정보보호론	국가 전산 7급	2018년 8월 18일

♤ 합격선/최종합격인원(74.16점/31명) - 채용예정인원 29명 / 필기합격 42명 ♤

1. 공개키 인증서의 구조를 정의한 ITU-T 권고안은? [2018년 국가 7급]

① X.25 ② X.121 ③ X.400 ④ X.509

♤ X.509 인증서

① X.509는 국제 표준 **공개키 인증서** 형식이다.
- X.509는 공개키 기반구조에서 가장 널리 사용되는 표준 규격 인증서이다.
- X.509는 매우 엄격한 수직적 구조이다.(상호 신뢰 기반 웹 모델이 아니다)

② X.509는 ITU-T(국제전기통신연합)에서 개발, ASN.1 구조를 채택하였다.

③ X.509 시스템에서 인증기관은 서로 구별되는 공개키를 가진 인증서를 발행한다.
- X.509 표준은 어떤 특정한 공개키 암호 알고리즘을 지정하지 않고 있다.
- X.509는 CRL(certificate revocation list) 구현을 위한 표준도 포함한다.

// X.509 v3의 디지털 인증서 구조

Certificate	
Version Number	인증서 버전
Serial Number	인증기관(CA)이 할당한 일련번호(인증서 고유번호)
Signature Algorithm ID	서명 알고리즘 식별자(인증서 서명에 사용)
Issuer Name	인증서를 발급하고 서명한 인증기관(CA) 이름
Validity period	인증서 유효기간
Not Before	인증서가 유효한 시작 날짜
Not After	인증서가 유효한 만료 날짜
Subject name	인증서 소유자 이름(공개키 소유 주체)
Subject Public Key Info	소유자의 공개키 정보
Public Key Algorithm	공개키 알고리즘
Subject Public Key	주체의 공개키 값
Issuer Unique Identifier(optional)	발급자의 유일 식별자(선택 항목)
Subject Unique Identifier(optional)	주체의 유일 식별자(선택 항목)
Extensions(optional)	확장 - 인증서 관련 추가 정보(선택 항목)
Certificate Signature Algorithm	인증서 서명 알고리즘
Certificate Signature	

정답 : ④

2. ㉠, ㉡에 들어갈 정보보안 위험의 처리 방식을 바르게 연결한 것은? [2018년 국가 7급]

(㉠)은(는) 사업 목적상 위험을 처리하는 데 들어가는 과도한 비용 또는 시간 때문에 일정 수준의 위험을 받아 들이는 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

♤ **위험 처리 방식**

// 위험(risk) – 금액으로 표현 가능
- 위험은 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성이다.
- 위험의 유형과 규모를 확인하기 위해서는 위험분석이 필요하다.

// 위험 수용
- 위험에 대한 조치를 취하지 않고, 현 상태의 위험을 허용하기로 결정하는 것이다.
- 위험 처리 비용이 과도하면, 일정 수준의 위험은 그냥 받아들이는 것이다.
- 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.

// 위험 전가
- 잠재적 위험 비용을 제3자에게 이전하거나 할당하는 것이다.
- 위험에 대한 보험을 들거나 다른 기관과의 계약을 통하여 잠재적 손실을 제3자에게 이전하거나 할당하는 방식이다.

// 위험 감소
- 위험을 감소시킬 수 있는 효과적인 대책을 채택하여 구현하는 것이다.

// 위험 회피
- 위험이 존재하는 프로세스나 사업을 포기하는 것이다.

정답 : ③

3. 다음에서 설명하는 컴퓨터 시스템의 평가기준은? [2018년 국가 7급]

○ 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

♤ **TCSEC 보안등급**

TCSEC 보안등급은 **미국**이 제정 발표한 정보보호제품 평가기준이다.

등급	등급별 보안 요구사항	비고
A1	• **검증된 설계**(verified design) - 가장 높은 등급 • 정형화된 검증 방법 사용(정형화된 보안 정책을 일정하게 유지) • 극비정보 취급, 형식상 엄격한 인증, 제한 및 감사 • 현재, A1 등급을 받은 시스템은 없다.(이상적인 시스템)	**강제적 및 임의적 접근제어**
B3	• **보안 영역**(security domain) • 매우 중요한 정보를 취급하는 고도의 안전한 환경 • 은닉채널(covert channel) 보호 timing, storage 모두	
B2	• **구조적 보호**(structured protection) • 은닉채널(covert channel) storage만 보호 • 트랩도어가 없음을 보증 • 참조 모니터는 B2이상	
B1	• **레이블된 보안 보호**(labeled security protection) • 분류된 데이터 처리 • 시스템 설계에 대한 명세와 검증	
C2	• **통제된 접근 보호**(controlled access protection) • 상업적 환경에 합리적인 분류나 보호의 수준은 낮음 • 리소스의 분리, 객체의 재사용, 감사추적의 보호와 책임추적 제공 • 각 사용자의 작업 내용을 기록, 감사할 수 있는 기능 제공	**임의적 접근제어**
C1	• **임의적 보안 보호**(discretionary security protection) • 개인 및 그룹의 정보 보호 • 식별과 인증, 자원의 임의적 보호 • 사용자는 자신이 생성한 파일에 대해 접근권한 설정이 가능하다.	
D	• **최소한의 보호**(minimal protection) - 가장 낮은 등급 • 평가는 수행되었지만 평가등급의 요구사항을 만족하지 못한 시스템	

정답 : ①

4. 유닉스 시스템 명령어에 대한 설명으로 옳지 않은 것은? [2018년 국가 7급]

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

♤ **유닉스 시스템 명령어 – mesg**

- mesg : 메시지 허용 또는 거부
- 현재 사용자 터미널에 대한 쓰기 접근을 제어한다.
- 메시지 거부를 설정하면, 네트워크의 다른 사용자가 현재 터미널로 write하지 못한다.

예	• 사용자가 텍스트 파일을 편집하고 있을 때, • 여러 메시지가 화면에 빈번하게 뜨면 작업에 방해가 될 수 있다. • 짜증날 수도 있다. • 이런 방해를 받기 싫을 때, • mesg 명령어를 이용하여 자신의 터미널에 대한 쓰기 접근을 막을 수 있다.

정답 : ②

5. 커버로스(Kerberos) 버전 4 인증 시스템에서 클라이언트가 응용서버에게 제시하는 티켓에 포함되는 구성요소가 아닌 것은? [2018년 국가 7급]

① 클라이언트 ID
② 클라이언트와 응용서버 간의 세션키
③ 인증서버의 네트워크 주소
④ 티켓의 유효시간

♤ **커버로스**

- 클라이언트가 **응용서버(실질서버)** 접속을 위해 제시하는 티켓은 SGT이다.

SGT에 포함된 정보	• 클라이언트 ID (사용자 ID) • 클라이언트 IP 주소 (사용자 IP 주소) • 티켓의 유효기간 • 클라이언트와 응용서버 간의 세션키[**세션키**($K_{사용자.응용서버}$)]

- **SGT** : Session Granting Ticket

정답 : ③

6. 정보통신기반 보호법 상 주요정보통신기반시설을 관리하는 기관의 장이 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있는 기관에 해당하지 않는 것은? [2018년 국가 7급]

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

♤ **정보통신기반 보호법 – 제9조(취약점의 분석·평가)**

① 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.
② 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.
③ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 **소관 주요정보통신기반시설의 취약점을 분석·평가**하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다.
〈개정 2002. 12. 18., 2007. 12. 21., 2009. 5. 22., 2013. 3. 23., 2015. 6. 22.〉
1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 **한국인터넷진흥원**(이하 "인터넷진흥원"이라 한다)
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**

④ 과학기술정보통신부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항의 규정에 의한 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다. 〈개정 2008. 2. 29., 2013. 3. 23., 2017. 7. 26.〉
⑤ 주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

정답 : ④

7. SHA-512 알고리즘의 처리 방식에 대한 설명으로 옳지 않은 것은? [2018년 국가 7급]

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 암호키를 사용한다.

♤ SHA-512 알고리즘

- 블록 단위로 메시지를 처리하는 과정은 80라운드로 이루어지며, 규칙성을 제거하기 위해 각 라운드마다 서로 다른 **암호키**를 사용한다.**(×)**
  → 먼저, SHA-512는 **키를 사용하지 않는 전용 해시함수**이다.
  → 그리고, 각 라운드에는 내부적으로 정해진 서로 다른 상수 80개가 이용된다.
  → 각 상수는 초기 80개 소수(2, 3, 5, .., 409)를 세제곱근한 값에서 일부를 추출한 값이다.

- SHA-512는 최대 크기가 2^{128}비트 미만인 메시지를 입력받아 512비트 해시값을 출력한다.
- SHA-512는 메시지 길이가 2^{128}비트와 같거나 더 길면 해당 메시지를 처리할 수 없다.
  → 그런데, 대부분의 컴퓨터 용량이 2^{128}비트보다 작으므로 이 제한은 문제가 되지 않는다.

- SHA-512는 마지막에 원래의 메시지 길이 값을 덧붙인다.(128비트의 부호없는 정수형)
- SHA-512는 메시지 길이가 1024비트 배수가 되도록 패딩을 한다.(메시지 길이 값 포함)
- SHA-512는 입력 데이터 길이를 1024비트인 블록으로 나누어서 처리한다.
- 패딩으로 추가되는 비트는 첫 번째 비트는 1이고 나머지 비트는 0이다.

- 필요한 초기값(512비트) 상수는 내부적으로 정해지는 8개의 상수를 이용한다.
- 각 상수는 초기 8개의 소수(2, 3, 5, 7, 11, 13, 17, 19)를 이용하여 구한다.
- 상수값은 8개의 소수를 각각 **제곱근한 값**에서 일부를 추출한 값이다.
- 예 : $\sqrt{19}$ = 4.35889894354이다. 소수점 이하 일부를 추출하여 상수값으로 사용한다.
  → 상수는 다양한 방법으로 만들 수 있다. SHA-512는 이런 방법을 사용할 따름이다.

- SHA-512는 80 라운드를 거친다.
- 각 라운드에는 내부적으로 정해지는 서로 다른 상수 80개가 이용된다.
- 각 상수는 초기 80개의 소수(2, 3, 5, .., 409)를 **세제곱근한 값**에서 일부를 추출한 값이다.

정답 : ④

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? [2018년 국가 7급]

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.

♤ **방화벽**

방화벽 구분	세부 내용
제1세대 방화벽 **패킷 필터링** **(packet filtering)**	• 낮은 수준의 보안성 제공 • 패킷 그 자체만을 보고 허용 또는 거부를 결정한다. • 패킷의 **헤더 정보만을 검사**하여 동작한다. • 패킷 필터링만으로는 공격에 대한 방어가 어렵다. • 방화벽 내부에서 패킷들의 연결 상태(세션)를 관리하지 않는다. • 상태 관리가 없는 이런 종류의 방화벽을 **"무상태 방화벽"**이라 한다. • 특정 IP나 포트를 허용 또는 거부하는 용도로 사용된다. • **네트워크층과 전송층에서 동작**한다.
제2세대 방화벽 **상태 검사** **(stateful inspection)**	• 중급 수준의 보안성 제공(패킷 필터링 단점 보완) • 패킷 필터링 + 연결(connection) 정보 기반 처리 • 상태 검사는 **세션 단위의 검사**를 실시한다.**(유상태 방화벽)** • 세션은 패킷의 집합이다.(하나의 세션에 속한 패킷은 같은 처리) • 상태 검사도 패킷 필터링 기능을 사용하며 현재 연결 세션의 트래픽 상태와 미리 저장된 상태와의 비교를 통하여 접근을 제어한다. • 확장된 상태 검사 방화벽 → 복잡하고 다양한 파생 세션을 모두 처리할 수 있다. → 파생 세션 처리를 위해 별도의 추가 정책이 필요 없다.
제3세대 방화벽 **응용 필터링** **(application filtering)**	• 높은 수준의 보안성 제공 가능 • TCP/IP 패킷 필터링 + 연결 정보 기반 + 응용 필터링 • 세션에 포함된 정보의 유해성을 검사한다.**(응용층에서 동작)** • 패킷 내용 검사 및 응용에 미칠 영향을 분석한다. • 패킷 필터링에 비해 많은 부하가 발생된다. • 세션을 **중간에서 분리하여 중계**하는 방식이다.(세션 중계) • 응용 방화벽에 해당하는 네트워크 장비 • 응용 방화벽 : IPS, WAF, UTM 등

정답 : ③

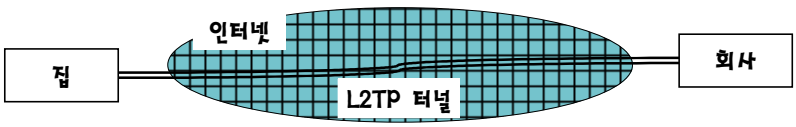
9. VPN의 터널링 기능을 제공하는 L2TP(Layer 2 Tunneling Protocol)에 대한 설명으로 옳지 않은 것은? [2018년 국가 7급]

① 데이터링크층에서 터널링을 지원한다.
② PPTP(Point-to-Point Tunneling Protocol)와 L2F(Layer2 Forwarding Protocol)의 기능을 결합한 프로토콜이다.
③ 데이터의 보안성을 높이기 위하여 IPsec과 결합하여 사용할 수 있다.
④ 패킷 인증, 암호화, 키 관리 기능을 제공한다.

♤ **가상사설망(VPN) – L2TP(Layer 2 Tunneling Protocol)**

• 패킷 인증, 암호화, 키 관리 기능을 제공한다.(×)
→ VPN이 제공하는 기본 기능은 **캡슐화, 인증, 데이터 암호화**이다.

VPN은 인터넷과 같은 공용 네트워크를 이용하여 **회사 전용선**처럼 운용하는 것이다.



// VPN 연결의 속성(크게 3가지) – Windows server 참조

인증	• 인증은 데이터 원본 **인증 및 데이터 무결성**을 제공하기 위한 것이다. • 인증 수준은 터널링 프로토콜 종류에 따라 다양하다. • 인증과 무결성을 위해 **메시지인증코드(MAC)를 사용**한다.
캡슐화	• 캡슐화는 데이터가 전송 네트워크를 **통과할 수 있도록 처리하는 것**이다. • 라우팅 정보가 포함된 헤더와 개인 데이터가 캡슐화 된다.
암호화	• 암호화는 공용 네트워크를 통과할 때 데이터의 **기밀성을 보장**하기 위한 것이다.

// L2TP(Layer 2 Tunneling Protocol) : 2계층

• L2TP는 L2F와 PPTP 프로토콜을 결합하여 만든 규격이다.(PPP도 지원)
• L2TP는 데이터링크층에서 터널링을 지원한다.
• L2TP는 터널을 확립해주기만 하고, IPsec 기술을 사용하여 암호화한다.
• L2TP는 대부분의 운영체제에서 기본적으로 지원한다.(안드로이드, iOS 등)

정답 : ④

10. 다음은 정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 개인정보 유출 등의 통지·신고에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은? [2018년 국가 7급]

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

법 개정

삭제

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

♤ **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.
〈개정 2014. 5. 28., 2016. 3. 22.〉

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

정답 : ③