

Improving Computer Science Curricula to Better Prepare Students to Develop Secure  
Applications

CS4991 Capstone Report, 2022

Azward Khan  
Computer Science  
The University of Virginia  
School of Engineering and Applied Science  
Charlottesville, Virginia USA  
[aak3sk@virginia.edu](mailto:aak3sk@virginia.edu)

## **Abstract**

Cyber security concerns in the United States have created a need for more people with the skills to handle these issues. I propose exposing students at the University of Virginia to real life cybersecurity applications by creating a new course, Cybersecurity in the Modern Workplace. Inspired by concepts taught in CS3420 (Advanced Software Development Techniques) and CS4630 (Defense Against the Dark Arts), the new course would teach students to design meaningful applications while incorporating cybersecurity techniques. Future criteria can be modified to ensure that the course stays relevant to priorities in a constantly evolving cyberspace.

## **1. Introduction**

Cyber security concerns in the United States have become an increasingly big issue with even United States President Joe Biden declaring October cyber security awareness month to bring attention to the matter. It is becoming more evident that computer science students should be better prepared in being able to develop applications with secure design. I propose the idea of a synthesized course, Cybersecurity in the Modern Workplace (CMW), combined with CS3420 (Advanced Software Development Techniques) and CS4630 (Defense Against the Dark Arts).

The goal of this synthesis would be to create a course that teaches students how to develop applications with an emphasis on implementing security techniques and design practices that prevent applications from being hackable. This in turn will enable students to be comfortable with security practices that can be beneficial in the United States' fight to improve cyber security.

## **2. Related Works**

A CNBC report from 2021 included getting the opinions and insights of cybersecurity experts; the report highlighted how ransomware attacks in the United States have become a big issue that continues to become worse<sup>1</sup>. While some governmental policies have been implemented to tackle the issue, the experts agreed that there is still much to do in terms of cybersecurity. My proposal provides a possible solution to this issue by having students at the University of Virginia have the ability to take courses involving more rigorous cybersecurity techniques that reflect on current issues. In Andreasson's *Cybersecurity: Public Sector Threats and Responses* from 2011, he highlights how other countries have become much more developed in cyber threats and cybersecurity<sup>2</sup>. This is a continuing trend today and more of a reason that students interested in cybersecurity should be exposed to meaningful techniques sooner rather than later.

## **3. Proposed Design**

In CS3240, which focuses on having students develop web apps, could require students to implement security aspects into their applications. However, given the nature of the course, it is unlikely that meaningful security techniques can be added without eliminating core concepts specific to the CS3240 curriculum. A separate synthesized course solely dedicated to teaching security techniques within applications would be more beneficial for students, CMW would plug in this gap.

The methodology to make such a course feasible would require examining the curricula of both CS3240 and CS4630. It would also require examining how techniques and concepts taught in CS4630 can be applied into the application development process demonstrated in

CS3240. Similar to CS3240, students would have to develop an application as a project, but they would focus on the security aspect. CMW would allow a course based on these principles to be offered which then would allow students to learn how to make meaningful applications with security techniques.

In CS3240, students are required to form groups in order to simulate working in a team similar to that in the actual workforce. In CMW, a similar procedure would take place, with students formed into groups for their project. The security techniques taught in CS4630 are more focused on how to prevent attacks at a machine language level. CMW would involve implementing application security which would be more focused on establishing protocols and maintaining system integrity. For example, a group might be tasked with creating a bank account system and must ensure that the application properly authorizes users and the app is not hackable. Students must test their system by trying to penetrate their applications. Ways to test an application's penetrability would be a topic also covered in this course. This will ultimately aid in creating work-ready students that can help tackle America's cyber security issues.

#### **4. Anticipated Results**

Through the creation of Cybersecurity in the Modern Workspace, the anticipated results would be to create more cybersecurity work-ready students at the University of Virginia. Being able to create projects that mimic applications they would be expected to design in the actual work environment would result in students who are already familiar with fundamental concepts once they get cyber engineering jobs. Over time, this can create a stronger cyber security front at a national level.

## **5. Conclusion**

The importance of cybersecurity education in the United States is always growing as we continue to lean towards a digital society with innovations in areas such as our phones, cars, and even cryptocurrency. There must be more urgency and more of a push for us to prepare ourselves. The University of Virginia should be enthusiastic about being a part of this and implementing a new course, Cybersecurity in the Modern Workplace, can help in this regard. This course would allow students to simulate working in cybersecurity situations that they would have to engage in in real scenarios. Such a course would not only help students but also contribute to America's need for better cybersecurity.

## **6. Future Work**

One of the main selling points of this course, CMW, is that it would be designed to present the student with concepts that are relevant to modern techniques. The cyber landscape is constantly changing, it would be necessary to revise the curriculum as time goes on. Students should have some sort of foundation of cybersecurity knowledge going into this course, so making Introduction to Cybersecurity (CS3710) may be necessary. Additionally, there needs to be more work to the design in regards to grading criteria. What exactly constitutes a secure application may be debatable and a strong but fair grading criteria needs to be implemented.

## References

<sup>1</sup>Andreasson, K. J. (2012). *Cybersecurity Public Sector Threats and responses*. CRC Press.

<sup>2</sup>CNBC. (2021, June 9). *Why The U.S. Can't Stop Cyber Attacks* [Video]. YouTube.

[https://www.youtube.com/watch?v=hSQf3hUx9J0&t=201s&ab\\_channel=CNBC](https://www.youtube.com/watch?v=hSQf3hUx9J0&t=201s&ab_channel=CNBC)