9. 소프트웨어 개발 보안 구축

SW 개발 보안의 3대 요소

- 기밀성(Confidentiality) : 인가되지 않은 개인 혹은 시스템 접근에 따른 정보 공개 및 노출을 차단하는 특성
- 무결성(Integrity) : 정당한 방법을 따르지 않고서는 데이터가 변경 될 수 없으며, 데이터의 정확성 및 완전성과 고의/악의로 변경되거나 훼손되지 않음을 보장하는 특성
- 가용성(Availability) : 권한을 가진 사용자나 애플리케이션이 원하는 서비스를 지속해서 사용할 수 있도록 보장하는 특성

*DoS(Denial of Service) _공격자 컴퓨터 1대, 직접 공격

시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 해 사용하지 못하게 하는 공격

DoS 공격 종류

- SYN 플러딩(Flooding) : 서버의 동시 가용 사용자 수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용하지 못하게 하는 공격
- UDP 플러딩(Flooding) : 대량의 UDP패킷을 만들어 임의의 포트 번호로 전송하여 지속적으로 자원을 고갈시키는 공격
- 스머프(Smurf)/스머핑(Smurfing) : 출발지 주소를 공격 대상의 IP로 설정하여 네트워크 전체에게 ICMP Echo 패킷을 직접 브로드캐스팅하여 마비시킴
- 죽음의 핑(PoD; Ping of Death) : ICMP 패킷(Ping)을 정상적인 크기보다 아주 크게 만들어서 전송
- 랜드어택(Rand Attack) : 출발지 IP와 목적지 IP를 같은 패킷 주소로 만들어 보내서 수신자가 자기 자신에게 응답을 보내게 함
- 티어드롭(Tear Drop) : IP 패킷의 재조합 과정에서 잘못된 Fragment Offset 정보로 인해 수신 시스템이 문제를 발생하도록 만드는 공격
- 봉크(Bonk)/보잉크(Boink) : 시스템의 패킷 재전송과 재조립이 과부하를 유발하게 하는 공격기법

*DDos(Distributed DoS)_공격자가 여러 대의 컴퓨터를 감염 시킴, 공격 지시

여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트 공격

DDoS 공격 도구

- Trinoo : 많은 소스로부터 통합된 UDP flood 서비스 거부 공격을 유발하는데 사용
- TFN(Tribe Flood Network) : Trinoo와 비슷한 분산 도구, 많은 소스에서 하나 혹은 여러 개의 목표 시스템에 대해 서비스 거부 공격
- Stacheldraht : 분산 서비스 거부 에이전트 역할

DRDoS(Distributed Refleection DoS)

공격자는 출발지 IP를 공격대상 IP로 위조하여 다수의 반사 서버로 요청 정보를 전송,

공격 대상자는 반사 서버로부터 다량의 응답을 받아서 서비스 거부(DoS)가 되는 공격이다.

애플리케이션 공격

- HTTP GET Flooding : 과도한 GET 메시지를 이용해 웹 서버의 과부하를 유발시키는 공격
- Slowloris(Slow HTTP Header DoS) : HTTP GET 메서드를 사용해 헤더의 최종 끝을 알리는 개행 문자열을 전송하지 않음
- RUDY(Slow HTTP POST DoS) : 요청 헤더의 Content-length를 비정상적으로 크게 설정하고 메시지 바디 부분을 매우 소량을 보내 계속 연결상태 유지시키는 공격 (999999 설정 이후 1바이트씩 전송)
- Slow HTTP Read DoS : TCP 윈도 크기와 데이터 처리율을 감소시킨 상태에서(Zero Window Packet) 다수 HTTP 패킷을 지속적으로 전송
- Hulk DoS : 공격자가 공격대상 웹사이트 URL을 지속적으로 변경하면서 다량으로 GET 요청을 발생시키는 서비스 거부 공격
- Hash DoS : 조작된 많은 수의 파라미터를 POST방식으로 웹 서버로 전달하여 다수의 해시 충돌 발생시키는 공격

네트워크 공격

- 스니핑(Sniffing) : 직접 공격을 하지 않고 데이터만 몰래 들여다보는 수동적 공격
- 네트워크 스캐너(Scanner), 스니퍼(Sniffer) : 네트워크 하드웨어, 소프트웨어 구성의 취약점을 탐색하는 공격 도구
- 패스워드 크래킹(Password Cracking)
  - 사전 크래킹(Dictionary) : ID와 패스워드가 될 가능성이 있는 단어를 파일로 만들어 놓음
  - 무차별 크래킹(Brute): 패스워드로 사용될 수 있는 글자를 무작위로 패스워드 자리에 대입
  - 패스워드 하이브리드 공격 : 사전 + 무차별

    - 레인보우 테이블 공격 : 패스워드 별로 해시 값을 미리 생성해서 역으로 패스워드를 찾음
- IP 스푸핑 : 침입자가 인증된 컴퓨팅 시스템인 것처럼 속이기 위해서 본인의 패킷 헤더를 인증된 호스트의 IP로 위조하여 타깃에 전송
- ARP 스푸핑 : 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply를 만들어 특정 호스트의 MAC 정보를 공격자의 MAC정보로 변경
- ICMP Redirect : 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꿈, Redirect 메시지를 공격자가 원하는 형태로 만들어서 공격
- 트로이 목마 : 겉보기에는 정상적인 프로그램으로 보이지만 실행하면 악성 코드를 실행하는 프로그램

시스템 보안 위협

- 버퍼 오버플로우(Buffer Overflow) : 메모리에 할당된 버퍼크기를 초과하는 양의 데이터를 입력해 공격
    - 유형 : 스택 버퍼 오버플로우, 힙 버퍼 오버플로우
    - 대응방안
        - 스택가드(Stack guard) : 버퍼 오버플로우 발생 시 카나리 값을 체크
        - 스택쉴드(Stack Shield) : 함수 시작 시 복귀 주소를 Global RET에 저장해두고 함수 종료 시 저장된 값과 스택의 RET값을 비교해서 다를 경우 프로그램 중단
        - ASLR(Address Space Layout Randomization) : 주소 공간 배치를 난수화, 리눅스에서 설정 가능
- 백도어 : 어떤 제품이나 컴퓨터 시스템, 암호시스템, 알고리즘에서 정상적인 인증 절차를 우회하는 기법
- 주요 시스템 보안 공격기법
    - 포맷 스트링 공격 : 외부로부터 입력된 값을 검증하지 않고 그대로 사용하는 경우 발생하는 취약점 공격법
    - 레이스 컨디션 공격 : 실행되는 프로세스가 임시파일을 만드는 경우 악의적인 프로그램을 통해 그 프로세스의 실행 중에 끼어들어 임시파일을 심볼릭 링크하는 공격기법
    - 키로거 공격 : 사용자의 키보드 움직임을 탐지해서 개인의 중요한 정보를 몰래 빼가는 해킹공격
    - 루트킷 : 시스템 침입 후 사실을 숨긴 채 차후의 침입을 위해 불법적인 해킹기능을 제공하는 프로그램(트로이 목마, 백도어..)의 모음

보안 관련 용어

- 스피어피싱(Spear Phishing) : 메일을 이용한 공격
- 스미싱(Smishing) : 문자메시지를 이용한 공격
- 큐싱(Qushing) : QR코드

- APT 공격(Advanced Persistent Threat) : 특정 타깃을 목표로 하여 다양한 수단을 통해 지속적이고 지능적인 맞춤형 공격기법
- 공급망 공격(Supply Chain Attack) : 소프트웨어 개발사의 네트워크에 침투하여 소스 코드를 수정하여 악의적인 코드를 삽입해 공격
- 제로데이 공격(Zero Day Attack) : 보안 취약점이 발견되어 널리 공표되기 전에 해당 취약점을 악용하여 공격
- 웜 : 스스로를 복제하여 네트워크로 전파하는 악성 소프트웨어 컴퓨터 프로그램
- 악성 봇(Malicious Bot) : 스스로 실행되지 못하고 해커에 의해 제어, 실행
- 사이버 킬체인 : 7단계 프로세스별 APT 공격 방어 분석모델
- 랜섬웨어 : 몸값을 요구하는 악성 소프트웨어
- 이블 트윈 공격 : 무선 Wifi 피싱기법
- 난독화(Obfuscation) : 프로그램 코드의 일부 또는 전체를 변경하여 역공학에 대비
- Tripwire : 크래커가 침입했을 때 알 수 있게 분석하는 도구, 데이터베이스 차이점 체크
- Ping : 원격 호스트가 정상적으로 운영되고 있는지를 확인하는 진단 목적으로 사용하는 명령어
- Tcpdump : 네트워크 인터페이스를 거치는 패킷의 내용을 출력해주는 프로그램, 모든 패킷 내용 도청할 수 있음

접근 통제 기법

- 식별(Identification): 자신이 누구라고 시스템에 밝히는 행위
- 인증(Authentication) : 주체의 신원을 검증하기 위한 활동
- 인가(Authorization) : 인증된 주체에게 접근을 허용하는 활동
- 책임추적성(Accountability) : 주체의 접근을 추적하고 행동을 기록하는 활동

서버 접근 통제 유형

- 임의적 접근 통제(DAC): 신분에 근거하여 객체에 대한 접근을 제한하는 방법
- 강제적 접근 통제(MAC): 주체가 갖는 접근 허가 권한에 근거하여 객체에 대한 접근을 제한하는 방법
- 역할 기반 접근 통제(RBAC): 중앙 관리자가 조직 내 맡은 역할에 기초하여 자원에 대한 접근을 제한하는 방법

인증 기술 유형

- 지식기반 : ID/패스워드
- 소지기반 : 공인인증서
- 생체기반 : 얼굴, 지문
- 특징기반 : 발걸음, 몸짓

접근 통제 보호 모델

- 벨-라파둘라 모델 : 미 국방부 지원 모델, 기밀성 강조

    - 벨기노라다(No Write Down/No Read Up) : 보안수준이 높은 주체는 보안 수준이 낮은 객체에 기록하면 안 됨
- 비바 모델 : 무결성 보장
    - 비무노라업(No Write Up/No Read Down): 낮은 등급의 주체는 상위 등급의 객체를 수정 할 수 없음

암호 알고리즘

암호 알고리즘 방식

알고리즘 방식	알고리즘 방식 종류		기법
양방향 방식	대칭 키 암호 방식	블록 암호 방식	DES, SEED, AES, ARIA, IDEA [2020년 3회]
		스트림 암호 방식	RC4, LFSR
	비대칭 키 암호 방식 (=공개키 암호 방식)		RSA, ECC, ELGamal, 디피-헬만(Diffie-Hellman)
일방향 암호 방식 (해시 암호 방식)	MAC		HMAC, NMAC
	MDC		ND5, SHA

양방향 (대비 비공)

- 대칭키(비공개키)
    - 암호화 = 복호화
    - 블록 암호 방식 : 고정 길이의 블록을 암호화하여 반복하는 알고리즘
        - DES : 블록 크기 64bit, 키 길이 56bit인 페이스텔 구조, 미국 연방 표준국(NIST) 암호화 알고리즘
        - AES : DES를 대체, 3 DES의 성능문제를 극복하기 위해 개발, 미국 표준 기술 연구소(NIST)
        - SEED : 한국인터넷진흥원(KISA) 개발
        - ARIA : 경량 환경 및 하드웨어에서의 효율성 향상을 위해 개발,국가정보원 + 산학연구협회가 개발
        - IDEA : 스위스 연방기술 기관에서 개발
    - 스트림 암호 방식 : 매우 긴 주기의 난수열을 발생시켜 평문과 더불어 암호문을 생성하는 방식
        - LFSR : 선형 되먹임 시프트 레지스터
        - RC4
- 비대칭키(공개키)
    - 암호화 ≠ 복호화
        - 디피-헬만 : 최초의 공개키 알고리즘, 이산 대수

- RSA : 3명의 MIT 수학교수가 고안, 소인수 분해 수학적 알고리즘
- ECC : RSA 암호 방식 대안, 타원 곡선 암호(ECC)
- ElGamal : 이산대수 계산이 어려운 문제를 기본원리로 함

일방향

복호화 불가능

- 해시 암호 방식 : MAC(키 사용), MDC(키 사용X)
  - MD5 : MD4개선, 프로그램이나 파일의 무결성 검사에 사용
  - SHA-1 : NSA에서 미 정부 표준으로 지정, DSA에서 사용
  - SHA-256/384/512 : 256비트의 해시값을 생성하는 해시함수
  - HAS-160 : 국내 표준 서명 알고리즘(KCDSA)를 위해 개발된 해시 함수, MD5 장점+SHA-1장점

IPSec(Internet Protocol Security)

IP계층에서 무결성과 인증을 보장하는 인증 헤더와 기밀성을 보장하는 암호화를 이용한 IP 보안 프로토콜

- 인증, 암호화, 키 관리 프로토콜로 구성

SSL(Secure Socket Layer)/TLS(Transport Layer Security)

전송계층과 응용계층 사이에서 클라이언트와 서버 간의 웹 데이터 암호화, 상호 인증 및 전송 시 데이터 무결성을 보장하는 보안 프로토콜

S-HTTP

웹 상에서 네트워크 트래픽을 암호화하는 주요 방법, 클라이언트와 서버 간 전송되는 모든 메시지를 각각 암호화해 전송하는 기술

개인정보보호 관련 법령

개인정보 보호법, 정보통신망법, 신용정보법

민감 정보 : 주체의 사생활을 현저하게 침해할 수 있는 정보(유전자 검사정보)
고유 식별정보 : 개인을 고유하게 구별하기 위해 부여된 식별 정보(주민번호)

입력 데이터 검증 및 표현 취약점

- XSS(Cross Site Script) : 검증되지 않은 외부 입력 데이터가 포함된 웹페이지를 사용자가 열람할 때 부적절한 스크립트가 실행되는 공격

- 사이트 간 요청 위조(CSRF; Cross Site Request Forgery) : 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격
- SQL 삽입(Injection) : 악의적인 SQL 구문을 삽입하고 실행시켜 정보를 열람, 조작할 수 있는 취약점 공격법

네트워크 보안 솔루션

- 방화벽(Firewall) : 기업 내부, 외부 간 트래픽을 모니터링 하여 시스템의 접근을 허용하거나 차단하는 시스템
- 웹 방화벽 (WAF; Web Application Firewall): 웹 어플리케이션 보안에 특화된 보안 장비
- 네트워크 접근 제어(NAC; Network Access Control) : 단말기가 내부 네트워크에 접속을 시도할 때 이를 제어하고 통제하는 기능을 제공하는 솔루션
- 침입 탐지 시스템(IDS; Intrusion Detection System) : 네트워크에 발생하는 이벤트를 모니터링하고, 비인가 사용자의 침입을 실시간으로 탐지하는 시스템
- 침입 방지 시스템(IPS; Intrusion Prevention System) : 네트워크에 대한 공격이나 침입을 실시간적으로 차단하는 시스템
- 무선 침입 방지 시스템(WIPS; Wireless Intrusion Prevention System) : 인가되지 않은 무선 단말기의 접속을 자동 탐지 및 차단하고 보안에 취약한 무선 공유기를 탐지
- 통합 보안 시스템(UTM; Unified Threat Management) : 다양한 보안 장비의 기능을 하나의 장비로 통합하여 제공하는 시스템
- 가상사설망(VPN; Virtual Private Network) : 인터넷과 같은 공중망에 인증, 암호화, 터널링 기술을 활용해 마치 전용망을 사용하는 효과를 가지는 보안 솔루션

시스템 보안 솔루션

- 스팸 차단 솔루션(Anti-Spam Solution) : 메일 서버 앞단에 위치하여 프록시(Proxy) 메일 서버로 동작
- 보안 운영체제(Secure OS) : 컴퓨터 운영체제의 커널에 보안 기능을 추가한 솔루션

콘텐츠 유출 방지 솔루션

- 데이터 유출 방지(DLP; Data Loss Prevention) : 조직 내부의 중요 자료가 외부로 빠져나가는 것을 탐지하고 차단
- 디지털 저작권 관리(DRM; Digital Right Management) : 디지털 저작물에 대한 보호와 관리 솔루션

비즈니스 연속성 계획 (BCP; Busniess Continuity Plan)

각종 재해, 장애, 재난으로부터 위기관리를 기반으로 재해복구, 업무복구 및 재개, 비상계획 등을 통해 비즈니스 연속성을 보장하는 체계

- BIA(Business Impact Analysis) : 장애나 재해로 인한 운영상의 주요 손실을 볼 것을 가정하여 비즈니스 영향 분석
- RTO(Recovery Time Objective) : 업무중단 시점부터 업무가 복구되어 다시 가동될 때까지의 시간
- RPO(Recovery Point Objective) : 업무중단 시점부터 데이터가 복구되어 다시 정상 가동될 때 데이터의 손실 허용 시점
- DRP(Disaster Recovery Plan) : 재난으로 장기간에 걸쳐 시설의 운영이 불가능한 경우를 대비한 재난 복구 계획
- DRS(Disaster Recovery System) : 재해 복구 센터

DRS의 유형

- Mirror Site : 재해 발생 시 복구까지의 소요 시간(RTO)은 즉시
- Hot Site : 4시간 이내
- Warm Site : 수일 ~ 수주
- Cold Site : 수주 ~ 수개월