2018년 국가직 7급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
④	③	①	②	④	④	③	③	④	③
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
②	②	②	④	①	④	①	④	②	③

문 1. 공개키 인증서의 구조를 정의한 ITU-T 권고안은?

① X.25 ② X.121
③ X.400 ④ X.509

답 ④

④ 공인인증서는 공개키와 소유자를 연결시켜주는 전자 문서로 오늘날 사용되는 대부분의 인증서는 X.509 인증서(버전3)를 표준으로 따른다.

문 2. ㉠, ㉡에 들어갈 정보보안 위험의 처리 방식을 바르게 연결한 것은?

> (㉠)은(는) 사업 목적상 위험을 처리하는 데 들어가는 과도한 비용 또는 시간 때문에 일정 수준의 위험을 받아들이는 것으로, 그 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.
> (㉡)은(는) 위험에 대한 책임을 제3자와 공유하는 것으로, 보험을 들거나 다른 기관과의 계약을 통하여 잠재적 손실을 제3자에게 이전하거나 할당하는 방식이다.

	㉠	㉡
①	위험 회피	위험 전가
②	위험 회피	위험 감소
③	위험 수용	위험 전가
④	위험 수용	위험 감소

답 ③

㉠ **위험수용**: 현재의 위험을 받아들이고 잠재적 비용 손실 비용을 감수하는 것.

㉡ **위험 전가**: 위험으로 인한 잠재적 비용을 보험이나 외주 등 제3자에게 이전하는 것.

<오답 체크>

위험 회피: 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것.

위험 분석 결과, 해결을 하기 어렵거나 보호대책을 세우는 데 지나치게 많은 비용이 들어갈 경우 해당 사업을 수행하지 않는다.

위험 감소: 위험으로 인한 피해를 감소하기 위해 정보보호 대책을 구현하는 것.

수용 가능한 위험수준을 넘어서는 위험에 대해 취약성을 해결하거나 위험의 빈도를 낮출 수 있는 통제를 적용한다.

문 3. 다음에서 설명하는 컴퓨터 시스템의 평가 기준은?

> ○ 컴퓨터 시스템의 보안성을 평가하기 위해 미국 정부의 표준으로 채택된 기준이다.
> ○ Rainbow 시리즈라는 미 국방부 문서 중의 하나로 오렌지 북(Orange Book)으로 불린다.
> ○ 안전성과 신뢰성이 입증된 컴퓨터 시스템을 보급하기 위해 단계별 보안 평가 등급(D, C1, C2, B1, B2, B3, A1)을 분류하여 각 기관별 특성에 맞는 컴퓨터 시스템을 도입 및 운영하도록 권고하고 있다.

① TCSEC ② CC
③ CMVP ④ ITSEC

답 ①

① **TCSEC**(Trusted Computer System Evaluation Criteria)
미국의 정보보호 시스템 평가 제도
컴퓨터시스템의 구축과 평가 등에 관한 지속적인 연구 결과로 미국 국방부 내 NCSC(미국 컴퓨터 보안 센터) 주도하에 1983년에 제정되었으며, 소위 'Orange Book'으로 불린다.
보안 등급 분류: A1 - B3 - B2 - B1 - C2 - C1 - D

<오답 체크> ② **CC**(Common Criteria, 국제공통평가기준)
국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준
보안 등급 분류: EAL7 ~ EAL1

③ **CMVP**(Cryptographic Module Validation Program)
미국과 캐나다에서 공동으로 개발한 암호화 모듈 검증 제도이다.

④ **ITSEC**(Information Technology Security Evaluation Criteria)
유럽의 정보보호 시스템 평가 제도
보안 등급 분류: E6 ~ E1

문 4. 유닉스 시스템 명령어에 대한 설명으로 옳지 않은 것은?

① grep - 파일 내 정규 표현식을 포함한 모든 행을 검색· 출력하는 명령
② mesg - 모든 로그인 사용자에게 메시지를 전송하는 명령
③ chmod - 파일이나 디렉토리의 접근 권한을 변경하는 명령
④ man - 각종 명령의 사용법을 출력하는 명령

답 ②

② **mesg**(message)
메시지 수신 허용/거부 설정 명령어.
mesg는 메시지를 전송하는 명령어가 아니라 메시지를 받을지 말지 설정하는 명령어이다. 메시지를 전송하는 명령어는 write와 wall이 있다.

♧ **write**
특정 사용자에게 메시지를 전송하는 명령어

♧ **wall**(write all)
접속한 모두에게 메시지를 전송하는 명령어

<오답 체크> ① **grep**
파일이나 디렉토리 내에서 지정한 패턴이나 문자열을 찾아 그 패턴을 포함하고 있는 모든 행을 표준 출력하는 명령어

③ **chmod**(change mode)
파일이나 디렉터리에 대한 권한을 변경하는 명령어

④ **man**
각종 명령어들의 자세한 사용법이나 매뉴얼을 볼 때 사용하는 명령어

문 5. 「정보통신기반 보호법」상 주요정보통신기반시설을 관리하는 기관의 장이 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있는 기관에 해당하지 않는 것은?

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원
② 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업
③ 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원
④ 「국가정보화 기본법」 제14조의 규정에 의한 한국정보화진흥원

답 ④

「정보통신기반 보호법」 제9조(취약점의 분석 · 평가)

③ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석 · 평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석 · 평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 **한국인터넷진흥원**
2. 제16조의 규정에 의한 **정보공유 · 분석센터**(대통령령이 정하는 기준을 충족하는 정보공유 · 분석센터에 한한다)
3. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 **정보보호 전문서비스 기업**
4. 「정부출연연구기관 등의 설립 · 운영 및 육성에 관한 법률」 제8조의 규정에 의한 **한국전자통신연구원**

문 6. SHA-512 알고리즘의 처리 방식에 대한 설명으로 옳지 않은 것은?

① 최대 크기가 2^{128}비트 이하인 메시지를 입력받아 512비트 메시지 다이제스트를 출력한다.
② 필요한 길이의 패딩과 128비트 블록을 추가하여 처리하려는 메시지의 전체 크기가 1,024비트의 배수가 되게 한다.
③ 8개 소수의 제곱근에서 얻은 이진수로 초기화된 512비트 버퍼를 알고리즘의 중간 값과 최종 값을 저장하는 데 사용한다.
④ 블록 단위로 메시지를 처리하는 과정은 80라운드로 이루어지며, 규칙성을 제거하기 위해 각 라운드마다 서로 다른 암호 키를 사용한다.

답 ④

④ 메시지를 처리하는 과정은 80라운드가 맞으나, 해시 함수는 암호키를 사용하지 않는다.

<오답 체크> ①② SHA-512 알고리즘은 1024비트 블록 단위로 메시지를 처리한다. 만일 메시지의 길이가 1024의 배수가 아니라면, 1024의 배수가 되도록 맞춰주어야 하므로 이럴 때 부족한 길이만큼 임의의 비트열을 채우는데, 이러한 임의의 비트열을 패딩(padding)이라고 한다.

이 때 패딩을 하기 전, 원래 어디까지가 원본 메시지인지 기록하기 위해서 원본 메시지의 비트열 길이를 기록해두는데, 이 메시지 길이를 기록하는 부분이 128비트이다.

메시지 길이를 표현하는 비트가 최대 128비트이기 때문에 입력 메시지의 길이는 최대 2의 128승까지만 가능하다.

③ 해시값을 계산하기 전 초기 해시값을 지정해야 한다. 초기 해시값은 8개의 소수를 뽑아 각 소수의 제곱근에서 계산된 64비트의 값들의 집합으로, 따라서 8 X 64 = 512비트가 된다.

이렇게 초기화된 해시값에 메시지 블록을 입력·계산하여 출력된 결과를 다시 해시값에 덮어쓰는 과정을 반복해나가며 최종 해시값을 출력한다. 따라서 초기 해시값이 저장된 저장 공간이 곧 연산 결과를 저장하는 버퍼가 된다.

문 7. 커버로스(Kerberos) 버전 4 인증 시스템에서 클라이언트가 응용서버에게 제시하는 티켓에 포함되는 구성요소가 아닌 것은?

① 클라이언트 ID
② 클라이언트와 응용 서버 간의 세션키
③ 인증 서버의 네트워크 주소
④ 티켓의 유효시간

답 ③

③ 클라이언트가 응용서버(서비스 서버)에 보내는 티켓에는 **접속하고자 하는 서버의 ID, 클라이언트의 ID, 클라이언트의 네트워크 주소, 티켓의 유효기간, 클라이언트와 서버가 서비스 기간 동안 공유하는 세션키**의 정보가 들어있다.
응용서버가 인증 서버의 네트워크 주소를 알 필요는 없다.

✠ 커버로스(Kerberos) 작동 순서
1. 클라이언트는 사용자의 ID와 원하는 TGS ID를 인증서버(AS)에 전송
2. AS는, TGS에 보내기 위한 티켓 승인 티켓을(TicketTGS)를 사용자의 패스워드로부터 얻은 키로 암호화한 후 클라이언트로 보낸다.
(티켓에는 재사용 방지를 위해 유효기간(lifetime)이 포함되어 있다. 티켓 승인 티켓은 클라이언트가 볼 수 없도록 인증서버와 TGS의 대칭키로 암호화되어 있다.)
3. 클라이언트는 사용자의 패스워드를 이용해 복호화를 하여 티켓 승인 티켓을 획득한다.
4. 사용자 ID, 요구하는 서비스 ID, 티켓 승인 티켓을 TGS에 전송한다.
5. TGS는 전송받은 메시지를 복호화하여 ID, 유효기간, IP와 네트워크 점검 등을 확인한 후 서비스 승인 티켓(TicketV)를 클라이언트로 전송한다.
6. 클라이언트는 사용자 ID와 서비스 승인 티켓을 서비스 서버(응용서버)로 보낸다.
(서비스 승인 티켓은 클라이언트가 볼 수 없도록 TGS와 서비스 서버의 대칭키로 암호화되어 있다.)
7. 서비스 서버는 ID와 티켓의 내용을 확인한 후 인증을 완료한다.

문 8. 방화벽은 검사 대상이나 동작 방식에 따라 패킷 필터링, 상태 검사(stateful inspection), 응용 레벨 게이트웨이, 회선 레벨 게이트웨이로 분류할 수 있다. 상태 검사 방화벽에 대한 설명으로 옳은 것은?

① 트래픽 정보 수집이 어렵고, IP 스푸핑 공격에 대응하기 어렵다.
② 서비스별로 프록시 서버 데몬을 두어 사용자 인증과 접근제어를 수행한다.
③ 패킷 필터링 기능을 사용하며 현재 연결 세션의 트래픽 상태와 미리 저장된 상태와의 비교를 통하여 접근을 제어한다.
④ 송.수신자 간의 직접적인 연결을 허용하지 않고, 송신자와 수신자 사이에서 프록시가 어떤 연결을 허용할지를 판단한다.

답 ③

③ **상태 검사**(stateful inspection) 방화벽
패킷 필터링 방식과 응용 레벨 게이트웨이 방식의 장점을 혼합한 3세대 방화벽 기술
종합적인 맥락에서 트래픽을 검사하면서 네트워크 연결의 작동 상태와 특성을 검사에 반영, 더 전체적인 방화벽 기능을 제공한다. 네트워크 트래픽과 관련된 모든 통신 채널을 상태목록에 저장한 후 누가, 언제, 어느 때 사용하였는지, 어떤 경로를 통하여 외부에 접속하였는지를 비교·분석하여 패킷의 수락 여부를 결정하는 방화벽

<오답 체크> ① **패킷 필터링 방화벽**(Packet filtering Firewall)
네트워크 계층과 전송 계층 사이에서 작동하며, 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등의 규칙을 설정하여 접속제어를 수행한다.
IP 주소와 포트 번호의 규칙을 통해서만 접속 제어만 수행하기 때문에, 패킷 내의 데이터 위·변조 공격에 대해서는 방어할 수 없다.

② **어플리케이션 게이트웨이**(Application Gateway)
각 서비스별로 프록시 데몬(전용 게이트웨이)이 존재한다.

④ **회로 레벨 게이트웨이**(Circuit Level Gateway)
패킷 필터와 어플리케이션 게이트웨이 사이의 중간 솔루션으로, 모든 응용 프로그램에 대한 프록시 역할을 한다.
전체 종단 간 TCP 연결을 허용하지 않는다. 두 개의 TCP 연결을 설정한다.

문 9. VPN의 터널링 기능을 제공하는 L2TP(Layer 2 Tunneling Protocol)에 대한 설명으로 옳지 않은 것은?

① 데이터 링크 계층에서 터널링을 지원한다.
② PPTP(Point-to-Point Tunneling Protocol)와 L2F(Layer 2 Forwarding Protocol)의 기능을 결합한 프로토콜이다.
③ 데이터의 보안성을 높이기 위하여 IPsec과 결합하여 사용할 수 있다.
④ 패킷 인증, 암호화, 키 관리 기능을 제공한다.

답 ④

④ L2TP는 자체적으로 암호화 또는 인증을 제공하지 않기 때문에 IPsec과 함께 사용되는 경우가 많다.

<오답 체크> ① L2TP는 Layer 2 Tunneling Protocol(계층 2 터널링 프로토콜)의 약자로, OSI 2계층 데이터 링크 계층에서 작동한다.

문 10. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 유출등의 통지·신고에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

> 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 (㉠) 또는 (㉡)에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
> 1. 유출등이 된 개인정보 항목
> 2. 유출등이 발생한 시점
> 3. 이용자가 취할 수 있는 조치
> 4. 정보통신서비스 제공자등의 대응 조치
> 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

	㉠	㉡
①	과학기술정보통신부	한국인터넷진흥원
②	과학기술정보통신부	개인정보보호위원회
③	방송통신위원회	한국인터넷진흥원
④	방송통신위원회	개인정보보호위원회

답 ③

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제27조의3(개인정보 유출등의 통지·신고)
① 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 **방송통신위원회 또는 한국인터넷진흥원**에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

문 11. 침입차단시스템이 제공하는 주요 보안 서비스가 아닌 것은?

① 접근 통제 ② 최대 권한 부여
③ 사용자 인증 ④ 감사 및 로그 기능

답 ②

② 접근 통제, 사용자 인증, 감사 및 로그 기능, 기밀성/무결성 등의 기능을 수행하지만, 권한 부여 기능은 없다.

문 12. ㉠, ㉡에 들어갈 네트워크 보안 공격을 바르게 연결한 것은?

> (㉠)은(는) TCP 연결 설정을 위한 3-way handshaking 과정에서 half-open 연결 시도가 가능하다는 취약성을 이용하는 공격 방식이다.
> (㉡)은(는) 서버와 클라이언트가 TCP 통신을 하고 있을 때, RST 패킷을 보내고 시퀀스 넘버 등을 조작하여 연결을 가로채는 공격 방식이다.

㉠	㉡
① SYN 플러딩	IP 스푸핑
② SYN 플러딩	세션 하이재킹
③ ARP 스푸핑	IP 스푸핑
④ ARP 스푸핑	세션 하이재킹

답 ②

㉠ **SYN flooding**(SYN 플러딩)
TCP 3-way handshaking을 이용한 DoS공격
공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.
이렇게 3-way handshaking 과정이 완전히 이루어지지 않은 상태로 연결이 유지되는 것을 이용해 공격하는 것을 half-open 연결 시도가 가능하다는 취약성을 이용한다고 표현한다.

㉡ **세션 하이재킹**(Session Hijacking) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.
서버가 기존 클라이언트와 통신을 하고 있는 도중에, 공격자가 서버로 RST 패킷을 보내 강제로 연결을 끊는다. 그리고 재빨리 적당한 순서의 시퀀스 넘버를 생성하여 서버로 보내면, 서버는 공격자가 보낸 시퀀스 넘버를 정상적인 것으로 받아들여 다시 세션을 연결하여 공격자와 서버 간의 연결이 확립된다.

▷ **ARP Spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.
공격자는 클라이언트와 서버 사이의 패킷을 읽고 확인한 후 정상적인 목적지로 향하도록 다시 돌려보내 연결이 유지되도록 한다.

▷ **IP Spoofing**(IP 스푸핑)
단말 사이가 IP 주소 기반의 트러스트 관계일 경우 인증 절차를 생략한다는 취약점을 이용한 공격으로, 공격자가 자신의 IP를 다른 사람의 IP로 속여 다른 사람 행세를 하는 것이다.

문 13. 다음에서 설명하는 암호 알고리즘은?

> ○ Koblitz와 Miller가 제안한 것이다.
> ○ RSA보다 키의 길이를 작게 하면서도 대등한 보안성을 제공한다.
> ○ 전자서명이나 키 교환에 활용될 수 있다.
> ○ 메모리와 처리능력이 제한된 분야에 효율적이다.

① ElGamal
② ECC(Elliptic Curve Cryptography)
③ Rabin
④ WHIRLPOOL

답 ②

② **ECC** 알고리즘
타원곡선 상의 이산대수(이산로그) 계산의 어려움을 이용한 공개키 암호 알고리즘. RSA 알고리즘에 비해 키 길이가 매우 짧은 것이 특징이며, 그 덕에 메모리가 처리능력이 제한된 무선통신 환경에서는 ECC가 매우 효과적이다.
RSA 512비트와 비슷한 안전성을 제공하는 ECC 키 길이는 106 비트면 충분하다. 이러한 차이는 키 길이가 길수록 더 두드러지게 나타나며, ECC 512비트는 RSA 15,000비트와 동일한 안전성을 가진다.

<오답 체크> ① **ElGamal** 알고리즘
이산대수의 어려움에 기반한 공개키 암호 알고리즘.
RSA는 같은 메시지, 같은 키 값을 이용할 경우 그 암호문이 항상 일정한 반면, ElGamal은 난수 k를 이용하기 때문에, 매 암호화 시 암호문이 바뀌어 RSA에 비해 더 안전하다.
다만, 암호화시 메시지의 길이가 두 배가 되는 단점이 있다.

③ **Rabin** 알고리즘
소인수분해의 어려움에 기반한 공개키 암호 알고리즘이다.
RSA 알고리즘의 변형이며 RSA에 비해 효율적이다.

④ **WHIRLPOOL** 알고리즘은 해시 함수 알고리즘으로, 블록 크기를 512비트로 나누어 계산하며, 512비트의 해시값을 출력한다.

문 14. ㉠, ㉡에 들어갈 웹 공격 기법을 바르게 연결한 것은?

> (㉠)은(는) 웹 해킹으로 서버 권한을 획득한 후, 해당 서버에서 공격자의 PC로 연결하고 공격자가 직접 명령을 입력하여 개인정보 전송 등의 악의적인 행위를 하는 공격이다. 이 기법은 방화벽의 내부에서 외부로 나가는 패킷에 대한 아웃바운드 필터링을 수행하지 않는 허점을 이용한다.
> (㉡)은(는) 공격자가 웹 서버의 게시판 등에 악성 스크립트를 삽입한 후, 사용자의 쿠키와 같은 개인정보를 특정 사이트로 전송하게 하거나 악성파일을 다운로드하여 실행하도록 유도하는 공격이다.

	㉠	㉡
①	디렉토리 리스팅	포맷 스트링
②	디렉토리 리스팅	XSS
③	리버스 텔넷	포맷 스트링
④	리버스 텔넷	XSS

답 ④

㉠ **Reverse Telnet**(리버스 텔넷) 공격
보통 방화벽을 운영할 땐 인바운드 규칙(외부에서 내부로의 접속 규칙)을 설치해 통제하기 때문에, telnet(텔넷) 프로토콜을 이용한 외부에서 내부로 원격 접속은 필터링이 가능해진다.
하지만 보통 아웃바운드 규칙(내부에서 외부로의 규칙)은 허술한 경우가 대부분이다. 이러한 취약점을 이용해 방화벽 내부에서 프로그램을 실행시켜 외부에 있는 공격자 컴퓨터 쪽으로 접속하도록 조작하여 악의적인 행위를 하는 공격이 리버스 텔넷 공격이다.

㉡ **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)
웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.

<오답 체크>

▷ **Directory Listing**(디렉토리 리스팅)
취약한 서버 설정으로 인해 웹 디렉토리내의 모든 파일 목록이 노출되는데, 공격자가 이 노출된 파일들을 열람 및 저장하고 소스 코드, 스크립트 등을 분석하여 개인정보 유출 및 다른 네트워크 공격에 이용할 수 있다.

▷ **Format String**(포맷 스트링) 공격
결과를 출력하기 위하여 사용되는 printf() 함수에서 지시자를 제대로 지정하지 않아 의도적으로 버그를 발생시켜, 메모리의 특정 위치의 값을 다른 것으로 변경시키는 공격이다. 해커는 이렇게 포맷 스트링의 취약점을 악용해 시스템의 권한을 획득하거나 특정 동작을 수행하게 만든다.

문 15. IEEE 802.11i에서 정의된 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol)에 대한 설명으로 옳지 않은 것은?

① 기존의 WEP(Wired Equivalent Privacy) 보안 구현 장치에서 소프트웨어적으로 동작할 수 있도록 고안되었다.
② CBC(Cipher Block Chaining)-MAC를 사용하여 메시지 무결성을 제공한다.
③ AES(Advanced Encryption Standard)의 CTR 블록 암호 모드를 사용한다.
④ WPA2(Wi-Fi Protected Access 2)에서 사용하는 보안 기술이다.

답 ①

① TKIP에 대한 설명이다.
TKIP는 기존의 WEP-RC4 보안의 문제점을 소프트웨어적으로 개선하여 단말과 액세스포인트에 패치하여 사용할 수 있도록 함으로써 이미 배치되어 사용중인 무선랜의 보안 문제점을 해결하자는 취지에서 개발된 보안 프로토콜이다.

○ **WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용
○ **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
○ **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증

문 16. 전자우편 보안을 위한 PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① 전자우편 메시지의 인증과 기밀성 제공을 위한 것으로 필 짐머만(Phil Zimmermann)이 고안하였다.
② 메시지 발송 시 메시지에 대한 서명, 압축, 암호화 순으로 처리할 수 있다.
③ 임의의 사용자는 여러 개의 공개·개인키 쌍을 가질 수 있도록 하고 있다.
④ 메시지 암호화를 위한 일회용 세션키를 사용하지 않기 때문에 공유 비밀키를 교환하기 위한 절차가 필요하다.

답 ④

④ PGP는 하이브리드 암호화 방식을 사용한다. 짧은 길이의 세션키를 생성해 전체 메시지를 암호화하고, 이 세션키를 RSA 또는 Diffie-Hellman 알고리즘을 이용해 이 세션키를 교환한다.
RSA 버전에서는, 전체 메시지를 암호화하는데 사용되는 짧은 키의 생성을 위해 IDEA 대칭키 알고리즘을 사용하며, 짧은 키를 암호화하기 위해 RSA 공개키 알고리즘를 사용한다.
Diffie-Hellman 버전은 전체 메시지를 암호화하기 위한 짧은 키를 위해 CAST 대칭키 알고리즘을 사용하며, Diffie-Hellman 알고리즘을 사용해 짧은 키를 암호화하기 위한 키를 생성한다.
<오답 체크> ③ 사용자는 여러 쌍의 공개키/개인키를 가지고 있으며, 한 사용자의 공개키에 구별이 가능하도록 식별자(identifier)를 붙인다.

★ PGP 메시지 발송 순서
1. 의사난수 생성기를 사용해 세션키를 생성
2. 세션키를 공개키 암호로 암호화(**서명**)
3. 메시지를 **압축**
4. 압축한 메시지를 대칭키(세션키)로 **암호화**
5. 암호화된 세션키와 압축&암호화한 메시지를 결합
6. 결합된 메시지를 텍스트 데이터로 변환

문 17. 스트림 암호에 대한 설명으로 옳은 것은?

① 대표적인 스트림 암호 방식인 RC4는 다양한 키 길이를 갖도록 설계된 바이트 기반의 알고리즘이다.
② 안전성은 키열(key stream)을 생성하는 의사 난수 생성기의 안전성에 반비례한다.
③ 블록 암호와 달리 구현이 어렵고 속도가 느린 단점이 있다.
④ 키열의 반복 주기가 짧을수록 암호문을 해독하기가 더 어려워진다.

답 ①

① **RC4** 알고리즘
다양한 키 길이를 가지는 바이트 단위로 작동하는 스트림 암호 알고리즘이다. 블록 암호에 비해 경량 및 고속 동작이 용이하여 무선환경이나 스트리밍 서비스 등과 같은 환경에서 많이 사용하며, SSL/TLS, WEP, WPA 등에서 사용한다.

<오답 체크> ② 스트림 암호의 안전성은 의사 난수 생성기의 안전성에 의존하기 때문에 비례한다.
③ 스트림 암호는 블록 암호에 비해 하드웨어 구현이 간편하고 속도가 빠르기 때문에 무선통신 등의 환경에서 주로 사용된다.
④ 키열의 반복 주기가 길수록 좋으며, 주기를 가능한 길게 하는 것이 의사 난수 생성기의 목표이다.

문 18. 「개인정보의 안전성 확보조치 기준」상 개인정보처리자가 개인정보를 암호화할 때 준수해야 할 사항으로 옳지 않은 것은?

① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
④ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어를 사용하여서는 아니 된다.

답 ④

「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화)

① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, **비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장**하여야 한다.
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.
1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 **상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장**하여야 한다.
⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

문 19. RSA 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① 대표적인 비대칭 암호 알고리즘으로, 널리 사용되고 있다.
② 공개키 {e,n}이 주어지면 지수 및 모듈러 연산을 통해 n과 무관한 임의 크기의 평문 블록을 하나의 암호문 블록으로 암호화할 수 있다.
③ 공개키 {e,n}의 n을 소인수분해할 수 있으면 개인키 {d,n}의 d를 알아낼 수 있다.
④ 일반적으로 키의 길이가 길수록 안전성은 높아지지만 알고리즘 수행시간은 길어진다.

답 ②

② RSA 암호화시 입력 데이터의 길이가 키의 길이(n)보다 크다면 예외가 발생한다. 따라서 키의 길이와 같거나 작도록 데이터를 나누어 암호화를 수행해야 한다.

◈ RSA 알고리즘 공개키와 개인키 생성 순서
○ 단계 1: 두 소수 p, q를 선정한다.
○ 단계 2: n = p × q를 계산한다.
○ 단계 3: Φ(n) = (p − 1) × (q − 1)을 계산한다.
(단, Φ(n)은 오일러의 Totient 함수이다.)
○ 단계 4: Φ(n)보다 작고, Φ(n)과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
○ 단계 5: e × d mod Φ(n) = 1의 관계를 갖는 d를 계산한다.
(단, mod는 나머지를 구하는 연산자이다.)
○ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

$$\text{암호문} = (\text{평문})^{e} \bmod n$$
$$\text{평문} = (\text{암호문})^{d} \bmod n$$

<오답 체크> ③ RSA 암호화는 소인수분해의 어려움에 기반한 알고리즘이다. 위의 키 생성 순서를 보면 n = p × q이다. 그러므로 n을 소인수분해할 수 있다면 p와 q를 알 수 있으며, Φ(n)도 알아낼 수 있다.
그러면 결국 e × d mod Φ(n) = 1 을 통해 개인키 d를 계산할 수 있게 된다.
④ 키의 길이가 길수록 소인수분해가 더욱 어려워져 안전성은 높아지지만, 안 그래도 느린 RSA 알고리즘의 수행시간은 더욱 길어지게 된다.

문 20. 중간 시스템(reflector)을 이용해서 서비스 거부(DoS)를 발생시키는 반사(reflection) DDoS 공격에 대한 설명으로 옳지 않은 것은?

① 공격 대상의 주소를 시작 주소로 갖는 패킷을 중간 시스템에 보낸다.
② 중간 시스템으로 네트워크 연결이 좋은 고용량의 네트워크 서버나 라우터가 이용될 수도 있다.
③ 사전에 중간 시스템 내부에 공격자의 명령 수행을 위한 비정상 프로그램이 작동하도록 해야 한다.
④ 중간 시스템이 요청 메시지에 대해서 큰 응답 메시지를 생성하는 서비스를 이용하면 공격 대상 시스템에 더 많은 피해를 줄 수 있다.

답 ③

③ 공격을 위해 사전에 악성 프로그램을 설치하는 과정이 필요한 것은 DDoS 공격이다.(악성 봇을 이용)
DRDoS 공격에서 중간 시스템은 공격자가 보내는 패킷에 대해 정상적으로 응답만 하면 되기 때문에 악성 프로그램을 설치할 필요가 없다.

▶ **DRDoS 공격**(Distributed Reflect DoS, 분산 반사 서비스 거부 공격)
패킷의 출발지 IP 주소를 공격 대상의 IP주소로 스푸핑한 TCP-SYN 패킷을 브로드캐스트로 다수의 시스템에 전송한다. 패킷을 받은 각 단말들은 이에 응답 패킷을 보내게 되는데, TCP-SYN 패킷의 출발지 IP 주소가 공격 대상의 IP 주소로 위조된 상태이기 때문에 응답 패킷은 공격 대상으로 향하게 된다. 이를 통해 각 단말들이 보내는 응답 패킷들이 공격 대상으로 몰리게 만들어 시스템 자원을 고갈시켜 서비스가 마비되게 만든다.