CSCI 2951-U: Topics in Software Security (Spring 2017)

- **Instructor:** Vasileios (Vasilis) Kemerlis
  - **Web:** https://cs.brown.edu/~vpk
  - **Email:** vpk@cs.brown.edu
  - **Office Hours:** 6PM–8PM, CIT 505

- **Meeting Time:** 3PM–5:20PM (M hour)
- **Meeting Location:** CIT 506

- **Prerequisites:** CSCI 1951-H (Software Security and Exploitation) or CSCI 1670 (Operating Systems)

Overview

In this course, we will (collectively) investigate the state-of-the-art in software exploitation and defense. More specifically, the course is structured as a *seminar* where students jointly present (with the instructor) research papers to their peers. We will begin with a summary of the most prevalent software defects, such as stack and heap buffer overflows, NULL pointer and pointer arithmetic errors, use-after-free and format string bugs, memory disclosure vulnerabilities, signedness errors, integer overflows, race conditions, etc., which are typically found in applications written in memory unsafe languages, like C and C++. Next, we will survey what we are up against: traditional and modern exploitation techniques, ranging from classical code injection and code-reuse attacks (return-to-libc, return-oriented programming) up to the newest goodies (just-in-time code reuse, blind ROP). For the bulk part, we will focus on the latest advances in protection mechanisms, mitigation techniques, and tools against the previously-mentioned vulnerability classes and exploitation methods.

Course Format

In each class, we will discuss 1–2 research papers. Students are expected to read the assigned papers and write a short review (critique) *before* each class. In addition, one student will do a short presentation about each paper for the day, which will be the starting point for our discussions.

In parallel, students will work on a semester-long project on an open research problem related to the topics covered in the course. Projects can have an *offensive* or *defensive* focus, or both, and projects relating to the students' own research interests are strongly encouraged, provided they also fit with the theme of the class.

Course Objectives

The goals of this course are twofold: (a) lean *how* and *why* (certain) software defenses can be bypassed; and (b) *familiarize* with experimental exploit mitigation techniques, in order to better *understand* the boundaries of protection mechanisms and *argue* about their effectiveness.

Paper Reviews

Everyone, apart from the presenter, is expected to read the paper(s) for the week and submit a *constructive* critique (review). The reviews should:

a) Be at most a page long.
b) Provide a summary of the assigned paper(s).
c) Discuss the pros and cons of the proposed idea, protection mechanism, or bypass technique.
d) Conclude with:
    1. at least two thought-provoking questions regarding the material covered in the paper(s);
    2. a brief direction of future work based on the ideas/topic of the assigned paper(s).

Paper Presentations

Each student will be presenting a (set of) research paper(s) to the class, and evaluated based on the following criteria:

a) **Understanding:** Does the presenter understand the material?
b) **Thoughtfulness:** Does the presenter have insights and opinions beyond what was in the paper?
c) **Clarity:** Can the audience understand the presentation? Is the "big picture" clear? Are there useful examples?
d) **Materials:** Do the slides or use of blackboard illustrate and support the talk? Are there diagrams to help convey the technicalities?
e) **Delivery:** Has the presenter practiced?
f) **Non-regurgitation:** Did the presenter do something beyond simply typing sections of the paper as bullet points? Did the presenter motivate the ideas in their own words, or just state ideas from the paper verbatim?
g) **Answering questions:** Can the presenter handle questions from the audience?

Course Project

The (semester-long) course project entails working on an *open* research problem, which can be *defensive* or *offensive* in nature (or both), and submitting (to the instructor) a workshop-quality research paper. Note that although the project may rely on concepts learned from existing papers, it *must* also introduce new ideas. Validation of prior work (in terms of effectiveness and/or performance) is permitted, but a more thorough analysis of the original work's strengths and weaknesses is expected.

Grading

- Class participation: 50%
    - Paper(s) presentation: 20%
    - Discussion participation: 20%
    - Paper reviews: 10%

- Project 50%
    - Interim report: 20%
    - Final report: 20%
    - Presentation: 10%

Credit Hours

Over 14 weeks, students will spend 3 hours per week in class (42 hours total). Required reading and weekly research questions is expected to take up approximately 7 hours per week (98 hours). In addition, researching and working on the final project is estimated at a total of approximately 40 hours over the course of the term.

Accommodations

Brown University is committed to the full inclusion of all students. Please inform me early in the term if you have a disability, or other conditions, which might require accommodations or modification of any of the course procedures. You may speak with me after class or during my office hours. For more information, please contact Student and Employee Accessibility Services at 401-863-9588 or SEAS@brown.edu. In addition, undergraduate students in need of short-term academic advice or support can contact one of the deans in the Dean of the College office. Graduate students can contact one of the deans in the Dean of the Graduate School office.