CSCI 2951U: Topics in Software Security

Introduction

Vasileios (Vasilis) Kemerlis

January 25, 2021

Department of Computer Science
Brown University

Course Overview (1/2)

- What is this course about?

Course Overview (1/2)

- What is this course about?
  - ✔ **State-of-the-art** in software exploitation and defense ➜ CSCI 1650++

Course Overview (1/2)

- What is this course about?
  - ✔ **State-of-the-art** in software exploitation and defense ➜ CSCI 1650++
  - ✘ 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`
   - CFI, CPI, ...

Software Exploitation

1. Code injection
2. Code reuse
   - Return-to-libc (`ret2libc`)
   - Return-oriented prog. (ROP)
   - Just-In-Time ROP (JIT-ROP)
   - Blind ROP (BROP)
   - Signal-oriented prog. (SROP)
   - ...
3. Data-only attacks

Course Overview (2/2)

- Why take this course?

Course Overview (2/2)

- Why take this course?

☻ Offense

✔ Learn **how** and **why** (certain) defenses can be **bypassed**

- Exploit “weaponization”

BROWN

Course Overview (2/2)

- Why take this course?

☺ Defense

- ✔ Understand the **boundaries** of protection mechanisms and argue about their **effectiveness**
- ✔ **Familiarize** with experimental mitigation techniques

☻ Offense

- ✔ Learn **how** and **why** (certain) defenses can be **bypassed**
  - Exploit "weaponization"

BROWN

Course Overview (2/2)

- Why take this course?

☺ Defense

- ✔ Understand the **boundaries** of protection mechanisms and argue about their **effectiveness**
- ✔ **Familiarize** with experimental mitigation techniques

☻ Offense

- ✔ Learn **how** and **why** (certain) defenses can be **bypassed**
  - Exploit "weaponization"

- Why are these useful?
  - To design effective (and efficient) software protection mechanisms you need to:
    (a) understand **what** sorts of attacks are possible
    (b) **how** exactly these attacks work
    (c) **why** previous attempts failed

BROWN

Prerequisites

- CSCI 1650 (Software Security and Exploitation)
  - Control-flow Hijacking
  - Code Injection (Shellcode dev.)
  - Code Reuse (ROP)
- CSCI 1670 (Operating Systems)
  - C/C++, x86 `asm`
  - Linking and Loading
  - Virtual Memory

BROWN

Prerequisites

- CSCI 1650 (Software Security and Exploitation)
  - Control-flow Hijacking
  - Code Injection (Shellcode dev.)
  - Code Reuse (ROP)
- CSCI 1670 (Operating Systems)
  - C/C++, x86 `asm`
  - Linking and Loading
  - Virtual Memory

✔ 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 1650 (Software Security and Exploitation)
  - Control-flow Hijacking
  - Code Injection (Shellcode dev.)
  - Code Reuse (ROP)
- CSCI 1670 (Operating Systems)
  - C/C++, x86 `asm`
  - Linking and Loading
  - Virtual Memory

✔ 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

BROWN

Logistics

Logistics

Meetings

- Mondays, 3PM – 5:20PM (M hour)
- Zoom

Logistics

Meetings

- Mondays, 3PM – 5:20PM (M hour)
- Zoom

@ Communication

- https://cs.brown.edu/courses/csci2951-u/
- course.csci.2951u.2021-spring.s01@lists.brown.edu

Logistics

Meetings

- Mondays, 3PM – 5:20PM (M hour)
- Zoom

@ Communication

- https://cs.brown.edu/courses/csci2951-u/
- course.csci.2951u.2021-spring.s01@lists.brown.edu

✪ **Check the website!**

- Announcements
- Lecture slides
- Readings

Logistics

Meetings

- Mondays, 3PM – 5:20PM (M hour)
- Zoom

@ Communication

- https://cs.brown.edu/courses/csci2951-u/
- course.csci.2951u.2021-spring.s01@lists.brown.edu

Grading

- ✔ Paper reviews ➜ 10%
- ✔ Paper presentations ➜ 20%
- ✔ Discussion part. ➜ 20%
- ✔ Project report ➜ 40%
- ✔ Project presentation ➜ 10%

✪ Check the website!

- Announcements
- Lecture slides
- Readings

Logistics

Meetings

- Mondays, 3PM – 5:20PM (M hour)
- Zoom

@ Communication

- https://cs.brown.edu/courses/csci2951-u/
- course.csci.2951u.2021-spring.s01@lists.brown.edu

- **Grading**
  - ✔ Paper reviews ➜ 10%
  - ✔ Paper presentations ➜ 20%
  - ✔ Discussion part. ➜ 20%
  - ✔ Project report ➜ 40%
  - ✔ Project presentation ➜ 10%

✪ **Check the website!**

- Announcements
- Lecture slides
- Readings

- **Study material**
  - No required textbook ➜ Assigned readings

Staff

▶ Instructor

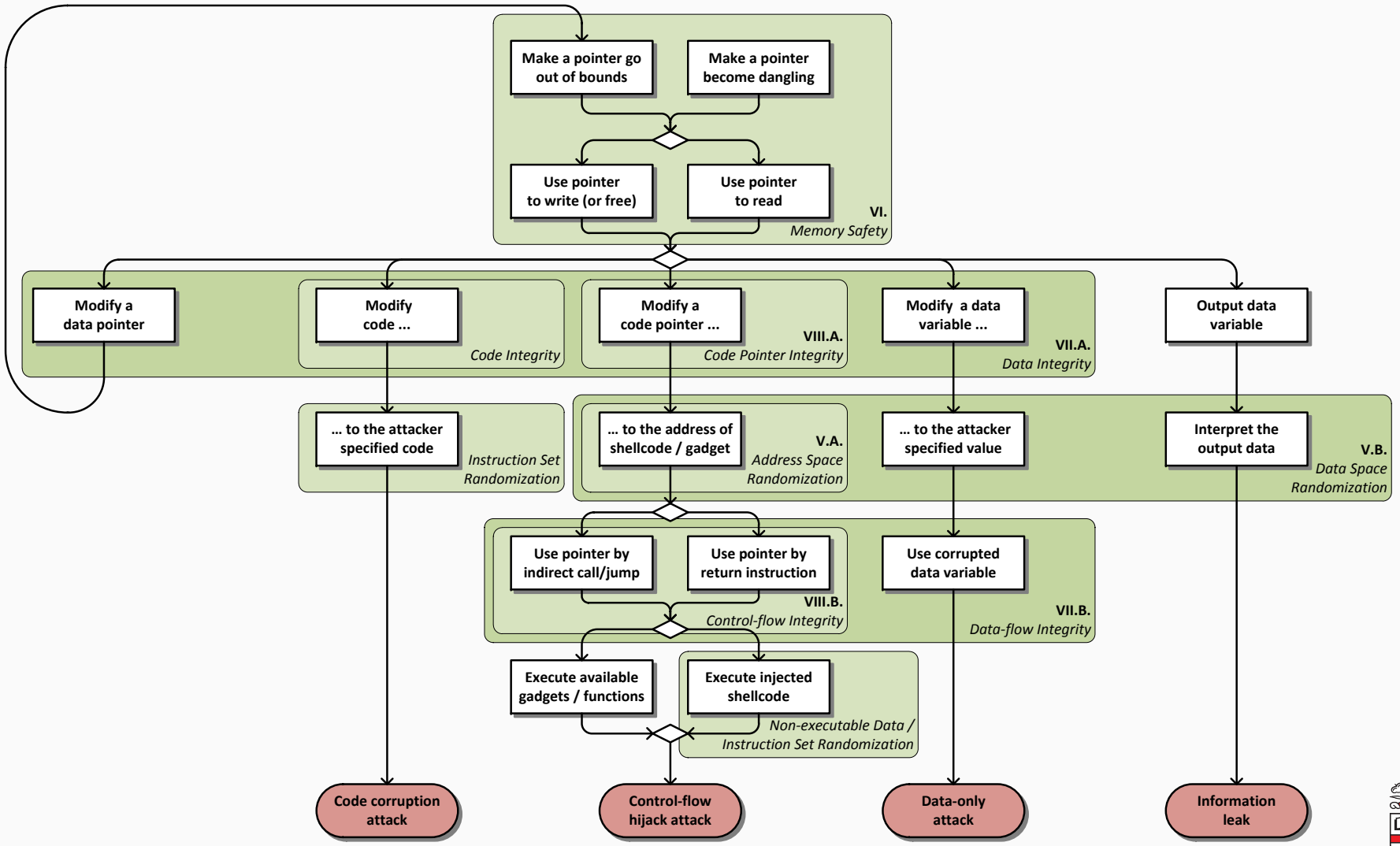
Vasileios (Vasilis) Kemerlis

- vpk@cs.brown.edu
- https://www.cs.brown.edu/~vpk

Office hours: Mon. 6PM – 7PM (Zoom)

BROWN

Memory Safety Circus



Source: "SoK: Eternal War in Memory." [IEEE S&P '13]