CSC 495/583 Fall 2017 Reading Question 2

Dr. Si Chen

Due on: 10/31/2017

Jump-Oriented Programing

First, if you are not familiar with code reuse attacks, please read the following papers:

- The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86)
- On the Effectiveness of Address-Space Randomization
- Code-pointer Integrity
- Control-Flow Bending: On the Effectiveness of Control-Flow Integrity
- ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks

Then read the paper - Jump-oriented programming: a new class of code-reuse attack and explain the **similarity and difference** between Jump-Oriented Programing and Return-Oriented Programing.

Submission

- Please upload your response **in PDF format** to D2L Assignment before 10/31/2017 23:59:59 EDT. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.