

CISC 367 – Spring 2016

Team Assignment – Buffer Overflow Attack via Socket

The goal of this assignment is to give you a deeper understanding of buffer overflow attacks. You are provided with two socket programs in C. One acts as `client` and the other `server`. Your assignment consists of testing whether the server is vulnerable to buffer overflow attack. If not, modify the server to create such a vulnerability. If yes, modify the server to eliminate the vulnerability.

- Compile both server and client programs using `/usr/bin/gcc` on `mlb.acad.ece.udel.edu`. When using `gcc`, make sure you give it the option `-fno-stack-protector`.
- Test the programs with two different shell terminals, one for server and the other for client. Be sure to use a random, 'large' port number.
- Try to figure out whether the server is vulnerable to the buffer overflow attack.
- Modify the server program as necessary and explain your modifications in detail.