

Introduction to Software Security

The 2nd Homework (2번째 과제)

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

Cho, Seong-je (조성제)

Spring, 2020

2번째 과제 목적

- 실제 생활에서 필요한 컴퓨터 보안 지식을 익힌다.
- Quiz 내용을 복습한다.
- 수업 중에 익힌 중요 내용을 실습을 통해 심층 이해한다.
- 컴퓨터 보안에 대한 학습 능력을 향상 시킨다.

두 번째 과제의 전체 개요

1. 주어진 내용들에 대해 조사하여 정리 (총 15점)
 - 1-1), 1-2), 1-3)에 대해서 정리
2. 주어진 Question들에 대해 정리 (총 24점)
 - 2-1), 2-2), 2-3), 2-4)에 대해서 정리
3. 주어진 각각의 프로그램에서 버그를 찾고, 그 버그를 수정하기 (총 18점)
 - 3-1), 3-2), 3-3)에 대해서 버그 찾고, 정정
 - 정정한 프로그램을 보고서에 나타내기 바랍니다.
4. [보너스 문제] 주어진 프로그램을 실행하고 실행 결과를 설명하기 (총 5점)
 - 실행 환경에 대해서도 설명 필요

1. 다음 내용들에 대해 조사/정리

1-1) 스마트폰에서 사용되는 '패스(PASS)' 앱이란? PASS 앱의 기능/역할은?

- 컴퓨터 보안(사이버 보안) 관점에서 설명하기 바랍니다.
- 예로, CIA, Authentication, Authorization 등에서 어떤 보안 목적을 달성할 수 있는지를 설명해도 됩니다.

1-2) 랜섬웨어(ransomware)란 무엇인가?

- 랜섬웨어의 주요 특징에 대해 설명하십시오.
 - Google 학술검색 (<https://scholar.google.com/>) 을 활용하는 것을 추천합니다
- 2020년에 발생한 Makop 랜섬웨어와 NEMTY 랜섬웨어에 대해 설명하십시오.
- 랜섬웨어 방어 기법에 대해서도 설명하십시오.

1-3) 크립토재킹(Cryptojacking) 공격이란 무엇인가?

- 크립토재킹 멀웨어에 대해 설명해도 좋습니다.
- 랜섬웨어와 비교 설명하십시오.
- 신문기사나 기술보고서를 참고해도 좋습니다.

2. 다음 Question들에 대해 정리

2-1) Malvertising과 Rogue software에 대해 자세히 비교 설명하시오.

- Rogue software를 Rogue security software라고도 합니다.
- Google 학술검색 (<https://scholar.google.com/>) 을 활용하는 것을 추천합니다.

2-2) 공격자나 악성코드 제작자들은, 자신의 멀웨어(malware)를 더 효과적을 만들기 위해 무엇을 하나요?

- 멀웨어가 사용하는 안티-멀웨어(anti-malware) 탐지 회피 기법을 설명해도 좋습니다.
 - Anti-malware = Anti-virus = Vaccine 프로그램

2-3) 암호학적 해시 함수(Cryptographic hash function)들의 주요 특징에 대해 설명하시오.

- 최소 3가지의 특징에 대해 설명하여야 합니다.
- 암호학적 해시 함수들의 예: MD5, SHA-256 등

2-4) 퍼징 기법(fuzzing technique)이란 무엇인가? 공격자는 왜 퍼징 기법을 사용하는가?

- Fuzzing technique = Fuzz testing

3. 다음 프로그램들의 버그 탐지 및 정정

3-1) What is the problem in the C program below? How can you fix it?

```
typedef unsigned int uint;
int getmin(int *arr, uint len) {
    int min;
    for (int i=0; i<len; i++)
        min = (min < arr[i]) ? min : arr[i];
    return min;
}
```

3-2) 아래 우측 프로그램은 구구단을 2단부터 9단까지 출력하는 프로그램의 일부분이다. 어느 부분에 문제가 있는지 지적하고, 수정하십시오.

바람직한 출력 형태

2 * 1 = 2

2 * 2 = 4

:

2 * 9 = 18

단과 단 사이에 한 줄이 공백이 있어야 함.

3 * 1 = 3

3 * 2 = 6

:

9 * 9 = 81

```
int x, y;
```

```
for (x=2; x<=9; x++)
```

```
    for (y=1; y=9; y++) ;
```

```
        printf ("%2d * %2d = %2d\n", x, y, x*y);
```

```
    printf("\n");
```

3. 다음 프로그램들의 버그 탐지 및 정정

3-3) 다음 하단의 프로그램에서

- (a) 발생 가능한 버그들을 행 번호와 함께 구체적으로 설명하시오.
- (b) 그 버그들이 발생하지 않게 프로그래밍 하는 방법을 설명하시오.

- 정정한 프로그램을 보고서에 나타내야 합니다.

```
1 int myfunction(int *array, int len) {
2     int *myarray, i;
3
4     myarray = malloc(len * sizeof(int));
5     if(myarray == NULL) {
6         return -1;
7     }
8     for(i = 0; i < len; i++) {
9         myarray[i] = array[i];
10    }
11    return myarray;
12 }
```

4. 다음 프로그램을 실행 결과를 설명하기

[보너스 문제입니다. 배점은 총 5점입니다.]

- 다음 프로그램을 실행하여 보고, 출력 결과에 대해 설명하십시오. 출력 결과에 대해 왜 그렇게 출력이 되었는지를 설명해야 합니다.
- 실행 환경에 대해서 설명하기 바랍니다. (예: MS Windows 10, 64비트 CPU 컴퓨터)

```
char x, y;
```

```
x = -128;
```

```
y = -x;
```

```
if (x == y) puts("1");
```

```
if ((x - y) == 0) puts("2");
```

```
if ((x + y) == 2 * x) puts("3");
```

```
if (((char)(-x) + x) != 0) puts("4");
```

```
if (x != -y) puts("5");
```


보고서 작성 시 포함 내용

● 보고서 표지에 포함될 내용

- 과목명(SW보안 개론), 분반 표시(2분반 또는 3분반),
- 과제번호 및 제목 (2nd 과제: 복습 및 보안 이슈 조사 정리)
- 성명, 학번
- 제출일 (**반드시 정확하게 표시**)

● 보고서 내용에 포함될 내용

- 1) 앞서 설명한 문제들에 대한 답변
- 2) 참고한 교재/자료/문서/논문 등이 있으면, 해당 내용 표시하여 보고서에 포함
- 3) Discussion
 - 토론 및 논의 사항
 - 건의 사항

과제물 수행 방식

- **개인 과제**
 - 개별적으로 조사하여 보고서로 정리
 - No Cheating
 - 만약, 과제 보고서 복제가 있다면, 보여준 사람과 복제한 사람 모두 0점
- **신뢰할 만한 교재/자료/문서/논문/사이트를 활용**
 - 보고서 작성 시에, 참조(참고)한 교재/자료/문서/논문/사이트 정보를 포함하여 기술
 - Trusted websites: <https://scholar.google.com/> , Sciece.gov, NIST – Glossary, ...
- **Deadline**
 - 4월 28일까지

과제물 제출

- 과제 보고서 파일을 첨부하여 이메일로 제출
- 이메일 제목 및 과제보고서 파일 이름
 - 이메일 제목: “SW보안개론(분반) 2번 과제 제출”
 - 2분반 이메일 제목: SW보안개론(2) 2번 과제 제출
 - 3분반 이메일 제목: SW보안개론(3) 2번 과제 제출
 - 보고서 파일 이름은 “ISS(분반)_HW2_이름_학번_mmdd” 형식으로
 - 예시) 3분반 홍길동 (32165678), 제출일이 4월 21일이면 →
“ISS(3)_HW2_홍길동_32165678_0421”
- 조재희 조교선생께 제출
 - 조재희 (jehee1204@gmail.com), 미디어센터 505호