

2020 정보처리기사 필기 - 5.3 소프트웨어 개발 보안 구축(2)

2020. 4. 17. 23:23

에러 처리의 개요

에러 처리의 개요

- 소프트웨어 실행 중 발생할 수 있는 오류들을 사전에 정의하여 오류로 인해 발생할 수 있는 문제들을 예방하기 위한 보안 점검 항목
- 예외처리 구문을 통해 오류에 대한 사항 정의

오류 메시지를 통한 정보 노출

- 오류 발생으로 실행 환경, 사용자 정보, 디버깅 정보 등 중요 정보를 소프트웨어가 메시지로 외부에 노출하는 보안 약점
- 오류 발생 시 최대한 내부에서 처리하거나 메시지를 최소한의 내용으로 출력하여 정보 노출을 방지해야 함

오류 상황 대응 부재

- 소프트웨어의 오류에 대한 에러 처리를 하지 않았거나 미비로 인해 발생하는 보안 약점

부적절한 예외처리

- 함수의 반환 값 또는 오류들을 세분화하여 처리하지 않고 광범위하게 묶어서 한 번에 처리하거나 누락된 예외가 존재할 때 발생하는 보안 약점

코드 오류

코드 오류의 개요

- 소프트웨어 구현 단계에서 코딩 중 실수하기 쉬운 형 변환, 자원 반환 등 오류를 예방하기 위한 보안 점검 항목

널 포인터 역참조

- 널 포인터가 가리키는 메모리에 어떠한 값을 저장할 때 발생하는 보안 약점
- 오류로 인해 반환되는 널 값을 포인터로 참조하는 경우 발생

부적절한 자원 해제

- 자원을 반환하는 코드를 누락하거나 프로그램 오류로 할당된 자원을 반환하지 못했을 때 발생
- 유한한 시스템 자원이 계속 점유하고 있으면 자원 부족이 발생

해제된 자원 사용

- 이미 반환된 메모리를 참조하는 경우 발생하는 보안 약점
- 반환된 메모리를 참조하는 경우 예상하지 못한 값 또는 코드를 수행하게 되어 의도하지 않은 결과가 발생됨

초기화되지 않은 변수 사용

- 변수 선언 후 값이 부여되지 않은 변수를 사용할 때 발생하는 보안 약점

캡슐화

캡슐화의 개요

- 정보 은닉이 필요한 중요한 데이터와 기능을 불충분하게 캡슐화하거나 잘못 사용함으로써 발생할 수 있는 문제를 예방하기 위한 보안 점검 항목

제거되지 않고 남은 디버그 코드

- 개발 중에 버그 수정이나 결과값을 확인을 위해 남겨둔 코드들로 인해 발생하는 보안 약점

시스템 데이터 정보 노출

- 시스템의 내부 정보를 시스템 메시지 등을 통해 외부로 출력하도록 구현했을 때 발생하는 보안 약점

Public 메소드로부터 반환된 Private 배열

- Private 배열을 Public 메소드에서 반환할 때 발생하는 보안 약점

Private 배열에 Public 데이터 할당

- Private 배열에 Public으로 선언된 데이터 또는 메소드의 파리 미터를 저장할 때 발생하는 보안 약점

API 오용

API 오용의 개요

- 소프트웨어 구현 단계에서 API를 잘못 사용하거나 보안에 취약한 API를 사용하지 않도록 하는 보안 검증 항목

DNS Lookup에 의존한 보안 결정

- 도메인명에 의존하여 보안 결정을 내리는 경우 발생하는 보안 약점
- IP 주소를 직접 입력하여 접근하게 하여 방지 가능



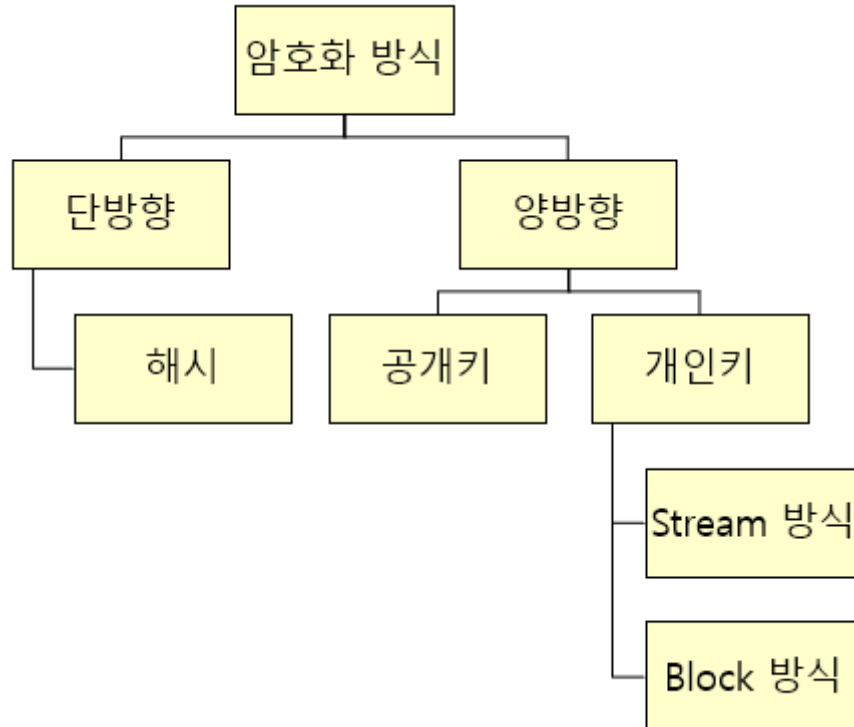
- 보안 문제로 사용이 금지된 API를 사용하거나 잘못된 방식으로 API를 사용했을 때 발생하는 보안 약점

1D1C 구독하기

암호 알고리즘

암호 알고리즘의 개요

- 중요정보를 보호하기 위한 평문을 암호화된 문장으로 만드는 방법



개인키 암호화 기법


- 동일한 키로 데이터를 암호화하고 복호화함
- 대칭 암호 기법, 단일키 암호화 기법이라고도 함
- Stream 기법: 평문과 동일한 길이의 스트림을 생성하여 비트 단위로 암호화
- Block 기법: 한 번에 하나의 데이터 블록을 암호화

공개키 암호화 기법

- 데이터를 암호화하는 공개키는 데이터베이스 사용자에게 공개하고 복호화하는 비밀키는 관리자에게만 공개
- 비대칭 암호화 기법이라고도 함
- RSA기법: 공개키와 비밀키는 메시지를 열고 잠그는 상수를 의미

양방향 암호화 알고리즘 종류

- SEED: 블록 크기는 128비트, 키의 길이에 따라 128, 256로 분류
- ARIA: 블록 크기는 128비트, 키의 길이에 따라 128, 192, 256로 분류
- DES: 블록 크기는 64비트, 키의 길이 56비트

 AES 블록 크기는 128비트, 키의 길이에 따라 128, 192, 256로 분류

해시(Hash)

- 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환
- SHA 시리즈, MD5, N-NASH, SNEFRU 등

1D1C 구독하기

필기 정리

| | |
|--|---|
| | 2020 정보처리기사 필기 정리 1d1cblog.tistory.com |
|--|---|

공감

구독하기

'2020 정보처리기사 > 5과목 : 정보시스템 구축 관리' 카테고리의 다른 글

| | |
|---|------------|
| 2020 정보처리기사 필기 - 5.4 시스템 보안 구축 (4) | 2020.04.19 |
| 2020 정보처리기사 필기 - 5.3 소프트웨어 개발 보안 구축(2) (0) | 2020.04.17 |
| 2020 정보처리기사 필기 - 5.3 소프트웨어 개발 보안 구축(1) (0) | 2020.04.17 |
| 2020 정보처리기사 필기 - 5.2 IT 프로젝트 정보 시스템 구축 관리(3) (0) | 2020.04.17 |
| 2020 정보처리기사 필기 - 5.2 IT 프로젝트 정보 시스템 구축 관리(2) (0) | 2020.04.17 |
| 2020 정보처리기사 필기 - 5.2 IT 프로젝트 정보 시스템 구축 관리(1) (0) | 2020.04.17 |

NAME

PASSWORD

HOMEPAGE



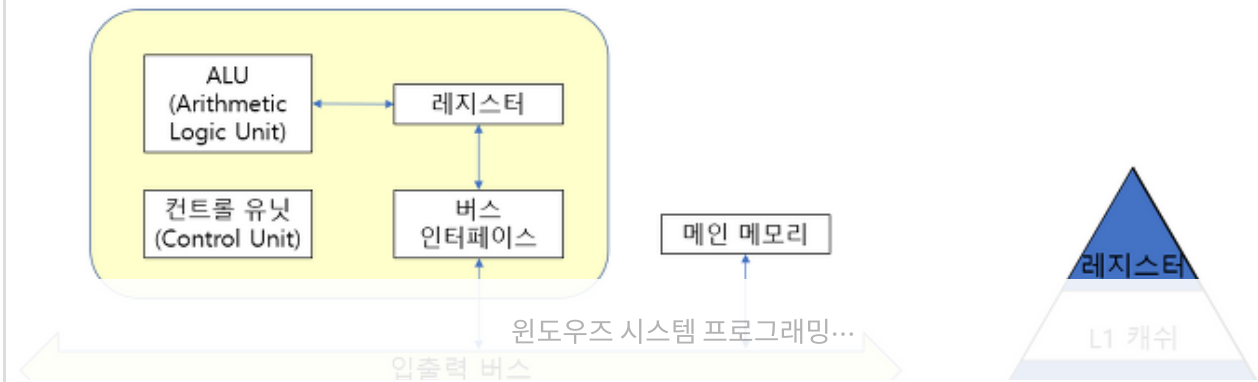
1D1C 구독하기

SECRET ☐ WRITE

PREV 1 2 3 4 5 6 ... 8 NEXT

Recent posts

윈도우즈 시스템 프로그래밍...



뇌를 자극하는

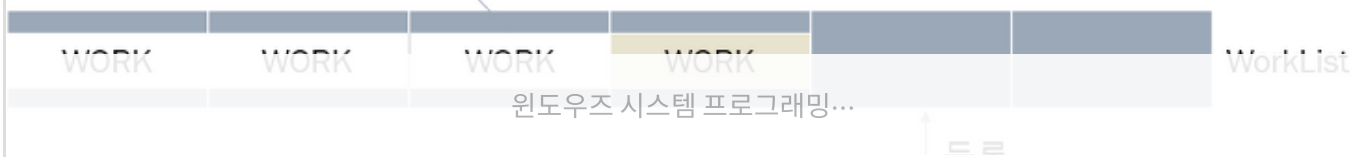
1D1C 구독하기

머리 속에
통째로 넣어
드리겠습니다

윈도우즈 시스템 프로그래밍...

쓰레드

할당



Powered by Tistory, Designed by wallel

Rss Feed and Twitter, Facebook, Youtube, Google+

1D1C 구독하기



1D1C 구독하기



1D1C 구독하기



1D1C 구독하기

