2019-서울시-정보보호론-A형-해설

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

해설에 대한 모든 권리는 곽후근(대방고시, 하이클래스)에 있습니다.

1번부터 10번 해설동영상은 https://www.youtube.com/watch?v=PMQwMutg2MI&t=326s,
11번부터 20번 해설동영상은 https://www.youtube.com/watch?v=zvV7nQcugpI&t=258s
을 참고하기 바랍니다.

1. 해시와 메시지 인증코드에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 순서대로 나열한 것은?

<보기>
해시와 메시지 인증코드는 공통적으로 메시지의 (㉠)을 검증할 수 있지만, 메시지 인증코드만 (㉡) 인증에 활용될 수 있다.

	㉠	㉡
①	무결성	상호
②	무결성	서명자
③	비밀성	상호
④	비밀성	서명자

정답 체크 :
(1)
해시함수 : 무결성
MAC : 무결성, 상호 인증(비밀키)
오답 체크 :
(2), (3), (4)
전자 서명 : 서명자 인증(개인키), 무결성, 부인 방지
대칭키, 비대칭키 : 비밀성

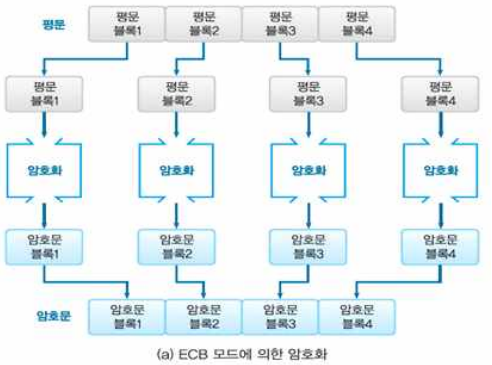
2. 바이러스의 종류 중에서 감염될 때마다 구현된 코드의 형태가 변형되는 것은?
① Polymorphic Virus
② Signature Virus
③ Generic Decryption Virus
④ Macro Virus
정답 체크 :
(1) Polymorphic Virus : 코드 조합을 다양하게 할 수 있는 조합(Mutation) 프로그램을 암호형 바이러스에 덧붙인다. (vs. Metamorphic - 행동도 변화)
오답 체크 :
(2) Signature Virus : 바이러스가 가진 특정한 문자열
(3) Generic Decryption Virus : 암호화된 바이러스가 실행을 위해 복호화 되는 것을 의미한다.
(4) Macro Virus : 엑셀 또는 워드와 같은 문서 파일의 매크로 기능을 이용하기 때문에 워드나 엑셀 파일을 열 때 감염된다. 누구나 바이러스를 만들어 배포하는 계기가 되었다.

3. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?
① 오용탐지는 새로운 침입 유형에 대한 탐지가 가능하다.
② 기술적 구성요소는 정보 수집, 정보 가공 및 축약, 침입 분석 및 탐지, 보고 및 조치 단계로 이루어진다.
③ 하이브리드 기반 IDS는 호스트 기반 IDS와 네트워크 기반 IDS가 결합한 형태이다.
④ IDS는 공격 대응 및 복구, 통계적인 상황 분석 보고 기능을 제공한다.
정답 체크 :
(1) 해당 설명은 이상탐지에 속하고, 오용탐지는 알려진 패턴(시그너처)에 기반한 것으로 알려지지 않은 침입 유형에 대한 탐지는 어렵다.
오답 체크 :
(2) 정보 수집, 정보 가공 및 축약(모든 정보를 탐지할 수 없음), 침입 분석 및 탐지, 보고 및 조치
(3) 호스트 기반(호스트에 설치) vs. 네트워크 기반(네트워크 중간에 설치)
(4) passive 보안에 속한다. IPS는 active 보안이다.

4. <보기>에서 블록암호 모드 중 초기 벡터(Initialization Vector)가 필요하지 않은 모드를 모두 고른 것은?

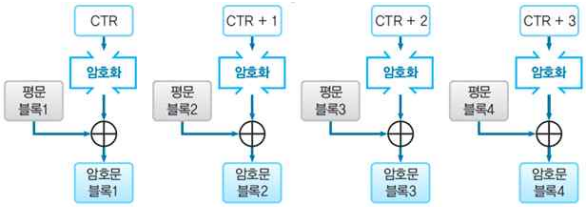
<보기> ㄱ. CTR 모드 ㄴ. CBC 모드 ㄷ. ECB 모드

① ㄱ
② ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ
정답 체크 :
(2) ECB는 그림에서 보는 바와 같이 IV(난수)가 필요하지 않다.



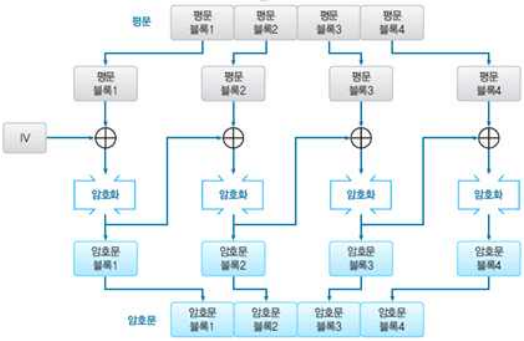
(a) ECB 모드에 의한 암호화

오답 체크 :
(1) CTR은 그림에서 보는 바와 같이 난수(CTR, IV)가 필요하다.



(a) CTR 모드에 의한 암호화

(3), (4) CBC는 그리멩서 보는 바와 같이 난수(IV)가 필요하다.



(a) CBC 모드에 의한 암호화

5. 스트림 암호(Stream Cipher)에 대한 설명으로 가장 옳지 않은 것은?

① Key Stream Generator 출력값을 입력값(평문)과 AND 연산하여, 암호문을 얻는다.

② 절대 안전도를 갖는 암호로 OTP(One - Time Pad)가 존재한다.

③ LFSR(Linear Feedback Shift Register)로 스트림 암호를 구현할 수 있다.

④ Trivium은 현대적 스트림 암호로 알려져 있다.

정답 체크 :

(1) AND가 아니라 XOR이다.

오답 체크 :

(2) OTP : 스트림 암호를 이용하여 키가 매번 바뀐다. (one time password가 아님)

(3) LFSR : 시프트 레지스터의 일종으로 의사 난수(키, 스트림 암호) 등을 만들 수 있다. 레지스터에 입력되는 값이 이전 상태 값들의 선형 함수(XOR)로 계산된다.

(4) Trivium : 하드웨어적으로 속도와 게이트 수를 적당히 조절했고, 소프트웨어적으로 효율적인 구현을 한 동기식(현재 암호문이 이전 암호문의 영향을 받지 않음) 스트림 암호이다.

6. <보기>에서 설명하는 DRM 구성요소는?

<보기> DRM의 보호 범위에서 유통되는 콘텐츠의 배포 단위 로서 암호화된 콘텐츠 메타 데이터, 전자서명 등의 정보로 구성되어 있다. 또한, MPEG-21 DID 규격을 따른다.

① 식별자

② 클리어링 하우스

③ 애플리케이션

④ 시큐어 컨테이너

정답 체크 :

(4) 시큐어 컨테이너 : 암호화된 콘텐츠에 대한 구조 표현 기술(메타 데이터, 전자 서명 등)

MPEG-21 DID(Digital Item Declaration) : 기본 처리단위가 되는 디지털 아이템을 표현하는 방법을 정의한다. 디지털 아이템은 멀티미디어 자원(소리, 동영상 등), 메타데이터 (MPEG-7), 식별자(URI, ISBN 등)로 구성된 멀티미디어 객체이다.
오답 체크 :
(1) 식별자 : DOI(Digital Object Identifier), 콘텐츠 식별자
(2) 클리어링 하우스 : 키 관리 및 라이선스 발급 관리
(3) 애플리케이션 : 응용 프로그램(DRM 대상물)

7. 이더넷(Ethernet)상에서 전달되는 모든 패킷(Packet)을 분석하여 사용자의 계정과 암호를 알아내는 것은?
① Nessus
② SAINT
③ Sniffing
④ IPS
정답 체크 :
(3) Sniffing : 패킷을 도청함(계정과 암호 도청)
오답 체크 :
(1) NESSUS : 원격지에서 다양한 방법을 통해 시스템이나 네트워크의 알려진 취약성에 대하여 점검을 수행
(2) SAINT : 관리자용 네트워크 진단도구
(4) IPS : 능동형(active) 침입 방지 시스템

8. 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화되어 있는 파일은?
① /etc/group
② /etc/passwd
③ /etc/shadow
④ /etc/login.defs
정답 체크 :
(3) /etc/shadow : 사용자 패스워드가 암호화
오답 체크 :
(1) /etc/group : 그룹이 등록되어 있는 파일
(2) /etc/passwd : 사용자에 대한 관리 정보
(4) /etc/login.defs : 사용자 계정의 설정(쉘)과 관련된 기본 값을 정의한 파일

9. 타원곡선 암호에 대한 설명으로 가장 옳지 않은 것은?
① 타원곡선 암호의 단점은 보안성 향상을 위하여 키 길이가 길어진다는 것이다.
② 타원곡선에서 정의된 연산은 덧셈이다.
③ 타원곡선을 이용하여 디피-헬먼(Diffie- Hellman) 키 교환을 수행 할 수 있다.
④ 타원곡선은 공개키 암호에 사용된다.
정답 체크 :

(1) ECC의 장점 : RSA에 비해 키의 비트 수가 적다. (보안성 향상을 위해 RSA 만큼 길어지지는 않음)
오답 체크 :
(2) 타원곡선에서 덧셈연산을 특별하게 정의함(암호화에 사용하기 위해)
(3) 타원곡선 디피-헬만 : 타원곡선 암호를 이용한 디피-헬먼 키 교환 방식
(4) 공개키 암호 : RSA, ECC, Rabin, ElGamal

10. 영지식 증명(Zero-Knowledge Proof)에 대한 설명으로 가장 옳지 않은 것은?
① 영지식 증명은 증명자(Prover)가 자신의 비밀 정보를 노출하지 않고 자신의 신분을 증명하는 기법을 의미한다.
② 영지식 증명에서 증명자 인증 수단으로 X.509 기반의 공개키 인증서를 사용할 수 있다.
③ 최근 블록 체인상에서 영지식 증명을 사용하여 사용자의 프라이버시를 보호하고자하며, 이러한 기술로 zk-SNARK가 있다.
④ 영지식 증명은 완정성(Completeness), 건실성(Soundness), 영지식성(Zero-Knowledgeness) 특성을 가져야 한다.
정답 체크 :
(2) 공인인증서(X.509) : 영지식 증명은 증명자가 자신이 알고 있는 지식과 정보를 공개하지 않으면서, 그 지식을 알고 있다는 사실을 검증자에게 증명하는 시스템이므로 X.509 인증서를 사용하면 안된다. X.509 자체가 지식과 정보를 공유하는 것이 된다.
오답 체크 :
(1) 영지식 증명 : 암호학에서 누군가가 상대방에게 어떤 사항(statement)이 참이라는 것을 증명할 때, 그 문장의 참 거짓 여부를 제외한 어떤 것도 노출되지 않는 interactive한 절차(패스워드를 알려주지 않고 패스워드를 알고 있다는 사실만을 알려줌)
(3) zk-SNARK(영지식 스나크) : 기존의 영지식 증명을 좀 더 간결하고(succinct) 비상호적인 환경(non-interactive)에서 적용 가능하도록 변형한 기술
(4) 영지식 증명의 세가지 성질
완전성 : 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득시킬 수 있어야 한다.
건실성 : 어떤 문장이 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 한다.
영지식성 : 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 한다.

11. 「개인정보 보호법」 상 주민등록 번호의 처리에 대한 설명으로 가장 옳지 않은 것은?
① 개인정보 처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.
② 행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.
③ 개인정보처리자는 정보 주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 개인정보처리자로부터 주민등록번호를 제공받은 자는 개인정보보호위원회의 심의·의결을 거쳐 제공받은 주민등록번호를 목적외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.
정답 체크 :
(4) “개인정보 보호법” 제24조의2(주민등록번호 처리의 제한) 상 ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우, 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우, 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우
오답 체크 :
(1) “개인정보 보호법” 제24조의2(주민등록번호 처리의 제한) 상 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.
(2) “개인정보 보호법” 제34조의2(과징금의 부과 등) 상 ① 행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.
(3) “개인정보 보호법” 제24조의2(주민등록번호 처리의 제한) 상 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.

12. <보기>의 설명에 해 당 되는 공격 유형으로 가장 적합한 것은?

<보기> SYN 패킷을 조작하여 출발지 IP 주소와 목적지 IP 주소를 일치시켜서 공격 대상에 보낸다. 이때 조작된 IP 주소는 공격 대상의 주소이다.

① Smurf Attack
② Land Attack
③ Teardrop Attack
④ Ping of Death Attack
정답 체크 :
(2) Land : 출발지 IP와 목적지 IP가 같고, 출발지 port와 목적지 port가 같은 것은 공격이다.
오답 체크 :
(1) Smurf : direct broadcasting과 ping flooding을 이용한 공격이다.
(3) Teardrop : sequence number가 겹치는 공격이다.
(4) Ping of death : ping을 보낼 때 패킷을 최대 길이(65,500바이트)로 보낸다.

13. TLS 및 DTLS 보안 프로토콜에 대한 설명으로 가장 옳지 않은 것은?
① TLS 프로토콜 에서는 인증서(Certificate)를 사용하여 인증을 수행할 수 있다.
② DTLS 프로토콜은 MQTT 응용 계층 프로토콜의 보안에 사용될 수 있다.
③ TLS 프로토콜은 Handshake·Change Cipher Spec·Alert 프로토콜과 Record 프로토콜 등으로 구성되어 있다.
④ TCP 계층 보안을 위해 TLS가 사용되며, UDP 계층 보안을 위해 DTLS가 사용된다.
정답 체크 :
(2) MQTT가 아니라 CoAP이다. MQTT와 CoAP는 IoT 전용 프로토콜이다. (IoT에서 사용하는 별도의 프로토콜)
오답 체크 :
(1) 인증서를 사용하여 서버와 클라이언트가 상호 인증을 수행
(3) TLS 프로토콜
Handshake : 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다. 인증서를 이용한 인증을 수행한다.
Change Cipher Spec : 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.
Alert : 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.
Record : 대칭 암호를 사용해서 메시지를 암호화하고 통신하는 부분이다. 대칭 암호와 메시지 인증 코드를 이용한다. 알고리즘과 공유 키는 핸드쉐이크 프로토콜을 사용해서 서버와 클라이언트가 상담하여 결정한다.
(4) TCP-TLS, UDP-DTLS(같은 Datagram을 사용)

14. 무선 통신 보안 기술에 대한 설명으로 가장 옳지 않은 것은?
① 무선 네트워크 보안 기술에 사용되는 WPA2 기술은 AES/CCMP를 사용한다.
② 무선 네트워크에서는 인증 및 인가, 과금을 위해 RADIUS 프로토콜을 사용할 수 있다.
③ 무선 AP의 SSID값 노출과 MAC 주소 기반 필터링 기법은 공격의 원인이 된다.
④ 무선 네트워크 보안 기술인 WEP(Wired Equivalent Privacy) 기술은 유선 네트워크 수준의 보안성을 제공하므로 기존의 보안 취약성 문제를 극복했다.
정답 체크 :
(4) 64비트 WEP 키는 전사 공격에 의해 수분 내에 깨진다.
오답 체크 :
(1) WPA2는 ACS, CCMP를 사용한다.
(2) WPA, WPA2에서 802.1x를 이용해서 Radius를 사용한다. 현재는 개선된 Tacacs+, Diameter를 사용한다.
(3) SSID 노출(브로드캐스팅되는 SSID에 접속), MAC 필터링(인가된 MAC으로 변조)
Tip! : 무선랜 보안 표준을 테이블로 비교하면 다음과 같다.

〈표 6-9〉 무선랜 보안 표준 비교

구분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access 2)
개요	1997년 재정(2003년 삭제)	WEP 방식 보완 (Wi-Fi Alliance)	IEEE 802.11i(2004년) 준수
인증	사전 공유된 비밀키 사용 (64비트, 128비트)	• 별도의 인증서버를 이용하는 EAP 인증 프로토콜(802.1x) • WPA-PSK(사전 공유된 비밀키)	• 별도의 인증서버를 이용하는 EAP 인증 프로토콜(802.1x) • WPA-PSK(사전 공유된 비밀키)
암호화	• 고정 암호키 사용(인증키와 동일) • RC4 알고리즘사용	• 암호키 동적 변경(TKIP) • RC4 알고리즘 사용	• 암호키 동적 변경(CCMP) • AES 등 강력한 블록 암호 알고리즘 사용
보안성	• 64비트 WEP 키는 수분 내 노출 • 취약하여 널리 쓰이지 않음	• WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	• 가장 강력한 보안 가능 제공

15. 서비스 거부 공격(DoS)에 대한 설명으로 가장 옳지 않은 것은?
① 공격자가 임의로 자신의 IP 주소를 속여서 다량으로 서버에 보낸다.
② 대상 포트 번호를 확인하여 17, 135, 137 번, UDP 포트 스캔이 아니면, UDP Flooding 공격으로 간주한다.
③ 헤더가 조작된 일련의 IP 패킷 조각들을 전송한다.
④ 신뢰 관계에 있는 두 시스템 사이에 공격자의 호스트를 마치 하나의 신뢰 관계에 있는 호스트인 것처럼 속인다.
정답 체크 :
(4) : DoS가 아닌 IP spoofing에 대한 설명이다.
오답 체크 :
(1) : Smurf attack (자원 고갈형 DoS)
(2) : 17(Quotd-오늘의 인용문), 135(TCP RPC), 137(UDP NetBIOS), UDP 포트스캔 : 자주 사용되는 것이 아니면 UDP flooding으로 간주(많이 보냄) (자원 고갈형 DoS)
(3) : Land attack(출발지 IP를 변조) (취약점 공격형 DoS)

16. 윈도우 운영체 제에서의 레지스트리(Registry)에 대한 설명으로 가장 옳은 것은?
① 레지스트리 변화를 분석함으로써 악성코드를 탐지할 수 있다.
② 레지스트리는 운영체제가 관리하므로 사용자가 직접 조작할 수 없다.
③ 레지스트리 편집기를 열었을 때 보이는 다섯 개의 키를 하이브(Hive)라고 부른다.
④ HKEY_CURRENT_CONFIG는 시스템에 로그인하고 있는 사용자와 관련된 시스템 정보를 저장한다.
정답 체크 :
(1) 내가 아닌 누군가가 수정했다면 악성 코드의 수정으로 볼 수도 있다.
오답 체크 :
(2) 사용자가 조작 가능하다(regedit)
(3) 하이브가 아니라 루트키라고 부름, 하이브(하드디스크에 저장된 레지스트리 파일)

(4) 해당 설명은 HKEY_CURRENT_USER이고, HKEY_CURRENT_CONFIG는 실행 시간에 수집한 자료(정보)를 담고 있다.

17. 침입차단시스템에 대한 설명으로 가장 옳은 것은?

① 스크린드 서브넷 구조(Screened Subnet Architecture)는 DMZ와 같은 완충 지역을 포함하며 구축 비용이 저렴하다.

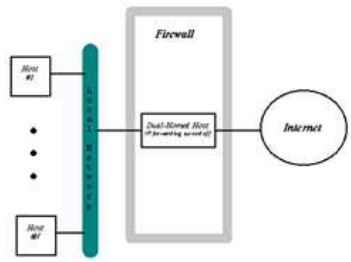
② 스크리닝 라우터 구조(Screening Router Architecture)는 패킷을 필터링하도록 구성되므로 구조가 간단하고 인증 기능도 제공할 수 있다.

③ 이중 네트워크 호스트 구조(Dual-homed Host Architecture)는 내부 네트워크를 숨기지만, 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

④ 스크린드 호스트 게이트웨이 구조(Screened Host Gateway Architecture)는 서비스 속도가 느리지만, 베스천 호스트에 대한 침입이 있어도 내부 네트워크를 보호할 수 있다.

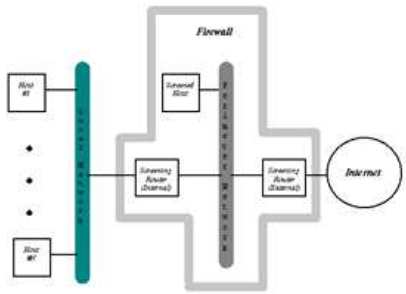
정답 체크 :

(3) dual-homed host : 베스천 호스트가 손상되면 무조건적인 접속을 허용한다. (1 bastion host)

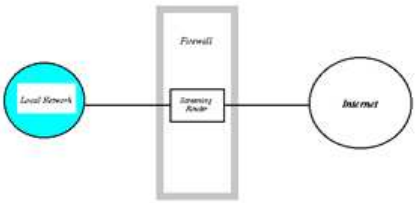


오답 체크 :

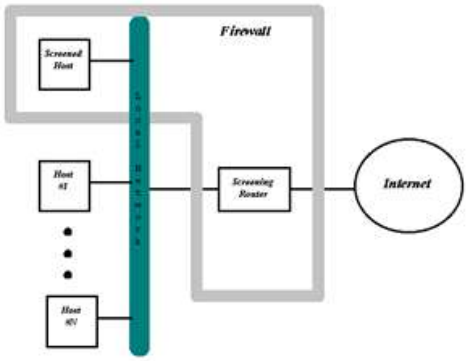
(1) screened subnet : 구축 비용이 많이 든다(2 screening routers + 1 bastion host)



(2) screening router : 인증 기능은 제공하지 않는다(3, 4 계층의 필터링만을 제공) (1 screening router)



(4) screened host : 베스천 호스트를 침입하면 내부 네트워크를 보호할 수 없다(1 screening router + 1 bastion host)



18. 최근 알려진 Meltdown 보안 취약점에 대한 설명으로 가장 옳은 것은?
① CPU가 사용하는 소비 전력 패턴을 사용하여 중요한 키 값이 유출되는 보안 취약점이다.
② CPU의 특정 명령어가 실행 될 때 소요되는 시간을 측정하여 해당 명령어와 주요한 키 값이 유출될 수 있는 보안 취약점이다.
③ SSL 설정 시 CPU 실행에 영향을 미쳐 CPU 과열로 인해 오류를 유발하는 보안 취약점이다.
④ CPU를 고속화하기 위해 사용된 비순차적 명령어 처리(Out-of-Order Execution) 기술을 악용한 보안 취약점이다.
정답 체크 :
(4) Meltdown : 비순차적 명령어 처리(순차적으로 명령어를 처리하는 것보다 속도를 높일 수 있음)로 인한 권한 상승 취약점을 공격이다.
오답 체크 :
(1) 부채널 공격 : 소비 전력 패턴
암호학에서 부채널 공격(side channel attack)은 알고리즘의 약점을 찾거나(암호 해독과는 다름) 무차별 공격을 하는 대신에 암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법이다. 예를 들어, 소요 시간 정보, 소비 전력, 방출하는 전자기파, 심지어는 소리를 통해서 시스템 파괴를 위해 악용할 수 있는 추가 정보를 얻을 수 있다.
(2) 부채널 공격 : 명령어에 소요되는 시간
(3) TLS overhead : SSL과 CPU 과열은 연관성을 가짐

19. <보기>는 TCSEC(Trusted Computer System Evaluation Criteria)에 의하여 보안 등급을 평가할 때 만족해야 할 요건들에 대한 설명이다. 보안 등급이 높은 것부터 순서대로 나열된 것은?

<보기>
ㄱ. 강제적 접근 제어가 구현되어야 한다.
ㄴ. 정형화된 보안 정책을 일정하게 유지하여야 한다.
ㄷ. 사용자가 자신의 파일에 대한 접근 권한을 설정할 수 있어야 한다.

① ㄱ-ㄴ-ㄷ
② ㄱ-ㄷ-ㄴ
③ ㄴ-ㄱ-ㄷ
④ ㄴ-ㄷ-ㄱ

정답 체크 :
(3)
(ㄱ) 강제적 접근 제어 : B1
(ㄴ) 정형화된 보안 정책 : B2
(ㄷ) 자신의 파일에 접근 권한 설정 : C1
A1(Verified Design, 완벽) > B3(Security Domains, OS에서 불필요한 것 모두 제거) > B2(Structured Protection, 인증 강화/역할 분리) > B1(Labeled Security, MAC) > C2(Controlled Access Protection, 계정별 로그인, 그룹 ID) > C1(Discretionary Security Protection, DAC) > D(Minimal Protection, 보안 설정 없음)

20. 정보보호 및 개인정보보호 관리체계인증(ISMS-P)에 대한 설명으로 가장 옳지 않은 것은?
① 정보보호 관리체계 인증만 선택적으로 받을 수 있다.
② 개인정보 제공 시 뿐만 아니라 파기 시의 보호조치도 포함한다.
③ 위험 관리 분야의 인증기준은 보호대책 요구사항 영역에서 규정한다.
④ 관리 체계 수립 및 운영 영역은 Plan, Do, Check, Act의 사이클에 따라 지속적이고 반복적으로 실행되는지 평가한다.
정답 체크 :
(3) 위험 관리는 보호대책 요구사항이 아니라 관리체계 수립 및 운영이다.
오답 체크 :
(1) 의무대상자는 ISMS, ISMS-P 인증 중 선택 가능하다.
(2) 개인정보 제공 시 보호조치와 개인정보 파기 시 보호조치를 포함한다.
(4) 경영순환주기인 PDCA 사이클을 정보보호에 적용
Tip! : ISMS-P의 인증기준 구성을 테이블로 정리하면 다음과 같다.

정보보호 및 개인정보보호 관리체계 인증기준 구성

영역	분야	적용 여부	
		ISMS	ISMS-P
1. 관리체계 수립 및 운영 (16개)	1.1. 관리체계 기반 마련	O	O
	1.2. 위험 관리 (3)	O	O
	1.3. 관리체계 운영	O	O
	1.4. 관리체계 점검 및 개선	O	O
2. 보호대책 요구사항 (64개)	2.1. 정책, 조직, 자산 관리	O	O
	2.2. 인적 보안	O	O
	2.3. 외부자 보안	O	O
	2.4. 물리 보안	O	O
	2.5. 인증 및 권한관리	O	O
	2.6. 접근통제	O	O
	2.7. 암호화 적용	O	O
	2.8. 정보시스템 도입 및 개발 보안	O	O
	2.9. 시스템 및 서비스 운영관리	O	O
	2.10. 시스템 및 서비스 보안관리	O	O
	2.11. 사고 예방 및 대응	O	O
	2.12. 재해복구	O	O
3. 개인정보 처리 단계별 요구사항 (22개)	3.1. 개인정보 수집 시 보호조치	-	O
	3.2. 개인정보 보유 및 이용 시 보호조치	-	O
	3.3. 개인정보 제공 시 보호조치	-	O
	3.4. 개인정보 파기 시 보호조치 (2)	-	O
	3.5. 정보주체 권리보호	-	O