2015-국회직-정보보호론-가형-해설

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

1. AES 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① Rijndael 알고리즘이 AES로 선정되었다.

② 블록 길이가 128 비트인 대칭 블록 암호이다.

③ 키의 길이에 따라 10, 12, 14 라운드를 가진다.

④ 키의 길이는 128, 192, 256 비트를 지원한다.

⑤ 페이스텔(Feistel) 구조를 기반으로 작성되었다.

오답 체크 :

(5) Feistel 구조 : SPN 구조를 기반으로 작성되었다.

정답 체크 :

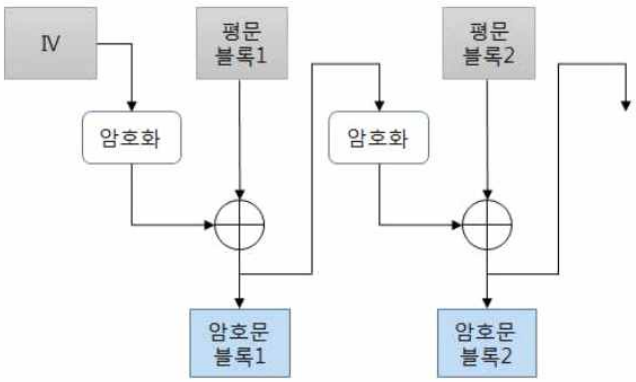
(1) Rijndael : Rijndael(라인델)이 다른 후보(MARS, RC6, Serpent, Twofish)를 누르고 NIST에 의해 AES로서 선정되었다.

(2) 블록 길이 : 128비트의 블록 길이를 가진다.

(3) 라운드 : 키의 길이에 따라 10, 12, 14 라운드를 가진다.

(4) 키 : 키의 길이는 128, 192, 256 비트를 지원한다.

2. 다음 그림이 나타내는 블록 암호 운용 모드는?



① ECB

② CBC

③ CFB

④ OFB

⑤ CTR

정답 체크 :

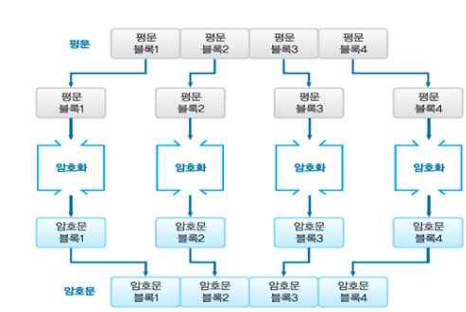
(3) CFB : 이전 단계의 암호문 블록을 암호화한 후 현재 단계의 평문 블록과 XOR해서 암호문 블록을 만든다.

오답 체크 :

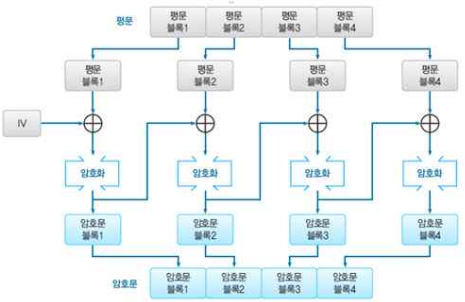
(1) ECB : 개별적으로 평문 블록을 암호화해서 암호문 블록으로 만든다.

(2) CBC : 이전 단계의 암호문 블록과 현재 단계의 평문 블록을 XOR해서 암호문 블록을 만

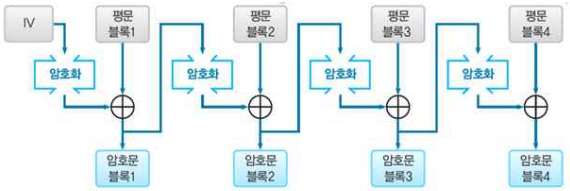
든다.
(4) OFB : 이전 단계의 출력 블록(평문 블록과 XOR해서 암호문 블록을 만들기 전 단계)을 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다.
(5) CTR : 개별적으로 카운터를 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다.
Tip! : 이들을 그림으로 나타내면 다음과 같다.



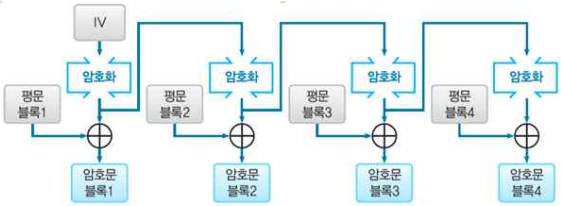
(a) ECB 모드에 의한 암호화



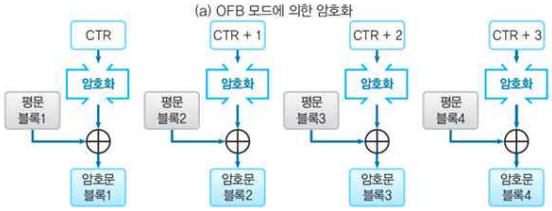
(a) CBC 모드에 의한 암호화



(a) CFB 모드에 의한 암호화



(a) OFB 모드에 의한 암호화



(a) CTR 모드에 의한 암호화

3. 키 분배 문제를 해결하기 위한 방법으로 옳지 않은 것은?
① 키를 사전에 공유
② 공개키 암호를 사용
③ Diffie-Hellman 알고리즘을 이용
④ 키배포센터(KDC)를 이용
⑤ SEED 암호 알고리즘을 이용
오답 체크 :
(5) SEED : 키를 SEED 알고리즘으로 암호화했다고 하더라도, 키를 암호화는데 필요한 키를 전송하는 문제가 발생한다. 즉, 해결 방법이 아니라 키 분배 문제가 발생한다.
정답 체크 :
(1) 공유 : 키를 사전에 공유하면, 키를 배송하지 않아도 된다.
(2) 공개키 : 개인키는 가지고 있고, 공개키를 공개하면 키를 배송하지 않아도 된다.
(3) Diffie-Hellman : 난수를 서로 교환하는 것만으로 비밀키를 만들어내므로, 키를 배송하지 않아도 된다.
(4) KDC : KDC와 사전에 공유된 비밀키를 이용하여 세션키를 만들면, 키 배송 문제를 해결할 수 있다.

4. TCP/IP 프로토콜 계층과 각 계층에서 구현되는 보안 기술의 연결로 옳은 것은?
① 응용 계층 - Kerberos

② 전송 계층 - IPSec
③ 네트워크 계층 - TLS
④ 데이터 링크 계층 - SSL
⑤ 물리 계층 - SET
정답 체크 :
(1) Kerberos : 응용 계층
오답 체크 :
(2) IPSec : 네트워크 계층
(3) TLS : 전송 계층(정확하게 정의하면 전송 계층과 응요 계층 사이에 존재한다.)
(4) SSL : 전송 계층(정확하게 정의하면 전송 계층과 응요 계층 사이에 존재한다.)
(5) SET : 응용 계층

5. 다음 중 충돌 저항성(Collision Resistance)과 관련이 높은 알고리즘은?
① AES
② DES
③ SHA-1
④ RSA
⑤ ECC
정답 체크 :
(3) SHA-1 : 충돌 저항성(약한 충돌, 강한 충돌)은 해시 함수에서 발생한다.
오답 체크 :
(1) AES : 대칭키 암호
(2) DES : 대칭키 암호
(4) RSA : 공개키 암호
(5) ECC : 공개키 암호

6. 특정한 목표를 겨냥해서 사전에 치밀하게 계획한 다음 장기적으로 집중적이고 은밀하게 공격 하는 수법은?
① DDoS 공격
② 리버스 엔지니어링 공격
③ 레이스 컨디션 공격
④ 세션 하이재킹 공격
⑤ APT 공격
정답 체크 :
(5) APT : 특정 기업 또는 기관의 핵심 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 공격자는 장기간 동안 공격 대상에 대해 IT인프라, 업무환경, 임직원 정보 등 다양한 정보를 수집하고, 이를 바탕으로 제로 데이 공격, 사회공학적 기법 등을 이용하여 공격 대상이 보유한 취약점을 수집·악용해 공격을 실행하는 것을 말한다.
오답 체크 :
(1) 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.
(2) 리버스 엔지니어링 : 장치나 시스템의 구조를 분석하여 원리를 발견하는 과정이다. 예를 들면, 실행 파일을 분석해서 소스 코드를 얻는 작업이다. 이미 만들어진 프로그램 동작 원리를 이해하거나 바이러스 또는 웜을 제작할 때 사용한다.
(3) 레이스 컨디션 : 한정된 자원을 동시에 이용하려는 여러 프로세스가 자원의 이용을 위해 경쟁을 벌이는 현상이다. 레이스 컨디션을 이용하여 root 권한을 얻는 공격을 의미한다.
(4) 세션 하이재킹 : 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.

7. XSS(Cross Site Scripting)에 대한 설명으로 옳지 않은 것은?
① 웹페이지가 사용자에게 입력 받은 데이터를 필터링 하지 않고 그대로 동적으로 생성된 웹페이지에 포함하여 사용자에게 재전송할 때 발생한다.
② 해킹을 통해 시스템 권한을 획득한 후 시스템에 직접 명령을 입력할 수 있는 쉘을 실행한다.
③ 쿠키를 통해 웹페이지 사용자의 정보 추출을 할 수 있다.
④ 클라이언트에서 실행되는 언어로 작성된 악성 스크립트 코드를 게시판, 이메일 등에 포함시켜 전달한다.
⑤ 웹사이트에 방문하는 사용자를 악성코드가 포함되어 있는 사이트로 리다이렉션 시킬 수도 있다.
오답 체크 :
(2) 해킹 : XSS 공격이 아니라, 백도어 공격에 해당한다.
정답 체크 :
(1) 재전송 : 반사 XSS 공격에 해당한다. 웹 애플리케이션의 지정된 변수를 이용할 때 발생하는 취약점을 이용하는 것으로, 검색 결과, 에러 메시지 등 서버가 외부에서 입력받은 값을 받아 브라우저에게 응답할 때 전송하는 과정에서 입력되는 변수의 위험한 문자를 사용자에게 그대로 돌려주면서 발생한다.
(3) 쿠키 : XSS 공격을 당하면 클라이언트의 쿠키가 공격자에게 전송된다.
(4) 게시판, 이메일 : 저장 XSS 공격에 해당한다. 웹 사이트의 게시판, 사용자 프로필 및 코멘트 필드 등에 악성 스크립트를 삽입해 놓으면, 사용자가 사이트를 방문하여 저장되어 있는 페이지에 정보를 요청할 때, 서버는 악성 스크립트를 사용자에게 전달하여 사용자 브라우저에서 스크립트가 실행되면서 공격한다.
(5) 리다이렉션 : XSS 공격을 당하면 악성 프로그램을 다운로드 할 수 없지만, 악성 프로그램을 다운로드 받는 사이트로 리다이렉트할 수 있다.

8. 다음에서 설명하는 보안 공격 은?

피싱(phishing) 보다 한 단계 진화된 수법으로 진짜 사이트 주소를 입력하더라도 가짜 사이트 로 접속을 유도해 개인정보를 훔치는 수법이다. 즉, 합법적으로 소유하고 있던 사용자의 도 메인을 탈취하거나 도메인 네임 시스템(DNS) 또는 프락시 서버의 주소를 변조함

으로써 사용자들로 하여금 진짜 사이트로 오인하여 접속하도록 유도한 뒤에 개인정보를 훔치는 공격 기 법이다.

① 파밍(Pharming) 공격
② 스미싱(Smishing) 공격
③ ARP 스푸핑(Spoofing) 공격
④ 세션 하이재킹(Session Hijacking) 공격
⑤ 중간자 개입(Man-in-the-middle) 공격

정답 체크 :

(1) 파밍 : Phishing(개인 정보)과 farming(대규모 피해)의 합성어이다. DNS Spoofing과 같이 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법이다.

오답 체크 :

(2) 스미싱 : SMS(문자 메시지)와 Phishing의 약자이다. Phishing은 Private Data(개인 정보)와 Fishing(낚시)의 약자이다. 공격자가 문자 메시지에 URL을 보내고, 사용자가 이를 클릭하면 해킹 툴이 스마트폰에 설치되어 개인 정보가 탈취된다.

(3) ARP 스푸핑 : 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.

(4) 세션 하이재킹 : TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 넘버를 사용한다. 이 시퀀스 넘버가 잘못되면 이를 바로잡기 위한 작업을 하는데, 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식이다.

(5) 중간자 개입 : 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다. 중간자 공격은 통신을 연결하는 두 사람 사이에 중간자가 침입하여, 두 사람은 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달한다.

9. 암호화가 필요한 정보들 중에서 정보주체를 제외하고 정보를 다루는 관리자조차 암호화된 정보의 원래 정보가 무엇인지 알 수 없어야 하는 정보는?

① 은행계좌번호
② 주민등록번호
③ 신용카드번호
④ 비밀번호
⑤ 여권번호

정답 체크 :

(4) 비밀번호 : 비밀번호를 분실했을 때 예전에는 관리자가 알 수 있었으나 현재는 임시 비밀번호를 설정해서 알려주거나, 아예 본인인증이 되면 새 비밀번호를 입력하도록 하는 형태로 바뀐 상태이다. 즉, 비밀번호는 자신을 제외하고 어느 누구에게도 알려져서는 안된다.

오답 체크 :

(1), (2), (3), (5) 은행계좌번호, 주민등록번호, 신용카드번호, 여권번호 : 공개된다고 하더라도 또 다른 증명이 없다면 어떤 일도 할 수 없다.

10. 소프트웨어 보안 약점의 유형과 그러한 약점을 이용한 공격의 예로 옳지 않은 것은?
① DB와 연동된 웹 어플리케이션에서 입력값에 대한 유효성 검증 누락 - SQL 삽입 공격
② 검증되지 않은 외부 입력이 웹서버의 동적 웹페이지 생성에 사용 - XSS 공격
③ 사용자 입력값을 외부사이트 주소로 사용하여 자동 연결 - 피싱(Phishing) 공격
④ XQuery를 사용하여 XML 데이터에 대한 동적 쿼리 생성 시 외부 입력에 대한 유효성 검증 누락 - 인증 우회 공격
⑤ 검증 되지 않은 외부 입력이 XPath 쿼리문 생성 시 문자열로 사용 - 리버스 엔지니어 링 공격
오답 체크 :
(5) XPath : 리버스 엔지니어링이 아니라 XQuery와 마찬가지로 인증우회 공격이다.
정답 체크 :
(1) SQL 삽입 : 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.
(2) XSS : 반사 XSS 공격에 해당한다. 웹 애플리케이션의 지정된 변수를 이용할 때 발생하는 취약점을 이용하는 것으로, 검색 결과, 에러 메시지 등 서버가 외부에서 입력받은 값을 받아 브라우저에게 응답할 때 전송하는 과정에서 입력되는 변수의 위험한 문자를 사용자에게 그대로 돌려주면서 발생한다.
(3) Phishing : 사용자로부터 입력되는 값을 외부사이트의 주소로 사용하여 자동으로 연결하는 서버 프로그램은 피싱 공격에 노출되는 취약점을 가질 수 있다. 일반적으로 클라이언트에서 전송된 URL 주소로 연결하기 때문에 안전하다고 생각할 수 있으나, 해당 폼의 요청을 변조함으로써 공격자는 사용자가 위험한 URL로 접속할 수 있도록 공격할 수 있다.
(4) XQuery : XML 문서를 조회할 경우 입력값 조작을 통해 XQuery나 XPath와 같은 쿼리문의 구조를 임의로 변경하여 허가되지 않은 데이터를 조회하거나 인증절차를 우회할 수 있다.

11. 디바이스 인증 수단으로 옳지 않은 것은?
① One Time Password
② MAC 주소값
③ 802.1x, WPA 표준 암호프로토콜
④ X.homesec-2
⑤ SSID
오답 체크 :
(1) One Time Password : OTP는 디바이스 인증 수단이 아니라 사용자 인증 수단이다.
정답 체크 :
(2) MAC : AP에 MAC을 등록해 놓고 등록된 MAC을 가진 디바이스만 인증을 수행해준다.
(3) 802.1x, WPA : 인증 서버(Radius 서버 등)를 통한 디바이스 인증을 수행한다.
(4) X.homesec-2 : 홈 네트워크를 위한 디바이스 인증 프로파일 표준이다. 참고로

X.homesec-1은 홈 네트워크를 위한 보안 기술의 프레임워크이고, X.homesec-3은 홈 네트워크 서비스를 위한 사용자 인증 메커니즘이다.
(5) SSID : 디바이스(스마트폰, 노트북 등)가 AP에 접속할 때 인증을 수행한다.

12. 해시함수의 설명으로 옳지 않은 것은?
① 양방향성을 가진다.
② 메시지가 다르면 매우 높은 확률로 해시값도 다르다.
③ 임의의 길이 메시지로부터 고정 길이의 해시값을 계산한다.
④ 해시값을 고속으로 계산할 수 있다.
⑤ MD5, RIPEMD-160, SHA-512 등이 있다.
오답 체크 :
(1) 양방향성 : 일방향성을 가진다. 즉, 해시값으로부터 메시지를 얻어낼 수 없다.
정답 체크 :
(2) 확률 : 충돌 내성 혹은 충돌 회피성(동일한 출력을 산출하는 서로 다른 두 입력을 계산적으로 찾기 어려운 성질)을 가진다.
(3) 임의 길이 : 입력이 1bit 혹은 1Tbit라도 고정된 길이의 출력을 가진다.
(4) 고속 : 해시 값을 고속으로 계산할 수 있다. 즉, 어떤 암호화 알고리즘도 현실적인 시간 내에 계산이 되지 않으면 의미가 없다.
(5) MD5, RIPEMD-160, SHA-512 : MD4, MD5, SHA-1, SHA-2(SHA-256, SHA-384, SHA-512), SHA-3, RIPEMD-160, HAS-160 등이 있다.

13. 공개키 암호인 RSA의 특징에 대한 설명으로 옳지 않은 것은?
① 매우 큰 소수를 사용하여 키를 만든다.
② 암·복호화 과정에 계산량이 많다.
③ 개인 인증서에도 사용한다.
④ 키를 교환해야 하는 불편함이 있다.
⑤ 디지털 서명에도 사용한다.
정답 체크 :
(4) 키를 교환 : 개인키는 가지고 있고, 공개키를 공개하면 키를 배송하지 않아도 된다.
오답 체크 :
(1) 매우 큰 소수 : N을 계산할 때, 매우 큰 소수 p와 q를 사용한다. 매우 큰 소수를 사용하기 때문에 소인수분해 문제를 가진다.
(2) 계산량 : 두 키의 수학적 특성에 기반하기 때문에, 메시지를 암호화 및 복호화 하는 과정에 여러 단계의 산술 연산이 들어간다. 그러므로 계산량이 많다.
(3) 개인 인증서 : 사용자(A)의 공개키에서 인증 기관의 개인키로 암호화하면 공인인증서가 된다. 이용자(B)는 공인인증서를 내려받아서 인증 기관의 공개키로 복호화하면 사용자(A)의 공개키를 사용할 수 있다.
(5) 디지털 서명 : 송신자의 개인키로 암호화를 암호화하고, 송신자의 공개키를 복호화를 수행하면 된다.

14. 시스템의 보안 취약점이 발견된 뒤 이를 막을 수 있는 패치가 발표되기 전에 그 취약점

을 이용한 악성코드나 해킹공격을 감행하는 수법은?
① APT 공격
② 스턱스넷 공격
③ DDoS 공격
④ 제로데이 공격
⑤ XSS 공격
정답 체크 :
(4) 제로데이 : 프로그램에 문제가 알려지고 난 후 보안패치가 나올 때까지 시간차를 이용해 공격하는 기법을 말한다.
오답 체크 :
(1) APT : 특정 기업 또는 기관의 핵심 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 공격자는 장기간 동안 공격 대상에 대해 IT인프라, 업무환경, 임직원 정보 등 다양한 정보를 수집하고, 이를 바탕으로 제로 데이 공격, 사회공학적 기법 등을 이용하여 공격 대상이 보유한 취약점을 수집·악용해 공격을 실행하는 것을 말한다.
(2) 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.
(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) XSS : 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

15. TLS 서브 프로토콜 중에서 데이터를 분할, 압축, 암호 등의 기능을 수행하는 프로토콜은?
① Handshake Protocol
② Change Cipher Spec Protocol
③ Alert Protocol
④ Record Protocol
⑤ Heartbeat Protocol
정답 체크 :
(4) Record : 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.
오답 체크 :
(1) Handshake : 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다.

인증서를 이용한 인증을 수행한다.
(2) Change Cipher Spec : 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.
(3) Alert : 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.
(5) Heartbeat : 리소스(컴퓨터)가 가용한지(살아있는지) 모니터할 때 사용하는 프토토콜이다. 여러개의 컴퓨터들을 모아놓은 클러스터링에서 각각의 컴퓨터가 살아있는지를 체크할 때 사용한다.

16. 다음 중 개인정보보호법에 대한 설명으로 옳지 않은 것은?
① 제3조 '개인정보 보호원칙'에 따르면, 개인정보는 목적 외의 용도로 활용해서는 안된다.
② 제4조 '정보주체의 권리'에 따르면, 정보주체는 자신의 개인정보의 처리에 관한 동의여부, 동의범위 등을 선택하고 결정할 수 있다.
③ 제15조 '개인정보의 수집·이용'에 따르면, 모든 개인정보의 수집은 정보주체의 동의를 받아야 한다.
④ 제21조 '개인정보의 파기'에 따르면, 개인정보의 보유기간이 경과하거나, 더 이상 불필요한 경우 지체 없이 그 개인정보를 파기해야 한다. 단, 다른 법령에 따라 보존해야 하는 경우도 있다.
⑤ 제34조 '개인정보 유출 통지 등'에 따르면, 개인정보 유출이 확인된 경우 지체없이 정보주체에게 유출된 항목과 시점, 경위 등을 통보해야 한다.
정답 체크 :
(3)
"개인정보 보호법" 제15조(개인정보의 수집·이용)에 따르면, 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 1. 정보주체의 동의를 받은 경우, 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우, 4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우, 5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, 6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

17. IPSec에 대한 설명으로 옳지 않은 것은?
① Tunnel Mode는 IP 헤더를 포함한 모든 Payload를 암호화 한다.
② Transport Mode에서 송·수신자의 IP 주소는 바뀌게 된다.
③ ESP 프로토콜은 인증을 사용하지 않을 수도 있다.
④ ESP 프로토콜의 경우 암호화 알고리즘으로 DES, 3DES, AES 등을 사용 할 수 있다.
⑤ AH 프로토콜의 경우 기밀성을 보장하지 못한다.
오답 체크 :
(2) Transport : 네트워크 계층 상위 계층인 전송, 응용 계층의 데이터에 대한 보호를 목적으로 하며, IP 패킷의 원본(payload)에 필드를 추가함으로서 구현하므로 IP 주소를 바꾸지 않는다.

정답 체크 :
(1) Tunnel : IP 헤더를 포함한 전체 IP 패킷에 대한 보호, 즉 네트워크, 전송, 응용 계층의 전체 데이터에 대한 보호를 목적으로 한다.
(3) ESP, 인증 : 기밀성, 무결성, 인증을 제공한다. ESP는 기밀성만 제공할 수도 있고, 인증만 제공할 수도 있다.
(4) ESP, 암호화 : DES, 3DES, 3IDEA, Blowfish, AES 등이 사용된다.
(5) AH : 무결성과 인증을 제공한다.

18. IT 시스템에 발생할 수 있는 다음의 보안 이슈들과 밀접한 관계를 가진 정보보호 요소는?

◦ IT 시스템의 저장된 데이터 변경 ◦ IT 시스템 메모리 변경 ◦ IT 시스템 간 메시지 전송 중 내용 변경

① 기밀성(Confidentiality)
② 무결성(Integrity)
③ 가용성(Availability)
④ 신뢰성(Reliability)
⑤ 책임추적성(Accountability)
정답 체크 :
(2) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
오답 체크 :
(1) 기밀성 : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.
(3) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.
(4) 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.
(5) 책임추적성 : 사용자 식별 및 활동 감사 추적을 의미하고, 책임성이라고도 한다.

19. 다음 중 이산 대수 문제의 어려움에 기초한 암호 알고리즘은?
① DES
② AES
③ Diffie-Hellman
④ RSA
⑤ SHA-2
정답 체크 :
(3) Diffie-Hellman : 이산 대수 문제의 어려움에 기초한다.
오답 체크 :
(1) DES : 페이스텔 구조에 기초한다.
(2) AES : SPN 구조에 기초한다.

(4) RSA : 소인수 분해 문제의 어려움에 기초한다.
(5) SHA-2 : 해쉬의 특성(일방향성, 충돌 내성 등)에 기초한다.

20. 다음 지문의 괄호 안에 들어갈 말로 옳은 것은?

( )은/는 HTTP 기반의 통신 서비스에서 보안 기능을 제공하기 위한 한 방안의 오픈 소스 라이브러리이다. C 언어로 작성되어 있는 중심 라이브러리 안에는, 기본적인 암호화 기능 및 여러 유틸리티 함수들이 구현되어 있다.

① IPSec
② OpenSSL
③ Kerberos
④ MySQL
⑤ PGP
정답 체크 :
(2) OpenSSL : 네트워크를 통한 데이터 통신에 쓰이는 프로토콜인 TLS와 SSL의 오픈 소스 구현판이다. C 언어로 작성되어 있는 중심 라이브러리 안에는, 기본적인 암호화 기능 및 여러 유틸리티 함수들이 구현되어 있다.
오답 체크 :
(1) IPSec : 네트워크 계층(network layer)으로 ip 계층을 보호하기 위한 프로토콜이다.
(3) Kerberos : MIT에서 개발한 비밀키(대칭키) 암호 기반 키 분배 및 사용자 인증 시스템이다. 클라이언, AS(TGT 발행), TGS(Ticket 발행), 서버로 구성되고, 중앙 집중형 인증 방식이다.
(4) MySQL : 관계형 데이터베이스 관리 시스템(RDBMS)이다. 오픈소스로 개발되며, GNU GPL(GNU General Public License)과 상업용 라이센스의 이중 라이센스로 관리되고 있다. MySQL은 데이터를 저장 및 액세스하는 스토리지 엔진(storage engine)과 SQL 파서(SQL parser)를 따로 분리하여 용도에 따라 스토리지 엔진을 선택할 수 있는 멀티 스토리지 엔진 방식을 채용하고 있다.
(5) PGP : 전자우편의 안전성을 위해 1991년 미국의 Phil Zimmermann에 의해 개발된 전자우편 보안 시스템이다.