2015년 서울시 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
①	④	③	①	③	②	④	④	②	④
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
①	②	②	④	①	①	④	②	③	①

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.

답 ①

패스워드에 사용자의 특성을 포함시키면 공격자가 패스워드를 유추하기 한결 수월해지므로 위험하므로, 개인 신상과 관련된 정보는 포함하지 않도록 해야 한다. 은행에서 계좌 비밀번호를 설정할 때 생일이나 전화번호 등을 사용하지 못하게 하는 것도 같은 맥락이다.

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

> ㉠ '키'를 사용하여 '문서'를 암호화할 때
> ㉡ '문서'를 암·복호화하는 데 필요한 '키'를 암호화할 때
> ㉢ '키'를 사용하여 암호화된 '문서'를 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

답 ④

◈ 하이브리드 암호화 방식 순서
1. 문서를 암호화하기 위한 세션키를 생성한다.
   (세션키는 송신자와 수신자와 공통으로 사용할 공유키)
2. 생성한 세션키를 이용해 문서를 암호화한다.**(대칭키 방식)**
3. 세션키를 수신자의 공개키로 암호화한다.**(공개키 방식)**
4. 암호화한 문서와 세션키를 수신자에게 전송
5. 수신자는 자신의 개인키를 이용해 암호화된 세션키를 복호화한다.**(공개키 방식)**
6. 얻은 세션키를 이용해 암호화된 문서를 복호화해서 원본 문서를 얻을 수 있다.**(대칭키 방식)**

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

답 ③

대칭키 암호 시스템 키 개수 : $\frac{n(n-1)}{2}$
공개키 암호 시스템 키 개수 : $2n$

10명일 때, 대칭키 방식 (10 X 9) / 2 = 45개
공개키 방식 2 X 10 = 20개
20명일 때, 대칭키 방식 (20 X 19) / 2 = 190개
공개키 방식 2 X 20 = 40개
③ 따라서 대칭키는 145개, 공개키는 20개가 더 필요하다.

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 시그너처와 일치하면 침입으로 판단한다.
> ㉢ 제로데이 공격을 탐지하기에 적합하다.
> ㉣ 임계값을 설정하기 쉽기 때문에 오탐률이 낮다.

① ㉠, ㉢ ② ㉠, ㉣
③ ㉡, ㉢ ④ ㉡, ㉣

답 ①

<오답 체크> ㉡ 오용탐지
㉣ 적당한 임계값을 설정하기는 어려워 오탐률이 높다.

- **오용 탐지**(Misuse Detection)
  = 시그니처 기반(Signature Base)
  = 지식 기반(Knowledge Base)
  이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지
  오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능
  전문가 시스템(Expert System)의 지식 DB를 이용한 IDS
  Zero Day attack(제로 데이 공격)에 취약

- **이상 탐지**(Anomaly Detection IDS)
  = 행위 기반(Behavior)
  = 통계적 탐지(Statistical Detection)
  정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)
  알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능
  오탐율 높고, 임계치 설정이 어려움

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

① 향후 연결요청에 대한 피해 서버에서 대응 능력을 무력화시키는 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.

답 ③

▷ **SYN Flooding**
TCP 3-way hancshaking을 이용한 DoS공격
공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.
서버의 자원을 낭비시키고 가용성을 떨어뜨려 서비스 불능 상태에 빠뜨리는 것이 목적이다.

③ 동시에 수신할 수 있는 SYN 패킷의 수가 제한되어 있기 때문에 서버가 정상 패킷을 받을 공간이 부족하게 되는 것이다. 동시에 서버에 연결을 시도할 수 있는 클라이언트의 최대 수를 백로그 큐(BackLog Queue) 크기라고 하며, DoS 공격에 대비하기 위해선 백로그 큐를 늘려야 한다.

<오답 체크> ④ SYN flooding 공격은 작은 수의 패킷으로도 공격이 가능하다.

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

답 ②

▶ **강제적 접근 제어**(MAC, Mandatory Access Control)
오직 관리자만이 객체과 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안 레벨에 기반한다.
관리자가 규칙을 작성하기 때문에 **규칙 기반 접근 제어**(Rule Based Access Control)이라고도 한다.

<오답 체크> ① **래티스**(Lattice) 모델 = **격자기반 접근통제**(Lattice base access control)
- 격자 구조, 정보흐름을 안전하게 통제
- 최소상계와 최대하계를 갖는 유한적인 반순서
- 하한 값과 상한 값을 갖는 주체와 객체로 이루어진 쌍에서 주체는 가장 낮은 범위를 객체는 가장 높은 범위의 접근 권한을 갖는 방식

③ **역할 기반 접근 제어**(RBAC, Role Based Access Control)
정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델

④ **임의적 접근 제어**(DAC, Discretionary Access Control)
정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델

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 암. 복호화를 반복하는 라운드 함수의 수행 횟수이고, 10/12/14 라운드로 이루어져 있다.
③ 128비트 크기의 입·출력 블록을 사용하고, 128/192/256비트의 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(SubstitutionPermutation Network) 구조를 따른다.

답 ④

▷ **AES**(Advanced Encryption Standard)
SPN구조
블록 128비트(16바이트)
키 길이 128비트 – 10라운드
키 길이 192비트 – 12라운드
키 길이 256비트 – 14라운드

<오답 체크> ④ 입력을 좌우로 나누어 한 블록의 출력값을 다른 블록에 적용하는 방식은 페이스텔 구조에 대한 설명이다.
SPN 구조는 각 단계에서 바이트 치환(SubBytes), 행 이동(ShiftRows), 열 혼합(MixColumns), 키 덧셈(AddRoundKey)의 4단계를 거치는 방식이다.

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 트랜젝션을 보호하기 위해 인증, 기밀성 및 메시지 무결성 등의 서비스를 제공한다.

답 ④

▷ SET는 비자와 마스터가 함께 개발한 전자 상거래 거래 프로토콜이다.
RSA 암호화 방식과 인증을 지원. 선 압축 후 전자서명
④ 기밀성, 무결성, 인증, 부인 방지 등의 서비스를 제공한다.
<오답 체크> ① 인증서를 발급할 땐 당연히 신원을 확인한다.
② SET는 온라인 전자 상거래를 위한 시스템이다.
③ 소프트웨어를 필요로 한다.

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

① 커버로스는 개방형 분산 통신망에서 클라이언트와 서버간의 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.

답 ②

② 패스워드는 당연히 암호화된 상태로 전송되어야 한다.
<오답 체크> ④ 커버로스는 대칭키를 사용한다.
커버로스 버전4는 DES 알고리즘 사용
커버로스 버전5는 DES 이외의 다른 알고리즘도 사용

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.

답 ④

④ 메시지 인증 코드(**MAC**, Message Authentication Code)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(발신지에 대한 인증)이 가능하다. 출처 인증은 가능하지만, 부인방지는 불가능하다.
<오답 체크> ① 대부분의 해시 함수는 가변 길이의 입력을 받아, 고정 길이의 값을 출력한다.
② 해시함수는 입력값의 범위가 출력값의 범위보다 훨씬 넓기 때문에, 다른 입력이 같은 출력값을 가질 수 있는 다대일(n : 1) 대응 함수이다. 입력값이 다른데 출력값이 같은 경우를 충돌(collision)이라고 하며, 해시함수는 이 충돌을 피할 수 없다.
③ MAC는 대칭키를 사용하는 해시값이다.

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.

답 ①

◈ **허니팟**(honeypot)
비정상적인 접근을 탐지하기 위해 의도적으로 설치해 둔 시스템
컴퓨터에 중요한 정보가 있는 것처럼 꾸며 공격자가 해당 컴퓨터를 공격하도록 한 뒤, 이를 통해 취약점과 공격 방법, 공격자의 패턴 등을 탐지할 수 있다

① 공격자를 허니팟으로 침입하도록 유인하여야 한다. 침입을 방지하는 규칙이 적용되어 있으면, 공격자가 들어오지 못하므로 허니팟이 제 역할을 할 수 없다.

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

답 ②

② **중간자 개입**(Man-In-The-Middle, MITM) 공격은 연결하는 두 송수신자 사이에 중간자가 침입하여 한쪽에서 전달된 정보를 도청한 뒤 이를 다른 쪽에 전달하는 공격이다.
두 송수신자는 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며, 중간자는 해당 정보를 도청만 한 뒤 그대로 보낼 수도 있고, 조작하여 보낼 수도 있다.
디피 헬만 키 교환은 중간자 공격에 취약하다는 단점이 있다.

<오답 체크> ① 디피 헬만은 키를 교환하기 위한 알고리즘으로, 서버의 가용성을 침해하는 DoS와는 상관이 없다.
DoS(Denial of Service, 서비스 거부 공격)은 해당 시스템의 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격이다.
DDoS(Distributed DoS, 분산 서비스 거부 공격)은 다수의 시스템을 이용해 DoS 공격을 하는 것이다.
DRDoS(Distributed Reflect DoS, 분산 반사 서비스 거부 공격)은 패킷의 출발지 IP 주소를 공격 대상의 IP주소로 스푸핑한 TCP-SYN 패킷을 브로드캐스트로 다수의 시스템에 전송하여, 패킷을 받은 단말들이 보내는 응답 패킷을 공격대상으로 몰리게 만들어 공격 대상의 시스템 자원을 고갈시켜 서비스를 마비시키는 공격이다.

③ **세션 하이재킹**(Session Hijacking) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.

④ **강제지연**(Forced-Delay) 공격
공격자가 통신을 주고 받는 두 송수신자 사이에 개입하여, 그들이 보내는 통신 정보를 가로채 두었다가 일정 시간이 흐른 뒤 전송하는 공격이다.
강제지연 공격은 빠른 메시지 전송이 중요한 전자상거래 등 e-비즈니스 사업에 큰 손해를 끼칠 가능성이 있다.

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

① 네트워크 환경에서 보안 요구사항을 만족시키기 위해 공개키 암호화 인증서 사용을 가능하게 해 주는 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, 인증기관, 등록기관, 디렉터리(저장소), 사용자 등이 있다.

답 ②

② 암호화된 메시지를 송신할 때는 수신자의 공개키를 사용하고 암호화된 메시지를 수신할 때는 수신자의 개인키를 사용한다.
암호화된 서명 송신 시에는 송신자의 개인키를 사용하고, 암호화된 서명 수신 시에는 송신자의 공개키를 사용한다.

14. 블록 암호는 평문을 일정한 단위(블록)로 나누어서 각 단위마다 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.

답 ④

④ 통계적 분석에 관한 설명이다.
수학적 분석은 수학적 이론을 이용하여 해독하는 방법이다. 통계적 분석은 수학적 분석 방법 중 하나에 해당하지만, 가장 적절하지 못한 답을 골라야 하기 때문에 ④번이 답이 된다.

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

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

① 크로스사이트 요청 위조
② 크로스사이트 스크립팅
③ SQL 인젝션
④ 비트플리핑 공격

답 ①

① 크로스사이트 요청 위조(**CSRF**, Cross-site request forgery)
로그인 된 피해자의 취약한 웹 애플리케이션에 피해자의 세션 쿠키와 기타 다른 인증정보를 자동으로 포함하여 위조된 HTTP 요청을 강제로 보내도록 하는 것이다.

<오답 체크> ② 크로스사이트 스크립팅(**XSS**, Cross-site Scripting)
웹 사이트에 악성 스크립트를 삽입한 뒤, 다른 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.

③ **SQL 인젝션**(SQL injection, SQL 삽입)
클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격하는 것이다.

④ **비트 플리핑**(bit flipping)이란 메모리에 저장된 값이 0에서 1로, 또는 1에서 0으로 바뀌는 오류가 발생하는 현상을 말한다. 메모리 집적도가 높아지면서 메모리 각 데이터 영역들간 간섭 현상이 발생할 가능성이 높아지고, 이러한 비트 플리핑 오류가 발생할 가능성이 더욱 높아진다. 공격자가 이러한 비트 플리핑 오류를 의도적으로 조작 가능하면 메모리 내의 데이터 값을 조작하여 부적절한 작업을 수행하는 게 가능해지는데, 이를 **비트 플리핑 공격**(bit flipping attack)이라고 한다. 최근 DRAM에서 이러한 비트 플리핑 공격이 가능한 것이 이론적으로 증명되었다.

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

① 패킷 필터링 ② 데이터 암호화
③ 접근제어 ④ 터널링

답 ①

◈ 가상사설망(VPN, Virtual Private Network)은 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 데이터 암호화, 무결성, 접근 제어, 터널링, 인증 등의 보안 서비스를 제공한다.

① 패킷 필터링(packet filtering) 서비스를 제공하는 건 침입차단 시스템, 방화벽(Firewall)이다.

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 재사용할 수 있어야 한다.

답 ④

④ 한 문서에 대한 서명은 해당 문서에만 적용되어야 하며, 다른 문서에 재사용할 수 없어야 한다.
서명의 진짜 주인이라 할지라도 다른 문서에 서명을 할 때는 새로운 서명을 생성해야 한다.

◈ 전자서명의 특성
- 위조 불가(unforgeable)
- 서명자 인증(authentic)
- 부인 방지(non-repudiation)
- 변경 불가(unalterable)
- 재사용 불가(not reusable)

18. 다음 <보기>에서 설명하는 것은 무엇인가?

< 보 기 >
IP 데이터그램에서 제공하는 선택적 인증과 무결성, 기밀성 그리고 재전송 공격 방지 기능을 한다. 터널 종단 간에 협상된 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)

답 ②

② **ESP**(Encapsulating Security Payload, 캡슐화 보안 페이로드)
대칭키 암호화를 통해, 기밀성과 무결성과 선택적 인증 제공

<오답 체크> ① **AH**(Authentication Header, 인증 헤더)
메시지 인증과 무결성 제공

③ **MAC**(Message Authentication Code, 메시지 인증 코드)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(송신자에 대한 인증)이 가능하다.

④ **ISAKMP**(Internet Security Association and Key Management Protocol)
시스템 사이에 어느 암호화 알고리즘과 해시 알고리즘을 사용할지 협상하고 키를 만든다.

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

< 보 기 >

AP와 통신해야 할 클라이언트에 암호화키를 기본으로 등록해 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)

답 ③

③ **WPA** 방식: RC4-TKIP를 통한 암호화(암호키 주기적인 변경), EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
WPA2 방식: AES-CCMP 사용, EAP를 통한 사용자 인증

<오답 체크> ① **WEP** 방식: 암호화를 위해 RC4 사용하며(암호키 계속 사용), 암호화와 인증에 동일한 키를 사용

② **TKIP**(Temporal Key Integrity Protocol, 임시 키 무결성 프로토콜)
WPA와 WPA2에서 사용하는 키 관리 및 암호화 알고리즘 중 하나이다. RC4 키 스트림 암호화 알고리즘에 보안성을 강화하였다.
일반적으로 WPA는 TKIP를 사용하고, WPA2는 AES(CCMP)를 사용한다고 말하는데, WPA와 WPA2 모두 TKIP와 AES를 선택적으로 골라 사용할 수 있다.

④ **EAP**(Extensible Authentication Protocol, 확장 가능 인증 프로토콜)
복수의 인증 프로토콜을 캡슐화시킬 수 있게하여, 다양한 인증방식을 선택가능케하는 범용의 인증 프레임워크
WPA와 WPA2에서 인증을 위해 사용한다.

20. 컴퓨터 포렌식(forensics)은 정보처리기기를 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 포렌식 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 증거자료를 찾아서 분석한 보고서를 제출하는 절차와 방법을 말한다.

답 ①

① 웹상의 홈페이지나 사이트에서 증거물을 수집하는 건 웹 포렌식이다.
웹 포렌식(Web Forensics)은 과거에는 단순히 웹 브라우저 포렌식을 의미하였다.
인터넷 브라우저는 사용자가 인터넷의 정보를 이용하는데 편리한 기능을 제공하기 위해 많은 로그 정보를 사용하는데, 이러한 웹 브라우저의 로그 기록을 통해 증거를 수집하는 것을 **웹 브라우저 포렌식**(Web Browser Forensics)이라고 한다.
하지만 최근에는 브라우저 내 응용프로그램으로, 또는 브라우저와 연계하여 사용하는 다양한 독립된 응용프로그램 때문에, 웹 브라우저의 로그만을 가지고는 사용자의 인터넷 사용 흔적을 모두 분석하기 어려워졌다.
따라서 최근의 **웹 포렌식**은 웹 브라우저뿐 아니라 이러한 응용프로그램들이 남긴 로그 정보들까지 모두 분석하는 기술을 의미한다.
네트워크 포렌식(Network Forensics)은 네트워크에서 오고가는 패킷을 수집한 후 이를 저장·분석하는 장비를 통해 법적증거자료를 추출하는 과정을 말한다.

◈ 디지털 포렌식(Digital Forensics)
▷ 시스템 포렌식(System Forensics): 서버나 PC등을 대상으로 하는 디지털 포렌식 전반을 총칭

- ▷ 네트워크 포렌식(Network Forensics): 네트워크에서 오고가는 패킷을 수집한 후 이를 저장·분석하는 장비를 통해 법적증거자료를 추출하는 과정
- ▷ 모바일 포렌식(Mobile Forensics): 모바일기기에서 증거자료를 확보하고 분석하여 증거자료를 추출하는 과정
  모바일 포렌식은 시스템 포렌식의 하위범주로 볼 수도 있다.
- ▷ 디스크 포렌식(Disk Forensics): 하드디스크나 USB, 플래시 메모리 등 저장매체에서 삭제된 데이터를 찾아내어 법원에 증거자료로 제출하는 과정
- ▷ 웹 포렌식(Web Forensics): 웹 브라우저 및 그와 연동하여 사용하는 응용프로그램들이 남긴 로그 정보들을 토대로 인터넷 사용 기록을 분석하는 과정