2017-국회직-정보보호론-가형-해설-곽후근

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
정답 체크 :
(4) 책임회피성이 존재하지 않고 책임추적성(사용자 식별 및 활동 감사 추적)을 목표로 해야한다.
오답 체크 :
(1) 기밀성 : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.
(2) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(3) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.
(5) 인증 : 사용자 인증(시스템 접근 통제)과 데이터 출처 인증(MAC)이 있다.
Tip! : 이외에도 부인 방지(송신부인방지와 수신부인방지)를 목표로 해야 한다.

2. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은?
① 공개된 채널을 통하여 서로 정보를 교환하는 것만으로 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.
정답 체크 :
(1) 공개된 채널을 통하여 서로가 가진 난수를 포함한 정보를 교환하는 것만으로 공통의 비밀키를 만들어 낼 수 있다.
오답 체크 :
(2) 전자서명을 하려면 공개키와 개인키가 있어야 하는데, Diffie-Hellman은 난수 관련 정보를 서로 교환해서 비밀키를 만들어내지만 공개키가 따로 존재하지는 않는다.
(3) 이산대수 문제에 기반한 알고리즘이다.
(4) 중간자 공격을 수행하는 것이 가능하다.
(5) 난수가 노출되면 비밀키가 안전하지 않다.

3. OWASP(The Open Web Application Security Project)에서 2013년에 발표한 10대 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
정답 체크
(4) 취약한 간접 객체 참조 : 취약한 직접 객체 참조이고 2013년 top 10 중 4위이다.
오답 체크 :
(1) 인젝션 : 2013년 top 10 중 1위이다.
(2) 크로스 사이트 요청 위조 : 2013년 top 10 중 8위이다.
(3) 인증 및 세션 관리 취약점 : 2013년 top 10 중 2위이다.
(5) 검증되지 않은 리다이렉트 및 포워드 : 2013년 top 10 중 10위이다.
Tip! : 2013년 OWASP top 10을 테이블로 정리하면 다음과 같다.

A1 - 인젝션	SQL, 운영체제, LDAP 인젝션 취약점은 신뢰할 수 없는 데이터가 명령어나 질의문의 일부분으로서 인터프리터로 보내질 때 발생한다. 공격자의 악의적인 데이터는 예상하지 못하는 명령을 실행하거나 적절한 권한 없이 데이터에 접근하도록 인터프리터를 속일 수 있다.
A2 - 인증 및 세션 관리 취약점	인증과 세션 관리와 관련된 애플리케이션 기능은 정확하게 구현되어 있지 않아서, 공격자가 패스워드, 키 또는 세션 토큰을 해킹하거나 다른 구현 취약점을 공격하여 다른 사용자 ID로 가장할 수 있다.
A3 - 크로스 사이트 스크립팅 (XSS)	XSS 취약점은 애플리케이션이 신뢰할 수 없는 데이터를 가져와 적절한 검증이나 제한 없이 웹 브라우저로 보낼 때 발생한다. XSS는 공격자가 피해자의 브라우저에 스크립트를 실행하여 사용자 세션 탈취, 웹 사이트 변조, 악의적인 사이트로 이동할 수 있다.
A4 - 취약한 직접 객체 참조	직접 객체 참조는 개발자가 파일, 디렉토리, 데이터베이스 키와 같은 내부 구현 객체를 참조하는 것을 노출시킬 때 발생한다. 접근 통제를 통한 확인이나 다른 보호수단이 없다면, 공격자는 노출된 참조를 조작하여 허가 받지 않은 데이터에 접근할 수 있다.
A5 - 보안 설정 오류	훌륭한 보안은 애플리케이션, 프레임워크, 애플리케이션 서버, 웹 서버, 데이터베이스 서버 및 플랫폼에 대해 보안 설정이 정의되고 적용되어 있다. 기본으로 제공되는 값은 종종 안전하지 않기 때문에 보안 설정은 정의, 구현 및 유지되어야 한다. 또한 소프트웨어는 최신의 상태로 유지해야 한다.
A6 - 민감 데이터 노출	많은 웹 애플리케이션들이 신용카드, 개인 식별 정보 및 인증 정보와 같은 중요한 데이터를 제대로 보호하지 않는다. 공격자는 신용카드 사기, 신분 도용 또는 다른 범죄를 수행하는 등 약하게 보호된 데이터를 훔치거나 변경할 수 있다. 중요 데이터가 저장 또는 전송 중이거나 브라우저와 교환하는 경우 특별히 주의하여야 하며, 암호화와 같은 보호조치를 취해야 한다.
A7 - 기능 수준의 접근통제 누락	대부분의 웹 애플리케이션은 UI에 해당 기능을 보이게 하기 전에 기능 수준의 접근권한을 확인한다. 그러나, 애플리케이션은 각 기능에 접근하는 서버에 동일한 접근통제 검사를 수행한다. 요청에 대해 적절히 확인하지 않을 경우 공격자는 적절한 권한 없이 기능에 접근하기 위한 요청을 위조할 수 있다.
A8 - 크로스 사이트 요청 변조(CSRF)	CSRF 공격은 로그온 된 피해자의 취약한 웹 애플리케이션에 피해자의 세션 쿠키와 기타 다른 인증정보를 자동으로 포함하여 위조된 HTTP 요청을 강제로 보내도록 하는 것이다. 이것은 공격자가 취약한 애플리케이션이 피해자로부터의 정당한 요청이라고 오해할 수 있는 요청들을 강제로 만들 수 있다.
A9 - 알려진 취약점이 있는 컴포넌트 사용	컴포넌트, 라이브러리, 프레임워크 및 다른 소프트웨어 모듈은 대부분 항상 전체 권한으로 실행된다. 이러한 취약한 컴포넌트를 악용하여 공격하는 경우 심각한 데이터 손실이 발생하거나 서버가 장악된다. 알려진 취약점이 있는 컴포넌트를 사용하는 애플리케이션은 애플리케이션 방어 체계를 손상하거나, 공격 가능한 범위를 활성화하는 등의 영향을 미친

	다.
A10 - 검증되지 않은 리다이렉트 및 포워드	웹 애플리케이션은 종종 사용자들을 다른 페이지로 리다이렉트 하거나 포워드하고, 대상 페이지를 결정하기 위해 신뢰할 수 없는 데이터를 사용한다. 적절한 검증 절차가 없으면 공격자는 피해자를 피싱 또는 악성코드 사이트로 리다이렉트 하거나 승인되지 않은 페이지에 접근하도록 전달할 수 있다.

4. 다음 중 TCP 세션하이재킹에 대한 설명으로 옳은 것은?

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

정답 체크 :

(3)

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, TCP 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식이다.

- 클라이언트와 서버 사이의 패킷을 통제. ARP 스푸핑 등을 통해 클라이언트와 서버 사이의 통신 패킷이 모두 공격자를 지나가게 하도록 하면 된다.
- 서버에 클라이언트 주소로 연결을 재설정하기 위한 RST(Reset) 패킷을 보냄. 서버는 해당 패킷을 받고, 클라이언트의 시퀀스 넘버가 재설정된 것으로 판단하고, 다시 TCP 쓰리웨이 핸드셰이킹을 수행한다.
- 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받는다.

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-ㅁ - ㄹ
⑤ ㄷ-ㄴ-ㅁ-ㄱ-ㄹ

정답 체크 :

(5)

해당 설명은 저장 XSS 공격에 해당한다.

(ㄷ) 공격자가 XSS 코드를 웹 서버에 저장한다. 이와 같이 XSS 코드를 저장하기 때문에 저장 XSS 공격이다.
(ㄴ) 웹 사용자가 XSS 코드에 접근한다.
(ㅁ) XSS 코드가 웹 서버에서 사용자에게 전달된다.
(ㄱ) 사용사 시스템에서 XSS 코드가 실행된다.
(ㄹ) 결과(사용자의 쿠키)가 공격자에게 전달된다.

6. ECC(Elliptic Curve Cryptography) 암호시스템에 대한 설명으로 옳지 않은 것은?
① 타원곡선상의 이산대수 문제에 기반을 둔다.
② 키 교환, 암호화, 전자서명에 모두 사용 가능 하다.
③ RSA 보다 짧은 공개키를 이용하여 비슷한 수준의 보안 레벨을 제공한다.
④ 임베디드 플랫폼 등과 같은 경량 응용 분야에는 적합하지 않다.
⑤ 비슷한 수준의 보안 레벨에서는 RSA 보다 전자서명 생성 속도가 빠르다.
정답 체크 :
(4) RSA보다 더 짧은 키를 사용하기 때문에 임베디드 플랫폼 등과 같은 경량 응용분야에 적합하다.
오답 체크 :
(1) 타원곡선 상의 이산대수 문제에 기반한다.
(2) 키 교환(ECC), 암호화(ECC), 전자서명(ECDSA)에 사용할 수 있다.
(3) 예를 들어, RSA가 1024비트가 필요하면 ECC는 160비트가 필요하다.
(5) 비슷한 수준의 보안레벨에서 ECC의 키가 더 짧기 때문에 전자서명 생성 속도가 RSA에 비해 빠르다.

7. 〈보기〉에서 설명하는 해시함수(H)의 특성으로 옳은 것은?

〈 보 기 〉
주어진 메시지 x에 대해, H(x) = H(y)인 x ≠ y를 만족하는 두 개의 메시지 x, y를 찾는 것이 어려울 때, 해시 함수가 이 성질을 가지고 있다고 한다.

① Second Pre-image Resistance
② Collision Resistance
③ Integrity
④ Onewayness
⑤ Uniform Distribution
정답 체크 :
(1) Second Pre-image Resistance : 메시지가 주어졌을 때, 해시값이 일치하는 다른 메시지를 찾는 것이다. Pre-image Resistance는 해시값에 해당하는 동일 메시지를 찾는 것이다. 약한 충돌 내성(어느 메시지의 해시 값이 주어졌을 때, 그 해시 값과 같은 해시 값을 갖는 다른 메시지를 발견해 내는 것이 매우 곤란한 성질)과 같은 의미이다.
오답 체크 :
(2) Collision Resistance(충돌 내성) : 강한 충돌 내성(해시 값이 일치할 것 같은, 다른 2개의 메시지를 발견해 내는 것이 매우 곤란한 성질)을 의미한다.
(3) Integrity(무결성) : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.

(4) Onewayness(일방향성) : 메시지에 대한 해시값을 구할 수 있지만, 해시값에 대한 메시지를 구할 수는 없다.
(5) Uniform Distribution(연속균등분포) : 확률 이론에서 확률에 참여하는 모든 멤버가 모두 같은 확률을 가지는 분포를 의미한다.

8. 시스템 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM이 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)
정답 체크 :
(5) 감사 : TPM은 감사를 위해 로그를 남기는 모듈이 아니다. 또한 로그를 위한 공간도 존재하지 않는다.
오답 체크 :
(1) 암호키 생성 및 저장 : random number generator과 RSA key generator를 이용해서 암호키를 생성하고 storage keys에 암호키를 저장할 수 있다.
(2) 인증된 부트 : 개인용 컴퓨터(PC) 주기판에 부착되며, 부팅 단계에서부터 시스템의 무결성 검증에 이용된다.
(3) 디바이스 및 플랫폼 인증 : TPM은 디바이스 및 플랫폼에 부착되는 고유한(Unique) 보안 모듈이므로 이를 이용하여 디바이스 및 플랫폼을 인증할 수 있다.
(4) 원격 검증 : PCR과 AIK를 이용해서 TPM이 있는 플랫폼을 원격으로 검증할 수 있다.

9. 네트워크에서 서비스를 제공하는 서버 혹은 시스템은 동시 접속 할 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 Tear Drop
⑤ Smurf
정답 체크 :
(2) SYN Flooding : 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.
오답 체크 :
(1) Ping of Death : 네트워크에서는 패킷을 전송하기 적당한 크기로 잘라서 보내는데, Ping of Death는 네트워크의 이런 특성을 이용한 것이다. 네트워크의 연결 상태를 점검하기 위한 ping 명령을 보낼 때, 패킷을 최대한 길게 하여(최대 65,500바이트) 공격 대상에게 보내면 패킷은 네트워크에

서 수백 개의 패킷으로 잘게 쪼개져 보내진다(DoS 공격).
(3) Boink : 처음에는 정상적인 순서의 단편을 보내다가 점검 순서번호가 어긋난 패킷을 보내는 방법으로, Bonk(순서번호가 1번인 단편을 계속 보내는 공격)보다 개선된 방식의 공격이다.
(4) TearDrop : 데이터의 송수신과정에서 데이터의 송신한계를 넘으면 MTU(1500byte) 조각으로 나누어 fragment number를 붙여 송신하고, 수신측에는 fragment 넘버로 재조합하여 분석한다. fragment 내의 나누어진 byte 정보인 fragmentation offset을 위조하여 offset을 중복되게 하거나 공간을 두면 수신측에서 재조합이 안 되어 다운이 되게 하는 공격이다.
(5) Smurf : 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.

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 MAC을 이용하여 송신자 인증이 가능하다.
③ MAC 검증을 위해서는 메시지와 공개키가 필요하다.
④ 해시 함수를 이용하여 MAC을 생성할 수 있다.
⑤ MAC 생성자와 검증자는 동일한 키를 사용한다.
정답 체크 :
(3) MAC을 검증하기 위해서는 메시지와 비밀키가 필요하다.
오답 체크 :
(1) MAC에 해시를 사용한다면 해시값를 통해 무결성을 확인할 수 있다.
(2) MAC에 사용하는 비밀키를 통해 인증을 수행할 수 있다.
(4) 해시 함수를 이용한 HMAC이 존재한다.
(5) MAC은 인증을 위해 생성자와 검증자가 동일한 키를 사용해야 한다.
Tip! : 현재까지 나온 MAC 관련 시험 문제에서 MAC을 만들기 위해 공개키를 사용할 수 없다라고 했는데 이론상 공개키를 사용하는 것은 가능하다. 만약, 공개키가 사용가능하다고 한다면 MAC을 검증하기 위해서는 메시지와 개인키가 필요하다.

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, ㅁ
③ ㄷ, ㄹ
④ ㄱ, ㄷ, ㄹ

⑤ ㄷ, ㄹ, ㅁ
정답 체크 :
(3)
(ㄷ) 도청 : 기밀성을 해치므로 수동적 공격이다.
(ㄹ) 트래픽 분석 : 기밀성을 해치므로 수동적 공격이다.
오답 체크 :
(1), (2), (4), (5)
(ㄱ) 신분 위장 : 무결성을 해치므로 적극적 공격이다.
(ㄴ) 메시지 변경 : 무결성을 해치므로 적극적 공격이다.
(ㅁ) 서비스 거부 : 가용성을 해치므로 적극적 공격이다.

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 지켜야하는 기본 원칙으로 옳지 않은 것은?
① 최량 증거의 원칙
② 재현의 원칙
③ 정당성의 원칙
④ 신속성의 원칙
⑤ 연계보관성의 원칙
정답 체크 :
(1) 최량 증거 : 포렌식의 기본 원칙이 아니라 포렌식 수행 절차에서 분석 및 조사에 포함되는 내용이다. 최량 증거 원칙은 복사본 등의 2차적인 증거가 아닌 원본을 제출하도록 요구하는 영미 증거법상의 원칙이다. 즉, 원본이 존재하지 않으면 가장 유사하게 복사한 최초 복제물이라도 증거로 제출해야 한다.
오답 체크 :
(2) 재현 : 법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 한다. 수행할 때마다 다른 결과가 나온다면 증거로 제시할 수 없다.
(3) 정당성 : 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(4) 신속성 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 함을 의미한다.
(5) 연계보관성 : 해당 설명은 재현의 원칙이고, 연계보관성의 원칙은 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.

13. 와이파이(Wi-Fi) 보안 기술에 대한 설명으로 옳지 않은 것은?
① IEEE 802.11 표준 기반의 무선랜 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.

정답 체크 :
(3) MAC 주소 인증 프로토콜은 단말의 MAC 주소를 미리 AP에 등록해 놓고, 단말이 접속을 요청하면 요청 MAC과 저장해 놓은 MAC을 비교해서 인증을 수행한다. 802.1x, EAP 인증 프로토콜에 사용한다(WPA, WPA2).
오답 체크 :
(1) IEEE 802.11과 802.11i를 기반으로 한다.
(2) WEP의 경우 비밀키의 비트 길이가 작고(64비트) 고정 암호키를 사용하기 때문에 보안에 취약하다.
(4) WPA는 TKIP(암호키 동적 변경)를 사용한다.
(5) WPA2는 CCMP(암호키 동적 변경)과 AES 등 강력한 블록 암호 알고리즘을 사용한다.

14. 접근제어 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 사 용자의 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 높이는데 있다.
⑤ RBAC(Role Based Access Control)는 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직내 개인 역할에 따라 허용 여부를 결정하는 모델이다.
정답 체크 :
(2) MAC : 해당 설명은 DAC이고, MAC는 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) 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.
(3) BLP : 미 국방부 지원 보안 모델로 보안 요소 중 기밀성 강조한다. 최초의 수학적 모델로 강제적 정책에 의해 접근 통제하는 모델이다. 보안 정책은 정보가 높은 레벨에서 낮은 레벨로 흐르는 것을 방지한다. BLP의 속성은 No Read Up(보안 수준이 낮은 주체는 보안 수준이 높은 객체를 읽어서는 안되는 정책), No Write Down(보안 수준이 높은 주체는 보안 수준이 낮은 객체에 기록해서는 안됨)이다.
(4) Biba : BLP의 단점을 보완한 무결성을 보장하는 최초의 모델이다. 비바의 속성은 BLP의 반대 개념인 No Read Down(높은 등급의 주체는 낮은 등급의 객체를 읽을 수 없음), No Write Up(낮은 등급의 주체는 상위 등급의 객체를 수정할 수 없음)이다.
(5) RBAC : 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.

15. 〈보기〉에서 설명하는 블록 암호 운영 모드로 옳은 것은?

〈 보 기 〉
• '한 단계 앞의 암호 알고리즘의 출력을 암호화한 값'과 '평문 블록'을 XOR 연산하여 암호문 블록을 생성하는 운영 모드이다.
• 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

정답 체크 :
(4) OFB : 이전 단계의 출력 블록(평문 블록과 XOR해서 암호문 블록을 만들기 전 단계)을 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 다른 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다.

오답 체크 :
(1) ECB : 개별적으로 평문 블록을 암호화해서 암호문 블록으로 만든다. 암호화와 복호화가 같은 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 대응하는 블록이 에러가 된다.
(2) CBC : 이전 단계의 암호문 블록과 현재 단계의 평문 블록을 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 다른 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다.
(3) CFB : 이전 단계의 암호문 블록을 암호화한 후 현재 단계의 평문 블록과 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 다른 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 1블록 전체와 다음 블록의 대응하는 비트가 에러가 된다.
(5) CTR : 개별적으로 카운터를 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다. 암호화와 복호화가 같은 구조를 하고 있다. 비트 단위의 에러가 있는 암호문을 복호화하면, 평문의 대응하는 비트만 에러가 된다.
Tip! : 첫 번째 조건에서 답을 나왔으므로 두 번째, 세 번째 조건을 볼 필요가 없다.

16. 다음 중 캐싱(Caching) 장비가 응답하지 않도록 설정된 다수의 HTTP GET 패킷을 특정 시스템에 전송하여 서비스를 마비시키는 공격으로 옳은 것은?

① Slowloris 공격
② HTTP GET Flooding 공격
③ ARP Spoofing 공격
④ DNS Spoofing 공격
⑤ HTTP CC(Cache-control) 공격

정답 체크 :
(5) HTTP CC : HTTP 1.1 버전의 CC(Cache-Control) 헤더 옵션은 자주 변경되는 데이터에 대해 새롭게 HTTP 요청 및 응답을 요구하기 위하여 캐시(Cache) 기능을 사용하지 않게 할 수 있다. 서비스 거부 공격 기법에 이를 응용하기 위해 'Cache-Control: no-store, mustrevalidate' 옵션을 사용하면 웹 서버는 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가하게 된다.

오답 체크 :

(1) Slowloris : 최소 대역폭과 사용하지 않는 서비스와 포드를 이용해서 서버에 많은 연결을 맺고 최대한 길게 연결을 지속한다. 주기적으로 HTTP 요청을 하고 요청을 멈추거나 끝내지 않는다.
(2) HTTP GET Flooding : 서버에 TCP 3-웨이 핸드셰이킹 과정을 통해 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것이다.
(3) ARP Spoofing : 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다.
(4) DNS Spoofing : 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.

17. 다음 지문의 ㉠에 들어갈 말로 옳은 것은?

리눅스 시스템에서 관리자(root) 권한이 필요 없는 프로그램에 소유자가 관리자로 되어 있 으면서 (㉠)가 설정된 경우에는 시스템의 보안에 허점을 초래할 수 있다. 실제로 이것이 설정된 파일은 백도어 및 버퍼 오버플로우 등 여러 공격에 이용된다.

① SetUID
② SetGID
③ Sticky Bit
④ Finger
⑤ Shadow
정답 체크 :
(1) SetUID : 8진수로 4000으로 표현한다. 사용자가 실행 파일의 사용자 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.
오답 체크 :
(2) SetGID : 8진수로 2000으로 표현한다. 사용자가 실행 파일의 그룹 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.
(3) Sticky Bit : 8진수로 1000으로 표현한다. 디렉토리에 sticky bit가 설정되면 디렉토리 안의 파일들은 파일 소유자, 디렉토리 소유자 또는 관리자(root)만이 수정하거나 삭제할 수 있다.
(4) Finger : 서버에 현재 로그인 중인 사용자 계정 정보 확인하여, 해커가 사용자의 이용 시간 및 계정의 존재 유무 확인한다.
(5) Shadow : 패스워드가 shadow 파일에 암호화되어 저장된다. 관리자(root)만이 접근할 수 있다.

18. 다음 중 버퍼 오버플로우(Buffer Overflow)에 취약한 C언어 함수로 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_p ath);
⑤ char *strcat(char *dest, const char *src);
정답 체크 :
(3) strcmp : str1과 str2는 정해진 문자열이고 단순 비교이므로 버퍼 오버플로우가 발생하지 않는다.

오답 체크 :
사용자 입력을 받아들이는 부분이 있고, 이의 길이를 제한하지 않으면 버퍼 오버플로우가 발생한다.
(1) scanf : 사용자의 입력을 buf에 받는다고 가정하면, 사용자의 입력 길이를 제한하는 부분이 없이 버퍼 오버플로우가 발생한다.
(2) gets : buf에 사용자 입력을 받는데, 사용자의 입력 길이를 제한하는 부분이 없이 버퍼 오버플로우가 발생한다.
(4) resolved_path : path가 절대 path로 변환되고 resolved_path에 저장되는데, 해당 절대 path의 길이가 resolved_path의 길이를 초과하면 버퍼 오버플로우가 발생한다.
(5) strcat : src 문자열을 dest 문자열 뒤에 붙이는데 src 문자열이 dest 문자열의 남아 있는 버퍼 크기를 초과하면 버퍼 오버플로우가 발생한다.

19. 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공하는 경우, 이용자에게 알리고 동의를 받아야하는 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 이용 기간
정답 체크 :
(4) 개인정보 보호책임자는 제3자가 웹 사이트 등을 통해 공개해야하는 상황으로 굳이 이용자에게 알리고 동의를 받아야 하는 내용이 아니다.
오답 체크 :
(1), (2), (3), (5)
“정보통신망법” 제24조의2(개인정보의 제공 동의 등) 상 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 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

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 보호하는데 사용할 암호키를 협상할 수 있다.

① Alert Protocol
② Handshake Protocol
③ Record Protocol
④ Change Cipher Spec Protocol
⑤ Encapsulating Security Payload Protocol
정답 체크 :
(2) Handshake : 클라이언트와 서버가 암호 통신에 사용할 알고리즘과 공유 키를 결정한다. 인증

서를 이용한 인증을 수행한다.

오답 체크 :

(1) Alert : 뭔가 에러가 발생했다는 것을 통신 상대에게 전달한다.

(3) 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) Change Cipher Spec : 암호 방법을 변경하는 신호를 통신 상대에게 전달한다.

(5) Encapsulating Security Payload(ESP) : IPSec에서 기밀성(암호화), 무결성, 인증, 재사용 방지를 제공하기 위해서 사용한다.