

2017년 국회직 9급 정보보호론 풀이

by 호이호이꿀떡

1. 다음 중 정보 보안 시스템을 설계하거나 운영할 때의 목표로 옳지 않은 것은?

- ① 기밀성 보장
- ② 무결성 보장
- ③ 가용성 보장
- ④ 책임회피성 보장
- ⑤ 사용자 인증

답 ④

④ 책임회피성이 아니라, 책임추적성이다.

- 정보 보안 시스템의 목표
- 기밀성(confidentiality)
 - 무결성(integrity)
 - 가용성(availability)
 - 인증(authentication)
 - 인가(authorization)
 - 부인방지(Nonrepudiation)
 - 책임추적성(accountability)
 - 신뢰성(reliability)

2. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은?

- ① 공개된 채널을 통하여 서로 정보를 교환하는 것으로 공통의 비밀키를 만들어 낼 수 있다.
- ② 부인방지를 제공하는 전자서명이 가능하다.
- ③ 인수분해 문제에 기반한 알고리즘이다.
- ④ 중간자 공격을 수행하는 것이 불가능하다.
- ⑤ 키 생성 시 사용된 난수가 노출되어도 비밀키는 안전하다.

답 ①

- ① 디피 헬만 키 교환(Diffie-Hellman key exchange)은 두 송수신자 간 공통의 비밀키를 생성하기 위한 방법이다.
- ② 서로간의 비밀키를 생성하기 위한 알고리즘일 뿐, 그 자체로 암호화나 전자 서명이 되는 것은 아니다. 또한 비밀키로는 전자 서명을 할 수 없다.
- ③ 이산대수의 어려움에 기반한 알고리즘이다.
- ④ 통신 상대방을 인증하지 않기 때문에 중간자 공격에 취약하다.
- ⑤ 송수신자가 각자 생성한 난수는 절대 비밀로 유지해야 한다. 난수가 노출될 경우 비밀키를 알 수 있게 된다.

3. OWASP(The Open Web Application Security Project) 에서 2013 년에 발표한 10 대 웹 취약점에 속하지 않는 것은?

- ① 인젝션
- ② 크로스 사이트 요청 변조
- ③ 인증 및 세션 관리 취약점
- ④ 취약한 간접 객체 참조
- ⑤ 검증되지 않은 리다이렉트 및 포워드

답 ④

OWASP(Open Web Application Security Project) TOP 10 2013

- A1 인젝션(Injection)
- A2 인증 및 세션 관리 취약점
(Broken Authentication and Session Management)
- A3 크로스 사이트 스크립팅(XSS, Cross Site Scripting)
- A4 안전하지 않은 객체 참조
(Insecure Direct Object Reference)
- A5 보안상 잘못된 구성(Security Misconfiguration)
- A6 민감한 데이터 노출(Sensitive Data Exposure)
- A7 기능 수준 접근 통제 누락
(Missing Function Level Access Control)
- A8 크로스 사이트 요청 변조
(CSRF, Cross Site Request Forgery)
- A9 알려진 취약점이 있는 컴포넌트 사용
(Using Components with Known Vulnerabilities)
- A10 검증되지 않은 리다이렉트 및 포워드
(Unvalidated Redirects and Forwards)

4. 다음 중 TCP 세션 하이재킹에 대한 설명으로 옳은 것은?

- ① 서버와 클라이언트의 통신에서 TCP 의 송신 포트 제어에 문제가 발생하도록 공격한다.
- ② 서버와 클라이언트의 통신에서 TCP 의 ACK 넘버 제어에 문제가 발생하도록 공격한다.
- ③ 서버와 클라이언트의 통신에서 TCP 의 시퀀스 넘버 제어에 문제가 발생하도록 공격한다.
- ④ 서버와 클라이언트의 통신에서 TCP 의 수신 포트 제어에 문제가 발생하도록 공격한다.
- ⑤ 서버와 클라이언트의 통신에서 TCP 의 체크섬 제어에 문제가 발생하도록 공격한다.

답 ③

TCP 세션 하이재킹은 서버와 클라이언트가 통신할 때 TCP 프로토콜의 시퀀스 넘버를 제어하는 데 취약점이 있다는 것을 이용하는 공격이다.

TCP 세션 하이재킹 단계

1. 클라이언트와 서버는 동기화 연결된 상태로 Established 상태이며, 공격자는 적절한 시퀀스 넘버를 획득하기 위해 스니핑을 하고 있다.
2. 공격자는 세션이 완전히 끊기지 않는 시퀀스 넘버 범위 내에서 RST 패킷을 생성하여 서버에 전송한다. 서버는 잠시 Closed 상태가 되고, 클라이언트는 Established 상태가 지속된다.
3. 그 때 바로 공격자는 시퀀스 넘버를 조작한 SYN 패킷을 보낸다.
4. 서버로부터 SYN/ACK 패킷을 전송받아, 공격자와 서버가 연결되어 Established 상태가 된다.
5. 공격자는 공격 전 클라이언트 서버와 통신을 하던 시퀀스 넘버를 알고 있는 상태이므로 클라이언트와 정상적으로 통신을 하며, 서버와는 공격자가 새로 생성한 시퀀스 넘버를 가지고 통신을 한다.

5. <보기>는 XSS(Cross-site Scripting) 공격을 수행하기 위한 각 단계들을 나타낸다. ㄱ~ㅁ을 순서에 맞게 나열한 것으로 옳은 것은?

< 보 기 >

ㄱ. 사용자 시스템에서 XSS 코드가 실행된다.
 ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.
 ㄷ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.
 ㄹ. 결과가 공격자에게 전달된다.
 ㅁ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.

- ① ㄴ-ㄱ-ㄷ-ㄹ-ㅁ
- ② ㄴ-ㄱ-ㄹ-ㄷ-ㅁ
- ③ ㄴ-ㄷ-ㅁ-ㄱ-ㄹ
- ④ ㄷ-ㄴ-ㄱ-ㄹ-ㅁ
- ⑤ ㄷ-ㄴ-ㅁ-ㄱ-ㄹ

답 ⑤

- ㄷ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.
↓
- ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.
↓
- ㅁ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.
↓
- ㄱ. 사용자 시스템에서 XSS 코드가 실행된다.
↓
- ㄹ. 결과가 공격자에게 전달된다.

6. ECC(Elliptic Curve Cryptography) 암호시스템에 대한 설명으로 옳지 않은 것은?

- ① 타원곡선 상의 이산대수 문제에 기반을 둔다.
- ② 키 교환, 암호화, 전자서명에 모두 사용 가능하다.
- ③ RSA 보다 짧은 공개키를 이용하여 비슷한 수준의 보안레벨을 제공한다.
- ④ 임베디드 플랫폼 등과 같은 경량 응용분야에는 적합하지 않다.
- ⑤ 비슷한 수준의 보안레벨에서는 RSA 보다 전자서명 생성 속도가 빠르다.

답 ④

타원 곡선 암호(ECC)에 타원 곡선 상의 이산대수 문제에 기반한 공개키 암호화 알고리즘이다.
 암호화 키 길이가 길고 시간이 오래 걸리는 RSA 의 대안으로 나온 것으로, 동일한 보안 수준에서 RSA 보다 키의 길이가 짧고 빠르다.
 ④ 짧은 키의 길이와 빠른 속도의 이점 덕분에, 자원이 넉넉지 않은 전자상거래나 무선 통신 등의 경량 프로세스 분야에 적합하다.

7. <보기>에서 설명하는 해시함수(H)의 특성으로 옳은 것은?

< 보 기 >

주어진 메시지 x 에 대해, $H(x) \neq H(y)$ 인 $x \neq y$ 를 만족하는 두 개의 메시지 x, y 를 찾는 것이 어려울 때, 해시함수가 이 성질을 가지고 있다고 한다.

- ① Second Pre-image Resistance
- ② Collision Resistance
- ③ Integrity
- ④ Onewayness
- ⑤ Uniform Distribution

답 ①

(국회직답게 일부러 다른 기출문제에 쓰이지 않았던 용어로, 그것도 영어로 문제를 출제했다)

해시 함수의 특성이라 하면, 아래의 세 가지 특성을 생각한다.

- 일방향성(one-wayness)
역산할 수 없다. 해시값으로부터 원본 메시지를 찾을 수 없다.
- 약한 충돌 내성(weak collision resistance)
주어진 해시값과 같은 해시값을 갖는 다른 메시지를 찾을 수 없다.
- 강한 충돌 내성(strong collision resistance)
출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없다.

여기에서 일방향성을 제 1 역상 저항성(first preimage resistance)이라 하고 약한 충돌내성을 제 2 역상 저항성(second preimage resistance)이라 한다.

- ① Second Pre-image Resistance (제 2 역상 저항성)
문제에서 x 가 주어져 있고, x 의 해시값과 같은 해시값을 갖는 y 를 찾기가 어렵다고 했으므로, 약한 충돌내성 또는 제 2 역상 저항성이 된다.
- ② Collision Resistance(충돌 저항성)
그냥 충돌 저항성을 말하면, 강한 충돌 저항성(내성)을 의미한다.
- ③ Integrity(무결성)
허가받지 않은 사용자에게 의해 데이터가 위·변조 되지 않아야 한다.
- ④ Onewayness(일방향성)
= 제 1 역상 저항성(first preimage resistance)
- ⑤ Uniform Distribution(균등 분포)
주어진 범위 내에서 각 결과가 나올 확률이 동일한 확률 분포를 균등 분포라고 한다.
해시의 결과값이 균등하게 분포되지 않고, 특정한 값에 몰린다면 충돌이 발생할 가능성이 높아진다.

8. 시스템 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM 이 지원하지 않는 기능은?

- ① 암호키 생성 및 저장
- ② 인증된 부트(Authenticated Boot)
- ③ 디바이스 및 플랫폼 인증
- ④ 원격 검증(Remote Attestation)
- ⑤ 감사(Audit)

답 ⑤

TPM(Trusted Platform Module, 신뢰할 수 있는 플랫폼 모듈)은 암호화 키를 포함하여 외부의 공격이나 내부의 다른 요인에 의해 변경이나 손상되는 것을 방지하는 등의 보안관련 기능을 제공하는 기술이다.

TPM 을 통해 암호화를 할 경우, 하드 디스크 자체가 암호화되기 때문에 디스크를 떼어내 다른 PC 에 연결하더라도 데이터를 볼 수 없다.

TPM 의 기능

인증된 부트(authenticated boot)

전체 운영체제를 단계적으로 부팅하면서 각 단계별로 인증된 부분인지 확인하는 과정

인증(certification)

운영체제 뿐 아니라, 다른 장치나 플랫폼에 대한 인증을 제공

암호화(encryption)

암호화 키를 생성하고, 데이터의 암호화 및 복호화 실행 여기에 추가적으로 원격 검증 기능도 가능하다.

9. 네트워크에서 서비스를 제공하는 서버 혹은 시스템은 동시 접속할 수 있는 사용자 수를 제한한다. 이러한 특성을 이용하여 다수의 존재하지 않는 사용자가 시스템에 접속한 것처럼 속여 다른 사용자가 서비스를 받지 못하게 하는 공격으로 옳은 것은?

- ① Ping of Death
- ② SYN Flooding
- ③ Boink
- ④ TearDrop
- ⑤ Smurf

답 ②

② SYN Flooding 에 대한 설명이다.

TCP 3-wayhandshaking 을 이용한 DoS 공격으로, 공격 대상 서버에 무수히 많은 SYN 패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK 패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격이다.

공격자가 보내는 수많은 SYN 패킷들에 대해 서버는 실제 존재하는 사용자가 보낸 것으로 착각하기 때문에 차단하지 않고 Received 상태로 기다리는 것이다.

① Ping of Death 은 icmp 패킷을 정보보다 매우 크게 만들어 공격하는 DoS 공격이다. 크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)화 되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

③④ Teardrop, Bonk, Boink 공격은 신뢰성을 제공하는 프로토콜의 취약점을 이용한 DoS 공격으로, 패킷의 순서번호를 조작하는 공격이다.

목표 대상 시스템은 이렇게 보내진 패킷들을 재조합하려고 시도하지만, 계속 실패하여 시스템 자원이 고갈되어 서비스 불능 상태에 빠진다.

• Teardrop 공격은 UDP 를 이용하여 패킷의 순서번호가 서로 중복되도록 조작하는 공격

• Bonk 공격은 패킷의 순서번호를 모두 1 로 조작하여 보내는 공격

• Boink 공격은 패킷의 순서번호를 처음에는 순서대로 보내다가 중간부터 반복되는 순서번호를 보내는 공격이다.

⑤ Smurf 공격은 ICMP flooding 이라 하며, 공격대상 호스트의 IP 주소로 위장된 소스 IP 주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상은 많은 양의 ICMP Echo 응답 패킷을 받아 시스템의 자원을 고갈된다.

10. 메시지 인증 코드(MAC: Message Authentication Code)에 대한 설명으로 옳지 않은 것은?

- ① MAC 검증을 통하여 메시지의 위조 여부를 판별할 수 있다.
- ② MAC 을 이용하여 송신자 인증이 가능하다.
- ③ MAC 검증을 위해서는 메시지와 공개키가 필요하다.
- ④ 해시함수를 이용하여 MAC 을 생성할 수 있다.
- ⑤ MAC 생성자와 검증자는 동일한 키를 사용한다.

답 ③

메시지 인증 코드(MAC: Message Authentication Code)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(송신자에 대한 인증)이 가능하다. 출처 인증은 가능하지만, 부인 방지는 불가능하다.

③ MAC 는 대칭키를 사용하므로, MAC 생성이나 검증 모두 대칭키(비밀키)를 사용한다.
선지를 잘 보면, ③과 ⑤이 반대되는 내용이다.

② 송신자 인증과 부인 방지는 다른 것이다.
부인 방지는 제 3 자에게 누가 어떤 내용의 메시지를 보냈는지, 메시지의 전송 및 수신에 대한 사실 확인이 가능한 것을 의미하고,
송신자 인증은 통신 당사자간 상대방의 신원을 확인할 수 있는 것을 의미한다. MAC 는 대칭키를 사용하기 때문에 네트워크 상의 상대방이 자신과 같은 비밀키를 가진 특정한이라는 걸 확인할 수 있다.

11. 수동적 보안 공격에 해당하는 것을 <보기>에서 모두 고르면?

< 보 기 >	
ㄱ. 신분 위장	ㄴ. 메시지 변경
ㄷ. 도청	ㄹ. 트래픽 분석
ㅁ. 서비스 거부	

- ① ㄱ, ㄴ
- ② ㄴ, ㄹ
- ③ ㄷ, ㄹ
- ④ ㄱ, ㄷ, ㄹ
- ⑤ ㄷ, ㄹ, ㅁ

답 ③

소극적 공격(수동적 공격)
도청(가로채기, interception)
트래픽 분석(traffic analysis)
메시지 내용 공개(release of message contents) 등
적극적 공격(능동적 공격)
차단(interruption)
변조(modification)
위조(fabrication)
신분 위장(masquerade)
서비스 거부 공격(Dos)
재전송 공격(replay attack) 등

12. 디지털 포렌식(Digital Forensic)을 통해 획득된 증거가 법적인 효력을 갖기 위해서는 증거를 발견(Discovery), 기록(Recording), 획득(Collection), 보관(Preservation)하는 절차가 적절해야 한다. 이를 만족하기 위해 지켜야 하는 기본 원칙으로 옳지 않은 것은?

- ① 최량 증거의 원칙
- ② 재현의 원칙
- ③ 정당성의 원칙
- ④ 신속성의 원칙
- ⑤ 연계보관성의 원칙

답 ①

① 최량 증거의 원칙(最良證據原則, Best evidence rule)이란 녹취나 서면증거를 채택할 때 최량(가장 적합한)의 증거, 보통 원본을 우선 채택하며, 구두진술은 원본이 더 이상 존재하지 않을 때 채택한다는 원칙이다.

하지만 디지털 증거에 있어서는 원본은 가상의 2진수 데이터이므로, 증이에 인쇄한 출력물 역시 원본으로 인정하기 때문에 최량 증거의 원칙이 적용되지 않는다.

포렌식의 원칙

- 재현의 원칙: 증거를 복구하는 과정에서 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함
- 정당성의 원칙: 모든 증거는 적법한 절차를 거쳐서 획득하여야 함
- 신속성의 원칙: 시스템 안의 디스크 또는 메모리 정보가 휘발되기 전에 빠르게 획득하여야 함
- 연계보관성의 원칙: 증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 함
- 무결성의 원칙: 증거가 위조/변조되어서는 안 됨

13. 와이파이(Wi-Fi) 보안 기술에 대한 설명으로 옳지 않은 것은?

- ① IEEE 802.11 표준 기반의 무선 랜 기술이다.
- ② WEP 방식은 현재 보안상 취약점이 발견되었다.
- ③ WEP 방식은 MAC(Media Access Control) 주소 인증 프로토콜을 사용한다.
- ④ WPA 방식은 TKIP(Temporal Key Integrity Protocol)를 사용한다.
- ⑤ WPA2 방식은 AES-CCMP(Counter Mode CBC-MAC Protocol)를 사용한다.

답 ③

③ WEP 방식은 공유키(PSK, Pre-shared Key) 인증 방식을 사용한다.

MAC 주소 인증이란, 공유기에 자주 사용하는 기기의 MAC 주소 테이블을 구성한 뒤, 저장된 MAC 주소로 접속할 때만 인터넷 연결이 되게 하는 방법이다.

WEP 방식: 암호화를 위해 RC4 사용하며(암호키 계속 사용), 암호화와 인증에 동일한 키를 사용

WPA 방식: RC4-TKIP 를 통한 암호화(암호키 주기적인 변경), EAP 를 통한 사용자 인증

WPA2 방식: AES-CCMP 사용, EAP 를 통한 사용자 인증

14. 접근 제어 모델에 대한 설명으로 옳지 않은 것은?

- ① DAC(Discretionary Access Control)는 정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.
- ② MAC(Mandatory Access Control)는 사용자 계정에 기반하며, 자원의 소유자가 다른 사용자의 보안 레벨을 수정할 수 있다.
- ③ BLP(Bell-LaPadula) 모델은 자신보다 높은 보안 레벨의 문서에 쓰기는 가능하지만, 보안 레벨이 낮은 문서에는 쓰기 권한이 없다.
- ④ BLP의 보안 목적은 기밀성이지만, Biba 모델은 정보의 무결성을 높이는 데 있다.
- ⑤ RBAC(Role Based Access Control)는 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

답 ②

- ② DAC(임의적 접근 제어)에 대한 설명이다.
MAC(강제적 접근 제어)는 오직 관리자만이 객체와 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안레벨에 기반한다.
- ③ BLP(벨 라파둘라) 모델은 기밀성을 중시한 모델
높은 보안수준의 문서 내용이 낮은 보안수준으로 흐르는 걸 방지하는 데 중점을 둔다.
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성(Simple security property, ss-속성) – NRU(No Read Up) 높은 등급의 데이터를 읽을 수 없다.
*-속성(Star property) – NWD(No Write Down) 낮은 등급의 데이터에 쓸 수 없다.
- ④ Biba(비바) 모델은 무결성을 중시한 모델
높은 보안수준의 문서 내용이 원하지 않는 방향으로 변경되는 것을 방지하는 데 중점을 둔다.
높은 등급의 데이터에 쓸 수 없고, 낮은 등급의 데이터를 읽을 수 없다.
단순 무결성 속성(Simple integrity property, si-속성): NRD(No Read Down), 낮은 등급의 데이터를 읽을 수 없다.
무결성 *-속성(integrity star property): NWD(No Write Up), 높은 등급의 데이터에 쓸 수 없다.

15. <보기>에서 설명하는 블록암호 운영모드로 옳은 것은?

- ‘한 단계 앞의 암호 알고리즘의 출력을 암호화한 값’과 ‘평문 블록’을 XOR 연산하여 암호문 블록을 생성하는 운영모드이다.
- 암호화와 복호화가 같은 구조를 가지고 있다.
- 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트에만 에러가 발생한다.

- ① ECB
- ② CBC
- ③ CFB
- ④ OFB
- ⑤ CTR

답 ④

- ‘한 단계 앞의 암호 알고리즘의 출력을 암호화한 값’과 ‘평문 블록’을 XOR 연산 -> 이 부분은 CFB 와 OFB 가 모두 가능한데,
암호화와 복호화가 같은 구조 -> 이걸 OFB와 CTR에 해당하는 설명이다.
- ① ECB(Electronic CodeBook, 전자 코드북 모드)
각 블록 단위로 별도로 암호화
병행 처리 가능, 에러의 전파 없다.
- ② CBC(Cipher Block Chaining, 암호 블록 연쇄 모드)
평문 블록을 이전 단계의 암호문 블록과 XOR 한 뒤, 암호화한다.
- ③ CFB(Cipher FeedBack, 암호 피드백 모드)
이전 단계의 암호문 블록을 암호화한 것을 평문 블록과 XOR 한다.
- ④ OFB(Output FeedBack, 출력 피드백 모드)
초기화 벡터(IV)를 계속 암호화해 나가면서, 평문 블록과 XOR 한다.
전 단계의 암호 알고리즘의 출력을 이번 단계의 암호 알고리즘의 입력으로 사용한다.
암호화와 복호화가 같은 구조
에러의 전파가 없다.
- ⑤ CTR(Counter mode, 카운터 모드)
1 씩 증가하는 카운터를 계속 암호화해 나가면서, 평문 블록과 XOR 한다.
카운터 값을 1 씩 증가하면서 암호화를 하여 키 스트림을 만드는 스트림 암호이다.
각 단계별로 연관성이 없어 병행 처리가 가능
암호화와 복호화가 같은 구조
에러의 전파가 없다.

18. 다음 중 버퍼 오버플로우(Buffer Overflow)에 취약한 C 언어 함수 로 옳지 않은 것은?

- ① int scanf (const char *format, ...);
- ② char *gets (char *buf);
- ③ int strcmp (const char *str1, const char *str2);
- ④ char *realpath (const char *path, char *resolved_path);
- ⑤ char *strcat (char *dest, const char *src);

답 ③

버퍼 오버플로우 공격에 취약한 함수

strcpy(), strcat(), gets(), getwd(), scanf(), fscanf(), sscanf(), vsprintf(), vsscanf(), realpath(), sprintf(), vsprintf(), gethostbyname() 등

버퍼 오버플로우 공격에 안전한 함수

strncpy(), strncat(), fgets(), fscanf(), vfscanf(), snprintf(), vsnprintf() 등

- ③ strcmp(str1, str2) 함수는 두 문자열 str1 과 str2 를 비교하여, 같으면 0 을, str1 이 더 크면 양수를, str2 가 더 크면 음수를 반환한다.

19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자가 이용자의 개인정보를 제 3 자에게 제공하는 경우, 이용자에게 알리고 동의를 받아야 하는 내용으로 옳지 않은 것은?

- ① 개인정보를 제공 받는 자
- ② 제공하는 개인정보의 항목
- ③ 개인정보를 제공 받는 자의 개인정보 이용 목적
- ④ 개인정보를 제공 받는 자의 개인정보 보호책임자
- ⑤ 개인정보를 제공 받는 자의 개인정보 보유 및 이용기간

답 ④

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제 24 조의 2(개인정보의 제공 동의 등)

① 정보통신서비스 제공자는 이용자의 개인정보를 제 3 자에게 제공하려면 제 22 조제 2 항제 2 호 및 제 3 호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

- 1. 개인정보를 제공받는 자
- 2. 개인정보를 제공받는 자의 개인정보 이용 목적
- 3. 제공하는 개인정보의 항목
- 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

② 제 1 항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제 3 자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

③ 제 25 조제 1 항에 따른 정보통신서비스 제공자 등은 제 1 항에 따른 제공에 대한 동의와 제 25 조제 1 항에 따른 개인정보 처리위탁에 대한 동의를 받을 때에는 제 22 조에 따른 개인정보의 수집·이용에 대한 동의와 구분하여 받아야 하고, 이에 동의하지 아니한다는 이유로 서비스 제공을 거부하여서는 아니 된다.

20. <보기>에서 설명하는 SSL 프로토콜로 옳은 것은?

< 보 기 >

이 프로토콜을 이용하여 서버와 클라이언트가 서로를 인증하고, 암호와 MAC 알고리즘, 그리고 SSL 레코드 안에 보낼 데이터를 보호하는 데 사용할 암호키를 협상할 수 있다.

- ① Alert Protocol
- ② Handshake Protocol
- ③ Record Protocol
- ④ Change Cipher Spec Protocol
- ⑤ Encapsulating Security Payload Protocol

답 ②

SSL/TLS 구조

- 핸드셰이크 프로토콜(handshake protocol)
 - 서버와 클라이언트가 서로를 인증하고 암호, MAC 알고리즘 레코드 데이터 보호에 사용될 암호화 키를 협상
 - 암호 사양 변경 프로토콜(change cipher spec protocol)
 - 핸드셰이크 프로토콜의 일부로 암호 방법을 변경
 - 경고 프로토콜(alert protocol)
 - 에러 코드를 전송
 - 애플리케이션 데이터 프로토콜(application data protocol)
 - HTTP 를 포함한 다양한 상위계층의 보안 서비스 제공
 - 레코드 프로토콜(record protocol)
 - SSL 의 실제 데이터를 다루며, Data 를 단편화 및 압축하고 MAC 을 적용하고 암호화하여 이를 TCP 에 전달
- ⑤ ESP(Encapsulating Security Payload Protocol)은 IPSec 에서 사용하는 프로토콜로, 암호화를 통하여 기밀성과 무결성, 선택적 인증 기능을 제공한다.