Computer Security Assignment 3

Due on 18 December 2018

Released on 30 November 2018

Question 1 — **Intrusion Detection.** (3 marks) Give at least three examples on how an intrusion detection system can actively respond to an attack.

Question 2 — **Buffer overflow.** (4 marks) Consider the following C code snippet.

```
/* Escapes all newlines in the input string, replacing them with "\n". */
/* Requires: p != NULL; p is a valid '\0'-terminated string */

void escape(char *p)
{
  while (*p != '\0')
  {
    switch (*p)
    {
      case '\n':
        memcpy(p+2, p+1, strlen(p));
        *p++ = '\\'; *p++ = 'n';
        break;
      default:
        p++;
    }
  }
}
```

You may assume that **escape()**'s argument is always non-null and points to a '\0'—terminated string. What's wrong with this code?

Question 3 — **Access control.** (3 marks) Early Intel processors (e.g., the 8086) did not provide hardware support for dual-mode operation (i.e., support for a separate user mode and kernel mode). As a result, most of the systems implemented on these processors did not support multi-user operation. List and explain one potential problem associated with supporting multi-user operation without hardware support for dual-mode operation.

(Hint: You may search the Internet on related information. Basically, in modern operating systems, privileged instructions are only executed with kernel mode.)

(Please send your answer in txt/pdf formats to chenyi_zhang@jnu.edu.cn)