보안

MM4220 게임서버 프로그래밍

정내훈

보안

- 보안
  - 위험이나 손실로부터 보호 받는 것
  - '안전'과의 차이 : 의도적인 공격으로 부터의 보호
- 보안의 종류
  - 컴퓨팅 보안
    - 해커에 의한 프로그램의 오동작을 막기
  - 네트워크 보안
    - 네트워크로 오고 가는 데이터의 유출과 변조 방지

보안

- 보안의 종류
  - 네트워크 보안
    - 패킷 암호화, 망분리
  - 컴퓨팅 보안
    - 클라이언트 프로그램 보안
      - 난독화, 클라이언트 변조 검사
    - 클라이언트 컴퓨터 보안
      - 유해 소프트웨어 차단
        - 바이러스, 트로이 목마
    - 서버 컴퓨터 보안
      - 운영팀의 몫, 보안 패치, 망분리
    - 서버 프로그램 보안
      - 서버 프로그램 해킹 방지
      - 클라이언트 해킹 감지 : 해킹 프로그램, 치트 프로그램, 오토

보안

- 네트워크 보안
  - 인터넷은 도청에 완전 무방비.
    - 무선 전화망은 안전 => 모바일 게임들이 보안이 허술한 이유 1
  - 암호화로 데이터를 보호 해야 한다.
  - 대책 :
    - SSL : 표준, 강력, 서버에 큰 부하
    - 간단한 XOR 암호화 : 허술, 작은 부하, 안하는 것보다 나음
      - 고정 키 방식은 너무 취약 => 실시간 키 생성

보안

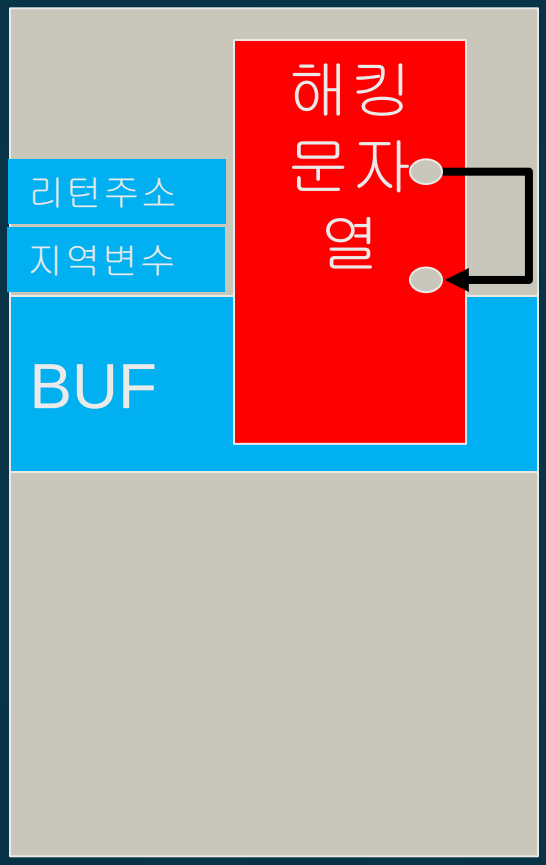
- 컴퓨팅 보안 : 클라이언트
  - 불가능 => 컨텐츠를 서버에서만 돌려야 하는 이유
    - 모바일은 상대적으로 안전 => 하지만 탈옥이 있다.
      - 모바일 게임이 보안이 허술한 이유 2
  - 그래도 해야 하는 이유
    - ID / PW 유출 => 100%플레이어 책임이지만 언론은 게임회사를 두들김.
    - 게임가드, nProtect…. => 왕짜증, 서버 연동 필요 (왕짜증)
    - 대안 : OTP (모바일)

보안

- 서버 컴퓨터 해킹
  - Stack Overflow : 모든 해킹의 시작
    - 모든 텍스트 길이 관리 (strcpy -> (strncpy, strcpy_s))
    - Linux가 해킹에 취약한 원인!!!!
  - SQL Injection :
    - DB에 저장되는 문자열에 SQL 명령어 심기
      - 예) 이름 = \"; UPDATE user_table SET gold=100000000 WHERE user_name = hacker;
      - 대책
        - 모든 특수 문자 대체 (' ' –> %20)
        - 클라이언트가 보내는 모든 문자열의 특수 문자는 변환코드로 변환
      - 디버깅용 백도어 삭제

Stack Overflow 공격

```
char buff[200];
```



[프로세스 스택 메모리]

보안

- Auto 프로그램
  - 자동 사냥/채집/레벨업/팩션노가다/스킬노가다 인공지능 프로그램
  - 클라이언트를 대체
    - ID/PASSWORD를 등록해 놓으면 24시간 앵벌이
  - 문제점
    - 경제 질서 왜곡/플레이 방해 -> 게임의 재미 저하 -> 사용자 떠남 -> 현질 감소 -> Auto 떠남 -> 게임 망함
    - 게임회사에서 Auto단속하는 것은 진심임.
      - 착해서 단속하는 것이 아니라 게임이 망하기 때문.
  - 해결방법
    - 클라이언트 검증
      - 패킷 암호화, 특수 패킷, 클라이언트 내부 메모리 검사, Delayed 처벌
    - 사용자 검증
      - 이미지 글자 읽기, 간단한 산수 문제, GM 대화

보안

- Auto 프로그램
  - 해결 OK?
    - 클라이언트 검사
      - 이틀만에 뚫림
      - 10만 잉여 중국 해커를 당할 수 가 없음
      - Auto 프로그램의 온라인화
        - 자동 업데이트, 실제 클라이언트와의 온라인 연동
    - 사용자 검사
      - 인공지능의 완성 : 오토인가 사람인가 구분 불가능
      - 조선족 알바 : 실시간 화면 전송, GM과 잡담해 줌
      - 한국인 확인 질문????

보안

- Auto 프로그램
  - 그래서?
    - 계속 되는 업데이트로 auto 프로그램의 제작 원가를 높임
    - 미약한 몸부림 (정책/기획 대처)
      - 중국 IP차단
      - 사용시간 제한
      - 사냥터 노후화
      - …
    - 게임성 희생 : 모든 아이템 거래 불가 (ex:검은사막)
    - Auto를 게임에 포함 : 대부분의 모바일 MMO

정리

- 암호화는 네트워크 기초시간에 배웠으므로 생략
- 서버 프로그램 보안
  - Stack 오버플로우 공격
  - SQL Injection 공격
- Auto에 대한 대책
  - 희생을 각오한 근본적인 대책
  - 계속적인 업데이트를 통한 억제