2017년 4월 8일 시행 9급 국가직 공무원 시험
정보보호론 문제와 해설

문 1. 컴퓨터 시스템 및 네트워크 자산에 대한 위협 중에서 기밀성 침해에 해당하는 것은?
① 장비가 불능 상태가 되어 서비스가 제공되지 않음
② 통계적 방법으로 데이터 내용이 분석됨
③ 새로운 파일이 허위로 만들어짐
④ 메시지가 재 정렬됨
[정답] ②
[해설]
① 장비가 불능 상태가 되어 서비스가 제공되지 않음 → 가용성 침해
③ 새로운 파일이 허위로 만들어짐 → 무결성 침해
④ 메시지가 재 정렬됨 → 무결성 침해

문 2. 공개키기반구조(PKI)에서 관리나 보안상의 문제로 폐기된 인증서들의 목록은?
① Online Certificate Status Protocol
② Secure Socket Layer
③ Certificate Revocation List
④ Certification Authority
[정답] ③
[해설]
① OCSP(Online Certificate Status Protocol) : CRL(인증서 폐지 목록)의 갱신 주기성 문제를 해결하기 위해 폐지나 효력 정지 상태를 파악하여 사용자가 실시간으로 인증서를 검증할 수 있는 프로토콜이다.
② SSL(Secure Socket Layer) : 웹서버와 웹브라우저에서 전달되는 데이터를 안전하게 송수신할 수 있도록 미국의 네스케이프 사가 개발된 프로토콜이다.
③ 인증서폐기목록(CRL : Certificate Revocation Rist) : 공개키기반구조(PKI)에서 관리나 보안상의 문제로 폐기된 인증서들의 목록으로 인증 기관(CA)은 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다.
④ 인증 기관(CA : Certification Authority) : 인증 업무를 수행하는 공공기관이며 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다.

문 3. AES 알고리즘의 블록크기와 키길이에 대한 설명으로 옳은 것은?
① 블록크기는 64비트이고 키길이는 56비트이다.
② 블록크기는 128비트이고 키길이는 56비트이다.
③ 블록크기는 64비트이고 키길이는 128/192/256비트이다.
④ 블록크기는 128비트이고 키길이는 128/192/256비트이다.
[정답] ④
[해설]
■ AES(Advanced Encryption Standard) 알고리즘 – SPN 암호 구조
- AES는 미국의 연방 표준 알고리즘으로 DES를 대신할 차세대 표준 알고리즘이다.
- 암호화 과정과 복호화 과정이 다른 SPN 암호 구조이다.

- 128비트 크기의 입·출력 블록을 사용하고, 128/192/256비트의 가변크기 키 길이를 제공한다.
- 라운드 횟수는 한 번의 암·복호화를 반복하는 라운드 함수의 수행 횟수이고, 10/12/14 라운드 수로 이루어져 있다.

키 길이	회전 수
128비트	10
192비트	12
256비트	14

문 4. 우리나라 국가 표준으로 지정되었으며 경량 환경 및 하드웨어 구현에서의 효율성 향상을 위해 개발된 128비트 블록암호 알고리즘은?

① IDEA
② 3DES
③ HMAC
④ ARIA

[정답] ④

[해설]

■ IDEA(International Data Encryption Algorithm) – Feistel 암호 구조
- 1991년에 제작된 블록 암호이며, 국제 데이터 암호화 알고리즘이다.
- 64비트의 블록에 고정된 128비트의 키를 이용하며, 8라운드로 구성되어 있다.
- 64비트 블록 암호화 알고리즘 중에는 가장 안전하고, 뛰어나다고 평가를 받는다.
- 하나의 블록을 177Mbps의 빠른 속도로 암호화한다.
- 0이 많이 들어간 키 같은 특정키에 대해서는 취약하다.

■ 3DES
- DES의 보안 강화를 위해 3번의 암호화 혹은 복호화 과정을 수행한다.
- 3개의 키 k_1, k_2, k_3을 선택하고, 평문 M을 DES의 암호화 함수를 3번 수행하여 암호화한다.
- 2개의 키 k_1, k_2을 선택하고, 평문 M을 DES의 암호화 함수와 복호화 함수를 수행하여 암호화한다.
- 3개의 키 k_1, k_2, k_3을 선택하고, 평문 M을 DES의 암호화 함수와 XOR를 이용하여 암호화한다.

■ HMAC(Hash-based Message Authentication Code)
- 해시 기반 메시지 인증 코드로 체크섬을 변경하는 것을 불가능하도록 한 MAC 기반의 메시지 인증 알고리즘이다.

문 5. '정보시스템과 네트워크의 보호를 위한 OECD 가이드라인' (2002)에서 제시한 원리(principle) 중 "참여자들은 정보시스템과 네트워크 보안의 필요성과 그 안전성을 향상하기 위하여 할 수 있는 사항을 알고 있어야 한다."에 해당하는 것은?

① 인식(Awareness)
② 책임(Responsibility)
③ 윤리(Ethics)
④ 재평가(Reassessment)

[정답] ①

[해설]

■ 정보시스템과 네트워크의 보호를 위한 OECD 가이드라인 (2002년)

① 인식(Awareness): 참여자들은 정보시스템 및 네트워크의 보안 필요성과 보안을 강화하기 위해 자신이 할 수 있는 일이 무엇인지 인식하고 있어야 함
② 책임(Responsibility): 모든 참여자들은 정보시스템 및 네트워크의 보안에 대해 책임을 짐
③ 대응(Response): 참여자들은 보안사고를 예방하거나 탐지하고 대응하는데 있어서 시기 적절하고 협조적인 방법으로 행동하여야 함
④ 윤리(Ethics): 참여자들은 타인의 정당한 이해관계를 존중해야 함
⑤ 민주주의(Democracy): 정보시스템과 네트워크의 보안은 민주사회의 기본가치에 걸맞아야 함
⑥ 위험분석(Risk assessment): 참여자들은 위험분석을 수행해야 함
⑦ 보안설계 및 시행(Security design and implementation): 참여자들은 보안을 정보시스템 및 네트워크의 필수적인 요소로 포함시켜야 함
⑧ 보안관리(Security management): 참여자들은 보안관리를 위한 종합적인 접근방식을 채택 해야 함
⑨ 재평가(Reassessment): 참여자들은 정보시스템 및 네트워크의 보안을 검토하고 재평가하여 보안에 관한 정책, 관행, 수단, 절차에 대해 적정한 수정을 하여야 함

문 6. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 정보통신 서비스 제공자등이 이용자 개인정보의 국외 이전을 위한 동의 절차에서 이용자에게 고지해야 할 사항에 해당하지 않는 것은?

① 이전되는 개인정보 항목
② 개인정보가 이전되는 국가, 이전일시 및 이전방법
③ 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간
④ 개인정보를 이전하는 자의 성명(법인인 경우는 명칭 및 정보 관리책임자의 연락처)

[정답] ④

[해설]

■ 제63조(국외 이전 개인정보의 보호)

① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.
② 정보통신서비스 제공자등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다.
③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

문 7. IPSec에서 두 컴퓨터 간의 보안 연결 설정을 위해 사용되는 것은?

① Authentication Header
② Encapsulating Security Payload
③ Internet Key Exchange
④ Extensible Authentication Protocol

[정답] ③

[해설]

① 인증 헤더(AH : Authentication Header) : 패킷의 무결성을 위해 송신자의 인증을 허용한다. 단말과 라우터 간의 IP 패킷에 대한 송신 인증 및 무결성 서비스를 제공한다.

② 보안 페이로드 캡슐화(ESP : Encapsulating Security Payload) : IP 패킷의 비밀성을 위해 송신자의 인증 및 데이터 암호화를 지원한다. ESP는 데이터의 비밀성을 제공하는데, 암호화되어 있지만 인증되지 않은 데이터 스트림에 대한 공격을 막기 위해 AH의 모든 기능이 포함되어 있다. IP 데이터그램에서 제공하는 선택적 인증과 무결성, 기밀성 그리고 재전송 공격 방지 기능을 한다. 터널 종단 간에 협상된 키와 암호화 알고리즘으로 데이터그램을 암호화한다.

③ IKE(Internet Key Exchange) : AH, ESP와 함께 암호화 키를 관리, SA를 협의하기 위해 어플리케이션 계층에서 사용하는 프로토콜이다. 동일한 암호 키를 오랫동안 사용하면 공격자에게 노출이 되므로, IKE는 공개키 기반으로 안전하게 키 관리를 하기 위한 방법이다. 주로 RSA와 Diffie-Hellman 등의 암호 기술을 사용한다.

④ 확장성 인증 프로토콜(Extensible Authentication Protocol) : 무선 및 점대점 프로토콜에서 사용되며 확장이 용이하도록 고안된 인증 방법이다. MD5, OTP, 스마트 카드 같은 인증 방식의 사용을 지원한다.

문 8. 다음 설명에 해당하는 것은?

> PC나 스마트폰을 해킹하여 특정 프로그램이나 기기 자체를 사용하지 못하도록 하는 악성코드로서 인터넷 사용자의 컴퓨터에 설치되어 내부 문서나 스프레드시트, 이미지 파일
> 등을 암호화하여 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구한다.

① Web Shell
② Ransomware
③ Honeypot
④ Stuxnet

[정답] ②

[해설]

① Web Shell(웹쉘) : 웹프로그램이 취약한 서버를 악의적인 코드 이용하여 관리자의 권한을 획득하는 방법이다.

③ Honeypot(허니팟) : '해커 잡는 덫'이란 뜻의 용어로, 공격자(크래커, 해커)를 잡는 유혹의 꿀단지라는 의미가 있는 용어이다. 컴퓨터 정보를 유출하거나 변조하여 일부러 취약점을 드러낸다. 중요한 시스템을 보호하기 위해서 잠재적 공격자를 유혹 한다. 가상으로 공격자의 침입을 유도해 신분을 확보하며 위장 서버와 추적 장치를 활용해 공격자 서버를 찾아낸다.

④ Stuxnet(스턱스넷) : 2010년 6월에 발견된 웜 바이러스로 MS-Windows를 통해 감염되어, 지멘스 산업의 소프트웨어 및 장비를 공격한다. 스턱스넷은 산업시설을 감시하고 파괴하는 악성 소프트웨어로는 최초이다.

문 9. 개인정보 보호법 시행령 상 개인정보처리자가 하여야 하는 안전성 확보 조치에 해당하지 않는 것은?

① 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
② 개인정보가 정보주체의 요구를 받아 삭제되더라도 이를 복구 또는 재생할 수 있는 내부 방안 마련
③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
[정답] ②
[해설]
■ 제30조(개인정보의 안전성 확보 조치)
① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

② 행정자치부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.
③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다.

문 10. 공개키 암호시스템에 대한 설명 중 ㉠~㉢에 들어갈 말로 옳게 짝지어진 것은?

○ (㉠)의 안전성은 유한체의 이산대수 계산의 어려움에 기반을 둔다.
○ (㉡)의 안전성은 타원곡선군의 이산대수 계산의 어려움에 기반을 둔다.
○ (㉢)의 안전성은 소인수분해의 어려움에 기반을 둔다.

	㉠	㉡	㉢
①	ElGamal 암호시스템	DSS	RSA 암호시스템
②	Knapsack 암호시스템	ECC	RSA 암호시스템
③	Knapsack 암호시스템	DSS	Rabin 암호시스템
④	ElGamal 암호시스템	ECC	Rabin 암호시스템

[정답] ④
[해설]
- DSS : ElGamal 서명을 개량한 방식이다.
- Knapsack 암호시스템 : 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 방법이다.

문 11. 가상사설망에서 사용되는 프로토콜이 아닌 것은?
① L2F
② PPTP
③ TFTP
④ L2TP
[정답] ③
[해설]
- VPN(가상사설망)은 공중 데이터망인 인터넷을 사설망처럼 이용해 회선비용을 크게 절감할 수 있는 기업통신 서비스를 말한다. VPN은 기본적으로 패킷을 캡슐화하거나 두 네트워크 간의 전용 회선을 확보할 수 있는 터널과 암호화 기법 등이 필요하다.

① L2F(Layer 2 Forwarding) : 미국의 시스코사 개발한 터널용 프로토콜로 데이터링크의 캡슐화가 가능하고, IP 프로토콜 이외에도 사용할 수 있는 융통성이 있는 프로토콜이다.
② PPTP(Point-to-Point Tunneling Protocol) : PPP에 기초하며 두 대의 컴퓨터가 직렬 인터페이스를 이용하여 통신할 때 사용한다. 전화선을 통해 인터넷에 연결하는 경우에 주로 사용되었다. 컴퓨터와 컴퓨터가 1:1 연결된 방식에서 데이터를 전송 시에 보안을 유지하면서 VPN을 지원해주는 프로토콜이다.
③ TFTP(간이 FTP, Trivial File Transfer Protocol) : TFTP는 사용자 인증을 제공하지 않는 프로토콜로 부팅 서버의 사용을 위해서 개발되었다. TFTP는 사용자 인증과정을 거치지 않고 곧바로 원격 파일을 읽거나 저장할 수 있는 프로토콜이다. FTP보다 사용은 단순하고, 기능이 좀 떨어지는 파일 전송 프로토콜이다. TFTP는 TCP보다는 UDP을 사용한다.
④ L2TP(Layer 2 Tunneling Protocol) : 미국의 시스코가 제안한 L2F(Layer 2 Forwarding)와 PPTP가 결합된 프로토콜로 PPTP는 하나의 터널만 지원하는 것에 비해 L2TP는 서로 다른 터널을 이용할 수 있으며, 헤더를 압축하거나 터널에 대한 인증 기능을 제공한다.

문 12. 메모리 영역에 비정상적인 데이터나 비트를 채워 시스템의 정상적인 동작을 방해하는 공격 방식은?
① Spoofing
② Buffer overflow
③ Sniffing
④ Scanning
[정답] ②
[해설]
① Spoofing : 위장한다.
③ Sniffing : 훔쳐본다.
④ Scanning : 공격시스템 공격하기 위해 취약 정보를 확인한다.

문 13. 시스템과 관련한 보안기능 중 적절한 권한을 가진 사용자를 식별하기 위한 인증 관리로 옳은 것은?
① 세션 관리
② 로그 관리
③ 취약점 관리
④ 계정 관리
[정답] ④
[해설]
■ 시스템과 관련한 보안 기능
- 계정과 패스워드 관리 : 적절한 권한을 가진 사용자를 식별하기 위한 인증 관리로 계정과 패스워드 관리가 보안의 시작이다.
- 세션 관리 : 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대한 관리 일정 시간이 지날 경우 적절히 세션을 종료하고, 비 인가자에 의한 세션 가로채기를 통제한다.
- 접근 제어 : 시스템이 네트워크 안에서 다른 시스템으로부터 적절히 보호될 수 있도록 네트워크 관점에서 접근을 통제한다.
- 권한 관리 : 시스템의 각 사용자가 적절한 권한으로 적절한 정보 자산에 접근할 수 있도록 통제한

다.

- 로그 관리 : 시스템 내부 혹은 네트워크를 통한 외부에서 시스템에 어떤 영향을 미칠 경우 해당 사항을 기록한다.
- 취약점 관리 : 시스템은 계정과 패스워드 관리, 세션 관리, 접근 제어, 권한 관리 등을 충분히 잘 갖추고도 보안적인 문제가 발생할 수 있다. 이는 시스템 자체의 결함에 의한 것으로 이 결함을 체계적으로 관리하는 것이 취약점 관리이다.

문 14. 무선랜을 보호하기 위한 기술이 아닌 것은?
① WiFi Protected Access Enterprise
② WiFi Rogue Access Points
③ WiFi Protected Access
④ Wired Equivalent Privacy
[정답] ②
[해설]
① WiFi Protected Access Enterprise : WPA방식에는 Personal과 Enterprise가 있으며 가정에서는 Personal, 기업이나 학교 에서는 장비가 추가로 필요한 Enterprise 버젼을 사용한다.
② WiFi Rogue Access Points : WiFi 악의적 액세스 포인트를 말한다. 관리자가 악의적인 목적으로 액세스 포인트에 권한을 부여하지 않거나 공격자가 추가한 악의적인 액세스 포인트이다.
③ WPA(Wi-Fi Protected Access) : WPA는 WEP 표준의 문제점을 보완하여 개발되었으며 2003년 Wi-Fi 보안 표준으로 변경되었다. WPA 방식은 48비트 길이의 초기벡터(IV)를 사용하며서 사용된 키는 WEP 방식의 64, 128비트보다 큰 256비트로 암호화한다.
④ WEP(Wired Equivalent Privacy) : 무선 통신 초기에 가장 널리 사용되는 Wi-Fi 보안 알고리즘으로 대부분의 접근 설정에서 암호화 방식 선택 시 가장 먼저 표시되었던 암호화 기술이다. WEP은 무선 LAN에 연결된 기기와 AP가 서로 주고받는 패킷을 64비트 혹은 128비트로 암호화하지만 공격에 취약하며 보안성이 약하다.

문 15. 다음 정보통신 관계 법률의 목적에 대한 설명으로 옳지 않은 것은?
① 정보통신기반 보호법 은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운영하도록 하여 국가의 안전과 국민 생활의 안정을 보장하는 것을 목적으로 한다.
② 전자서명법 은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다.
③ 통신비밀보호법 은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.
④ 정보통신산업 진흥법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.
[정답] ④
[해설]
④번은 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 목적이다.

- 정보통신산업 진흥법 : 정보통신산업의 진흥을 위한 기반을 조성함으로써 정보통신산업의 경쟁력

을 강화하고 국민경제의 발전에 이바지함을 목적으로 한다.

문 16. 위험분석 및 평가방법론 중 성격이 다른 것은?
① 확률 분포법
② 시나리오법
③ 순위결정법
④ 델파이법
[정답] ①
[해설]
■ 정량적 기법
- 모든 개념을 “양”혹은 “수치”로 요소를 평가한다.
- 방법론 : 수학 공식 접근법, 확률 분포 추정법, 몬테칼로 시뮬레이션, 과거 자료 분석법, 점수법 등이 있다.

■ 정성적 기법
- 모든 개념을 “성질”, “질적”인 요소를 평가한다.
- 방법론 : 델파이법, 이야기식 시나리오 법, 순위 결정법, 퍼지 행렬법, 질문 서법 들이 있다.

문 17. 보안 침해 사고에 대한 설명으로 옳은 것은?
① 크라임웨어는 온라인상에서 해당 소프트웨어를 실행하는 사용자가 알지 못하게 불법적인 행동 및 동작을 하도록 만들어진 프로그램을 말한다.
② 스니핑은 적극적 공격으로 백도어 등의 프로그램을 사용하여 네트워크상의 남의 패킷 정보를 도청하는 해킹 유형의 하나이다.
③ 파밍은 정상적으로 사용자들이 접속하는 도메인 이름과 철자가 유사한 도메인 이름을 사용하여 위장 홈페이지를 만든 뒤 사용자로 하여금 위장된 사이트로 접속하도록 한 후 개인 정보를 빼내는 공격 기법이다.
④ 피싱은 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.
[정답] ①
[해설]
틀린 설명을 올바르게 고치면 다음과 같다.
② 스니핑은 소극적 공격 방법이다.
③ 사용자들이 접속하는 도메인 이름과 철자가 유사한 도메인 이름이 아니라 도메인 이름이 동일하게 만든다.
④ 피싱(Phishing)은 Phishing은 개인정보와 낚시의 합성어로, 정상 웹서버를 해킹하여 위장사이트를 만들어 놓고 네티즌들이 프로그램을 내려 받도록 하거나 E-메일을 이용하여 개인 정보를 빼내어 범죄에 악용하는 행위를 일컫는다.

문 18. 다음 설명에 해당하는 것은

○ 응용 프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 말한다. ○ 컴퓨터 메모리에서 애플리케이션 호스트 시스템에 해를 끼치지 않고 작동하는 것이 허락된 보호받는 제한 구역을 가리킨다.

① Whitebox
② Sandbox
③ Middlebox
④ Bluebox
[정답] ②
[해설]
■ 샌드박스(Sandbox)
아이들을 모래밭(샌드 박스)의 밖에서 놀리지 않는다는 의미로 보호된 영역 내에서 여러 응용 프로그램을 동작시키는 것으로, 외부 요인에 의해 악영향이나 공격자로부터 방어를 목적으로 하는 보안 모델이다.

문 19. 각 주체가 각 객체에 접근할 때마다 관리자에 의해 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 주체에게만 접근 권한을 부여하는 기법은?
① Mandatory Access Control
② Discretionary Access Control
③ Role Based Access Control
④ Reference Monitor
[정답] ①
[해설]
② DAC(Discretionary Access Control, 임의 접근제어) : 가장 널리 사용되는 모델로 오늘날 대부분의 운영체제에서 채택하여 사용하고 있다. 파일, 디렉토리의 소유자가 사용자나 사용자 그룹에 따라서 임의적으로 접근을 제어하는 방식이다. 정보 소유자가 정보의 보안 레벨을 결정 하고 이에 대한 정보의 접근제어를 설정하는 모델이다.
③ RBAC(Role-Based Access Control, 역할 기반 접근제어) : 특정 역할들을 정의하고 각 역할에 따라 접근 권한을 지정하고 제어하는 방식이다. 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙들에 기반을 둔다. 조직의 사용자가 수행해야 하는 직무와 직무 권한 등급을 기준으로 객체에 대한 접근을 제어한다. 접근 권한은 직무에 허용된 연산을 기준으로 허용함으로 조직의 기능 변화에 따른 관리적 업무의 효율성을 높일 수 있다.
④ Reference Monitor : 사용자가 특정 보안 영역에 액세스 하거나 사용할 권리가 있는지, 접속 확인과 사용자 인증을 위한 감사를 시행하며 관리한다.

문 20. 임의로 발생시킨 데이터를 프로그램의 입력으로 사용하여 소프트웨어의 안전성 및 취약성 등을 검사하는 방법은?
① Reverse Engineering
② Canonicalization
③ Fuzzing
④ Software Prototyping
[정답] ③

[해설]

■ Fuzzing

소프트웨어에 있는 버그를 찾아내는 방법으로 소프트웨어가 오류가 발생할 수 있도록 비정상적인 데이터를 전달하여 검사한다. 방법에는 새로운 데이터를 생성해 전달하는 방식인 Generation Fuzzer과 기존 데이터를 변형하여 전달하는 방식인 Mutation Fuzzer가 있다.

① Reverse Engineering(역공학) : 소프트웨어 소스를 분석하여 설계서를 만든다.

② Canonicalization(정규화) : 정보 기술에서 표준 규격에 맞도록 만드는 과정으로 데이터의 규정 일치를 확인하여 비정규 데이터를 정규 데이터로 만드는 작업이다.

④ Software Prototyping(소프트웨어 프로토타입) : 아파트의 모델하우스처럼 소프트웨어 개발 전에 사용자가 쉽게 이해할 수 있도록 만든 임시적으로 소프트웨어이다.