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)
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)
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:
  - (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

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

---

**vpk@cs.brown.edu** (Brown University)
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:
  - (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)**
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 Û 10%
• Assignments Û 60%
• 3x CTF-like write-ups

Midterm Û 10%
Final Û 20%

Communication
• https://cs.brown.edu/courses/csci1951-h/
• Piazza (TBA)

Check the website!
• Announcements
• Lecture slides
• Readings
• Assignment descriptions

Study material
■ No required textbook Û Lecture slides & assigned readings
■ Optional textbook:

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

Meetings

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

Grading

- Participation: 10%
- Assignments: 60%

Midterm: 10%
Final: 20%

Communication

- [cs.brown.edu/courses/csci1951-h/](https://cs.brown.edu/courses/csci1951-h/)
- Piazza (TBA)

Announcements

- Lecture slides
- Readings
- Assignment descriptions

Study material

- No required textbook
  - Lecture slides & assigned readings
- Optional textbook:

vpk@cs.brown.edu (Brown University)

CSCI 1951H

Fall '16
### Logistics

<table>
<thead>
<tr>
<th>Meetings</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mondays, 3PM – 5:20PM (M hour)</td>
</tr>
<tr>
<td>• CIT 477 (Lubrano)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <a href="https://cs.brown.edu/courses/csci1951-h/">https://cs.brown.edu/courses/csci1951-h/</a></td>
</tr>
<tr>
<td>• Piazza (TBA)</td>
</tr>
</tbody>
</table>
## Logistics

<table>
<thead>
<tr>
<th>Meetings</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Mondays, 3PM – 5:20PM (<em>M hour</em>)</td>
</tr>
<tr>
<td>• CIT 477 (<em>Lubrano</em>)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <a href="https://cs.brown.edu/courses/csci1951-h/">https://cs.brown.edu/courses/csci1951-h/</a></td>
</tr>
<tr>
<td>• Piazza (TBA)</td>
</tr>
</tbody>
</table>

⭐ **Check the website!**

- Announcements
- Lecture slides
- Readings
- Assignment descriptions
Logistics

Meetings

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

Grading

- Participation → 10%
- Assignments → 60%
  - 3x CTF-like write-ups
- Midterm → 10%
- Final → 20%

Communication

- https://cs.brown.edu/courses/csci1951-h/
- Piazza (TBA)

Check the website!

- Announcements
- Lecture slides
- Readings
- Assignment descriptions
Logistics

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

Grading
- Participation → 10%
- Assignments → 60%
  - 3x CTF-like write-ups
- Midterm → 10%
- Final → 20%

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

Communication
- https://cs.brown.edu/courses/csci1951-h/
- Piazza (TBA)

Check the website!
- Announcements
- Lecture slides
- Readings
- Assignment descriptions

vpk@cs.brown.edu (Brown University)
<table>
<thead>
<tr>
<th>Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instructor</strong></td>
</tr>
<tr>
<td>Vasileios (Vasilis) Kemerlis</td>
</tr>
<tr>
<td>· <a href="mailto:vpk@cs.brown.edu">vpk@cs.brown.edu</a></td>
</tr>
<tr>
<td>· <a href="https://www.cs.brown.edu/~vpk">https://www.cs.brown.edu/~vpk</a></td>
</tr>
<tr>
<td>Office hours: Mon. 6PM – 8PM (CIT 505)</td>
</tr>
<tr>
<td><strong>Teaching Assistant</strong></td>
</tr>
<tr>
<td>Luke Camery</td>
</tr>
<tr>
<td>· <a href="mailto:lcamery@cs.brown.edu">lcamery@cs.brown.edu</a></td>
</tr>
<tr>
<td>Office hours: Tue. 7PM – 9PM (CIT 227) &amp; Sun. 1PM – 3PM (CIT 227)</td>
</tr>
</tbody>
</table>