클라이언트 해킹과 나

하재승
@ipkn
ipknHama@gmail.com

목표

수박 겉핥기 식

여러 해킹방법들 소개

각 방법으로 할 수 있는 ~~(했던?)~~ 일들

해킹 기법들

데이터 내용 확인 + 고치기
패킷 내용 확인 + 고치기
실행파일 고치기
내 코드 끼워넣기
그 외) 키보드, 마우스 매크로

해킹 결과

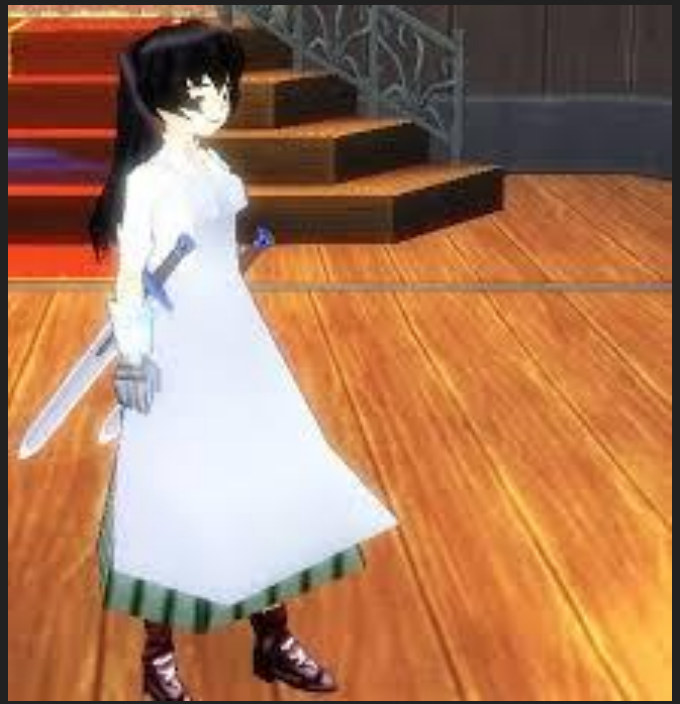
자동 사냥
전투에서 이득 - 에임핵, 월핵

각종 편의 기능 구현
캐릭터 꾸미기 (얻지 못한 비싼 아이템)

데이터 파일 고치기

예: 데이터 바꿔치기

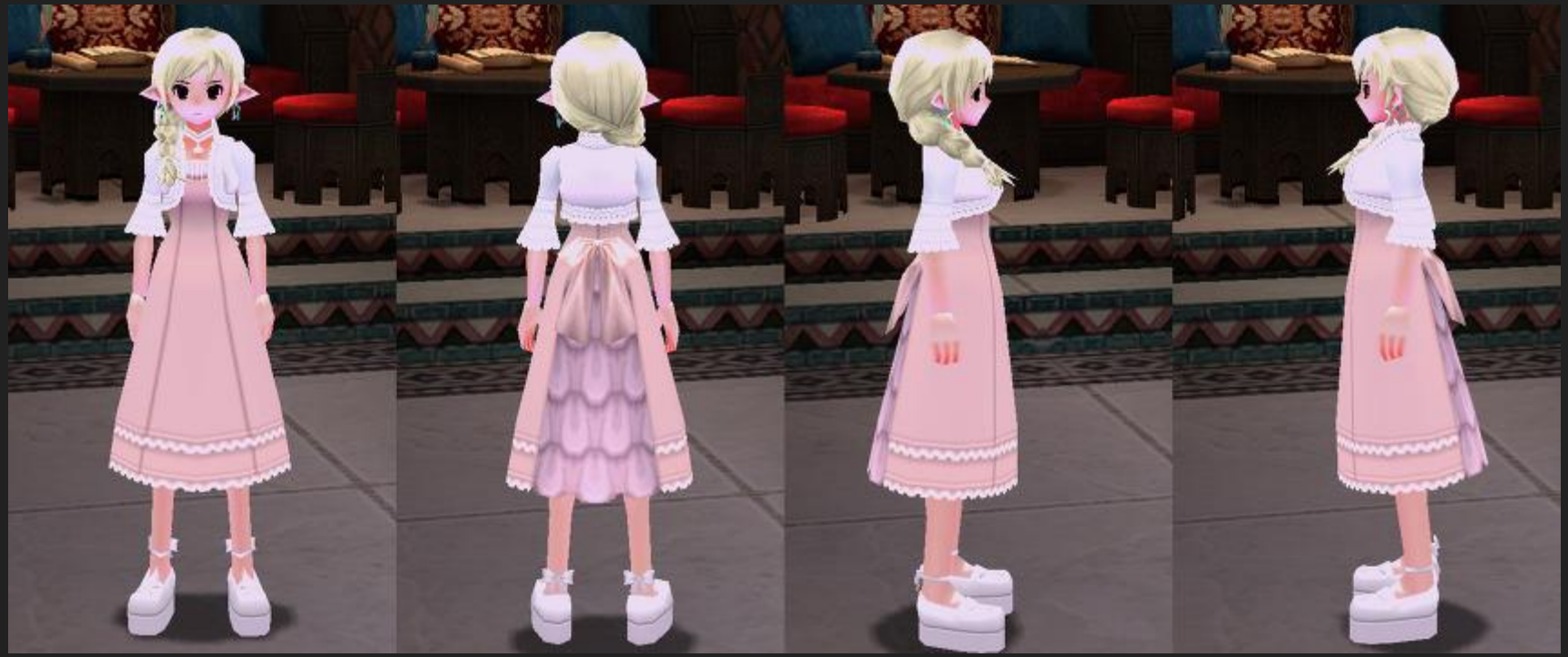
이 평범한 옷의 데이터를



마비노기, 포포 스커트

이 옷과 교체한다면?

(마비노기, 볼레노 앤 점퍼 스커트)



예: 게임내 자동사냥으로 스킬 수련하기

자동 사냥 기능: 평타를 반복적으로 사용

실행할 내용이 적힌 파일이 클라이언트에 저장

평타 사용 -> 스킬 시전으로 변경

자동사냥 켜두면 지정한 스킬 무한 반복

```
<pattern name="attack">
 <param_decl />
 <sequence>
  <cmd name="auto_attack" combo="5"
   timeout="20000" />
 </sequence>
</pattern>
```

```
<pattern name="attack">
 <param_decl />
 <sequence>
  <cmd name="prepare_skill" skill_id="스킬넘버"
    try_cnt="3" target="1" />
 </sequence>
</pattern>
```

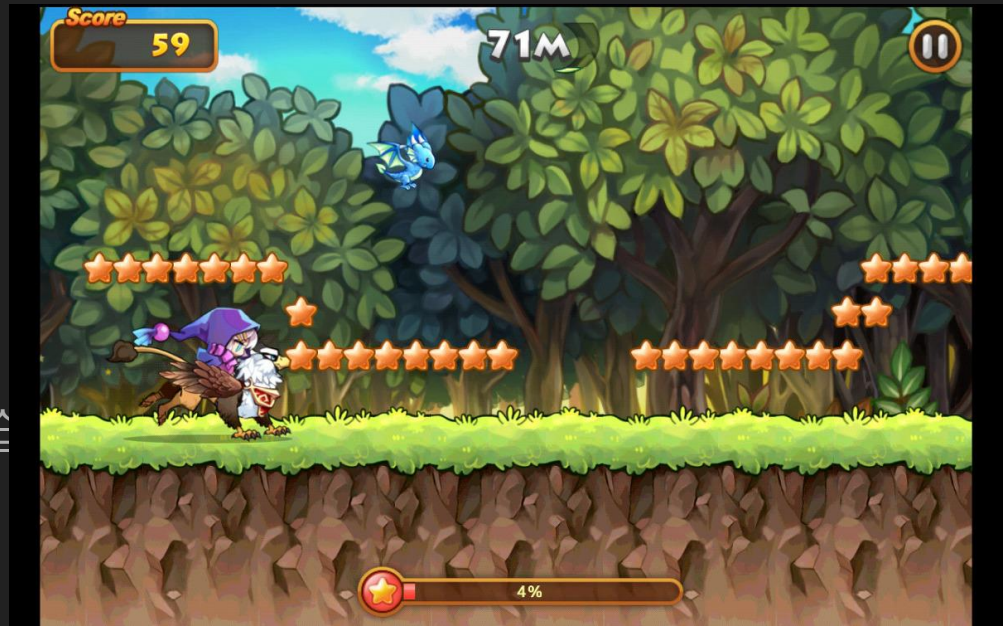
패킷 내용 확인 + 고치기

런게임 많던 시절

윈드러너, 쿠키런, 프린세스 러시, ...

하트 1개를 소모해서 플레이
최고 점수 업데이트
플레이 중 얻은 골드로 강화

(윈드러너 플레이 모습



리플레이 어택

시작할 때, 끝날 때 패킷이 하나씩 감을 확인

끝나고 보내는 패킷을 캡쳐

플레이를 잘한 경우를 골라

캡쳐한 패킷을 다시 보냄

PROFIT!!!

예: 숫자 조작

게임 내에 보이는 동물을 잡으면 1~5캐쉬를 얻는 기능

패킷에 해당 숫자가 담겨서 서버로 전송

해당 숫자를 100만으로 고치면
결제 없이 100만 캐쉬를 얻음

??!!

실행파일 고치기

if 문

```
HANDLE h = CreateMutex(...)

if (h && GetLastError() == ERROR_INVALID_HANDLE)
{
      // Exit Client
      ...
}
```

if (f()) ...

```
        call    f(int)
        test    al, al
        je      .L2
        mov     eax, DWORD PTR [rbp-4]
        imul    eax, DWORD PTR [rbp-4]
        jmp     .L3
.L2:
        mov     eax, 0
.L3:
        leave
        ret
```

JE → JNE, JMP, NOP

JE 명령: 같으면 점프 74 ...
JNE 명령: 다르면 점프 75 ...
JMP 명령: 항상 점프 EB ...
NOP 명령: 아무것도 안함 90

1바이트 변경하면 if문을 원하는 대로 고칠 수 있음

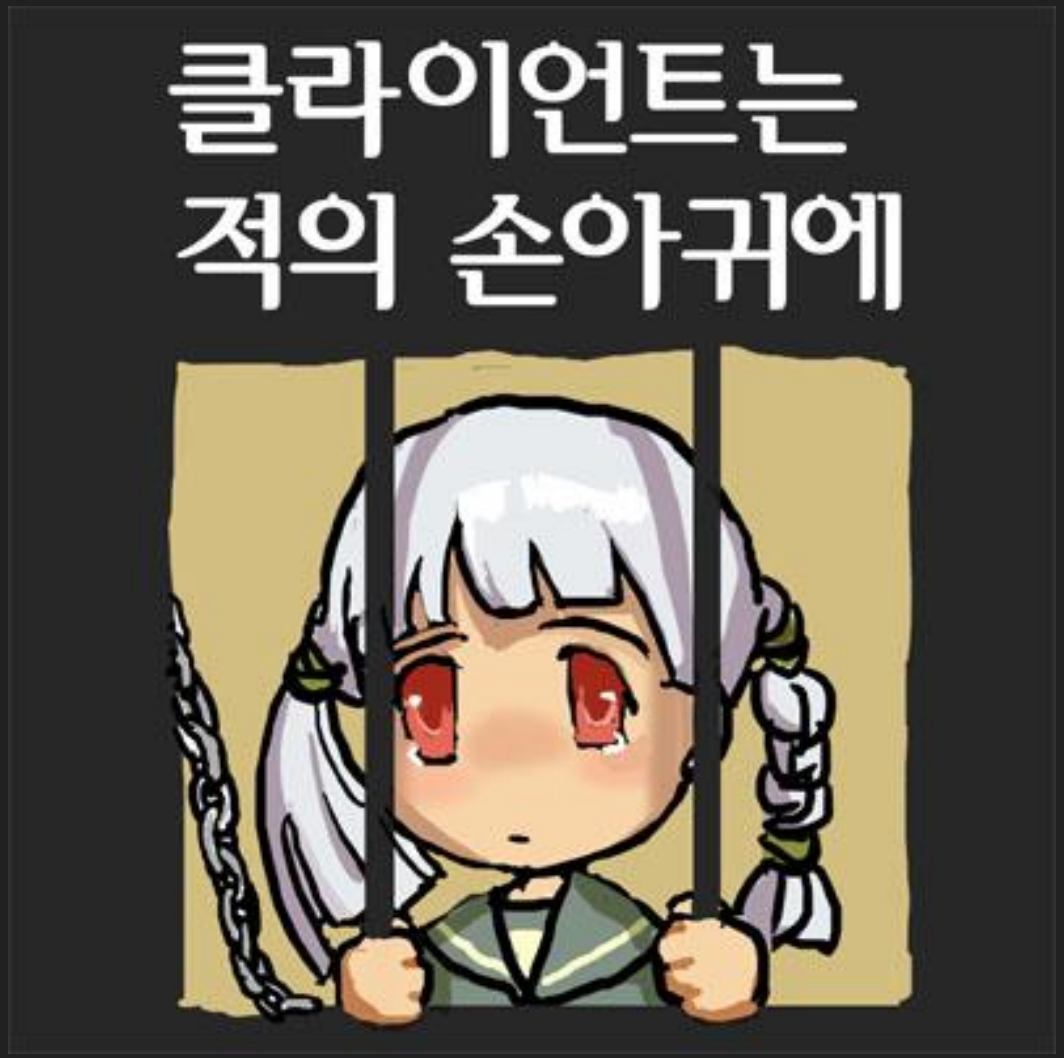
활용

암호가 맞으면 진행 → 암호가 틀리면 진행

멀티 클라이언트 금지 → 허용

경매장 NPC 근처에서만 경매장 사용 가능
→ 어디서나 사용 가능 (서버 체크가 없는 경우)

내 코드 끼워넣기



(2004, 월간 게이머즈)

실행파일 변조를 더 확장해서..

내가 가진 코드를 강제로 프로그램에 집어넣기

직접 고치거나
인젝션 "Injection", 후킹 "Hooking"

DLL Injection - CreateRemoteThread, LoadLibrary
DirectX 내부 함수 바꿔치기 등

예: 자동 거미줄 줍기

디스어셈블리+분석을 통해

전체 아이템을 저장한 hashtable

GetDistance(character, itemID)

CmdPickUpItem(itemID)

예: 스마트 워치 한글화

문자열 출력 부분을 찾음

해당 함수가 시작할 때 한글 범위의 글자면
    내 함수를 호출하게 수정
    한글에 맞는 글자를 대신 그려줌

QnA