1. 소프트웨어 개발 보안 설계

* 소프트웨어 개발 보안 설계

1. SW 개발 보안의 개념

소스 코드 등에 존재하는 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동을 말한다

요구사항 명세 -> 설계 -> 구현 -> 테스트 -> 유지 보수

1. SW 개발 보안의 구성요소

정보보안의 세 가지 요소인 기밀성, 무결성, 가용성을 지키고 서버 취약점을 사전에 방지하여 위협으로부터 위험을 최소화 하는 구축 방법

1. SW 개발 보안의 3대 요소

* 기밀성 : 인가되지 않은 개인 혹은 시스템 접근에 따른 정보 공개 및 노출을 차단하는 특성, 인가된 사용자에 대해서만 자원 접근이 가능해야 하는 특성
* 무결성 : 정당한 방법을 따르지 않고선 데이터가 변경될 수 없으며, 데이터의 정확성 및 완전성과 고의/악의로 변경되거나 훼손 또는 파괴되지 않음을 보장하는 특성, 인가된 사용자에 대해서만 자원 수정이 가능하며 전송 중인 정보는 수정되지 않아야함
* 가용성 : 권한을 가진 사용자나 애플리케이션이 원하는 서비스를 지속 사용할 수 있도록 보장하는 특성, 인가된 사용자는 가지고 있는 권한 범위 내에서 언제든 자원 접근이 가능해야 하는 특성

1. SW 개발 보안 용어

* 자산 : 조직의 데이터 또는 조직의 소유자가 가치를 부여한 대상
* 위협 : 조직이나 기업의 자산에 악영향을 끼칠 수 있는 사건이나 행위
* 취약점 : 위협이 발생하기 위한 사전 조건으로 시스템의 정보 보증을 낮추는데 사용되는 약점
* 위험 : 위협이 취약점을 이용하여 조직의 자산 손실 피해를 가져올 가능성

1. SW 개발 보안을 위한 공격기법의 이해
2. DoS 공격

* 개념

시스템을 악의적으로 공격해서 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격

특정 서버에 수많은 접속 시도를 만들어 다른 이용자가 정상적으로 서비스 이용을 하지 못하게 하거나 서버의 TCP 연결을 소진 시키는 등의 공격이다

* 종류

SYN 플러딩 : TCP 프로토콜의 구조적인 문제를 이용한 공격, 서버의 동시 가용 사용자 수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용 불가능하게 하는 공격

UDP 플러딩 : 대량의 UDP 패킷을 만들어 임의의 포트 번호로 전송하여 응답 메시지 ICMP 를 생성하게 하여 지속해서 자원을 고갈 시키는 공격

스머프 / 스머핑 : 출발지 주소를 공격 대상의 IP로 설정하여 네트워크 전체에게 ICMP Echo 패킷을 직접 브로드캐스팅하여 마비시키는 공격

죽음의 핑 : ICPM 패킷을 정상적인 크기보다 아주 크게 만들어 전송하면 다수의 IP 단편화가 발생하고, 수신 측에서는 단편화된 패킷을 처리 하는 과정에서 많은 부하가 발생하거나, 재조합 버퍼의 오버플로가 발생하여 정상적인 서비스를 하지 못하도록 하는 공격 기법

랜드 어택 : 출발지 IP 와 목적지 IP 를 같은 패킷 주소로 만들어 보냄으로써 수신자가 자기 자신에게 응답을 보내게 하여 시스템의 가용성을 침해하는 공격기법

티어 드롭 : IP 패킷의 재조합 과정에서 잘못된 Fragment Offset 정보로 인해 수신시스템이 문제를 발생하도록 만드는 DoS 공격

공격자는 IP Fragment Offset 값을 서로 중첩되도록 조작하여 전송하고, 이를 수신한 시스템이 재조합하는 과정에서 오류가 발생, 시스템의 기능을 마비시키는 공격 방식

봉크 : 패킷을 분할하여 보낼 때 처음 패킷을 1번으로 보낸 후 다음 패킷을 보낼 때도 순서번호를 모두 1번으로 조작하여 전송하는 DoS 공격

보잉크 : 처음 패킷을 1번으로 보낸 후 다음 패킷을 100번, 다음 패킷을 200번, 20번째 패킷을 2002번, 21번째 패킷을 100번, 22번째 패킷을 다시 2002번 등으로 중간에 패킷 시퀀스 번호를 비정상적인 상태로 보내서 부하를 일으키게 하는 공격 기법

1. DDoS 공격

DDoS는 DoS의 또 다른 형태로 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트를 공격하는 기법이다

해커들이 취약한 인터넷 시스템에 대한 액세스가 이뤄지면, 침입한 시스템에 소프트웨어를 설치하고 이를 실행시켜 원격에서 공격을 개시한다

DDoS 공격 구성 요소

* 핸들러 : 마스터 시스템의 역할을 수행하는 프로그램
* 에이전트 : 공격 대상에 직접 공격을 가하는 시스템
* 마스터 : 공격자에게서 직접 명령을 받는 시스템
* 공격자 : 공격을 주도하는 해커의 컴퓨터
* 데몬 프로그램 : 에이전트 시스템의 역할을 수행하는 프로그램

1. DRDoS 공격

공격자는 출발지 IP를 공격대상 IP로 위조하여 다수의 반사 서버로 요청 정보를 전송, 공격 대상자는 반사 서버로부터 다량의 응답을 받아서 서비스 거부가 되는 공격

출발지 IP 변조 -> 공격 대상자 서버로 응답 -> 서비스 거부

1. 세션 하이재킹

케빈 미트닉이 사용했던 공격 방법 중 하나로 TCP의 세션 관리 취약점을 이용한 공격 기법

비동기화 상태 탐지 -> ACK 패킷 비율 모니터링 -> 특정 세션에서 패킷 유실 및 재전송이 증가되는 것을 탐지 -> 기대하지 않은 접속의 리셋 탐지

1. 애플리케이션 공격

* HTTP GET 플러딩

과도한 Get 메시지를 이용하여 웹 서버의 과부하를 유발 시키는 공격

* Slowloris

HTTP GET 메서드를 사용하여 헤더의 최종 끝을 알리는 개행 문자열 \r\n\r\n을 전송하지 않고 \r\n 만 정송하여 대상 웹 서버와 연결상태를 장시간 지속

* RUDY Attack

요청 헤더의 Context-Lenght 를 비정상적으로 크게 설정하여 메시지 바디 부분을 매우 소량으로 보내 계속 연결상태를 유지시키는 공격

* Show Read Attack

TCP 윈도 크기를 낮게 설정하여 서버로 전달하고, 해당 윈도 크기를 기준으로 통신하면서 데이터 전송이 완료될 때까지 연결을 유지하게 만들어 서버의 연결 자원을 고갈 시키는 능력

* Hulk DoS

공격자가 공격대상 웹 사이트 웹 페이지 주소를 지속적으로 변경하면서 다량으로 GET 요청을 발생시키는 서비스 거부 공격

* Hash DoS

공격자가 HTTP POST 메서드를 사용하여 많은 수의 파라미터를 서버에 전달 하면 파라미터를 관리하는 해시테이블에서 해시 충돌이 발생하도록 하여 서버 자원 고갈

1. 네트워크 공격

* 스니핑 : 공격대상에게 직접 공격을 하지 않고 데이터만 몰래 들여다보는 공격
* 네트워크 스캐너, 스니퍼 : 네트워크 하드웨어 및 소프르웨어 구성의 취약점 파악을 위해 공격자가 취약점을 탐색하는 공격 도구
* 패스워드 크래킹 : 사전 크래킹 공격, 무차별 크래킹 공격, 패스워드 하이브리드 공격, 레인보우 테이블 공격
* IP 스푸핑 : 침임자가 인증된 컴퓨터 시스템인 것 처럼 속여 타깃 시스템의 정보를 빼내기 위해서 본인의 패킷 헤더를 인증된 호스트의 IP 어드레스로 위조하여 타깃에 전송하는 공격 기법
* ARP 스푸핑 : 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply를 만들어 희생자에게 지속적으로 전송하여 희생자의 ARP Cache Table에 특정 호스트의 MAC 정보를 공격자의 MAC 정보로 변경, 희생자로부터 특정 호스트로 나가는 패킷을 공격자가 스니핑 하는 공격 기법
* ICMP Redirect : 3계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격기법
* 트로이 목마 : 악성 루틴이 숨어 있는 프로그램으로 겉보기에는 정상적인 프로그램으로 보이지만 실행하면 악성 코드를 실행

1. 시스템 보안 위협

* 버퍼 오버플로 공격

스택 버퍼 오버플로 : 메모리 영역 중 Local Value 나 함수의 Return Address 가 저장되는 스택 영역에서 발생하는 오버플로 공격

힙 버퍼 오버플로 : 프로그램 실행 시 동적으로 할당되는 힙 영역에 할당된 버퍼 크기를 초과하는 데이터를 입력하여 메모리의 데이터와 함수 주소 등을 변경

* 접근 통제 보호 모델

벨-라파듈라 모델 : 미 국방부 지원 보안 모델로 보안 요소 중 기밀성을 강조하며 강제적 정책에 의해 접근 통제하는 모델

비바 모델 : 벨-라파듈라 모델의 단점을 보완한 무결성을 보장하는 최초의 모델

* 3A : 유 무선 이동 및 인터넷 환경에서 가입장에 대한 안전하고 신뢰성 있는 인증, 권한 부여, 계정 관리를 체계적으로 제공하는 정보 보호 기술

인증, 권한 부여, 계정관리

* 인증 관련 기술

SSO : 커버로스에서 사용되는 기술로 한 번의 인증 과정으로 여러 컴퓨터상의 자원을 이용

커버로스 : 1980년대 중반 MIT의 Athena 프로젝트의 일환으로 개발되었으며 클라이언트/서버 모델에서 동작하고 대칭 키 암호기법에 바탕을 둔 티켓 기반 프로토콜

OAuth : 사용자가 비밀번호를 제공하지 않고 다른 웹사이트나 애플리케이션의 접근권한을 부여

1. SW 개발 보안을 위한 암호화 알고리즘

대칭키 : DES, AES, SEED

비대칭 키 : 디피-헬만, RSA

일방향 암호 방식 ( 해시 암호 방식 )

임의 길이의 정보를 입력받아, 고정된 길이의 암호문을 출력

* MAC : 키를 사용하는 메시지 인증 코드로 메시지의 정당성을 검증하기 위해 메시지와 함께 전송
* MDC 키를 사용하지 않는 변경 감지 코드로 수신자는 받은 데이터로부터 새로운 MDC 를 생성하여 송신자에게 받은 MDC와 비교하여 변경되지 않음을 보장

암호 알고리즘 상세

대칭키 암호화 알고리즘

* DES : 1975년 IBM에서 개발하고 미국의 연방 표준국 NIST 에서 발표한 대칭 키 기반 블록 암호화 알고리즘 DES를 3번 적용하여 보안을 더욱 강화항 3 DES도 활용됨
* SEED : 1999년 국내 한국인터넷진흥원이 개발 128BIT 비밀키로부터 생성된 16개의 64BIT 라운드 키를 사용하여 총 16회의 라운드를 거쳐 평문 블록을 ㅎ암호문 블록으로 암호화
* AES : 2001년 미국 표준 기술 연구소에서 발표한 블록 암호화 알고리즘, DES의 개인 키에 대한 전사적 공격이 가능해지고 3 DES 의 성능 문제르 극복하기 위해 개발
* ARIA : 2004년 국가정보원과 산학연구협회가 개발
* IDEA : DES 를 대체하기 위해 개발
* LFSR : 시프트 레지스터의 일종
* SkipJack : 미 국가안보국 NSA 에서 개발

비대칭 키 암호화 알고리즘

디피-헬만, RSA, ECC, EIGamal

해시 암호화 알고리즘

MD5, SHA-1, SHA-256, HAS-160, HAVAL

데이터베이스 암호화 기법

* API : 애플리케이션 레벨에서 암호 모듈을 적용
* Plug-In : 암 복호화 모듈이 db 서버에 설치
* TDE : db 서버의 DBMS 커널이 자체적으로 암 복호화 기능 수행
* Hybrid : API, Plug-In 방식 혼합

1. 안전한 전송을 위한 데이터 암호화 전송

* PPTP : 마이크로소프트사가 개발한 프로토콜, PPP에 기초하여 두대의 컴퓨터가 직렬 인터페이스를 이용하여 통신할때 사용
* L2F : 시스코사에서 개발한 프로토콜로 하나의 터널에 여러개의 연결을 지원하여 다자간 통신이 가능하도록 하는 프로토콜
* L2TP : L2F + PPTP 호환성이 뛰어나다
* IPSec : IP 계층 에서 무결성과 인증을 보장하는 인증 헤더와 기밀성을 보장하는 암호화 ESP 를 이용한 IP 보안 프로토콜

기밀성, 비 연결형 무결성, 인증

전송 모드와 터널 모드가 있다 전송모드는 IP 상위 프로토콜 데이터를 보호 터널 모드는 IP 패킷 전체를 보호