Eureka!: Advancing Cybersecurity Learning through Inquiry-Based Laboratories

Curby Alexander, Ph.D.
Texas Christian University
USA
curby.alexander@tcu.edu

Abstract: Cybersecurity is rapidly becoming one of the most important industries in the world, in regards to the national, financial, and environmental well-being of every nation. There are currently about half a million cyber attacks every minute, and the attacks will continue to increase in complexity and frequency as hackers adapt their strategies to the ever-changing cyber physical landscape. It is critical to train and educate the future workforce on the fundamental aspects of cyber and mobile security, and to improve their ability to identify, prevent, and respond to emerging threats. The purpose of this paper is to discuss the development of a collection of cybersecurity labs - called Eureka Experiences - designed to teach sophisticated concepts in an engaging, efficient, and affordable virtualization environment. This presentation will also address the future research and development of these labs, and propose possible strategies for adapting them to a wide range of learners.

We are living in a world where cyber attacks, privacy violations, phishing scams, and data breaches have become commonplace. Recently, CNBC reported that there are about half a million cyber attack attempts every minute (Taylor, 2016). In addition, hackers will be able to launch increasingly sophisticated attacks in the near future due to the ever-shifting cyber physical landscape (e.g., the emerging Internet of Things). However, there is a shortage of cybersecurity professionals and practitioners. A Cisco report estimated that there will be 1.5 million unfilled positions in the cybersecurity industry by 2019 (Cisco, 2015). Therefore, it is critical to train and educate the future workforce on the fundamental aspects of cybersecurity, and to improve their ability to identify, prevent, and respond to emerging threats.

Due to the complicated and abstract nature of many cybersecurity concepts and techniques, it is challenging for students to comprehend them in an effective manner. To address this challenge, we have developed creative and innovative solutions that can help transform the status quo of cybersecurity education. Our approach is inspired by the following well-known fact: students learn more effectively from interest than from effort. There are two main forms of interest: personal and situational. Generally speaking, personal interest is relatively stable and resides within the individual, while situational interest is spontaneous, transitory, and environmentally active. Students show obvious differences in the level of personal interest in different cybersecurity topics. If a student has little prior personal interest in a topic, the teacher needs to stimulate initial situational interest, which can be triggered temporarily by environmental factors such as unexpected events or surprising topics. Furthermore, the teacher needs to prolong and maintain the initial interest by engaging students in meaningful and thoughtful activities.

Purpose of Study

The two major goals of this project are to create environmental factors that can arouse students' situational interest and design activities that can facilitate effective learning. Our project design is based on the inquiry-based learning model and enabled by recent advances in virtualization technology.

Specifically, our project consists of a set of inquiry-based, interest-excitement, hands-on laboratories that are hosted on an affordable, scalable, extensible, and low-maintenance container-based virtualization platform.

Laboratories

The set of laboratories (abbreviated as "labs" hereafter) targets students at different levels, taking them on an interactive journey where they observe facts, ask questions, gather information, investigate clues, research answers, and ultimately implement appropriate measures. These labs feature a series of mock security incident scenes filled with unexpected stimuli. For each scene, students are given a number of intriguing questions and challenging tasks: i) What exactly happened (e.g., discover the facts and the timeline of the incident)? ii) How did it happen (e.g., use hints and clues to find out the vulnerabilities that caused the incident)? iii) Select and implement appropriate cybersecurity technologies to thwart similar attacks in the future. At the end of each lab, students will be asked to review and formalize their "free reflections," and then to turn them into written summaries. Many of these lab activities begin with a clear connection to certain cybersecurity concepts, which help students respond to them actively. Through these activities, we strive to make abstract concepts tangible, encourage learning in a non-lecture format, expose the students to scientific methods in action, and convey the excitement of performing experiments.

In order for teachers with different instructional capacities and resources to adopt our lab curriculum, the labs need to be hosted on a computing platform that is affordable, scalable, extensible, and low-maintenance. Recently, container-based virtualization (Docker, 2019) emerges as a more efficient solution that can greatly improve performance over hypervisor-based virtualization (e.g., VMware ESXi) at a reduced cost. A container is typically composed of just the application and its dependencies. It runs as an isolated process in the user space on the host operating system, sharing the kernel with other containers. Thus, it can pack considerably more applications into a single physical server than that of a hypervisor-based virtual machine, which significantly reduces cost and improves scalability. In addition, a container is not tied to any specific infrastructure; it can be hosted on any cloud provider, which offers substantial flexibility and reduces maintenance overhead. We will ship our labs in standardized containers so that they are very easy to deploy.

This project involves three types of labs: outreach, core, and advanced. Outreach labs are exploratory in nature with the goal to stimulate curiosity and interest from a wide range of audiences, especially community college students. Core labs aim to convey a broad spectrum of cybersecurity concepts and techniques to diverse student learners in a hands-on setting. Advanced labs concentrate on introducing emerging cybersecurity technologies and inspiring student research.

Design Principles

Interest is the key to an enjoyable learning experience, which helps make acquiring knowledge a natural progression. While the field of cybersecurity is of incredible beauty, many of its elegant concepts are surprisingly challenging for comprehension. Students usually have to spend a large amount of time working through mathematical barriers and internal blocks in order to comprehend these complicated concepts. Unfortunately, strenuous work and long hours often lead to frustration and loss of interest. Labs, especially the ones inspired by real-world problems, are an effective means

of stimulating interest and facilitating comprehension. We adopt the following key principles in the design of our proposed inquiry-based, interest-excited, and hands-on labs.

Principle 1: Spark Curiosity: Ask, Don't Tell.
An instructor's very first step is to ignite student interest in a subject matter. It is true that some students do not have prior personal interest in cybersecurity. Nonetheless, situational interest can be triggered temporarily by features of the immediate situation (e.g., unsolved mysteries or unexpected events). Inspired by the inquiry-based learning model, we will use questions to introduce a new cybersecurity topic in order to focus the students' minds on the lab material that is coming. These questions are designed to connect the topic to something with which the students are familiar. Such a connection helps them realize the importance and relevance of the topic. For example, alluding to something in the recent or popular press (such as a wide-spread virus) is quite effective in sparking curiosity that will encourage interest. Moreover, these questions need to be crafted with the aim to create wonderment or suspense (e.g., providing some mystery or puzzle) to further stimulate interest. Lastly, many of these questions should be directed to elicit student discussion, which is also very effective in arousing interest.

Principle 2: Sustain Interest: Discover through Action.
Since situational interest is short term, we naturally come to the next step: prolong and maintain the triggered interest throughout the lesson. When you can hold the interest of the students, it will lead to deeper levels of comprehension and thought. Active involvement (e.g., hands-on activities) and social connections (e.g., group work) are effective measures for sustaining interest. Hence, we will make a conscious effort to engage students in meaningful problem-solving activities with appeal in groups through discussion or individually. These problem-solving activities include formulating a hypothesis, carrying out meaningful research, analyzing data, deriving conclusions, and translating solutions into implementation. For example, in some of our labs, students are grouped to perform network reconnaissance, data collection and analysis, and reasoning to solve a puzzle/problem. Lab material organization is another important factor affecting interest. Lab materials need to be concrete (e.g., relevant, coherent, and easy to understand), which is vital to prolonging situational interest. Furthermore, background knowledge preparation also influences interest. When students have basic knowledge of a subject area, they feel more interested because they have a sense of what they are learning. As a result, we will organize lab materials to provide sufficient topic knowledge, which helps form a deeper understanding.

Principle 3: Prevent Frustration: Build from the Ground Up.
Negative emotions (such as frustration) associated with learning are a primary reason for students' disengagement, withdrawal, or even failure. Students possess different backgrounds, and thus, varied abilities to carry out lab tasks. It is important that each lab can be carried out by an average student in a timely manner. For instance, some portions of our proposed labs require programming and debugging skills. Hence, students may have to spend a large amount of time on coding activities that are not closely related to security concepts but necessary for carrying out the lab tasks. To address this issue, the design of our labs should be modular and flexible so that they can be easily adapted to fit different student groups. The lab design also needs to convey to students the sense that "I can do this," along with the

expectations to be achieved. Higher perceived competence leads to increased intrinsic motivation, interest, and engagement.

Principle 4: Adopt with Ease: Implement without Detriment.
If the labs are what the instructors need but not what they can easily use, we lose the battle before it starts. It is critical that our proposed labs can be easily adopted (i.e., time- and cost-effective implementation) by an average instructor. To be specific, the cost of purchasing necessary equipment or software needs to be affordable. The required lab preparation time (such as installation and configuration) needs to be reasonable. Modifying and debugging the labs should be feasible tasks. Thus, we propose to host our proposed labs on a generic, flexible and extensible container-based virtualization computing platform, which can save setup time and costs. We also plan to design each lab as an individual application. Inside each application, data and configurations should be decoupled. Additionally, we will make security systemic within the application. Lastly, we will provide detailed supporting documents and training for prospective users.

Future Directions

As this project moves forward, the research and design team will assess learning outcomes from these cybersecurity labs. We will assess the outcomes of the project based on the following two key factors: i) The effectiveness of the proposed labs on improving students' ability to understand, evaluate, and apply fundamental security concepts and techniques; ii) The time- and cost-effectiveness of the proposed labs. Student learning will focus on cybersecurity concepts, learner engagement, and the influence of the labs on student interest in cybersecurity careers.

The time- and cost-effectiveness factors will measure the appropriateness of the design of the proposed labs and the platform. Researchers will measure the amount of effort that the instructors and students need to spend to complete the lab activities. For example, we will measure how long it takes for an instructor (or a teaching assistant) to prepare each lab, how long it takes for a student to complete each lab, and student and instructor perceptions about the clarity of the lab instructions.

Conclusion

The need for skilled, highly-trained cybersecurity professionals has never been greater, and the demand for qualified security experts will only grow. As the strategies used by hackers continue to become more sophisticated and relentless, defense strategies will need to increase in complexity and elegance. The cost to institutions for developing and deploying high-quality cybersecurity educational learning environments requires expensive hardware and considerable time required to set up each lab. Additionally, the cybersecurity concepts and skills the students are learning are complicated, require a lot of time, and can lead to frustration and subsequent disengagement from the content. The Eureka Labs we are designing address both of these barriers to creating an effective learning environment. First, they are built upon a container-based virtualization platform that runs off each student's operating system without consuming large amounts of memory. These containers can be easily accessed and deployed from the cloud, significantly reducing the amount of time needed to set up the lab environment. This places the student and instructor focus on the concepts at hand rather than wasting time and energy setting up the lab. Second, the labs are designed around an inquiry-based framework that allow the students to focus on the

relevant issues and experiment with cybersecurity concepts. We believe this design strategy for our labs will be effective for teaching cybersecurity concepts, will reduce the load for setting up and deploying cybersecurity learning environments, and lead to a more enjoyable, efficacious learning experience for the next generation of cybersecurity professionals.

References

Cisco.(2015). Mitigating the cybersecurity skills shortage. Retrieved from http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

Cisco. (2019). Cisco visual networking index: Global mobile data traffic forecast update, 2016 - 2021 white paper. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-forecast-qa.pdf

Docker. (2019). What is a container? Retrieved from https://www.docker.com/what-container?

Taylor, H. (2016). Biggest cybersecurity threats in 2016. Retrieved from http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html