박문각 남부고시학원　손경희 선생

2015 서울시 9급 정보보호론

[2015 서울시]
1. 패스워드가 갖는 취약점에 대한 대응방안으로 적절치 않은 것은? 1
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.
[해설]
- 패스워드를 만들 때 사용자와 관련된 내용을 포함시키면 사용자 정보를 통해 패스워드를 유추하여 공격할 수 있기 때문에 공격이 더 수월해 질 수 있다.

[2015 서울시]
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? 4

㉠ 키를 사용하여 문서를 암호화할 때 ㉡ 문서를 암 . 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
[해설]
- 하이브리드 시스템은 기본적으로 대칭키 암호시스템에 기반하고 있다고 생각하면 더 이해하기 쉽다. 대칭키 암호시스템으로 문서를 암/복호화하여 송수신하는데. 대칭키 분배의 문제를 공개키 암호시스템으로 해결한 것이다. 즉, 송신자는 대칭키를 수신자의 공개키를 통하여 암호화하여 전송하고, 이를 받은 수신자는 자신의 개인키를 통하여 복호화하여 대칭키를 분배한다.

[2015 서울시]
3. 현재 10명이 사용하는 암호시스템을 20명이 사용할 수 있도록 확장하려면 필요한 키의 개수도 늘어난다. 대칭키 암호시스템과 공개키 암호시스템을 채택할 때 추가로 필요한 키의 개수를 각각 구분하여 순서대로 나열한 것은? 3
① 20개, 145개　　② 20개, 155개
③ 145개, 20개　　④ 155개, 20개
[해설]
- 공개키의 개수는 2n개이므로, 20개 증가한다.
- 대칭키의 개수는 n(n-1)/2개이므로 현재 10명이 가지고 있는 키의 개수는 45개이며, 20명일 때를 계산하면 190개가 된다. 현재 10명이 사용하던 시스템을 확장하는 것이므로 (190 -

45)로 계산하면 키는 145개 확장이 필요하다.

4. 다음은 오용탐지(misuse detection)와 이상탐지(anomaly detection)에 대한 설명이다. 이상탐지에 해당되는 것을 모두 고르면? 1

㉠ 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 ㉡, ㉣

[해설]

- 오용탐지는 알려진 공격법이나 보안정책을 위반하는 행위에 대한 패턴을 지식 데이터베이스로부터 찾아서 특정 공격들과 시스템 취약점에 기초한 계산된 지식을 적용하여 탐지해 내는 방법으로 지식 기반(Knowledge-Base)탐지라고도 한다. 문제의 보기에서는 ㉡과 ㉣이 여기에 해당된다.
- 비정상적인 행위(이상) 탐지는 시스템 사용자가 정상적이거나 예상된 행동으로부터 이탈하는지의 여부를 조사함으로써 탐지하는 방법을 말한다. 통계적인 자료를 근거로 하거나 특징 추출에 의존한다. 정상적인 행위에서 이탈하는 것을 탐지하기 때문에 제로데이 공격도 탐지 할 수 있다.

[2015 서울시]

5. SYN flooding을 기반으로 하는 DoS 공격에 대한 설명으로 옳지 않은 것은? 3

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.

[해설]

- SYN flooding 공격은 TCP 연결의 3way handshake 3단계 통신의 Syn 플래그를 악용한 공격이며, 운영체제의 원인은 아니다.

[2015 서울시]

6. 다음은 접근통제(access control) 기법에 대한 설명이다. 강제접근제어(Mandatory Access Control)에 해당되는 것은? 2

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

[해설]

- 강제적접근제어는 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근 통제이며, 모든 객체는 기밀성을 지니고 있다고 보고 객체에 보안 레이블을 부여하여 사용한다.

박문각 남부고시학원　손경희 선생

[2015 서울시]
7. 다음은 AES(Advanced Encryption Standard) 암호에 대한 설명이다. 옳지 않은 것은? 4
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, 128/192/256 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.
[해설]
- 입력을 좌우 블록으로 분할하여 한 블록을 라운드 함수에 적용시킨 후에 출력값을 다른 블록에 적용하는 과정을 좌우 블록에 대해 반복적으로 시행하는 것은 페이스텔 구조이다.

[2015 서울시]
8. SET(Secure Electronic Transaction)의 설명으로 옳은 것은? 4
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.
[해설]
- 보기 1번 : SET 참여자들이 신원을 확인하고 인증서를 발급한다.
- 보기 2번 : 온라인상에서 금융거래 안전성을 보장하기 위한 시스템이다.
- 보기 3번 : 신용카드 사용을 위해 상점에서 소프트웨어를 요구한다.

[2015 서울시]
9. 다음 중 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은? 2
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.
[해설]
- 커버로스는 MIT 아테네 프로젝트에서 개발된 신뢰할 수 있는 제3자 인증 프로토콜로서, 인증과 메시지 보호를 제공하는 보안 시스템의 이름이다. 대칭키 암호방식을 사용하여 분산 환경에서 개체 인증 서비스를 제공한다.

[2015 서울시]

10. 다음 중 해시함수의 설명으로 옳은 것은? 4
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.
[해설]
- 보기 1번 : 입력이 가변길이이고, 출력은 고정되어 있다.
- 보기 2번 : 보기의 내용으로 충돌이 발생할 수 있지만, 충돌저항성이 있어야 한다.
- 보기 3번 : 해시함수는 해시값의 생성에 있어서 비밀키를 사용하는 MAC(Message Authentication Code)과 비밀키를 사용하지 않는 MDC(Manipulation Detection Code)로 나눌 수 있다.

[2015 서울시]
11. 다음에서 허니팟(honeypot)이 갖는 고유 특징에 대한 설명으로 옳지 않은 것은? 1
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.
[해설]
- 허니팟은 침입을 방지하는 개념이 아니라. 가상으로 해커의 침입을 유도해 신분을 확보하며 위장서버와 추적장치를 활용해 해커를 유인해낸다. 해커들에게 허니팟은 일부러 취약점을 드러낸다. 취약점 공략을 위해 허니팟을 공격하는 해커들은 해킹경로와 해킹수법을 드러내 신분이나 해킹위치를 역추적당하게 된다.

[2015 서울시]
12. Diffie-Hellman 알고리즘은 비밀키를 공유하는 과정에서 특정 공격에 취약할 가능성이 존재한다. 다음 중 Diffie-Hellman 알고리즘에 가장 취약한 공격으로 옳은 것은? 2
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
[해설]
- Diffie-Hellman 알고리즘은 키의 분배 및 교환에 주로 사용되는 알고리즘이다. 송/수신자 사이에 공격자가 서로에 송/수신자인 것처럼 공격한다면 숭/수신자는 공격을 당할 수 있다. 이런 공격이 중간자 공격이며, Diffie-Hellman 알고리즘은 중간자 공격에 취약하다.

[2015 서울시]
13. 다음은 공개키 기반 구조(PKI)에 대한 정의이다. 옳지 않은 것은? 2
① 네트워크 환경에서 보안 요구사항을 만족시키기 위해 공개키 암호화 인증서 사용을 가능하

게 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.
[해설]
- 암호화된 메시지를 송신할 때에는 수신자의 개인키를 사용하며, 암호화된 서명 송신 시에는 송신자의 공개키를 사용한다.

[2015 서울시]
14. 블록 암호는 평문을 일정한 단위(블록)로 나누어서 각 단위마다 암호화 과정을 수행하여 암호문을 얻는 방법이다. 블록암호 공격에 대한 설명으로 옳지 않은 것은? 4
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.
[해설]
- 보기 4번은 통계적 분석의 내용이며, 수학적 분석은 수학적 이론을 이용하여 해독하는 방법으로 통계적인 방법이 포함된다.

[2015 서울시]
15. 다음은 웹사이트와 브라우저에 대한 주요 공격 유형 중 하나이다. 무엇에 대한 설명인가? 1

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
[해설]
- 크로스 사이트 요청 변조(CSRF; Cross-Site Request Forgecy) : 로그인한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹 어플리케이션에 전송하는 취약점이다. 데이터를 등록.변경의 기능이 있는 페이지에서 동일 요청(Request)으로 매회 등록 및 변경 기능이 정상적으로 수행이 되면 CSRF 공격에 취약한 가능성을 가지게 된다. 악의적인 사용자 또는 제3자는 사용자의 브라우저 내에서 서버가

유지하고 있는 신뢰를 이용해서 웹 서버를 공격할 수 있다.
- 크로스사이트 스크립팅(XSS; Corss Site Scripting) : 타 사용자의 정보를 추출하기 위해 사용되는 공격 기법으로 게시판이나 검색 부분, 즉 사용자의 입력을 받아들이는 부분에 스크립트 코드를 필터링하지 않음으로써 공격자가 스크립트 코드를 실행할 수 있게 되는 취약점이다. XSS는 과부하를 일으켜 서버를 다운시키거나 피싱공격으로도 사용 가능하고, 가장 일반적인 목적은 웹 사용자의 정보 추출이다.
- SQL 삽입공격(SQL Injection) : 웹 어플리케이션은 사용자로부터 SQL 구문을 입력 받는 부분, 즉 데이터베이스와 연동되어야 하는 부분으로 크게 로그인, 검색, 게시판으로 나눌 수 있다. 로그인 하는 과정에서 아이디와 패스워드 부분에 특정한 SQL문이 삽입되어 그것이 그대로 데이터베이스에 전송되어 공격자는 원하는 결과를 볼 수 있다. 즉, 데이터베이스와 연동되는 입력란에 공격자가 원하는 SQL문을 삽입하여 공격한다.
- 비트플리핑 공격 : DRAM에서 발견된 취약점을 활용해 실제 PC, 노트북 해킹이 이론 수준을 넘어 실제로 가능하다는 것이 검증되었고, 핵심은 DRAM이 점점 더 고집적화 될수록 메모리 구조 상 내부 영역들 간 간섭 현상이 발생할 가능성이 높아진다. 이른바 '비트 플리핑'이라 불리는 현상이다. 이러한 현상을 악용해 PC나 노트북에서 X86 아키텍처에서 구동되는 리눅스의 관리자 권한을 획득할 수 있다는 사실을 실험을 통해 확인되었다.

[2015 서울시]
16. 가설사설망(VPN)이 제공하는 보안 서비스에 해당하지 않는 것은? 1
① 패킷 필터링 ② 데이터 암호화
③ 접근제어 ④ 터널링
[해설]
- 가설사설망(VPN)에서는 암호화 혹은 인증 터널을 통해 전송되는 데이터의 기밀성, 무결성, 인증과 같은 보안 서비스가 보장된다.
- 보기 1번의 패킷 필터링은 방화벽에 관련된 내용이다.

[2015 서울시]
17. 전자서명(digital signature)은 내가 받은 메시지를 어떤 사람이 만들었는지를 확인하는 인증을 말한다. 다음 중 전자서명의 특징이 아닌 것은? 4
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.
[해설]
- 전자서명의 특징 중에 재사용 불가가 있으며, 이는 한번 서명한 서명문은 또 다른 문서에 사용할 수 없다는 것이다.

[2015 서울시]
18. 다음 <보기>에서 설명하는 것은 무엇인가? 2

<보기>
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)
[해설]
- AH(Authentication Header) : 데이터가 전송 도중에 변조되었는지를 확인할 수 있도록 데이터의 무결성에 대해 검사한다. 그리고 데이터를 스니핑한 뒤 해당 데이터를 다시 보내는 재생 공격(Replay Attack)을 막을 수 있다.
- ESP(Encapsulating Security Payload) : 메시지의 암호화를 제공한다. 사용하는 암호화 알고리즘으로는 DES-CBC, 3DES, RC5, IDEA, 3IDEA, CAST, blowfish가 있다.
- IKE(Internet Key Exchange) : ISAKMP(Internet Security Association and Key Management Protocol), SKEME, Oakley 알고리즘의 조합으로, 두 컴퓨터 간의 보안 연결(SA, Security Association)을 설정한다. IPSec에서는 IKE를 이용하여 연결이 성공하면 8시간 동안 유지하므로, 8시간이 넘으면 SA를 다시 설정해야 한다.

[2015 서울시]
19. 다음 <보기>에서 설명하고 있는 무선네트워크의 보안 프로토콜은 무엇인가? 3

<보기>
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)
[해설]
- WEP : 암호화키는 64bit는 40bit RC4, 128bit는 104bit RC4에 무작위 24bit IV(Initial Vector)로 구성되어 있지만, IV의 길이가 짧아 반복되어 사용하기 때문에 짧은 시간에 해킹이 가능하다.
- WPA-PSK : TKIP(temporal Key Integrity Protocol) 알고리즘 또는 AES 알고리즘의 사용이 가능하다.

[2015 서울시]
20. 컴퓨터 포렌식(forensics)은 정보처리기기를 통하여 이루어 지는 각종 행위에 대한 사실관계를 확정하거나 증명하기 위해 행하는 각종 절차와 방법이라고 정의할 수 있다. 다음 중 컴퓨터 포렌식에 대한 설명으로 옳지 않은 것은? 1

박문각 남부고시학원　손경희 선생

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 증거 자료를 찾아서 분석한 보고서를 제출하는 절차와 방법을 말한다.

[해설]

- 보기 1번의 내용은 웹 포렌식에 대한 설명이며, 네트워크 포렌식은 네트워크를 통해 전송되는 데이터를 대상으로 증거를 획득하거나 분석하는 것을 말한다.