Thesis Project Portfolio

Preparing the Next Generation of Engineers: Adjusting the Curriculum for Cybersecurity Education

(Technical Report)

The Missing Piece of Cybersecurity Education, from an STS Perspective

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jason Lee

Spring, 2024

Department of Computer Science

Table of Contents

Executive Summary

As technology continues to spread to a broader audience, cybersecurity education needs to play catch up in order to adjust to the growing number of inexperienced and non-security minded personnel. My technical report discusses curriculum changes to all Engineers and Computer Science majors. This change would increase the number of professionals interested in security while also introducing more security-minded personnel into the workplace, and give UVA a headstart in combating weak links in cybersecurity training. My STS research paper discusses how to tackle cybersecurity education to those who are unfamiliar with the implicit rules of the internet. Applying these tactics should make cybersecurity education more effective across a broader audience. These two reports both discuss educating non-experts on cybersecurity, as they are the most vulnerable personnel in any critical infrastructure. In order to preserve the integrity of the internet and keep the public safe, the points brought up must be taken to heart.

Introducing two courses, Protecting the (Internet of) Things and Keeping Your Systems Secure, introduces security early into all engineering strands, and expands upon topics not covered in depth in our current curriculum (such as mobile device security). By introducing these topics and raising awareness of security threats to students, current gaps in knowledge for Engineers and Computer Science majors would be addressed and can lead to developments of more secure systems in the future.

Making Intro to Cybersecurity mandatory, adding a mandatory security course, and addressing topics that are not deeply explored in our current CS curriculum should lead to a better trained and more security conscious group of Engineering alumni. It may also increase the number of undergraduates that sign up for the cybersecurity focal path, but may also cause gender

differences within the field due to the gamification of the mandatory engineering course. Hands-on learning would also further skills that are sought after in the workplace, leading to better employment opportunities after graduation.

My STS research question was, “Why is it so difficult to teach cybersecurity education to a wider audience?” The significance lies within several reports discussing how non-experts and those who are much less experienced with dealing with cybersecurity incidents are most likely to be targets or victims of attacks. To properly train these personnel, we must understand why just teaching concepts such as buffer overflows or SQL injection attacks are not enough to prevent weak systems from being developed. My STS report dives into surveys on tech literacy and competence, performs a literature review on curriculums in both undergraduate and K-12 settings as well as legislation dealing with digital devices, and analyzes this data with respects to cultural lag and tacit knowledge and the framework of the diffusion of innovation/information.

In terms of evidence, legislation is often written by mal-informed congress members or government employees with little to some knowledge on the subject, instead of industry experts. This leads to legislation that is broad, has unintended consequences, and most often leads to confusion and security vulnerabilities. Along with this, in terms of attempting to recruit more students to join the cybersecurity field, under-funded and under-priviledged areas may struggle to properly implement these courses, while undergraduate students are taught the theories behind the attacks more often than the execution of the attacks themselves, leading to those members being somewhat unprepared for the workplace. Cultural lag exists between SES factors and age, and the tacit knowledge that is lost in between makes those who are unfamiliar less likely to react properly in important situations. Exposing users to the internet (in a safe and controlled manner) can help bridge this gap in tacit knowledge and make our systems more secure.