[Provisional Title]:

[Subtitle]

Brendon Ky

December 8, 2021

1 Introduction

1.1 Motivation

The proliferation of the Internet and IoT devices means that we live in a world where computers are increasingly ubiquitous, inter-connected, and essential to daily life. With this comes an equal need to ensure the security of these devices. Currently, there is a tremendous disparity between the number of qualified cybersecurity professionals, and the amount needed to meet the industry's demands, one which is only projected to grow in coming years.

Beyond even the rudimentary threats faced by average individuals, several recent high-profile breaches have highlighted the vulnerability created when our technical demands outstrip our ability to meet those demands. In 2021, two major hacks made headline news. First, it was revealed that hackers had managed to infiltrate software used by all levels of local, state, and federal government, as well as some of the largest corporations in the United States, in what would become known as the SolarWinds Hack. Around the same time, Colonial Pipeline—a major oil pipeline in the United States—suffered a ransomware attack, forcing them to pay millions of dollars in ransom in order to resume service. Only a few years prior, the American credit bureau Equifax notoriously suffered from one of the most significant data breaches in history. The breach directly impacted over 140 million individuals, which is nearly half of all Americans.

These aforementioned hacks are only three of the most recent and infamous examples. What's even more astounding is how most of these attacks are carried out. While not a simple feat by any means, these attacks are in no ways groundbreaking. They fundamentally rely on vulnerabilities and techniques which have been around for years, if not decades. In order to prevent such catastrophic embarrassments from occurring in the future, it is essential to develop a strong workforce of cybersecurity professionals.

This immense demand places a tremendous burden on the higher educational system. Despite these pressures, the current state of academic literature regarding cybersecurity education is dismal. Up until recently (when compared to many other fields in Computer Science) cybersecurity was seen as a strictly professional discipline. It was conceived as a job which needed to be done, existing at the intersection of various fields, rather than a field of its own right. The job of cybersecurity, was the domain of IT professionals, not college students, and consequently, that's who all of the educational materials were developed for. For decades, all materials relevant to teaching cybersecurity tailored towards developing skills and preparing for certifications, rather than establishing establishing a strong educational background suitable for an undergraduate course of study.

This issue is further compounded by the many unique challenges of cybersecurity education. As a field, it is highly intersectional, drawing on a broad range of topics from systems architecture, cryptography, law enforcement, networking, software development and beyond. Owing to it's unique and diverse nature, it is difficult to adopt practices from adjacent fields.

1.2 Current State of Cybersecurity Education

1.3 Research Subject

2 Literature Review

3 Methods

For this research project, we will be developing a number of hands-on activities for a Capture the Flag (CTF) platform, where students will be tasked with completing a sequence of cybersecurity-related challenges. These activities will be designed and implemented based on the various previously identified design philosophies. In order to gather data about these designed materials, students who have already completed the introductory cybersecurity course (CS 597N) will be asked to perform these activities as part of the successor course CS 560. We will make it clear that their participation is part of an experiment, and students will be given the opportunity to opt out of participating, as it will not impact their grade in the course in any way. We will evaluate the performance and knowledge of the participants before and after completing these activities so as to measure the learning outcomes achieved by the activities.

Separately, we would like perform a second study by reaching out to former students who have taken courses which implement hands-on activities in order to survey them on their experiences with such activities on a volunteer basis.

All of participants in both studies will be senior-level undergraduate, or graduate students currently studying Computer Science at UMass Amherst. This will be the only selection criteria for participants in this research. We expect approximately 40-50 students to participate in the first study (corresponding to the number of students expected to be enrolled in CS 560). In the second study, we anticipate approximately 50-100 total participants.

4 Evaluation

There will be three primary deliverables created over the course of the spring semester.

- The creation of several experimental educational CTF-like lab activities designed around the previously identified design philosophies.
- Surveys evaluating the efficacy each of these lab activities.
- Surveys of former students measuring their experiences with lab activities in cybersecurity courses.

The ultimate goal will be to synthesize these three results in order to draw meaningful and empirically validated conclusions about each of various philosophies.

5 Communication

I will meet with my thesis committee chair, professor Kermani, at least once weekly for an hour, with additional meetings scheduled if it becomes necessary. In these meetings, we will discuss and evaluate what I have accomplished over the previous week, and then plan what will be worked on over the following week. Beyond these meetings, I will be spending 10-15 hours weekly working on the research project.

6 Timeline