[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, a disparity 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— 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 such as 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

One of the few points broadly agreed upon across the literature, is that there is a stark lack of agreement; in other words, all of the researchers in this area can only agree to disagree. This disagreement is only further compounded by the despairing lack of quantitative research into the subject. The extant literature largely focuses on alternative approaches to teaching, in opposition to the traditional professor-led lecture-based approach to instruction. From these alternative approaches, to categorize them into two rough themes: *hands-on learning* and *collaborative-learning*. However, even these loose categories quickly disintegrate upon closer inspection.

The bulk of the literature believes that the *hands-on learning* approach— where students engage with in-class activities to apply what they have been learning in a course— has the greatest potential for successful educational outcomes. There are several factors which make this approach seem attractive. First, this model has seen wide adoption and success within computer science at large; owing to how intimately computer science and cybersecurity, it is a natural conclusion that the same pedagogical approaches should be similarly effective. Second, there is already a strong tradition among cybersecurity professionals of hands-on competitive exercises, such as Capture-the-Flags (CTFs) and King of the Hill (KotH) competitions. This tradition makes it easy to co-opt the vast amount of pre-existing skills and resources around these challenges for educational purposes.

While seemingly straightforward, it would be a mistake to view this approach as a monolith. There is a wide divergence regarding how these activities are best integrated into the classroom environment. This disagreement largely revolves around the degree of assistance or guidance provided by the instructor to the students.

There is a widely-held school of thought, that the most ideal approach to learning is through totally self-guided exploration, an approach which can be described as *minimal-guidance*. However, there is also a highly vocal countercurrent to this prevailing belief. Proponents of this approach accuses *minimal-guidance* of being overly dogmatic, and out of touch with the reality of psychological and educational research. This approach, which can be described as *maximal-guidance*, advocates for providing students with all of the requisite information to complete their hands-on activities. Naturally, in the center of this maximalist-minimalist spectrum there also exists a compromise approach.

1.3 Research Subject

While there is a great amount of qualitative research expounding the various approaches, there is little in the way of empirically qualified data to validate these claims. Even though the *maximal-guidance* approach is founded upon a substantial body of psychological research, which offers the veneer or scientific justification, the reality is that this research is scarcely less qualitative or more rigorous than that presented in favor of *minimal-guidance*. In light of this, there is a tremendous

opportunity for novel research to investigate the individual merits of each of the various schools of thought.

I would like to propose precisely this as the subject of my research. While there is a notable body of speculative work done on these various approaches, there has been virtually no serious investigation to validate their hypotheses. For my research, I intend to design a number of educational hands-on activities founded in each of the identified schools of thought in order to experimentally affirm or reject the validity of the competing claims. To further this investigation, I also plan on conducting surveys of computer science students at this university, who have formerly taken cybersecurity courses which integrate hands-on activities into the course's instruction. I will evaluate the courses' curriculum, and the design of the activities so as to properly classify them into the different design philosophies. The students will then be asked to evaluate their experiences in the class, specifically relating to the use of these activities, and report on how they were perceived.

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