Security Injections @Towson

Welcome, Marilyn Soyars!

Security Injections, Java CS1 - Buffer Overflow

1. Background 2. Code Responsibly 3. Laboratory Assignment
4. Discussion Questions

Buffer Overflow - "Data Gone Wild" - CS1

Background

Summary:

Buffer overflow occurs when data is input or written beyond the allocated bounds of of a buffer, array, or other object causing a program crash or a vulnerability that attackers might exploit.

Description:

A buffer overflow occurs when data is written beyond the boundaries of a fixed length buffer overwriting adjacent memory locations which may include other buffers, variables, and program flow instructions. Considered the “nuclear bomb” of the software industry, the buffer overflow is one of the most persistently exploited security vulnerabilities and frequently used attacks.

Video by Lydia Spurrier and Miya Dubler.

Risk: How Can It Happen?

Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or allow the execution of malicious code. However, Java is designed to avoid buffer overflow by checking the bounds of a buffer (like an array) and preventing any access beyond those bounds. Even though Java may prevent a buffer overflow from becoming a security issue, it is essential for all programmers to understand the concepts described below.

Real-world Example:

A buffer overflow in a 2004 version of AOL's AIM instant-messaging software exposed users to buffer overflow vulnerabilities. If a user posted a URL in their “I'm away” message, any of his or her friends who clicked on that link might be vulnerable to attack. AOL's response was to suggest that users update to a new version that would fix the bug.

Paul Roberts “AOL IM 'Away' message flaw deemed critical”, Infoworld, August 9, 2004 http://www.infoworld.com/article/04/08/09/HNaolimflaw_1.html

Example in Code:

```
public class Overflow {
  public static void main(String[] args) {
    int[] vals = new int[10];
    for (int i =0; i < 20; i++) {
      vals[i] = i;
    }
  }
}
```

When this program is run, the loop counter will exceed the value of a suitable index for the array. When the assignment statement tries to store a value in vals[10], buffer overflow occurs. The result is unpredictable. Depending on the operating system and the specific nature of the overflow, it may not cause any apparent problems, or it will cause the program to crash. Buffer Overflow can occur in many languages. In Java, the code results in an ArrayIndexOutOfBoundsException.

Answer the following questions:

Question 1

A buffer overflow can write over adjacent data such as:

☑ ✓ Variables

☑ ✓ Program flow instructions

☑ ✓ Other buffers

(hint: Read summary and description sections to answer this question.)

Question 2

An unchecked buffer overflow causes:

☑ ✓ data to be corrupted

☑ ✓ A program crash

☐ the program to correct itself

☑ ✓ the execution of malicious code

☑ ✓ unexpected behavior

(hint: Read Risk and Real-world Example sections to answer this question.)

Go To Next Section

This project is supported by the National Science Foundation under grants DUE-1241738 and DUE -0817267. Any opinions, findings, conclusions, or recommendations expressed are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Powered by a modified version of Class2Go