Security Injections @ Towson

Module: Buffer Overflow - CS0 C++

Student: Benjamin Wasserman

Date: 09/13/2018

ID: 1812986123

Discussion Questions

Describe the buffer overflow problem.

The buffer overflow problem occurs when data is written beyond the bounds that were allocated. This could cause overwriting, the program to crash, as well as other issues.

How could you prevent a buffer overflow from occurring in your program?

We can prevent a buffer overflow from occurring by checking the bounds of all input, and checking any data that can be input into statically allocated memory.

Give three real life examples of buffer overflow attacks (research on the web).

The Morris Worm used buffer overflow as one of its exploits to propagate over the internet. In 2001, the Code Red Worm used a buffer overflow in Microsoft's Internet Information Services for an attack. Buffer overflows in Xbox games have also been exploited so that users have been able use the software without buying it.

What can result from a buffer overflow ?

A buffer overflow can result in a program crashing, data being overwritten, attacks from vulnerabilities, and other problems.

Provide three different examples of code that contains buffer overflows.

```
// Example 1
int test[10];
for (int i = 0; i < 12; i++) {
    test[i] = 7;
}

// Example 2
int elements;
cout << "Enter the number of elements" << endl;
cin >> elements;

// Example 3
int test[10];
test[-1] = 5;
```