Enhancing Cybersecurity Education and Workforce Through Colorado-Washington Security Scholar Program

Yan Bai[*], Sang-Yoon Chang[+], Ken Lew[*], and Simeon Wuthier[+]
[*]School of Engineering and Technology, University of Washington Tacoma
[+]Computer Science Department, University of Colorado Colorado Springs

Abstract - Colorado-Washington Security Scholars Program (CWSSP) is a scholarship program for training and educating cybersecurity engineering students. Hosted in two universities for the students in the cybersecurity degree programs, the cross-campus program emphasizes virtual teamwork and collaborations in learning cybersecurity and executing the cybersecurity projects. This paper explains how the CWSSP program uniquely enhances the cybersecurity education and workforce development particularly focusing on the mechanisms to incorporate collaborations for the student scholars' training and the outcomes of the collaborations. We share our experience and insights from delivering the scholarship program in this paper.

1 Introduction

The CyberCorps (R): Scholarship for Service (SFS) program has a history dated back to 1998 where a directive was signed stating that the Executive Branch would need to assess the vulnerabilities of cybersecurity within the nation's critical infrastructure and to produce detailed plans in defending and protecting against future cyber threats. Hence in the year of 2000, SFS was created with the purpose in mind to further enhance the existing relationship between higher education institutions with different federal agencies to strengthen the Information Assurance (IA) disciplines as well as other federal initiatives within IA. Since then, SFS represents the opportunity for scholarship recipients to participate in Federal, State, Local or Tribal Government as a cybersecurity professional. [1]

Started in August 1, 2019, with the same spirit of collaboration to strengthen the nation's cybersecurity professionals through SFS, the University of Colorado at Colorado Springs (UCCS) and University of Washington Tacoma (UWT) proposed a collaborative program called Colorado-Washington Security Scholars Program (CWSSP). The collaboration between the two universities stemmed from a grant awarded by the National Science Foundation under the CyberCorps (R): Scholarship for Service (SFS) program to establish the CWSSP program.

Throughout this paper, we would explore the events and activities that took place between two campuses as well as some key data and outcome from CWSSP collaboration. [2,3]

2 Collaboration in research projects

Virtual Teams Course - CWSSP emphasizes teamwork building on the cross-campus program being hosted across two geographically distant universities in Colorado and Washington states. To promote and facilitate virtual teamwork, CWSSP includes a Virtual Teams Course which teaches the participating student scholars the knowledge and techniques to improve on their virtual teams and collaboration skills and practice. The Virtual Teams Course is a hybrid course where the course kicks off from an in-person setting and is followed by the virtual/remote classes for the rest. Dr. Kay Yoon, an expert in communications, delivers this unique course and designed it based on the state-of-the-art research in communications in social science, including the application of the transactive memory systems theory for a course assignment [4].

CWSSP Conferences (Student Presentations) - CWSSP Conference is held once a year in one of the university campuses. While this year's conference is supposed to be held at UWT campus, however due to the global pandemic, it was held virtually. The purpose of this conference is to give scholars a platform to present and share their research with other fellow scholars as well as other guests within the two campuses.

Interdisciplinary Research - With SFS fund support, we initiated a large interdisciplinary research project among two institutions, UCCS and UW Tacoma in blockchain and supply chain. Our team consists of 15 members with various academic backgrounds including computer science, information systems, mathematics, business, and economics. Part of preliminary results from our SFS student members were presented at the 24th University of Washington Annual Undergraduate Research Symposium and at the UCCS annual research symposium, Mountain Lion Research Week (from which the CWSSP work won the sole Top Scholar Award).

Other Blockchain Projects - Thanks to the CWSSP workshops, conferences, and offline meetings, there have been numerous opportunities to exchange research ideas and collaborate on research projects. As a result, CWSSP scholars and faculty have been productive with their research outcomes [4-6,8], by collaborating on and developing the necessary building blocks to assist in research directions. Examples of this include a proof-of-work blockchain network simulator [5], machine-learning-based anomaly detection on Bitcoin networking [6], and the discovery of denial-of-service vulnerabilities within the Bitcoin Core consensus protocol (submitted for peer-reviewed publication). This ongoing research are described in greater detail in the rest of this section.

Blockchain Network Simulator [5] - A proof-of-work blockchain network simulator was developed within the CWSSP program as a means to visualize the preliminary information about how blockchain technology's function, and what kind of parameters can be measured. When a UWT student scholar visited UCCS, a UCCS scholar provided a demo for the simulator to facilitate the simulator use for research. It was also followed by virtual remote meetings to further the effort and network with other scholars. We are actively distributing the simulator so that it enables and facilitates others conducting research in blockchain networking security; the first author of the simulator work, Simeon Wuthier, is in active communications with others interested in using the simulator for their own research, including a student working on his Thesis Dissertation outside of the US.

Machine Learning to Secure Blockchain Networking [6] - The UCCS scholar working on the aforementioned blockchain network simulator, Simeon Wuthier, has implemented a working Bitcoin node to not only help validate the blockchain-networking simulator but also to enable data-driven research and study. The data based on the active Bitcoin node fueled and drove the machine learning algorithm for securing blockchain networking. More specifically, the research work used semi-supervised learning to build anomaly detection against the networking threats, including those from the state-of-the-art research and discoveries in blockchain networking such as Eclipse attack [7] and DoS.

Novel DoS Vulnerabilities on Blockchain - While researching blockchain implementations, and more specifically, the Bitcoin Core source code along with its compiled application, a scholar helped to discover some critical portions of code that become vulnerable to a DoS attack when targeted by a modified/malicious Bitcoin node. From this discovery, we have been in direct communication with the Bitcoin developers to work on patching these issues and securing the implementation against modified Bitcoin nodes.

3 Constructing the Master's-to-PhD pipeline to generate the cybersecurity leaders with PhD degrees to secure the national cyberspace.

University of Washington Tacoma (UW Tacoma) and University of Colorado Colorado Springs (UCCS) established an articulation agreement in 2017 to facilitate admission and degree completion of students earning Master of Cybersecurity & Leadership (MCL) degree at UW Tacoma to the PhD in Engineering-Concentration in Security degree program at UCCS. Per the agreement, all students that graduate from UW Tacoma MCL degree program with a 3.3 GPA or higher will be admitted directly into the PhD in Engineering-Concentration in Security degree program at UCCS, so long as they otherwise meet the UCCS requirements for admission. Additionally, 21 semester credit hours will transfer to with approval of UCCS Computer Science Department PhD in

Security committee. This agreement has proven beneficial to both institutions. Seven MCL alumnus are puring PhD in Security at UCCS.

Apart from the seven MCL graduates that are pursuing the PhD program at UCCS, this year would be the first year where our MCL graduate student who is also a SFS scholar is entering the PhD program at UCCS in 2021 Fall. Since SFS scholars are required to be committed as a full-time student, this MCL graduate student has participated in various research projects within the University of Washington system as well as collaborating with faculty and other PhD students at UCCS in research projects. With a program like CWSSP, that particular graduate student benefited from the tight relationship between the two campuses and was able to build a strong foundation in collaboration and in establishing research direction even before MCL graduation and into the PhD program. In other words, CWSSP is a platform for SFS scholars to network and work on research topics with other faculties and professionals in the area of cybersecurity. This enhances the overall experience of SFS scholars within CWSSP regardless if their next pathway would be joining the workforce or if they would continue on their education path within cybersecurity.

4 Project Outcomes

CWSSP was launched in Fall 2019 and is ongoing. This section describes the project outcomes in the first two years of the program since its launch. In these two years, CWSSP recruited and supported one PhD scholar, six master's scholars, and six bachelor student scholars.

Employment data - CWSSP is a part of the CyberCorps Scholarship for Service (SFS) program where the scholars are required to fulfill the service requirements to work in the US government after graduation. CWSSP provided a total of 9 scholar graduates and those graduates began their security-clearance-required employment at the US government, including Department of Defense (DoD), Department of State (DoS), National Renewable Energy Laboratory (NREL), Washington State Government and National Security Agency (NSA).

Diversity - CWSSP prioritizes diversity and inclusion for the scholar selections. The students supported in the past two years include three female students, one Hispanic student, one African American student, and two Southeast Asian students.

Outreach - CWSSP is designed for outreach and specifically has the CWSSP Conference to outreach and network beyond the CWSSP and the participating departments. Our CWSSP Conferences in 2020 and 2021 included cybersecurity experts' presentations from the academic, government, and industry sectors. The scholars also attend the yearly nationwide SFS Career Fair events to represent CWSSP and network with the cybersecurity experts and potential employers beyond CWSSP.

Testimony - CWSSP has a systematic evaluation plan to solicit and receive feedback from the scholars to improve the program every year. The evaluations include semesterly surveys and individual communications between the scholar and the faculty. The student responses have been overall positive about the program and demonstrates that the CWSSP program improves the student's aptitude in cybersecurity research/project and virtual teamwork. Example qualitative responses about the overall program quality and usefulness include: "It [the CWSSP program] is potentially life changing and people need to know about the opportunity" and "This program has provided me a great opportunity to achieve more than just an education" and "It met and exceeded expectations." Other feedback/responses helped improve the CWSSP events and components, for example, "I think a research discussion session would be a nice touch, since everyone's research is similar, everyone would have things to contribute" and "[...] I enjoyed being involved in events as a group where I could interact with others."

5 Lessons learned

From Faculty - CWSSP is a unique CyberCorps SFS program enhancing the host institutions' degree programs by focusing on cybersecurity research/projects and virtual teamwork/collaborations. Having these focuses anchor the design and the execution of CWSSP components and mechanisms provided a unifying theme and goal. Sharing these visions and the success cases also helped engage the student scholars.

From Students - Additionally, the program has been beneficial to the participants through the hands-on research projects and collaboration across campuses. In fact, the two authors that are student scholars of the program have seen many opportunities for networking and gaining real-world experience. By driving the research across many projects, and learning effective collaboration skills, this has been a valuable learning experience not only for the education provided by the program, but from the interactions with potential future employers, and experts in the cybersecurity field.

6 Conclusion

The CWSSP collaboration is unique and it shows the creativity of the collaboration through various events and projects while all communication was through a virtual environment. According to our project outcomes, not only does CWSSP enhance the cybersecurity education between the two campuses, but the program also better helps and prepares its scholars for the cybersecurity workforce within government agencies. More importantly, it broadens the perspective of all its scholars with multidisciplinary research and increases their professional network by connecting with other professionals outside of their own campus.

Acknowledgements

The research was in part supported by the National Science Foundation (NSF) Grant 1921576 and 19922410.

8. References

[1] *CyberCorps®: Scholarship for Service*. [Online]. Available: https://www.sfs.opm.gov/. [Accessed: 22-Jun-2021].

[2] “Colorado-Washington Security Scholars Program,” *University of Colorado, Colorado Springs*. [Online]. Available: https://cwssp.uccs.edu/. [Accessed: 22-Jun-2021].

[3] “Cybercorps Scholarships to Expand Cybersecurity Education,” *Cybercorps Scholarships to Expand Cybersecurity Education | UW Tacoma*. [Online]. Available: https://www.tacoma.uw.edu/news/article/cybercorps-scholarships-expand-cybersecurity-education. [Accessed: 22-Jun-2021].

[4] K. Yoon and S.Y. Chang, “Teaching Team Collaboration in Cybersecurity: A Case Study from the Transactive Memory Systems Perspective,” *IEEE Global Engineering Education Conference (EduCon)*, 2021.

[5] S. Wuthier and S.-Y. Chang, “Proof-of-Work Network Simulator for “Blockchain and Cryptocurrency Research,” *ICDCS 2021 - 41st IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2021.

[6] J. Kim, M. Nakashima, W. Fan, S. Wuthier, X. Zhou, I. Kim, S.Y. Chang, “Anomaly Detection based on Traffic Monitoring for Secure Blockchain Networking, *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021.

[7] Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on bitcoin’s peer-to-peer network. In: 24th USENIX Security Symposium (USENIX Security 15). pp. 129–144 (2015)

[8] L. Wang, S. Lin, Y. Bai, S.Y. Chang, X. Li and P. Liu, "A Privacy Preserving Method for Publishing Set-valued Data and Its Correlative Social Network," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1-7, doi: 10.1109/ICC40277.2020.9149167.