 충돌 저항성(weak collision resistance)

4. 다음은 하이브리드 암호시스템을 이용하여 송신자가 메시지 M을 수신자에게 전달하기 위한 과정을 4단계로 나타낸 것이다. (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

1. 송신자는 임의로 (가) K를 선택한다.
2. 송신자는 K를 이용하여 M을 (나) 암호 알고리즘으로 암호화한다.
3. 송신자는 K를 (다) 암호 알고리즘으로 암호화한다.
4. 송신자는 단계 2, 3에서 생성한 암호문을 수신자에게 전송한다.

(가) (나) (다)

- ① 세션키 대칭키 공개키
② 세션키 공개키 대칭키
③ 공개키 대칭키 공개키
④ 공개키 공개키 대칭키

5. AES에 대한 설명으로 옳지 않은 것은?

- ① SPN 구조를 사용한다.
② 128비트 블록 단위로 암호화한다.
③ 암호화 함수와 복호화 함수가 동일하다.
④ 키 길이에 따라 10, 12, 14 라운드로 구성된다.

6. 인증 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① S/Key 인증은 해시함수 체인을 사용한다.
② 공개키 암호를 이용한 인증에서는 상대방의 공개키를 알고 있어야 한다.
③ 영지식 증명(zero-knowledge proof)으로 비밀정보를 노출하지 않고 비밀정보의 소유를 증명할 수 있다.
④ 커beros(Kerberos)에서 티켓발급 서버(TGS)는 서비스 서버의 접속에 필요한 티켓을 사용자의 공개키로 암호화하여 전달한다.

7. 양자 컴퓨터 시대의 암호에 대한 설명으로 옳은 것은?

- ① AES는 키 길이를 증가시켜도 더 이상 안전성을 유지할 수 없다.
② 양자 키 분배 프로토콜을 사용하면 안전하게 암호키를 공유할 수 있다.
③ 양자내성암호(PQC)는 양자 알고리즘을 이용하여 양자 컴퓨터에서만 동작하도록 설계된 암호이다.
④ 인수분해의 어려움에 의존하는 RSA는 쇼어(Shor) 알고리즘을 이용한 양자 컴퓨터의 공격에도 안전성을 유지할 수 있다.

8. 다음 설명에 해당하는 것은?

암호 연산을 하드웨어로 이동함으로써 시스템 보안을 향상하기 위해 신뢰 컴퓨팅 그룹(Trusted Computing Group)에서 표준화한 개념이다. 기본적으로 인증된 부트(authenticated boot), 인증, 암호화 기능을 제공한다.

- ① TrustZone
② SIEM(Security Information & Event Management)
③ TEE(Trusted Execution Environment)
④ TPM(Trusted Platform Module)

9. 「개인정보 보호법」상 공개된 장소에 고정형 영상정보처리기를 설치·운영할 수 있는 경우가 아닌 것은?

- ① 범죄의 예방 및 수사를 위하여 필요한 경우
② 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
③ 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우
④ 촬영된 영상정보를 저장하지 아니하는 경우로서 개인정보보호 위원회가 정하는 경우

10. ISMS-P 인증을 위한 ‘관리체계 수립 및 운영’ 영역 중 하나인 ‘관리체계 운영’에 속하는 인증기준에 대한 설명으로 옳은 것은?

- ① 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
- ② 선정한 보호대책을 이행계획에 따라 효과적으로 구현하고 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
- ③ 조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
- ④ 조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.

11. 재사용이 불가능하도록 매번 새로운 패스워드를 생성하는 인증 방식은?

- ① SSO
- ② OTP
- ③ PIN
- ④ RADIUS

12. 다음 설명의 (가), (나)에 들어갈 용어를 바르게 연결한 것은?

무선 랜 보안을 위해 WEP(Wired Equivalent Privacy)에서는 (가)를 암호화 알고리즘으로 사용하였다. 이후에 WEP 방식의 보안 취약점을 해결하기 위하여 IEEE 802.11i 표준이 만들어졌는데, 여기서는 무선 데이터의 무결성과 기밀성을 제공하기 위하여 AES를 기반으로 하는 (나)를 제안하였다.

(가) (나)

- | | |
|----------|------|
| ① CRC-32 | CCMP |
| ② CRC-32 | TKIP |
| ③ RC4 | CCMP |
| ④ RC4 | TKIP |

13. 다음 제시문에 해당하는 위험처리 전략은?

어떤 조직에서 시스템 로그인 패스워드의 도용을 방지하기 위하여 3가지 이상의 문자 조합으로 8글자 이상의 패스워드가 강제 설정되도록 하는 모듈을 개발·적용하려고 한다.

- ① 위험감소
- ② 위험회피
- ③ 위험전가
- ④ 위험수용

14. 반사형 XSS 공격에 대한 설명으로 옳은 것은?

- ① 악성 스크립트가 웹 서버에서 실행된다.
- ② 악성 스크립트는 웹 서버 측 데이터베이스에 저장된다.
- ③ 공격자가 보낸 악의적 링크를 사용자가 클릭하게 한다.
- ④ 사용자와 웹 서버 간의 신뢰 관계를 악용하여 공격자가 원하는 서버 동작을 발생시킨다.

15. ISMS-P 인증 추진체계에서 인증기관에 해당하는 것은?

- ① 금융보안원(FSI)
- ② 한국정보통신진흥협회(KAIT)
- ③ 한국정보통신기술협회(TTA)
- ④ 개인정보보호협회(OPA)

16. 리눅스의 find 명령에 대한 설명으로 옳지 않은 것은?

- ① 명령: find / -name '*.c'
설명: 확장자가 c인 파일을 모두 찾는다.
- ② 명령: find / -mtime -2
설명: 최근 48시간 이내에 마지막으로 수정된 파일을 모두 찾는다.
- ③ 명령: find / -user user1
설명: 소유자가 user1인 파일을 모두 찾는다.
- ④ 명령: find / -type 4755
설명: 권한 설정이 4755로 설정된 파일을 모두 찾는다.

17. DNS 스푸핑 공격에 대한 설명으로 옳지 않은 것은?

- ① 사용자가 악의적인 웹 사이트에 접속하도록 하는 공격이다.
- ② 공격자는 사용자의 DNS 질의에 대해 위조된(spoofed) 응답이 사용자에게 전달되게 한다.
- ③ DNS 캐시 포이즈닝(poisoning)은 위조된 DNS 응답이 로컬 DNS 서버의 캐시에 저장되므로 일정 기간 사용자에게 피해를 줄 수 있다.
- ④ 디지털 서명으로 DNS 데이터그램의 진위 여부를 확인할 수 있는 SSH(Secure Shell)가 DNS 캐시 포이즈닝 공격을 방지하기 위해 설계되었다.

18. 정보보호 최고책임자 또는 개인정보 보호책임자를 지정하도록 하는 근거가 되는 법률이 아닌 것은?

- ① 개인정보 보호법
- ② 전자금융거래법
- ③ 정보보호산업의 진흥에 관한 법률
- ④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

19. 리눅스 /etc/group 파일의 4개 필드에 대한 설명으로 옳지 않은 것은?

- ① 첫 번째 필드는 그룹의 이름을 나타낸다. groupadd 명령을 이용하여 새로운 그룹을 생성할 수 있다.
- ② 두 번째 필드는 그룹 패스워드를 나타내는 부분이지만 /etc/gshadow 파일에서 별도 관리하는 경우에는 'x'로만 표기된다.
- ③ 세 번째 필드는 리눅스에서 그룹에 부여한 번호로 그룹 생성 이후에는 변경할 수 없다.
- ④ 네 번째 필드에 해당 그룹에 속한 사용자의 로그인 ID가 기록된다.

20. 「정보통신기반 보호법」의 내용으로 옳지 않은 것은?

- ① 「정보통신기반 보호법」은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.
- ② 과학기술정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.
- ③ 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설인 도로·철도·지하철·공항·항만 등 주요 교통시설에 대한 관리기관의 장이 「정보통신기반 보호법」 제7조제1항에 따라 기술적 지원을 요청하는 경우 과학기술정보통신부장관에게 우선적으로 그 지원을 요청하여야 한다.
- ④ 중앙행정기관의 장은 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위하여 필요한 경우이거나, 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요한 경우에 해당 관리기관의 장에게 주요정보통신기반시설의 취약점을 분석·평가하도록 명령할 수 있다.

21. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」상 클라우드컴퓨팅서비스 제공자가 즉시 그 사실을 과학기술정보통신부장관에게 알려야 하는 경우는?

- ① 이용자 정보가 유출된 때
- ② 클라우드컴퓨팅 사업의 수요가 대규모로 발생한 때
- ③ 사전예고 없이 당사자 간 계약으로 정하였거나 대통령령으로 정하는 기간 이상 서비스 중단이 발생한 때
- ④ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고가 발생한 때

22. 패킷 필터링 방화벽에서는 포트 번호를 사용하여 특정 서비스를 허용하거나 차단하는 필터링 규칙을 적용한다. 서비스 명과 포트 번호가 옳게 짝지어지지 않은 것은?

- ① DNS - 161
- ② FTP(제어) - 21
- ③ HTTPS - 443
- ④ SMTP - 25

23. IPSec ESP(Encapsulating Security Payload)의 패킷 포맷에 대한 설명으로 옳지 않은 것은?

- ① 32비트의 보안 매개변수 색인(security parameter index) 필드에는 같은 보안연관(security association)에 속하는 각 패킷에 대해서로 다른 보안 매개변수 색인값이 주어진다.
- ② 32비트의 순서 번호(sequence number) 필드에는 데이터그램의 순서를 나타내는 카운터 값이 저장된다.
- ③ 8비트의 다음 헤더(next header) 필드는 IP 데이터그램에 의해 전달되는 페이로드의 데이터 유형을 나타낸다.
- ④ ICV(Integrity Check Value) 필드에는 IP 헤더와 ICV를 제외한 전체 패킷에 대해 계산한 인증 데이터가 저장된다.

24. OAEP(Optimal Asymmetric Encryption Padding)에 대한 설명으로 옳지 않은 것은?

- ① 동일한 메시지에 대하여 OAEP 패딩 결과는 항상 동일하다.
- ② OAEP는 RSA 암호의 안전성을 높이기 위한 메시지 패딩 규격이다.
- ③ OAEP 패딩을 적용한 RSA에서는 수신자가 암호문의 변조 여부를 확인할 수 있다.
- ④ OAEP 패딩을 적용한 RSA에서는 동일한 메시지와 동일한 공개키를 사용해도 생성된 암호문이 달라질 수 있다.

25. HTTP 버전 1.1 GET 요청 메시지의 헤더 라인에 대한 설명으로 옳지 않은 것은?

- ① Accept: 클라이언트가 수용할 수 있는 매체의 형식
- ② Cookie: 서버에게 반환하는 쿠키 정보
- ③ Server: 서버의 URL 정보
- ④ User-Agent: 클라이언트 프로그램(브라우저 등) 정보