

2017 년 국가직 9 급 정보보호론 풀이

by 호이호이꿀떡



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 재정렬됨

답 ②

- ② 내용이 분석되었다는 것은 드러내지 않았던 정보가 알려졌다는 얘기이므로, 기밀성 침해에 해당한다.
- ① 가용성 침해
 - ③ 위조(fabrication) -> 무결성 침해
 - ④ 메시지 순서가 임의로 조작, 변조(modification) -> 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

답 ③

- ③ Certificate Revocation Rist(CRL, 인증서 폐기 목록)

CA(인증기관)이 발행

- 인증서 취소 사유

사용자 개인키가 노출되었거나 훼손된 경우

CA 가 사용자를 더 이상 인증해줄 수 없는 경우

CA 의 인증서가 노출되었거나 훼손된 경우

- ① Online Certificate Status Protocol(OCSP, 온라인 인증서 상태 프로토콜)

공개키 인증서의 폐지나 효력 정지 상태를 실시간으로 검증할 수 있는 프로토콜

- ② Secure Socket Layer(SSL)

인터넷 상에서 데이터를 안전하게 전송할 수 있도록 해주는 프로토콜이다.

- ④ Certification Authority(CA, 인증기관)

공개키 인증서와 인증서 폐기목록을 생성하고 발급

문 3. AES 알고리즘의 블록크기와 키길이에 대한 설명으로 옳은 것은?

- ① 블록크기는 64 비트이고 키길이는 56 비트이다.
- ② 블록크기는 128 비트이고 키길이는 56 비트이다.
- ③ 블록크기는 64 비트이고 키길이는 128/192/256 비트이다.
- ④ 블록크기는 128 비트이고 키길이는 128/192/256 비트이다.

답 ④

AES(Advanced Encryption Standard)

SPN 구조

블록 128 비트(16 바이트)

키 길이 128 비트 - 10 라운드

키 길이 192 비트 - 12 라운드

키 길이 256 비트 - 14 라운드

DES(Data Encryption Standard)

페이스텔(Fiestel) 구조

블록 64 비트

키 길이 56 비트 + 패리티 8 비트 = 64 비트

16 라운드

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

- ① IDEA
- ② 3DES
- ③ HMAC
- ④ ARIA

답 ④

④ 국산 블록암호 알고리즘

- SEED - 한국정보보호진흥원

128 비트 블록

키 길이 128 또는 256 비트

페이스텔 구조 16 라운드

국내 전자상거래에 이용

- ARIA

128 비트 블록

키 길이 128/192/256 비트

Involutional SPN 구조 12/14/16 라운드

KS 국가 표준, 효율성에 맞게 최적화, 다양한 환경에 적합

- HIGHT

64 비트 블록

키 길이 128 비트

페이스텔 변형 구조 32 라운드(간단한 알고리즘)

제한적 자원의 환경 하에서 구현 가능

① IDEA

64 비트 블록, 키 길이 128 비트, 8 라운드

② 3DES

보안 강화를 위해 DES 를 3 번 반복한다.

3 개를 키(k1, k2, k3)를 사용하여,

k1 으로 암호화 -> k2 로 복호화 -> k3 로 암호화를 진행하는 방식

③ HMAC(Hash-based Message Authentication Code, 해시 기반 메시지 인증 코드)

키를 이용한 메시지 인증 코드로, 패딩 등을 이용하여 MAC 보다 더 복잡하다.

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)

답 ①

※ 정보시스템과 네트워크의 보호를 위한 OECD 가이드라인

- 1) 인식
참여자들은 정보시스템과 네트워크 보호의 필요성과 그 안전성을 향상시키기 위하여 취할 수 있는 사항을 알고 있어야 한다.
- 2) 책임
모든 참여자들은 정보시스템과 네트워크의 보호에 책임이 있다.
- 3) 대응
참여자들은 정보보호사고를 정보보호사고를 예방, 탐지, 대응하기 위해서 적기에 협력해서 행동해야 한다.
- 4) 윤리
참여자들은 타인의 적법한 이익을 존중해야 한다.
- 5) 민주성
정보시스템과 네트워크의 보호는 민주주의 사회의 근본적인 가치들에 부합하여야 한다.
- 6) 위험평가
참여자들은 위험평가를 시행해야 한다.
- 7) 정보보호의 설계와 이행
참여자들은 정보보호를 정보시스템과 네트워크의 핵심요소로 수용하여야 한다.
- 8) 정보보호 관리
참여자들은 정보보호관리에 정보보호관리에 대해 포괄적인 접근방식을 채택해야 한다.
- 9) 재평가
참여자들은 정보시스템과 네트워크의 보호를 검토하고 재평가하여 정보보호 정책, 관행, 조치, 절차를 적절히 수정해야 한다.

문 6. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상 정보통신 서비스 제공자등이 이용자 개인정보의 국외 이전을 위한 등의 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·이용기간
- ④ 개인정보를 이전하는 자의 성명(법인인 경우는 명칭 및 정보 관리책임자의 연락처)

답 ④

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제 63 조(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 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제 3 항 각 호의 사항 모두를 제 27 조의 2 제 1 항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.
- ③ 정보통신서비스 제공자등은 제 2 항에 따른 동의를 받으면 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 제 2 항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

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

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

답 ③

③ Internet Key Exchange(IKE, 인터넷 키 교환)

세션키 교환 프로토콜

RSA 와 디피 헬만 등의 공개키 기술을 기반으로, 암호화에 사용할 세션키를 관리하고 SA(보안 연계)를 협의하기 위한 프로토콜이다.

- ① Authentication Header(AH, 인증 헤더)
메시지 인증을 무결성 제공
- ② Encapsulating Security Payload(ESP, 캡슐화 보안 페이로드)
대칭키 암호화를 통해, 기밀성과 무결성과 선택적 인증 제공
- ④ Extensible Authentication Protocol
복수의 인증 프로토콜을 캡슐화시킬 수 있게 하여, 다양한 인증방식을 선택 가능하게 하는 범용의 인증 프레임워크로, 무선 네트워크와 점대점 연결에 자주 사용된다.

문 8. 다음 설명에 해당하는 것은?

PC 나 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 준다면 금품을 요구한다.

- ① Web Shell
- ② Ransomware
- ③ Honeypot
- ④ Stuxnet

답 ②

② 랜섬웨어(Ransomware)

인질의 몸값을 뜻하는 ransom 과 제품을 뜻하는 ware 의 합성어

컴퓨터에 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.

- ① 웹 셸(Web Shell)
공격자가 공격 대상 서버에 악의적으로 제작한 스크립트 파일을 업로드하여 관리자 권한을 획득하는 해킹법이다.
주소 asp, php, jsp, cgi 등 웹스크립트 파일을 통해 이루어진다.
- ③ 허니 팻(honeypot)
비정상적인 접근을 탐지하기 위해 의도적으로 설치해 둔 시스템
컴퓨터에 중요한 정보가 있는 것처럼 꾸며 공격자가 해당 컴퓨터를 공격하도록 한 뒤, 이를 통해 취약점과 공격 방법, 공격자의 패턴 등을 탐지할 수 있다.
- ④ 스텍스넷(Stuxnet)
독일 지멘스사의 원격 감시 제어 시스템인 SCADA 의 제어 소프트웨어 및 장비를 공격한다. 스텍스넷은 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

답 ②

- ② 정보주체의 요구로 개인정보를 삭제했는데, 복구나 재생이 가능하다면 개인정보가 의도치 않게 남용될 가능성이 있다.

「개인정보 보호법 시행령」

제 30 조(개인정보의 안전성 확보 조치)

- ① 개인정보처리자는 법 제 29 조에 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 행정안전부장관은 개인정보처리자가 제 1 항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. <개정 2013.3.23., 2014.11.19., 2017.7.26.>
- ③ 제 1 항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 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 |

답 ④

• 비대칭키 암호(공개키 암호)

RSA : 소인수분해

Rabin : 소인수분해

ElGamal : 이산대수

ECC : 타원곡선 상의 이산대수

Schnorr : 이산대수, ElGamal 에 기반, 짧은 키 길이

DSA : 이산대수, Schnorr 의 응용

DSS : 이산대수, 전자서명 전용

ECDSA : 내부적으로 타원곡선

Knapsack : 부분집합의 합을 구하는 문제(NP-complete 문제)

KCDSA : 국산, 국내표준

ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

문 11. 가상사설망에서 사용되는 프로토콜이 아닌 것은?

- ① L2F ② PPTP
- ③ TFTP ④ L2TP

답 ③

계층별 보안 프로토콜

PPTP - 2 계층

L2F - 2 계층

L2TP - 2 계층

IPSec - 3 계층

SSL/TLS - 4 계층

SOCKSv5 - 5 계층

SSH(Secure Shell) - 7 계층(telnet 이나 FTP 를 암호화)

- ③ TFTP(Trivial File Transfer Protocol, 간이 파일 전송 프로토콜)
파일 전송 프로토콜인 FTP의 간단 버전으로, FTP는 TCP를 사용하는 반면, TFTP는 UDP를 사용하여 인증 과정이 없어 보안에 취약하다.

문 12. 메모리 영역에 비정상적인 데이터나 비트를 채워 시스템의 정상적인 동작을 방해하는 공격 방식은?

- ① Spoofing
- ② Buffer overflow
- ③ Sniffing
- ④ Scanning

답 ②

- ② 버퍼 오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.
- ① Spoofing(스푸핑)이란 네트워크 상에서 자신의 신분을 속이거나 다른 사용자로 위장해 공격 대상에 불법 접근하여 정보를 빼내는 것이다.
- ③ Sniffing(스니핑)은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 말한다.
- ④ Scanning(스캐닝)은 공격대상이나 서버를 공격하기에 앞서 공격 대상에 대한 취약점 등의 정보를 수집하기 위한 활동을 말한다.

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

답 ④

- ④ 사용자가 적절한 권한을 가졌는지 식별하는 것이기 때문에, 사용자에 대한 정보가 담긴 계정에 대한 관리이다.

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

답 ②

- ② WiFi Rogue Access Points(불법 액세스 포인트)
해커가 악의적인 목적을 가지고 정상적인 AP 인 척 설치한 불법 액세스 포인트이다.
- ① WiFi Protected Access Enterprise(WPA Enterprise)
무선랜 인증 및 암호화 기술인 WPA 의 기업 모드
- ③ WiFi Protected Access(WPA)
- ④ Wired Equivalent Privacy(WEP)

WEP 방식: 암호화를 위해 RC4 사용하며(암호키 계속 사용), 암호화와 인증에 동일한 키를 사용

WPA 방식: RC4-TKIP 를 통한 암호화(암호키 주기적인 변경), EAP 를 통한 사용자 인증

48 비트 길이의 초기벡터(IV) 사용

WPA2 방식: AES-CCMP 사용, EAP 를 통한 사용자 인증

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 진흥법」은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

답 ④

④번의 내용은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 목적이다.

법 조문을 달달 외우지 않더라도, 문장에 '개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성' 부분을 통해, 정보통신 사업자보다 이용자의 보호를 중시하는 내용임을 추론할 수 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 1 조 (목적)

이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

① 「정보통신기반 보호법」 제 1 조(목적)

이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

② 「전자서명법」 제 1 조(목적)

이 법은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을

정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다.

③ 「통신비밀보호법」 제 1 조(목적)

이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.

④ 「정보통신산업 진흥법」 제 1 조(목적)

이 법은 정보통신산업의 진흥을 위한 기반을 조성함으로써 정보통신산업의 경쟁력을 강화하고 국민경제의 발전에 이바지함을 목적으로 한다.

문 16. 위험분석 및 평가방법론 중 성격이 다른 것은?

- ① 확률 분포법
- ② 시나리오법
- ③ 순위결정법
- ④ 델파이법

답 ①

정량적 위험 분석: 위험의 크기를 수치로 계산

ALE(연간 예상 손실) 계산법

과거 자료 분석법

수학 공식 접근법

① 확률 분포법

몬테칼로 시뮬레이션

점수법

정성적 위험 분석: 위험의 크기를 개략적으로 판단

④ 델파이법

② 시나리오법

③ 순위 결정법

퍼지 행렬법

질문서법

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 개인정보를 빼내는 공격 기법이다.
- ④ 피싱은 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.

답 ①

① **크라임웨어(crimeware)**는 범죄(crime)와 제품(ware)의 합성어로, 스파이웨어, 브라우저 하이잭커, 키로거 등 온라인상에서 불법 활동을 조장하기 위해 만들어진 컴퓨터 프로그램들을 총칭하는 용어다.

② **스니핑(sniffing)**은 다른 상대방들의 패킷 교환을 엿듣는 것은 맞지만, 적극적 공격이 아닌 **소극적 공격**에 해당한다.

③ **피싱(phishing)**에 대한 설명이다.

파밍(pharming)은 사용자가 자신의 웹 브라우저에서 올바른 도메인을 입력해도 가짜 웹 페이지에 접속하게 하여 개인정보를 훔치는 것이다.

④ **파밍(pharming)**에 대한 설명이다.

피싱(phishing)은 인터넷 사용자에게 가짜 도메인을 알려주어, 가짜 사이트로 접속을 유도하는 공격이다.

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 제한구역을 가리킨다.

- ① Whitebox
- ② Sandbox
- ③ Middlebox
- ④ Bluebox

답 ②

② 샌드박스(Sandbox)

프로그램이나 코드를 실행할 때, 격리된 공간(샌드박스)를 제공하고 그곳을 벗어나 허용되지 않은 작업을 하지 못하도록 방지하는 기술
원래의 운영체제와 완전히 독립되어 실행되기 때문에 보안에 유리하다.

① 화이트박스 검사(White-box testing)

응용 프로그램의 내부 구조와 동작을 검사하는 소프트웨어 테스트 방식

블랙박스 검사(Black-box testing)

소프트웨어를 내부 구조나 작동 원리를 모르는 상태에서 입력과 출력 등 소프트웨어의 실행 결과물을 검사하는 소프트웨어 테스트 방식

③ 미들박스(Middlebox)

네트워크 제공자와 이용자 중간에서 각종 부가 기능을 제공하는 기기나 소프트웨어(SW)

④ 블루박스(Bluebox)

애플의 공동창업자인 스티브 워즈니악이 학창 시절 공중 전화기에 돈을 넣지 않고 무료 통화를 사용할 수 있게 개발한 기기이다. 세계 최초의 해킹 툴로 평가받는다.

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

답 ①

① Mandatory Access Control(MAC, 강제적 접근 제어)

오직 관리자만이 객체와 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안레벨에 기반한다.

관리자가 규칙을 작성하기 때문에 **규칙 기반 접근 제어(Rule Based Access Control)**이라고도 한다.

② Discretionary Access Control(DAC, 임의적 접근 제어)

정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

③ Role Based Access Control(RBAC, 역할 기반 접근 제어)

정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

④ Reference Monitor(참조 모니터)

모든 접근 요청이 지나쳐야하는 하나의 구간으로, 보안 커널 데이터베이스(SKDB)를 참조하여 객체에 대한 접근허가 여부를 결정한다.

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

답 ③

- ③ Fuzzing(퍼징)은 컴퓨터 프로그램에 유효한, 예상치 않은 또는 무작위 데이터를 입력하여, 프로그램의 충돌이나 빌트인 코드 검증의 실패, 잠재적인 메모리 누수 발견 등 소프트웨어의 버그를 찾아내는 방법이다.
- ① Reverse Engineering(역공학)은 완성된 장치나 소프트웨어를 분석하여 기술적인 원리나 내부 구조를 발견하는 과정이다.
- ② Canonicalization(정규화)은 IT 에서 규격에 맞도록 만드는 과정. 데이터의 규정 일치와 검증된 형식을 확인하고, 비정규 데이터를 정규 데이터로 만드는 것이다.
- 데이터베이스에서의 정규화는 DB normalization 이라 한다.
- ④ Software Prototyping(소프트웨어 프로토타입 모델)
- 소프트웨어 개발 접근법의 하나로, 개발 초기에 시스템의 모형인 프로토타입(prototype)을 제작해 사용자에게 보여주고 사용자가 정보시스템을 직접 테스트한 뒤, 기능의 추가, 변경 및 삭제 등을 요구하면 이를 즉각 반영하여 정보 시스템 설계를 다시 하고 프로토타입을 재구축하는 과정을 사용자가 만족할 때까지 반복해 나가면서 시스템을 개선시켜 나가는 방식