2016-지방직-정보보호론-A형-해설

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

1. 보안 공격 유형 중 소극적 공격으로 옳은 것은?
① 트래픽 분석(traffic analysis)
② 재전송(replaying)
③ 변조(modification)
④ 신분 위장(masquerading)
정답 체크 :
(1) 트래픽 분석 : 기밀성을 해치는 소극적 공격이다.
오답 체크 :
(2) 재전송 : 무결성을 해치는 적극적 공격이다.
(3) 변조 : 무결성을 해치는 적극적 공격이다.
(4) 신분 위장 : 무결성을 해치는 적극적 공격이다.
Tip! : 다음은 공격 방법, 적극적/소극적, 기밀성/무결성/가용성 관점에서 정리한 표이다.

Attacks	*Passive/Active*	*Threatening*
Snooping (Sniffing) Traffic analysis	Passive	Confidentiality
Modification Masquerading (Spoofing) Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

2. 암호학적 해시 함수가 가져야 할 특성으로 옳지 않은 것은?
① 서로 다른 두 입력 메시지에 대해 같은 해시값이 나올 가능성은 있으나, 계산적으로 같은 해시값을 갖는 서로 다른 두 입력 메시지를 찾는 것은 불가능해야 한다.
② 해시값을 이용하여 원래의 입력 메시지를 찾는 것은 계산상으로 불가능해야 한다.
③ 입력 메시지의 길이에 따라 출력되는 해시값의 길이는 비례해야 한다.
④ 입력 메시지와 그 해시값이 주어졌을 때, 이와 동일한 해시값을 갖는 다른 메시지를 찾는 것은 계산상으로 불가능해야 한다.
정답 체크 :
(3) 해시값 길이 : 입력이 1bit 혹은 1Tbit라도 고정된 길이의 출력을 가진다.
오답 체크 :
(1) 서로 다른 두 입력 메시지 : 해시가 가져야 하는 강한 충돌 내성을 나타낸다.
(2) 원래의 입력 메시지 : 해시가 가져야 하는 일방향성을 나타낸다.
(4) 다른 메시지 : 해시가 가져야 하는 약한 충돌 내성을 나타낸다.

3. 다음 내용에 해당하는 공개키 기반 구조(PKI)의 구성요소로 옳은 것은?

○ 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다. ○ 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다. ○ 인증서 폐기 목록(certificate revocation list)을 작성한다.

① 사용자
② 등록 기관
③ 인증 기관
④ 디렉토리

정답 체크 :

(3) 인증 기관 : 인증서의 관리를 행하는 기관으로, 키 쌍을 작성한다(이용자가 작성하는 경우도 있다). 그리고 공개 키 등록 때 본인을 인증하고, 인증서를 작성해서 발행하거나 인증서를 폐지한다.

오답 체크 :

(1) 사용자 : PKI를 사용해서 자신의 공개 키를 등록하고 싶어 하는 사람과 등록되어 있는 공개 키를 사용하고 싶어 하는 사람을 의미한다.

(2) 등록 기관 : 인증기관의 일 중 「공개 키의 등록과 본인에 대한 인증」을 대행하는 기관이다.

(4) 디렉토리 : 인증서를 보존한다. PKI 이용자가 인증서를 입수할 수 있도록 한 데이터베이스이다. 인증서 저장소(repository)라고도 한다.

4. ㉠ 과 ㉡ 에 들어갈 용어로 옳은 것은?

(㉠)은(는) 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다. (㉡)은(는) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털 콘텐츠에 삽입하는 기술이다.

	㉠	㉡
①	크래커(Cracker)	커버로스(Kerberos)
②	크래커(Cracker)	워터마킹(Watermarking)
③	핑거프린팅(Fingerprinting)	커버로스(Kerberos)
④	핑거프린팅(Fingerprinting)	워터마킹(Watermarking)

정답 체크 :

(4)

(ㄱ) 핑거프린팅 : 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다. 판매되는 콘텐츠마다 구매자의 정보가 들어있으므로 불법적으로 재배포된 콘텐츠 내에서 핑거프린팅된 정보를 추출하여 구매자를 식별하고, 법적인 조치를 가할 수 있게 된다.

(ㄴ) 워터마킹 : 동영상이나 음성 데이터에 사용자가 알 수 없는 형태로 저작권 정보를 기록하는 장치이다. 디지털 워터마킹에는 작성자, 저작권자, 작성일 등이 인간의 눈이나 귀로는 알지 못하도록 숨겨져 있으며, 만약 불법 복제를 위해 디지털 워터마킹 정보를 삭제하려 하면 원래의 동영상이나 음성 정보가 삭제되도록 설계되어 있다.

오답 체크 :

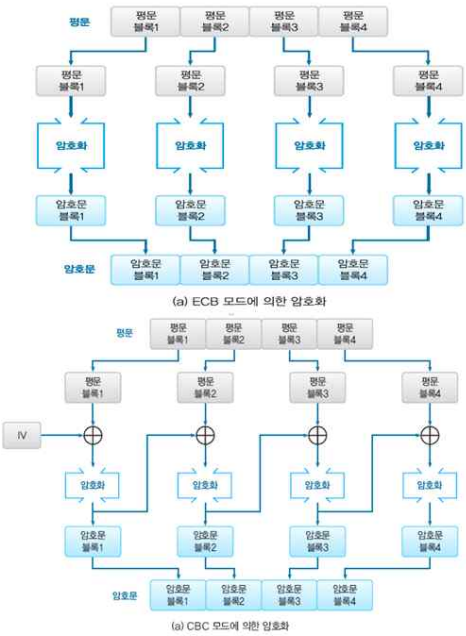
(1), (2), (3)
크래커 : 고의 또는 악의적으로 다른 사람의 컴퓨터에 불법적으로 침입하여 데이터나 프로그램을 엿보거나 변경하는 등의 컴퓨터 범죄 행위를 저지르는 사람을 가리킨다. 소프트웨어를 불법으로 복사하여 배포하는 사람을 가리키기도 한다.
커버로스 : MIT에서 개발한 비밀키(대칭키) 암호 기반 키 분배 및 사용자 인증 시스템이다. 클라이언, AS(TGT 발행), TGS(Ticket 발행), 서버로 구성되고, 중앙 집중형 인증 방식이다.

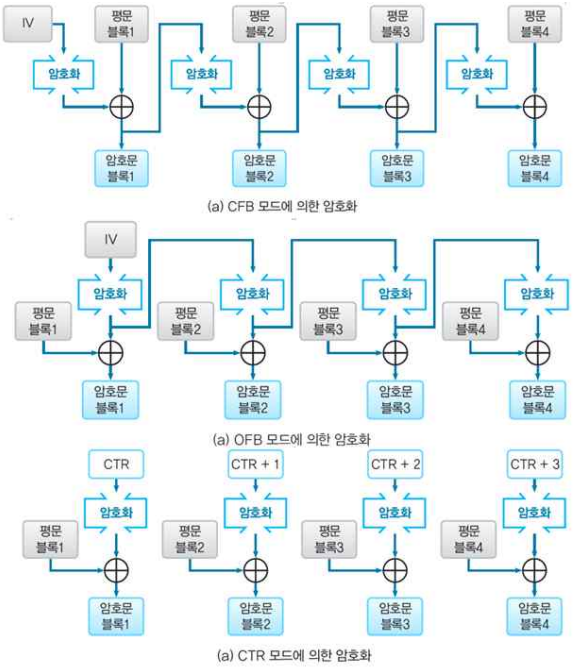
5. 다음 내용에 해당하는 암호블록 운용 모드를 바르게 나열한 것은?

ㄱ. 코드북(codebook)이라 하며, 가장 간단하게 평문을 동일한 크기의 평문블록으로 나누고 키로 암호화하여 암호블록을 생성한다. ㄴ. 현재의 평문블록과 바로 직전의 암호블록을 XOR한 후 그 결과를 키로 암호화하여 암호블록을 생성한다. ㄷ. 각 평문블록별로 증가하는 서로 다른 카운터 값을 키로 암호화하고 평문블록과 XOR하여 암호블록을 생성한다.

	ㄱ	ㄴ	ㄷ
①	CBC	ECB	OFB
②	CBC	ECB	CTR
③	ECB	CBC	OFB
④	ECB	CBC	CTR

정답 체크 :
(4)
(ㄱ) ECB : 개별적으로 평문 블록을 암호화해서 암호문 블록으로 만든다.
(ㄴ) CBC : 이전 단계의 암호문 블록과 현재 단계의 평문 블록을 XOR해서 암호문 블록을 만든다.
(ㄷ) CTR : 개별적으로 카운터를 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다.
오답 체크 :
(1), (3)
OFB : 이전 단계의 출력 블록(평문 블록과 XOR해서 암호문 블록을 만들기 전 단계)을 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다.
(2) 순서가 틀리다.
Tip! : CFB는 이전 단계의 암호문 블록을 암호화한 후 현재 단계의 평문 블록과 XOR해서 암호문 블록을 만든다. 이들을 그림으로 나타내면 다음과 같다.





6. 네트워크 공격에 대한 설명으로 옳지 않은 것은?

① Spoofing : 네트워크에서 송·수신되는 트래픽을 도청하는 공격이다.

② Session hijacking : 현재 연결 중인 세션을 가로채는 공격이다.

③ Teardrop : 네트워크 프로토콜 스택의 취약점을 이용한 공격 방법으로 시스템에서 패킷을 재조립 할 때, 비정상 패킷이 정상 패킷의 재조립을 방해함으로써 네트워크를 마비시키는 공격이다.

④ Denial of Service : 시스템 및 네트워크의 취약점을 이용하여 사용 가능한 자원을 소비함으로써, 실제 해당 서비스를 사용하려고 요청하는 사용자들이 자원을 사용할 수 없도록 하는 공격이다.

정답 체크 :

(2) 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.

오답 체크 :

(1) Spoofing : 해당 설명은 Sniffing(Snooping)이고, Spoofing은 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근 제어를 우회하는 공격 행위이다. 일례로, IP Spoofing 공격은 서버와 트러스트(Trust)로 관계를 맺고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다. IP Spoofing 이외에도 ARP, Port, Content(Payload), DNS Spoofing 등이 존재한다.

(3) 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.
(4) Denial of Service : DoS(서버를 서비스 거부 상태로 만듦)의 공격 유형에는 취약점 공격형과 자원 고갈형이 존재한다. 취약점 공격형은 teardrop, land attack이 해당되고, 자원 고갈형은 flooding 공격이 해당된다.

7. 스택 버퍼 오버플로우 공격의 수행 절차를 순서대로 바르게 나열한 것은?

ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격 쉘 코드의 주소가 반환된다. ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우 시켜서 공격 쉘 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다. ㄷ. 공격 쉘 코드를 버퍼에 저장한다. ㄹ. 공격 쉘 코드가 실행되어 루트 권한을 획득하게 된다.

① ㄱ → ㄴ → ㄷ → ㄹ
② ㄱ → ㄷ → ㄴ → ㄹ
③ ㄷ → ㄴ → ㄱ → ㄹ
④ ㄷ → ㄱ → ㄴ → ㄹ
정답 체크 :
(3)
(ㄷ) 공격 쉘 코드 : eggshell이라고 부른다.
(ㄴ) 특정 함수 : strcpy와 같은 입력 문자열의 길이를 검사하지 않는 함수를 공격한다. 함수의 복귀 주소가 eggshell의 주소로 바뀐다.
(ㄱ) 복귀 주소 : 함수의 호출이 완료되면 eggshell의 주소가 반환된다.
(ㄹ) 루트 권한 : eggshell이 SetUID 비트가 설정되어 있다면 루트 권한을 얻을 수 있다.

8. 접근통제(access control) 모델에 대한 설명으로 옳지 않은 것은?
① 임의적 접근통제는 정보 소유자가 정보의 보안 레벨을 결정하고 이에 대한 정보의 접근제어를 설정하는 모델이다.
② 강제적 접근통제는 중앙에서 정보를 수집하고 분류하여, 각각의 보안 레벨을 붙이고 이에 대해 정책적으로 접근제어를 설정하는 모델이다.
③ 역할 기반 접근통제는 사용자가 아닌 역할이나 임무에 권한을 부여하기 때문에 사용자가 자주 변경되는 환경에서 유용한 모델이다.
④ Bell-LaPadula 접근통제는 비밀노출 방지보다는 데이터의 무결성 유지에 중점을 두고 있는 모델이다.
정답 체크 :
(4) Bell-LaPadula : 무결성은 Biba 또는 Clark-Wilson이고, Bell-LaPadula 모델은 미 국방부 지원 보안 모델로 보안 요소 중 기밀성(비밀성) 강조한다.
오답 체크 :
(1) DAC : 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
(2) MAC : 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야

에 적합하다.
(3) RBAC : 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.

9. 개인정보 보호법령 상 개인정보 영향 평가에 대한 설명으로 옳지 않은 것은?
① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인 정보 파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려 되는 경우에는 위험 요인분석과 개선 사항 도출을 위한 평가를 하고, 그 결과를 행정자치부 장관에게 제출하여야 한다.
② 개인정보 영향 평가의 대상에 해당하는 개인정보 파일은 공공 기관이 구축·운용 또는 변경하려는 개인정보 파일로서 50만 명 이상의 정보주체에 관한 개인정보 파일을 말한다.
③ 영향 평가를 하는 경우에는 처리하는 개인정보의 수, 개인 정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도, 그 밖에 대통령령으로 정한 사항을 고려하여야 한다.
④ 행정자치부 장관은 제출 받은 영향 평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.
정답 체크 :
(2) “개인정보 보호법 시행령” 제35조(개인정보 영향평가의 대상) 상 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. 1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일, 2. 구축ㆍ운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일, 3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
오답 체크 :
(1) “개인정보 보호법” 제33조(개인정보 영향평가) 상 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 하고 그 결과를 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관 중에서 의뢰하여야 한다.
(3) “개인정보 보호법” 제33조(개인정보 영향평가) 상 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다. 1. 처리하는 개인정보의 수, 2. 개인정보의 제3자 제공 여부, 3. 정보주체의 권리를 해할 가능성 및 그 위험 정도, 4. 그 밖에 대통령령으로 정한 사항
(4) “개인정보 보호법” 제33조(개인정보 영향평가) 상 행정안전부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.
Tip! : 장관의 이름이 행정자치부장관에서 행정안전부장관이 바뀐 것을 알 수 있다. 관련 법규는 수정 내용을 매년 체크를 해야 하지만, 그 중에서 장관의 이름은 주의 깊게 살펴보아야 한다.

10. 정보보호 시스템에서 사용된 보안 알고리즘 구현 과정에서 곱셈에 대한 역원이 사용된다. 잉여류 Z_{26}에서 법(modular) 26에 대한 7의 곱셈의 역원으로 옳은 것은?

① 11
② 13
③ 15
④ 17
정답 체크 :
(3)
Zm은 0보단 크고 m보단 작은 수의 집합을 나타낸다. 그리고 Zm*는 0보단 크고 m보단 작은 수 중에서 m과 최대공약수가 1인 수의 집합을 의미한다. a에 대한 덧셈의 역원은 (a+b) mod m = 0를 만족하는 b를 의미하고, a에 대한 곱셈의 역원은 (axb) mod m = 1를 만족하는 b를 의미한다. 주어진 조건으로 문제를 풀면 (7xb) mod 26 = 1를 만족하는 b를 찾으면 된다. 주어진 보기에서 15를 대입하면 (7x15) mod 26 = 1 -> 105 mod 26 = 1이 되어 조건을 만족하게 된다.

11. 응용 계층 프로토콜에서 동작하는 서비스에 대한 설명으로 옳지 않은 것은?
① FTP : 파일전송 서비스를 제공한다.
② DNS : 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.
③ POP3 : 메일 서버로 전송된 메일을 확인하는 서비스를 제공한다.
④ SNMP : 메일전송 서비스를 제공한다.
정답 체크 :
(4) SNMP : 해당 설명은 SMTP이고, SNMP는 네트워크 관리와 모니터링을 위해 사용된다.
오답 체크 :
(1) FTP : 파일을 전송하기 위한 프로토콜이다.
(2) DNS : 도메인 혹은 호스트 이름을 IP 주소로 변환해 준다. Inverse DNS는 IP 주소를 도메인 혹은 호스트 이름으로 변환한다.
(3) POP3 : 클라이언트가 메일 서버로부터 메일을 받을 때 사용하는데, 메일 서버에 메일 사본을 저장하지 않는다.

12. 개인정보 보호법 상 용어 정의로 옳지 않은 것은?
① 개인정보 : 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)
② 정보주체 : 업무를 목적으로 개인정보 파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공 기관, 법인, 단체 및 개인
③ 처리 : 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위
④ 개인정보 파일 : 개인정보를 쉽게 검색 할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물
정답 체크 :
(2) “개인정보 보호법” 제2조(정의) 상 해당 설명은 “개인정보처리자”를 의미하고, “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

13. 다음 설명에 해당하는 OECD 개인정보보호 8 원칙으로 옳은 것은?

개인정보는 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

① 이용 제한의 원칙(Use Limitation Principle)
② 정보 정확성의 원칙(Data Quality Principle)
③ 안전성 확보의 원칙(Security Safeguards Principle)
④ 목적 명시의 원칙(Purpose Specification Principle)

정답 체크 :
(2) 정보 정확성의 원칙 : 개인정보는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지하여야 한다.

오답 체크 :
(1) 이용 제한의 원칙 : 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안된다.
(3) 안전성 확보의 원칙 : 개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호장치를 마련해야 한다.
(4) 목적 명시의 원칙 : 개인정보를 수집할때는 목적이 명확해야 하고, 이를 이용할 경우에도 애초의 목적과 모순되지 않아야 한다.

14. 현행 우리나라의 정보보호 관리체계(ISMS) 인증에 대한 설명으로 옳지 않은 것은?
① 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에 근거를 두고 있다.
② 인증 심사의 종류에는 최초 심사, 사후 심사, 갱신 심사가 있다.
③ 인증에 유효 기간은 정해져 있지 않다.
④ 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

정답 체크 :
(3) 유효기간 : 유효기관은 3년(=사후+사후+갱신)이다.

오답 체크 :
(1) 법률 : “정보통신망법” 제45조(정보보호 관리체계의 인증)에 근거를 두고 있다.
(2) 인증심사 : 최초심사 -> 사후심사(1년) -> 사후심사(1년) -> 갱신심사(1년)
(4) 정보통신망 : “정보통신망법” 제45조 제1항 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 제4항(과학기술정보통신부장관이 필요한 사항을 정함)에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

15. 보안 서비스에 대한 설명을 바르게 나열한 것은?

ㄱ. 메시지가 중간에서 복제·추가·수정되거나 순서가 바뀌거나 재전송 됨이 없이 그대로 전송되는 것을 보장한다. ㄴ. 비인가된 접근으로부터 데이터를 보호하고 인가된 해당 개체에 적합한 접근 권한을 부

여한다.
ㄷ. 송·수신자 간에 전송된 메시지에 대해서, 송신자는 메시지 송신 사실을, 수신자는 메시지 수신 사실을 부인하지 못하도록 한다.

	ㄱ	ㄴ	ㄷ
①	데이터 무결성	부인 봉쇄	인증
②	데이터 가용성	접근통제	인증
③	데이터 기밀성	인증	부인 봉쇄
④	데이터 무결성	접근통제	부인 봉쇄

정답 체크 :
(4)
(ㄱ) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(ㄴ) 접근통제 : 인가된 사람만이 데이터에 접근하도록 하고, 접근이 정상적으로 허락되지 않은 사용자가 접근하는 것을 막는다.
(ㄷ) 부인봉쇄 : 송신부인방지(어떤 메시지가 송신되었을 때 수신자는 그 메시지가 실제로 송신자라고 주장하는 주체에 의해 송신되었음을 확인한다). 수신부인방지(어떤 메시지가 수신되었을 때 송신자는 그 메시지가 실제로 수신자라고 주장하는 주체에 의해 수신되었음을 확인한다).
오답 체크 :
(1), (2), (3)
인증 : 상대방의 신원을 확인시켜 준다. 사용자 인증(시스템 접근 통제)과 데이터 출처 인증(MAC)이 있다.
기밀성 : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.

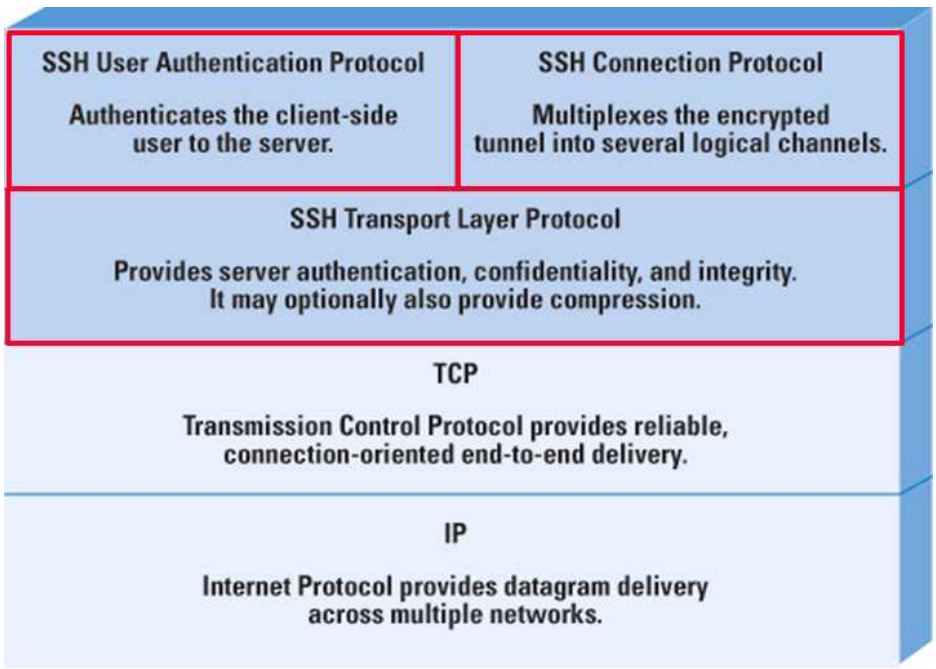
16. 다음에 해당하는 방화벽의 구축 형태로 옳은 것은?

○ 인터넷에서 내부 네트워크로 전송되는 패킷을 패킷 필터링 라우터에서 필터링 함으로써 1차 방어를 수행한다.
○ 배스천 호스트에서는 필터링된 패킷을 프록시와 같은 서비스를 통해 2차 방어 후 내부 네트워크로 전달한다.

① 응용 레벨 게이트웨이(Application-level gateway)
② 회로 레벨 게이트웨이(Circuit-level gateway)
③ 듀얼 홈드 게이트웨이(Dual-homed gateway)
④ 스크린 호스트 게이트웨이(Screened host gateway)
정답 체크 :
(4) 스크린 호스트 게이트웨이 : 베스천 호스트(Screened Host)와 스크린 라우터(Screening Router, 패킷 필터링 라우터)를 혼합하여 사용한 방화벽이다. 외부 네트워크와 내부 네트워크 사이에 스크린 라우터를 설치하고, 스크린 라우터와 내부 네트워크 사이에 베스천 호스트를 설치한다.
오답 체크 :
(1) 응용 레벨 게이트웨이 : 응용 계층(layer 7)에서 동작하고, 패킷 필터링 방식(layer 4)과는

달리 외부와 내부 네트워크 간의 직접적인 패킷 교환을 허용하지 않는다.
(2) 회로 레벨 게이트웨이 : OSI 참조 모델의 응용 계층(Layer 7)에서 세션 계층(Layer 5) 사이에서 동작하며, 각 서비스별로(specific) 프락시가 존재하는 응용 수준 게이트웨이(application level gateway) 방식과 달리, 어느 응용 프로그램에서도 사용할 수 있는 일반적인(general) 프락시를 사용한다.
(3) 듀얼 홈드 게이트웨이 : 두 개의 NIC를 가진 베스천 호스트(Bastion Host)를 말하며, 하나의 NIC는 외부 네트워크에 연결되고 다른 하나의 NIC는 보호하고자 하는 내부 네트워크에 연결된다. 네트워크 간의 직접적인 접근은 허용되지 않는다. 라우팅 기능이 활성화되어 있을 때, 문제가 되는 방화벽 유형이다. (비정상 패킷도 포워딩 가능성 존재)

17. SSH(Secure SHell)를 구성하고 있는 프로토콜 스택으로 옳지 않은 것은?
① SSH User Authentication Protocol
② SSH Session Layer Protocol
③ SSH Connection Protocol
④ SSH Transport Layer Protocol
정답 체크 :
(2)
SSH의 프로토콜 스택은 다음과 같다. 그림에서 보는바와 같이 SSH Session Layer Protocol은 존재하지 않는다. SSH User Authentication Protocol은 사용자 인증을 위해 사용되고, SSH Connection Protocol은 로그인 세션, 명령어 원격 실행, 연결 포워딩을 수행한다. 그리고 SSH Transport Layer Protocol은 인증, 기밀성, 무결성, 압축 등을 제공한다.



18. 위험 분석 방법에 대한 설명을 바르게 나열한 것은?

ㄱ. 시스템에 관한 전문적인 지식을 가진 전문가 집단을 구성하고 토론을 통해 정보시스템이 직면한 다양한 위협과 취약성을 분석하는 방법이다.

ㄴ. 자산의 가치 분석, 위협 분석, 취약점 분석을 수행하여 위험을 분석하는 방법이다. ㄷ. 표준화된 보호대책의 세트를 체크리스트 형태로 구현하여 이를 기반으로 보호대책을 식별하는 방법이다.

	ㄱ	ㄴ	ㄷ
①	시나리오법	기준선 접근법	상세위험분석 접근법
②	시나리오법	상세위험분석 접근법	기준선 접근법
③	델파이법	기준선 접근법	상세위험분석 접근법
④	델파이법	상세위험분석 접근법	기준선 접근법

정답 체크 :

(4)

(ㄱ) 델파이법 : 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고, 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.

(ㄴ) 상세위험 접근법 : 모든 정보자산에 대해 상세 위험 분석을 하는 방법이다. 자산가치, 위협, 취약점의 평가에 기초한 위험을 산정하므로 근거가 명확하지만, 상당힌 시간과 노력이 소요된다.

(ㄷ) 기준선 접근법 : 모든 시스템에 대하여 표준화딘 정보보호대책 세트를 제공(체크리스트 형태)한다. 비용 및 시간을 절약할 수 있지만 과보호 또는 부족한 보호가 될 가능성이 상존한다.

오답 체크 :

(1), (2)

시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여, 일정 조건 하에서 위협에 대한 발생 가능한 결과들을 추정(시나리오)하는 방법이다.

(3) 순서가 틀리다.

Tip! : 위험분석방법은 결과 성격에 따라 정량적, 정성적 방법이 존재하고, 요구사항(수준)에 따라 기준선 접근법, 상세 위험 접근법 등이 존재한다.

19. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상 개인정보 취급 방침에 포함되어야 할 사항이 아닌 것은?

① 이용자 및 법정대리인의 권리와 그 행사 방법

② 개인정보에 대한 내부관리계획

③ 인터넷 접속 정보 파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항

④ 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집 방법

정답 체크 :

(2) “정보통신망법” 제28조(개인정보의 보호조치) 상 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행은 맞지만 개인정보 취급방침에 포함되어야 할 사항은 아니다.

오답 체크 :

(1), (3), (4)

“정보통신망법” 제27조의2(개인정보 취급방치의 공개) 상 개인정보 처리방침에는 다음 각 호의 사항이 모두 포함되어야 한다. 1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법, 2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는

법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목, 3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조제1항 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다), 4. 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 처리방침에 포함한다), 5. 이용자 및 법정대리인의 권리와 그 행사방법, 6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항, 7. 개인정보 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

20. 전자서명 방식에 대한 설명으로 옳지 않은 것은?
① 은닉 서명(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자 만이 서명을 확인할 수 있는 방식이다.
② 부인방지 서명(undeniable signature)은 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
③ 위임 서명(pro x y signature)은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.
④ 다중 서명(multisignature)은 동일한 전자문서에 여러 사람이 서명하는 방식이다.
정답 체크 :
(1) 은닉 : 해당 설명은 은닉 서명이 아니고 설명 또한 틀리다. 특정 검증자를 지정하는 것은 불가능하다. 왜냐하면 검증은 공개키로 하는데 공개키를 누구에게나 공개되어 있기 때문이다. 은닉 서명이란 보낸 메시지가 검증할 수 있는 메시지라는 것을 보장하면서도 보낸 사람의 익명성을 보장해준다.
오답 체크 :
(2) 부인방지 : 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
(3) 위임 : 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.
(4) 다중 : 동일한 전자문서에 여러 사람이 서명하는 방식이다.