

* 디자인 패턴

- 생성: abstract, builder, prototype, singleton, factory method
- 구조: adapter, bridge, composite, decorator, facade, flyweight, proxy
- 행위: observer, visitor, command, interpreter, iterator, mediator, memento, state

* 린바우 분석기법(객동기)

- 객체: 객체 다이어그램
- 동적: 상태 다이어그램
- 기능: 자료흐름도

*

- 개체 무결성: 기본키는 null 값이 될 수 없음
- 참조 무결성: 외래키는 참조할 수 없는 값을 가질 수 없음
- 도메인 무결성: 특정 속성값은 그 속성이 정의된 도메인에 속한 값이어야 함

* DDL: create, alter, drop

DML: select, insert, delete, update

DCL: commit, rollback, grant, revoke

* Keying

1. 양방향

1) 개인키

- 스트림 방식: LFSR, RC4
- 블록방식: DES(IBM), AES, SEED(국내), ARIA(국내), IDEA, RC5

+) 대칭 암호: 속도 빠름, 키 교환 필요

2) 공개키 암호화: RSA(MIT), ECC -> 비대칭 암호(암호화 키는 공개, 복호화 키는 비밀)

* SW 비용 추정 모형

1) COCOMO: LOC(비관치, 낙관치, 기대치) 기반 비용

- Embedded: 초대형
- Organic: 중소 규모, 5만 라인
- Semi-Detached: 중간단계, 30만 라인

2) Putnam: Payleigh-Norden 곡선의 노력 분포도 -> SLIM

3) 기능 점수 모델

* 시스템 품질 속성:가용성, 변경용이성, 성능, 보안성, 사용편의성, 시험용의성

* CASE(computer aided software engineering)

- 모듈의 재사용성 향상
- 자동화된 기법
- 유지보수 간편
- 원천 기술: 구조적 기법, 프로토타이핑, 자동프로그래밍, 정보 저장소, 분산처리

- 상위 CASE -> 요구 분석과 설계 단계 지원

: 모순 검사, 오류 검증, 자료흐름도 작성

- 하위 CASE -> 코드 작성, 테스트, 문서화

* 블랙박스 테스트 VS 화이트박스

1) 블랙박스 테스트 -> 내부구조나 작동원리를 모르는 상태, 동작 검사

- 경계값 분석
- 기능 테스트

2) 화이트박스 테스트 -> 내부 구조와 동작을 검사, 내부 소스코드 테스트

- 문장 검증
- 선택 검증
- 경로 검증
- 조건 검증
- 기본 경로는 사이클을 최대 한 번만 지나야함

* 속성 = attribute = 차수 degree

튜플 = cardinality

* E-R 그래픽 표현

- 개체타입: 사각형
- 속성: 원형
- 관계타입: 마름모
- 연결: 선
- 다중 값 속성: 이중타원

* 이상현상

- 삽입 이상
- 삭제 이상
- 갱신 이상

* 정규형

1-2-3-BCNF-4-5 도-부-이-결-다-조

- 도: 도메인 분해
- 부: 부분 함수 종속 제거
- 이: 이행 함수 종속 제거
- 결: 결정자가 후보키가 아닌 함수 종속 제거
- 다: 다중치 종속 제거
- 조: 조인 종속 제거

* 결합도

(낮) date – stamp – control – external – common – content (높)

* 응집도

(약) 우연적 – 논리적 – 시간적- 절차적 – 교환적 – 순차적 – 기능적 (강)

* A class: ~127

B class: 128~191

C class: 192~223

D class: 224~239

E class: 240~255

* 페이지 교체 알고리즘

- OPT(optimal)
- FIFO
- LR(least recently used)
- LFU
- MFU
- NUR(not used recently)

* VLAN: 논리적으로 LAN 구성

STP: 우선순위에 따라 1개의 경로만

ARP: 물리적 네트워크 주소로 대응

* 빌드 자동화 도구: ANT, Maven, Gradle

형상 관리 도구: GIT, CVS, Subversion

* 저작권 관리 구성 요소

- 콘텐츠 분배자
- 패키지
- 클리어링 하우스
- DRM 컨트롤러

* 정렬

- 퀵 정렬: 많은 자료 이동을 없애고 하나의 파일을 부분적으로 나누어 가면서 정렬
- 삽입정렬: 가장 간단한 정렬 방식
- 셸 정렬: 삽입 정렬 확장 개념
- 선택 정렬: n개의 레코드 중 최소값을 찾음
- 버블 정렬: 인접한 두 개의 레코드 키 값을 비교하여 위치 교환
- 힙 정렬: 전이진 트리 이용
- 2-way 합병 정렬: 이미 정렬되어 있는 두 개의 파일을 한 개의 파일로 합병

* $O(N \cdot \log 2N)$: 퀵정렬, 병합정렬

$O(N^2)$: 버블정렬, 삽입정렬, 선택정렬

* 인터페이스 구현 검증 도구: xUnit, STAF, Fitness, NTAF, Selenium watir

* 스택을 이용한 연산: 재귀호출, 후위표현, 깊이우선탐색
큐를 이용한 연산: 선택정렬

* 스택: 한쪽 끝으로만 삽입, 삭제 작업(top-bottom), 후입선출
큐: 한쪽에서는 삽입, 다른 한쪽에서는 삭제, 선입선출

* 병행제어 기법

- 로킹 기법
- 타임 스탬프 기법
- 최적 병행 수행 기법: 검증, 확인, 낙관적
- 다중 버전 기법

* CSMA/CA: 충돌 방지(collision avoidance)
CSMA/CD: 충돌 감지(collision detection)

* 연산자

1) 순수 관계 연산자

- select σ : 수평단절, 행을 다가져옴
- project π : 수직단절, 열을 다가져옴
- join \bowtie
- division \div

2) 일반 집합 연산자

- union 합집합
- intersection 교집합
- difference 차집합
- cartesian product 교차곱

* 스레싱 현상: 페이지수행 시간보다 교환시간이 커질 때 발생하는 것

*

- SAN: 멀티 프로토콜 기능 활용, 여러 저장장치나 백업 장비 단일화
- MBR: memory buffer register, 잠시 기억되는 레지스터
- NAC: network access control, 보안 관리
- NIC: 물리 계층과 데이터 계층의 서비스 제공

* SSH(Secure Shell)

- 기본 네트워크 포트 22번
- 전송되는 데이터 암호화
- 공개키를 서버에 등록
- 원격 명령실행이나 셸 서비스 수행

*

- Bell-Papadula Model: 상하 관계가 구분된 정보 보호
- BLP 기밀성 모델: 불법적인 비밀 유출 방지에 중점
- Clark-Wilson 무결성 모델: 자료의 변조 방지
- Chinese Wall: 충돌을 야기하는 정보의 흐름 없어야함

* 생명 주기 프로세스

- 기본: 획득, 공급, 개발, 운영, 유지보수
- 지원: 품질 보증, 검증, 확인, 활동 검토, 문제 해결
- 조직: 관리, 기반 구조, 훈련, 개선 프로세스

* SPICE 모델: 소프트웨어 프로세스 평가 및 개선하는 국제 표준

0단계: 불안정

1단계: 수행

2단계: 관리

3단계: 확립

4단계: 예측

5단계: 최적화

* 해싱 함수

- 제산법: 해시표로 나눈 나머지를 홈 주소로 사용
- 제곱법
- 폴딩법(중첩법): XOR한 값
- 숫자분석법: 키 값을 이루는 숫자의 분포 분석
- 기수 변환법: 진수를 달느 진수로 변환
- 무작위 방법

* 즉각 갱신 기법: 데이터베이스 로그를 필요로 하는 회복 기법

* IEEE 802 표준 규약

- IEEE 802.3: CSMA/CD
- IEEE 802.4: 토큰 버스
- IEEE 802.5: 토큰 링
- IEEE 802.8: Fiber optic LANS
- IEEE 802.9: 음성/데이터 통합 LAN
- IEEE 802.11: 무선 LAN(CSMA/CA)

* 페이지징: 동일한 크기로 나누는 기법

세그먼테이션: 다양한 크기로 나누는 기법

* Char(문자): 문자 하나를 저장

String(문자열): 나열된 여러 개의 문자

* SDDC(software defined data center): 소프트웨어 정의 데이터 센터
Wi-SUN(와이선): 사물 인터넷 서비스를 위한 저전력 장거리
BaaS: 서비스형 블록체인

* 정적 분석 도구: pmd, cppcheck, SonarQube, ccm
동적 분석 도구: valance

* IPSec(IP Security)

- ESP: 발신지 인증, 데이터 무결성, 기밀성 보장
- 운영모드는 Tunnel 모드, Transport 모드로 분류
- AH: 발신지 호스트 인증, IP 패킷의 무결성 보장

* Secure Os 보안운영체제의 기능

- 강제접근통제(MAC): 등급에 따라
- 임의접근통제(DAC): 사용자의 신원에 따라
- 사용자계정컨트롤(UAC): 관리자 수준의 권한이 필요한 작업 수행할 때 사용자에게 알림
- 자료별 접근통제(Date-Label Access Control)
- 객체 재사용 방지
- 완전한 중재 및 조정
- 감사 및 감사기록 축소
- 안전한 경로
- 보안 커널 변경 방지
- 해킹 방지
- 통합 관리

* mkdir: 디렉토리 생성 명령어

ftp: 응용계층 프로토콜

nmap: 스캐닝, 보완취약

* UNIX 명령어

- ls: 디렉토리, 파일목록 출력
- cat: 파일 내용 출력
- chmod: 접근 권한 변경

* WAS: 애플리케이션 수행 미들웨어

MOM: 메시지 지향 미들웨어

RPC: 원격 프로시저 호출

ORB: 네트워크 호출 미들웨어

* 객체지향 분석 방법론

- Booch: 미시적, 거시적 개발 프로세스
- Jacobson: use case 사용
- Coad-Yourdon: E-R 다이어그램
- Wirfs-Brock: 고객 명세서
- 럼바우 기법

* 체크박스: 여러개의 선택 상황에서 1개 이상

라디오버튼: 여러 항목 중 하나만

텍스트박스: 데이터 입력하고 수정

토글: 둘중 하나

* 세션 하이재킹

- 비동기화 상태 탐지
- ACK STORM 탐지
- 패킷의 유실 및 재전송 증가 탐지

* 기본키: 후보키 중에서 선택된 주 키

후보키: 유일하게 식별하기 위한 기본키, 유일성과 최소성 만족

슈퍼키: 유일성 만족, 최소성은 만족X

외래키: 릴레이션에서 참조하고 있는 것

* byte = 1 Byte

short = 2 Byte

int = 4 Byte

long = 8 Byte

* 커널

- 프로세스(CPU 스케줄링) 관리
- 기억장치 관리
- 파일 관리
- 입출력 관리
- 프로세스 간 통신
- 데이터 전송 및 변환
- 주기억장치에 상주

VS 쉘

- 시스템과 사용자간의 인터페이스 담당
- 명령어 해석기
- 보조기억장치에 상주

- * 접근제어자 in 자바
 - public: 모든 접근을 허용
 - protected: 같은 패키지에 있는 객체와 상속관계의 객체만 허용
 - default: 같은 패키지에 있는 객체만 허용
 - private: 현재 객체 내에서만 허용
- * 인터넷 계층의 프로토콜
 - IP: 데이터 주소를 지정하고 경로 설정
 - ICMP: 오류처리와 전송 경로 변경을 위한 제어 메시지 관리
 - IGMP: 멀티캐스트 그룹 유지
 - ARP: IP주소를 네트워크 접속 장치의 물리적 주소로 변환
 - RARP: ARP 반대(물리적 주소를 IP 주소로 변환)
- * CMM 모델: 초기, 관리, 정의, 정량적 관리, 최적화
- * SOA(service oriented architecture): 표현, 프로세스, 서비스, 비즈니스, 영속 계층
- * SREM: 우주 국방 시스템, 실시간 처리
 - PSL/PSA: 미시간 대학
 - HIPO: 하향식 소프트웨어
 - SADT: 구조적 요구 분석

*

	MAC	DAC	RBAC
권한 부여	시스템	데이터 소유자	중앙 관리자
접근 결정	보안등급	신분	역할
정책 변경	고정적	변경 용이	변경 용이
장점	안정적, 중앙 집중적	구현 용이, 유연함	관리 용이

- * XSS: 웹페이지에 악의적인 스크립트를 포함시켜 사용자 측에서 실행되게 유도-> 정보 유출 유발
- * 시퀀스 다이어그램: 액터, 활성 객체, 라이프라인, 메시지, 제어 삼각형
- * ISO/IEC 9126: 품질 특성 및 척도
 - ISO/IEC 14598: 제품 평가
 - ISO/IEC 12119: 패키지 소프트웨어 평가
- * McCabe cyclomatic의 수 $V(G) = \text{화살표} - \text{동그라미} + 2$
- * Mashup: 웹에서 제공하는 정보를 이용해 새로운 소프트웨어나 서비스, 데이터베이스를 만드는 기술

- * Quantum Key Distribution: 양자 암호 관련
- * Grayware: 사용자 동의를 받아 설치하는 프로그램
- * 파레토 법칙: 오류의 80%는 전체 모듈의 20% 내에서 발견
- * 교착상태 필요 충분 조건: 상호 배제, 점유와 대기, 환형 대기, 비선점
- * IPv6: 유니캐스트, 멀티캐스트, 애니캐스트
IPv4: 브로드 캐스트
- * 백도어 탐지 방법
 - 무결성 검사
 - 로그 분석
 - SetUID 파일 검사
 - 열린 포트 검사
 - 바이러스 및 백도어 탐지 툴 이용
- * JSON: 데이터의 객체를 속성, 값의 쌍 형태로 표현하는 방식
- * XML: 특수한 목적을 갖는 마크업 언어를 만드는데 사용
- * tripwire: 크래셔가 침입하여 백도어를 만들어 놓거나 설정 파일을 변경했을 때 분석하는 도구
- * PICONET: UWB 기술, 블루투스 기술을 사용해 통신망을 형성하는 무선 네트워크 기술
- * tcp wrapper: 접속 인가 여부 점검
- * 사용자 수준 스레드: 전환 없이 스레드 교환 가능
커널 수준 스레드: 성능 향상, 시스템 동시 호출, 독립적 스케줄링
- * IP 프로토콜
 - 패킷 분할, 병합하는 기능 수행
 - 비연결형 서비스
 - 헤더 체크섬만 제공
 - BEST EFFORT 원칙에 따름
- * UDP
 - 비연결형 및 비신뢰성 전송 서비스
 - 전송 속도가 빠름
 - 순서 재조정 기능 지원X
 - 복구 기능 제공X

* RIP

- IGP에 해당
- Bellman-Ford 알고리즘 사용
- 소규모 네트워크 환경에 적합
- 15홉 이하로 한정

* active -> partially committed -> committed

↓

failed -> aborted(roll back)

* 단위테스트 도구: CppUnit(C++), JUnit(자바), HttpUnit(웹 사이트)

* 오버로딩: 이름 동일, 매개변수의 수나 타입 다름
오버라이딩: 상속관계에서만 발생

* 유스케이스 구성 요소: 연관, 확장, 일반화

* 미들웨어

- 통합된 시스템
- 메시지 큐 활용
- 비동기 방식
- 이기종 분산 데이터 시스템의 데이터 동기
- 느리고 안정적인 응답 필요

* LAPB: X.25의 링크 계층에서 사용되는 프로토콜

* FCS(프레임 검사 시퀀스): 전송 오류 검출

* 원천부호화 방식: DM, DPCM, ADM, ADPCM

* 정 마크 방식: 2 out of 5

* OFDM: 하나의 정보를 여러 개의 반송파로 분할하고, 분할된 반송파 사이의 주파수 간격을 최소화하기 위해 직교 다중화해서 전송하는 통신방식으로 와이브로 및 디지털 멀티미디어 방송 등에 사용

* OMA 레퍼런스 모델: common facilities, application interface, domain interface

* Hamming code: 한 비트에 에러가 발생했을 경우 이를 수신측에서 정정할 목적으로 사용되는 것

* 브룩스 법칙: 새로운 인력을 투입할 경우 작업 적응 기간과 부작용으로 인해 일정을 더욱 지연시키고, 프로젝트에 혼란을 가져오게 된다는 법칙