정보보안기사 필기 요약

Part1. 시스템 보안

CPU : 입력장치로부터 자료를 받아 연산 후 결과를 출력 장치로 전송하는 과정을 제어하는 핵심 장치 (연산, 레지스터, 제어, 버스)
기억장치 (레지스터, 캐시, 주기억장치, 보조기억장치)

CPU구성요소

1. ALU (연산장치) : 산술연산, 논리연산
2. 레지스터 : 소규모 데이터, 중간 결과를 기억해두는 고속 영역
3. Control Unit(제어장치) : 명령어 해석, 제어신호 발생
4. 내부 CPU 버스 : ALU 레지스터간의 데이터 이동

레지스터 종류
PC(Program Counter) : 다음에 수행할 주기억장치 주소 기억
MAR(Memory Address Register) : 주기억장치에 접근하기 위한 주기억장치 주소 기억
MBR(Memory Buffer Register) : 주기억 장치 입/출력 자료 기억
IR(Instruction Register) : 주기억 장치 -> 인출한 명령코드 기억

버스 종류 (입출력 영향을 끼침)
데이터 버스 : 데이터 전송 용도
주소 버스 : 기억장소 위치, 식별
제어 버스: CPU, 기억장치, I/O 장치사이의 제어신호 전송

CPU 명령 실행 주기

1. 인출 (Instruction Fetch) : 메모리 데이터를 로드하여 레지스터에 적재
2. 간접 (Indrection) : 간접주소 방식 채택 경우 – CPU가 메모리 참조시 메모리 주소를 참조
3. 실행 (Execution) : 명령, 데이터 > 산술 , 논리연산 수행
4. 인터럽트 (Interrupt): 예기치않은 문제 발생시에도 업무처리가능 하게 하는 기능

기억장치 계층구조

레지스터	기억장치용량	장치비용	속도
캐시	작음	큼	빠름
주기억장치			
보조기억장치.	큼	작음	느림

캐시메모리 : CPU와 주기억장치 속도차이 극복을 위한 버퍼 메모리(기억장치)

캐시메모리 사상방식

1. 직접사상(Direct Mapping): Main Memory를 여러구역으로 분할하여 캐시슬롯과 직접 매핑
2. 집합 연관사상(Set Associate Mapping): 직접 + 연관 방법 메모리를 세트(블록)으로 분할하여 매핑
3. 연관 사상(Associate Mapping): Main Memory 블록들이 캐시 슬롯에 어느곳이든 적재 가능

캐시메모리 관리 방식 (CPU 원하는 데이터가 캐시메모리에 적재하도록 관리)
(호출기법)

1. Demand Fetch : 필요시 캐시 인출
2. Pre-Fetch : 예상되는 데이터를 미리 패치

(교체기법)

캐시 메모리 교체 알고리즘

1. FIFO(First In First Out): 가장 오래 있었던 Page 교체 / 자주 사용되는 페이지가 교체될 수 있음
2. LFU(Least Frequently Used): 가장 사용횟수가 적은 Page 교체 / 가장 새로 들어온 페이지 교체될 수 있음
3. LRU(Least Recently Used):가장 오랫동안 사용되지 않은 Page 교체 / 오버헤드 우려
4. NUR(Not Used Recently): 미사용 Page 교체 (참조/수정비트 사용)
5. SCR(Second chance Replacement): 최초 참조 비트 1, 1-> 0 두번기회

페이지교체시 문제점

Page Fault(페이지부재), DemadPaging, Thrashing(부재가 너무빈번하여 프로세스 수행보다 페이지 교체 시간소요가 더 소모됨)

가상메모리(Virtual Memory) : Virtual Address Space 사용, 물리적 메모리보다 더 큰용량 제공

가상메모리 관리 단위 (페이지 Vs 세그먼트) : 비연속 할당

페이지 : 동일한크기의 최소 논리 분할 단위 / 내부단편화

세그먼트 : 용도별로 논리적 단위로 나눔 / 외부단편화

연속할당 : 고정분할, 가변 분할

I/O 인터페이스 (주기억장치 - 보조기억장치 입출력)

1. CPU 경유 : 프로그램에 의한 I/O, 인터럽트에 의한 I/O
   - 프로그램에 의한 I/O : CPU 가 주변장치를 연속 감시하는 Polling 방식
   - 인터럽트에 의한 I/O : 인터럽트 요청 감지시 수행작업을 중지
2. CPU 비경유 : DMA(Direct Memory Access Controller) , Channel I/O
   - DMA : 메모리와 주변장치를 직접 관리, 속도 빠름 (Cycle Stealing: CPU사용하지않는 버스 점유, Brust Mode: 점유)
   - 채널 I/O(I/O Processor): I/O장치의 복잡함으로 DMA 한계를 보완하여 별도 전용 처리기능 프로세서 탑재
     1. Multiplexer Channel : 저속장치, 시분할 방식
     2. Selector : 고속장치, 단일 입출력

운영체제

: 컴퓨터 시스템의 자원들을 효율적으로 관리, 사용자의 컴퓨터 사용 편의성 환경 제공

운영체제의 목적

1. 처리능력 향상
2. 신뢰성 향상
3. 응답시간의 단축
4. 자원 활용률 향상
5. 가용성 향상

운용체제 주요 자원 관리 기능

1. 프로세스 관리
2. 기억장치 관리
3. 주변장치 관리
4. 파일 관리

프로세스 관리 (Process Management)

프로세스 : - 레지스터, 스택, 포인터, 실행중인 프로그램, 데이터 등의 집합체
- 실행중인 프로그램 , PCB 보유 , Library Call, 자원할당의 기본 단위

스레드 : - 제어의 흐름, 프러세스에서 실행의 개념 , CPU 작업의 기본 단위, System Call

CPU 스케줄링 기법 (:프로세스 상태 전이)
: 컴퓨터의 자원을 효율적으로 사용하기 위한 정책, 자원을 요청하는 프로세스 순서를 정함
점유방식

1. 선점(Preemptive): 프로세스 CPU 점유 시 다른프로세스 점유 가능 (Round-robin, SRT)
2. 비선점(Non-preemtive): 프로세스 CPU 점유시 독점 (FCFS, SJF, HRN)

(비선점 방식)

1. FCFS(First Come First Service): 대기큐에 도차간 순서에 따라 CPU 할당
2. SJF(Short Job First): 수행시간이 짧은 작업부터 CPU 할당
3. HRN(Highest Ratio Next): SJF 개선하여 프로세스 우선순위로 할당

(선점)

1. Round-robin : 각 프로세스는 같은 시간을 CPU에서 할당 받음
2. SRT(Shortest Remaining Time) : 수행시간이 짧은 작업부터 CPU할당하지만 수행중 다른 프로세스가 더 짧은시간 일때 점유 가능

Multi Level Queue : 여러종류의 그룹(큐)로 나누어 각자 독자적인 스케줄링 기법을 사용
Multi Level Feedback Queue: 그룹(큐)들을 라운드로빈 + 비선점방식 (Hybrid 스케줄링)
병행성제어
상호 배제(Mutual Exclusion Techniques) : 다수의 프로세스 동일 자원 접근 시 무결성 보장, 임계영역 사용

1. 임계영역(Critical Section): 공유자원의 독점을 보장하는 코드 영역, 병렬컴퓨팅 일부로도 쓰임, 세마포어 개념이용
   세마포어: 공유자원의 개수를 나타내는 변수
2. 모니터 상호배제 기법 : 하나의 프로세스만이 모니터내부의 존재, 모니터 내부의 지역변수로 정의

교착상태(Dead Lock): 하나이상의 프러세스가 더 이상 계속할 수 없는 특정 사건을 기다리고 있는 상태
교착상태 발생조건

1. 상호배제 : 하나이상의 프로세스가 자원을 배타 점유
2. 점유와 대기: 부분할당으로 다른 종류의 자원을 요구하면서 자원 점유
3. 비선점 : 자원이 해제 되지 않음
4. 환형대기 : 프로세스와 자원들이 원형을 이루며 서로 상대방의 자원을 요청

교착상태 대응 방법(예방, 회피, 발견, 회복)

1. 예방(Prevention) : 필요 조건을 부정, 교착상태 예방
   - 점유와 대기 부정: 필요한 자원을 일시에 요청
   - 비선점 조건의 부정: 자원점유 후 자원 요청시 자원해제 선 요청
   - 환형대기 조건 부정: 프로세스들의 자원별로 우선순위 결정
   - 상호배제 조건 부정: 자원 비공유 전제
2. 회피(Avoidence) : 가능성을 인정, 회피
   - 은행원 알고리즘 (안전상태, 불안전상태): 프로세스가 요구한 최대 요구량 만큼 자원을 할당 안전순서서열 존재, 교착상태는 불안전상태에서만 일어남.
3. 발견(Dectection) : 교착상태 발생 허용, 원인을 규명하고 해결
   - 교착상태 발견 알고리즘: 교착상태 발생 검사 알고리즘 , 교착상태 빈도수 파악
   - 자원할당 그래프 : 방향그래프를 이용, 그래프 소거법을 이용하여 교착상태 감지
4. 회복(Recovery)
   - 프로세스중지
   - 선점

장치관리기법
디스크
디스크 접근 시간

1. 탐색시간 : 현위치에서 특정실린더로 디스크 헤드가 이동하는 데 소요되는 시간
2. 회전 지연시간 : 섹터가 디스크 헤드까지 도달하는 시간

3. 전송시간 : 데이터 전송 시간

디스크 스케줄링 기법

1. FCFS(First-Come First Served) : 먼저들어온 요청 우선처리
2. SSTF(Shortest-Seek-Time First) : 탐색거리가 가장 짧은 트랙 요청 우선 처리
3. SCAN(엘레베이터 알고리즘): Head가 이동하는 모든 요청을 서비스 끝까지 처리후 역방향 처리
4. C-SCAN: SCAN 에서 바깥쪽에서 안쪽으로 이동
5. C-LOOK: 진행방향에서 요청없을시 헤드를 처음위치로 이동

파일 시스템(File System)

FAT(File Allocation Table)

1. FAT16: 대부분 MS 호환가능, 2GB, 암호화 및 압축 불가능, 파일명 최대 영문8자, 클러스터 1632KB
2. FAT32: 2TB, 암호화 및 압축 불가능, 파일명 최대 영문 256자, 클러스터 4KB
3. NTFS(New Technology File System): 암호화 및 압축 지원, 가변클러스터

EXT(Extended File System)

1. EXT: MINIX File System 보완, 최대 2GB, 파일명 255bytes, 단편화문제
2. EXT2: 2GB, 볼륨32TB, 오류 수정 지원
3. EXT3: 저널링기능, 온라인 파일 시스템 증대, 디스크조각화 최소화
4. EXT4: 16GB, 볼륨 16Exabyte, 온라인 조각모음, 저널 체크섬, 하위호환 가능

UFS(Unix File Sysyem) : 유닉스 파일 시스템 (부트블록, 슈퍼블록, 실린더그룹, i-node 테이블)

1. 슈퍼블록: 파일 시스템 크기, i-node 테이블의 크기
2. I-node 테이블: 파일정보 – 파일크기, 위치, 유형 허가권, 날짜

RAID : 디스크 고장 시 복구를 위해 2개이상에 디스크에 데이터를 저장하는 기술, 저 가용성 디스크를 배열 구조로 중복 구성

RAID 0 : 최소 2개 디스크, 데이터를 나누어 저장, 장애발생 시 복구 불가
RAID 1 : 디스크 완전 이중화, 많음 비용 발생, ReadWrite 병렬가능
RAID 2 : Hamming Code를 이용하여 오류 복구
RAID 3 : Parity 정보를 별도 디스크에 저장
RAID 4 : Parity 정보를 별도 디스크에 블록별 저장 Write 성능 저하
RAID 5 : 분산 Parity 구현, 안전성 향상
RAID 6 : Parity 다중화, 장애발생 상황에서도 다른 정상 동작

리눅스 서버 보안
라눅스 핵심 구성요소

1. 쉘 : 명령어 해석기, 명령의 입출력 수행 (Bash, Bourne, C, korn), 프로그램 실행
2. 커널 : 주기억장치에 상주, 사용자 프로그램 관리
3. 파일 시스템 : 정보를 저장하는 기본적 구조, 계층(트리)구조

리눅스 파일 종류

1. 루트 파일 시스템 : 시스템 프로그램, 디렉터리
2. 일반 파일 : 프로그램, 원시 프로그램파일, 텍스트 등
3. 디렉터리 파일 : 디렉터리에 관한 정보를 저장하는 논리적인 단위
4. 특수 파일 : 주변장치에 연결된 파일

리눅스 부팅
Run Level

0. PROM 감시

1. 사용자 로그인 불가능한 상태, 암호변경할 때 사용
2. 공유된 자원이 없는 다중 사용자 단계
3. 공유 자원을 가진 다중 사용자 단계
4. 사용 되지 않는 단계
5. 3단계 기동후 X-Windows 실행
6. 재부팅 단계 > 3단계로 재부팅

리눅스 인증과 권한 /etc/passwd
Passwd 파일 구조
Root : x : 0 : 0 : root : /root : /bin bash
사용자계정 : 패스워드(/etc/shadow) : UserID : GroupID : Home Directory : Shell

리눅스 권한 관리
Umask (r = 4 , w = 2, x= 0 , User : Group : Other) : Default 권한 , 파일 666 , 디렉토리 777
chmod : 권한 부여 명령 (chmod 777 파일명 , chmod u+g, g-w, o+r 파일명)
chown : 파일에 대한 사용자, 그룹 변경 (chown 소유자 : 그룹)

특수권한 관리(setuid , setgid, stickybit)
1. setuid : 파일을 소유자권한으로 실행가능 (4000 , u+s)
2. setgid : 파일을 그룹 권한으로 실행가능 (2000, g+s)
3. stickybit : 공용 디렉토리 (1000

로그파일 /var/log
현재 사용자 확인 : w, who – 로그인 사용자 ID, 사용 터미널, 로그인 시간
로그인한 사용자 정보 : /var/utmp
로그인, 로그아웃 정보 : /var/wtmp (last 명령어 사용)
로그인 실패 정보 : /var/btmp

Syslog(syslogd /etc/syslogd.conf 로그수준) : 로그수준을 읽고, 로그를 기록
유형 emerg > alert > crit > err > warn > notice > info > debug

작업스케줄러 관리
Cron : 반복적인 프로세스 작업을 수행할 때 사용하는 batch 프로그램 (/etc/crontab)
30 * * * * root /home/test.txt : 30분 마다 test 실행
분 시 일 월 요일 사용자 실행명령

At : 한번만 실행

파일 무결성 검사
: 초기 상태 파일 정보에 대해 해시값 저장, 이후 비교
Tripwire (--init : 초기화 , --check : 무결성 검사)

윈도우 클라이언트 및 서버 보안
파일 시스템 (FAT, NTFS)

윈도우 인증 시스템 (Winlogon, GINA, LSA, SAM, SRM)
1. Winlogon : 윈도우 로그인 프로세스

2. GINA(msgina.dll) : Winlogon Gina로딩하여 계정과 암호를 LSA 전달
3. LSA (lsas.exe) : SRM 작성한 감사로그 기록, 계정과 암호 검증을 위해 LTLM 모듈 로딩, 계정검증
4. SAM : 사용자 계정정보 해시값 저장
5. SRM : 사용자 고유 SID 부여 SID 권한 부여

윈도우 실행 프로세스

1. Wininit.exe : 윈도우 시작 프로그램
2. Services.exe : 윈도우 서비스 관리
3. Lsm.exe : 시스템관리작업, 주요 함수 실행, 호스트컴퓨터-서버 연결관리
4. Svchost.exe : 서비스를 관리하기위한 프로세스
5. Conost.exe : 키보드, 마우스 입력 허용 , 문자 출력 셸의 기본 기능 수행

공유폴더 (Net BIOS :445)
공유폴더 확인 : net share
공유폴더 삭제 : net share /delete

레지스트리 : MS 운영체제에서 OS및 응용 프로그램등에 필요한 정보를 저장하고 관리하기 위한 계층형 데이터 베이스
Key, Value, Data Type, Data로 이루워져 있음
루트키 (레지스트리 최상위 키)

1. HKEY_CLASSES_ROOT : 확장자, 프로그램간의 연결 정보
2. HKEY_LOCAL_MACHINE : HW, SW 설치 정보
3. HKEY_USERS : 사용자 정보
4. HKEY_CURRENT_CONFIG : 디스플레이, 프린터 정보

주요 레지스트리 키
버전 정보 : HKLM₩SOFTWARE₩Microsoft₩Windows NT₩Current Version
컴퓨터 이름 : HKLM₩SYSTEM₩ControlSet00X₩Control₩ComputerName₩ActiveComputerName
시작프로그램 : HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Current Version₩ Run[]
최근에 실행한 명령어 :HKU₩{USER}₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩RunMRU

이벤트 로그 및 웹 아티팩트 분석
윈도우 이벤트 로그 : 이벤트 뷰어를 통해 확인가능 , .evt
웹 아티팩트 분석 : 사용자가 웹 사이트를 이용한 흔적을 분석 하는 것 (웹 브라우저 캐시, 히스토리, 쿠키)
Window XP, 7 (index.dat) / Window 10 (WebCacheV01.dat WebCacheV24.dat)

바이러스 (자가복제 가능) Vs 악성코드 (자가복제 불가능)

세대 별 바이러스
1세대 (원시형 바이러스): 고정된 크기 주기억장치에 상주하여 감염 (돌 바이러스, 예루살렘 바이러스)
2세대 (암호화 바이러스): 프로그램을 암호화 시킴, 암호화방식이 일정하여 복호화 방식 쉬움 (폭포 바이러스 ,느림보 바이러스)
3세대 (은폐형 바이러스): 다른 실행파일에 기생 감염 시 백신을 속여 감염 여부 확인이 어려움 (맥가이버 바이러스 , 브레인 바이러스)
4세대 (갑옷형 바이러스): 10만개 이상의 암호화기밥을 사용하여 은폐 (다형성 바이러스, 자체변형 바이러스)
5세대 (매크로 바이러스): 매크로 명령을 사용하는 프로그램을 감염, 누구나 쉽게 생성/배포 가능 (Melisa 바이러스 Nimda 바이러스)

악성코드

Shellcode : 작은 크기의 코드로 소프트웨어 취약점을 이용하는 기계어 코드
HeapSpray : 셸코드를 힙영역에 뿌리는 것 전역변수를 이용한다.
예방 방법 (ASLR 설정 - 메모리 동적 주소 할당)
Sysctl -w kernel.radomize_va_space=1
버퍼 오버플로우 : 프로세스가 사용가능한 메모리 공간을 초과해 발생되는 공격

스택 오버플로우 : 스택에 저장되어있는 복귀주소가 지역변수에 의해 침범

비권고 함수 : strcpy, strcat, getwd, gets, scanf, sprint

권고 함수 : strncat, strncpy, fgets, fscanf, vfscanf, snprintf

힙 버퍼 오버플로우: 동적으로 할당되는 공간이 힙에 저장되어 경계값을 검사하지 않고 사용 시 메모리가 경계를 초과

APT(Advanced Persistant Threat) : 특정 공격들을 SNS를 사용하여 지속적으로 수행하는 공격 (침투 – 탐색 – 수집/공격 - 유출)

정보보안기사 필기 요약

Part2. 네트워크 보안

OSI 7계층
7 Application (응용) : 사용자에게 서비스 제공 (FTP, SNMP, HTTP, Mail ...) // 게이트웨이
6 Presentation (표현) : 포맷, 압축, 암호화, 텍스트/그래픽 16진수 변환 (GIF, ASCII, EBCDIC)
5 Session (세션) : 가상연결, 통신 방식(반이중, 전이중, 완전이중) 결정 (SSL)
4 Transport (전송) : 에러제어, 데이터흐름제어, 논리적 주소 연결, 신뢰도/품질 보증 (TCP, UDP)
3 Network (네트워크) : 라우팅, 논리적 주소 연결(IP), 데이터 흐름 제어 (IP, ICMP, ARP, RIP, OSPF, BGP) // 라우터
2 Data Link (데이터링크) : 물리주소 결정, 에러제어, 흐름제어 (PP2P, L2TP) // 브릿지, 스위치
1 Physical (물리) : 전기적, 기계적 연결 정의 (케이블, 광섬유) // 케이블, 리피터

응용계층
HTTP (TCP:80 , State-less)
전송방식
Get: 쿼리스트링(url) 데이터 전달
Post: Http body 데이터 전달, 크기제한 없음
OPtions: 응답 메시지 없이 전송
Put : 메시지 + 데이터요청 URL 포함
Delelte : URL 지정된 자원 삭제
Trace : 경로 기록
* HTTP Header - body 구분 ~~₩r₩n₩r₩n~~

정보유지 방법
Cookie : 클라이어언트에 정보 저장, Text, 최대 4kb
Session : 서버에 정보 저장, Object

SMTP(Simple Mail Transfer Protocol , 25) :전자우편 표준 프로토콜
Store-and-Forward 방식
MTA(Mail Transfer Agent), MDA(Mail Delivery Agent), MUA(Mail User Agent)
MDA// POP3(TCP 110): 수신후 메일 삭제 , IMAP(143): 수신후 메일 저장

FTP(File Transfer Protocol) : 파일전송 프로토콜
등록된 사용자만 파일전송 가능, 그 외는 익명으로 사용
ftpusers : FTP차단 유저
전송모드
Active Mode (TCP: 21, 20)
21번포트 : 접속
20번포트 : 데이터 전송
Passive Mode (TCP: 21, 1024~)
21번포트 : 접속
1024번~65535번 : 데이터 전송 (Random)

SNMP(Simple Network Management Protocol): 네트워크 장애, 통계, 상태 정보를 실시간으로 수집 및 분석하는 네트워크 관리 시스템

전송계층 : 송/수신자 논리적 연결, 연결지향 서비스 제공
TCP(Transmission Control Protocol):
클라이언트-서버 연결지향
신뢰성 있는 데이터전송, 에러제어(FEC, BEC), 흐름제어(슬라이딩 윈도우), 순서제어, 혼잡제어(TCP Slow Start, Go-Back-N)

완전이중
netstat: TCP 상태정보 확인

UDP(User Datagram Protocol) exVoIP
데이터 송수신 속도 빠름
비신뢰성
비접속형

인터넷 계층 : 송신자-수신자 IP주소 경로 결정, 전송 / 패킷 전달에 대한 책임
* 패킷 + IP Header : Datagram
라우팅 : IP헤더에서 IP주소를 읽어 경로 결정

IP(Internet Protocol) // TCP/IP
IPv4(128), IPv6(128)
주소화, 데이터그램포맷, 패킷 핸들링
MTU(Maximum Transmission Unit): 한번에 통과할 수 있는 패킷의 최대 크기 (ifconfig , ipconfig 확인가능)
IP : 네트워크주소 + 호스트주소

ICMP(Internet Control Message Protocol) Ping
오류제어 프로토콜
질의 메시지 기능
ICMP메세지
3 Destination Unreachable(목적지 찾을 수없음)
4 Source quench(패킷이 너무 빨라 네트워크 제어)
5 Redirection(패킷 라우팅 경로 수정, Smurf)
8 | 0 Echo request / reply (Host 존재 확인)
11 Time exceeded (시간경과, 패킷 삭제)
12 Parameter problem (IP Header 잘못된 정보 있음)
13 | 14 Timestamp request | reply (비슷한 시간에 정보 추가)

ARP / RARP
ARP(Address Resolution Protocol)
IP주소를 MAC주소로 변경
ARPCache Table : MAC , IP 주소를 보유하고 있는 테이블
RARP (MAC 주소를 IP주소로 변경)

네트워크 접근 계층(데이터링크, 물리): IP주소 › MAC 주소 변환, 에러제어, 흐름제어
CSMA/CD(Carrier Sense Multiple Access/ Collision Detection) : 유선 랜 메세지 송수신 방법
충돌을 감시하여 비어있는 채널을 재사용하게 만듬

CSMA/CA(Carrier Sense Multiple Access/ Collision Avoidence) : 무선 랜 메세지 송수신 방법
수신자에게 간단한 전송을 유발하여 프레임을 전송하는 방법

네트워크 기반 공격 기술의 이해 및 대응
서비스 거부 공격(DoS : Denial of Service) : 특정 서비스를 계속적으로 호출하여 컴퓨터 자원 고갈(CPU, Memory, Network) 로직공격(IP Header 변조), 플러딩 공격(무작위 패킷 공격)

DDoS(Distributed Denial of Service): 다수의 분산되어 있는 공격자 서버로 특정 시스템을 공격하는 방법

DDos (분산 서비스 공격)

1) TCP SYN Flooding : TCP SYN패킷을 이용하여 수많은 연결요청을 통해 일반 사용자의 가용성을 저해 시킴
2) ICMP Flodding (Smurf Attack): ICMP 패킷 이용 서비스 및 포트가 필요없음
3) Tear Drop: fragment 재조합 취약점 이용, offset 값을 조작하여 중첩 유발
4) Ping of Death: Ping을 이용하여 ICMP MTU이상의 패킷 크기 조정
5) Land Attack : 송신자 IP주소 - 수신자IP주소를 같게 설정 트래픽 유발
6) HTTP Get Flooding : 정상적 연결 이후 HTTP Get 지속적으로 요청 -> 다량의 Request 호출
7) Cache Control Attack : Cache-Control Header 옵션을 사용하여 항상 새로운 페이지를 요청
8) Slow HTTP Get/Post Attack : Get(TCP/UDP)- 정상 IP 기반 공격 , 소량의 트래픽/세션 연결
   Post- Post지시자 사용, 대량데이터를 장시간에 걸쳐 분할 연결
9) Hash DoS: 해시테이블의 인덱스 정보가 중복되도록 유도 조회 시 CPU자원 소모
   (*HTTP Get, Post Request 시 변수를 해쉬테이블 구조로 관리)
10) Hulk Dos: 공격대상 URL을 지속적으로 변경하여 DDoS 차단정책 우회 Get Flooding 수행

포트스캐닝(Port Scanning) : NMAP

1) TCP Open Scan :3-Way-Handshaking을 이용하여 포트 확인, 연결수립
   (Open: SYN+ACK, Close:RST+ACK)
2) TCP Half Open Scan : SYN 패킷 전송 응답 정보로 포트 확인, 연결 X
   (Open: SYN+ACK, Close:RST+ACK)
3) FIN Scan : FIN 패킷 전송 (Open: 응답 X , Close: RST)
4) UDP Scan : UDP패킷 전송 (Open: 응답 X, Close: ICMP Unreachable), 신뢰성 낮음
5) X-MAS Scan: FIN, PSH, URG 패킷 전송 (Open: 응답 X, Close: RST)
6) NULL Scan: NULL패킷 전송(Open : 응답 X, Close: RST)

스니핑 공격(Sniffing Attack): 수동적 공격 , Promiscuous 모드 사용, tcpdump이용

Session Hijacking: 스니핑 공격을 이용하여 이미 인증을 받은 세션을 탈취하여 인증 우회
(Hunt, Arpsppof, IPWatcher, Ferret, Hemster, WireShark)

스푸핑 공격(Spoofing Attack)
TCP/IP구조 취약점을 이용하여 IP 변조 후 SynFlooding , 인증우회

ARP Spoofing : 클라이언트 MAC주소를 탈취하여 서버 인증우회, 연결이 끊어지지 않도록 Release 해야함

네트워크 대응 기술 및 응용
침입차단 시스템(Firewall): 네트워크 경유 후 트래픽 모니터링, 접근통제

- 인바운드 : 외부에서 내부로 들어오는 규칙
- 아웃바운드: 내부에서 외부로 나가는 규칙

1) 패킷필터링(네트워크,전송계층): IP주소, Port 번호등을 이용해 접속제어 , 유연성 높음
2) 애플리케이션 게이트웨이(응용계층): Proxy Gateway, 보안성우수, 유연성 결여
3) 회선 게이트웨이(응용-세션 계층): Client측에 Proxy를 인식할 수 있는 수정된 프로그램, 관리수월
4) 상태 기반 패킷 검사(전 계층): 세션 추적 가능, 방화벽 표준, 내부 대응 어려움
5) 심층 패킷 분석(DPI :Deep Packet Inspection): 콘텐츠 까지 모두 검사 상태기반 패킷 검사에서 발전

침입차단 시스템 구축 유형
스크리닝 라우터 : 내부 네트워크와 외부 네트워크 사이의 패킷 트래픽을 permit/drop
배스천 호스트 : 내부 네트워크 전면에서 내부 네트워크 전체를 보호, 외부 인터넷과 내부 네트워크를 연결
듀얼 홈드 호스트 : 2개의 NIC로 외부 네트워크와 내부 네트워크를 연결, Proxy 기능
스크린드 호스트 : Packet Filtering Router(패킷 perm/drop), Bastion Host(패킷 인증)구성
스크린드 서브넷 : 외부네트워크와 내부네트워크 사이에 하나 이상의 경계 네트워크 생성
(스크리닝 라우터 2개, 배스천 호스트 1개)

침입탐지 시스템(Intrusion Detection System : IDS)

DB에 저장된 패턴정보를 바탕으로 시스템의 침입을 실시간으로 모니터링하는 보안 시스템 (수동적)

- 오용탐지 : 침입패턴 – 활동로그 비교 , 오탐율(FP) 낮음, 새로운 패턴 탐지 불가능
  (패턴 비교, 전문가 시스템, 유전 알고리즘)
- 이상탐지 : 정상패턴 – 활동로그 비교 , 오탐율 높음, 새로운 패턴 탐지 가능
  (신경망, 통계, 특징 추출, 머신러닝)

- NIDS(Network based IDS): 네트워크 패킷 검사(DoS, 해킹) 부가장비 필요
- HIDS(Host based IDS): 시스템상에 설치, 시스템로그 검사(바이러스, 웜)

Snort : 패킷탐지 침입탐지 시스템

Alert tcp any any -> any any ((msg: “massage”; sid : 10000000; content:”content” flag:SYN)

룰 헤더 룰옵션

〈룰 헤더〉

Action (alert, log, pass, dynamic)

Protocol(TCP,UDP, IP)

송신지, 수신지(any, 127.0.0.1)

Derection -> 〈〉

〈룰옵션〉

Msg: log 내용

Sid: 고유 ID

Content : 검사할 콘텐츠 내용

Flag(SYN, FIN , PSH):패킷 검사

Nocase: 대소문자 구분 x

침입대응 시스템(Intrusuon Prevention System : IPS)

공격 시그니처를 찾아 비정상 패턴을 감시하고 차단 (능동적)

허니팟(Honeypot): 의도적으로 취약한 사이트를 해킹에 노출시켜 해킹 기법, 행동 분석

가상 사설망(Virtual Private Network): 공중망을 이용하여 사설망을 가상으로 구축하는 방법 (USB사용 인증)

1)SSL VPN : 웹브라우저(SSL)을 이용한 VPN 소프트웨어 설치 필요 없음 (인증, 무결성, 기밀성, 부인 봉쇄)

2)IPSEC VPN: 터널모드(전체암호화, 새로운헤더 생성), 전송모드(End to End 보안)를 이용한 VPN

3)PPTP VPN: IP네트워크에 전송하기 위한 터널링 기법 (네트워크계층)

4)L2TP VPN: PPTP 호환성 터널링 프로토콜(네트워크 계층)

NAC(Network Access Control): 등록되지 않은 단말기 식별, 차단(End Point 솔루션), 네트워크 무결성

1) 정책관리 서버 : 정책설정, 접근 로그관리
2) 차단 서버 : 단말기 통제, 단말기 정보 수집 분류, 트래픽 감지
3) 에이전트 : 사용자 단말기 설치, 무선인증 지원
4) 콘솔 : 웹기반 네트워크 보안정책 성정, 감사, 모니터링, 대시보드 제공

ESM(Enterprise Security Management):

기업의 정보보안 정책을 반영, 보안시스템 통합한 통합 보안관제 시스템

-기업자산 및 자원관리

-보안감사, 상관성 분석

무선랜 보안기법

1)SDR(Service Set ID): AP는 동일한 SSID를 가진 클라이언트만 접속 허

2)WEP(Wired Equivalent Privacy): IEEE 802.11b RC4 스트림암호화 알고리즘, 40bit 키사용

3)WPA(Wi-Fi Protected Access): IEEE 802.1x/EAP, 128bit 동적 암호화

4)WPA2 : IEEE802.11i, WPA+AES

정보보안기사 필기 요약

Part3. 어플리케이션 보안

인터넷응용보안

1. FTP (File Transfer Protocol) : 파일 전송 프로토콜 (TCP 20 , 21 , 1024 ~ 65535)

(1) Active Mode : 접속 - 21번 Port / 데이터 전송 - 20번 Port

(2) Passive Mode : 접속 - 21번 Port / 데이터 전송 - 1024~ Port

FTP 종류

(1) FTP : ID/PW 인증, TCP

(2) tFTP : 인증 X , UDP

(3) sFTP : 전송구간에 암호화 기법사용 (기밀성)

FTP log 기록 (FTP 접속시 -l)

Xferlog 파일 기록

Sat Oct 29 21:35:39 2020 1 111.11.111.11 70 /home/aa.txt a _i r test ftp 0 * c

2020년 10월 29일 토요일 21시 35분 39초 111.11.111.11 IP에서 aa.txt 파일 업로드 성공

C (complete) : 성공

FTP 보안 취약점

Bounce Attack : 익명 FTP 서버 경유 호스트 스캔

Brute Force : 무작위 대입

tFTP Attack : 인증없이 접근

Anoymous FTP Attack

FTP Server week point

Sniffing

*FTP 사용자는 반드시 계정을 /etc/password nologin 으로 관리할 것

2. E-Mail 보안

Email 전송 방법

(1) SMTP (Simple Mail Transfer Protocol) TCP 25 / DNS MX / 응용계층

전자우편 송신 통신 규약

(2) POP3(Post Office Protocol Version3) TCP 110 / 응용계층

원격서버로 TCP/IP 통신으로 E-Mail 수신시 사용 수신 후 서버에서 메일 삭제

(3) IMAP

메일 서버에 저장 , 소프트웨어 상관 X, 복잡성 / 보안문제 해결

Email 보안 기법
(1) PGP (Pretty Good Privacy)
MIME(Multipurpose Internet Mail Extension) 객체 + 암호화 , 전자서명 프로토콜
송수신자 보안서비스 제공 / 평문 메시지 암호화
메세지 암호화(3DES, IDEA), 서명(DSS/SHA), 압축, 분할
전자우편 호환성, 세션키생성 (RSA, DiffieHelmen), 이메일 호환(ASC Code)

(2) PEM (Privacy Enhanced Mail)
인터넷 이메일 보안 시스템 중 하나
중앙 집중화된 키 인증 방식 -> 구현 어려움
군사, 은행 사용
메시지암호화(DES-CBC), 디지털서명(RSA, MD2, MD5), 인증(DES, MD2, MD5)
세션키 생성(DES , RSA, MD2), 전자우편 호환성

(3)S/MIME (Secure Multi-PurPose Internet Mail Extension)
표준보안 메일규약
메일 전체 암호화 (RSA, DES, SHA-1)
CA로부터 공개키 인증필요
첨부파일 보안
RSA사에서 개발

/etc/mail/access 작성규칙
RELAY : 특정 도메인 relay허용
DISCARD : 메일 수신 후 폐기
501 : 전체, 부분 특정 도메인 일치 시 메일 거부
550 : 특정 도메인 메일 거부

Spam 메일 차단 방법
RBL(Real Time Blocking List) : 참조서버로부터 유해 메일 전송IP 차단
SPF(Sender Policy Framework) : 발신자 SPF레코드를 DNS 저장 후 정보 확인

Spam Assasin (Perl)
점수를 이용하여 스팸차단 (90% 이상)
RBL 서버 참고
웹 서버 보안 (Web Server Security)
HTTPD(80)
Fork 함수를 통해 자식프로세스를 생성
설정파일 : /etc/httpd/conf/httpd.conf

아파치 웹서버 보안
주요 디렉터리 및 파일 접근 권한
Directory Listing

Server Tokens : 웹서버 정보 노출 (Prod : 최소한)
Server Signiture : 아파치 버전 및 서버 이름 노출

윈도우 웹서버 (IIS : Internet Information Server) : FTP, SMTP NNTP
서비스 : FTP, WWW, SMTP(메일), NNTP(뉴스)
계정 및 그룹 : IUSR_MACHINE(인터넷 접근 익명 계정)
IWAM_MACHINE(out-of-process 웹 애플리케이션 계정)
폴더 : %windir%₩system32₩inetsrv(IIS 프로그램)
%windir%₩system32₩inetsrv₩iisadmin(IIS 관리 프로그램)
%windir%₩help₩iishelp(IIS 도움말)
%systemdrive%₩inetpub(웹, FTP, SMTP 루트폴더)
웹사이트 : 기본 80 : %systemdrive%₩inetpub₩wwwroot
관리 3693 : %systemdrive%₩system32₩inetsrv₩iisadmin

웹 로그 분석
서버에서 발생하는 log : /var/log/httpd/access_log
서버에서 발생하는 에러 log : SeverRoot/logs/error_log

ErrorLog Level
Crit : 중대한 에러 발생
Emerge : 에러
Warn : 경고
Error : 중대하지 않는 에러

HTTP 상태코드
200 OK
403 Forbidden
404 Not Found
502 Bad Gateway
504 Gateway Time-out

DNS보안
DNS 확인 : ipconfig /displaydns DNS Cache 테이블 확인
DNS Query (UDP 53) : Recursive Query(순환) - Local DNS에 질의
Iterative Query(반복) - Local DNS - 외부 DNS Server 질의
DNSSEC : DNS 응답 정보에 전자서명 값 첨부

DB보안
DB위협요소
집합 (Aggregation) : 낮은 보안 등급의 정보들을 이용하여 높은 등급의 정보를 알아 내는 것
추론 (Inference) : 보안등급이 없는 정보를 접근하여 기밀정보를 유추

DB 보안 기법
Plugin : 데이터베이스 서버에 별도 암호화 솔루션 설치
API : 암호화 API 호출을 통해 암호화 수행

백업 방식
전체 백업
차등 백업 : 가장 최근에 수행된 전체 백업 이후 변경된 모든 DB 백업
증분 백업 : 가장 최근 백업 이후 변경된 것만 백업

전자상거래 보안

전자화폐: 전자기기에 전자기호 형태로 화폐적 가치를 저장, 전자적 지급수단으로 활용
전자화폐 요구조건
① 불추적성 (익명성) : 사생활 보호
② 가치이전성 : 즉시 양도 가능
③ 분할성 : 똑같은 가치 분할 가능
④ 독립성(완전 정보화) : 디지털 데이터 자체로서 완벽한 화폐가치를 가져야함
⑤ 익명성 취소 : 불법적으로 사용될 경우 사용자 노출 허용
Ex) 몬덱스, 비자캐시, PC Pay, Ecash, NetCash, 비트코인

SET(Secure Electronic Transaction)

- 신용카드 촉진을 위해 VISA와 MASTER CARD 공동 개발한 프로토콜
- 전자 상거래 인증 상호 작용 보장
- SSL 보다 속도 느림
- 지급결제 처리 복잡
- 기밀성, 무결성, 인증, 부인봉쇄 지원
- 이중서명, 이중해시
- 대칭키, 공개키, 전자서명, 해시함수, 전자봉투, 공개키 인증(X.509), 이중서명
- 알고리즘 : DES, RSA, SHA
- 사용자가 전자지갑 소프트웨어가 필요함

SSL(Secure Socket Layer) 443

- Netscape 개발
- 안전한 통신 지원
- 전송, 응용계층
- http, ftp, telnet, mail
- 기밀성, 무결성, 인증
- Random : 재생공격방지를 위한 난수

SSL구성요소

① Change Cipher Spec Protocol : SSL중 가장 단순한 프로토콜
협의된 알고리즘, 키교환 알고리즘, MAC 암호화, HASH 알고리즘 -> 클라이언트, 웹서버 공지
② 비정상적인 동작이 발생 될 때 사용되는 프로토콜 Level , Description 필드 있음
③ Record Protocol :
송신 - 협의된 알고리즘을 사용해 데이터를 암호화하고 산출된 데이터를 SSL에서 처리가 가능한 크기의 블록으로 나눔 후 압축 MAC(Message Authentication Code)를 붙여 전송
수신 - 데이터 복호화, MAC유효성 검사, 압축 해제, 재결합 -> 상위계층 전달

SSL HandShaking

①Client Hello : 클라이언트 브라우저 (암호알고리즘, 키교환 알고리즘, MAC암호화, HASH 알고리즘) > 서버
②ServerHello : 서버 (서버지원 알고리즘) > 클라이언트
2.5 Server Hello Done : 서버 (요청종료 공지)> 클라이언트
③Certificate : 클라이언트 (인증서 요청) > 서버(인증서) > 클라이언트(인증서 확인)
④Exchange Key (Premaster Key 전송) : 클라이언트(서버 공개키 암호화) > 서버
⑤인증서 확인 : 서버(Premaster Key) > 복호화
⑥Master Key 생성 : 서버 , 클라이언트 (PremasterKey 사용) > Session key 생성
⑦Client Finished : 클라이언트 (완료 공지) > 서버
⑧Server Finished : 서버 (동의, 알고리즘공지) > 서버

*Open SSL 취약점 (Heart Bleed):
오픈 암호화 라이브러리 하트비트 라는 확장모듈에서 웹브라우저 요청 시 데이터 길이 검증 없이 메모리 데이터 64kb 평문 노출

IPSEC(IP Security) : 안전한 인터넷 통신 규약, 가상 전용 회선 구축
전송방법
①터널모드 : IPsec탑재한 중계 장비가 패킷 전체를 암호화 + 새로운 IP header
New IP + ESP AH + IP …
②전송모드 : 출발지에서 암호화 목적지에서 복호화 End to End , Payload(데이터)만 암호화
IP + ESP AH + Payload …
AH : 데이터 무결성, IP 패킷 인증 / ESP : 암호화 전송, Replay Attack 방지

OTP(One Time Password): 한번만 생성된 난수를 패스워드로 사용
①동기식 (시간,이벤트): 고정된 시간 간격 주기로 난수 값 생성(시간), 인증횟수 기준값(이벤트)
②비동기식 (질의응답): 사용자(로그인) > 서버 (질의값) > 사용자 (OTP질의입력) > OTP 생성

SQL Injection
입력값을 우회해 SQL쿼리를 전송하여 DB값을 얻어내거나 권한 탈취 (' or 1=1 #)
공격 도구 : Havij, Panglin, HDSL
인증우회, Blind SQL Injection, Mass SQL Injection, Union SQL Injection

XSS(Cross Site Scripting):
실행가능한 스크립트를 재전송하는 공격 기법
세션갈취
공격대상 : 클라이언트

CSRF(Cross Site Request Forgery):
사용자의 권한을 탈취하여 웹사이트를 요청
서버와 클라이언트의 신뢰관계를 이용
공격대상 : 서버

DRM(Digital Right Management): 디지털콘텐츠 저작권 저작자의 권리, 이익을 보호 및 관리하는 시스템
WaterMarking: 디지털 콘텐츠 소유권 추적 기술
Fingerprint(Dual Water Marking) : 디지털 콘텐츠 구매자 정보 삽입

디지털 포렌식: 디지털 기기를 대상으로 한 특정 행위의 사실관계 증명을 위한 방법 및 절차
(준비- 획득/이송- 분석 - 분석서 작성 - 보관)
디지털 포렌식 원칙
①정당성 원칙(적법 절차) : 수집된 자료의 적법절차
②재현 원칙: 재현가능성
③신속성
④절차 연속성: 담당자 및 책임자 명확
⑤무결성: 증거 위변조 금지

휘발성데이터 수집 우선순위
Register/Cache > RoutingTable, ARPCache, ProcessTable, Kernal Statics > Memory > 임시파일 > Disk > Remote Logging, Monitoring Date > Physical Configuration, Network Topology > Archival media

비휘발성 데이터 수집 우선순위
Registry , 시간, Cache, Cookie, History, Email
암호화된 파일, 윈도우 로그

정보보안기사 Part4. 정보보호 일반

정보보호목표

기밀성(Confiedentiality): 인가된 사용자만이 정보에 접근할 수 있음.
비인가 사용자에게 정보가 노출되지 않음 (보안등급 설정)

무결성(Integrity): 인가된 사용자만이 권한에 따라 정보를 변경할 수 있음.
비인가 사용자의 정보 변경을 금지함. (해시함수)

가용성(Availablity): 인가된 사용자가 시스템 자원을 필요로할 때 접근 가능함 (RAID, DRS-Mirror)

정보보호 공격유형

변조(Modification): 원래의 데이터를 조작, 소스프로그램 변경 후 악성코드 실행, 특정 URL 접속 (Redirection ››)

가로채기(Interception): 네트워크상에서 전송되는 데이터를 복사, 열람하는 공격으로 **수동적공격** (Sniffing)

차단(Interruption): 정상적인 서비스를 방해하는 행위 (Dos, 프로세스 자원 고갈 공격)

위조(Fabrication): 송신되는 메시지를 변조하여 사용자를 속임

정보보호 대책

구체성분류

① 일반통제: 소프트웨어 생명주기에 대한 통제 (직무분리, 시스템 개발, 논리/물리적보안, 하드웨어통제, 비상계획 수립)

② 응용통제: 트랜잭션, 데이터 무결성 확보를 위한 통제 (입력, 처리, 출력 통제)

통제시점분류

① 예방통제: 능동적인 통제로 문제점을 사전에 식별하여 통제 수행
물리적 접근통제- 승인받지 못한 사용자의 정보시스템 접근을 금지
논리적 접근통제- 인증받지 못한 사용자의 정보시스템 접근 금지 (담장, 자물쇠, 보안 경비원 , 직무분리)

② 탐지통제: 발생한 사건(위협)을 식별하는 통제 (CCTV, 보안 감사, 감사로그, 침입탐지, 경보)

③ 교정통제: 발생한 사건을 교정 탐지된 위협과 취약점에 대응 (백신 소프트웨어)

사용자인증 방식 및 원리

① 지식기반인증 (Something you know : Password)
- 패스워드 공격 기법: 무차별공격 (BruteForce Attack, John the Ripper, hydra), 사전공격 (Dictionary Attack), 트로이목마, 사회공학, 스니핑

② 소유기반인증 (Something you have : 스마트카드, OTP)

③ 존재(생체)기반인증 (Something you are : 손바닥, 손, 홍채, 망막, 지문)
존재기반 : 생채특성, 지문, 얼굴, 홍채
생채인증 특징 : 보편성, 유일성, 지속성, 성능, 수용성(거부감이 없어야함), 저항성(위조 불가능)
생채인증 평가항목 : FRR(False Reject Rate, Type 1 Error): 잘못된 거부율
FAR(False Acceptance Rate, Type 2 Error): 잘못된 승인률

④ 행동기반 인증 (개인의 고유한 행동적 특성을 사용해 인증하는 기술: 서명, 키스트로크, 마우스 움직임, 걸음걸이, 모바일 패턴)

커버로스 인증

- 중앙집중형 사용자 인증 프로토콜 (RFC1510)
- 대칭키 암호화 기법을 기반으로하는 티켓기반 인증 프로토콜
- 윈도우서버 운영체제의 기본 인증프로토콜

커버로스 구성요소

KDC(Key Distribution Center): TGS+AS / 사용자와 서비스 암호화키 유지, 인증서비스 제공, 세션키 생성 및 분배

AS(Authentication Service): 실질적 인증 수행

Principals: 커버로스 프로토콜을 사용하는 모든 실제

TGS(Ticket Granting Service): 티켓을 만들고 세션키, 티켓 분배

Ticket: 인증토큰

접근통제(Access Control)

정보접근의 단계

식별-인증-인가

식별(Identification): 사람이나 객체의 유일성을 확인하는 절차

인증(Authentication): log-on 정보를 확인하는 보안 절차

인가(Authorization): 접근 권한 유무 판별 후 접근 권한 부여

접근통제(Access Control): 주체에 대한 객체의 접근을 통제
- 비인가된 접근을 감시
- 객체의 기밀성, 무결성, 가용성을 보장

인증방식에 따른 분류

인증	내용	기반	종류
Type 1	Something you know	지식	Password, Pin
Type 2	Something you have	소유	Smart Card, OTP
Type 3	Something you are	존재	홍채, 지문 , 정맥
Type 4	Something you do	행동	음성, 서명, 패턴

2-Factor 인증
인증방식 2가지를 동시에 사용하는 인증 방법

접근통제기술
① MAC(Mandatory Access Control : 강제적 접근 통제)
오직 관리자에 의해서 권한과 자원이 할당 됨
관리자로 부터 권한을 부여 받은 목록을 Security Lable에 작성

② DAC(Discretionary Access Control : 임의적 접근 통제, 신분기반)
자원에 대한 접근을 객체의 소유자가 권한을 부여 한다.

③ RBAC(Role Based Access Control : 역할 기반 접근통제)
관리자는 사용자에게 권리와 권한이 정의된 Role(역할)을 만들어 사용자에게 Role(역할)기반으로
권한을 할당하고 관리한다.

항목	MAC	DAC	RBAC
권한 부여자	System	Data Owner	Center Authority
접근 여부 결정 기준	Security Label (보안 등급)	신분 (identity)	역할 (Role)
장점	중앙 집중관리 안정적 시스템	유연 구현 용이	관리 용이
단점	구현 및 운영의 어려움 고비용	트로이목마 , ID 도용문제	제어정책이 제대로 반영되기 어려움
예시	방화벽 UNIX / Linux	ACL	HIPAA(보건보험)

접근통제 방법
① Capablity List : 주체별로 객체를 linked리스트로 연결하고 권한 할당
탐색시간이 오래걸림
② Access Control List : 주제와 객체간의 접근 권한을 테이블로 구성
사용자가 분포도가 안정적일 때 적합

접근통제 모델
① Bell-Lapadula
높은 등급의 정보가 낮은 레벨로 유출되는 것을 통제하는 모델 (기밀성 모델)
최초의 수학적 모델
TCSEC 근간
② Biba
주체에 의한 객체 접근의 항목 (무결성보장 모델)
No Read Down, No Write Up
③ Clark and Wilson (클락 윌슨 모델)
무결성중심의 상업용 설계, Application 보안 요구사항을 다룸
④ 만리장성 모델 (Chinese Wall = Brewer-Nash)
서로 상충 관계에 있는 객체간의 정보 접근을 통제하는 모델
기밀성중심의 상업용 설계

키분배 프로토콜

① 대칭키 암호화 (=비밀키):

암호화키와 복호화키가 동일한 암호화 기법 키교환 알고리즘 중요도 높음

- 기밀성 제공 무결성 인증 부인방지 X
- 암호화, 복호화 속도 빠름
- 대용량 Data 암호화 적합

스트림 암호 / 블록암호

구분	스트림암호 (Stream Cipher)	블록 암호(Block Cipher)
개념	Bit, 바이트 단위 암호화	Bit x n 블록단위로 암호화
방법	평문을 XOR 1Bit 단위 암호화	블록단위 치환 대칭 반복 (Feistel , SPN)
장점	실시간암호/복호화, 속도	대용량의 평문 암호화
종류	RC4, SEAL, OTP	DES, 3DES, AES, IDEA, SEED

② 공개키 암호화 (=비대칭키, 개인키) : 공개키로 암호화 개인키로 복호화하는 암호화 방법

인증, 서명 암호화 수행

키 배분, 공유, 키 저장문제 해결

인증, 부인방지 O

공개키암호화 종류

구분	특징	수학적 이론	장점	단점
Diffie Hellman	최초의 공개키 알고리즘 키 분배 전용 알고리즘	이산대수	키 분배에 최적화	인증불가 위조에 취약
RSA	대표적 공개키 알고리즘	소인수분해	Library 다양화	키 길이 증가
DSA	전자서명 알고리즘 표준	이산대수	간단한 구조	전자서명 전용 암호화, 키 교환 불가
ECC	PDA, 스마트폰 핸드폰	타원곡선	오버헤드 적음	키 테이블 필요

전자서명 서명과 인증

전자서명(Digital Signature): 서명자가 해당 전자문서에 서명하였음을 나타내기 위해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보

- 개인의 고유성 인증, 무결성/ 추적성 확보

전자서명 특징

① 위조불가 : 합법적 서명자(개인키 有)만이 전자서명 생성 가능

② 변경불가 : 서명한 내용을 변경 할 수 없음

③ 재사용불가 : 서명을 다른 전자문서의 서명으로 사용불가

④ 부인방지 : 서명후 서명자는 서명한 사실을 부인할 수 없음

⑤ 서명자인증 : 전자서명 서명인을 검증 가능 (서명자의 공개키)

메세지, 전자서명, 키교환

----------송신자----------

메시지 1

① Message Digest 생성 - 해쉬함수

② 전자서명 - 송신자의 개인키 (RSA)

③ 전자서명 암호화 - 송신자의 비밀키(대칭키) (DES)

메시지 2

④ Message - 송신자의 비밀키(대칭키) (DES)

⑤ 암호문 생성

----------전자서명 완료----------

⑥ 송신자의 비밀키(대칭키) 암호화 전달 - 수신자의 공개키 (RSA)

----------수신자----------

⑦ 송신자의 비밀키 획득 (DES) - 수신자의 개인키

메세지 1

⑧ 전자서명 획득 - 송신자의 비밀키(대칭키) (DES)

⑨ Message Digest 획득 - 송신자의 공개키 (RSA)

사용자인증

메세지 2

⑩ Message 획득 - 송신자의 비밀키(대칭키) (DES)

⑪ Message Digest 획득 - 해쉬함수
메시지인증

⑫ 전자서명확인 -⑨,⑪Message Digest 비교

---------- 인증완료----------

송신자: 개인키 - 전자서명
  공개키 - 전자서명 확인
수신자: 개인키 - 복호화
  공개키 - 암호화

전자서명 기법의 종류

RSA	소인수분해 암호화/복호화 송신자의 개인키와 공개키 사용
EIGamal	이산대수
Schnorr	EIGamal기반 크기 축소 IC 카드 활용
DSS (Digital Signature Standard)	EIGamal기반 계산량 감소 미국 전자서명 표준 전자서명만 지원
KCDSA (Korea Certificate-based Digital Signature Algorithm)	이산대수 국내 전자서명 표준
ECC	타원곡선 짧은 키 사용 짧은 시간 내 전자서명 생성 ECDSA(Elliptic Curve Digital Signature Algorithm)

PKI(Public Key Infrastructure)
공개키 암호 방식을 바탕으로 디지털인증서를 활용하는 SW, HW, USER, 정책 및 제도 총칭
은행, 증권, 카드 보험에서 사용하는 공인인증 구조로 공인인증서(X.509, ITU-T표준)을 통해 인증받는 구조

PKI 기능

인증 (Authentication)	사용자에 대한 신원 확인 (공개키 인증)	인증서 X.509
기밀성 (Confidentiality)	송/수신정보 암호화	암호/복호 화 AES, SEED, 3DES
무결성 (Integrity)	송/수신정보 위조불가 보장	해시함수 SHA, MD5
부인봉쇄 (Non-Repudiation)	송/수신자 송수신 사실 부인 불가	전자서명
접근 제어 (Access Control)	허가된 수신자만 정보 접근	DAC, MAC, RBAC
키 관리 (Key Management)	공개키 생성, 등록, 분배, 폐지, 관리	CA

PKI 구성
인증관련기관
① 인증기관(CA :Certification Authority): 인증정책 수립, 인증서 관리
② 등록기관(RA :Registration Authority): 신원확인, CA인증서 발급요청
인증서 암호/키 관리
③ CRL(Certificate Revocation List): 인증서 폐기 목록
④ Directory : 인증서, 암호키 저장 및 관리 (X.500, LDAP)
인증도구
⑤ X.509: CA 발행하는 인증서 기반 공개키 인증서 표준 포맷 (사용자신원 + 키정보)
⑥ 암호키 : 개인키,공개키

X.509 인증서 내용
인증서버전, 인증서 고유번호, 발급자의 서명, 발급자 정보
인증서 유효기간, 주체 정보, 공개키, 주체키

암호학(Cryptology)
암호화기법
① 치환(Substitution): 혼돈 ,문자열을 다른 문자열로 이동하면서 교체
A-C B-D C-E
② 전치,순열(Transposition, Permutation): 확산, 문자의 순서를 바꿈
A-C B-E D-A
③ 대칭키(비밀키) 암호화: 송/수신자의 키가 동일
④ 공개키 암호화: 개인키(사설키), 공개키
⑤ 양자암호: 양자역학의 원리를 이용한 암호화 방식

정보이론(Claud Shannon- Infomation Theory):
혼돈(chaos): 암호문과 평문과의 상관관계를 숨김 (대치)
확산(diffusion): 통계적 성질을 암호문 전반에 퍼뜨려 숨김 (전치, 순열)

대칭키 암호화
(1) 스트림암호화 기법(RC4, SEAL, OTP):
비트/바이트 단위로 암호화 수행
고속암호화, 하드웨어 구현용이
wifi, OTP

(2) 블록암호화 기법(DES, 3DES, AES):
고정된 길이의 입력 블록 - 고정된길이 출력블록 변환하는 알고리즘
Feistel(역추적가능), SPN(역추적 불가능)구조
① ECB(Electronic Code Book): 가장 단순한 모드 블록을 순차적으로 암호화 (독립적)
② CBC(Cipher Block Chain): 블록 / IV(Initialization Vector) XOR 연산 (독립적)
③ CFB(Cipher FeedBack): 암호화 IV / 블록 XOR 연산 (연쇄적)
④ OFB(Output Feedback): IV 암호화 - (블록2전송) XOR 블록1 연산 (연쇄적) 영상데이터, 음성데이터
⑤ CTR(CounTer): 블록 / 키스트림 XOR 암호화시 1증가하는 카운터 암호화

블록암호화 알고리즘
① DES(Data Encryption Standard): Feistel
대칭키 암호화 알고리즘으로 미국/국제표준 알고리즘
입력:64Bit 출력:64Bit 치환암호+전치암호(혼합암호)
*현재는 128Bit이상 사용

② IDEA(International Data Encryption Algorithm): SPN
스위스에서 개발한 대칭키 암호화 알고리즘
입력:128Bit 출력:64Bit
전자우편 PGP방식에 사용
HW/SW 구현 용이
DES 2배 빠른속도

③ RC5(Ron&s Code 5):
DES 10배 빠른속도
32/64/128Bit

④ AES(Advanced Encryption Standard): SPN
NIST(미국국립표준연구소) 표준 알고리즘
크기제한 없음
128/192/256Bit

⑤ SEED: Feistel
KISA/ETRI 대칭키 블록 암/복호화 알고리즘
128Bit

암호분석 방법의 종류
① 암호문 단독 공격 (COA : Ciphertext only Attack):
암호문만으로 공격 , 통계적 성질/문장특성 추정

② 알려진 평문 공격 (KPA : Known Plaintext Attack):
암호문에 대응하는 일부 평문 가용

③ 선택 평문 공격 (CPA : Chosen Plaintext Attack):
평문 선택시 대응되는 암호문을 얻을 수 있는 상태에서의 공격

④ 선택 암호문 공격 (CCA : Chosen Ciphertext Attack):
암호문 선택시 대응되는 평문을 얻을수 있는 상태에서의 공격

비대칭키암호화
① 디피헬먼(Diffie-Hellman):
최초의 공개키 암호화 알고리즘
IPSEC IKE 키교환 알고리즘
중간자 공격에 취약

② RSA(Rivest, Shamir, Adelman):
공개키 암호화방식의 산업표준
소인수분해
전자서명

해시(Hash)함수 (MD5, SHA-256, LSH):
복호화가 불가능한 일방향 암호기술
무결성만 지원

해시함수 조건
① 압축: x 길이 평문을 고정된 길이의 출력값으로 변환
② 일방향 (One Way Function, 선이미지 회피성): 역방향 계산 불가능
③ 효율성: 해시값 계산에 시간이 많이 소요되지 않아야 함
④ 충돌회피 (Collision free, 강한 충돌회피성): h(M1)=h(M2) M1,M2 계산불가능
⑤ 2차 선이미지 회피성 (약한 충돌회피성): h(M1) = h(M2) M1!= M2 계산불가능

정보보안기사 Part5. 정보보안 관리 및 법규

정보보호 관리 이해

ISMS (infomation Security Management System)

정보보호 관리체계인증

정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인터넷 인증기관이 증명하는 제도

관리체계 수립 및 운영, 보호대책 요구사항에 대한 인증

ISMS-P (infomation Security Management System - Personal)

정보보호 및 개인정보보호 관리체계 인증

정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도

ISMS+개인정보 처리 단계별 요구사항에 대한 인증

법령	과학기술정보통신부	방송통신위원회	행정안전부
고시	정보보호	개인정보보호	
	ISMS-P		

ISMS 의무 인증 대상자

① 정보통신망서비스를 제공하는 자 (ISP) : 인터넷 접속 / 인터넷 전화

② 직접 정보통신 시설 사업자 (IDC) : 서버 호스팅 / 코로케이션

③ 정보통신서비스 매출액 100억 또는 이용자 수 100만명 이상인 사업자

④ 연간 매출액 및 세입등이 1500억이상인 기업 중 상급종합병원 / 1만 이상 재학생이 있는 학교

-미 인증 시 3000만 원 이하 과태료

정보보호 거버넌스 체계 수립

Secvurity PDCA(Plan, Do, Check, Act)

① 관리체계기반 마련 : 상위수준의 정보보호 정책 수립, 정보보호 관리체계 인증 범위 확정, 모든 정보자산 식별

② 위험관리 : 자산식별, 위협, 취약점 점검, 위험평가 수행, 보호대책 계획 수립

③ 관리체계 운영 : 정보보호 관리체계 수립 이행 단계, 보호대책 구현, 보호대책 공유 운영현황 관리

④ 관리체계 점검 및 개선 : 매년 1회 이상 관리체계 점검 및 개선

정보보호 위험평가

위험관리 : 위험을 식별, 분석, 평가, 보호대책을 수립하여 조직의 손실을 최소화 하는 일련의 활동 (정성적/정량적기법)

위험관리구성 : 자산(Asset), 위험(가능성 Risk), 위협(조건,사건,행위 Threat), 취약점(Vulnerablity)

위험분석 : 위험분석 및 평가 방법론 과학적/정형적인 과정

(1) 접근 방식에 따른 위험분석 기법

기준선 접근법(Base Line Approach), 전문가 판단(Infomal Approach), 상세위험분석(정성적/정량적 분석기법 Detailed Risk Analysis), 복합적 접근법(Combined Approach)

(2) 정량적 위험분석과 정성적 위험분석

① 정량적 위험분석

ALE(연간기대손실)= SLE(위험발생확률) X ARO(손실크기)

유형 : 수학공식 접근법, 확률 분포 추정법, 확률 지배, 몬테카를로 시뮬레이션, 과거 자료 분석법

분석시간, 노력, 비용⤊

② 정성적 위험분석

위험에 대한 우선순위를 정하는 기법

유형 : 델파이 법, 시나리오법, 순위 결정법, 질문서법

주관적 분석

위험대응 전략

① 위험수용 : 위험을 받아들이고 비용을 감수

② 위험감소 : 위험을 감소시킬 수 있는 대책을 구현

③ 위험회피 : 위험이 존재하는 프로세스나 사업을 포기

④ 위험전가 : 잠재적 비용을 제3자에게 이전하거나 할당

정보보호 대책 구현 및 운영 (ISMS / ISMS-P)

(1) 관리체계 수립 및 운영

관리체계기반마련, 위험 관리, 관리체계운영, 관리체계 점검 및 개선

(2) 보호대책 요구사항

정책/조직 자산관리, 인적보안, 외부자보안, 물리보안, 인증 및 권한관리, 접근통제, 암호화적용, 정보시스템도입 및 개발보안

시스템 및 서비스 영관리, 시스템 및 서비스 보안관리, 사고 예방 및 대응, 재해복구

(3) 개인정보 수집 시 보호처리

개인정보 집 시 보호조치, 개인정보 보유 및 이용 시 보호조치, 개인정보 제공 시 보호조치, 개인정보 파기 시 보호조치, 정보주체 권리보호

업무 연속성 계획 및 재난복구 계획

BCP (Business Continuity Planning, 사업 연속성 계획)

- 상시에 기업의 존립 유지를 위한 프로세스를 정의한 복구 절차
- 업무의 중단상황 그 이후 업무 기능 및 프로세스 지원

BCP 절차

① 연속성 계획 정책 선언서 개발

② BIA(Business Impact Analysis) 수행

③ 예방통제 식별

④ 복구전략 개발

⑤ 연속성 계획 개발

⑥ 계획 및 테스트 및 훈련

⑦ 계획의 유지 관리

DRP(Disaster Recovery Planning, 재해 복구 계획)

- 비상 환경에서 기업의 존립을 위한 필수적인 IT자원에 대학 복구 절차
- 사이트의 목표시스템, 응용 프로그램, 컴퓨터 설비의 운영 재개와 같은 IT 중심 계획

비상계획 형태 (업무/IT/보안/인명자산/신뢰)

① BCP(Business Continuity Plan) : 복구 시 필수 업무 운영 유지 절차제공

② BRP(Business Recovery or Resumption Plan): 재해 후 즉시 업무 운영의 복구 절차제공

③ COOP(Continuity Of Operation Plan): 필수적/전략적 기능 대체사이트에서 30일 이상 유지 절차제공

---

④ DRP(Disaster Recovery Plan): 대체 사이트에서의 복구 능력 촉진 절차 제공

⑤ IT Contingency Plan/Continuity Of Support Plan: 응용/지원시스템 복구 절차/능력제공

---

⑥ CIRP(Cyber Incident Response Plan): 악성 사이버 사건 탐지/대응/확산 방지 절차제공

---

⑦ OEP(OccupantEmergencyPlan): 인명 최소화 + 자산충격보호

---

⑧ CCP(Crisis Communication Plan): 현 상황 개선, 주주, 공적 기관에 알리는 절차제공

BIA(Business Impact Analysis, 사업영향분석)

- 비즈니스 별로 위험을 분석, 복구 목표수립 (정량적/정성적)
- 자원식별, 최대유휴시간 산정, 업무프로세스 우선순위 결정

재해복구 시스템의 종류

Mirror	Active-Active	0~min
Hot	Active-Standby	~24H
Warm	중요한업무위주	~D
Cold	서버/소프트웨어 구매	~W

정보보호 시스템 인증

정보보호 시스템 제품을 객관적으로 평가하여 정보보호 제품의 신뢰성을 향상시키려는 인증제도

TCSEC(Trusted Computer System Evaluation Criteria, Orange Book)
- 독립적인 시스템 평가
- BLP(Bell-LaPAdula)모델 기반
- 기밀성 강조
- 정보 조달 요구사항 표준화
- 기능성 보증 구분x

ITSEC(Infomation Technology Security Evaluation Criteria)
- OS, 장치 평가
- 기밀성, 무결성, 가용성
- 기능성 보증 구분

CC(Common Criteria)
- CCRA 가입국 간의 정보보호 제품에 대한 상호인증
- ISO15408인증
- 주요기능 PP(Protection Profile), ST(Security Target, 보안명세서) ToE(Target of Evaluation, 평가대상) EAL(Evaluation Assurance Lv. 등급)

GDPR(General Data Protection Regulation)인증
- 유럽연합 내의 개인 데이터 보호기능 강화 통합하는 EU규정
- 주요원칙 (개인정보처리, 동의, 아동개인정보, 민감정보)

클라우드 컴퓨팅 서비스 보안 인증제도

클라우드 서비스 종류

IaaS(Infrastructure as a Service) : 컴퓨팅 자원, 스토리지 등 정보시스템 인프라를 제공하는 서비스

Saas(Software as a Service) : 애플리케이션 제공 서비스

Paas(Platform as a Service) : 클라우드 개발 플랫폼 제공 서비스

SECaaS(Security as a Service) : 클라우드 기반 보안 서비스 제공

개인정보영향평가제도

제35조(개인정보 영향평가의 대상)

1. 민감정보 개인정보 파일 5만명 이상
2. 내/외부 공공기관 개인정보파일 연계 50만명 이상
3. 개인정보파일 100만명 이상

ISO 27000 표준

ISO 27001 : 인터넷 진흥원에서 개발한 ISMS 인증 (ISMS 수립, 구현, 운영, 모니터링, 검토, 유지 및 개선하기 위한 요구사항 규정)

정보보호 관련 윤리 및 법규

OECD 개인정보 8원칙

개인정보의 일반원칙으로 인정

수집제한의원칙 / 정보의 정확성의 원칙 / 목적 명확화의 원칙 / 이용제한의 원칙 / 처리방침 공개의 원칙 / 정보주체의 참여의 원칙 / 책임의 원칙

정보통신망법 적용대상

① 정보통신서비스 제공자

② 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은자

③ 개인정보의 취급 업무를 위탁받은자

④ 방송사업자

ex) 포털, 병원, 학교등 360만 사업자 / 부처, 지자체, 학교 등 20만 공공기관

제21조(개인정보의파기)

1. 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야한다.

제24조의2(주민등록번호 처리의 제한)

1. 주민등록처리가 불가피한 경우 행정안전부령으로부터 정하여 처리할 수 있다.

제 30조(개인정보 처리방침의 수립 및 공개)
① 개인정보의 처리 목적
② 개인정보의 처리 및 보유 기간
③ 개인정보의 제3자 제공에 관한 사항
④ 개인정보처리의 위탁에 관한 사항
⑤ 정보주체와 법정대리인의 권리/의무 및 그 행사 방법에 관한 사항
⑥ 제 31조에 따른 개인정보보호책임자의 성명 또는 개인정보보호업무 및 관련 고충 사항을 처리하는 부서의 명칭과 전화번호
⑦ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치/운영 및 그 거부에 관한 사항

제33조(개인정보 영향평가)
① 처리하는 개인정보의 수
② 개인정보의 제3자 제공 여부
③ 정보주체의 권리를 해할 가능성 및 그 위험 정도

정보통신기반 보호법(시행령)
제9조(정보보호책임자의 지정 등)
1. 법 제5조 제4항 본문에 따라 관리기관의 장은 소관 주요정보통신기반시설의 보호 업무를 담당하는 4급/4급 상당 공무원, 5급/5급상당 공무원, 영관급장교 또는 임원급 관리/운영자를 정보보호책임자로 지정하여야 한다.