Building a Cyber Range for UVA Computer Science Students

An Analysis of the Social Impact Cybersecurity Competitions

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Chase Hildebrand

October 27, 2023

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Kent Wayland, Department of Engineering and Society

Briana Morrison, Department of Computer Science

General Research Problem: Expanding the Horizons of Hands-On Cybersecurity Education

How can we better prepare students for the rapidly growing cybersecurity industry?

In the modern online world, cybersecurity is becoming more important than ever to protect our digital lives. In 2022, cyberattacks cost US companies over $10.3 billion in damages (Federal Bureau of Investigation 2022). Employers have been scrambling to hire cybersecurity professionals to keep ahead of bad actors attempting to infiltrate corporate and government networks. In February 2023, there were over 750,000 job openings for cybersecurity professionals (Morgan, 2023). To counter this, schools should offer an avenue for students to gain the knowledge and skills required to start a career in cybersecurity and meet these demands. Schools are starting to offer more cybersecurity classes and degrees, some, such as Rochester Institute of Technology and Dakota State University, have gone as far as to make an entire cybersecurity department. These schools have invested resources into building large scale computing clusters that are designed to simulate real networks, allowing students to safely get hands-on cybersecurity experience in realistic situations without worrying about malicious traffic leaking to the outside internet. These clusters are called cyber ranges. Students whose schools have not invested as much in cyber security, like UVA, may not have access to these resources. For my technical project, I will implement a cyber range for UVA, which will act as a framework describing how universities can quickly and cheaply build cyber ranges for their students.

One of the primary motivations for building this system is to train students to compete in cybersecurity competitions. As the field of cybersecurity expands, people have turned to cybersecurity competitions for a variety of reasons: government and companies, to recruit top talent, students to sharpen their skills, and educators to train the next generation of cyber professionals. These competitions have had relative success when compared to traditional education and may prove to be a more effective method of teaching students cybersecurity. Through my STS project, I seek to investigate the extent to which competitions have influenced the cybersecurity educational landscape.

Technical Research Question: Building a Cyber Range for UVA Computer Science Students

How can we develop an effective and scalable computing solution that allows students to efficiently practice cybersecurity in a controlled environment?

Students best learn cybersecurity with hands-on activities and engagements. There are a few boundaries to these engagements, though. First, setting up an environment where they can safely practice cyber security is difficult and often requires specialized systems and networking knowledge not taught in classes. Second, building larger networks is tedious without automation, which is also tedious and difficult to program without experience. Third, hosting these virtualized networks, especially larger ones, requires powerful computing hardware.

Given these technical boundaries, most students have limited opportunities to participate in hands-on cyber activities. Often, the only cybersecurity opportunities students are aware of are through classes. UVA's current Network Security course teaches network defense by having students use Docker, a software for running applications in an isolated environment, on their laptop. This solves the automation and setup issue, but it cuts out a technology that comprises

70% of the market share in corporate networks: Windows. There is no good way to run Windows services in Docker containers. Furthermore, using Docker prevents students from safely practicing another important part of network security: firewalling. While it is possible to do from Docker, it is not secure to do so in most cases. One solution to this is to use a technology that can simulate full computer hardware, like VMWare Workstation Pro or Vagrant, but this brings a large amount of computational overhead and would be inequitable for students who don't have powerful laptops. Finally, with this method there is no way for students to participate in engagements between multiple students.

To solve these problems my team and I plan to build a platform specifically designed to let students practice cyber security in a safe and controlled environment. We will do this in three phases: evaluation and design, installation, and automation development.

In the evaluation and design phase, we will evaluate different software and system architectures to determine which best fits our requirements. The software we have chosen to evaluate for simulating networks of computers are Apache CloudStack, OpenStack, OpenNebula, and Proxmox because they are well-maintained, featureful, and have community support. To evaluate each of these systems, we will build mock-ups of each of them in our lab using a technique that lets us run virtual machines inside of virtual machines, called nested virtualization. We will evaluate each software's effectiveness of fulfilling our design requirements using the following criteria: presence of must-have features, presence of nice-to-have features, user interface design, ease of setup and maintenance, availability of automation tooling, availability of community support.

After determining which software best fits our requirements, we will begin the second phase: production installation. In this phase, we will rebuild the system we designed in the first phase, but this time using physical servers rather than virtual machines.

The final phase of the project is to develop automation to automatically build virtual networks for users. At its current state, users have to manually provision networks themselves. This typically takes hours, even for a small network. Our automation will take in a user-specified configuration and provision a network based on it in the cyber range. The purpose of this is to remove the burden of manually setting up networks and to reduce network provision time by orders of magnitude. Event organizers and professors can leverage this automation to quickly set up competition environments or labs for students, enabling users to practice defending larger networks without having to spend large amounts of time setting them up.

Our success with this project will not only allow UVA students to learn and explore in a hands-on environment on their own, but give professors, club leaders, and competition organizers the tools to provide computational resources to all students at scale. Additionally, this project will also function as an inspiration and starting point for other schools to build similar systems for their cybersecurity students, making the entire field as a whole more accessible.

STS problem: An Analysis of the Social Impact Cybersecurity Competitions

To what extent have competitions influenced the cybersecurity education landscape?

Cybersecurity competitions emerged from niche games hackers played against each other to practice and improve their craft without affecting real infrastructure. They were created to solve the shortage of technically skilled people required to operate, support, and build secure systems (Department of Homeland Security, 2023). Until 2010, cybersecurity competitions were "designed and geared towards industry professionals and students in academia… not to attract interests" (Balon, 2023, p. 11762). As the field of cybersecurity gained traction, competitions have become more popular, not only as mere games or training mechanisms for professionals but also as a magnet drawing newcomers into the field.

In 2011, twenty competitions were registered on ctftime.org, a site used to track cybersecurity competitions. As of December 2023, this number has grown to over 330 (CTFtime, 2023). As competitions gain popularity and recognition, teams have become increasingly competitive, sometimes training for months for a single competition. Schools have started adding competition-like curriculum to cyber classes, encouraging and advertising cyber competitions, and funding trips and entrance fees for competitions. This project's goal is to determine to what extent competitions have influenced the cybersecurity education landscape and explore the presumed symbiotic relationship between the two.

Cybersecurity competitions take several forms, the most popular being attack-defense, capture the flag, and penetration testing. Attack-defense competitions, also known as red versus blue, comprise of two sides -- the attackers (red team), who try to break into a network, and the defenders (blue team), who try to defend the network from the attackers. In capture the flag competitions, competitors are given a series of problems, each worth a certain number of points based on difficulty, and the team or individual who solves the most wins. In penetration testing competitions, competitors attempt to find as many vulnerabilities in a network as they can in a given period of time and then write a report based on their findings.

In each of these competitions, competitors are required to work together to reach a common goal. Success demands not only extensive knowledge and problem-solving skills but also effective communication between team members. Cybersecurity classes highlight the importance of the security mindset, which emphasizes thinking like an attacker (Schneier, 2008). Competitions allow students to practice this way of thinking. By taking learning out of the classroom in a hands-on setting, competitions help reinforce what students learn. Zichermann and Cunningham (2011), authors of Gamification by Design, reveal that gamification increases skill retention by 40 percent.

Competitions also provide unique networking opportunities that would normally be inaccessible for uninvolved students. They commonly have career fairs that enable students to connect with prospective employers, industry professionals, and experts in the field. Additionally, bringing students together from different schools or, in the case of national competitions, across the country allows them to share ideas and promote intellectual diversity.

I will research how competitions have influenced cybersecurity education by using actor-network theory to analyze how different groups interact with one another when preparing for, competing in, and debriefing from/reflecting on cybersecurity competitions. Then, I will interview competition organizers, competitors, and competition sponsors from both companies and the government to gather information about what they and the community gain from cybersecurity competitions, why they are participating, and how—from their perspective—competitions affect cybersecurity education. After analyzing the actors directly involved with competitions, I will expand the scope of the sociotechnical system to include actors in adjacent avenues of cybersecurity education, such as traditional classroom-based education seen in most universities, and industry professionals working in cyber security. To get perspective on how these actors fit into the system, I will interview cybersecurity professors, security operations center (SOC) analysts, and penetration testing professionals. Through these interviews, I will gather information on how competitions influence academia and evaluate the extent to which they have shaped cybersecurity education.

Conclusion

This project aims to provide the tools and understanding to build student opportunities to help them succeed in the field of cybersecurity. The technical portion outlines the implementation of a fully fledged cyber range, empowering students to explore cybersecurity on their own, with a team, or in a more structured setting with ease. The STS portion will present an analysis of how cybersecurity competitions fit into the education landscape, highlighting their importance in the growing industry. The answers to both of these questions will answer the larger question of how we can better prepare our students to defend our digital world from the threats that try to tear it down.

References

Balon, T., & Baggili, I. (Abe). (2023). Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Education and Information Technologies*, *28*(9), 11759–11791. https://doi.org/10.1007/s10639-022-11451-4

CTFtime. (n.d.). *CTFtime.org / All about CTF (Capture The Flag)*. Retrieved December 12, 2023, from https://ctftime.org/event/list/

cybercrimemag. (2018, February 23). Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/jobs/

Department of Homeland Security. (2023, January 12). *Cybersecurity Competitions | Homeland Security*. https://www.dhs.gov/science-and-technology/cybersecurity-competitions

Federal Bureau of Investigation. (2022). *Internet Crime Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Schneier, B. (2008, March 20). *Inside the Twisted Mind of the Security Professional | WIRED*. https://www.wired.com/2008/03/securitymatters-0320/

Zichermann, G., & Cunningham, C. (2011). *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*. O’Reilly Media, Inc.