
CHUNGNAM NATIONAL UNIVERSITY

# 시스템 프로그래밍

## - Binary Bomb 해체하기-

**조교의 지시전에 절대 시작하지 마시오!!**

2010.10.18.

백종철
bjc08@cnu.ac.kr

Embedded System Lab. Computer Engineering Dept.
Chungnam National University


# 개요

- 실습명
  - Binary Bomb 해체하기
- 목표
  - 현재까지 자신이 배운 내용 최종 정리!
- 내용
  - 소개
  - 주의사항
  - Step 1: Bomb donwload
  - Step 2: 폭탄 해체하기
  - 점수의 계산
  - 제출방법


# 소개

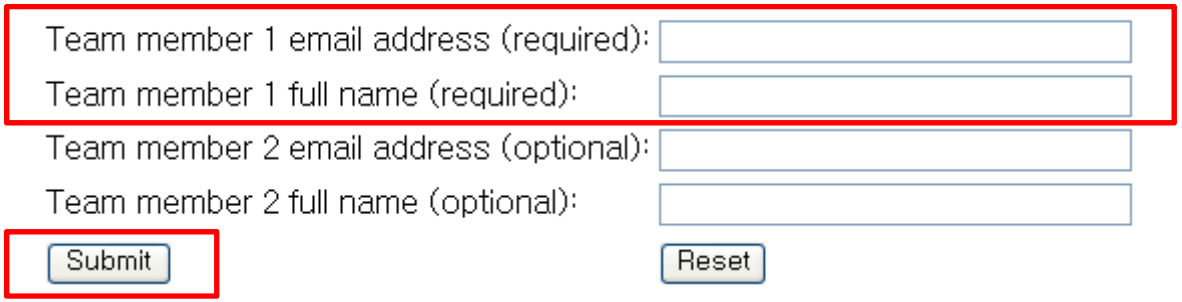
- 사악한 Dr. Evil 이 우리의 리눅스 머신(embedded.cnu.ac.kr)에 Binary Bomb을 설치했습니다.
- Binary Bomb은 순차적인 여러 단계로 이루어진 프로그램입니다.
- 각 단계마다 여러분은 화면에 문자열을 입력해야 합니다.
- 만약 여러분이 정확한 문장(암호)을 입력한다면 해당 구문의 폭탄은 해체 될 것이며 다음 단계의 구문으로 넘어갈 것입니다.
- 반면에 입력한 문장(암호)이 틀려 폭탄이 터지면 화면에 "BOOM!!!" 이 출력되고 프로그램은 종료됩니다.
- 각 단계에 설치된 폭탄을 모두 해체해야 Dr. Evil 이 설치한 폭탄이 해체됩니다.

# 주의 사항 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

- 본 Mini Project의 프로그램은 168.188.128.32 서버에서만 동작하도록 설정되어 있습니다. (모니터링 프로그램에 의해 부정행위로 처리될 수 있음)
- 모든 사람의 폭탄해제 암호는 프로그램에 의해 전혀 다른 방식으로 생성 됩니다.
- 본 Mini Project의 모든 상황은 E-mail을 통해 보고되므로 부정행위의 소지가 있는 행동에 각별히 주의바랍니다.
- 다운 받은 폭탄(bomb)파일이 관리소홀로 인해 삭제될 경우도 0점 처리
- 부정한 방법(바이너리 해킹 등)으로 해제 시도 시, 모니터링 프로그램에 의해 부정행위로 보고됨, 이 경우 0점 처리 + 기존 과제 모두 0점
- 폭탄의 해체/폭발 정보는 자동으로 서버로 전송되어 점수가 계산됩니다.
- 반드시 하나의 폭탄만을 다운 받을 것 (하나 이상의 폭탄을 다운받는 자는 Copy로 간주하고 0점 처리)
- 기타 모든 주의사항을 위반하여 발생한 문제에 대해서는 각자가 책임 지는 것을 원칙으로 한다.

# Step 1. Binary bomb donwload

- 인터넷 익스플로러를 수행시키고 http://embedded.cnu.ac.kr:15101에 접속하면 폭탄 다운로드 페이지가 나옵니다.
- 자신의 이메일과 학번을 넣고 submit 버튼을 누르면 bombXX.tar 파일을 다운로드 받을 수 있습니다. (개인과제이므로 한 사람에 대한 정보만 입력할 것)




  - Ex) bjc08@cnu.ac.kr // 200850410
- 받은 파일을 winscp를 이용하여 각 계정에 업로드 후 “tar xvf bombXX.tar ” 를 실행하여 파일을 풉니다.

# Step 2. Binary bomb donwload

- 성공적으로 폭탄을 받은 학생은 폭탄이름(bombXX)를 출석 부를 때 알려주시기 바랍니다
- 수업에 참여하지 않은 학생은 공1418로 조료를 직접 찾아와 받으시길 바랍니다
- 반드시 하나의 폭탄만을 다운 받을 것 ( 하나 이상의 폭탄을 다운받는 자는 copy로 간주하고 0점 처리 )


# Step 3: 폭탄 해체하기

- bomb.c 파일을 확인하여 폭탄의 구성을 확인한 후 도구들을 이용하여bomb 파일을 분석하고 암호를 알아내야 합니다.
- bomb.c 파일은 폭탄의 껍데기이며 6단계(?)의 암호장벽 부분은 모듈로 컴파일되어 바이너리 속에 숨겨져 있습니다.
- ./bomb을 수행시키면 각 단계별로 암호를 입력 받으며, 다음과 같이 한꺼번에 입력할 수도 있습니다.
  - shell> ./bomb solution.txt
- 폭탄을 분석하기 위해서는 gdb나 ojbdump 등의 도구를 사용하십시오. 도구의 사용법은 교과서, 매뉴얼, 자료실 등에 올려 놓은 자료 또는 인터넷을 통해 참고하십시오.
- 폭탄함수의 알고리즘에 대한 힌트 없음
- 실행 후 Ctrl-C 명령 가능 – 실수로 폭탄이 터지지 않도록 주의!

# 예시 1

## 입력 실패

```
Starting program: /root/test/lab05/bomb2/bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
i don't know

Breakpoint 1, main (argc=1, argv=0xbffff7c4) at bomb.c:73
73          phase_1(input);                  /* Run the phase
(gdb) s

BOOM!!!
The bomb has blown up.
Your instructor has been notified.

Program exited with code 010.
```

## 첫 번째 입력 성공

```
root@embedded:~/syspro/bomblab01/bombs/bomb2# ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
When I get angry, Mr. Bigglesworth gets upset.
Phase 1 defused. How about the next one?
```

# 예시 2

## 실행 중지

```
root@embedded:~/syspro/bomblab01/bombs/bomb2# ./bomb
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
When I get angry, Mr. Bigglesworth gets upset.
Phase 1 defused. How about the next one?
^CSo you think you can stop the bomb with ctrl-c, do you?
Well...OK. :-)
root@embedded:~/syspro/bomblab01/bombs/bomb2#
```

## 한번에 입력

- shell> ./bomb solution.txt

```
root@embedded:~/syspro/bomblab01/bombs/bomb2# ./bomb solution.txt
Welcome to my fiendish little bomb. You have 6 phases with
which to blow yourself up. Have a nice day!
Phase 1 defused. How about the next one?



Congratulations! You've defused the bomb!
Your instructor has been notified and will verify your solution.
root@embedded:~/syspro/bomblab01/bombs/bomb2#
```

# 점수 계산

- 아래의 웹페이지를 통해 실시간으로 각자의 진행상황(해체/폭발)을 확인 할 수 있습니다.
  - http://embedded.cnu.ac.kr/sysp01.html
  - 폭탄을 모두 해체할 경우 60점

| Bomb Name | Phases Defused | Explosions | Score | Comments |
|---|---|---|---|---|
| bomb1 | 0 | 4 | -1 | |
| bomb2 | 7 | 1 | 60 | |

Summary [phase:cnt] [1:0] [2:0] [3:0] [4:0] [5:0] [6:0] [7:1] total defused = 1/2

2 people working in 2 teams. 1/2 people have defused their bombs.

- 틀린 암호를 입력하여 폭탄이 터질 경우 ¼점 감점
  - 4회 : –1점 / 40회 : -10점

- Time Attack 방식으로 채점, 모든 폭탄을 제거 했을 경우 완료 메일을 bjc08@cnu.ac.kr로 제출


# 제출

- Project 기간 : 10월 18일 ~ 10월 31일 (2주일)
  - 10월 31일 밤 11시 59분 59초 데몬을 종료

- 보고서
  - 결과화면을 붙임
  - 결과화면에 학번이 보이도록!
  - 풀이과정에 대한 자세한 설명 (각 단계별 1~6단계 +α)
  - Miniterm project를 통해 느낀 점 및 에피소드 그리고 하고 싶은 말

- 종료 후 데모 예정 (자신이 직접 하지 않았다면 감점 심할 것임)

- 메일제목: [sys01]_bomb_학번_이름

- 제출방식이 틀린 분은 감점 대상입니다!

# 기타 참고 사항

- Gdb
  - GNU debugger로 프로그램을 Line by Line으로 추적할 수 있고, 메모리, 레지스터, 소스코드, 어셈블리코드(여기선 bomb에 관한 소스코드를 제공하지 않았습니다), 브레이크포인트 등을 보거나 활용할 수 있습니다.

- 참고
  - 책, 자료실, man gdb, http://www.unknownroad.com/rtfm/gdbtut/gdbtoc.html , 인터넷 등

- objdump –t : bomb의 심볼 테이블을 보여준다.
- objdump –d bomb >> dis.txt