

CSCI 1650: Software Security and Exploitation

Introduction

Vasileios (Vasilis) Kemerlis

September 04, 2024

Department of Computer Science
Brown University



Course Overview

- ▶ What is this course about?



Course Overview

► What is this course about?

- ✘ Memory unsafe code (written in C/C++, asm, ...)

► Software Security

1. Prevalent software defects

- Stack/Heap smashing
- Format string bugs
- Pointer errors
- ...

2. Modern defenses

- W^X, ASLR
- Stack/Heap canaries
- RELRO, BIND_NOW
- BPF_SECCOMP, FORTIFY_SRC
- ...



Course Overview

► What is this course about?

- ✘ Memory unsafe code (written in C/C++, asm, ...)
- ✘ Control-flow hijacking

► Software Security

1. Prevalent software defects

- Stack/Heap smashing
- Format string bugs
- Pointer errors
- ...

2. Modern defenses

- W^X, ASLR
- Stack/Heap canaries
- RELRO, BIND_NOW
- BPF_SECCOMP, FORTIFY_SRC
- ...

► Software Exploitation

1. Code injection

2. Code reuse

- Return-to-libc (`ret2libc`)
- Return-oriented prog. (ROP)
- Just-In-Time ROP (JIT-ROP)
- ...

**YOU
HAVE BEEN
HACKED**



Course Overview (cont'd)

- ▶ Why take this course?



► Why take this course?

☹ Offense

- ✓ Learn how to **break** software
 - Exploit development
 - Code “weaponization”
 - Binary exploitation

► Why take this course?

☹ Offense

- ✓ Learn how to **break** software
 - Exploit development
 - Code “weaponization”
 - Binary exploitation
- ★ Using only **gdb!**
(plus `objdump`, `readelf`, ..., etc.)

Course Overview (cont'd)

► Why take this course?

😊 Defense

- ✓ Understand the **boundaries** of protection mechanisms and argue about their **effectiveness**

😞 Offense

- ✓ Learn how to **break** software
 - Exploit development
 - Code “weaponization”
 - Binary exploitation
- ★ Using only **gdb!**
(plus **objdump**, **readelf**, ..., etc.)



Course Overview (cont'd)

► Why take this course?

😊 Defense

- ✓ Understand the **boundaries** of protection mechanisms and argue about their **effectiveness**

😬 Offense

- ✓ Learn how to **break** software
 - Exploit development
 - Code “weaponization”
 - Binary exploitation
- ★ Using only **gdb!**
(plus **objdump**, **readelf**, ..., etc.)

► Why are these useful?

- To protect software (against certain threats) you need to:
 - (a) understand what sorts of attacks are possible
 - (b) how exactly these attacks work



Prerequisites

- ▶ **CSCI 0330 (Introduction to Computer Systems)**
CSCI 0300 (Fundamentals of Computer Systems)
 - C/C++, x86 asm
 - Virtual memory
 - Linking and loading
- ▶ **CSCI 1670 (Operating Systems)**
 - Memory management



Prerequisites

- ▶ **CSCI 0330** (Introduction to Computer Systems)
CSCI 0300 (Fundamentals of Computer Systems)
 - C/C++, x86 asm
 - Virtual memory
 - Linking and loading
- ▶ **CSCI 1670** (Operating Systems)
 - Memory management
- ✓ Having taken the following courses is a plus, but not required:
 - **CSCI 1660** (Computer Systems Security)
 - **CSCI 2951E** (Topics in Computer System Security)



Prerequisites

- ▶ **CSCI 0330** (Introduction to Computer Systems)
CSCI 0300 (Fundamentals of Computer Systems)
 - C/C++, x86 asm
 - Virtual memory
 - Linking and loading
- ▶ **CSCI 1670** (Operating Systems)
 - Memory management
- ✓ Having taken the following courses is a plus, but not required:
 - **CSCI 1660** (Computer Systems Security)
 - **CSCI 2951E** (Topics in Computer System Security)
- ★ We will review (most of) the important concepts



🕒 Meetings

- MW 3PM – 4:20PM (T hour)
- Salomon Center 001 & Zoom



🕒 Meetings

- MW 3PM – 4:20PM (T hour)
- Salomon Center 001 & Zoom

@ Communication

- <https://cs.brown.edu/courses/csci1650/>
- Ed Discuss. | cs1650tas@lists.brown.edu



🕒 Meetings

- MW 3PM – 4:20PM (T hour)
- Salomon Center 001 & Zoom

@ Communication

- <https://cs.brown.edu/courses/csci1650/>
- Ed Discuss. | cs1650tas@lists.brown.edu

★ Check the website!

- Announcements
- Lecture slides/code/video
- Readings
- Assignment descriptions

🕒 Meetings

- MW 3PM – 4:20PM (T hour)
- Salomon Center 001 & Zoom

▶ Grading

- ✓ Participation → 10% (Ed)
- ✓ Assignments → 60%
 - 4x CTF-like write-ups
- ✓ Midterm → 10%
- ✓ Final → 20%

@ Communication

- <https://cs.brown.edu/courses/csci1650/>
- Ed Discuss. | cs1650tas@lists.brown.edu

★ Check the website!

- Announcements
- Lecture slides/code/video
- Readings
- Assignment descriptions



🕒 Meetings

- MW 3PM – 4:20PM (T hour)
- Salomon Center 001 & Zoom

▶ Grading

- ✓ Participation → 10% (Ed)
- ✓ Assignments → 60%
 - 4x CTF-like write-ups
- ✓ Midterm → 10%
- ✓ Final → 20%

▶ Study material

- No required textbook → Lecture slides/code & assigned readings
- Optional textbook:
 - Hacking: The Art of Exploitation, 2nd Edition. Jon Erickson. No Starch Press, 2008, ISBN 1593271441

@ Communication

- <https://cs.brown.edu/courses/csci1650/>
- Ed Discuss. | cs1650tas@lists.brown.edu

★ Check the website!

- Announcements
- Lecture slides/code/video
- Readings
- Assignment descriptions

► Instructor

Vasileios (Vasilis) Kemerlis

- vpk@cs.brown.edu
- <https://cs.brown.edu/~vpk>

Office hours: Mon. 6PM – 7PM (Zoom)



► Teaching Assistants

Maya Magavi → HTA

- mmagavi@cs.brown.edu

Alexander Portland → TA

- aportlan@cs.brown.edu

Bahar Birsal → TA

- bbirsal@cs.brown.edu

Caroline Cahill → TA

- ccahill5@cs.brown.edu

James Hu → TA

- jhu74@cs.brown.edu

Javier Fernandez Garcia → TA

- jferna35@cs.brown.edu

Kamyar Mirfakhraie → TA

- kmirfakh@cs.brown.edu

Kendra Lee → TA

- klee165@cs.brown.edu



► Teaching Assistants (cont'd)

Lucy Gramley → TA

· lgramley@cs.brown.edu

Pauline Nguyen → TA

· pnguye37@cs.brown.edu

Subham Kumar Das → TA

· sdas52@cs.brown.edu

Thu Luu → TA

· tluu6@cs.brown.edu

Yen Chu → TA

· ychu12@cs.brown.edu

Yu Nie → TA

· ynie8@cs.brown.edu

