CE4062/CZ4062 Computer Security

Tutorial 4 – Software Security (3)

1. Answer the following questions
   a. Why are non-executable stack and heap not enough to defeat buffer overflow attacks?

   b. Distinguish three types of fuzzing techniques?

   c. What is a code reuse attack?

2. For string copy operation, strncpy is regarded as "safer" than strcpy. However, improper use of strncpy can also incur vulnerabilities. Please describe the problem in the following program, and what consequences it will cause.

```c
#include <stdio.h>
#include <string.h>
int main() {
  char src[] = "geeksforgeeks";

  char dest[8];
  strncpy(dest, src, 8);
  int len = strlen(dest);

  printf("Copied string: %s\n", dest);
  printf("Length of destination string: %d\n", len);

  return 0;
}
```

Figure Q2

3. StackGuard is a mechanism for defending C programs against stack-based buffer overflows. It detects memory corruption using a canary, a known value stored in each function's stack frame immediately before the return address.
   a. In some implementations, the canary value is a 64-bit integer that is randomly generated each time the program runs. Explain why this prevents the basic form of buffer-overflow attacks
   b. What is a security drawback to choosing the canary value at compile time instead of at run time?
   c. If the value must be fixed, what will be a good choice?
   d. List an attack which can defeat the StackGuard.

4. One possible solution to defeat buffer overflow attacks is to set the stack memory as Non-executable (NX). This is usually achieved by the OS and the paging hardware. However, imagine that a machine does not support the non-executable feature, then we can implement this functionality at the software level. The compiler can allocate each stack frame in a separate page, and associate a software-manipulated NX bit at the bottom of this page, controlling if this page (stack frame) is non-executable. The structure of a stack frame is shown in the Figure below.

Since the NX bit is at the bottom of the memory page, the buffers inside this stack frame is not able to overwrite this bit to make it executable. Describe a buffer overflow attack that can still overwrite NX bits.

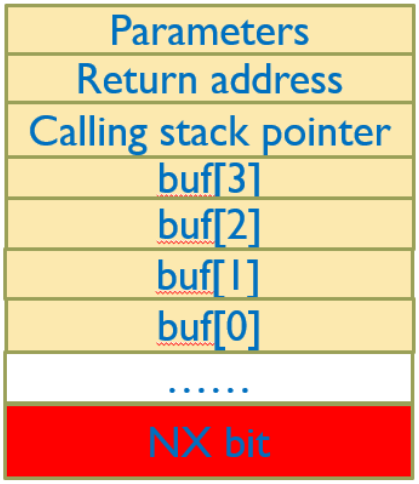

Figure Q4