

# 게임 무결성 확보 실험

IT융합공학부 권혁동

# Contents

서론

환경 설정

실험 결과

결론



# 서론

- 메모리 조작

- 각종 데이터가 메모리에 상주한다는 점을 이용
- 특정 **값이 위치한 주소를 찾아서 그 값을 변조**

- 방법

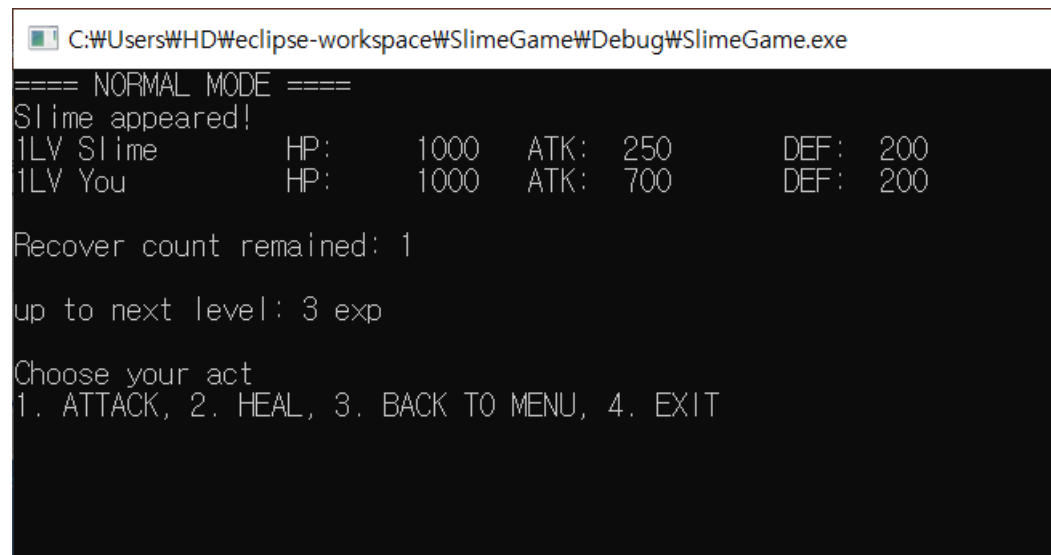
- 인게임에서 특정 수치, 값을 확인
- 에디터를 통해 해당 **값이 위치한 메모리 주소 확보**
- **확보한 메모리 주소에 원하는 값을 입력**

# 서론

- 방어 기법
  - 메모리 상에 값 조회를 어렵게
  - 메모리 보호 구역(SGX, TrustZone 등)에서 연산
  - 서버에서 연산
- 실제로 방어 기법이 **효과가 있는지 실험**

# 환경 설정

- 간단한 게임을 제작
- 치트 엔진을 통해 값 조작을 확인
- 공격 대상
  - 방어 수단 미적용
  - 변수 쪼개기
  - 마스킹
- 안전 환경(SGX)은 구현에 실패



C:\Users\WHD\workspace\SlimeGame\Debug\SlimeGame.exe

```
==== NORMAL MODE ====
Slime appeared!
1LV Slime      HP:      1000   ATK:   250   DEF:   200
1LV You        HP:      1000   ATK:   700   DEF:   200

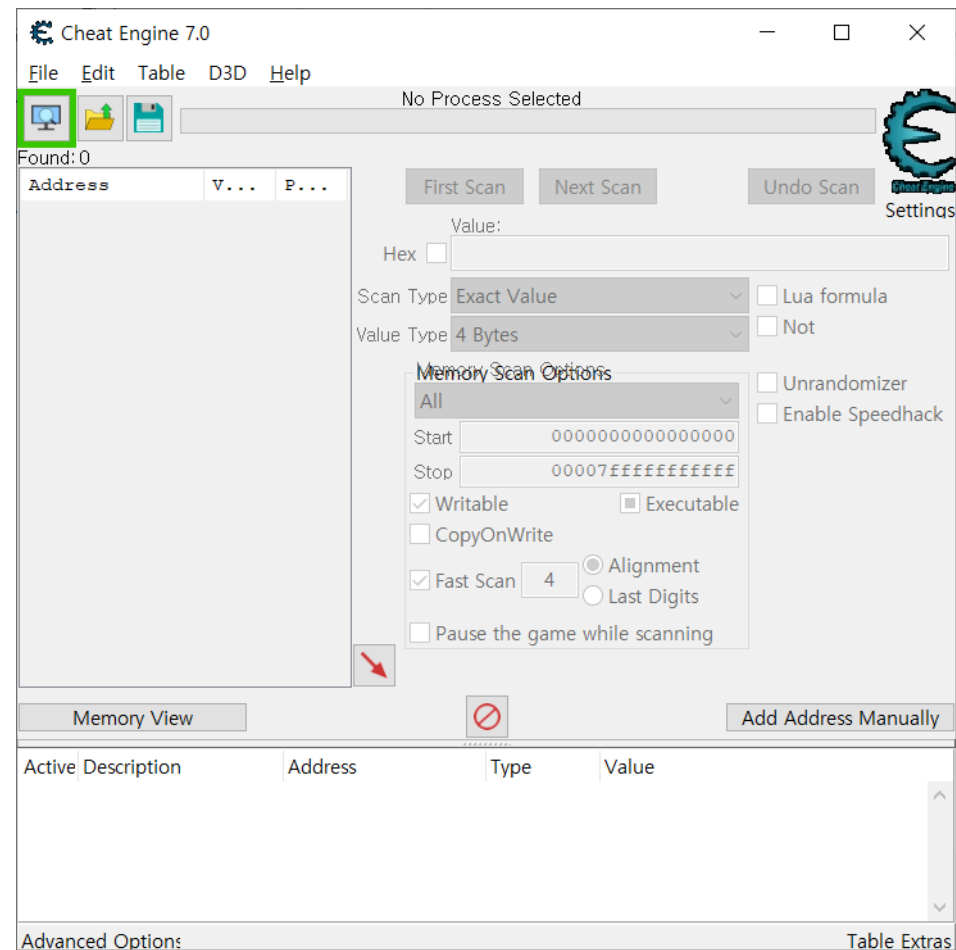
Recover count remained: 1

up to next level: 3 exp

Choose your act
1. ATTACK, 2. HEAL, 3. BACK TO MENU, 4. EXIT
```

# 환경 설정

- 치트 엔진
  - **오픈소스** 메모리 변조 툴
  - **게임 핵 제작에 사용됨**
  - **불법적인 사용은 금지**
- 사용 방법
  - 특정 값을 스캔
  - 스캔한 값이 상주 된 주소 확인
  - 확인한 주소에 값 입력
  - 값 변조 확인
  - 변조가 안되었을 시 다른 주소 확인 후 반복



# 실험 결과

- 방어 수단 미적용
  - 공격에 즉시 성공
    - 화면 상에 노출된 값을 통해 값이 상주한 주소 획득 가능
- 변수 쪼개기
  - 공격 시도에 시간이 걸림
  - 변수를 쪼개 단위를 알지 못할 경우 공격이 어려움
  - 화면 상의 노출된 값을 통해서 값이 상주한 주소 유추 불가능
- 마스킹
  - 공격 시도에 시간이 걸림
  - 마스킹 키를 알지 못하면 공격이 어려움
  - 화면 상의 노출된 값을 통해 값이 상주한 주소 유추 불가능

# 결론

- 값을 **다르게 저장**하는 것으로 **메모리 변조 방어**가 가능
  - 변수 쪼개기
  - 마스킹
  - 연산에 들어가는 자원, 시간이 늘어남
- **조건부 공격이 가능**
  - 리버스 엔지니어링 기술
- **안전 환경**에서 구현한 다음 **방어가 가능한지 실험이 필요**