CSCI 1650: Software Security and Exploitation (Fall 2023)

- **Instructor:** Vasileios (Vasilis) Kemerlis
    - **Web:** https://cs.brown.edu/~vpk
    - **Email:** vpk@cs.brown.edu
    - **Office Hours:** M 6PM–7PM (via Zoom)
- **Meeting Time:** MW 3PM–4:20PM (T hour)
- **Meeting Location:** MacMillan 117
    - **Instruction Type:** Hybrid (via Zoom)
- **Web:** https://cs.brown.edu/courses/csci1650/
- **Email:** cs1650tas@lists.brown.edu

- **Prerequisites:** CSCI 1670 (Operating Systems),
  or CSCI 0330 (Introduction to Computer Systems),
  or CSCI 0300 (Fundamentals of Computer Systems)

Overview

This course covers software exploitation techniques and state-of-the-practice mechanisms for hardening software. Specifically, we will begin with a summary of prevalent software defects, typically found in applications written in memory unsafe languages, like C/C++, and proceed with studying traditional and modern exploitation techniques, ranging from classical code injection and code reuse up to the latest goodies (e.g., JIT-ROP). We will also be focusing on defenses against certain vulnerability classes and the way(s) to bypass them. Students will be introduced to advanced software exploitation techniques and countermeasures, and study, in depth, the boundaries and effectiveness of standard hardening mechanisms, such as non-executable memory, address space randomization, and toolchain-based hardening.

Course Objectives

The goals of this course are twofold: (a) lean *how* and *why* (certain) software defenses can be bypassed; and (b) *familiarize* with exploit development techniques, in order to better *understand* the boundaries of protection mechanisms and *argue* about their effectiveness.

Grading

- Class participation: 10%
- Assignments: 90%
- ~~Midterm: 0%~~
- ~~Final: 0%~~

Assignments

Over the course of the semester there will be four CTF-like (Capture The Flag) assignments. In every CTF, a set of vulnerable binaries will be given, and students will be asked to: (a) construct an attack payload that triggers the respective bug(s); and (b) develop a complete, end-to-end, working exploit for every identified vulnerability.

Study Material

There is *no required* textbook; the study material will mainly consist of (online) *assigned readings*. Optionally, you may use the following book:

- *Hacking: The Art of Exploitation*, 2nd Edition. Jon Erickson.
  No Starch Press, 2008, ISBN 1593271441.

Credit Hours

Over 14 weeks, students will spend three (3) hours per week in class (42 hours total). In addition, the required reading is expected to take up approximately seven (7) hours per week (98 hours). Lastly, working on CTF assignments is estimated at a total of approximately 40 hours over the course of the term.

Lectures (tentative)

- **Lecture 1**: Introduction
  - Virtual address space organization
  - Overview of the Extensible Linking Format (ELF)
- **Lecture 2 & 3**: Basic Concepts
  - x86 instruction set, calling conventions
  - Dynamic linking/loading
  - `gdb`, `nm`, `objdump`, `nm`, `...`
- **Lecture 4 & 5**: Control-flow Hijacking & Code Injection
  - Control-data corruption techniques
- **Lecture 6 & 7**: Shellcode Development
  - Assembling/disassembling
  - Alphanumeric shellcode
  - Raw `syscall` invocation methods
- **Lecture 8 & 9**: Non-Executable Memory & Return-to-libc
  - Executable space protection
  - Advanced `ret2libc` exploitation
- **Lecture 10 & 11**: Code Reuse
  - `ret2libc` chaining, `%esp` lifting
- **Lecture 12 & 13**: Addr. Space Rand. & Return-Oriented Programming
  - Address Space Layout Randomization (ASLR)
  - Return-Oriented Prog. (ROP): Exploitation without code injection
- **Lecture 14 & 15**: Memory Disclosure & Just-In-Time Code Reuse
  - Format string vulnerabilities
  - Techniques for bypassing ASLR
- **Lecture 16 & 17**: Toolchain-based Hardening & Adv. Mem. Disclosure
  - Stack canaries
- **Lecture 18 & 19**: Toolchain-based Hard. (cont'd) & Advanced ROP
  - `FORTIFY_SOURCE`, `RELRO`
  - Stack pivoting
- **Lecture 20 – 23**: Special Topics
  - Control-flow Integrity
  - Heap exploitation
  - C++ exploitation
  - Kernel exploitation
  - …

Accommodations

Brown University is committed to the full inclusion of all students. Please inform me early in the term if you have a disability, or other conditions, which might require accommodations or modification of any of the course procedures. You may speak with me after class or during my office hours. For more information, please contact Student Accessibility Services (SAS) at 401-863-9588 or SEAS@brown.edu. In addition, undergraduate students in need of short-term academic advice or support can contact one of the deans in the Dean of the College office. Graduate students can contact one of the deans in the Dean of the Graduate School office.

Mental Health

Being a student can be very stressful. If you feel you are under too much pressure or there are psychological issues that are keeping you from performing well at Brown, I encourage you to contact Counseling and Psychological Services (CAPS). They can provide both confidential counseling and notes supporting extensions on assignments for health reasons.

Diversity and Inclusion

Our intent is that this course provides a welcoming environment for all students who satisfy the prerequisites. Our TAs have undergone training in diversity and inclusion, and all members of the CS community, including faculty and staff, are expected to treat one another in a professional manner. If you feel you have not been treated in a professional manner by any of the course staff, please contact any of Vasilis (the Instructor), Roberto Tamassia (Dept. Chair), Tom Doeppner (Dept. Vice Chair) or Laura Dobler (Diversity and Inclusion Staff Member). We will take all complaints about unprofessional behavior seriously. Lastly, your suggestions are encouraged and appreciated. Please let me know of ways to improve the effectiveness of the course for you personally, or for other students or student groups. To access student support services and resources, and to learn more about diversity and inclusion in the Department of Computer Science, please visit: https://cs.brown.edu/about/diversity/resources/.