Domain 3. 기술적 보안

Part 1. 정보보호 개론

Chapter 1. 정보보호 일반

1. 정보보호 관리

1) 정보보호 정책

(1) 정책의 의미

- 상급관리자의 지시: 컴퓨터보안프로그램생성, 프로그램의 목적 제시, 각각의 책임을 할당하는 등
- 구체적인 보안규칙: 특정한 시스템에 적용되는
- 특정한 관리적 결정: 전자우편 프라이버시정책, 팩스보안정책등...

** 컴퓨터보안정책: 컴퓨터 보안관련 결정의 문서화

(2) 컴퓨터 보안 쟁점의 세가지 유형

ㄱ.pc보안프로그램을 설정하기위한 프로그램 정책

ㄴ. 조직에 관계된 개별쟁점을 다루는 쟁점정책

ㄷ.관리적으로 개별시스템을 보호하도록 하는 결정에 초점맞춘 개별시스템 정책

(3) 보안정책 구현 도구 (표준, 지침, 절차)

(4) 정책,표준,지침,절차의 정의및 특성

- **정책 (Policy):** 정보보호에 대한 상위수준의 목표/방향 제시, 경영목표를 반영하고 정보보호 관련상위정책과 일관성유지, 모든사람이 반드시 지켜야할 요구사항을 전반적이며 개략적으로 규정
- **표준(Standard)**: 정책의 만족을 위해 반드시 준수해야할 구체적인 사항이나 양식을 규정, 조직의 환경,요구사항에 따라 모든사용자들이 준수하도록 요구되는 규정
- **지침(Guidelines)**:선택가능하거나 권고적인 내용이며 융통성있게 적용할수있는 사항, 정책에 따라 특정 시스템, 분야별로 정보보호 활동에 필요하거나 도움이 되는 세부정보를 설명
- **절차(Procedures)**: 정책을 만족하기위해 수행해야하는 사항을 순서에 따라 단계적으로 설명, 구체적인 적용을 위해 필요한 적용절차등의 구체적이고 세부적인 방법을 기술

(5) 보안목적

관리절차의 첫번째 단계는 개별시스템에 대한 보안목적을 정의하는 것,

보안목적: 구체적이며 잘 정의되어있어야한다. 달성가능한것이어야 한다.
모든 보안목적을 달성할수는 없으므로 필수적인것만 다루는것이 필요하다.

(6) 상호의존성 (보안정책은 아래 요소와 상호의존적이다.)

ㄱ. 프로그램 관리 ㄴ. 접근통제 ㄷ. 조직의 광범위환 정책과의 연결

(7)비용 고려: 보안정책의 개발과 이행은 수없이 많은 잠재적인 비용과 관련이 있다.

2. 암호화

1) 데이터의 암복호화

(1) 암호란: 평문을 해독불가능한 형태로 바꾸고 다시 암호화된 통신문을 해독가능한 형태로 변환하기위한 원리,수단,방법등을 취급하는 기술 또는 학문 (FIPS의 정의)

- 인증: 암복호화가 이루어지기전에 상대방의 컴퓨터가 허락받은 컴퓨터인지 확인하는 것

(2) **현대적 암호이론의 창시자인 claude shannon 양질암호가 갖는 기본속성**

ㄱ. 암호해독자에게 힘들게 해독의 난이도 증가 ㄴ. 키의 크기는 적정한 범위한에서 작을 것

ㄷ. 암호화 및 복호화작업은 간단할 것 ㄷ. 동일암호문내에서 타부분으로 오류파급 적게 일어나도록 할것 ㅁ. 암호문이 평문에 비해 길어지지 않을 것

(3) 암호화 알고리즘의 개요

어떤 알고리즘을 써야하나? ㄱ. 널리 사용되는것 ㄴ. 깊이 분석된것 ㄷ. 보안적이라고 받아들여진것 ㄹ. 특허화되지 않았으면서 우수한 것

3. 최신동향및 보안 솔루션

1) DRM

(1) 개념: 디지털컨텐츠가 생성될때부터 배포,이용될때까지 전과정의 라이프 사이클에 걸쳐서 활용되는 소프트웨어와 서비스, 저작권 승인과 집행을 위한 소프트웨어와 보안기술, 지불, 결재기능이 모두 포함

컨텐트의 자유로운 복제는 허용하되 불법사용은 철저히 막는것이 목적이다.

C-drm과 E-drm은 사용권한제어는 유사, 기술과 사용환경은 상이하다.

C-drm: 디지탈컨텐츠의 상업적 가치보호 E-drm: 기업내부 문서 자원보호

(2) **핵심기술요소**

ㄱ. **암호화및 키관리**:

ㄴ. **워터마킹**: 디지털컨텐츠에 보이지않는 마크를 삽입, 소유권증명

ㄷ. **핑거프린팅**: 구매자의 정보가 삽입되어 판매

ㄹ. **패키저**: 보호대상 컨텐츠를 허가된 사용자만 이용할수있게 패키징

ㅁ.**TRM** (Temper Rsistent Module): 컨텐츠 가공,사용하는과정에서 복호화키,컨텐츠가 노출되는것 방지 기술

a. Tamper hardening: code obfuscation, debugger detection, encryption
b. Tamper evidence: 모듈 시그니쳐의 변형여부 검사
c. Tamper detection: 탬퍼링 여부 발견시 폐기및 갱신관리
d. Secure registry: 전자서명과 인증서를 내장한 모듈
e. Trust authentication: 중간자 공격 감시하기위한 모듈to모듈 커뮤니케이션

ㅂ.**사용권한관리기술**: 컨텐츠의 사용횟수,형태,사용기간,3자양도제어하여 권리, 배포, 편집, 복사, 다운로드, 출력, 사용기간, 양도권한등을 관리하는 기술

a. 컨텐츠 식별체계: 모든 저작물에 유일한 식별자를 부여하기위한 식별및 등록체계 정의
b. 메타데이타: 저작물,저작자,저작권자, 권리운용 정보로 구별하여 컨텐츠의 메타데이타 정의
c. 권리표현기술: XrML, ODRL, XACML 등이 있으며 모두 확작성을 제공하는 XML방식임

(3) 권한통제 기술

초기 drm제품, 전용뷰어, 플러그인 삽입방식 -> 컨텐츠 포맷 지원의 한계

최근 API후킹, 파일시스템 필터 등 통해 모든 컨텐츠 포맷, 어플리케이션에 범용적으로 적용하는 추세

built-in : 응용프로그램 소스가 존재하는 포맷

plug-in: plug-in adk제공하는 포맷, adobe reader, winamp

API 후킹: 커널레벨의 system api후킹, drm컨트롤러에서 어플리케이션통제: 모든 윈도우 응용프로그램

OLE: active document server에서 ole인터페이스 이용 제어 (ms오피스, 아래한글)

VBA: vba에서 drm제어, MS office제품군: 보안성 낮음

2) DLP

(1) 개념: 정보유출방지 솔루션, 다양한 정보유출경로와 매체를 감시,통제, 인가된 사용자의 고의적인 불법행위에 의해 외부로 중요정보가 새나가는것을 추적하는 솔루션

(2) 기능:

ㄱ. 정보유출 방지기능 ㄴ. UTM기능 ㄷ. 세부기능 (접근제어, 암호화, 필터링, 활동감시, 네트웍감시 및 차단, 외장메모리 및 프린터 통제, 안티바이러스, 방화벽, IPS)

(3) 종류: 네트웍기반 제품, end-point 제품

(4**) 방향:**

ㄱ. **가상화**: 보호정보를 가상 저장공간에 저장, 접근제어와 결합하여 불법적 정보접근방지

ㄴ. **지능화** : 외부로 송신되는 정보의 자동 필터링, 키워드목록기반의 시그니처 탐지, 해쉬탐지

ㄷ.**안전성**: 네트워크 가용성 저해를 피하기위한 엔드포인트 점검기술

ㄹ. **포괄성**: 내부의 중요정보가 유출될수있는 다양한 경로의 점검

3) DB 보안

(1) 개념; DB 에 저장되어있는 데이터에 대한 비인가자의 접근, 의도적 /비의도적 데이타변경, 파괴로부터 데이터의 **무결성**을 보장한다.

(2) db보안실행의 접근

ㄱ. 접근전략

a. 접근제어 방법: 사용자가 DB에 직접적인 경로를 통해 접근할때 이를 통제

b. 정보흐름제어 방법: 권한이 부여되지않는 데이터 사이에서 부당한 데이터 전달을 통제

c. 추론제어 방법: 간접적인 수단(추론채널,통계추론)등으로 정보를 부당하게 접근하지못하도록 통제

ㄴ. 보안방안

a. DBMS계층:

- 사용자에게 계정및 암호를 부여하여 DBMS접근통제
- 허가규칙: 정당한 사용자에게 정당한 데이타 접근규칙 제공
- (grant/revoke) view: 물리적인 테이블 보고

b. 데이터 암호화

- 기밀데이터에 대한 불법접근 방지/ db파일 도난예방
- 신용카드번호/ 주민번호등의 보안
- 내부관리자의 기밀데이터에 대한 접근권한 제한
- 정부규제법안의 요구사항 만족

c. 접근제어/감사

- 임의적 접근제거, 강제적 접근제어, 역할기반 접근제어
- 실시간 감시 및 침입차단기능
- 데이터베이스 시스템 자체에 대한 크래킹시도 차단

d. 기업통합보안

- IDS,Firewall,ESM 등 외부의 내부네트워크 침입시도의 원천차단

(3) **보안대책**

a. **현행 데이터베이스 보안체계의 문제점:**

- 외부위협차단위한 네트웍보안관리에 치중 - 유출/파괴/변조에 대한 보안대응책 미흡

b. **데이터베이스 보안대책:**

- 재난복구 원격지백업, - 재난복구시스템 구축/운영, - 국가중요기반시설및 금융기관 필수

4) NAC

(1) 개념: 네트웍에 접근시도시 정당한사용자인지, 보안정책을 준수하는 단말인지 검사해 네트웍접근통제

a. 필요성

- 사용자 PC보안수준 강화 - 내부 네트웍 무결성 보장 - 정보자산 접근통제

(2) 기능:

a. 주요 구성요소: -에이전트, -정책관리 서버(인증/무결성검사), -정책실행서버(네트웍장비)

b. 주요기능:

- 네트웍 접근통제 -자산관리

(3) 유형

a. 네트웍기반 NAC: 구현간단, 사용자 개입최소,

b. 호스트기반 NAC: SPES, PMS기능 : 비인가,취약한 사용자에 대한 다양한 제어, 관리

c. 인프라스트럭쳐기반 NAC: 네트웍기반+ 인프라스트럭쳐기반의 장점 모두 수용

Part 2. 기술적 보안

Chapter 1. 시스템 보안

1. 운영체제

1) 개요

(1) 목적: a. 처리능력 향상, b. 응답시간 단축, c. 신뢰도 향상, d. 사용 가능도 향상

(2) 기능: 프로그램생성/실행, 입출력동작, 파일시스템조작, 통신,오류발견, 응답, 자원할당,계정관리, 보호

2) 구조

(1) 커널과 유틸리티:

a.커널: 하드웨어 특성으로부터 프로그램을 격리시키고 , 하드웨어와 직접 상호작동함으로 프로그램에 일관된 서비스 제공, 기능:프로세스와 파일의 관리,입출력장치관리,메모리관리,시스템 호출인터페이스

b.**유틸리티**: 정의된 시스템호출을 통해서 커널과 통신, 프로세스 스케줄링, 기억장치괸리, 파일시스템관리, 운영체제의 고유기능

** **시스템호출**: 이중모드에서 사용자모드는 특권명령을 사용할수없는데 이런경우에 사용자 프로세스는 운영체제에 도움을 요청하게 되는데 이를 시스템 호출이라 한다. 실행중인 프로그램과 운영체제 사이에 인터페이스 제공

(2) 이중모드 구조:

a. 사용자 모드: 특권이 부여되지않는 상태로 동작, 시스템리소스에 제한적 액세스, 보호받는 하위시스템들은 각자가 소유한 보호된 공간에서 실행, 상호 간섭않는다.

b. 모니터모드: 커널모드, 수퍼바이저 모드, 문제일으킬 소지있는 명령은 특권명령으로 분류, 모니터모드에서만 수행, 모든 명령의 수행이 가능

(3) 프로세스관리: 하드웨어에 의존된 최 하위단계수준, 프로세스스케줄링 통해 실행가능한 프로세스 추적관리

(4) 주기억장치관리: 주소변화,기억보호,버퍼기억

(5) 보조기억장치 관리: HDD등의 기억장치에 대한 접근관리, 제어 수행

(6) 입출력시스템 관리: 중아시스템과 외부와의 효율적 통신방법제공, 키보드,디스플레이,프린터, 자기테이프, 자기디스크,

a. 장치구동기

b.. 데이터 입출력방식

- 프로그램에 의한 입출력 (CPU) - 인터럽트에 의한 입출력(인터페이스) -DMA에 의한 입출력

c. 버퍼와 스풀링 버퍼(주기억장치를 버퍼) 스풀링(디스크를 매우 큰 버퍼로)

d. 파일관리

e. 인터럽트: 시스템에 예기치 않은 상황이 발생했을때 그것을 운영체제에 알리고 해결하는 매커니즘

*** 인터럽트의 종류: (예제문제)

- **입출력인터럽트**: 프로세스가 요청한 입출력의 완료등과 관련하여 발생
- **클럭인터럽트** : 프로세스의 시간 할당량 종료와 관련하여 발생
- **콘솔인터럽트**: 콘솔터미널에서 인터럽키 누를때 발생
- **프로세스간 통신 인터럽트**: 임의의 프로세스가 지역호스트, 원격호스트의 다른 프로세스로부터

통신메시지를 받은 겨우
-**시스템 호출인터럽트:** 시스템 호출을 하였을때 발생
- **프로그램 오류인터럽트**: 프로그램의 실행중 논리적인 오류로 인하여 발생
-**하드웨어 검사 인터럽트**: 하으뒈어 상의 오류가 있을때 발생
3) 유닉스시스템
(1) 특징: 대화식 운영체제, 멀티태스킹, 멀티유저환경,계층적파일시스템, 이식성
**** 대화식 운영체제(Shell)
기능: 쉘이란 명령어 해석기, 동시에 하나이상의 프로그램 수행,
종류:
- Bsh: bourne shell, 1979년 UNIX system V와 함께 제공
- Csh: Berkeley UNIX 와 함께 제공, 다양한 하드웨어 이식가능
- Ksh: 벨연구소의 David Korn이 개발한 쉘, bourne쉑 기능에 C쉘에서 처음도입된 몇가지 유용한 기능추가
-TCsh: 코넬대학에서 K쉘의 매끄로운 히스토리편집기능 포함시킨 C쉘의 수정본 개발한것
4) 윈도우시스템
(1) 특징: 빠른처리속도, 프로그램 접근의 용이성, 자동인식기능, 바로가기기능, 멀티태스킹기능, 개체연결포함기능(OLE), 다중모니터 지원
5) 리눅스시스템
(1) 특징: 리누스토발즈에 의해 탄생, 유닉스와 동일한 특징, 멀티태스킹, 가상메모리, TCP/IP사용이 가능
(2) X윈도우의 특징: -서버클라이언트 방식, 통신을 위해x프로토콜 사용

2. 운영체제 보안

1) 윈도우 보안
(1) 윈도우파일시스템
a. FAT: 순차적인 검색, FAT32: 고용량(2G)이상, 윈도우95 osr이후, FAT0, FAT1: 백업용
b. NTFS: 파일정보를 MFT라는 파일테이블에 저장, 자체보안기능설정가능, 압축저장가능
(2) 네트웍드라이브: net user 드라이브명 \\ip\공유명\ 계정&패스워드
(3) 공유폴더보안:
관리공유: ADMIN$, IPC$, C$
관리공유 해제: HKLM\system\curruntconrolset\services\lanmanserver\parameters\ DWORD 0
(4) 컴퓨터 바이러스및 악성코드
**** 컴퓨터 바이러스 종류
- 부트바이러스: 부트영역에 감염되는 바이러스, 도스부팅후 치료요 (brain, michelangelo, monkey, anti-cmos, WYX)
- 파일바이러스: 실행가능한 프로그램에 감염, (도스용파일, 윈도우용 파일바이러스, 매크로바이러스)
- 부트,파일바이러스: 부트,파일모두 감염 (나타스, 절반바이러스, 침입자바이러스, 테킬라바이러스)
- 매크로바이러스: 매크로기능을 이용, 자기를 복제
(5) 백도어및 웜공격
-전파방법; 전자메일 첩부파일, 정상적인 전자메일 첩부파일, 네트웍쓰기 권한 악용, 서비스 취약점이용
-백도어: 트로이목마: 자기복제기능이 없음, 악의적 코드를 내장해 배포하거나 위장해서 배포
-Joke: 피해는 없으나 사용자를 놀라게
- Hoax/Myth: 일종의 스팸메일 부작용, -스파이웨어: 개인정보일부를 해당SW개발자가 알수있도록 제작
2) 리눅스 보안
(1) SUID/ SUID파일점검

(2) 비정상 파일이나 소유자가 없는 파일점검
(3) 특정디렉토리에서 백도어 파일검색
(4).bash_history 점검 : 흔적, 파일사이즈가 0이면 누군가 히스토리 삭제한것
(5)로그인 보안설정
(6) 올바른 로그온 관리
(7) 서버 자원사용 제한: /etc/security/limits.conf 파일이용하여 소프트웨어/하드웨어 제한 pam_limits.so
(8) 사용자 로그인 제어: pam_access.so이용 /etc/security/access.conf파일 이용 로그인 제어

3. 서버 보안

1) 접근통제 기술
(1) 시스템 접근통제
(2) 계정및 패스워드 보호정책
a. 효과적인 계정관리기법사용, 사용자별 권한그룹 지정하여 관리, root권한제한, 공개된 계정사용제한
b. 인증방법 다양: OTP, PAM(pluggable authentication), SSH
c. 계정관리는 그룹별로 생성, 유닉스계열에서 set user id, set group id 사용제한하여 root권한사용제한
d. PAM; 시스템관리자가 응용프로그램들이 사용자를 인증하는 방법을 선택할수있도록 해주는 공유라이브러리 묶음, PAM을 사용하는 응용프로그램을 재작성하지않고 인증방법을 변경할수있음 다양한 형태의 인증방식을 부가적으로 추가할 수 있음
(3)시스템 접근통제 기술
a. 접근통제 리스트는 시스템의 서비스및 사용자의 특성을 고려하여 접근통제리스트를 설정하낟.
- DAC: 임의적 접근통제, 주체나 소속된 그룹의 id에 근거하여 접근제어
- MAC: 강제적 접근통제, 객체에 포함된 정보의 비밀성과 비밀정보에 대하여 주체가 갖는 정형화된 권한에 의거하여 객제에 대한 접근제어
- MLS: 다단계 보안정책: 미국방성에서 시작, 컴퓨터에서의 정보와 사용자간의 보안정책을 명시, 기본보안정책외의 제한속성 정의: 보안등급이 같거나 큰객체에 쓰기 가능하지만 낮은 객체에는 쓰기 금지
- RBAC: 역할기반 접근제어: 보안관리와 감사 용이,

***** RBAC이 제공하는 세가지 기본 보안정책:**
- **특권의 최소화:** rbac이 역할할당자들에 의해 수행되는 작업들이 단지 설정된것의해 허가된것만 가능
- **직무의 분리**: 상호배타적 역할이 보장되어야 한다.
- **데이터 추상화**: 계정에 대한 credit과 debit같은 추상화 허가방법 제공

2) 사회공학적 공격: 피싱,파밍
3) 보안취약성및 위협
(1) 위협: 자산이 지니고있는 취약성을 이용하여 자산에 손상을 입힌다.
*** **위협의 종류: 자연에 의한 위협**, **인간에 의한 의도적 위협**(도청, 정보수정,시스템 해킹) , **인간에 의한 비의도적 위협**(자료입력실수, 정원변동)
(2) 취약성: 자산이 잠재적으로 가지고 있는 약점
4) 취약성 점검도구
(1) SATAN / SARA: 유닉스기반, pc,서버, 라우터,IDS에 대해서 취약점 분석 html보고서
(2) SAINT: 유닉스기반의 네트웍취약점 점검도구, 원격점검가능,
(3) COPS: 유닉스기반, 시스템 내부존재하는 취약점 점검, 취약한 패스워드 점검
(4) **Nessus:** 유닉스, 클라이언트, 서버구조로 클라이언트 취약점 점검
(5) **nmap** : 포트스캐닝 도구로서 tcp connect방식, stealth모드로 포트스캐닝

Chapter 2. 네트워크 보안

1. 네트워크 일반

1) TCP/IP란

(1) 개념, 정의: 네트웍에서 검퓨터들이 자원을 공유하고 서로간에 협력하면서 작업할수있게 만들어진 프로토콜

(2) 역할:

TCP: 전송내용이 상대에게 정확하게 전달되었는가를 확인하는 통신규약,

IP: 통신경로를 선택하는 순서에 관한 규약

(3) 기본서비스

a. 원격로그인 b. 파일전송 c. 전자우편

독립적인 개방형구조로서 하드웨어,운영체제,접속매체의 차이와 관계없이 동작되도록 설계

(4) 역사

1970년 ARPANET호스트에서 네트웍제어 프로토콜 NCT 사용시작

1974년 TCP 본격구성

1981년 IP 발표

1982년 국방통신기관과 ARPA에서 TCP/IP 개발

1984년 도메인이름 시스템 소개

(5)프로토콜

데이터의 송수신을 위하여 만들어진 규약

인터넷: 전세계의 컴퓨터 통신망들을 서로 연결하는 전세계 최대의 컴퓨터 통신망이다.

2) TCP/IP설정

(1) 윈도우와 unix

(2) 설정

-ip주소:

IP의 특성: - 비연결 프로토콜 , - 필요시 패킷을 분리 - 32비트 인터넷주소사용하여 주소지정

- 최대패킷크기: 65,536 - 헤더부분에 관해서만 첵섬 - 프로토콜 필드는 선택적 지정

- 패킷활동 시간 제한 -IP데이타그램:헤더영역과 텍스트영역으로구성

Class D: 멀티캐스팅 위한 것, 네트웍id.호스트id없음, 주로 목적지 주소로만 쓰인다

Class E: 특수용도를 위해 인터넷에 의해 예약, 연구목적으로만 사용

*** 이더넷의 기본적 특성

- Bus 로 사용하는 동축케이블의 전송용량은 초당 10Mbps
- 케이블은 500m 가 최고 200개까지의송수신기 부착가능
- 케이블간 연결위해 리피터 사용, - 두 송신기 사이엔 두개까지의 중계장치만 가능

3) OSI 7 레이어

(1) 구성및 역할

-**응용계층:** 사용자응용프로토콜에 네트웍인터페이스 제공,

-**표현계층:** 일관성있는 인터페이스제공,

-**세션계층**: 시스템,애플,사용자간의 연결설정, 상위계층에서 통신끝나면 연결종료, 암호를 확인/속도조절

-**전송계층**: 신뢰성 보장, 정보의 전달을 관리감독, 네트웍에서 온 정보를 세션층의 특정어플로 보냄

-**네트웍계층**: 주소를 확인하거나 시스템간 데이터를 전달하는데 사용, 내것이면 전송계층으로 보냄,

-데이터링크계층: 물리계층을 통해 정보가 전달되는 방식을 정의, 에러검출, 수정

-**물리계층:** 데이터를 비트단위로 쪼개어 전기적인 신호로 변환

2. 네트워크 기반기술

1) 침입차단 시스템

(1) 개요

a. 최소의 권한 b. 겹겹의 방어 c. 병목-점(choke point) d.취약부분(weakest point)

e. 고장허용: 고장허용을 위해선 모든패킷을 막는것이 기본이다.

f. 패킷필터링:

(2) 기능

a. **패킷필터링의 장단점:**

- 장점: 비용X, 빠르다. 성능우수, 투명성보장, 기존시스템바꾸지 않아도됨. OSI 계층3,4에서 처리

- 단점: 정교한 통제어렵다. 필터수 증가하면 성능저하, 침입사실 인지 어렵다. 로깅,사용자인증기능 난해

*** 패킷필터와 프락시 서버 비교

	패킷필터	프락시 서버
TCP 트래픽 검사방식	주소,포트로 모든패킷에 규칙적용	TCP세션에 규칙적용,데이터흐름제어
UDP 트래픽 검사방식	UDP통신 상태유지, RPC트래픽도 처리	UDP만 제어, 가변적포트- RPC제어 못함
유연성	매우 유연	유연성의결함
구성의 용이성	선택항목많음	선택항목 적음
관리의 용이성	프로토콜수줄이고 규칙간소화하면 관리용이	쉽고 주소숨기기 기능제공
기타	주소숨기기 기능은 별도작업, 로그인/경보기능	로그인기능이 뛰어나며 경보기능

2) **침입탐지시스템**

(1) 개요: 단순한 접근제어기능을 넘어서 침입의 패턴데이터베이스와 전문가시스템을 이용하여 네트웍,시스템 사용을 모니터링하고 침입을 탐비하는 보안 시스템이다.

a. IDS의 장점: - 신기술적용이 빠르다. - 내외부 해킹 차단 - 접속하는ip와 상관없이 차단(모든패킷검사)

- 시스템 칩입에 대응 -침투경로까지 추적 -데이터 안전한곳으로 전환

(2) 기능

- 감시및 분석 - 시스템 구성/취약성 감사 -시스템과 데이터파일의 무결성 평가

-패턴에 의한공격인식 - OS의 audit trail관리로 보안정책위반하는 사용자 감시

a. 네트웍 구성에 따른 분류

ㄱ. **호스트기반 IDS:** 단일호스트에서 침입탐지, 오탐이 적다. 성능저하,

- 단일호스트 기반: 단일 호스트로부터 생성 수집된 audit data를 사용

-다중호스트기반: 다수 호스트로부터 생성 수집된 audit data를 사용

ㄴ. **네트웍기반 IDS:** 네트웍캡처링에 기반, 패킷을 분석해서 침입탐지, 권한없는 접근, 권한초과하는 접근탐지에 뛰어나다. 암호화되거나 모호한 공격은 놓치기 쉽다. 각각의 서브넷에 대해 종속된 호스트인터페이스가 요구된다.

**** NIDS와 HIDS의 차이

	NIDS	HIDS
탐지대상	네트웍통과하는 패킷	시스템 내부 사용자 활동
설치단위	네트워크	세그먼트 호스트

기반기술　패킷캡처링, 패킷조각모음　　프로세스 모니터링
　　프로토콜별 패킷분석　　실시간로그분석, TTY모니터링

---

3) 이동,무선통신 기술

(1) 무선랜의 보안기술

a. SSID 설정을 통한 접속 제한

b. 폐쇄시스템 운영: SSID값을 NULL로 하여 인증을요청하는 사용자를 차단하도록 AP설정,운영

c. MAC 주소 인증

d. WEP인증: 단방향 인증방식제공으로인한 취약성, 고정된 공유키 사용으로 취약

e. 동적WEP인증: 인증서버 필요,

f. EAP인증: 모든 링크에 적용, 다양한 인증방법, 데이터암호화 기능

g. 공격자의 패킷도청방지 대책: EAP, WEP 암호화

h. AP장비 물리적 차단

i. 무선랜 단말기의 관리강화

j. AP장비의 전파 출력 조정

k. 암호화 키 길이 증가

4) 네트웍기반 공격

(1) **Dos공격**

a. **Land attack:** 출발지/목적지IP동일, 루프상태에 빠지게 함

*** 대응방안: 라우터나 패킷필터링 도구이용하여 네트웍유입되는 패킷중 소스주소가 내부IP인 패킷차단

b. **Tear Drop** 공격 (Targa/ newtear/ nestea) 헤더가 조작된 일련의 IP패킷조각들을 전송

- 패킷재조합 수행시 부하 발생

c. **Ping of Death**: ICMP패킷을 정상크기보다 아주 크게 만드렁진 패킷전송, 부하로 인해 성능 저하시킴

d. **Sync Flooding**공격: half-open 연결로 인한 부하발생

***대응방안: 공격가능성을 줄이거나 피해최소하기위한 방법만 존재, 설계상의 취약성에 기인

e. 기타: 스머프공격, UDP Flood 공격

(2) DDos 공격

a. **트리누 공격:** 많은 호스트로부터 통합된 **UDP flood 서비스 거부공격**유발시키는 도구,

- 공격자= 마스터: 27665 /TCP　- 마스터 =데몬들:27444/UDP 데몬들: 임의포트로 UDP플러딩

b. **TFN 공격**: UDP Flood 공격, TCP SYN flood, ICMP echo, 스머프공격

(3) 네트웍 스캐닝 공격

a. 포트스캐닝 공격

Stealth scan　포트열리면 SYN/ACT패킷 받은후 RST패킷보내 연결끊는다.

FIN, Xmas, Null 스캔: 포트가 열리면 응답없고 닫혀있으면 RST/ACT 패킷

UDP open: 포트열리면 응답업고 포트닫혀있을경우 ICMP unreachable

Chapter 3. 어플리케이션 보안

1. 인터넷 응용 보안

1) 인터넷 보안

(1) 자원보호

a. 물리적인 보호

b. **추상적 자원의 보호(더어렵다): 무결성, 가용성, Privacy보장**

c. **정보정책의 필요성**

- **네트웍보안 이전에 실시할것:** 네트웍의 위험요소평가, 정보접근/방어 정책 개발

- 인간이 가장 취약한 요소, 보안및 보안정책에 대한 지속적인교육과 의식화가 반드시 필요

d. 인터넷 보안기법:

ㄱ. 권한 (authorization) /인증 (authentication)/.무결성(integrity), 신원확인에 대한 문제가 있다.
인터넷에서 서로를 확인하기위한 메카니즘으로 공개키 암호화시스템 사용, (비대칭알고리즘)

ㄴ. 공개키를 등록하고 비밀키는 보관한다. 비밀키에 의해 암호화된 데이타는 공개키로 해독된다.

ㄷ. PGP : 대표적인 공개키 암호화 시스템

(2) **Pricacy 보호**

a. **일반적인 암호화 기법**: PGP라는 공개키 암호화시스템 주로 사용, 비대칭암호화시스템으로 암호화시 사용되는 키와 해독시 사용되느 ㄴ키가 서로 다른 키라는 특징을 가진다.

b. **해독:** 송신자가 송신자의 비밀키이용하여 메시지 암호화한 후 암호호된 데이타를 수신자의공개키를 이용하여 다시 암호화한다. 수신자는 우선 송신자의 공개키로 수신된 데이타를 해독하고 해독된 데이타를 자신의 비밀키로 마지막으로 해독한다. **공개키 암호화 기법은 인증,권한, 비밀보장 문제를 해결한다**.

(3) 웹브라우저 보안

(4) 메일보안

a. 메일필터링 기법: 메시지 규칙기능 사용

b.첨부파일 보안: 첨부파일을이용한 웜및 악성스크립트 공격 방어

c. PGP활용: 내용/파일 암호화하여 수신자 만이 그 내용을 볼수있게하는 기밀성 제공, 송신자를 검증해준다.

***** PGP 특징**

- 인증받은 메시지와 파일에 대한 전자 서명 생성과 확인작업
- 키 관리를 graphic interface로 지원
- 공개키를 4056 비트까지 생성
- RSA와 DSS등 두가지 형태의 공개키 생성이 가능

** 키는 공개키 서버에 보관하는 것이 가장 좋다.

(5) 웹기반 메일서비스 보안

a. 웹기반 메일서비스의 보안취약성 이해

b. 코드 기반 공격

c. SSL 활용

SSL: 인터넷사용자에게 안전한 정보를 교환하기 위한 보안 프로토콜, 전자상거래,은행거래시 사용

전송계층 바로위에서 보안기능 수행, SSL v3.0 이후 Ieft에서 표준화되어 TLS로 명명, SSL은 핸드쉐이크 프로토콜, Change Ciper Spec, Alert 프로토콜, Record 프로토콜로 각기 기능 수행

--> 보안기능: **사용자 상호인증, 웹사이트이용시 사이트 인증, 데이터 기밀성, 메시지 기밀성**

2) 웹어플리케이션 보안

(1) OWASP

a. **인젝션 취약점:** 악의적인공격자가 삽입한 데이터에 인터프리터는 의도하지않는 명령어를 실행하거나 데이터를 변경할수 있다. **대응:** 저장프로시저 등 이용하여 인터프리터방식 회피, 사용자입력값 모두 encode, Secure Coding (입력되는 문자값 필터링)

b. **XSS 취약점**: 암호화는 검증절차없이 사용자가 제공하는 데이터를 어블리케이션에서 받아들이거나 웹브라우저로 보낼때 발생, **대응**: 스크립트 무효화, HTML태그 필터링, 중요정보 쿠기저장 금지, session과 ip를 묶어서 버측에 저장

c. **취약한 인증및 세션관리**: 사용자 가장을 위해 비번,키,인증토큰 손상, **대응:** 컨테이너가 제공하는 표준세션ID사용, SSL자격증명과 세션ID항상 보호,로그오프시 세센종료/소멸확인

d. **불완전한 직접 객체 참조**: 파일,디렉토리,db기록, 키 등의 내부구현객체에 대한 참조를 url 혹은 폼

메시지로 노출시킬때 발생 **대응**: 직접 객체 참조 제거, 직접객체에 대한 유효성 검사 강화

e. **크로스사이트 요청 변조(CSRF)**: victim 브라우저가 사전승인된 요청을 취약한 웹어플리케이션에 보내게 함으로써 victim브라우저가 공격자에게 득이 되는 악의적 행동수행 **대응**: POST만 사용하도록 권고했지만 CSRF막지못함, secret validation token

f. **잘못된 보안설정**: 관리자페이지/계정 사용, 보안패치 미실시 **대응**: 시스템 구성확인, 보안패치, 보안지침준수

g. **URL접속제한 실패**: 권한없는 사용자에게 연결주소,URL표시되지않도록 함으로 민감기능 보호, 이 url에 직접접속함으로 승인되지않은 동작수행, **대응:** 불필요접속제한, 사용자별 권한설정, ip접속제한, url에 예측가능한 페이지 존재여부 점검, 관리자페이지 접속제한 점검

h. **확인되지 않는 리다이렉션 및 전달**: 대상페이지를 매개변수정의가 유효성 체크하지 않을경우 공격자는 확인되지않는 매개변수를 전송시켜 인증,권한부여검사를 무시하게할수있음 **대응:** 웹브라우저 보안패치, url이동시 마우스클릭보다 키보드 직접입력

i. **불완전한 암호 저장**: 암호화기능을 잘 사용하지않는다. 약하게 보호된 데이터를 이용하여 신원을 도용하거나 신용카드 사기같은 범죄 **대응:** 적절한 암호매커니즘 보호, 표준강력한 암호알고리즘 사용, 모든키, 인증서 및 암호를 제대로 저장

j. **불충분한 전송레이어 보호:** 민감한 정보를 암호화하지않고 통신하여 정보노출, **대응:** 민감한 데이터에 TLS(SSL) 전송사용, 개별적 전송메시지 암호화

(2) 웹 방화벽

무료 웹방화벽

- Modsecurity 아파치 웹서버용 공개 웹방화벽
- Webknight IIS 웹서버용 공개 웹방화벽