CSCI 1650: Software Security and Exploitation

Introduction

Vasileios (Vasilis) Kemerlis

September 08, 2021

Department of Computer Science
Brown University
What is this course about?
### 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)
   - ...

YOU HAVE BEEN HACKED
Course Overview (2/2)

▶ 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`, ...)

▶ 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
Why take this course?

**Offense**

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

Why are these useful?

- To protect software (against certain threats) you need to:
  1. Understand what sorts of attacks are possible
  2. How exactly these attacks work
Why take this course?

規定 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.)
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:
  1. understand what sorts of attacks are possible
  2. how exactly these attacks work
Prerequisites

- **CSCI 0330** (Introduction to Computer Systems)
  - C/C++, x86 *asm*
  - Virtual memory
  - Linking and loading

- **CSCI 0300** (Fundamentals of Computer Systems)

- **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)
  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
Logistics

• MW 3PM – 4:20PM (T hour)
• MacMillan 117 & Zoom

Grading
- Participation: 10% (Ed)
- Assignments: 90%
- Midterm: 0%
- Final: 0%

• Check the website!

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

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

Study material
- No required textbook
- Optional textbook:
Logistics

 Meetings

- MW 3PM – 4:20PM (T hour)
- MacMillan 117 & Zoom
## Logistics

### Meetings
- MW 3PM – 4:20PM (T hour)
- MacMillan 117 & Zoom

### Communication
- [https://cs.brown.edu/courses/csci1650/](https://cs.brown.edu/courses/csci1650/)
- Ed Discuss. | cs1650tas@lists.brown.edu

---

vpk@cs.brown.edu (Brown University)  
CSCI 1650  
Fall '21
Logistics

 Meetings

• MW 3PM – 4:20PM (T hour)
• MacMillan 117 & 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
Logistics

 Meetings

- MW 3PM – 4:20PM (T hour)
- MacMillan 117 & Zoom

 Grading

- Participation ➔ 10% (Ed)
- Assignments ➔ 90%
  - 4x CTF-like write-ups
- Midterm ➔ 0%
- Final ➔ 0%

 Communication

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

 Check the website!

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

### Meetings
- MW 3PM – 4:20PM (T hour)
- MacMillan 117 & Zoom

### Grading
- Participation → 10% (Ed)
- Assignments → 90%
  - 4x CTF-like write-ups
- Midterm → 0%
- Final → 0%

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

### Communication
- [https://cs.brown.edu/courses/csci1650/](https://cs.brown.edu/courses/csci1650/)
- Ed Discuss. | cs1650tas@lists.brown.edu

### Check the website!
- Announcements
- Lecture slides/code/video
- Readings
- Assignment descriptions
## Staff

### Instructor

Vasileios (Vasilis) Kemerlis  
- vpk@cs.brown.edu  
- https://cs.brown.edu/~vpk  
Office hours: Mon. 5PM – 7PM (via Zoom)

### Teaching Assistants

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Email</th>
<th>Office hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTA</td>
<td>Zachary Espiritu</td>
<td><a href="mailto:zespirit@cs.brown.edu">zespirit@cs.brown.edu</a></td>
<td>TBA</td>
</tr>
<tr>
<td>TA</td>
<td>Andrew Boden</td>
<td><a href="mailto:aboden@cs.brown.edu">aboden@cs.brown.edu</a></td>
<td>TBA</td>
</tr>
<tr>
<td>TA</td>
<td>Andrew Cooke</td>
<td><a href="mailto:acooke1@cs.brown.edu">acooke1@cs.brown.edu</a></td>
<td>TBA</td>
</tr>
<tr>
<td>TA</td>
<td>Maura Driscoll</td>
<td><a href="mailto:mdrisco5@cs.brown.edu">mdrisco5@cs.brown.edu</a></td>
<td>TBA</td>
</tr>
<tr>
<td>TA</td>
<td>Ben Givertz</td>
<td><a href="mailto:bgivertz@cs.brown.edu">bgivertz@cs.brown.edu</a></td>
<td>TBA</td>
</tr>
<tr>
<td>TA</td>
<td>Brandon Lee</td>
<td><a href="mailto:blee50@cs.brown.edu">blee50@cs.brown.edu</a></td>
<td>TBA</td>
</tr>
</tbody>
</table>
Teaching Assistants (cont’d)

TA ➔ Zachary Mothner
   • zmothner@cs.brown.edu
   • Office hours: TBA

TA ➔ Ian Rackow
   • irackow@cs.brown.edu
   • Office hours: TBA

TA ➔ Daniel Ramirez
   • dcivita1@cs.brown.edu
   • Office hours: TBA

TA ➔ Alex Reuter
   • areuter@cs.brown.edu
   • Office hours: TBA

TA ➔ Marina Triebenbacher
   • mtrieben@cs.brown.edu
   • Office hours: TBA