George Litvinov
Topics in SWE
Paper Proposal
Spring 2022

Teaching Security – The Practical Way: Implementing the Course Material

Proposed Topic:

As discussed previously, I would like to continue upon my midterm paper and implement the practical CTF-like course material for the fundamental theory-centric security course at Columbia – *COMS W4181 Security I*, in order to introduce the practical component of the course in a gamified way.

Project Flow:

The goal of the project will be to sift through the Syllabus of the Columbia course, and determine practical exercises that will go hand-in-hand with the lectures. Additionally, I will be taking my paper's survey as well as syllabi from other universities' security courses into account to gauge what topics are most important to cover in the practical component.

The second stage of the project will be to determine what Open-Source CTF framework is the most suitable for our purposes. Some criteria while researching the frameworks to consider would be:

- Can students register individually?
- How easy is it to implement a time-based release of assignments?
- Are there built-in anti-cheat mechanisms such as flag randomization?
- Can additional material other than the flag be submitted (for example, solution code)?
- What controls does the instructor (administrator) have?
- How modular is it?

This criteria will be further developed once the project starts taking shape.

The third stage of the project will be the implementation of unique challenges that will allow students to grow their practical skill. These challenges will be separated into multiple categories that were identified initially, and their point values will be assigned based on their difficulty. As an example, challenges for memory safety may include a buffer overflow challenge with an unsafe function, a ROP-chain attack, an overflow circumventing a canary, and a heap overflow. All of these challenges should be expected to be fulfilled by all students. Additionally, I may develop another more difficult challenge for each category that will require self-learning. The course may require the student to fulfill 1-2 of these challenges over the course of the semester, in order to promote students looking into a topic that interests them.

~~The fourth stage of the project will be to evaluate the faculty's as well as the students' responses to such a way of including practical exercises in a security course. The responses will~~

George Litvinov
Topics in SWE
Paper Proposal
Spring 2022

~~be collected either through an interview (with faculty) and a survey (students) or a survey for both.~~

Throughout the project I will be keeping Prof. Bellovin and Prof. Suman in the loop through a weekly meeting, collecting valuable feedback as well as wishes for additional features that should be implemented in order to maximize the portal’s usability in a classroom setting. The first meeting was already held.

After developing the portal, I will attempt to present the project to a few students in order to get their reaction.

Lastly, any tweaks and improvements will be done before presenting the final version of the project in this class.

For any clarifications on what this topic entails my paper, “Teaching Security – The Practical Way”, should be referenced.