

과정명	
03차시	시스템 보안운영

<1> 운영체제

[1] 운영체제 기능 및 구조

- 운영체제는 메모리, 파일, 입출력장치 프로세서 등과 같은 모든 시스템 자원을 관리하는 다양한 응용프로그램의 운영을 위하여 이들이 요구하는 자원의 가용성을 최적화시키는 역할을 함
- 운영체제는 정보시스템 보안의 기본적인 제공자로 다양한 프로그램의 개념을 지원하고 다중 프로그래밍과 자원의 공유를 허용하며, 정보시스템의 자원 및 정보를 최대한 효율적으로 관리하고 운영하여 사용자들에게 편의성을 제공함
- 운영체제 보안이 제공하는 기능으로는 메모리 보호, 파일 보호, 접근 통제, 사용자 인증 등이 있음
- 운영체제의 기능
 - (1) 프로세스 관리
 - 하드웨어에 의존된 가장 하위 단계 수준
 - 프로세스 스케줄링을 통해 실행 가능한 프로세스 추적 관리
 - (2) 주기억장치 관리
 - 주기억장치의 접근을 관리, 제어하는 장치의 부분
 - 주소변환, 기억보호, 버퍼기억 등의 기능을 수행
 - (3) 보조기억장치 관리
 - 하드디스크나 디스켓 등의 기억 장치에 대한 접근 관리, 제어들을 수행하는 기능
 - (4) 입·출력 시스템 관리
 - 컴퓨터 입출력 장치는 중앙 시스템과 외부에 효율적인 통신 방법을 제공
 - 입·출력 장치는 주변 장치라고 하며 키보드, 디스플레이 장치, 자기테이프, 자기 디스크 등이 있음
 - (5) 파일 관리
 - 프로그램이나 데이터를 파일 단위로 관리하며, 저장 장치에 파일 단위로 저장
- 운영체제의 구조는 정보시스템 자원 관리 계층에 따라 분류함
 - (1) 프로세서 관리
 - 동기화 및 프로세서 스케줄링 담당
 - (2) 메모리 관리
 - 메모리의 할당 및 회수 기능 담당
 - (3) 프로세스 관리
 - 프로세스의 생성, 제거, 메시지 전달, 시작과 정지 등의 작업 진행
 - (4) 주변장치 관리
 - 주변장치의 상태파악과 입·출력 장치의 스케줄링을 담당
 - (5) 파일정보 관리
 - 파일의 생성과 소멸, 열기와 닫기, 유지 및 관리를 담당
- 커널은 기본 개념은 프로세스와 파일의 관리임
- 커널은 하드웨어 특성으로부터 프로그램들을 격리시키고, 하드웨어와 직접 상호 작동함으로써 프로그램에 일관된 서비스를 제공함
- 운영체제의 종류

(1) 서버

- 하나의 서버에 다수의 사용자가 접속하는 환경기반
- 웹 서버, 메일서버 등

(2) 데스크톱

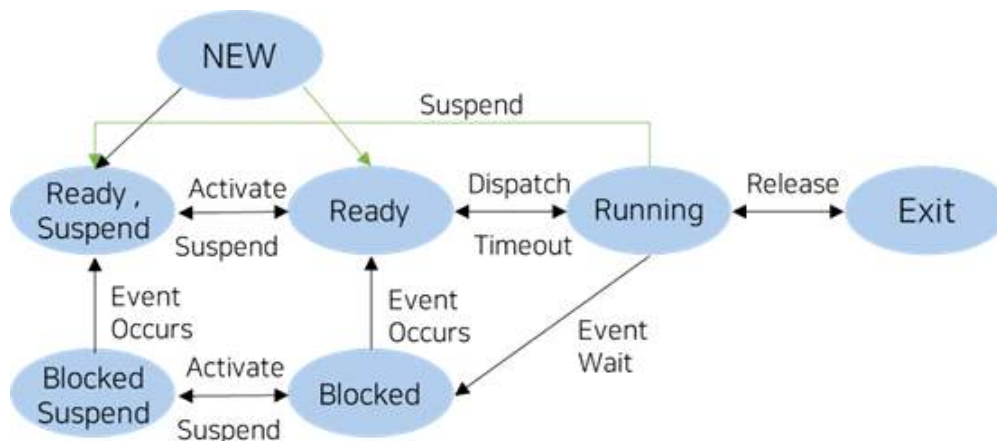
- 개인용 컴퓨터에서 사용하는 운영체제(Windows 등)

(3) 리눅스 기반 모바일

- 일반 컴퓨터의 운영체제와 비슷하나 상대적으로 사양이 낮음
- 다양한 멀티미디어 제공
- Android, iOS 등

[2] 프로세스 관리

- 프로세스는 시스템 작업의 기본 단위이며 현재 수행 상태에 있는 응용프로그램, 운영체제의 일부인 CPU 스케줄러 등의 프로그램을 의미함



- 하나의 프로세스는 생성되어 완료될 때까지 여러 상태변화들을 거치게 됨

(1) 생성

- 프로세스가 생성되었지만 아직 운영체제에 의해 실행 가능한 프로세스 집합이 들어가지 못한 상태

(2) 실행

- 현재 CPU를 차지하여 실행 중인 상태

(3) 준비

- 프로세스가 실행되고 있지 않지만 즉시 CPU를 사용할 수 있도록 대기하고 있는 상태

(4) 대기

- 어떤 사건이 발생하기 전까지 실행될 수 없는 상태

(5) 보류

- 프로세스가 디스크 등에 보관되어 있는 상태

(6) 교착

- 프로세스가 결코 일어날 수 없는 사건을 기다리는 상태

(7) 종료

- 운영체제에 의해서 실행 가능한 프로세스 집합으로부터 해제된 상태

- 프로세스를 생성하는데 필요한 작업

(1) 프로세스 이름 결정

(2) 프로세스 리스트에 생성된 프로세스 추가

(3) 생성된 프로세스에 초기 우선순위 부여

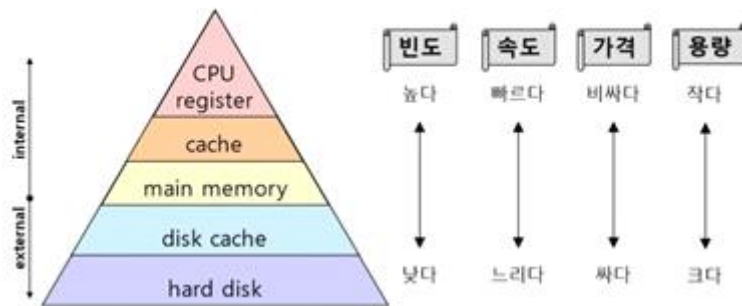
(4) 생성된 프로세스에 PCB 생성

(5) 생성된 프로세스에 초기 자원 할당

- 프로세스 스케줄링은 멀티 프로세스 시스템 내에 존재하는 여러 개의 프로세스 중 어떤 프로세스에게 CPU 사용권을 넘겨줄 것인지를 결정하는 일임
- 멀티 프로세스 시스템 과정에서는 생성된 프로세스가 준비 상태로 넘어가고 실행되기를 기다리고 있는 여러 프로세스를 운영체제가 큐에 보관하고 관리하며 CPU가 사용 가능해지면 대기 큐에서 기다리고 있던 몇 개의 프로세스 중 한 프로세스에게 CPU 사용권을 넘겨줌
- 프로세스 스케줄링은 준비 완료 상태에 있는 프로세스들 중 어느 것을 CPU에 할당 시킬 것인가를 결정하는 문제를 취급하는 것으로서, CPU 효율 및 처리량(Throughput)의 최대화와 반환 기간(Turnaround Time)의 최소화가 목적임

[3] 기억장치 관리

- 계층적인 기억장치의 구성은 주기억장치보다 훨씬 빠른 기억 장치를 요구하게 되었는데 이는 CPU 내에 존재하게 되며 이를 캐시(Cache) 기억 장치라고 함
- 캐시 기억장치는 시스템에서 왕복 작업의 수준을 하나 더 증가시키며 주기억장치에 있는 프로그램을 실행하기 전에 고속의 캐시 기억장치로 프로그램을 적재함으로써 프로그램의 더욱 빠른 실행이 가능해짐



- 메모리 할당기법은 기억 장소에 프로그램이나 데이터가 들어올 경우 기억 장소의 위치를 결정하는 기법임
 - (1) 최적 적합(Best Fit)
 - 입력된 프로그램을 수용할 수 있는 공간 중 가장 작은 공간을 할당
 - (2) 최초 적합(First Fit)
 - 입력된 프로그램을 수용할 수 있는 공간 중 가장 먼저 발견된 공간을 할당
 - (3) 최악 적합(Worst Fit)
 - 입력된 프로그램을 수용할 수 있는 공간 중 가장 큰 공간을 할당
- 가상기억 장치는 시스템에 설치된 물리적 기억장치의 효율적 사용을 위해 사용자에게서 물리적 기억장치를 숨기고 논리적으로 확장된 기억장치를 제공하는 기법
 - (1) 요구페이징
 - 실행할 프로그램의 일부만 메모리에 적재하는 것으로 프로그램의 최대 크기 제한이 사라짐
 - (2) 페이징 교체 알고리즘
 - 1) 선입선출(FIFO)
 - 주기억장치에서 가장 많은 시간을 보낸 페이지부터 교체하는 알고리즘
 - 페이지들의 주기억장치 적재 순서를 기록하여 선입선출 큐를 유지 관리
 - 2) 최근 최소 사용(LRU)
 - 가장 오랜 기간 사용되지 않았던 페이지를 교체하는 알고리즘
 - 일반적으로 선입선출 알고리즘보다 적은 페이지 부재율을 나타냄

3) 최적 교체(OTP)

- 가장 오랫동안 참조되지 않을 페이지를 희생 페이지로 선택하는 방식

(3) 스래싱

- 과도한 페이지징 작업
- 메모리 영역에 접근하게 될 경우, 메모리에 페이지 폴트율이 높은 것을 의미하며 심각한 성능 저하 초래
- 활발하게 사용되는 페이지 집합을 지원해 줄 만큼 프레임이 충분히 할당 받지 못한 프로세스는 페이지 폴트가 발생

[4] 보안 운영체제

- 기존의 운영체제에 내재된 보안상의 결함으로 인한 각종 침해로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 통합시킨 보안 커널을 추가적으로 이식한 운영체제
- 보안커널을 통해 모든 접근 행위가 안전하게 통제됨
- 참조 모니터는 사용자가 특정 객체에 액세스할 권리가 있는지, 해당 객체에 특정 행위를 할 수 있는지를 검사하는 기능으로 보안 운영체제와 프로세스와 파일의 정보 흐름을 감시하는 보안 모듈임
- 신뢰 컴퓨팅 베이스(TCB)는 보안 정책의 시행을 책임지는 하드웨어, 펌웨어, 소프트웨어 및 이들의 조합을 포함하는 정보시스템 내의 모든 보호 메커니즘을 의미함

<2> 클라이언트 보안

[1] Windows 보안

(1) NTFS(NT File System)

- 디스크를 NTFS로 포맷하면 5MB의 공간이 파일 시스템의 정보공간으로 필요하므로 플로피에서는 사용할 수 없으며 NTFS 파일 시스템으로 포맷을 하면 자체의 보안을 설정할 수 있음
- 로컬시스템에 로그인 한 사용자에게 대해 같은 폴더에 대한 액세스 권한을 각각 다르게 설정할 수 있으며 파일 시스템 자체가 압축을 지원하기 때문에 별도의 압축 프로그램을 사용하지 않아도 데이터를 압축하여 저장 가능

(2) 공유 폴더 보안

- 윈도우 탐색기의 [도구]-[폴더 옵션]에서 [보기]탭을 선택하면 '숨김 파일 및 폴더 표시 안함 w'를 선택하여 숨겨진 파일의 공유 설정을 방지 가능
- 오프라인 파일 탭을 이용하여 오프라인에서 네트워크 공유 파일을 이용할 수 있는 기능을 해제

(3) 레지스트리(Registry)

- 운영체제 내에서 작동하는 모든 프로그램의 시스템 정보를 담고 있는 DB
- 해당 시스템에 대한 프로세서의 종류, 주기억장치의 용량, 접속된 주변장치의 정보, 시스템 매개변수, 응용소프트웨어에서 취급하는 파일의 타입과 각종 매개변수들이 저장되어 있음

[2] 클라이언트 보안 위협

(1) 키보드 입력 정보의 노출

- 키로거 프로그램 등을 이용해 키보드로 입력되는 내용을 가로채 다른 컴퓨터에 개인의 ID와 비밀번호뿐만 아니라 계좌번호, 신용카드 번호 등을 유출시킴

(2) 웜·바이러스의 감염

- 악성 코드가 설치되면 개인 사용자 PC에서 사용자의 키 입력 값 정보, 쿠키 정보, 중요 파일 정보 등이 손상되거나 공격자의 PC로 전송되어 노출될 수 있음
- 사용자의 컴퓨터에 악성코드가 실행될 경우 속도나 시스템에 영향을 줄 뿐만 아니라 수집한 정보를 악용하여 사용자가 속한 내부망에 침입할 수 있는 네트워크 구간을 확보하거나 같은 네트워크 구간 내에 타 PC를 공격하여 점령한 후 DDoS 공격 등을 통해 네트워크 전체를

마비시킬 위험도 있음

(3) 스파이웨어의 감염

- 스파이웨어는 사용자의 동의 없이 PC에 불법 설치되는 악성 프로그램으로 ID/Password 등의 사용자 로그인 정보, 사용자의 방문 웹 사이트 정보 또는 키보드 입력 정보 등 중요정보를 수집하여 제3자에게 또는 공격자에게 전송하는 기능을 수행

(4) 단순 ID/Password의 사용

- ID/Password 인증 수단의 안정성 및 보안성은 패스워드에 의해 좌우됨
- 공격자가 패스워드를 알게되면 이용자 PC에 접속하여 PC에 저장된 국가정보 및 행정문서, 개인정보 등의 중요 문서를 탈취할 수 있음

<3> 서버 보안

[1] 인증과 접근통제

- 멀티유저(Multi-User) 시스템인 리눅스나 유닉스는 각각의 사용자만이 접근 가능한 파일, 디렉토리들이 있는 반면 퍼미션은 일련의 규정들을 적용시킬 수 있으며 이런 퍼미션에 의해 사용자들은 자신의 영역을 갖게됨
- passwd 파일은 계정에 대한 정보를 가지고 있으며 사용자들의 고유성을 나타내는 uid부터 어느 그룹에 속해 있는지 등의 정보가 들어있음
- /etc/shadow은 사용자 계정에 대한 암호화된 패스워드 및 관련 정보를 포함하는 파일로 루트 사용자만 접근할 수 있음

[2] 로그 관리

- 로그는 침해사고 원인분석, 디지털 포렌식 등 정보시스템에서 가장 중요한 부분으로 네트워크를 통해 서버에 접속하는 순간부터 접속을 끊는 순간까지의 모든 행동들이 로그 파일이나 로그 서버에 저장됨
- 리눅스 시스템에서는 /var/log에 기본 로그 파일들이 위치함

- 로그 파일의 종류 및 특성

(1) Lastlog

- 사용자의 최근 로그인 시간을 사용자 이름, 터미널, 마지막 로그인 시간으로 출력함
- /var/log/last 파일에 저장됨
- 텍스트 편집기로는 볼 수 없으며, lastlog라는 명령을 통해서만 확인 가능

(2) Wtmp

- 파일이 생성되는 순간부터 사용자의 로그인과 로그아웃한 정보들을 보여줌
- 사용자들의 접속 기록에 대해 많은 정보를 가지고 있기 때문에 공격자들이 가장 먼저 지우고 나가려하는 파일이고 이러한 이유로 피해 시스템 분석에 있어 매우 중요한 역할을 함

(3) Btmp

- 주로그인에 실패할 경우 이 파일에 저장됨
- 일반적으로 이 파일은 생성되지 않아서 직접 생성해주어야 하며 /var/log/btmp라는 빈 파일 하나만 생성해주면 되고, Lastb라는 명령을 통해서 확인 가능

(4) Utmp

- 유닉스 시스템의 가장 기본적인 로그
- 로그인 계정 이름, 로그인한 환경(initab id), 로그인한 디바이스(console, tty 등), 로그인한 쉘의 프로세스 ID, 로그인한 계정의 형식, 로그오프 여부, 시간에 대한 저장 구조의 확인 가능

(5) Messages

- 로그 파일 중 가장 중요한 부분

- 로그인 기록부터 디바이스 정보, 시스템 설정 오류, 파일 시스템, 네트워크 세션 기록 등 가장 다양한 정보를 가지고 있는 파일
- 침입자의 공격 형태가 어느정도 기록되어 지기도 함

(6) Secure

- 텔넷이나 FTP, 원격접속 등 인증과정을 거치는 모든 로그를 secure 로그에 저장

(7) httpd log

- 웹 서버를 운영하고 있다면 access_log와 error_log 파일이 /var/log/httpd에 생기게 됨

(8) History

- 사용된 명령어 목록을 저장하는 파일
- /var/log에 위치하지 않고 사용자의 홈 디렉토리에 사용자별로 존재
- 공격자는 침입 후 관리자 권한을 획득하고 이 파일을 지우려고 함

(9) Syslog

- 시스템의 운영과 관련한 전반적인 로그
- /var/log/messages 파일에 하드웨어의 구동, 서비스의 동작과 에러 등 다양한 로그를 남김

<4> 시스템 공격

[1] 시스템 공격 유형

(1) 버퍼 오버플로우

- 프로그래밍에서 버퍼에 지정된 크기보다 더 큰 데이터를 입력함으로써 버퍼의 한계를 넘어서는 현상
- 프로그래밍을 할 때 문자 배열의 경계 값 검사를 하지 않아 발생하는 취약점이며 공격자는 이를 시스템의 루트 권한을 획득하는 등의 공격을 하는데 악용할 수 있음

(2) 포맷 스트링

- 1990년대 말에 알려지기 시작한 데이터 형태에 대한 불명확한 정의로 인해 발생하는 공격

(3) 백도어

1) 넷버스

- 인터넷을 통해 외부인이 자신의 컴퓨터로 들어와 파일 삭제 또는 정보 유출이 가능한 프로그램
- 다른 파일을 감염시키지는 않음

2) 백오리피스

- 원격지 네트워크에서 사용자가 모르게 정보 수집, 시스템 명령어 수행, 시스템 재구성 등 시스템을 통제할 수 있는 클라이언트/서버 애플리케이션
- 악용의 목적을 위해 만들어진 백도어 프로그램

3) 스쿨버스

- 전형적인 트로이목마로 강력하고 사용하기 쉬움
- 서버 파일이 상대방 컴퓨터에 설치되어 있어야만 클라이언트 파일을 이용해 서버 파일이 설치된 컴퓨터를 원격 조정 가능

4) 루트킷

- 환경 파일을 변경하거나 시스템파일(실행파일)을 변경함으로써 공격자가 의도하는 기능을 수행하게 함
- 체크섬이나 타임스탬프의 변경도 가능하여 해킹 피해시스템 분석이 어려움

(4) 무차별 공격

- 가장 기본적인 공격 방법으로 특정 값을 찾아내기 위해서 모든 조합을 시도하게 되는 공격

(5) 하트블리드 공격

- 2014년 4월에 발견된 오픈소스 암호화 라이브러리인 OpenSSL의 소프트웨어 버그로 서버와 클라이언트 간 정보 탈취 가능

(6) 메모리 해킹

- 피해자 PC 메모리에 상주한 악성코드를 이용한 해킹 방법

(7) MITB 공격

- 웹 브라우저 내에 악성 프로그램이 설치된 상태에서 이루어지며, 악성 프로그램은 메모리에 로딩된 웹 페이지의 내용을 도청하거나 위/변조할 수 있는 공격
- SSL/TLS로 통신 구간이 암호화되어 있더라도 MITB의 위협이 존재
- MITB를 통해 웹 페이지를 위/변조하는 공격을 Web Injection이라고 함