CHEESE: Cyber Human Ecosystem of Engaged Security Education

Baijian Yang
byang@purdue.edu
Purdue Polytechnic Institute
West Lafayette, USA

Rajesh Kalyanam
Purdue University
West Lafayette, USA
rkalyana@purdue.edu

Craig Willis
University of Illinois at Urbana-Champaign
Champaign, USA
willis8@illinois.edu

Mike Lambert
University of Illinois at Urbana-Champaign
Champaign, USA
lambert8@illinois.edu

Christine Kirkpatrick
San Diego Supercomputer Center
San Diego, USA
christine@sdsc.edu

ABSTRACT

The CHEESE project supplements and enhances traditional cybersecurity education with hands-on, practical experience in common cybersecurity flaws and solutions. CHEESE requires only a web browser, allowing users to develop cybersecurity skills without compromising their own computer or spending hours setting up a complex virtual machine (VM) or sandbox environment. In this tutorial we will conduct a hands-on walkthrough of a couple of cybersecurity demonstrations on CHEESE and present an overview of the platform and the community-driven contribution and development process.

CCS CONCEPTS

• **Security and privacy → Network security**; **Software and application security**; • **Applied computing → Computer-assisted instruction**; **Interactive learning environments**.

KEYWORDS

cybersecurity, containers, cloud computing, education

ACM Reference Format:
Baijian Yang, Rajesh Kalyanam, Craig Willis, Mike Lambert, and Christine Kirkpatrick. 2019. CHEESE: Cyber Human Ecosystem of Engaged Security Education. In *The 20th Annual Conference on Information Technology Education (SIGITE '19), October 3–5, 2019, Tacoma, WA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3349266.3351393

1 INTRODUCTION

Cybersecurity has increasingly featured front and center in our current digital era. With the pervasive adoption of computing devices for activities ranging from social media, to banking, travel and communication; cybersecurity is now vital in protecting personal and privileged information. To better prepare the future information technology workforce, various initiatives have been put in place to impart cybersecurity instruction. However, outside of a few recognized institutions of academic excellence in cybersecurity education and training, programs may fail to make the transition from theory to practice. CHEESE seeks to remedy this situation by providing a publicly accessible resource that supplements and enhances cybersecurity education with practical, hands-on training. We envision CHEESE to be a collaborative, community-driven effort with educators, students, and researchers contributing, evaluating, and developing demonstrations of cybersecurity flaws and solutions to be hosted on CHEESE.

CHEESE utilizes container technology due to its ability to encapsulate applications with various software dependency stacks, while incorporating fine-grained control and resource restrictions. Furthermore, containers can be easily extended and revised, enabling collaborative and incremental development and reuse. Using CHEESE requires just a web browser, obviating the need for the non-trivial setup that is typically required by other such training platforms. Our publicly accessible training platform CHEESEHub (https://www.hub.cheesehub.org), is based on the National Data Service's (NDS) Labs Workbench [2], a scalable, web-based platform for the deployment of containerized applications and tools. CHEESEHub is open-source and employs the GitHub feature request, issue reporting, and contribution pipeline. All contributed demonstrations also require background information on the cybersecurity flaw being demonstrated and detailed instructions for following along with the demonstration. CHEESEHub employs the Software Carpentry model for presenting this information and to organize such documentation into lessons on various cybersecurity topics. Interested faculty can incorporate any of these lessons in their teaching plans.

2 WORKSHOP FORMAT

In our 90-minute tutorial, we will spend 60 minutes with attendees walking through three demonstrations of cybersecurity exploits hosted on CHEESEHub: *ARP Poisoning*, *SQL Injection*, and the *HeartBleed* bug. Each attendee will be able to launch their own copy of the containers for each demonstration and follow along with the Software Carpentry style lessons on each of these exploits.

SIGITE '19, October 3–5, 2019, Tacoma, WA, USA

ACM ISBN 978-1-4503-6921-3/19/10.
https://doi.org/10.1145/3349266.3351393

In the remaining 30 minutes, tutorial instructors will present a broad overview of the CHEESEHub platform and underlying technologies. The presentation will also include details on the contribution process and demonstrate how new contributions can seamlessly integrated into the platform, and how documentation can be compiled into Software Carpentry lessons.

3 EXPECTED AUDIENCE AND LEARNING OUTCOMES

3.1 Expected Audience

This workshop is targeted towards cybersecurity students and instructors. While the students may be familiar with these three exploits from their coursework, they may have not had the opportunity to execute these exploits themselves and study their real-world impacts. Cybersecurity instructors may be interested in CHEESEHub from the perspective of a new resource that they can use in their classroom instruction. The community-driven nature of CHEESE necessitates the involvement of a broad community of potential users that can help drive the development and deployment of containers demonstrating various well-known and recently discovered exploits. By providing a cybersecurity learning lab in the cloud, CHEESE lowers the barriers for students and institutions to offer hands-on training to students via netbooks or lab/library computers with web browsers, broadening access and participation to a wider community.

3.2 Learning Outcomes

- Cybersecurity students will get hands-on experience running a few common exploits and see one example of their real-world impact.
- Cybersecurity students will learn about a novel and popular technology: containerization.
- Cybersecurity instructors will learn about the CHEESEHub platform and various ways of incorporating it into their teaching activities.
- Cybersecurity students and instructors will learn about ways that they can contribute to the platform; either as container developers or reviewers.
- Workshop presenters can gain valuable feedback on the usability of the platform and suggestions for feature enhancements and new demonstrations. Presenters can also connect with interested contributors and users of the platform.

4 PRIOR WORK

CHEESE was inspired by prior work on the IEEE TryCybSI project. TryCybSI [1] also used containerization and cloud computing to host demonstrations of twelve cybersecurity exploits, research applications, and cryptography assignments. While TryCybSI used the Amazon Web Services' EC2 container service (ECS) for load balanced deployment of containers, NDS Labs uses the more feature-rich and cloud provider agnostic Kubernetes framework for load-balanced container orchestration. While TryCybSI has been presented at conferences before, this would be our first hands-on workshop with either platform.

ACKNOWLEDGMENTS

This work was funded by the NSF award no: 1820573.

REFERENCES

[1] Rajesh Kalyanam and Baijian Yang. 2017. Try-CybSI: An Extensible Cybersecurity Learning and Demonstration Platform. In *Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17)*. ACM.

[2] Craig Willis, Mike Lambert, Kenton McHenry, and Christine Kirkpatrick. 2017. Container-based Analysis Environments for Low-Barrier Access to Research Data. In *Proceedings of the Practice and Experience in Advanced Research Computing (PEARC 2017) on Sustainability, Success, and Impact*. ACM.