EC700 – Vulnerability, Defense Systems, and Malware Analysis

Organisational

Instructor: Manuel Egele
Email: megele@bu.edu
Schedule: M/W 12:20 – 14:05
Location: PHO 210
Office Location: PHO 337
Office Hours: By appointment

Course Description

This will be a project-led course to survey and understand the landscape of vulnerability detection, malware analysis, and defense systems. The official course title is Special Topics in Security: Vulnerability, Defense Systems, and Malware Analysis. The course title is intended to be parsed with the word “analysis” applied to each subject area:

- We analyze proposed and currently used systems for finding vulnerabilities on a system or in software.
- We analyze proposed and currently used systems for defending against vulnerabilities that might be present on a system.
- We analyze proposed and currently used systems for performing malware analysis.

Immanuel Kant once said: *Experience without theory is blind, but theory without experience is mere intellectual play.*

Thus, the course uses projects to guide exploration of research and understanding of the booming security field. The projects give context to thinking about what goes into the general problem domain, what problems are easy, and what are hard. The projects are also our starting point for exploring each topic: vulnerability detection, malware understanding, and designing effective defenses.

I will request that students fill out a questionnaire before the course commences to assess their background knowledge. The course will then be carried out in multiple epochs (planned three). In each epoch, students form groups in one of the problem areas to conduct their project in. For the following epoch, students have to choose one of the remaining subject areas. The goal of this rotation is
that by the end of the semester each student worked on one project in each of the three subject areas.

At the end of each epoch, groups present (and demo) their projects to the entire class. This has the added benefit that students get practice in presentation preparation and presenting in front of a critically-thinking audience.

In addition to the projects, the course features a distinct seminar course component. That is, for each lecture, the class will read a recent paper from one of the course’s topic areas. One student will be in charge of presenting the paper and lead the discussion. To further encourage that discussion, the class is split into proponents and opponents for each paper. The goal of these discussions is to hone the students’ skills to identify good research traits and how to structure and execute scientific experiments and papers.

**Grading**

Epoch 1 Project & Presentations: 30%
Epoch 2 Project & Presentations: 30%
Epoch 3 Project & Presentations: 30%
Participation: 10%