정보보호론

문 1. 전자 서명(digital signature) 보안 메커니즘이 제공하는 보안 서비스가 아닌 것은? 2

① 근원 인증
② 메시지 기밀성
③ 메시지 무결성
④ 부인 방지

[해설]
전자 서명의 특징
- **위조불가**: 서명자만이 서명문을 생성할 수 있다.
- **부인방지**: 서명자는 서명 후에 사실을 부인할 수 없다.
- **재사용 불가**: 한번 서명한 서명문은 또 다른 문서에 사용할 수 없다.
- **변경 불가**: 내용 변경시 서명문 자체가 변경되어 변조 사실을 확인이 가능하다.
- **서명자 인증**: 서명자의 서명문은 서명자의 식별이 가능하다.

문 2. AES(Advanced Encryption Standard)에 대한 설명으로 옳은 것은? 1

① DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘이다.
② Feistel 구조로 구성된다.
③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.
④ 2001년에 국제표준화기구인 IEEE가 공표하였다.

[해설]
AES(Advanced Encryption Standard)
- DES가 페이스텔 구조인 반면, AES는 비페이스텔 구조.
- AES 선정 조건 : 속도가 빠를 것. 단순하고 구현하기 쉬울 것. 스마트 카드나 8비트 CPU 등의 계산력이 작은 플랫폼에서부터 워크스테이션과 같은 고성능의 플랫폼에 이르기까지 효율적으로 동작.
- 2001년에 미국의 표준화기구인 NIST(National Institute of Standard and Technology)에 의해 공표.

문 3. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은? 4

① 호스트 기반 IDS와 네트워크 기반 IDS로 구분한다.
② 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단한다.
③ 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.
④ IDS는 방화벽처럼 내부와 외부 네트워크 경계에 위치해야 한다.

[해설]
- 침입탐지시스템(IDS)에서 **네트워크 기반 IDS는** 외부 네트워크 경계에 위치되지만, **호스트 기반 IDS는** 시스템 내부에 설치될 수 있다.

문 4. RSA 암호 알고리즘에서 두 소수, p = 17, q = 23과 키 값 e = 3을 선택한 경우, 평문 m = 8에 대한 암호문 c로 옳은 것은? 1

① 121 ② 160
③ 391 ④ 512

[해설]
m^e mod n = c
n = p * q = 17 * 23 = 391
8^3 mod 391 = 121

문 5. IEEE 802.11i RSN(Robust Security Network)에 대한 설명으로 옳은 것은? 2

① TKIP는 확장형 인증 프레임워크이다.
② CCMP는 데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드로 이용한다.
③ EAP는 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용한다.
④ 802.1X는 무결성 보장을 위해 CBC-MAC를 이용한다.

[해설]
- IEEE 802.11i 태스크그룹은 2002년 RSN(Robust Security Network) 보안 구조를 표준에 반영함으로 무선구간에서의 데이터 보호기능을 더욱 강화하였다.
- EAP는 확장형 인증 프레임워크이며, WPA2에서 인증에 사용된다.
- CCMP는 무결성 보장을 위해 CBC-MAC을 이용한다.

문 6. CC(Common Criteria) 인증 평가 단계를 순서대로 바르게 나열한 것은? 1

가. PP(Protection Profile) 평가
나. ST(Security Target) 평가
다. TOE(Target Of Evaluation) 평가

① 가→나→다
② 가→다→나
③ 나→가→다
④ 다→나→가

[해설]
- PP(Protection Profile) 평가 : PP의 완전성, 일치성, 기술성 평가
- ST(Security Target) 평가 : ST가 PP의 요구사항을 충족하는지 평가
- TOE(Target Of Evaluation) 평가 : TOE가 ST의 요구사항을 충족하는지 평가

문 7. SQL 삽입 공격에 대한 설명으로 옳지 않은 것은? 4

① 사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생한다.
② 공격이 성공하면 데이터베이스에 무단 접근하여 자료를 유출하거나 변조시키는 결과가 초래될 수 있다.
③ 사용자의 입력값으로 웹 사이트의 SQL 질의가 완성되는 약점을 이용한 것이다.
④ 자바스크립트와 같은 CSS(Client Side Script) 기반 언어로 사용자 입력을 필터링하는 방법으로 공격에 대응하는 것이 바람직하다.

[해설]

- 자바스크립트와 같은 CSS(Client Side Script) 기반 언어로 사용자 입력을 필터링하는 것은 변조의 위험이 있기 때문에 SSS(Server Side Script) 기반 언어로 필터링하는 방법으로 공격에 대응하는 것이 바람직하다.
- SQL 삽입 공격은 웹에서 사용자가 입력하는 값이 DB 질의어와 연동이 되는 경우에는 클라이언트 측과 서버 측에서도 입력값을 검증해야 한다.

문 8. 유닉스/리눅스의 파일 접근 제어에 대한 설명으로 옳지 않은 것은? 3

① 접근 권한 유형으로 읽기, 쓰기, 실행이 있다.
② 파일에 대한 접근 권한은 소유자, 그룹, 다른 모든 사용자에 대해 각각 지정할 수 있다.
③ 파일 접근 권한 변경은 파일에 대한 쓰기 권한이 있으면 가능하다.
④ SetUID가 설정된 파일은 실행 시간 동안 그 파일의 소유자의 권한으로 실행된다.

[해설]

- 파일 접근 권한 변경은 파일 소유자나 슈퍼 유저만이 chmod를 이용하여 가능하다.

문 9. IPSec에 대한 설명으로 옳지 않은 것은? 3

① 전송(transport) 모드에서는 전송 계층에서 온 데이터만을 보호하고 IP 헤더는 보호하지 않는다.
② 인증 헤더(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.
③ 보안상 안전한 채널을 만들기 위한 보안 연관(Security Association)은 양방향으로 통신하는 호스트 쌍에 하나만 존재한다.
④ 일반적으로 호스트는 보안 연관 매개변수들을 보안 연관 데이터베이스에 저장하여 사용한다.

[해설]

- 보안 연관(Security Association)은 애플리케이션마다 독립적으로 생성되고 관리되며, 양방향으로 통신하는 호스트 쌍에 여러개가 존재할 수 있다.

문 10. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 명시된 것으로 옳지 않은 것은? 4

① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.
② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
③ 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.
④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기할 수 있다.

[해설]

- 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제25조(침해사고 등의 통지 등) ① 클라우드컴퓨팅서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고(이하 "침해사고"라 한다)가 발생한 때
2. 이용자 정보가 유출된 때
3. 사전예고 없이 대통령령으로 정하는 기간(당사자 간 계약으로 기간을 정하였을 경우에는 그 기간을 말한다) 이상 서비스 중단이 발생한 때

② 클라우드컴퓨팅서비스 제공자는 제1항제2호에 해당하는 경우에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.
③ 과학기술정보통신부장관은 제2항에 따른 통지를 받거나 해당 사실을 알게 되면 피해 확산 및 재발의 방지와 복구 등을 위하여 필요한 조치를 할 수 있다.
④ 제1항부터 제3항까지의 규정에 따른 통지 및 조치에 필요한 사항은 대통령령으로 정한다.

- 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개) ① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
② 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제2호에 따른 정보통신서비스를 말한다. 이하 제3항에서 같다)를 이용하는 자는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제3호에 따른 정보통신서비스 제공자를 말한다. 이하 제3항에서 같다)에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
③ 과학기술정보통신부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 제1항 및 제2항에 따른 정보를 공개하도록 권고할 수 있다.
④ 과학기술정보통신부장관이 제3항에 따라 정보를 공개하도록 권고하려는 경우에는 미리 방송통신위원회의 의견을 들어야 한다.

- 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호) ① 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.
② 클라우드컴퓨팅서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우에는 다음 각 호의 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 이용자 정보를 제공받는 자
2. 이용자 정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 이용자 정보의 항목
4. 이용자 정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.
④ 클라우드컴퓨팅서비스 제공자는 사업을 종료하려는 경우에는 그 이용자에게 사업 종료 사실을 알리고 사업 종료일 전까지 이용자 정보를 반환하여야 하며 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 사업 종료일 전까지 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.
⑤ 제3항 및 제4항에도 불구하고 클라우드컴퓨팅서비스 제공자와 이용자 간의 계약으로 특별히 다르게 정한 경우에는 그에 따른다.
⑥ 제3항 및 제4항에 따른 이용자 정보의 반환 및 파기의 방법·시기, 계약 종료 및 사업 종료 사실의 통지 방법 등에 필요한 사항은 대통령령으로 정한다.

문 11. 인증기관이 사용자의 공개키에 대한 인증을 수행하기 위해 X.509 형식의 인증서를 생성할 때 서명에 사용하는 키는? 2

① 인증기관의 공개키
② 인증기관의 개인키
③ 사용자의 개인키
④ 인증기관과 사용자 간의 세션키

[해설]
- 공개키 인증서는 인증기관의 개인키로 전자서명 되어있으므로, 인증서 생성시 서명에 사용하는 키는 인증기관의 개인키이다.

문 12. 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은? 3

① 메시지는 대칭 암호 방식으로 암호화한다.
② 일반적으로 대칭 암호에 사용하는 세션키는 의사 난수 생성기로 생성한다.
③ 생성된 세션키는 무결성 보장을 위하여 공개키 암호 방식으로 암호화한다.
④ 메시지 송신자와 수신자가 사전에 공유하고 있는 비밀키가 없어도 사용할 수 있다.

[해설]
- 생성된 세션키는 기밀성 보장을 위하여 공개키 암호 방식으로 암호화한다.

문 13. 해시함수의 충돌저항성을 위협하는 공격 방법은? 1

① 생일 공격
② 사전 공격
③ 레인보우 테이블 공격
④ 선택 평문 공격

[해설]
- 충돌 저항성(Collision Resistance) : 같은 출력($h(x) = h(x')$)을 갖는 임의의 서로 다른 입력 x와 x′를 찾는 것이 계산상 어려워야 한다.
- 해시 길이가 n비트인 해시 함수가 역상 저항성과 제2 역상 저항성을 갖추기 위해서는 2n보다 효과적인 공격 기법이 없어야 한다. 즉, 역상 저항성과 제2 역상 저항성의 안전성은 n비트이다. 이에 반해, 충돌 저항성에 대한 안전성은 생일 공격에 의해 n/2비트이다. 따라서 우리가 일반적으로 고려하는 해시 함수는 충돌 저항성 공격에 안전한 해시 함수(충돌 저항 해시 함수)이다. 이에 대한 안전성은 n/2 비트이다.
- 생일 패러독스(birthday paradox) : 생일 문제(生日問題)란 확률론에서 유명한 문제로, 몇 명 이상 모이면 그 중에 생일이 같은 사람이 둘 이상 있을 확률이 충분히 높아지는지를 묻는 문제이다. 얼핏 생각하기에는 생일이 365~366가지이므로 임의의 두 사람의 생일이 같을 확률은 1/365~1/366이고, 따라서 365명쯤은 모여야 생일이 같은 사람이 있을 것이라고 생각하기 쉽다. 그러나 실제로는 23명만 모여도 생일이 같은 두 사람이 있을 확률이 50%를 넘고, 57명이 모이면 99%를 넘어간다. 이 사실은 일반인의 직관과 배치되기 때문에 생일 역설이나 생일 패러독스라고도 한다.

문 14. 블록 암호 운용 모드에 대한 설명으로 옳지 않은 것은? 3

① CFB는 블록 암호화를 병렬로 처리할 수 없다.
② ECB는 IV(Initialization Vector)를 사용하지 않는다.
③ CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록만 영향을 받는다.
④ CTR는 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.

[해설]
- CBC 모드는 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트에 에러가 발생한다.

문 15. 「개인정보 보호법」상 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은? 2

① 범죄의 예방 및 수사를 위하여 필요한 경우
② 공공기관의 장이 허가한 경우
③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
④ 시설안전 및 화재 예방을 위하여 필요한 경우

[해설]
- 개인정보 보호법 제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

문 16. SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는 데 악용될 수 있는 명령어는? 4

① HELO
② MAIL FROM

③ RCPT TO

④ VRFY

[해설]
- HELO : SMTP 송신자가 SMTP 세션을 초기화하기 위하여 SMTP 수신자 에게 보내는 전통적인 명령
- MAIL FROM : 송신자의 메일 주소를 통지
- RCPT TO : 수신자의 메일 주소를 통지
- VRFY : SMTP 수신자에게 편지함 사용이 가능한지를 확인하도록 요청

문 17. 다음 법 조문의 출처는? 3

> 제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

① 국가정보화 기본법

② 개인정보 보호법

③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

④ 정보통신산업진흥법

[해설]
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

문 18. 위조된 출발지 주소에서 과도한 양의 TCP SYN 패킷을 공격 대상 시스템으로 전송하는 서비스 거부 공격에 대응하기 위한 방안의 하나인, SYN 쿠키 기법에 대한 설명으로 옳은 것은? 3

① SYN 패킷이 오면 세부 정보를 TCP 연결 테이블에 기록한다.

② 요청된 연결의 중요 정보를 암호화하고 이를 SYN-ACK 패킷의 응답(acknowledgment) 번호로 하여 클라이언트에게 전송한다.

③ 클라이언트가 SYN 쿠키가 포함된 ACK 패킷을 보내오면 서버는 세션을 다시 열고 통신을 시작한다.

④ TCP 연결 테이블에서 연결이 완성되지 않은 엔트리를 삭제하는 데까지의 대기 시간을 결정한다.

[해설]
- SYNCOOKIE를 사용하게 되면 세션이 이루어지기 전에는 해당 세션에 대한 정보를 backlog queue 에 저장하지 않으므로 SYN Flooding 공격을 방어 할 수 있다.
- SYN 쿠키 기법은 SYN 패킷을 수신한 서버가 시간정보, 클라이언트 시작 순서번호, 클라이언트 IP 주소, 비밀번호 등을 입력값으로 해시값을 쿠키로 구한다.
- SYN 쿠키가 포함된 ACK 패킷을 보내오면 TCP 연결 테이블에 기록한다.

문 19. ISO/IEC 27001:2013 보안관리 항목을 PDCA 모델에 적용할 때, 점검(check)에 해당하는 항목은? 1

① 성과평가(performance evaluation)

② 개선(improvement)

③ 운영(operation)

④ 지원(support)

[해설]
- 성과평가(performance evaluation) : Check에 해당
- 개선(improvement) : Act에 해당
- 운영(operation) : Do에 해당
- 지원(support) : Plan에 해당

문 20. 다음에서 설명하는 블록체인 합의 알고리즘은? 3

> ○ 비트코인에서 사용하는 방식이 채굴 경쟁으로 과도한 자원 소비를 발생시킨다는 문제를 해결하기 위한 대안으로 등장하였다.
> ○ 채굴 성공 기회를 참여자에 따라 차등적으로 부여한다.
> ○ 다수결로 의사 결정을 해서 블록을 추가하는 방식이 아니므로 불특정 다수가 참여하는 환경에서 유효하다.

① Paxos

② PoW(Proof of Work)

③ PoS(Proof of Stake)

④ PBFT(Practical Byzantine Fault Tolerance)

[해설]
- PoW(Proof of Work, 작업 증명 알고리즘)은 가장 일반적으로 사용되는 블록체인 합의 알고리즘이다. 하지만, PoW는 시간이 지날수록 과도한 에너지 낭비 및 채굴의 독점화의 문제점이 발생하였고 이를 해결하기 위해 PoS(Proof of Stake, 지분 증명 알고리즘) 도입되었다.
- PoW 기반의 블록체인에서 블록의 유효성을 검증하고 새 블록을 만드는 과정을 채굴이라 한다면 PoS 기반의 블록체인에서는 단조(Forging)이라고 하며, 새로운 블록의 생성 및 무결성을 검증하는 검증자는 Validator라 한다.
- 블록생성의 조건이 PoW(Proof of Work, 작업 증명 알고리즘)은 연산능력이라 할 수 있지만, PoS(Proof of Stake, 지분 증명 알고리즘)은 보유지분이다. 또한 블록생성속도도 PoW은 느리지만, PoS는 빠르고 자원소모도 적다.