**CS 370 Introduction to Security Week 8: Problem Set 8**

Instructor Name: Rakesh Bobba

# Introduction/Purpose

The purpose of this assignment is to help you gain a better understanding and insight into software vulnerabilities such as buffer overflows other data and code injection attacks covered in Week 8

Before beginning make sure you have watched the lecture videos on the following and completed the associated practice quizzes.

* Common Software Vulnerabilities
* Input Handling Vulnerabilities
* Buffer Overflow I
* Buffer Overflow II
* OS Interaction Vulnerabilities

Chapter 4.4 from Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson

# Instructions/Questions

Please answer the questions below.

## Software Vulnerabilities and Injection Attacks

Q1 [4 pts] What is an injection attack? Give 2 examples of injection attacks

Q 2 [4 pts] Describe what a Cross-Site Scripting attack is. What type of an attack is this?

Q3 [4 pts] What is SQL Injection? How can it be prevented?

## Buffer Overflow

Q4 [5 pts] What is a buffer overflow? What are the 3 distinct parts of process memory that buffer overflows typically target?

Q5 [3 pts] At a high-level, what are the three steps to exploiting a buffer overflow? What are the possible consequences of a buffer overflow?

Q6 [3 pts] What is stack smashing?

Q7 [5 pts] What is StackGuard and how does is protect against stack smashing attacks?

Can it prevent stack smashing - why or why not? Is StackGuard a compile time or run-time defense?

Q8 [2 pts] What is an advantages of runtime defenses against compile-time defenses?

Q9 [3 pts] What properties should the *canary value* in StackGuard have?

Q10 [5 pts] Name five mechanisms/ways you can think of to protect against buffer overflow attacks.

Q11 [2 pts] What is one advantage of Return Address Defender (RAD) over StackGuard?

Q12 [3 pts] What is the difference between StackGaurd and Guard Pages?

## OS Interaction Vulnerabilities

Q13 [4 pts] What is a TOCTOU error? What is one way to prevent them?

Q14 [4 pts] What is a race condition? Why do they happen?

Q15 [4 pts] How can environmental variables be used for code injection?

# Submission Details

Submit a PDF file with the questions and your corresponding answers

The assignment is worth 55 points. It is due Wednesday of Week 9 at Midnight.