2014-국회직-정보보호론-가형-해설

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

1. TCP SYN flood 공격에 대해 가장 바르게 설명한 것은?
① 브로드 캐스트 주소를 대상으로 공격
② TCP 프로토콜의 초기 연결 설정 단계를 공격
③ TCP 패킷의 내용을 엿보는 공격
④ 통신 과정에서 사용자의 권한 탈취를 위한 공격
⑤ TCP 패킷의 무결성을 깨뜨리는 공격
해설)
정답 체크 :
(2) 초기 연결설정 단계 : 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.
오답 체크 :
(1) 브로드캐스트 주소 : Smurf(ping flooding) 공격에 해당한다.
(3) 패킷의 내용 : 스니핑(Sniffing) 공격에 해당한다.
(4) 사용자의 권한 탈취 : 세션 하이재킹(Session Hijacking) 공격에 해당한다.
(5) 무결성 : 세션 하이재킹(Session Hijacking) 공격에 해당한다.

2. 다음 중 로봇 프로그램과 사람을 구분하는 방법의 하나로 사람이 인식할 수 있는 문자나 그림을 활용하여 자동 회원 가입 및 게시글 포스팅을 방지하는데 사용하는 방법은?
① 해쉬 함수
② 캡차(CAPTCHA)
③ 전자서명
④ 인증서
⑤ 암호문
해설)
정답 체크 :
(2) 캡차 : 어떠한 사용자가 실제 사람인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법이다. 사람은 구별할 수 있지만 컴퓨터는 구별하기 힘들게 의도적으로 비틀거나 덧칠한 그림을 주고 그 그림에 쓰여 있는 내용을 물어보는 방법이 자주 사용된다.
오답 체크 :
(1) 해쉬함수 : 임의의 길이의 데이터를 고정된 길이의 데이터로 매핑하는 함수이다. 암호학에서 매핑된 해싱 값만을 알아가지고는 원래 입력 값을 알아내기 힘들다는 사실에 의해 사용될 수 있다.
(3) 전자서명 : 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는 데

이용하려고, 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다. 공개 키 기반 구조(PKI) 기술측면에서 전자서명이란 전자문서의 해시(HASH)값을 서명자의 개인키(전자서명생성정보)로 변환(암호화)한 것으로서 RSA사에서 만든 PKCS#7 의 표준이 널리 사용되고 있다. 디지털 서명은 송신자가 자신의 신원을 증명하는 절차이고, 전자서명은 그 절차의 특정 단계에서 사용하는 정보이다.
(4) 인증서 : 전자 서명의 검증에 필요한 공개키(전자서명법에는 전자서명검증정보로 표기)에 소유자 정보를 추가하여 만든 일종의 전자 신분증(증명서)이다. 공인 인증서, 공개키 증명서, 디지털 증명서, 전자 증명서 등으로도 불린다. 공인인증서는 개인키(전자서명법에는 전자서명생성정보로 표기)와 한 쌍으로 존재한다.
(5) 암호문 : 암호화한 후의 메시지로 중간에서 도청자가 암호문을 가로채어 갖게 된다고 하더라고 특정 비밀값을 모른다면 암호문을 평문으로 복호화 할 수 없다.

3. Bell-LaPadula 보안 모델은 다음 중 어느 요소에 가장 많은 관심을 가지는 모델인가?
① 비밀성(Confidentiality)
② 무결성(Integrity)
③ 부인방지(Non-repudiation)
④ 가용성(Availability)
⑤ 인증(Authentication)
해설)
정답 체크 :
(1) 비밀성 : Bell-LaPadula 모델은 미 국방부 지원 보안 모델로 보안 요소 중 기밀성 강조한다.
오답 체크 :
(2) 무결성 : Biba 모델은 BLP의 단점을 보완한 무결성을 보장하는 최초의 모델이다. Clark-Wilson은 무결성 중심의 상업용 모델로 설계된 모델이다.

4. 네트워크의 OSI 3계층 주소(IP 주소)와 연관된 2계층 주소(MAC 주소)를 틀리게 알려주어서 정보를 가로채는 데에 활용되는 공격 기법은?
① Smurf 공격
② Teardrop 공격
③ DDoS 공격
④ ARP Spoofing 공격
⑤ Phishing 공격
해설)
정답 체크 :
(4) 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.
오답 체크 :
(1) Smurf : 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스

거부 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.
(2) Teardrop : 데이터의 송수신과정에서 데이터의 송신한계를 넘으면 MTU(1500byte) 조각으로 나누어 fragment number를 붙여 송신하고, 수신측에는 fragment 넘버로 재조합하여 분석한다. fragment 내의 나누어진 byte 정보인 fragmentation offset을 위조하여 offset을 중복되게 하거나 공간을 두면 수신측에서 재조합이 안 되어 다운이 되게 하는 공격이다.
(3) DDoS : 악성코드(봇)에 의한 에이전트를 전파하고, 좀비 PC에 의한 공격을 수행한다. 좀비 PC로 구성된 네트워크를 봇넷(Botnet)이라고 한다. DoS는 1:1로 공격하지만, DDoS는 N:1로 공격을 수행한다.
(5) Phishing : rivate data(개인 정보)와 fishing(낚는다)의 합성어이다. 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 금융정보와 같은 개인정보를 빼내는 사기기법을 말한다.

5. 다음 중 사이버 환경에서 사용자 인증의 수단으로 가장 적절하지 않은 것은?
① 패스워드
② 지문
③ OTP(One Time Password)
④ 보안 카드
⑤ 주민등록번호
해설)
정답 체크 :
(5) 주민등록번호 : 주민등록번호는 노출이 될 수 있기 때문에 주민등록번호 자체만으로는 사용자 인증이 될 수 없다. 사용자 인증의 보조 수단으로 사용될 수는 있다.
오답 체크 :
(1) 패스워드 : 지식 기반 인증에 사용한다.
(2) 지문 : 생체 기반 인증에 사용한다.
(3) OTP : 소지 기반 인증에 상용한다.
(4) 보안카드 : 소지 기반 인증에 상용한다.

6. 다음 중 소인수 분해 문제의 어려움에 기초한 암호 알고리즘은 무엇인가?
① Diffie-Hellman
② SHA-1
③ AES
④ DES
⑤ RSA
해설)
정답 체크 :
(5) RSA : 소인수 분해 문제의 어려움에 기초한다.
오답 체크 :
(1) Diffie-Hellman : 이산대수 문제의 어려움에 기초한다.

(2) SHA-1 : 해쉬의 특성(일방향성, 충돌 내성 등)에 기초한다.
(3) AES : SPN 구조에 기초한다.
(4) DES : 페이스텔 구조에 기초한다.

7. 인터넷 뱅킹 등에서 숫자를 화면에 무작위로 배치하여 마우스나 터치로 비밀번호를 입력하게하는 가상 키보드의 사용 목적으로 가장 적절한 것은?
① 키보드 오동작 방지
② 키보드 입력 탈취에 대한 대응
③ 데이터 입력 속도 개선
④ 비밀번호의 무결성 보장
⑤ 해당 서비스의 가용성 보장
해설)
정답 체크 :
(2) 가상 키보드 : 숫자를 화면에 무작위로 배치하여 마우스나 터치로 비밀번호를 입력하게 하면 동일한 자판의 배열로 입력된 것이 아니기 때문에 keylog와 같은 키보드 입력 탈취에 대응할 수 있다.

8. 다음 NTFS 파일시스템에 대한 설명 중 옳지 않은 것은?
① 파티션에 대한 접근 권한 설정이 가능함
② 사용자별 디스크 사용 공간 제어 가능
③ 기본 NTFS 보안 변경 시 사용자별 NTFS 보안 적용 가능
④ 미러(Mirror)와 파일 로그가 유지되어 비상시 파일 복구 가능
⑤ 파일에 대한 압축과 암호화를 지원하지 않음
해설)
오답 체크 :
(5) 압축과 암호화 : LZ77(1977년에 만들어낸 무손실 데이터 압축 알고리즘)의 변형된 알고리즘을 사용하여 파일 데이터를 압축한다. FES(Encrypting File System) 기능으로 파일을 암호화하고 빠른 암호화/복호화를 위해 FEK(Eile Encryption Key)를 통한 대칭키 방식의 암호화를 수행한다.
정답 체크 :
(1) 접근 권한 : 2개의 ACL(Discretionary ACL, System ACL)을 이용하여 접근 권한을 설정한다.
(2) 사용 공간 제어 : Quotas를 이용하여 사용자별 디스크 사용량을 제한한다.
(3) 사용자별 NTFS 보안 적용 : 사용자별 또는 그룹별 보안 적용이 가능하다.
(4) 비상 시 파일 복구 : USN 저널을 사용하여 파일의 모든 변경 내용을 로그로 기록한다. 시스템 오류 발생으로 재부팅될 경우 잘못된 처리 작업을 롤백(Rollback)한다.

9. '정보통신망 이용촉진 및 정보보호 등에 관한 법률'은 정보통신망의 안전성을 확보하기 위한 목적으로 정보보호 최고책임자의 업무를 규정하고 있다. 다음 중 정보보호 최고책임자의 업무에 해당 되지 않은 것은?
① 보안서버 적합성 검토

② 사전 정보보호 대책 마련
③ 침해사고의 예방 및 대응
④ 정보보호 관리체계의 인증 심사
⑤ 정보보호 사전 보안성 검토
해설)
오답 체크 :
(4) 정보보호 관리체계의 인증 심사는 정보보호 관리체계 심사기관에서 수행하고, 심사기관이란 “정보보호 관리체계 인증 등에 관한 고시”에 따라 미래창조과학부가 인증심사 업무를 수행할 수 있도록 지정한 기관을 말한다.
정답 체크 :
(1), (2), (3), (5) “정보통신망 이용촉진 및 정보보호 등에 관한 법률” 제45조의3(정보보호 최고책임자의 지정 등)에 명시된 정보보호 최고책임자의 총괄 업무는 다음과 같다.
1. 정보보호관리체계의 수립 및 관리·운영, 2. 정보보호 취약점 분석·평가 및 개선, 3. 침해사고의 예방 및 대응, 4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등, 5. 정보보호 사전 보안성 검토, 6. 중요 정보의 암호화 및 보안서버 적합성 검토, 7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

10. 다음 설명에 해당하는 정보보호 평가기준은?

- 국제적으로 통용되는 제품 평가 기준 - 현재 ISO 표준으로 제정되어 있음 - 일반적인 소개와 일반 모델, 보안기능 요구사항, 보증 요구 사항 등으로 구성되어 있음

① CC
② BS 7799
③ ITSEC
④ TCSEC
⑤ TNI
해설)
정답 체크 :
(1) CC : CC라는 기준으로 TCSEC과 ITSEC은 통합되었다. 1996년에 초안이 나와 1999년에 국제 표준으로 승인되었다. PP, ST, TOE라는 인증 과정을 거친다.
오답 체크 :
(2) BS 7799 : 정보 보안 경영 시스템의 개발, 수립 및 문서화에 대한 요구 사항들을 정한 국제 인증 규격이다. 1995년 영국 표준으로 제정된 것으로 1999년 개정을 거쳐 국제표준화기구(ISO)에 의해 국제 표준으로도 제정되었다(ISO 27001).
(3) ITSEC : 1991년 5월 유럽 국가들이 발표한 공동 보안 지침서이다. TCSEC이 기밀성만을 강조한 것과 달리 무결성과 가용성을 포괄하는 표준안을 제시하였다.
(4) TCSEC : 흔히 Orange Book이라고 부르며, Rainbow Series라는 미 국방부 문서 중 하나이다. 1960년대부터 시작된 컴퓨터 보안 연구를 통하여 1972년에 그 지침이 발표되었다. 1983년에 미국 정보 보안 조례로 세계에 최초로 공표되었고 1995년에 공식화되었다.
(5) TNI : 흔히 Red Book이라고 부르며, Rainbow Series라는 미 국방부 문서 중 하나이다. LAN과 인트라넷(Intranet)의 보안을 다룬다.

11. 웹 쿠키에 대한 설명으로 가장 옳지 않은 것은?
① 웹 서비스 사용자의 PC 저장소에 저장 됨
② 웹 서비스의 세션을 유지하는 데 사용 될 수 있음
③ 서버에서 웹 서비스 사용자의 접근 기록을 추적할 수 있음
④ 쿠키는 Java Script 같은 웹 개발 언어를 통해서는 접근이 불가함
⑤ 상태 정보를 저장하지 않는 HTTP를 보완하기 위한 기술임
해설)
정답 체크 :
(4) Java Script로 접근이 불가 : 자바 스크립트는 document.cookie 속성으로 쿠키를 만들고, 읽고, 삭제할 수 있다.
오답 체크 :
(1) 사용자의 PC 저장소에 저장 : 인터넷 사용자가 어떠한 웹사이트를 방문할 경우 그 사이트가 사용하고 있는 서버를 통해 인터넷 사용자의 컴퓨터에 설치되는 작은(4KB) 기록 정보 파일이다.
(2) 세션을 유지 : 쿠키는 영구 쿠키와 세션 쿠키가 있는데 세션 쿠키는 세션을 유지하는데 사용될 수 있다.
(3) 접근 기록 추적 : 쿠키에는 접근 기록이 있고, 클라이언트가 서버에 접속할 때 쿠키를 전송하므로 서버가 해당 접근 기록을 추적할 수 있다.
(5) 상태정보 : 일반적으로 HTTP는 무상태(stateless)이다. 즉, 연결을 맺고 연결을 끊음으로써 어떠한 상태 정보도 가지고 있지 않는다. 이를 보완하기 위해 쿠키를 사용한다.

12. 다음은 '전자서명법'에서 공인인증기관의 업무 수행에 관한 조항이다. 괄호 안에 들어갈 말은?

(　　)은 인증 업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증 업무 수행에 있어 지 켜야 할 구체적 사항을 전자서명인증업무지침으로 정하여 고시 할 수 있다.

① 미래창조과학부 장관
② 개인정보보호위원장
③ 국가정보원장
④ 산업통상자원부 장관
⑤ 공정거래위원장
해설)
정답 체크 :
(1) "전자서명법" 제8조(공인인증기관의 업무수행) : 과학기술정보통신부장관(예전 : 미래창조과학부장관)은 인증업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증업무수행에 있어 지키어야 할 구체적 사항을 전자서명인증업무지침으로 정하여 고시할 수 있다.
Tip! : 해당 장관의 이름은 해당 조직이 해산되면 바뀔 수 있으므로 최신 관련 법규를 확인해 봐야 한다.

13. 커버로스(Kerberos)에 대한 설명 중 맞는 것은?
① 커버로스는 공개키 암호를 사용하기 때문에 확장성이 좋다.

② 커버로스 서버는 서버인증을 위해 X.509 인증서를 이용한다.
③ 커버로스 서버는 인증 서버와 티켓 발행서버로 구성된다.
④ 인증 서버가 사용자에게 발급한 티켓은 재사용 할 수 없다.
⑤ 커버로스는 two party 인증 프로토콜로 사용 및 설치가 편리하다.
해설)
정답 체크 :
(3) 인증 서버와 티켓발행서버 : AS(Authentication Server)와 TGS(Ticket Granting Server)로 구성된다.
오답 체크 :
(1) 공개키 암호 : 대칭키 암호를 사용한다. 전체적인 과정 중에 일부분을 공개키 암호로 사용할 수 있지만 전체적으로는 대칭키 암호를 기반으로 한다.
(2) 서버 인증 : 클라이언트가 티켓(Ticket)을 통해 보내온 타임스탬프(TS)를 이용한다.
(4) 티켓 재사용 : 인증 서버가 발생한 TGT는 서비스 유형마다 한번 발급되므로 동일 서비스 유형에 대해서는 재사용이 가능하다.
(5) two party 인증 프로토콜 : two party는 서버와 클라이언트만 존재하는 것이고, 커버로스는 TTP(Trusted Third Party, 신뢰된 서드 파티) 인증 프로토콜이다(클라어언, 서버, 인증 서버 및 티켓발행서버가 존재).

14. 다음은 공격자가 남긴 C 프로그램 파일과 실행 파일에 관한 정보이다. 제시된 정보로부터 유추할 수 있는 공격으로 가장 적합한 것은?

```
$ ls -l
total 20
-rwsr-xr-x 1 root root 12123 Sep 11 11:11 util
-rw-rw-r-- 1 root root     70 Sep 11 11:11 util.c
$ cat util.c
# include <stdlib.h>
void main() {
   setuid(0);
   setgid(0);
   system("/bin/bash");
}
```

① Eavesdropping 공격
② Brute Force 공격
③ Scanning 공격
④ Backdoor 공격
⑤ 패스워드 유추 공격
해설)
정답 체크 :
(4) Backdoor : 공격자가 백도어를 통해 남긴 파일은 SetUID 비트가 설정되어 있다. 이는 공격자가 해당 파일을 실행하면 루트 권한을 획득함을 의미한다. 실행 파일의 내용은 공격자(user id)를 루트로 설정하고, 공격자의 그룹(group id)을 루트로 설정한 후 쉘(bash shell)을

실행한다.
오답 체크 :
(1) Eavesdropping : 도청을 의미한다.
(2) Brute Force : 가능한 모든 조합을 이용(대입)해서 공격하는 것을 의미한다.
(3) Scanning : IP 혹은 포트가 열려있는지를 확인하기 위해서 사용한다.
(5) 패스워드 유추 : 주어진 정보를 이용해서 패스워드를 유추하는 것을 의미한다.

15. 다음 중 공인인증서에 포함되지 않은 것은?
① 가입자의 이름
② 가입자의 전자서명검증정보
③ 공인인증기관의 서명키
④ 공인인증서의 일련번호
⑤ 공인인증서의 유효기간
해설)
정답 체크 :
(3) 공인인증기관의 서명키는 공인인증기관의 개인키로서 공인인증기관만이 가지고 있어야 하므로 공인인증서에 포함되면 안된다.
오답 체크 :
(1), (2), (4), (5) “전자서명법” 제15조(공인인증서의 발급) 상 공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다. 1. 가입자의 이름(법인의 경우에는 명칭을 말한다), 2. 가입자의 전자서명검증정보, 3. 가입자와 공인인증기관이 이용하는 전자서명 방식, 4. 공인인증서의 일련번호, 5. 공인인증서의 유효기간, 6. 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보, 7. 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항, 8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격등의 표시를 요청한 경우 이에 관한 사항, 9. 공인인증서임을 나타내는 표시

16. 사진이나 텍스트 메시지 속에 데이터를 잘 보이지 않게 은닉하는 기법으로서, 9.11 테러 당시 테러리스트들이 그들의 대화를 은닉하기 위해 사용한 기법은?
① 전자서명
② 대칭키 암호
③ 스테가노그라피(Steganography)
④ 영지식 증명
⑤ 공개키 암호
해설)
정답 체크 :
(3) 스테가노그라피 : 메시지의 내용을 읽지 못하게 하는 것이 아니라, 메시지의 존재 자체를 숨기는 기법이다. 메시지를 숨겨 넣는 방법을 알게 되면 메시지의 내용은 금방 노출된다.
오답 체크 :
(1) 전자서명 : 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는 데 이용하려고, 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다. 공개 키 기반 구조(PKI) 기술측면에서 전자서명이란 전자문서의 해시(HASH)값을 서명자의 개

인키(전자서명생성정보)로 변환(암호화)한 것으로서 RSA사에서 만든 PKCS#7 의 표준이 널리 사용되고 있다. 디지털 서명은 송신자가 자신의 신원을 증명하는 절차이고, 전자서명은 그 절차의 특정 단계에서 사용하는 정보이다.
(2) 대칭키 암호 : 암호화키(비밀키, 비공개)와 복호화키(비밀키, 비공개)가 동일한 암호를 의미한다. 속도가 빠르나 키 배송 문제가 있다.
(4) 영지식 증명 : 암호학에서 누군가가 상대방에게 어떤 사항(statement)이 참이라는 것을 증명할 때, 그 문장의 참 거짓 여부를 제외한 어떤 것도 노출되지 않는 interactive한 절차를 뜻한다. 예를 들어, 관리자에게 패스워드를 노출하지 않고 패스워드를 알고 있다는 사실을 증명하는 것을 의미한다.
(5) 공개키 암호 : 암호화키(공개키, 공개)와 복호화키(개인키, 비공개)가 틀린 암호를 의미한다. 속도가 느리나 키 배송 문제가 없다.

17. 다음은 정보보호의 3대 기본 목표 중 무엇에 대한 설명인가?

권한이 없는 사용자들은 컴퓨터 시스템 상의 데이터 또는 컴퓨터 시스템 간에 통신 회선을 통 하여 전송되는 데이터의 내용을 볼 수 없게 하는 기능

① 비밀성(Confidentiality)
② 가용성(Availability)
③ 신뢰성(Reliability)
④ 무결성(Integrity)
⑤ 책임추적성(Accountability)
해설)
정답 체크 :
(1) 비밀성(기밀성) : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.
오답 체크 :
(2) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.
(3) 신뢰성 : 의도된 행위에 대한 결과의 일관성을 유지하는 것으로 정보나 정보시스템을 사용함에 있어서 일관되게 오류의 발생 없이 계획된 활동을 수행하여 결과를 얻을 수 있도록 하는 환경을 유지하는 것이다.
(4) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(5) 책임추적성 : 사용자 식별 및 활동 감사 추적을 의미하고, 책임성이라고도 한다.

18. 다음 중 전자 상거래를 위한 신용 카드 기반의 전자지불 프로토콜은?
① SSL(Secure Socket Layer)
② PGP(Pretty Good Privacy)
③ OTP(One Time Password)
④ SSO(Single Sign On)
⑤ SET(Secure Electronic Transaction)
해설)

정답 체크 :
(5) SET : 전자상거래 당사자들에게 신뢰성과 안전성을 제공하기 위하여 인증, 비밀성 등의 보안 기능과 지불 기능을 제공하는 전자상거래 전용 프로토콜이다.
오답 체크 :
(1) SSL : 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜이다. 웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에 적용할 수 있다.
(2) PGP : 전자우편의 안전성을 위해 1991년 미국의 Phil Zimmermann에 의해 개발된 전자우편 보안 시스템이다.
(3) OTP : 고정된 비밀번호 대신 사용되는 매번 새롭게 바뀌는 일회용 비밀번호이다. S/KEY 방식, 시간 동기화 방식, 챌린지/응답 방식, 이벤트 동기화 방식 등이 있다.
(4) SSO : 모든 인증을 하나의 시스템에서 한다는 의미이다. 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면, 다른 시스템에 대한 접근 권한도 모두 얻는다. 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos)를 이용한 윈도우의 액티브 디렉토리(Active Directory)가 있다.

19. 정보보호를 위해 사용되는 해쉬 함수(Hash function)에 대한 설명 중 옳지 않은 것은?
① 주어진 해쉬값에 대응하는 입력값을 구하는 것이 계산적으로 어렵다.
② 무결성을 제공하는 메시지 인증 코드(MAC) 및 전자서명에 사용된다.
③ 해쉬값의 충돌은 출력공간이 입력공간보다 크기 때문에 발생한다.
④ 동일한 해쉬값을 갖는 서로 다른 입력값들을 구하는 것이 계산적으로 어렵다.
⑤ 입력값의 길이가 가변이더라도 고정 된 길이의 해쉬값을 출력한다.
해설)
정답 체크 :
(3) 충돌 : 입력공간이 출력공간보다 크기 때문에 발생한다. 즉, 입력 메시지를 계속해서 늘리면 출력값이 같은 메시지들이 존재하여 충돌이 발생한다.
오답 체크 :
(1) 해쉬값에 대응하는 입력값 : 일방향성을 의미한다.
(2) MAC 및 전자서명 : HMAC과 같이 MAC을 만들 때 해쉬를 이용할 수 있다. 속도를 빠르게 하기 위해 메시지의 해쉬값에 서명을 한다.
(4) 서로 다른 입력값 : 강한 충돌 내성을 의미한다.
(5) 고정된 길이의 해쉬값 : 입력이 1bit 혹은 1Tbit라도 고정된 길이의 출력을 가진다.

20. 대칭키 암호에 대한 설명으로 옳지 않은 것은?
① 공개키 암호 방식보다 암호화 속도가 빠르다.
② 비밀키 길이가 길어 질수록 암호화 속도는 빨라진다.
③ 대표적인 대칭키 암호 알고리즘으로 AES, SEED 등이 있다.
④ 송신자와 수신자가 동일한 비밀키를 공유해야 된다.
⑤ 비밀키 공유를 위해 공개키 암호 방식이 사용 될 수 있다.
해설)
오답 체크 :

(2) 비밀키 길이 : AES의 경우 비밀키의 길이가 길어지면 라운드 수가 증가하여 암호화 속도가 느려진다.
정답 체크 :
(1) 암호화 속도 : 공개키 암호는 두 키의 수학적 특성에 기반하기 때문에, 메시지를 암호화 및 복호화 하는 과정에 여러 단계의 산술 연산이 들어간다. 따라서 대칭키 암호에 비하여 속도가 매우 느리다는 단점을 지니고 있다.
(3) 알고리즘 : DES, 3-DES, AES, SEED, Blowfish, IDEA, RC4, RC5, RC6 등이 존재한다.
(4) 동일한 비밀키 : 암호화키와 복호화키가 동일하다.
(5) 비밀키 공유 : 공개키를 사용하면 암호화키는 공개하기 때문에 대칭키에 발생하는 키 배송 문제가 없다.