# 2016-서울시-정보보호론-A형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)



1. 다음 중 X.509 v3 표준 인증서에 포함되지 않는 것은?

① 인증서의 버전(Version)

② 서명 알고리즘 식별자(Signature Algorithm ID)

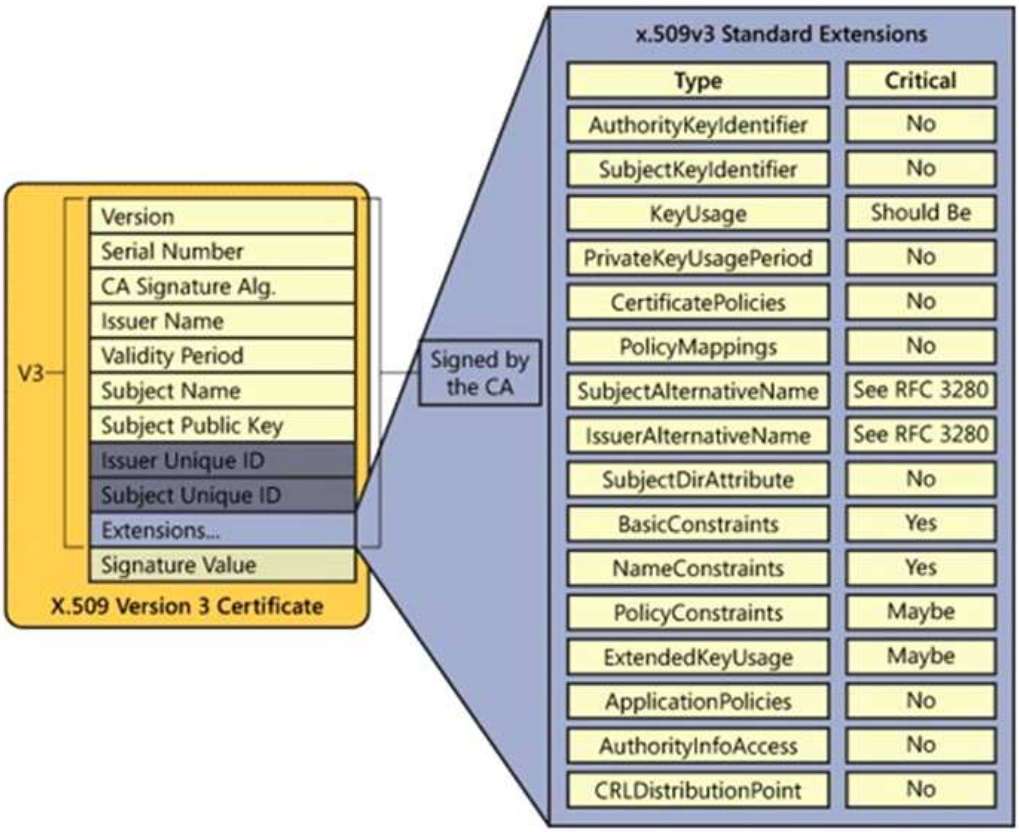
③ 유효기간(Validity Period)

④ 디렉토리 서비스 이름(Directory Service Name)

정답 체크 :

(4)

아래 그림에서 보는 바와 같이 X.509 v3 표준 인증서에는 Version, Signature Algorithm ID(CA Signature Alg.), Validity Period는 포함되어 있지만, Directory Service(컴퓨터 네트워크의 사용자와 네트워크 자원에 대한 정보를 저장하고 조직하는 응용 소프트웨어) Name은 포함되지 않는다.




2. 다음 중 성격이 다른 공격 유형은?

① Session Hijacking Attack

② Targa Attack

③ Ping of Death Attack
④ Smurf Attack
정답 체크 :
(1) Session Hijacking : TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 넘버를 사용한다. 이 시퀀스 넘버가 잘못되면 이를 바로 잡기 위한 작업을 하는데, 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식이다. 다른 보기는 DoS 공격(서비스 거부 공격)인데, Session Hijacking은 MITM 공격(중간자 공격)이다.
오답 체크 :
(2) Targa : 여러 종류의 서비스 DoS 공격을 실행할 수 있도록 만든 '공격 도구'로 이미 나와 있는 여러 DoS 공격 소스들을 사용해 통합된 '공격 도구'를 만든 것이다. bonk, joit, land, nestea, newtear, syndrop, teardrop, winnuke 등이 있다.
(3) Ping of Death : 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
(4) Smurf : 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부(DDoS) 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.

3. Stack에 할당된 Buffer overflow Attack에 대응할 수 있는 안전한 코딩(Secure Coding) 기술의 설명으로 옳지 않은 것은?
① 프로그램이 버퍼가 저장할 수 있는 것보다 많은 데이터를 입력하지 않는다.
② 프로그램은 할당된 버퍼 경계 밖의 메모리 영역은 참조하지 않으므로 버퍼 경계 안에서 발생될 수 있는 에러를 수정해 주면 된다.
③ gets()나 strcpy()와 같이 버퍼 오버플로우에 취약한 라이브러리 함수는 사용하지 않는다.
④ 입력에 대해서 경계 검사(Bounds Checking)를 수행해 준다.
정답 체크 :
(2) 버퍼 경계 안 : 버퍼 오버플로우는 버퍼 경계 밖의 함수의 복귀 주소에서 에러가 발생하기 때문에 버퍼 경계 밖에서 발생될 수 있는 에러를 수정해 주어야 한다.
오답 체크 :
(1) 많은 데이터 : 입력값 길이를 검사하면 버퍼가 저장할 수 있는 것보다 많은 데이터가 입력되는 것을 막을 수 있다.
(3) gets(), strcpy() : 입력값 길이에 대한 검사를 할 수 있는 fgests(), strncpy()를 사용한다.
(4) 경계 검사 : 입력값 길이에 대한 검사를 수행하는 함수를 사용한다.

4. 전자화폐(Electronic Cash)에 대한 설명으로 옳지 않은 것은?
① 전자화폐의 지불 과정에서 물품 구입 내용과 사용자 식별 정보가 어느 누구에 의해서도 연계되어서는 안된다.

② 전자화폐는 다른 사람에게 즉시 이전할 수 있어야 한다.
③ 일정한 가치를 가지는 전자화폐는 그 가치만큼 자유롭게 분산이용이 가능해야 한다.
④ 대금 지불 시 전자화폐의 유효성 확인은 은행이 개입하여 즉시 이루어져야 한다.
정답 체크 :
(4) 은행 개입 : 전자지불 시스템의 지불 서버와 같은 지불 브로커 없이 독립적인 구조로 결재를 수행하는 신용 기반으로 은행이 개입하지 않는다.
오답 체크 :
(1) 연계 : 정당한 사용자의 화폐 사용 내역은 알려져서는 안된다. 사용자의 사생활은 보호되어야 할 뿐만 아니라 사용자의 구매내역 등이 추적 불가능해야 한다.
(2) 이전 : 전자화폐를 받은 상점이나 사용자는 다시 해당 전자화폐를 다른 상점이나 제 3의 사용자에게 사용이 가능해야 한다.
(3) 분산이용 : 현금에 상응하는 화폐가치가 IC 카드 혹은 네트워크를 통해 결재된 후 인출된다. 이 후 해당 화폐가치는 이전이 가능하다(분산 이용 된다).

5. Linux system의 바이너리 로그파일인 btmp(솔라리스의 경우는 loginlog 파일)를 통해 확인할 수 있는 공격은?
① Password Dictionary Attack
② SQL Injection Attack
③ Zero Day Attack
④ SYN Flooding Attack
정답 체크 :
(1) Password Dictionary : btmp(loginlog)는 실패한 로그인 시도에 대한 로그이므로 패스워드 사전 공격(사전 파일에 주어진 패스워드를 차례대로 공격)을 확인할 수 있다.
오답 체크 :
(2) SQL Injection : access.log를 보면 접근 시도를 알 수 있는데, 접근 시도 파일 중에 SQL Injection 공격 문제가 없는지 살펴보아야 한다.
(3) Zero Day : 프로그램에 문제가 알려지고 난 후 보안패치가 나올 때까지 시간차를 이용해 공격하는 기법을 말한다. 그러므로 로그를 통해 공격을 확인할 수 없다.
(4) SYN Flooding : 공격을 당해 syncookies(SYN 패킷들을 SYN Backlog에 저장하지 않고, syncookies를 만들어 클라이언트에 보냄)가 작동할 때에는 /var/log/messages 파일에 SynFlooding 공격이 진행중이라는 메시지가 출력된다.

6. 다음 바이러스 발전 단계에 따른 분류에 대한 설명으로 옳지 않은 것은?
① 원시형 바이러스는 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스이다.
② 암호화 바이러스는 바이러스 프로그램 전체 또는 일부를 암호화시켜 저장하는 바이러스이다.
③ 갑옷형 바이러스는 백신 개발을 지연시키기 위하여 다양한 암호화 기법을 사용하는 바이러스이다.
④ 매크로 바이러스는 매크로를 사용하는 프로그램 데이터를 감염시키는 바이러스이다.
정답 체크 :
(1) 원시형 : 부트 바이러스(플로피 디스크나 하드 디스크의 부트 섹터에 감염되는 바이러스

로, 부팅할 때 자동으로 동작)와 파일 바이러스(파일을 직접 감염시키는 바이러스)가 있다. 원시형 바이러스는 코드의 변형이나 변화 없이 고정된 크기를 가진다.
오답 체크 :
(2) 암호화 : 바이러스 코드를 쉽게 파악하고 제거할 수 없도록 암호화한 바이러스이다. 바이러스 제작자들은 백신의 진단을 우회하기 위해 자체적으로 코드를 암호화하는 방법을 사용하여 백신 프로그램이 진단하기 힘들게 만들기 시작하였다.
(3) 갑옷형 : 백신 프로그램이 특정 식별자를 이용하여 바이러스를 진단하는 기능을 우회하기 위해 만들어진 바이러스이다. 다형성(갑옷형) 바이러스는 코드 조합을 다양하게 할 수 있는 조합(Mutation) 프로그램을 암호형 바이러스에 덧붙인다.
(4) 매크로 : 엑셀 또는 워드와 같은 문서 파일의 매크로 기능을 이용하기 때문에 워드나 엑셀 파일을 열 때 감염된다. 누구나 바이러스를 만들어 배포하는 계기가 되었다.

7. 공개키 기반구조(Public Key Infrastructure, PKI)를 위한 요소 시스템으로 옳지 않은 것은?
① 인증서와 인증서 폐지 목록을 공개하기 위한 디렉토리
② 사용자 신원을 확인하는 등록기관
③ 인증서 발행업무를 효율적으로 수행하기 위한 인증기관 웹 서버
④ 인증서를 발행 받는 사용자(최종 개체)
정답 체크 :
(3) 인증기관 : 인증기관은 인증서의 관리를 행하는 기관으로, 키 쌍을 작성한다(이용자가 작성하는 경우도 있다). 그리고 공개 키 등록 때 본인을 인증하고, 인증서를 작성해서 발행하거나 인증서를 폐지한다. 인증기관은 사람 혹은 조직을 의미하고, 웹 서버를 의미하지 않는다.
오답 체크 :
(1) 디렉토리(저장소) : 인증서를 보존한다. PKI 이용자가 인증서를 입수할 수 있도록 한 데이터베이스이다.
(2) 등록기관 : 인증기관(CA)의 일 중 「공개키의 등록과 본인에 대한 인증」을 대행하는 기관이다.
(4) 사용자 : PKI를 사용해서 자신의 공개 키를 등록하고 싶어 하는 사람과 등록되어 있는 공개 키를 사용하고 싶어 하는 사람을 의미한다.
Tip! : PKI의 구성 요소를 그림으로 나타내면 다음과 같다.

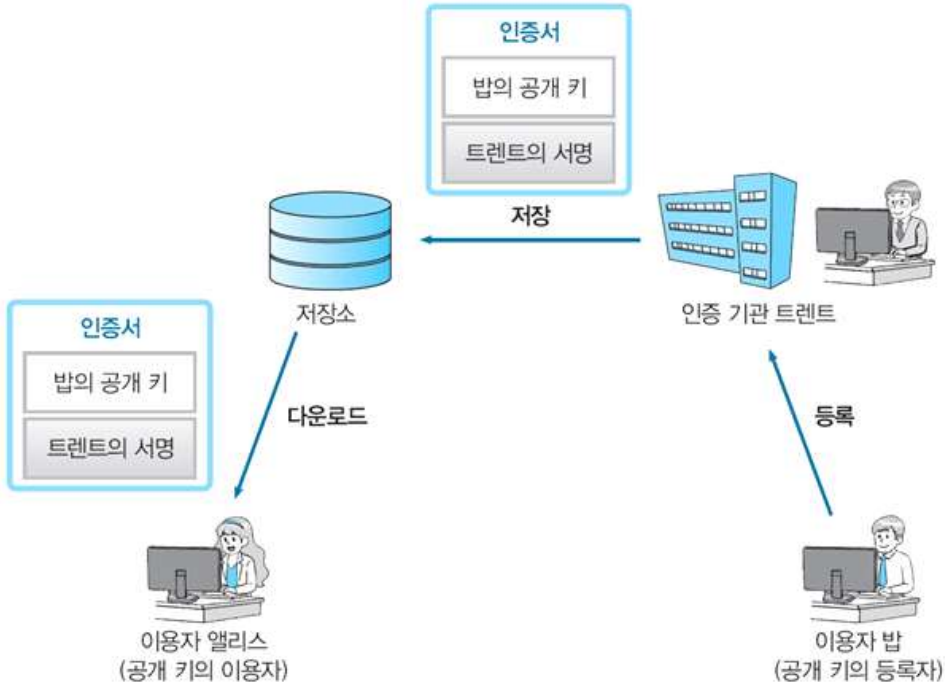



그림 11-3 • PKI 구성 요소

8. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header 에서 검출할 수 없는 정보는 무엇인가?

① 수신 시스템이 처리할 수 있는 윈도우 크기
② 패킷을 송신하고 수신하는 프로세스의 포트 번호
③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
④ 송신 시스템의 TCP 패킷의 생성 시간

정답 체크 :

(4) 생성 시간 : 패킷의 헤더에는 통신을 위해 필요한 필수 정보가 들어가야 한다. 보기의 TCP 패킷의 생성 시간은 어디에도 사용할 수 없는 의미 없는 정보이다.

오답 체크 :

(1), (2), (3)

TCP 패킷의 헤더는 다음과 같다.

| 필드 | 크기(비트) | 설명 |
|---|---|---|
| 송신측의 포트 번호 | 16 | 데이터를 보내는 애플리케이션의 포트 번호 |
| 수신측의 포트 번호 | 16 | 데이터를 받을 애플리케이션의 포트 번호 |
| 순서 번호 | 32 | 송신하는 데이터의 일련번호로 선두 위치를 나타냄 |
| 인정(ACK) 번호 | 32 | 수신된 데이터의 순서 번호에 수신된 데이터 크기를 더한 값 |
| 데이터 오프셋 | 4 | 데이터가 시작되는 위치 |
| 예약 필드 | 6 | 사용하지 않음 |
| 제어 비트 | 6 | SYN, ACK, FIN 등의 제어 번호 |
| 윈도우 크기 | 16 | 수신측에서 수신할 수 있는 데이터의 크기 |
| 체크섬 | 16 | 데이터 오류 검사에 필요한 정보 |
| 긴급 위치 | 16 | 긴급하게 처리할 데이터의 위치 |
| 옵션 | 가변길이 | 기타 정보를 위한 부분 |

9. 아래 <보기>의 지문은 신문에서 발췌한 기사이다. 빈칸에 들어갈 단어로 적절한 것은?

<보기>

취업준비생 김다정(28)씨는 지난 5월 7일 [ ] 공격으로 취업을 위해 모아뒀던 학습 및 준비 자료가 모두 암호화돼 버렸다. 컴퓨터 화면에는 암호를 알려주는 대가로 100달러(약 11만 5000원)를 요구하는 문구가 떴지만, 결제해도 데이터를 되찾을 수 없다는 지인의 조언에 데이터복구 업체를 통해 일부 자료만 복구해 보기로 했다. 그런데 업체를 통해 데이터 일부를 복구한 지 하루 만인 지난 10일 또 다시 [ ] 공격을 받아 컴퓨터가 먹통이 돼 버렸다.

① 하트블리드(Heart bleed)
② 랜섬웨어(Ransomware)
③ 백오리피스(Back Orifice)
④ 스턱스넷(Stuxnet)

정답 체크 :

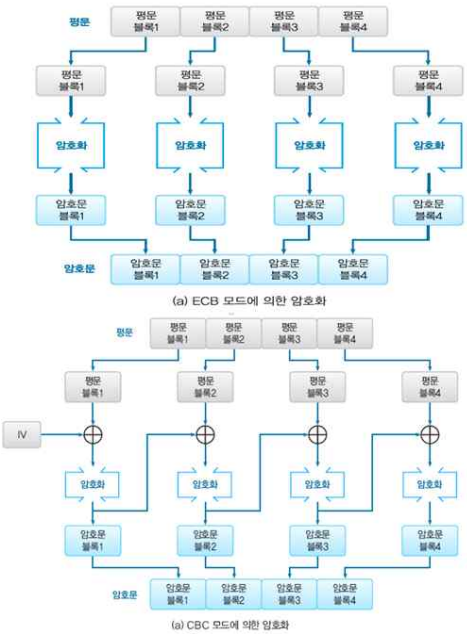
(2) 랜섬웨어 : 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.

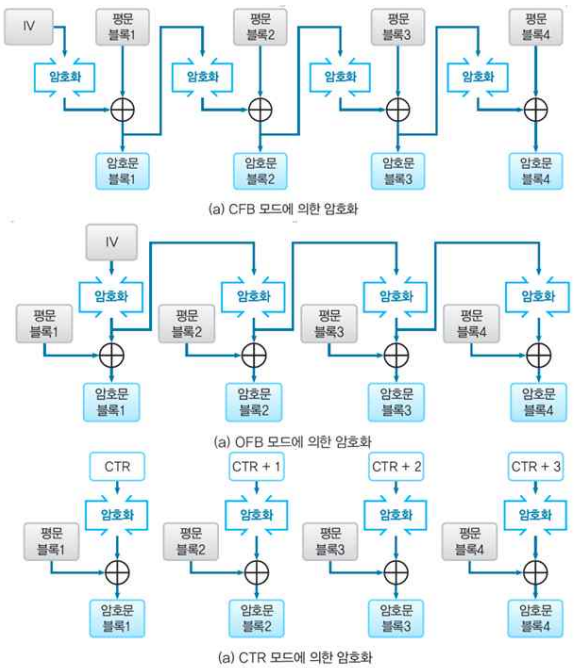
오답 체크 :

(1) 하트블리드 : 인터넷에서 각종 정보를 암호화하는 데 쓰이는 오픈소스 암호화 라이브러리인 오픈SSL(OpenSSL)에서 발견된 심각한 보안 결함을 일컫는 말이다. 하트블리드 버그를 이용하면 특정 버전의 오픈SSL을 사용하는 웹 서버에 침입할 수 있으며 개인 정보도 빼낼 수 있다.

(3) 백오리피스 : 사용자 정보를 빼내는 해킹 프로그램으로 바이러스처럼 자신을 복제하는 기능은 없지만 큰 피해가 우려되기 때문에 트로이 목마 바이러스로 분류된다. 백오리피스는 윈도 운영체계(OS) 환경의 PC에 저장된 중요정보를 빼내거나 파괴, 변조 등을 가능하게 한다.
(4) 스턱스넷 : 국가 및 산업의 중요 기반 시설을 제어하는 SCADA(Supervisory Control And Data Acquisition) 시스템을 대상으로 한 웜이다. 전파를 위해 윈도우 서버 서비스의 취약점을 이용해 공유 폴더를 공격했으며 윈도우 쉘 .lnk(바로가기) 취약점을 이용해 USB를, 윈도우 프린트 스플러 서비스의 취약점인 공유 프린터를 전파 개체로 활용했다.

10. 다음 중 Cipher Block Chaining 운용 모드의 암호화 수식을 제대로 설명한 것은? (단, $P_i$는 i번째 평문 블록을, $C_i$는 i번째 암호문 블록을 의미한다.)
① $C_i=E_k(P_i)$
② $C_i=E_k(P_i \oplus C_{i-1})$
③ $C_i=E_k(C_{i-1}) \oplus P_i$
④ $C_i=E_k(P_i) \oplus C_{i-1}$
정답 체크 :
(2) $C_i=E_k(P_i \oplus C_{i-1})$ : CBC
오답 체크 :
(1) $C_i=E_k(P_i)$ : ECB
(3) $C_i=E_k(C_{i-1}) \oplus Pi$ : CFB
(4) $C_i=E_k(P_i) \oplus C_{i-1}$ : 다섯 종류의 블록모드에 속하지 않는다.
Tip! : OFB는 $C_i=E_k(O_{i-1}) \oplus Pi$이고, CTR은 $C_i=E_k(CTR_i) \oplus P_i$이다.
이들을 그림으로 나타내면 다음과 같다.




11. 공통평가기준(Common Criteria, CC)에 대한 설명 중 옳지 않은 것은?
① 보호프로파일(Protection Profile)과 보안목표명세서(Security Target) 중 제품군에 대한

요구사항 중심으로 기술되어 있는 것은 보안목표명세서(Security Target)이다.
② 평가대상에는 EAL 1에서 EAL 7까지 보증등급을 부여할 수 있다.
③ CC의 개발은 오렌지북이라는 기준서를 근간으로 하였다.
④ CC의 요구사항은 class, family, component로 분류한다.
정답 체크 :
(1) 제품군에 대한 요구사항 중심으로 기술되어 있는 것은 보호프로파일(Protection Profile)이고, 보안목표명세서(Security Target)는 개발자가 작성하며 제품 평가를 위한 상세 기능을 정의한다.
오답 체크 :
(2) 7 개의 보증 등급을 가진다. 보증 등급은 기능 시험(EAL-1), 구조 시험(EAL-2), 방법론적 시험과 점검(EAL-3), 방법론적 설계, 시험, 검토(EAL-4), 준정형적 설계 및 시험(EAL-5), 준정형적 검증된 설계 및 시험(EAL-6), 정형적 검증(EAL-7)로 나눠진다.
(3) CC는 TCSEC와 ITSEC는 통합했는데, TCSEC는 오렌지북이라고 불린다. 그러므로 CC는 오렌지북을 근간으로 한다.
(4) 보안기능요구사항은 Functional Classes, Functional Families, Functional Components, Detailed Requirements, Functional Packages로 구성된다. 보증요구사항은 Assurance Classes, Assurance Families, Assurance Components, Detailed Requirements, Evaluation Assurance Levels로 구성된다.

12. <보기>에서 설명하는 암호화 알고리즘으로 옳은 것은?

<보기>
- Ron Rivest가 1987년에 RSA Security에 있으면서 설계한 스트림 암호이다.
- 바이트 단위로 작동되도록 만들어진 다양한 크기의 키를 사용 한다.
- 사용되는 알고리즘은 랜덤 치환에 기초해서 만들어진다.
- 하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.

① RC5
② SEED
③ SKIPJACK
④ RC4
정답 체크 :
(4) RC4 : 1987년에 로널드 라이베스트(Ron Rivest)가 만든 스트림 암호로, 전송 계층 보안(TLS)이나 WEP등의 여러 프로토콜에 사용되어 왔다. 옥텟(바이트) 단위를 기반으로 한다. 따라서 비트 단위의 암호보다 소프트웨어적인 실행 속도가 빠르다.
오답 체크 :
(1) RC5 : 미국 RSA 연구소의 리베스트(Rivest)가 개발한 것으로 32/64/128비트의 키를 가지며, 속도는 DES의 약 10배이다.
(2) SEED : SEED는 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 2월 한국인터넷진흥원과 국내 암호전문가들이 순수 국내기술로 개발한 128비트 블록 암호 알고리즘이다. 2009년 256 비트 키를 지원하는 SEED 256을 개발하였다.
(3) SKIPJACK : 미 국가안보국(NSA, National Security Agency)에서 개발한 Clipper 칩에

내장된 블록 알고리즘이다. 64비트의 입출력, 80비트의 키, 총 32라운드를 가진다.

13. 다음 중 Spoofing 공격에 대한 설명으로 옳지 않은 것은?
① ARP Spoofing : MAC주소를 속임으로써 통신 흐름을 왜곡 시킨다.
② IP Spoofing : 다른이가 쓰는 IP를 강탈해 특정 권한을 획득한다.
③ DNS Spoofing : 공격대상이 잘못된 IP주소로 웹 접속을 하도록 유도하는 공격이다.
④ ICMP Redirect : 공격자가 클라이언트의 IP주소를 확보 하여 실제 클라이언트처럼 패스워드 없이 서버에 접근한다.
정답 체크 :
(4) ICMP Redirect : 해당 설명은 IP Spoofing을 의미하고, ICMP Redirect는 3계층에서 스니핑 시스템을 ICMP Redirect 메시지를 통해 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.
오답 체크 :
(1) ARP Spoofing : 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다.
(2) IP Spoofing : 트러스트(Trust)로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다.
(3) DNS Spoofing : 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.

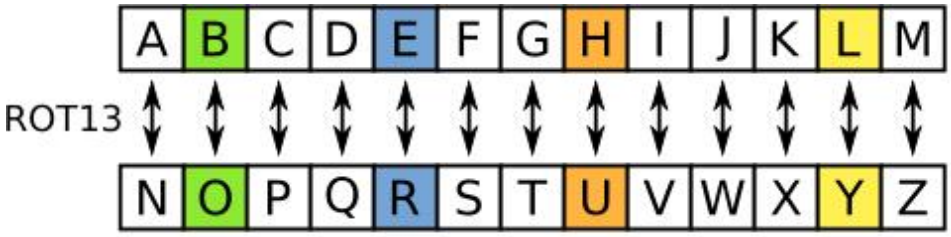
14. 다음 중 ISMS(Information Security Management System) 의 각 단계에 대한 설명으로 옳은 것은?
① 계획 : ISMS 모니터링과 검토
② 조치 : ISMS 관리와 개선
③ 수행 : ISMS 수립
④ 점검 : ISMS 구현과 운영
정답 체크 :
(2) 조치(Act) : ISMS 관리와 개선을 수행한다.
오답 체크 :
(1) 계획(Plan) : ISMS 수립을 수행한다.
(3) 수행(Do) : ISMS 구현과 운영을 수행한다.
(4) 점검(Check) : ISMS 모니터링과 검토를 수행한다.

15. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳은 것은 무엇인가?
① TGT(Ticket Granting Ticket)는 클라이언트가 서비스를 받을 때마다 발급 받아야 한다.
② 커버로스는 독립성을 증가시키기 위해 키 교환에는 관여하지 않아 별도의 프로토콜을 도입해야 한다.
③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션 통신을 한다.
④ 공격자가 서비스 티켓을 가로채어 사용하는 공격에는 취약한 방식이다.

정답 체크 :
(3) 커버로스는 비밀키(대칭키) 암호 기반 키 분배 및 사용자 인증 시스템이다. 중앙 집중식 인증 버서를 이용한다.
오답 체크 :
(1) TGT는 서비스 유형마다 한번만 발급 받으면 된다.
(2) 커버로스 자체가 키 교환에 관여하기 때문에 별도의 프로토콜을 도입하지 않아도 된다.
(4) 공격자가 서비스 티켓을 가로챈다고 하더라도 세션키를 모르기 때문에 공격을 수행할 수 없다.

16. 다음 중 시스템 내부의 트로이목마 프로그램을 감지하기 위한 도구로 가장 적절한 것은?
① Saint
② Snort
③ Nmap
④ Tripwire
정답 체크 :
(4) Tripwire : 먼저 시스템에 존재하는 파일에 대해 DB를 만들어 저장한 후, 생성된 DB와 비교하여 추가, 삭제되거나 변조된 파일이 있는지 점검하고 관리자에게 레포팅 해 주는 무결성 검사 도구이다.
오답 체크 :
(1) Saint : 기관이 운영하는 네트워크상의 시스템 보안취약점을 진단하고 평가해주는 미국의 보안 컨설팅 업체에서 만들어낸 관리자용 네트워크 진단 도구 이다. 기존의 네트워크 보안취약점진단도구인 SATAN과 프로그램구조가 매우 흡사하다.
(2) Snort : 스노트(Snort)는 무료의 오픈 소스 네트워크 침입 차단 시스템(IPS)이자, 네트워크 침입 탐지 시스템(IDS)으로서, 마틴 로시가 1998년에 개발하였다. 실시간 트래픽 분석과 IP에서의 패킷 로깅을 수행하는 능력을 갖고, 프로토콜 분석, 내용 검색 그리고 매칭을 수행한다. 사용자 인증과는 무관하다.
(3) Nmap : 가장 대표적인 포트 또는 IP 스캔 프로그램으로서 로컬 및 네트워크 시스템에 대한 스캔을 통해 자신이 관리하는 시스템에 자신도 알지 못하는 포트가 열려 있는지를 확인할 수 있는 도구다.

17. ROT13 암호로 info를 암호화한 결과는?
① jvxv
② foin
③ vasb
④ klmd
정답 체크 :
(3)
ROT13(Rotate by 13)은 단순한 카이사르 암호의 일종으로 영어 알파벳을 13글자씩 밀어서 만든다. 흔히 ROT-13 혹은 rot13이라고도 쓴다. 아래 그림에서 보는 바와 같이 “info”를 암호화하면 “vasb”가 된다.




Tip! : ROT13은 ROT(N)으로 응용이 가능하기 때문에 해당 문제가 출제되면 첫 번째 글자면 밀어보면 답을 찾을 수 있을 것이다.

18. 무선랜에서의 인증 방식에 대한 설명 중 옳지 않은 것은?
① WPA 방식은 48비트 길이의 초기벡터(Ⅳ)를 사용한다.
② WPA2 방식은 AES 암호화 알고리즘을 사용하여 좀 더 강력한 보안을 제공한다.
③ WEP 방식은 DES 암호화 방식을 이용한다.
④ WEP 방식은 공격에 취약하며 보안성이 약하다.
정답 체크 :
(3) WEP는 RC4 암호화 방식을 이용한다.
오답 체크 :
(1) WEP는 24비트 초기벡터를 사용하는데, WPA는 48비트 초기벡터를 사용한다.
(2) WPA는 RC4를 사용하나, WPA2는 AES를 사용한다.
(4) WEP는 키의 비트 길이가 짧기 때문에 보안에 약하다.

19. 다음 중 ISO 27001의 통제 영역별 주요 내용으로 옳은 것은?
① 정보보안 조직 : 정보보호에 대한 경영진의 방향성 및 지원을 제공
② 인적 자원 보안 : 정보에 대한 접근을 통제
③ 정보보안 사고 관리: 사업장의 비인가된 접근 및 방해 요인을 예방
④ 통신 및 운영 관리 : 정보처리시설의 정확하고 안전한 운영을 보장
정답 체크 :
(4) 통신 및 운영 관리 : 정보처리 시설의 정확하고 안전한 운영을 위한 통제항목이다.
오답 체크 :
(1) 정보보안 조직 : 해당 설명은 보안 정책에 해당되고, 정보보안 조직은 조직 내에서 정보보호를 관리하는데 사용하는 통제항목이다.
(2) 인적 자원 보안 : 해당 설명은 접근 통제에 해당되고, 인적 자원 보안은 인적 오류, 절도, 사기, 시설의 오용에 따른 위험을 줄이기 위한 것이다.
(3) 정보보안 사고 관리 : 해당 설명은 물리적 & 환경적 보안을 의미하고, 정보보안 사고 관리는 침해사고에 대한 대응 및 절차의 수립 및 이행을 위한 통제항목이다.

20. 「개인정보보호법」에 따르면 주민등록번호를 처리하기 위해서는 법에서 정하는 바에 따라야 하는데, 그에 대한 내용 중 옳지 않은 것은?
① 주민등록번호 처리는 원칙적으로 금지되고 예외적인 경우에만 허용한다.
② 주민등록번호는 암호화 조치를 통해 보관해야 한다.
③ 개인정보처리자는 법령에서 주민등록번호의 처리를 허용 한 경우에도 주민등록번호를 사용

하지 않는 인터넷 회원 가입 방법을 정보주체에게 제공해야 한다.
④ 기 보유한 주민등록번호는 수집 시 동의 받은 보유기간 까지만 보유하고 이후에는 즉시 폐기해야 한다.
정답체크 :
(4)
“개인정보 보호법” 부칙 제2조(주민등록번호 처리 제한에 관한 경과조치) 상 ① 이 법 시행 당시 주민등록번호를 처리하고 있는 개인정보처리자는 이 법 시행일부터 2년 이내에 보유하고 있는 주민등록번호를 파기하여야 한다. 다만, 제24조의2제1항 각 호의 개정규정의 어느 하나에 해당하는 경우는 제외한다. ② 제1항에 따른 기간 이내에 보유하고 있는 주민등록번호를 파기하지 아니한 경우에는 제24조의2제1항의 개정규정을 위반한 것으로 본다.
오답 체크 :
(1), (2), (3)
“개인정보 보호법” 제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다. ③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.