CSCI 1650: Software Security and Exploitation

Introduction

Vasileios (Vasilis) Kemerlis
September 11, 2017

Department of Computer Science
Brown University
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
   • ...

Software Exploitation
1. Code injection
2. Code reuse
   • Return-to-libc (ret2libc)
   • Return-oriented prog. (ROP)
   • Just-In-Time ROP (JIT-ROP)
   • ...
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
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?

- To protect software (against certain threats) you need to:
  - Understand what sorts of attacks are possible
  - 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.)
### Course Overview (2/2)

#### Why take this course?

<table>
<thead>
<tr>
<th>Defense</th>
<th>Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️ Understand the <strong>boundaries</strong> of protection mechanisms and argue about their <strong>effectiveness</strong></td>
<td>✔️ Learn how to <strong>break</strong> software</td>
</tr>
<tr>
<td>- Exploit development</td>
<td>- Exploit development</td>
</tr>
<tr>
<td>- Code “weaponization”</td>
<td>- Code “weaponization”</td>
</tr>
<tr>
<td>- Binary exploitation</td>
<td>- Binary exploitation</td>
</tr>
<tr>
<td>✔️ Using only <strong>gdb</strong>!</td>
<td>✭ Using only <strong>gdb</strong>!</td>
</tr>
<tr>
<td>(plus <strong>objdump</strong>, <strong>readelf</strong>, ..., <strong>etc.</strong></td>
<td>(plus <strong>objdump</strong>, <strong>readelf</strong>, ..., <strong>etc.</strong></td>
</tr>
</tbody>
</table>

---

vpk@cs.brown.edu (Brown University)  
CSCI 1650
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
• Mondays, 3PM – 5:20PM (M hour)
• CIT 477 (Lubrano)

Grading
Participation Ü 10%
Assignments Ü 60%

Midterm Ü 10%
Final Ü 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:

vpk@cs.brown.edu (Brown University) CSCI 1650 Fall '17 5 / 6
Logistics

⊕ Meetings

• Mondays, 3PM – 5:20PM (M hour)
• CIT 477 (Lubrano)

Grading

4 Participation

4 Assignments

4 Midterm

4 Final

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:

vpk@cs.brown.edu (Brown University)
## Logistics

### Meetings
- Mondays, 3PM – 5:20PM (M hour)
- CIT 477 (Lubrano)

### Communication
- [https://cs.brown.edu/courses/csci1650/](https://cs.brown.edu/courses/csci1650/)
- Piazza | cs1650tas@lists.brown.edu
### Meetings
- Mondays, 3PM – 5:20PM (M hour)
- CIT 477 (Lubrano)

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

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

 Meetings

- Mondays, 3PM – 5:20PM (M hour)
- CIT 477 (Lubrano)

 Grading

- Participation → 10%
- Assignments → 60%
  - 3x/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
- Mondays, 3PM – 5:20PM (M hour)
- CIT 477 (Lubrano)

### Grading
- Participation → 10%
- Assignments → 60%
  - 3x/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/](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. 6PM – 8PM (CIT 505)

Teaching Assistant

Frederick Rice
- frice@cs.brown.edu
Office hours: Wed. 6PM – 8PM (CIT 506)