Software Security

Return-to-libc Attacks & Return-Oriented Programming (Part II)

Professor Travis Peters
CSCI 476 - Computer Security
Spring 2020

Some slides and figures adapted from Wenliang (Kevin) Du's
Computer & Internet Security: A Hands-on Approach (2nd Edition).
Thank you Kevin and all of the others that have contributed to the SEED resources!

Today

Announcements

- ***REMINDER:*** Please fill out the *Early Semester Check-In Survey* *>>> link on the website*
- Lab 03 due today!

Goals & Learning Objectives

- ~~Return-to-libc Attacks & Return-Oriented Programming~~
  - ~~The non-executable stack countermeasure~~
  - ~~The main idea of the ***return-to-libc attack***~~
  - Challenges in carrying out the attack
  - *Function Prologues & Epilogues*
  - Lab 04 Work Time: Launching a return-to-libc attack
- Next Time…
  - Generalizing the return-to-libc attack: ***Return-Oriented Programming (ROP)***
    - Overcoming `/bin/sh` (`/bin/dash`) countermeasure
    - Chaining arbitrary functions (or parts of functions)