

# 2015-서울시-정보보호론-A형-해설-곽후근

1. 패스워드가 갖는 취약점에 대한 대응방안으로 적절치 않은 것은?

- ① 사용자 특성을 포함시켜 패스워드 분실을 최소화한다.
- ② 서로 다른 장비들에 유사한 패스워드를 적용하는 것을 금지한다.
- ③ 패스워드 파일의 불법적인 접근을 방지한다.
- ④ 오염된 패스워드는 빠른 시간 내에 발견하고, 새로운 패스워드를 발급한다.

정답 체크 :

(1) 사용자 특성 : 패스워드에 사용자 특성을 포함하면 사회공학적으로 패스워드를 유추할 수 있다.

오답 체크 :

- (2) 서로 다른 장비 : 서로 다른 장비에는 서로 다른 패스워드를 적용해야 한다. 유사한 패스워드를 적용하면 한 장비의 패스워드가 유출되면 나머지 장비들도 안전하지 않다.
- (3) 불법적인 접근 : 패스워드 파일은 암호화가 되어 있다고 하더라도 불법적인 접근을 막아야 한다.
- (4) 오염된 패스워드 : 패스워드에 문제가 생기면 새로운 패스워드를 발급해야 한다.

2. 대칭키 암호시스템과 공개키 암호시스템의 장점을 조합한 것을 하이브리드 암호시스템이라고 부른다. 하이브리드 암호시스템을 사용하여 송신자가 수신자에게 문서를 보낼 때의 과정을 순서대로 나열하면 다음과 같다. 각 시점에 적용되는 암호시스템을 순서대로 나열하면?

- ㉠ 키를 사용하여 문서를 암호화할 때
- ㉡ 문서를 암호·복호화하는 데 필요한 키를 암호화할 때
- ㉢ 키를 사용하여 암호화된 문서를 복호화할 때

- ① ㉠ 공개키 암호시스템, ㉡ 대칭키 암호시스템, ㉢ 공개키 암호시스템
- ② ㉠ 공개키 암호시스템, ㉡ 공개키 암호시스템, ㉢ 대칭키 암호시스템
- ③ ㉠ 대칭키 암호시스템, ㉡ 대칭키 암호시스템, ㉢ 공개키 암호시스템
- ④ ㉠ 대칭키 암호시스템, ㉡ 공개키 암호시스템, ㉢ 대칭키 암호시스템

정답 체크 :

(4)

하이브리드 암호시스템은 대칭키(빠른 속도)와 공개키(키 배송 문제가 없음)의 장점을 조합한다.

- (ㄱ) '키'를 사용하여 '문서'를 암호화할 때 : 대칭키 암호시스템
- (ㄴ) '문서'를 암호·복호화하는 데 필요한 '키'를 암호화할 때 : 공개키 암호시스템
- '문서'를 암호·복호화하는 데 필요한 '키'를 복호화할 때 : 공개키 암호시스템
- (ㄷ) '키'를 사용하여 암호화된 '문서'를 복호화할 때 : 대칭키 암호시스템

3. 현재 10명이 사용하는 암호시스템을 20명이 사용할 수 있도록 확장하려면 필요한 키의 개수도 늘어난다. 대칭키 암호 시스템과 공개키 암호시스템을 채택할 때 추가로 필요한 키의 개수를 각각 구분하여 순서대로 나열한 것은?

- ① 20개, 145개
- ② 20개, 155개
- ③ 145개, 20개
- ④ 155개, 20개

정답 체크 :

(3)

대칭키 개수의 개수는 사용자가 n명이라면  $n(n-1)/2$ 이 된다. 공개키 개수의 개수는 사용자가 n명이라면  $2n$ 이 된다. 사용자면 10명이면 대칭키는 45개가 되고 공개키는 20개가 된다. 그리고 사용자가 20명이면 대칭키는 190개가 되고 공개키는 40개가 된다. 따라서 추가로 필요한 키의 개수는 145개 (=190개 - 45개), 20개(=40개 - 20개)가 된다.

4. 다음은 오용탐지(misuse detection)와 이상탐지(anomaly detection)에 대한 설명이다. 이상탐지에 해당되는 것을 모두 고르면?

- ㉠ 통계적 분석 방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다.
- ㉡ 미리 축적한 시그니처와 일치하면 침입으로 판단한다.
- ㉢ 제로데이 공격을 탐지하기에 적합하다.
- ㉣ 임계값을 설정하기 쉽기 때문에 오탐률이 낮다.

- ① ㉠, ㉢
- ② ㉠, ㉣
- ③ ㉡, ㉢
- ④ ㉡, ㉣

정답 체크 :

(1)

(㉠) 통계적 분석 방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다 : 이상탐지  
(㉢) 제로데이 공격을 탐지하기에 적합하다 : 이상탐지

오답 체크 :

(2), (3), (4)

(㉡) 미리 축적한 시그니처와 일치하면 침입으로 판단한다 : 오용탐지  
(㉣) 임계값을 설정하기 쉽기 때문에 오탐률이 낮다 : 오용탐지

5. SYN flooding을 기반으로 하는 DoS 공격에 대한 설명으로 옳지 않은 것은?

- ① 향후 연결요청에 대한 피해 서버에서 대응 능력을 무력화 시키는 공격이다.
- ② 공격 패킷의 소스 주소로 인터넷상에서 사용되지 않는 주소를 주로 사용한다.
- ③ 운영체제에서 수신할 수 있는 SYN 패킷의 수를 제한하지 않은 것이 원인이다.
- ④ 다른 DoS 공격에 비해서 작은 수의 패킷으로 공격이 가능하다.

정답 체크 :

(3) 제한 : SYN 패킷의 수를 제한하기 때문에 문제가 발생한다.

오답 체크 :

- (1) 무력화 : 서버가 더 이상의 SYN 패킷을 받을 수가 없다.
- (2) 소스 주소 : 공격자로부터 SYN 패킷을 받고 서버가 SYN+ACK 패킷을 보내지만 공격자의 주소가 인터넷상에서 사용되지 않는 주소이기 때문에 서버는 ACK 응답을 받지 못한다.
- (4) 적은 수의 패킷 : 예를 들어, UDP flooding은 공격자가 공격 대상보다 좋은 성능의 컴퓨터로 UDP 패킷을 많이 보내야 하는데, SYN flooding은 서버의 제한된 SYN 패킷 수만큼만 보내면 된다.

6. 다음은 접근통제(access control) 기법에 대한 설명이다. 강제 접근제어(Mandatory Access Control)에 해당되는 것은?

- ① 각 주체와 객체 쌍에 대하여 접근통제 방법을 결정함
- ② 정보에 대하여 비밀 등급이 정해지며 보안 레이블을 사용함
- ③ 주체를 역할에 따라 분류하여 접근권한을 할당함
- ④ 객체의 소유자가 해당 객체의 접근통제 방법을 변경할 수 있음

정답 체크 :

(2) 보안 레이블(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 분야에 적합하다.

오답 체크 :

- (1) ACM 또는 LBAC : 쌍(LBAC) : 객체들(자원, 컴퓨터, 어플리케이션)과 주체들(개인, 그룹, 조직) 사이의 상호작용에 기반을 둔 복잡한 접근 제어 모델이다.
- (3) 역할(RBAC) : 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
- (4) 소유자(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.

7. 다음은 AES(Advanced Encryption Standard) 암호에 대한 설명이다. 옳지 않은 것은?

- ① 1997년 미 상무성이 주관이 되어 새로운 블록 암호를 공모했고, 2000년 Rijndael을 최종 AES 알고리즘으로 선정하였다.
- ② 라운드 횟수는 한 번의 암호 복호화를 반복하는 라운드 함수의 수행 횟수이고, 10/12/14 라운드로 이루어져 있다.
- ③ 128비트 크기의 입력·출력 블록을 사용하고, 128/192/256 비트의 가변크기 키 길이를 제공한다.
- ④ 입력을 좌우 블록으로 분할하여 한 블록을 라운드 함수에 적용시킨 후에 출력값을 다른 블록에 적용하는 과정을 좌우 블록에 대해 반복적으로 시행하는 SPN(Substitution-Permutation Network) 구조를 따른다.

정답 체크 :

(4) SPN : 해당 설명은 Feistel 구조이고, SPN 구조는 SubBytes(바이트 대체), ShiftRows(행 이동), MixColumns(열 섞기), AddRoundKey(라운드 키와 XOR)를 사용한다.

오답 체크 :

- (1) 1997년과 2000년 : 1997년 1월 2일 NIST(미국 표준 기술 연구소)는 AES의 모집을 개시하였다. 2000년 10월 2일 Rijndael(라인델)이 다른 후보(MARS, RC6, Serpent, Twofish)를 누르고 NIST에 의해 AES로서 선정되었다.
- (2) 라운드 수 : 라운드 수는 10/12/14이고, 라운드 수에 따라 키 길이가 바뀐다.
- (3) 블록과 키 길이 : 128비트의 블록 길이를 가지고, 라운드 수에 따라 128/192/256의 키 길이를 가진다.

8. SET(Secure Electronic Transaction)의 설명으로 옳은 것은?

- ① SET 참여자들이 신원을 확인하지 않고 인증서를 발급한다.
- ② 오프라인상에서 금융거래 안전성을 보장하기 위한 시스템이다.
- ③ 신용카드 사용을 위해 상점에서 소프트웨어를 요구하지 않는다.
- ④ SET는 신용카드 트랜잭션을 보호하기 위해 인증, 기밀성 및 메시지 무결성 등의 서비스를 제공한다.

정답 체크 :

(4) 인증, 기밀성, 무결성 : 기밀성, 무결성, 부인 방지, 인증 등을 보장한다.

오답 체크 :

- (1) 인증서 : 거래 상대의 신원을 확인하고 인증서를 발급해야 한다.
- (2) 오프라인 : 온라인상의 전자상거래를 위해 만들어진 것이다.
- (3) 소프트웨어 : 카드 소지자에게 전자지갑 소프트웨어의 사용을 요구하여 불편을 초래할 수 있다.

9. 다음 중 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?

- ① 커버로스는 개방형 분산 통신망에서 클라이언트와 서버 간의 상호인증을 지원하는 인증 프로토콜이다.
- ② 커버로스는 시스템을 통해 패스워드를 평문 형태로 전송한다.
- ③ 커버로스는 네트워크 응용 프로그램이 상대방의 신분을 식별할 수 있게 한다.
- ④ 기본적으로 비밀키 알고리즘인 DES를 기반으로 하는 상호인증시스템으로 버전4가 일반적으로 사용된다.

정답 체크 :

(2) 패스워드 : 이전 버전에서는 패스워드를 암호화해서 전송했고, 버전4에서는 패스워드를 클라이언트와 AS(인증 서버)가 서로 가지고 있고 전송하지 않는다.

오답 체크 :

- (1) 인증 프로토콜 : 커버로스는 MIT에서 개발한 비밀키(대칭키) 암호 기반 키 분배 및 사용자 인증 시스템이다. 중앙 집중식 인증 서버를 이용한다.
- (3) 상대방 신분 식별 : Authenticator(인증자)를 이용하여 사용자를 인증한다.
- (4) 버전4 : 버전5(AES)까지 출시되었으나 버전4(DES)를 많이 사용한다.

10. 다음 중 해시함수의 설명으로 옳은 것은?

- ① 입력은 고정길이를 갖고 출력은 가변길이를 갖는다.
- ② 해시함수(H)는 다대일(n : 1) 대응 함수로 동일한 출력을 갖는 입력이 두 개 이상 존재하기 때문에 충돌(collision)을 피할 수 있다.
- ③ 해시함수는 일반적으로 키를 사용하지 않는 MAC(Message Authentication Code) 알고리즘을 사용한다.
- ④ MAC는 데이터의 무결성과 데이터 발신지 인증 기능도 제공한다.

정답 체크 :

(4) MAC : 해시는 무결성을 제공하고, MAC은 무결성과 인증을 제공한다.

오답 체크 :

- (1) 입력과 출력 : 입력은 가변길이를 갖고, 출력은 고정길이를 갖는다.
- (2) 충돌 : 동일한 출력을 갖는 입력이 두 개 이상 존재하기 때문에 충돌을 피할 수 없다.
- (3) MAC : 해시는 키를 사용하지 않고, MAC은 키를 사용한다.

11. 다음에서 허니팟(honeypot)이 갖는 고유 특징에 대한 설명으로 옳지 않은 것은?

- ① 시스템을 관찰하고 침입을 방지할 수 있는 규칙이 적용된다.
- ② 중요한 시스템을 보호하기 위해서 잠재적 공격자를 유혹한다.
- ③ 공격자의 행동 패턴에 대한 유용한 정보를 수집할 수 있다.
- ④ 대응책을 강구하기에 충분한 시간 동안 공격자가 머물게 한다.

정답 체크 :

(1) 규칙 적용 : 정보를 수집하거나 대응책을 강구할 뿐 규칙을 적용하여 침입을 방지하지는 않는다.

오답 체크 :

- (2) 유혹 : 크래커를 유인하는 함정을 꿀단지에 비유한 것에서 명칭이 유래한다.
- (3) 정보 수집 : 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 한다.
- (4) 대응책 강구 : 침입자를 오래 머물게 하여 추적이 가능하므로 능동적으로 방어할 수 있고, 침입자의 공격을 차단할 수 있다.

12. Diffie-Hellman 알고리즘은 비밀키를 공유하는 과정에서 특정 공격에 취약할 가능성이 존재한다. 다음 중 Diffie-Hellman 알고리즘에 가장 취약한 공격으로 옳은 것은?

- ① DDoS(Distributed Denial of Service) 공격
- ② 중간자 개입(Man-in-the-middle) 공격
- ③ 세션 하이재킹(Session Hijacking) 공격
- ④ 강제지연(Forced-delay) 공격

정답 체크 :

(2) 중간자 개입 : 상대방의 난수가 진짜 상대방의 난수인지 알 방법이 없다.

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.
- (3) 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.
- (4) 강제지연 : 공격자가 통신을 주고 받는 두 송수신자 사이에 개입하여, 그들이 보내는 통신 정보를 가로채 두었다가 일정 시간이 흐른 뒤 전송하는 공격이다.

13. 다음은 공개키 기반 구조(PKI)에 대한 정의이다. 옳지 않은 것은?

- ① 네트워크 환경에서 보안 요구사항을 만족시키기 위해 공개키 암호화 인증서 사용을 가능하게 해주는 기반 구조이다.
- ② 암호화된 메시지를 송신할 때에는 수신자의 개인키를 사용하며, 암호화된 서명 송신 시에는 송신자의 공개키를 사용한다.
- ③ 공개키 인증서를 발행하여 기밀성, 무결성, 인증, 부인 방지, 접근 제어를 보장한다.
- ④ 공개키 기반 구조의 구성요소로는 공개키 인증서, 인증 기관, 등록기관, 디렉터리(저장소), 사용자

등이 있다.

정답 체크 :

(2) 개인키와 공개키 : 암호화된 메시지를 송신할 때에는 수신자의 공개키를 사용하며, 암호화된 서명 송신 시에는 송신자의 개인키를 사용한다.

오답 체크 :

(1) 기반 구조 : 공개키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택사항의 총칭이다. 예를 들면, PKCS, RFC, X.509, API 사양서 등을 들 수 있다.

(3) 보장 : 공개키로 암호화하면 기밀성을 보장하고, 개인키로 암호화하면 무결성, 인증, 부인 방지를 보장한다.

(4) 구성요소 : PKI의 구성 요소에는 공개키 인증서(공인인증서), 인증기관, 등록기관, 디렉터리(저장소, 데이터베이스), 사용자(이용자) 등이 있다.

14. 블록 암호는 평문을 일정한 단위(블록)로 나누어서 각 단위 마다 암호화 과정을 수행하여 암호문을 얻는 방법이다. 블록암호 공격에 대한 설명으로 옳지 않은 것은?

① 선형 공격 : 알고리즘 내부의 비선형 구조를 적당히 선형화시켜 키를 찾아내는 방법이다.

② 전수 공격 : 암호화할 때 일어날 수 있는 모든 가능한 경우에 대해 조사하는 방법으로 경우의 수가 적을 때는 가장 정확한 방법이지만 일반적으로 경우의 수가 많은 경우에는 실현 불가능한 방법이다.

③ 차분 공격 : 두 개의 평문 블록들의 비트 차이에 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 키를 찾아내는 방법이다.

④ 수학적 분석 : 암호문에 대한 평문이 각 단어의 빈도에 관한 자료를 포함하는 지금까지 모든 통계적인 자료를 이용하여 해독하는 방법이다.

정답 체크 :

(4) 수학 : 해당 설명은 통계적 분석을 의미하고, 수학적 분석은 수학적 이론을 이용하여 해독한다. 일반적으로 수학적 분석이 통계적 분석을 포함하나 가장 틀린 답은 해당 지문이 된다.

오답 체크 :

(1) 선형 : 평문과 암호문 비트를 몇 개 정도 XOR 해서 0이 되는 확률을 조사한다.

(2) 전수 : 가능한 모든 조합을 이용(대입)해서 공격하는 것을 의미한다.

(3) 차분 : 평문의 일부를 변경할 때 암호문이 어떻게 변화하는지 관찰하여 조사한다.

15. 다음은 웹사이트와 브라우저에 대한 주요 공격 유형 중 하나이다. 무엇에 대한 설명인가?

웹페이지가 웹사이트를 구성하는 방식과 웹사이트가 동작 하는 데 필요한 기본과정을 공략하는 공격으로, 브라우저에서 사용자 몰래 요청이 일어나게 강제하는 공격이다. 다른 공격과 달리 특별한 공격 포인트가 없다. 즉, HTTP 트래픽을 변조 하지도 않고, 문자나 인코딩 기법을 악의적으로 사용할 필요도 없다.

① 크로스사이트 요청 위조

② 크로스사이트 스크립팅

③ SQL 인젝션

④ 비트플리핑 공격

정답 체크 :

(1) CSRF : 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한

행위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격이다. 즉, 일단 사용자가 웹 사이트에 로그인한 상태에서 CSRF 공격 코드가 삽입된 페이지를 열면, 이후에는 사용자의 행동과 관계 없이 사용자의 웹 브라우저와 공격 대상 웹 사이트 간의 상호 작용이 이루어진다.

오답 체크 :

(2) 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.

(3) SQL Injection : 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.

(4) Bit flipping : 공격자가 암호문을 변경해서 평문을 바꾸는 공격 방법이다. 공격자는 동일한 메시지에서 중요 정보를 변경한다. 예를 들어, 송금 메시지 전송에서 암호문 중에 숫자 부분을 찾아서 변경할 수 있다면 평문의 송금 금액을 변경할 수 있다.

16. 가상사설망(VPN)이 제공하는 보안 서비스에 해당하지 않는 것은?

- ① 패킷 필터링
- ② 데이터 암호화
- ③ 접근제어
- ④ 터널링

오답 체크 :

(1) 패킷 필터링 : VPN이 아닌 방화벽에서 제공하는 기능이다.

정답 체크 :

(2) 암호화 : IPSec(3계층)에서 제공한다.

(3) 접근제어 : SSL(4계층)에서 제공한다.

(4) 터널링 : L2F, PPTP, L2TP(2계층)에서 제공한다. 터널링 자체에서 보안 기능을 제공하지는 않지만 터널링 자체를 보안으로 보는 견해가 존재하므로 가장 틀린 답은 아니다.

17. 전자서명(digital signature)은 내가 받은 메시지를 어떤 사람이 만들었는지를 확인하는 인증을 말한다. 다음 중 전자서명의 특징이 아닌 것은?

- ① 서명자 인증 : 서명자 이외의 타인이 서명을 위조하기 어려워야 한다.
- ② 위조 불가 : 서명자 이외의 타인의 서명을 위조하기 어려워야 한다.
- ③ 부인 불가 : 서명자는 서명 사실을 부인할 수 없어야 한다.
- ④ 재사용 가능 : 기존의 서명을 추후에 다른 문서에도 재사용 할 수 있어야 한다.

정답 체크 :

(4) 재사용 가능 : 재사용 불가이다. 즉, 서명문의 해시값을 전자서명에 이용하므로 한 번 생성된 서명을 다른 문서의 서명으로 사용할 수 없다.

오답 체크 :

- (1) 서명자 인증 : 서명문의 서명자를 확인할 수 있다.
- (2) 위조 불가 : 서명자만이 서명문을 생성할 수 있다.
- (3) 부인 불가 : 서명자가 나중에 서명한 사실을 부인할 수 없다.

Tip! : 이외에도 변경 불가가 있다. 변경 불가는 서명된 문서는 내용을 변경할 수 없기 때문에 데이터가 변조되지 않았음을 보장하는 무결성을 만족한다.

18. 다음 <보기>에서 설명하는 것은 무엇인가?

<보기>  
IP 데이터그램에서 제공하는 선택적 인증과 무결성, 기밀성 그리고 재전송 공격 방지 기능을 한다. 터널 종단 간에 협상 된 키와 암호화 알고리즘으로 데이터그램을 암호화한다.

- ① AH(Authentication Header)
- ② ESP(Encapsulation Security Payload)
- ③ MAC(Message Authentication Code)
- ④ ISAKMP(Internet Security Association & Key Management Protocol)

정답 체크 :

(2) ESP : 기밀성, 무결성, 인증, 재사용 방지를 제공한다.

오답 체크 :

- (1) AH : 무결성과 인증을 제공한다.
- (3) MAC : 무결성과 인증을 제공한다.
- (4) ISAKMP : RFC 2408에 규정되어 있으며, 구체적으로는 어떠한 인증 알고리즘, 암호화 기술, 암호 키 교환 규약을 사용할 것인지 등의 보안 수단을 상대방에게 알리기 위한 메시지 형식이다. 인터넷 표준 암호 키 교환 프로토콜인 IKE의 일부로 규정되어 있다.

19. 다음 <보기>에서 설명하고 있는 무선네트워크의 보안 프로토콜은 무엇인가?

<보기>  
AP와 통신해야 할 클라이언트에 암호화키를 기본으로 등록 해 두고 있다. 그러나 암호화키를 이용해 128비트인 통신용 암호화키를 새로 생성하고, 이 암호화키를 10,000개 패킷마다 바꾼다. 기존보다 훨씬 더 강화된 암호화 세션을 제공한다.

- ① WEP(Wired Equivalent Privacy)
- ② TKIP(Temporal Key Integrity Protocol)
- ③ WPA-PSK(Wi-Fi Protected Access Pre Shared Key)
- ④ EAP(Extensible Authentication Protocol)

정답 체크 :

(3) WPA-PSK : WEP처럼 AP와 통신해야 할 클라이언트에 암호화키를 기본으로 등록해 두고 있다. 암호화키를 이용해 128비트인 통신용 암호화키를 생성하고, 이 암호화키를 10,000개 패킷마다 바꾼다.

오답 체크 :

- (1) WEP : 1997년 제정된 802.11 표준에서 도입되었던 WEP는 전통적인 유선 네트워크와 비슷한 데이터 보안성을 제공하기 위해 만들어졌다. 64비트 또는 128비트 키값을 사용하는 WEP는, 한 때 매우 보편적으로 사용되었으며 라우터의 보안 설정에서 가장 우선적으로 표시되는 옵션이었다.

2001년 초, 암호학자들이 몇 가지 치명적인 취약점을 발견하였으며, 이를 이용하면 누구나 구할 수 있는 소프트웨어를 사용해 몇 십 분만에 WEP 연결을 크랙할 수 있다.

(2) TKIP : WEP의 취약성을 보완하기 위해 RC4 암호 알고리즘의 입력 키 길이를 128 비트로 늘리고 패킷당 키 할당, 키값 재설정 등 키 관리 방식을 개선하였다. 네트워크에 접근하는 사람을 제한할 수 있는 기능도 있다.

(4) EAP : EAP는 EAP 방식들이 만들어내는 키 요소와 매개변수의 전송 및 이용을 제공하기 위한 인증 프레임워크이다. RFC가 정의하는 방식들의 수는 많으며 수많은 업체에 특화된 방식들과 새로운 제안들이 존재한다. EAP는 유선 프로토콜이 아니며 단지 메시지 포맷을 정의하기만 할 뿐이다. EAP를 사용하는 개별 프로토콜은 프로토콜의 메시지 내의 EAP 메시지들을 캡슐화하는 방법을 정의한다. 예를 들면, EAP-TLS, EAP-MD5, EAP-PSK 등이 있다.

20. 컴퓨터 포렌식(forensics)은 정보처리기를 통하여 이루어지는 각종 행위에 대한 사실 관계를 확정하거나 증명하기 위해 행하는 각종 절차와 방법이라고 정의할 수 있다. 다음 중 컴퓨터 포렌식에 대한 설명으로 옳지 않은 것은?

① 컴퓨터 포렌식 중 네트워크 포렌식은 사용자가 웹상의 홈페이지를 방문하여 게시판 등에 글을 올리거나 읽는 것을 파악하고 필요한 증거물을 확보하는 것 등의 인터넷 응용프로토콜을 사용하는 분야에서 증거를 수집하는 포 렌식 분야이다.

② 컴퓨터 포렌식은 단순히 과학적인 컴퓨터 수사 방법 및 절차뿐만 아니라 법률, 제도 및 각종 기술 등을 포함하는 종합적인 분야라고 할 수 있다.

③ 컴퓨터 포렌식 처리 절차는 크게 증거 수집, 증거 분석, 증거 제출과 같은 단계들로 이루어진다.

④ 디스크 포렌식은 정보기기의 주·보조기억장치에 저장되어 있는 데이터 중에서 어떤 행위에 대한 증거 자료를 찾아서 분석한 보고서를 제출하는 절차와 방법을 말한다.

오답 체크 :

(1) 네트워크 : 해당 설명은 웹 포렌식이고, 네트워크로 전송되는 데이터를 대상으로 한다.

정답 체크 :

(2) 컴퓨터 : 컴퓨터 관련 조사·수사를 지원하며 디지털 데이터가 법적 효력을 갖도록 하는 과학적·논리적 절차와 방법을 연구하는 학문이다.

(3) 처리 절차 : 수행 절차는 수사 준비, 증거물 획득(증거 수집), 보관 및 이송, 분석 및 조사, 보고서 작성이다.

(4) 디스크 : 비휘발성 저장매체(HDD, SSD, USB, CD 등)를 대상으로 한다.