COMP 4384: Assignment #2

Revision 1

Due on October 15, 2020 at 1:00 PM

30 Points (10% Overall)

Problem 1

(10 points)
The code at `https://gist.github.com/atamrawi/e5a8170e96f4a2dc71598c80d6be9344` is a utility that facilitates copying integers from one buffer (`srcBuffer`) to another (`dstBuffer`). The utility prompts the user to enter the number of integers to copy and based on that value will copy the desired number of integers from (`srcBuffer`) to (`dstBuffer`). To avoid buffer overflow attacks, the utility developer added a check at line 29 to prevent users from copying more than available integers (`MAX_BUF_SZ`) from the (`srcBuffer`) and possibly corrupt memory. Study the code and answer the following questions:

A. (*8 points*) Explain how you can craft a malicious input that will allow you to copy more than available integers (`MAX_BUF_SZ`) and bypass the check on line 29. *Your answer must include a detailed explanation of the exposed vulnerability and your attack work-flow supported by concrete examples.*

B. (*2 points*) Show how you can modify the code so you can prevent the vulnerability exposed in **A**.

Problem 2

(10 points)

The code at (`https://gist.github.com/atamrawi/59dbbce0efc2543b30449e849325759d`) corresponds to a store app that will allow you to buy *imitation keys* or *genuine keys*. An imitation key costs \$1000 while a genuine key costs $\$100,000$. Given that you start with an account balance of $\$1,100$, discuss how would you be able to purchase the genuine key?
Note: *Your answer must include a detailed explanation of the exposed vulnerability and your attack work-flow supported by concrete examples.*

Problem 3

(10 points)

Explain how would you crack the code at `https://gist.github.com/atamrawi/42e9af96c8aa360c5de88db788e26b5b` to get the key at line 43? Write a solution summary if you are able to crack it, otherwise, write a summary describing the techniques you have attempted.