**<5과목: 정보시스템 구축관리>**

소프트웨어 개발에서 정보보안 3요소

기밀성: 인가된 사용자에 대해서만 자원 접근이 가능하다

무결성: 인가된 사용자에 대해서만 자원 수정이 가능하며 전송중인 정보는 수정되지 않는다

가용성: 인가된 사용자는 가지고 있는 권한 범위 내에서 언제든 자원 접근이 가능하다

틀린 것: 휘발성: 인가된 사용자가 수행한 데이터는 처리 완료 즉시 폐기되어야 한다

어떤 외부 컴퓨터가 접속되면 접속 인가 여부를 점검해서 인가된 경우에만 접속이 허용되고, 그 반대의 경우에는 거부할 수 있는 접근제어 유틸리티

TCP wrapper

Zing

기기를 키오스크에 갖다 대면 원하는 데이터를 바로 가져올 수 있는 기술로 10츠 이내 근접거리에서 기가급 속도로 데이터 전송이 가능한 초고속 근접무선통신(NFC: Near Field Communication)

취약점 관리를 위한 응용 프로그램의 보안 설정

실행 프로세스 권한 설정

운영체제의 접근 제한

운영체제의 정보 수집 제한

틀린 것: 서버 관리실 출입 통제

소프트웨어 개발 프레임워크와 관련한 설명

반제품 상태의 제품을 토대로 도메인별로 필요한 서비스 컴포넌트를 사용하여 재사용성 확대와 성능을 보장받을 수 있게 하는 개발 소프트웨어

설계 관점에 개발 방식을 패턴화 시키기 위한 노력의 결과물인 소프트웨어 디자인 패턴을 반제품 소프트웨어 상태로 집적화시킨 것으로 볼 수 있다

프레임워크의 동작 원리를 그 제어 흐름의 일반적인 프로그램 흐름과 반대로 동작한다고 해서 IoC(Inversion of Control)이라고 설명하기도 한다

개발해야 할 애플리케이션의 일부분이 이미 내장된 클래스 라이브러리로 구현이 되어 있다, 따라서 그 기반이 되는 이미 존재하는 부분을 확장 및 이용하는 것, 동일한 로직 반복을 줄일 수 있다

Java 기반의 대표적인 소프트웨어로는 스프링(Spring)이 있다

생산성 향상과 유지보수성 향상 등의 장점이 있다

틀린 것:

라이브러리와는 달리 사용자 코드에서 프레임워크를 호출해서 사용, 그에 대한 제어도 사용자 코드가 가지는 방식

라이브러리와는 달리 사용자 코드가 직접 호출하여 사용, 소프트웨어 개발 프레임워크가 직접 코드의 흐름을 제어할 수 없다

클라우드 기반 HSM(Cloud-based Hardware Security Module)에 대한 설명

클라우드(데이터센터) 기반 암호화 키 생성, 처리, 저장 등을 하는 보안기기

국내에서는 공인인증제의 폐지와 전자서명법 개정을 추진하면서 클라우드 HSM용어가 자주 등장

클라우드에 인증서를 저장하므로 기존 HSM 기기나 휴대폰에 인증서를 저장해 다닐 필요가 없다

틀린 것: HW가 아닌 SW적으로만 구현되기 때문에 SW식 암호기술에 내재된 보안 취약점을 해결할 수 없다는 단점

Mesh Network

다른 국을 향하는 호출이 중계에 의하지 않고 직접 접속되는 그물 모양의 네트워크

통신량이 많은 비교적 소수의 국 사이에 구성될 경우 경제적이며 간편하지만, 다수의 국 사이에는 회선이 세분화되어 비경제적일 수도 있다

해당 형태의 무선 네트워크의 경우 대용량을 빠르고 안전하게 전달할 수 있어 행사장이나 군 등에서 많이 활용된다

물리적 위협으로 인한 문제

화재, 홍수 등 천재지변으로 인한 위협

하드웨어 파손, 고장으로 인한 장애

방화, 테러로 인한 하드웨어와 기록장치를 물리적으로 파괴하는 행위

틀린 것: 방화벽 설정의 잘못된 조작으로 인한 네트워크, 서버 보안 위협

악성코드의 유형 중 다른 컴퓨터의 취약점을 이용하여 스스로 전파하거나 메일로 전파되며 스스로를 증식하는 것

Worm

틀린 것:

Rogue Ware: 가짜 백신 프로그램, 거짓 내용으로 사용자를 속여 결제하게끔 유도

Adware: 팝업 광고 표시 프로그램

Reflection Attack: 동일한 프로토콜을 양방향으로 사용하는 시도 응답 인증 시스템을 공격하는 방법

Ping of Death: 시스템 공격 기법 중 하나로 허용범위 이상의 ICMP 패킷을 전송하여 대상 시스템의 네트워크를 마비

Session Hijacking: 공격 대상이 이미 시스템에 접속되어 세션에 연결되어 있는 상태를 가로채기 하는 공격

Piggyback attack: 다른 사용자의 합법적 연결에서 비활성 간격을 통해 시스템에 액세스하는 활성형태의 도청

XSS: Cross Site Scripting, 상대방의 브라우저에 스크립트가 실행되도록 해 사용자의 세션을 가로채거나, 웹사이트를 변조하거나, 악의적 콘텐츠를 삽입하거나, 피싱 공격을 진행하는 것

대칭 암호 알고리즘, 비대칭 암호 알고리즘에 대한 설명

대칭 암호 알고리즘은 비교적 실행 속도가 빠르기 때문에 다양한 암호의 핵심 함수로 사용될 수 있다

비대칭 암호 알고리즘은 자신만이 보관하는 비밀키를 이용하여 인증, 전자서명 등에 적용이 가능하다

대표적인 대칭키 암호 알고리즘으로는 AES, IDEA 등이 있다

틀린 것: 대칭 암호 알고리즘은 비밀키 전달을 위한 키 교환이 필요하지 않아 암호화 및 복호화의 속도가 빠르다

월별(man-month) 생산성 측정

두 명의 개발자 5개월 10000라인 코드 개발 -> 10000 / (5 \* 2)

RBAC: Role-Based Access Control, 조직 내에서 직무, 직책 등 개인의 역할에 따라 권한을 결정, 부여하는 접근 정책

COCOMO(Constructive Cost Model) 모형의 특징

프로젝트를 완성하는데 필요한 man-month로 산정 결과를 나타낼 수 있다

보헴(Boehm)이 제안한 것으로 원시코드 라인 수에 의한 비용 산정 기법이다

비교적 작은 규모의 프로젝트 기록을 통계 분석하여 얻은 결과를 반영한 모델이며 중소 규모 소프트웨어 프로젝트 비용 추정에 적합하다

틀린 것: 프로젝트 개발 유형에 따라 object, dynamic, function의 3가지 모드로 구분한다

각 사용자 인증의 유형에 대한 설명

지식: 주체는 ‘그가 알고 있는 것’을 보여주며 예시로는 패스워드, PIN 등이 있다

소유: 주체는 ‘그가 가지고 있는 것’을 보여주며 예시로는 토큰, 스마트카드 등이 있다

행위: 주체는 ‘그가 하는 것’을 보여주며 예시로는 서명, 움직임, 음성 등이 있다

틀린 것: 존재: 주체는 ‘그를 대체하는 것’을 보여주며 예시로는 패턴, QR 등이 있다(‘그를 나타내는 것’, 홍채, 지문)

시스템의 사용자가 로그인하여 명령을 내리는 과정에 대한 시스템의 동작

Authentication(인증): 자신의 신원(Identity)을 시스템에 증명하는 과정, 아이디와 패스워드를 입력하는 과정이 가장 일반적인 예시

틀린 것: Authorization(허가)

SDN(Software Defined Networking)

네트워크를 제어부, 데이터 전달부로 분리하여 네트워크 관리자가 보다 효율적으로 네트워크를 제어, 관리할 수 있는 기술

기존의 라우터, 스위치 등과 같이 하드웨어에 의존하는 네트워크 체계에서 안정성, 속도, 보안 등을 소프트웨어로 제어, 관리하기 위해 개발됨

네트워크 장비의 펌웨어 업그레이드를 통해 사용자의 직접적인 데이터 전송 경로 관리가 가능하고, 기존 네트워크에는 영향을 주지 않으면서 특정 서비스의 전송경로 수정을 통하여 인터넷 상에서 발생하는 문제를 처리할 수 있음

프로젝트 일정 관리 시 사용하는 PERT 차트에 대한 설명

각 작업들이 언제 시작하고 언제 종료되는지에 대한 일정을 막대 도표를 이용하여 표시

시간선(Time-line) 차트라고도 한다

수평 막대의 길이는 각 작업의 기간을 나타낸다

틀린 것: 작업들 간의 상호 관련성, 결정경로, 경계시간, 자원할당 등을 제시한다

소프트웨어 생명주기 모델 중 나선형(Spiral Model)과 관련한 설명

소프트웨어 개발 프로세스를 위험 관리(Risk Management) 측면에서 본 모델

시스템을 여러 부분으로 나누어 여러 번의 개발 주기를 거치면서 시스템이 완성

요구사항이나 아키텍처를 이해하기 어렵다거나 중심이 되는 기술에 문제가 있는 경우 적합한 모델

계획 및 정의 – 위험 분석 – 공학적 개발 – 고객 평가

틀린 것: 위험 분석(Risk Analysis)은 반복적인 개발 진행 후 주기의 마지막 단계에서 최종적으로 한 번 수행

고 가용성 솔루션(HACMP): 각 시스템 간에 공유 디스크를 중심으로 클러스터링으로 엮여 다수의 시스템을 동시에 연결할 수 있다

조직, 기업의 기간 업무 서버 등의 안정성을 높이기 위해 사용될 수 있다

여러 방식으로 구현, 2개의 서버를 연결하는 것으로 2개의 시스템이 각각 업무를 수행하는 구현 방식이 널리 사용

점대점 연결 방식(Point-to-Point Mode): 네트워크에 있어 물리적으로는 중계 장치를 통과하지 않고 한 지점에서 다른 지점으로 직접 가는 채널, 두 스테이션간을 별도의 회선을 사용하여 1 대 1로 연결, 회선 구성이 간단하고 대용량 전송에 유리, 별도의 회선과 포트에 따른 높은 설치비용

스턱스넷(Stuxnet): 웜 바이러스, 윈도우를 통해 감염, 지맨스산업의 SW 및 장비를 공격

루팅(Rooting): 모바일 기기에서 구동되는 안드로이드 운영체제에서 최상위 권한(루트 권한)을 얻음으로 해당 기기의 생산자 또는 판매자 측에서 걸어 놓은 제약을 해제하는 행위

Switch Jamming: 위조된 매체 접근 제어(MAC) 주소를 지속적으로 네트워크로 흘려보내 스위치 MAC 주소 테이블의 저장 기능을 혼란시켜 더미 허브(Dummy Hub)처럼 작동하게 하는 공격

Parsing: 하나의 프로그램을 런타임 환경이 실제로 실행할 수 있는 내부 포맷으로 분석하고 변환하는 것

LAN Tapping: LAN신호를 직접 자신에게 끌어오는 방식의 공격

FTP(SYN) Flooding: TCP의 3 Way Handshake 취약점을 이용한 DoS 공격으로 다량의 SYN패킷을 보내 백로그큐를 가득 채우는 공격, FTP 프로토콜을 사용한 서버에 다량의 SYN 패킷을 보내 마비시키는 것

DAS(Direct-Attached Storage, 직접 연결 저장장치): 하드디스크와 같은 데이터 저장장치를 호스트 버스 어댑터에 직접 연결하는 방식, 저장장치와 호스트 기기 사이에 네트워크 디바이스 없이 직접 연결하는 방식으로 구성

NAS(Network-Attached Storage, 네트워크 연결 저장장치)

NFC: 근거리 무선 통신

취약점 관리를 위해 일반적으로 수행하는 작업

무결성 검사

응용 프로그램의 보안 설정 및 패치(Patch) 적용

불필요한 서비스 및 악성 프로그램의 확인과 제거

틀린 것: 중단 프로세스 및 닫힌 포트 위주로 확인(활성화 프로세스와 열린 포트를 중심으로 확인)

소프트웨어 생명주기 모델 중 V 모델과 관련한 설명

Perry에 의해 제안, 세부적인 테스트 과정으로 구성되어 신뢰도 높은 시스템을 개발하는데 효과적

개발 작업과 검증 작업 사이의 관계를 명확히 들어내 놓은 폭포수 모델의 변형, 코딩 단계에서 위쪽으로 꺾여 V모양

폭포수 모델이 산출물 중심이라면 V 모델은 작업과 결과의 검증에 초점을 둔다

검증(Verification) 단계: 요구사항 분석 – 시스템 설계 – 아키텍쳐 설계 – 모듈 설계

틀린 것: 요구 분석 및 설계 단계를 거치지 않으며 항상 통합테스트를 중심으로 V 형태를 이룬다

블루투스 공격과 해당 공격에 대한 설명

블루프린팅(BluePrinting): 블루투스 공격 장치의 검색 활동을 의미

블루버그(BlueBug): 블루투스 장비 사이의 취약한 연결 관리를 악용한 공격

블루스나프(BlueSnarf): 블루투스의 취약점을 활용하여 장비의 파일에 접근하는 공격, OPP를 사용하여 정보를 열람

블루재킹(BlueJacking): 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼뜨리는 것

OPP(Obex Push Protocol): 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위하여 개발됨

DoS(Denial of Service) 공격과 관련한 내용

Ping of Death 공격은 정상 크기보다 큰 ICMP 패킷을 작은 조각(Fragment)으로 쪼개어 공격 대상이 조각화 된 패킷을 처리하게 만드는 공격 방법

SYN Flooding은 존재하지 않는 클라이언트가 서버별로 한정된 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 이용하지 못하게 하는 것

Land 공격은 패킷 전송 시 출발지 IP주소와 목적지 IP주소 값을 똑같이 만들어서 공격 대상에게 보내는 공격 방법

Smurf 공격은 브로드캐스트를 활용하여 공격 대상이 네트워크의 임의의 시스템에 패킷을 보내게 만드는 공격

Honeypot: 1990년대 David Clock이 처음 제안, 비정상적인 접근의 탐지를 위해 의도적으로 설치해 둔 시스템, 침입자를 속여 실제 공격당하는 것처럼 보여줌으로써 크래커를 추적 및 공격기법의 정보를 수집하는 역할, 쉽게 공격자에게 노출되어야 하며 쉽게 공격이 가능한 것처럼 취약해 보여야 한다

Hadoop: 오픈 소스를 기반으로 한 분산 컴퓨팅 플랫폼, 대형 스토리지, 빅데이터 관련

MapReduce: 대용량 데이터를 분산처리 하기위해 구글이 개발한 프로그래밍 모델, 임의의 순서로 분산처리 후 합침

Apache: W3C에서 사용하고 아파치 소프트웨어 재단에서 관리 및 운영하는 서버용 오픈소스 소프트웨어

Docker: 소프트웨어 컨테이너 안에 응용프로그램들을 배치시키는 일을 자동화 해 주는 오픈소스 소프트웨어

StackGuard: Stack 상에 일정한 주소 번지에 프로그램이 선언한 Canary를 심어 스택이 변조된 경우 Canary를 체크하여 프로그램을 비정상적으로 종료시키는 기법

Cipher Container: 자바에서 암호화 복호화 기능을 제공하는 컨테이너

Scytale: 암호화 기법으로 단순하게 문자열의 위치를 바꾸는 방법

간트 차트(Gantt Chart)에 대한 설명

프로젝트를 이루는 소작업별로 언제 시작되고 언제 끝나야 하는지를 한 눈에 볼 수 있도록 도와준다

자원 배치 계획에 유용하게 사용된다

CPM 네트워크로부터 만드는 것이 가능하다

틀린 것: 수평 막대의 길이는 각 작업에 필요한 인원수를 나타낸다(기간을 나타낸다)

Scrapy: Python 기반의 웹 크롤링 프레임워크, 가볍고 빠르고 확장성이 좋음

Li-fi: 스펙트럼의 빛을 이용한 5세대 이동 통신 기술

SBAS(위성항법보강시스템): GPS의 오차를 보정해 신뢰성과 안정성을 높인 기법

Secure 코딩에서 입력 데이터의 보안 약점과 관련한 설명

SQL 삽입: 사용자의 입력값 등 외부 입력값이 SQL 쿼리에 삽입되어 공격

크로스사이트 스크립트: 검증되지 않은 외부 입력값에 의해 브라우저에서 악의적인 코드가 실행

운영체제 명령어 삽입: 운영체제 명령어 파라미터 입력값이 적절한 사전검증을 거치지 않고 사용되어 공격자가 운영체제 명령어를 조작

틀린 것: 자원 삽입: 사용자가 내부 입력값을 통해 시스템 내에 사용이 불가능한 자원을 지속적으로 입력함으로써 시스템에 과부하 발생

(자원을 조작할 수 있는 문자열을 삽입하여 시스템이 보호하는 자원에 임의로 접근할 수 있는 취약점)

Windows 파일 시스템인 FAT과 비교했을 때의 NTFS의 특징

대용량 볼륨에 효율적

자동 압축 및 안정성

저용량 볼륨에서의 속도 저하

틀린 것: 보안에 취약

DES: 64비트 암호화 알고리즘, 7비트마다 오류 검출을 위한 정보가 1비트씩 들어가기 때문에 실질적으로 56 비트이다. 추가적으로 AES 암호화 알고리즘은 AES-128, AES-192, AES-256으로 나뉘며 숫자는 비트수이다.

리눅스에서 생성된 파일 권한이 644일 경우 umask 값

022

666에서 파일 권한 644를 빼면 022가 된다

wtmp: 리눅스 시스템에서 사용자의 성공한 로그인/아웃 정보 기록, 시스템의 종료/시작 시간 기록, var/log/wtmp

utmp: 현재 로그인 사용자의 상태 정보를 담고 있는 로그 파일

btmp: 실패한 로그인 정보를 담고 있는 로그 파일

last log: 마지막으로 성공한 로그인 정보를 담고 있는 로그 파일

상향식 비용 산정 기법 중 LOC(원시 코드 라인 수) 기법에서 예측치를 구하기 위해 사용하는 항목

낙관치

기대치

비관치

틀린 것: 모형치

DPI(Deep Packet Inspection): OSI 7 Layer 전 계층의 프로토콜과 패킷 내부의 컨텐츠를 파악하여 침입 시도, 해킹 등을 탐지하고 트래픽을 조정하기 위한 패킷 분석 기술, 네트워크에서 전송되는 패킷의 헤더와 페이로드 내 정보를 분석하는 컨텐츠 내용 분석 기술, 네트워크 보안, 관리, 컨텐츠 관리 등이 목적

PLCP(Physical Layer Convergence Procedure): 물리 계층 수렴 처리, 논리적인 802.11 MAC 부계층과 물리적인 특성을 연결하는 역할, 802.11 MAC 부계층이 물리적 특성에 관계없이 동작하도록 함

Traffic Distributor: 네트워크 통신 간에 트래픽을 분배해주는 솔루션

소프트웨어 개발 방법론의 테일러링(Tailoring)과 관련한 설명

프로젝트에 최적화된 개발 방법론을 적용하기 위해 절차, 산출물 등을 적절히 변경하는 활동

관리 측면에서의 목적 중 하나는 최단기간에 안정적인 프로젝트 진행을 위한 사전 위험을 식별, 제거하는 것

기술적 측면에서의 목적 중 하나는 프로젝트에 최적화된 기술 요소를 도입하여 프로젝트 특성에 맞는 최적의 기법과 도구를 사용하는 것이다

틀린 것: 프로젝트 수행 시 예상되는 변화를 배제하고 신속히 진행하여야 한다

Tailoring: 프로젝트 상황 특성에 맞게 정의된 소프트웨어 개발 방법론 절차, 사용 기법 등을 수정 및 보완하는 작업

침입 탐지 시스템(IDS, Intrusion Detection System)과 관련한 설명

HIDS(Host-Based Intrusion Detection)는 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고 어떤 작업을 했는지에 대한 기록을 남기고 추적한다

NIDS(Network-Based Intrusion Detection)로는 대표적으로 Snort가 있다

Misuse Detection: 오용 탐지, Signature Base나 Knowledge Base라고도 불리며 이미 발견되고 정립된 공격 패턴을 입력해두었다가 탐지 및 차단한다

외부 인터넷에 서비스를 제공하는 서버가 위치하는 네트워크인 DMZ(Demilitarized Zone)에는 IDS가 설치될 수 있다

틀린 것: 이상 탐지 기법(Anomaly Detection)은 Signature Base나 Knowledge Base라고도 불리며 이미 발견되고 정립된 공격 패턴을 입력해두었다가 탐지 및 차단한다(Behavior, Statistical Detection으로 불림, 평균적 시스템의 상태 기준으로 비정상적인 행위나 자원의 사용이 감지되면 이를 알려줌)

침입 탐지 시스템의 모델

오용 탐지: 잘 알려진 시스템의 취약점을 공격하는 패턴의 침입을 탐지(새로운 공격 패턴을 막기 어려움)

이상 탐지: 잘 알려지지 않은 공격 탐지에 적합, 기존 패턴과 급격하게 다른 패턴을 발견하면 침입을 판단

정보 보안을 위한 접근통제 정책

Mandatory Access Control(MAC): 강제접근통제, 정보 시스템 내에서 어떤 주체가 특정 개체에 접근하려 할 때 양쪽의 보안 레이블(Security Label)에 기초하여 높은 보안 수준을 요구하는 정보(객체)가 낮은 보안 수준의 주체에게 노출되지 않도록 하는 접근 제어 방법

Discretionary Access Control(DAC): 임의접근통제, 접근하는 사용자의 신원에 따라 접근 권한을 부여하는 방식

Role-Based Access Control(RBAC): 역할기반 접근통제

User Access Control(UAC): 사용자계정통제, 프로그램에서 관리자 수준의 권한이 필요한 작업을 수행할 때 사용자에게 알려서 제어할 수 있도록 돕는 기능

Data-Label Access Control, Label-Based Access Control: 자료별 접근 통제, 개별 행, 열에 대해 쓰기 권한, 읽기 권한을 가졌는지를 명확하게 결정하는 제어 방식

Tajo: 타조, 하둡(Hadoop) 기반 데이터 웨어하우스 시스템

One Seg: 원 세그, 일본과 브라질에서 상용 중인 디지털 TV 방송 기술의 일종(주로 모바일 기기 대상)

Foursquare: 포스퀘어, 위치 기반 소셜 네트워크 서비스

Tensorflow: 텐서플로, 2015년 오픈소스로 공개된 구글 브레인 팀의 두 번째 기계 학습 시스템

PaaS-TA(Platform as a Service-올라타): 한국지능정보사회진흥회(NIA)가 지원하는 오픈소스 기반의 개방형 클라우드 컴퓨팅 플랫폼, 국내 IT 서비스 경쟁력 강화를 목표로 개발, 인프라 제어 및 관리 환경, 실행 환경, 개발 환경, 서비스 환경, 운영 환경으로 구성

정보 보안을 위한 접근 제어(Access Control)에 관련한 설명

적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것

시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트로 볼 수 있다

네트워크 장비에서 수행하는 IP에 대한 접근 제어는 관리 인터페이스의 접근 제어, ACL(Access Control List) 등 있다

틀린 것: DBMS에 보안 정책을 적용하는 도구인 XDMCP를 통해 데이터베이스에 대한 접근 제어를 수행할 수 있다

(XDMCP: X Display Manager Control Protocol, 사용자 인증이 완료되면 X 서버의 로그인 세션을 시작한다)

VLAN: Virtual Local Network, 물리적 배치와 상관없이 논리적으로 LAN을 구성하여 Broadcast Domain을 구분할 수 있게 해주는 기술로 접속된 장비들의 성능 향상 및 보안성 증대 효과가 있음

STP: Spanning Tree Protocol, 2개 이상의 스위치가 여러 경로로 연결될 때, 무한 루프 현상을 막기 위해서 우선순위에 따라 1개 경로로만 통신하도록 하는 프로토콜

ARP: Address Resolution Protocol, 네트워크 상에서 IP주소를 물리적 네트워크 주소로 대응(Bind)시키기 위해 사용, IP를 MAC 주소로 바인딩

SQL Injection(SQL 삽입) 공격과 관련한 설명

SQL Injection은 임의로 작성한 SQL 구문을 애플리케이션에 삽입, 내부 데이터베이스 서버의 데이터를 유출 및 변조하고, 관리자 인증을 우회하는 보안 약점 공격방식

SQL Injection 취약점이 발생하는 곳은 주로 웹 어플리케이션과 데이터베이스가 연동되는 부분이다

로그인과 같이 웹에서 사용자의 입력값을 받아 데이터베이스 SQL문으로 데이터를 요청하는 경우 SQL Injection을 수행할 수 있다

동적 쿼리에 사용되는 입력 데이터에 예약어 및 특수문자가 입력되지 않게 필터링 되도록 설정하여 방지 가능

틀린 것: DBMS의 종류와 관계없이 SQL Injection 공격 기법은 모두 동일하다

Software Defined Storage, SDS

가상화를 적용하여 필요한 공간만큼 나눠 사용할 수 있도록 하며 서버 가상화와 유사

컴퓨팅 소프트웨어로 규정하는 데이터 스토리지 체계이며 일정 조직 내 여러 스토리지를 하나처럼 관리하고 운용하는 컴퓨터 이용 환경

스토리지 자원을 효율적으로 나누어 쓰는 방법으로 이해할 수 있음

비용 산정 기법: Cocomo model, Putnam model, 기능 점수 모델

Cocomo model: LOC(Line of Code) 기반 비용 산정 방식

- Organic: 5만 라인 이하의 프로젝트에 적합, 소규모 팀이 개발에 사용

- Semidetached: 30만 라인 이하의 프로젝트에 적합, 트랜잭션 처리 시스템 등

- Embeded: 30만 라인 이상의 프로젝트에 적합, 하드웨어가 포함된 실시간 시스템 등

Putnam model: Rayleigh-Norden 곡선의 노력 분포도를 이용한 비용 산정 기법

기능 점수 모델: 기능 점수를 산출하여 비용 산정

폭포수 모형: 소프트웨어 생명주기 모형 중 Boehm이 제시, 고전적 생명주기 모형, 선형 순차적 모델, 타당성 검토/계획/요구사항 분석/설계/구현/테스트/유지보수의 단계를 통해 소프트웨어를 개발하는 모형

프로토타입 모델(Prototype Model): 발주자나 개발자 모두에게 공동의 참조 모델을 제공하여 사용자의 요구사항을 충분히 분석할 목적으로 시스템의 일부분 또는 시제품을 일시적으로 간결히 구현, 요구사항을 반영하는 개발 모델, 유지보수가 없어지고 개발 단계 안에서 유지보수가 이루어진다고도 볼 수 있다

나선형 모델(Spiral Model): 폭포수 프로토타입의 장점에 위험 분석 기능을 추가, 여러 번의 개발 과정을 거쳐 점진적으로 완벽한 SW를 개발하는 것, 비교적 대규모 시스템에 적합, 계획 및 정의 – 위험 분석 – 공학적 개발 – 고객 평가, 소프트웨어를 개발하면서 발생할 수 있는 위험을 관리하고 최소화하는 것을 목적으로 한다

ICMP(Internet Control Message Protocol): IP동작에서 네트워크 진단이나 제어 목적으로 사용

ICMP Flooding: 서비스 거부 DoS 공격의 방법, 스머프 공격(Smurf Attack)이라고 부름, Ping Flooding, SYN Flooding

Ping Flood: 특정 사이트에 매우 많은 ICMP Echo를 보내면, 이에 대한 응답(Respond)을 하기 위해 시스템 자원을 모두 사용해버려 시스템이 정상적으로 동작하지 못하도록 하는 공격 방법, 보내는 쪽의 네트워크 대역폭이 대상 시스템이 확보한 네트워크 대역폭보다 더 크면 됨,

SYN Flooding: 막대한 양의 TCP SYN 패킷을 대상 시스템으로 보내서 시스템을 마비시키는 공격 방법

MQTT(Message Queuing Telemetry Transport): IBM 개발, 발행/구독 프로토콜, TCP/IP를 통해 실행, 기본 네트워크 연결을 제공, IoT 환경에서 자주 사용, 사물통신/사물인터넷과 같이 대역폭이 제한된 통신환경에 최적화하여 개발된 푸시기술 기반의 경량 메시지 전송 프로토콜, 메시지를 매개자(Broker)를 통해 송신자가 특정 메시지를 발행하고 수신자가 메시지를 구독하는 방식, IBM이 주도하여 개발

MLFQ(Multi Level Feedback Queue, MFQ): 짧은 작업이나 입출력 위주의 프로세스에 우선순위를 부여하는 선점형 스케줄링 기법

Zigbee: 홈 네트워크 및 무선 센서망에서 사용되는 기술로 버튼 하나의 동작으로 집안 어느 곳에서나 전등 제어 및 홈 보안 시스템을 제어 관리하는 가정 자동화를 목표로 출발하였음

시스템 인증: 토큰 기반 인증, SSO 인증

토큰 기반 인증: 하드웨어와 소프트웨어의 토큰 장치를 사용하는 인증 기법, 하드웨어 장치는 스마트카드를 사용, 소프트웨어 장치는 개인 식별 번호를 사용하는 강력한 인증 방법

SSO(Single Sign On): 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면 다른 시스템에 대한 접근 권한도 얻는 시스템

Hash, Encryption

Hash: 단방향, 복호화 불가능

Encryption: 양방향, 역으로 복호화 가능

패스워드는 보통 단방향 Hash를 기본으로 저장

문제점: 같은 패스워드를 Hashing하면 같은 결과값이 나타나게 되고 이는 문제를 발생

해결법: 다른 암호값으로 저장되도록 추가되는 값 = Salt

상향식 비용 산정 기법

LOC 기법: 원시 코드 라인 수(Source Line of Code)의 비관치, 낙관치, 기대치를 측정, 예측치 구함

Effort Per Task: LOC기법을 보완, 각 기능을 구현시키는데 필요한 노력을 생명 주기의 각 단계별로 산정

하향식 비용 산정 기법

전문가 감정 기법: 두 명 이상의 전문가에게 비용 산정을 의뢰하는 기법, 개인적이고 주관적

델파이 기법: 전문가 감정 기법의 주관적인 편견 보완, 한 명의 조정자와 여러 전문가의 의견을 종합하여 산정

OWASP(The Open Web Application Security Project): 오픈소스 웹 어플리케이션 보안 프로젝트, 주로 웹에 관한 정보 노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구

SAN: 네트워크상에 광채널 스위치의 이점인 고속 전송과 장거리 연결 및 멀티 프로토콜 기능을 활용, 각기 다른 운영체제를 가진 여러 기종들이 네트워크상에서 동일 저장장치의 데이터를 공유하게 함으로써, 여러 개의 저장장치나 백업 장비를 단일화시킨 시스템

MBR: Memory Buffer Register, 기억장치를 출입하는 데이터가 잠시 기억되는 레지스터

NAC: Network Access Control, PC의 MAC 주소를 IP관리 시스템에 등록, 일관된 보안 관리 기능을 제공

NIC: 물리 계층과 데이터 계층의 서비스를 제공

SSH(Secure Shell)에 대한 설명

전송되는 데이터는 암호화된다

키를 통한 인증은 클라이언트의 공개키를 서버에 등록해야 한다

서로 연결되어 있는 컴퓨터 간 원격 명령 실행이나 셀 서비스 등을 수행한다

틀린 것: SSH의 기본 네트워크 포트는 220번을 사용한다(22번을 사용한다)

CBD(Component Based Development) SW 개발 표준 산출물

기존의 시스템이나 소프트웨어를 구성하는 컴포넌트를 조합하여 하나의 새로운 애플리케이션을 만드는 방법론

생산성과 품질을 높이고, 유지보수 비용을 최소화할 수 있다

컴포넌트 제작 기법을 통해 재사용성을 향상시킨다

독립적인 컴포넌트 단위의 관리로 복잡성을 최소화할 수 있다

개발 공정

개발준비 – 분석 – 설계 – 구현 – 테스트 – 전개 – 인도

요구파악 단계: 요구사항 기술서, 용어 사전, 개념 모델, 유스케이스 모델

분석 및 설계: 객체 모델, UI설계서, 아키텍쳐 기술서, 인터페이스 명세서, 컴포넌트 명세서/설계서, DB 설계서

구현: 개발 표준 정의서, 플랫폼 종속적 코드

테스트: 테스트 계획서, 컴포넌트 테스트 보고서, 통합 테스트 보고서, 인수 테스트 보고서

Bell-Lapadula Model: BLP, 군대의 보안 레벨처럼 정보의 기밀성에 따라 상하 관계가 구분된 정보를 보호하기 위해 사용, 자신의 권한보다 낮은 보안 레벨 권한을 가진 경우에는 높은 보안 레벨의 문서를 읽을 수 없고 자신의 권한보다 낮은 수준의 문서만 읽을 수 있다, 자신의 권한 보다 높은 보안 레벨의 문서에는 쓰기가 가능하지만 보안 레벨이 낮은 문서의 쓰기 권한은 제한된다, 정보의 불법적인 파괴나 변조보다는 불법적인 비밀 유출 방지에 중점, 기밀성

Clark-Wilson Integrity Model: 비밀 노출 방지보다 자료의 변조 방지가 더 중요함(금융, 회계, 데이터, 기업 재무재표)

Chinese Wall: 충돌을 야기시키는 어떠한 정보의 흐름도 없어야 한다, 이익의 충돌 금지, 최근 일을 한 적이 있는 파트너는 동일 영역에 있는 다른 회사 자료에 접근해서는 안된다

Sqoop: 하둡(Hadoop)과 관계형 데이터베이스 간에 데이터를 전송할 수 있도록 설계된 도구, 커넥터를 사용하여 관계형 데이터베이스 시스템(RDBMS)에서 HDFS로 데이터를 수집하는 빅데이터 기술

라우팅 프로토콜인 OSPF(Open Shortest Path First)에 대한 설명

네트워크 변화에 신속하게 대처할 수 있다

멀티캐스팅을 지원한다

최단 경로 탐색에 Dijkstra 알고리즘을 사용한다

틀린 것: 거리 벡터 라우팅 프로토콜이라고 한다(RIP, 링크 상태 알고리즘을 사용)

소프트웨어 비용 추정 모델(Estimation Models)

COCOMO: 시스템의 비용을 산정하기 위해 시스템을 구성하고 있는 모듈과 서브 시스템의 비용 합계를 계산

Putnam: 소프트웨어 개발 주기의 각 단계별로 요구할 인력의 분포를 가정하는 모델

Function-Point(FP): 요구 기능을 증가시키는 인자별로 가중치를 부여하여 기능의 점수를 계산하여 비용을 산정

틀린 것: PERT; 계획 평가 및 재검토 기술, 프로젝트 관리를 분석하거나 주어진 완성 프로젝트를 포함한 일을 묘사하는데 쓰이는 모델

Error

사본/필사 오류(Transcription Error): 작업자나 광 문자 인식(OCR) 프로그램에서 발생하는 데이터 입력 오류, 임의의 한 자리를 잘못 기록한 경우(1234 -> 1235)

생략 오류(Omission Error): 입력 시 한 자리를 빼놓고 기록한 경우(1234 -> 124)

전위 오류(Transposition Error): 입력 시 좌우 자리를 바꾸어 기록한 경우(1234 -> 1243)

이중 오류(Double Transposition Error): 전위 오류가 두 가지 이상 발생한 경우(1234 -> 2143)

추가 오류(Addition Error): 입력 시 한 자리 추가로 기록한 경우(1234 -> 12345)

임의 오류(Random Error): 위의 오류가 두 가지 이상 결합하여 발생한 경우(1234 -> 13245)

ISO 12207 표준의 기본 생명주기의 주요 프로세스

기본 생명주기 프로세스: 획득, 공급, 개발, 운영, 유지보수

지원 생명주기 프로세스: 품질 보증, 검증, 확인, 활동 검토, 문제 해결 프로세스

조직 생명주기 프로세스: 관리, 기반구조, 훈련, 개선 프로세스

SPICE 모델

수준 0부터 수준 5까지 총 6개 수준

0단계: 불안정(구현 전 or 목적 달성 전)

1단계: 수행(목적이 전반적으로 이루어짐)

2단계: 관리(작업 산출물 인도)

3단계: 확립(공학 원칙을 지킴)

4단계: 예측(산출물의 양적 측정이 가능해져, 일관된 수행 가능)

5단계: 최적화(지속적으로 업무 목적 만족)

N-Screen: N개의 서로 다른 단말기에서 동일 컨텐츠를 자유롭게 이용 가능한 서비스

Memristor: Memory + Register, 전원 공급이 끊어져도 다시 전원이 공급되면 이전 상태 복원

MEMS: 센서, 엑추에이터 등 기계구조를 다양한 기술로 미세 가공 후 전기기계적 동작이 가능케 한 초 미세장치

SNMP: 하드웨어 신기술 아님, 간이 망 관리 프로토콜

해쉬(Hash) 기법에 대한 설명

임의의 길이의 입력 데이터를 받아 고정된 길이의 해쉬값으로 변환

대표적인 해쉬 알고리즘으로 HAVAL, SHA-1 등이 있다

해쉬 함수는 일방향(One-Way Function) 이다

틀린 것: 주로 공개키 암호화 방식에서 키 생성을 위해 사용한다

암호화 방식

단방향

해시

SHA, SHA-1, MD4, MD5, N-NASH, SNEFRU 등

특징: 임의의 길이의 입력 데이터나 메시지를 고정 길이의 값이나 키로 변환, 암호화, 무결성 검증을 위해 사용

양방향

개인키(암호화, 복호화 시 동일한 개인키를 이용, 대칭, 단일키)

Stream 방식:

평문과 동일한 길이의 스트림을 생성하여 비트 단위로 암호화, LFSR, RC4

비트/바이트/단어들을 순차적으로 암호화

Block 방식: 한 번에 하나의 데이터 블록을 암호화, DES, SEED, AES, ARIA

특징: 암호화/복호화 속도가 빠르며, 알고리즘이 단순, 공개키 암호 기법보다 파일 크기가 작음, 사용자의 증가에 따라 관리해야 할 키의 수가 상대적으로 많아진다

공개키(암호화 시 사용자에게 공개되는 공개키 사용, 복호화 시 비밀키 사용, 비대칭 암호 기법)

복호화키는 비공개

송신자는 수신자의 공개키로 문서를 암호화

비밀키(대칭키)는 N(N-1)/2 이고, 공개키(비대칭키)는 2N개 이다(N: 인원 수)

RSA(소인수분해), ECC(타원곡선), EIGAMAI(이산대수)

특징: 키의 분배가 용이하고, 관리해야 할 키 수가 적음, 암호화/복호화 속도가 느리며 알고리즘이 복잡, 개인키 암호화 방법보다 파일의 크기가 큼

IPSec(IP Security)에 대한 설명

ESP는 발신지 인증, 데이터 무결성, 기밀성 모두를 보장한다

운영 모드는 Tunnel 모드와 Transport 모드로 분류된다

AH는 발신지 호스트를 인증하고, IP 패킷의 무결성을 보장한다

틀린 것: 암호화 수행 시 일방향 암호화만 지원한다(일방향 암호화는 해시 암호화)

IPSec: IP계층(3계층)에서 무결성과 인증을 보장하는 인증 헤더와 기밀성을 보장하는 암호화를 이용해 양 종단 구간에 보안 서비스를 제공하는 터널링 프로토콜

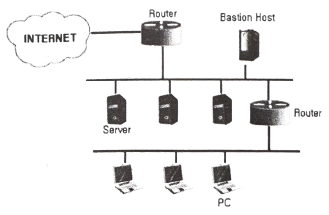
IKE(Internet Key Exchange): 보안 관련 설정들을 생성, 협상 및 관리하는 프로토콜(UDP 500번 포트 사용)

ESP(Encapsulating Security Payload): 메시지 인증코드, 암호화 이용 인증(무결성), 발신지 인증, 기밀성 제공 프로토콜

AH(Authentication Header): 기밀성 제외, 메시지 인증 코드를 이용해 인증(무결성), 발신지 인증 제공 프로토콜

Stack Guard: 메모리 상에서 프로그램의 복귀 주소와 변수 사이에 특정 값을 저장해 두었다가 그 값이 변경되었을 경우 오버플로우 상태로 가정하여 프로그램 실행을 중단하는 기술

ASLR(Address Space Layout Randomization): 프로그램을 실행할 때 마다 스택, 힙, 공유 라이브러리 등을 메모리에 적재할 때 주소를 랜덤화 시키는 기법으로, 공격자로 하여금 메모리 상의 주소를 추측하기 어렵게 한다



스크린 서브넷(Screen Subnet): 외부 네트워크와 내부 네트워크 사이에 두는 완충적인 통신망

Secure OS 기능

식별 및 인증, 계정 관리

강제적 접근 통제

임의적 접근 통제

객체 재사용 방지

완전한 중재 및 조정

감사 및 감사기록 축소

안전한 경로

보안 커널 변경 방지

해킹 방지(Anti-Hacking)

통합 관리

nmap: 서버에 열린 포트 정보를 스캐닝해서 보안취약점을 찾는데 사용하는 도구

mkdir: 디렉토리를 생성하는 리눅스 명령어

ftp: 응용계층 프로토콜

라우터: 브리지와 같이 LAN과 LAN의 연결 기능에 데이터 전송의 최적 경로를 선택할 수 있는 기능이 추가된 것, 서로 다른 LAN이나 LAN과 WAN의 연결도 수행, 3계층(네트워크)까지의 프로토콜 구조가 다른 네트워크 간의 연결을 위해 프로토콜 변환 기능을 수행

Trip Wire: 리눅스 시스템을 외부의 크래커 공격과 내부의 악의적인 사용자의 공격으로부터 시스템을 지켜내는 역할을 하는 프로그램, 크래커가 침입하여 백도어를 만들어 놓거나 설정 파일을 변경했을 때 분석하는 도구

Tcpdump: 컴퓨터에 부착된 네트워크를 통해 송수신되는 기타 패킷을 가로채고 표시할 수 있게 도와주는 SW

Cron: 스케쥴러를 실행시키기 위해 작업이 실행되는 시간 및 주기 등을 설정, ()표현식을 통해 배치 수행시간을 설정

Netcat: TCP 또는 UDP를 사용하여 네트워크 연결을 읽고 쓰는데 사용되는 컴퓨터 네트워킹 유틸리티

방법론

구조적 방법론: 정형화된 분석절차에 따라 사용자 요구사항을 파악하여 문서화하는 처리 중심의 방법론, 분할, 정복

객체지향 방법론: 현실 세계의 개체를 기계의 부품처럼 하나의 객체로 만들어 소프트웨어를 개발할 때 기계의 부품을 조립하듯이 객체들을 조립해서 필요한 소프트웨어를 구현하는 방법론

정보공학 방법론: 정보 시스템의 개발을 위해 계획, 분석, 설계, 구축에 정형화된 기법들을 상호 연관성 있게 통합 및 적용하는 자료중심의 방법론

컴포넌트기반 방법론: 기존의 시스템이나 소프트웨어를 구성하는 컴포넌트를 조합하여 하나의 새로운 애플리케이션을 만드는 방법론

암호화에 대한 설명

평문: 암호화되기 전의 원본 메시지

암호문: 암호화가 적용된 메시지

복호화: 암호문을 평문으로 바꾸는 작업

키: 적절한 암호화를 위하여 사용하는 값

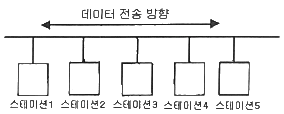
OTT(Over The Top): 개방된 인터넷을 통해 방송프로그램, 영화 등 미디어 컨텐츠를 제공하는 서비스

SDDC(Software Defined Data Center): 데이터 센터의 모든 자원이 가상화되어 서비스되고, 소프트웨어 조작만으로 자동 제어 관리되는 데이터 센터

Wi-SUN: 스마트 그리드와 같은 장거리 무선 통신을 필요로 하는 사물 인터넷(IoT) 서비스를 위한 저전력 장거리(Low-Power Wide Area, LPWA) 통신 기술

Baas: 블록체인 개발환경을 클라우드로 서비스하는 개념, 블록체인 네트워크에 노드의 추가 및 제거가 용이, 블록체인의 기본 인프라를 추상화하여 블록체인 응용프로그램을 만들 수 있는 클라우드 컴퓨팅 플랫폼

LAN 네트워크 토폴로지



버스 스테이션: 버스가 정거장을 들리듯 데이터가 전송됨

스마트 그리드: 전기의 생산, 운반, 소비 과정에 정보통신 기술을 접목하여 공급자와 소비자가 서로 상호작용함으로써 효율성을 높인 지능형 전력망 시스템, 전기 및 정보통신 기술을 활용하여 전력망을 지능화, 고도화 함으로써 고품질의 전력 서비스를 제공하고 에너지 이용효율을 극대화하는 전력명

디지털 아카이빙: 지속적으로 보존할 가치를 가진 디지털 객체를 장기간 관리하여 이후의 이용을 보장하는 활동

세션 하이재킹 탐지 방법

비동기화 탐지: 서버와 시퀀스 넘버를 주기적으로 탐지, 비동기 상태 탐지

Ack Storm 탐지: 급격한 ACK 비율 증가 시 탐지

패킷의 유실 및 재전송 증가 탐지: 공격자가 중간에 끼어서 작동하므로 패킷의 유실과 서버와의 응답이 길어짐

소프트웨어 공학에 대한 설명

소프트웨어공학이란 소프트웨어의 개발, 운용, 유지보수 및 파기에 대한 체계적인 접근 방법

소프트웨어공학은 소프트웨어 제품의 품질을 향상시키고 소프트웨어 생산성과 작업 만족도를 증대시키는 것이 목적

소프트웨어공학의 궁극적 목표는 최소 비용으로 계획된 일정보다 가능한 빠른 시일 내에 소프트웨어를 개발하는 것

소프트웨어공학은 신뢰성 있는 소프트웨어를 경제적인 비용으로 획득하기 위해 공학적 원리를 정립하고 이를 이용하는 것

Logic Bomb: 프로그램에 어떤 조건이 주어져 숨어있던 논리에 만족되는 순간 폭탄처럼 자료나 소프트웨어를 파괴, 자동으로 잘못된 결과가 나타나게 한다

Cyberbullying: 사이버 상에서 특정인을 집단적으로 따돌리거나 집요하게 괴롭히는 행위

Evil Twin Attack, Phishing: 소셜 네트워크에서 악의적인 사용자가 지인 또는 특정 유명인으로 가장하여 활동하는 공격 기법