Laynie Tierney

CS-405-R4888 Secure Coding

21 March 2024

2-3 Activity Buffer Overflow Coding

The provided code presents a scenario where user input can lead to buffer overflow, potentially overriding a constant value representing a secret account number. To address this issue without changing the position of the account\_number variable, the code needs modification to prevent buffer overflow while still allowing user input.

The solution involves utilizing the std::setw() function from the <iomanip> header to limit the number of characters read by std::cin. By setting the maximum width to 20 characters, the input buffer is restricted, preventing overflow. This ensures that even if the user attempts to input more than 20 characters, the buffer will not be overrun, preserving the integrity of the secret account number.

This approach effectively safeguards against buffer overflow without altering the structure of the code or the position of the account\_number variable. It adheres to C/C++ best practices and ensures that the secret account number remains secure from unauthorized access through input manipulation.

A screenshot of a computer program

Description automatically generated