CSCI 1650: Software Security and Exploitation

Introduction

Vasileios (Vasilis) Kemerlis

September 04, 2019

Department of Computer Science
Brown University
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)
   • ...
Course Overview (1/2)

► 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 (1/2)

▶ 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)
   • ...

vpk@cs.brown.edu (Brown University)  CSCI 1650  Fall '19
Why take this course?

- Understand the boundaries of protection mechanisms and argue about their effectiveness.
- Learn how to break software:
  - Exploit development
  - Code “weaponization”
  - Binary exploitation

Using only gdb! (plus objdump, readelf, ... etc.)

Why are these useful?

(a) To protect software (against certain threats) you need to:
(b) understand what sorts of attacks are possible
(c) how exactly these attacks work
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.)
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 (2/2)

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)
  - 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.
**Prerequisites**

- **CSCI 0330** *(Introduction to 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)**
  - 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
Logistics

Meetings
• Mon. and Wed., 1PM – 2:20PM
• CIT 368

Grading
• Participation: 10%
• Assignments: 60%
• 4x CTF-like write-ups
• Midterm: 10%
• Final: 20%

Communication
• https://cs.brown.edu/courses/csci1650/
• Piazza | cs1650tas@lists.brown.edu
• Check the website!
• Announcements
• Lecture slides/code
• Readings
• Assignment descriptions

Study material
• No required textbook
• Lecture slides/code & assigned readings
• Optional textbook:
Logistics

 Meetings

- Mon. and Wed., 1PM – 2:20PM
- CIT 368
Logistics

Meetings

- Mon. and Wed., 1PM – 2:20PM
- CIT 368

Communication

- https://cs.brown.edu/courses/csci1650/
- Piazza | cs1650tas@lists.brown.edu

No required textbook
- Lecture slides/code & assigned readings
- Optional textbook:
Logistics

 Meetings

- Mon. and Wed., 1PM – 2:20PM
- CIT 368

 Communication

- https://cs.brown.edu/courses/csci1650/
- Piazza | cs1650tas@lists.brown.edu

 Check the website!

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

Meetings
- Mon. and Wed., 1PM – 2:20PM
- CIT 368

Grading
- Participation → 10%
- Assignments → 60%
  - 4x CTF-like write-ups
- Midterm → 10%
- Final → 20%

Communication
- https://cs.brown.edu/courses/csci1650/
- Piazza | cs1650tas@lists.brown.edu

Check the website!
- Announcements
- Lecture slides/code
- Readings
- Assignment descriptions
Logistics

 Meetings

- Mon. and Wed., 1PM – 2:20PM
- CIT 368

 Grading

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

 Study material

- No required textbook → Lecture slides/code & assigned readings
- Optional textbook:

 Communication

- https://cs.brown.edu/courses/csci1650/
- Piazza | cs1650tas@lists.brown.edu

 Check the website!

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

Vasileios (Vasilis) Kemerlis
- vpk@cs.brown.edu
- https://cs.brown.edu/~vpk
Office hours: Mon. 3PM – 5PM (CIT 505)

Teaching Assistants

HTA ➔ Alexander Gaidis
- agaidis@cs.brown.edu
- Office hours: Wed. 5PM – 7PM (CIT 203)

TA ➔ Hannah Baackmaan-Friedlaender
- hbaackma@cs.brown.edu
- Office hours: Mon. 5PM – 7PM (CIT 203)

TA ➔ Changmin Teng
- cteng2@cs.brown.edu
- Office hours: Tue. 4PM – 6PM (CIT 205)

TA ➔ David Liu
- dliu19@cs.brown.edu
- Office hours: Thu. 10AM – 12PM (CIT 203)

TA ➔ Mneera Abdullah
- malsaud@cs.brown.edu
- Office hours: Fri. 4PM – 6PM (CIT 203)