Introduction to Software Security

The 6th Quiz

Computer Security & OS Lab
Dept. of Software Science, DKU

Cho, Seong-je (조성제)

Spring, 2020

6번째 Quiz에 대한 가이드라인

- **3번, 4번, 5번 슬라이드 문제를 풀어서, Quiz 보고서로 제출 바랍니다.**
  - 실습용으로 구축하여 제공한 Linux Ubuntu에서 실습하는 것을 권장합니다.
    - 실습용 Ubuntu에 프로그램 편집기 vim 을 설치하였습니다.
    - 실습 환경에서 문제가 생기면, 연락 주기 바랍니다. (유근하 조교선생에게 연락해도 됩니다.)
  - Quiz 풀이를 통해 수업 시간에 설명한 내용과 다른 부분을, 직접 확인하기 바랍니다.
  - 컴파일 시에, stack-protector 기법이 적용될 때와 적용되지 않을 때의 차이점을 이해하기 바랍니다.

  - 참고로, 유근하 조교가 제공한 Linux 실습 환경은 다음과 같습니다. (`uname -a` 명령 실행 결과)

    Linux ubuntu 5.3.0-46-generic #38~18.04.1-Ubuntu SMP Tue Mar 31 04:17:56 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

- **부록(연습용) 문제는 보고서로 제출할 필요는 없지만, 풀어보기 바랍니다.**
  - 즉, 9번, 10번 슬라이드 내용은 지식 습득과 실력 향상을 풀이해 보기 바랍니다.

Answer the following 8 sub-questions (①②③④, ⑤⑥⑦⑧)

```
// File name: cmu.c
// Ubuntu on x86 architecture
#include <stdio.h>

typedef int zip_dig[5];

int main() {
        zip_dig cmu = {1, 5, 2, 1, 3};
        zip_dig mit = {0, 2, 1, 3, 9};
        zip_dig ucb = {9, 4, 7, 2, 0};

        printf("0x%x\n", cmu);
        printf("0x%x\n", mit);
        printf("0x%x\n", ucb);

}
```

```
ubuntu:~$ gcc –o cmu1 cmu.c
ubuntu:~$ ./cmu1
0xffffe440
0xffffe460
0xffffe480
```

(1) cmu.c를 **위와 같이** 컴파일한 후 실행한 출력이 위와 같을 때, **①②③④의 값은?**
그 이유도 설명하시오.

① cmu[8] = ? ② cmu[11] = ? ③ucb[-5] = ? ④ucb[-14] = ?

---

(2) cmu.c를 **아래와 같이** 컴파일한 후 출력이 아래와 같을 때, **⑤⑥⑦⑧ 의 값은**?
그 이유도 설명하시오.

```
ubuntu:~$ gcc -fno-stack-protector -o cmu0 cmu.c
ubuntu:~$ ./cmu0
0xffffe480
0xffffe460
0xffffe440
```

⑤ cmu[-8] = ? ⑥ cmu[-11] = ? ⑦ ucb[8] = ? ⑧ ucb[17] = ?

Answer the following two-sub questions

```
/* myarr.c  on Ubuntu/x-86 arch. */
 1  #include <stdio.h>

 2  main() {
 3      int k = 100;
 4      int a[4] = {0, 1, 2, 3};
 5      int b[4] = {4, 5, 6, 7};
 6      int c[4] = {8, 9, 10, 11};

 7      a[-1] = 0xAA;
 8      a[7] = 0xBB, a[10] = 0xCC;
 9      c[-2] = 0xDD, c[-6] = 0xEE;
10      printf("k = 0x%d\n", k);
11      for(int i=0, i<12; i++) {
12          printf ("%3d (0x%x)   ", a[i], a[i]);
13          if (i % 4 == 0) printf ("\n");
14      }
15  }
```

1) Ubuntu/x-86 구조에서,
다음과 같이 컴파일 한 후 실행하고 결과를 확인하시오.
gcc에서 `-m32` 옵션은 32-bit 구조 실행파일을 생성합니다.

```
$ gcc –m32 –o myarr myarr.c
$ ./myarr
```

2) 왼쪽 프로그램에서 11번 줄을 다음과 같이 변경한 후

```
for (int i=0;  i> -12;  i--) {
```

아래와 같이 컴파일한 후 실행하고 결과를 확인하시오.
`-fno-stack-protector` 옵션은 스택 보호 기법을 불능화합니다.

```
$ gcc –m32 –fno-stack-protector –o myarr0 myarr.c
$ ./myarr0
```

Answer the following question

우측 프로그램을 서로 다른 옵션으로 컴파일하여 생성한 실행 파일을 수행한 경우의 차이점에 대해 설명하시오.
우측 소스 프로그램의 이름은 stack_guard.c 이다.

```
$ make stack_guard
cc  stack_guard.c   -o stack_guard
$ ./stack_guard
```

Then, compile the program with other compiler option below, and execute it.

```
$ gcc –fno-stack-protector -o stack_guard0 stack_guard.c
$ ./stack_guard0
```

```
$ ./stack_guard0
buf: bffffb58, &passIsGood: bffffb74
Enter password: cccccdddddeeeeeffff^A^E^B^A
$ python –c “ print ‘x’*30 + ‘\x01’ ” | ./stack_guard0
Enter password:
you win!
```

```
// File name: stack_guard.c
#include <string.h>
#define goodPass “GOODPASS”

int main() {
   char passIsGood = 0;
   short canary = 20;
   char buf[28];

   printf("buf: %08x, &passIsGood: %08x\n", buf, &passIsGood);
   printf(“Enter password: \n”);
   gets(buf);
   if (canary != 20) {
            printf(“buffer overflow attack!\n”);
            exit(-1);
   }

   if (strcmp (buf, goodPass) == 0) passIsGood = 1;
   if (passIsGood == 1)
            printf("you win!\n");
}
```

Solving & Writing

- Solve the question individually (by yourself).
  - You must write a report including the answers to the quizzes by yourself.
  - No cheating

- The **cover page** of the report must include
  - Title (제목): "**The 6th Quiz of Intro. to SW Security**"
  - 분반 (2분반 또는 3분반)
  - Student name, Student number
  - Date of submission

- Deadline
  - Submit your report by **26th April**.

Submission

- **File** naming of the answer report for the **6th** Quiz
  - **ISS(분반)_Qz6_이름_학번_mmdd**
  - If you are in the 2nd class, name = "전우치", student number = 32171234, submission date = 24th April, then the filename for this Quiz is **ISS(2)_Qz6_전우치_32171234_0424**

- **Submit your report to TA by email.**
  - **Email** title: " SW보안개론(분반) 6번 Quiz 답안 제출"
    - The title for the 2nd class: "**SW보안개론(2) 6번 Quiz 답안 제출**"
    - The title for the 3rd class: "**SW보안개론(3) 6번 Quiz 답안 제출**"
  - TA: 한승재 (Seungjae Han) googgkstmdwo@naver.com

부록 (연습용)

Answer the following questions

Assume that you run the following C program on Ubuntu / 32-bit Intel architecture.

Note that sizeof(short)=2, and sizeof(int) = 4.

(1) Show the output of the program at the right side.
(우측 프로그램의 출력은?)

(2) Explain why the output is shown.
(왜 그러한 출력이 나오는지 설명하시오.)

```
int main(void) {      /* my_test.c */
    short dsw[20];
    int dku[20];

    dsw[3] = 0xeeff;
    dsw[4] = 0x5577;
    dku[3] = 0xaabbccdd;
    dku[5] = 0x11223344;

    printf("%x, %d \n", dsw+3, *(dsw+3));
    printf("%x, %d \n", &(dku[3]+2), *(dku+5));
}
```

Answer the following questions

- Explain the main differences between stack and heap segment on Linux OS/i-386 architecture in detail.

- What is a disassembler?