Treyvien Kirk

7/14/2024

Jennifer McCullough

Griffiss Institute

Viceroy Maven Program

CYSE 368

Summer 2024

Table of Contents

Introduction

My internship is with the Griffiss Institute's Viceroy Maven program which focuses on developing and gaining experience in the discipline of cybersecurity within various government sectors. The internship lasted from June 3rd to August 9th, 2024, and presented me the opportunity to travel to White Marsh, Maryland to work with the Department of Defense (DoD) in their Aberdeen Proving Grounds (APG) locations. By outlining the objectives of the internship, detailing my experiences, explaining what I've learned, and sharing my overall thoughts of the internship program, I will be able to fully detail if I've been able to succeed in meeting these objectives as well as my own and learn to use this experience to further grow in my cyber career.

I decided to take on this opportunity after applying to it from an Old Dominion University related email presenting potential internship opportunities. After applying and completing an interview process, they presented me a great opportunity to learn more and enhance my cybersecurity skills along with learning technical sectors of the DoD. Additionally, I was able to learn more insights of the program through another colleague's experience which helped encourage me to pursue the opportunity.

Griffiss Institute is a 501(c)(3) nonprofit corporation established in 2002 in Rome, New York that works in partnership with the Department of Defense and works to accelerate STEM talent and technology that is comprised of an elite international network of academic, government, and industry partners (Griffiss Institute, 2024). The Viceroy Scholars program encourages a direct mission of developing foundational expertise in critical cyber operation skills for future military and civilian leaders of the Armed Forces and the Department of Defense (Griffiss Institute, 2024). Griffiss Institute also has a supportive history with Old Dominion University in providing a $400,000 award to help grow a diverse cybersecurity workforce pipeline (Grinkewitz, 2022).

Goals & Objectives

To start, Griffiss Institute pinpoints their objectives for the program and what they hope to foster into their Maven students after completing the program. Their first objective is to develop early student interest in challenging DoD and National Security problem sets. Their second objective is to enhance the pipeline of cyber and electromagnetic spectrum students at the secondary school level. Third is to increase the number of cyber and EMS instructors at secondary and collegiate levels. Their fourth is to hone student competencies in leadership, teamwork, and oral and written communications. Their fifth is to reduce student financial barriers to increase retention and enhance geographic mobility. Their last objective is to provide

exciting internship experiences hosted by engaging and supportive mentors, leading to permanent employment within the DoD.

In addition to these objectives for the Viceroy Maven program, my own personal goal for the program includes learning and developing core cybersecurity related skills and experience fundamental tools that can benefit my cybersecurity career. In addition to this, I would like to gain new connections that could be beneficial in gaining a new perspective of how to progress and succeed within the cybersecurity field.

Overview

To begin explaining my experience, an overview of the setting and projects should be described. Griffiss Institutes' Viceroy program collaborated with the Department of Defense and their Army Research Laboratory (ARL) location to provide me the opportunity to relocate and work at APG and their private host site in Maryland. Due to operational security, there may be certain areas that I am unable to expand upon as this information is not approved for public release. I was given the ability to stay in a neighboring hotel provided by the program that also provided me the opportunity to explore areas close to the location. Through working with the DoD and their secure locations, I was able to obtain security clearances in order to participate in the program and work in specific sectors containing operational security. Another benefit to gaining a clearance through this opportunity is it allows me to find another opportunity requiring one easier by only needing a sponsor to claim it. To further grasp the setting of the internship, I also had the opportunity to drive my own vehicle to and from various site locations, tours, orientations, and other events.

Initial Thoughts

Before diving into the internship experience, a description of my initial thoughts and impressions should be described. The Viceroy program was immensely helpful and supportive of helping me to clear any confusions I had before and during the internship to ensure I was as comfortable as possible while away from home along with reaffirming to me their goal to make this a great internship experience for me. The ARL organization I worked with also provided many supportive resources in helping me to understand the area and how to make the most of my time while here. For instance, learning about the location and how to stay safe from bugs, plants, and unexploded ordinances. Additionally, they provided many resources and points of contact when interns had an issue or concern.

Furthermore, into the overview of my internship experience, I was tasked with working on three main projects. The first involved a package that utilized Robotic Operating Systems (ROS) version 1 & 2 software for ground and aerial unmanned systems. The second consisted of utilizing the Defense Information System Agency (DISA) tools to harden and secure multiple information systems. The third project involved me collaborating with local Maryland public

schools to introduce and demonstrate firsthand experiences of various cybersecurity topics to high school students. Each of these projects presented a new perspective and understanding of incorporating various cybersecurity aspects into practical and systematic situations.

Management Environment

My management environment during the internship consisted of multiple points of contact with many being more specific to the Viceroy program and others being specific to the ARL organization. My main POC for the Viceroy program is a very accommodating woman that works to make sure we are taken care of along with enjoying the internship program and achieving what we hoped to gain from it. I would meet with her every week and present an update of how my internship is going and clarify any plans and schedules for Viceroy related events and activities. The ARL organization called for me to work jointly with multiple supervisors/mentors that all focus on different purposes and projects but still meet the goal of helping me to learn and gain more experience. The main mentor I have reported to and worked with the most during my time was highly effective in helping me to fulfill various plans and help me to understand topics related to our projects and the field in which he specializes in. During my time, I would regularly report to him about any questions, updates, and scheduling as he presented to be the main POC and frontrunner for gathering any information needed for our projects and events. My additional mentors also provided much help to me in clarifying any project issues and keeping up to date with our project progression day by day through routine meetings. Overall, my mentors and POCs provided me a reliable source of contact when questions, concerns, or issues arose during my internship time and have provided me with insights and experiences that will help me advance my career.

Projects Duties

To better understand how I have gained a distinct perspective on various cybersecurity aspects, a breakdown of each project and how they have helped me will provide more insight into each of them. Due to operational security however, various projects will not include distinct details about them to protect their confidentiality until they are released to the public. One respective case of this was my first project involving many confidential pieces that cannot be released to the public yet. The project involved using ROS which is an open-source software framework containing libraries and tools to help build and reuse robotics applications (Open Robotics, n.d.). Specifically, we used ROS versions 1&2 to build and restructure the information used for the purpose of the mission. The ROS 1 software libraries were originally used with an unmanned ground vehicle and was taken to be restructured into ROS2 compatibility to perform on unmanned aerial systems. In order to do this, an understanding of how ROS 1 works along with a deeper understanding of the specific parts of ROS 1 that we are using for the project is needed. Then an understanding of the difference between ROS 1&2 is needed in order to properly migrate code from version 1 to version 2. Lastly, an understanding of how the newly

restructured code works with the additional pieces added to the code to fit the functionalities needed for the unmanned aerial systems. These various aspects helped me build my coding skills by more specifically helping me to learn how to figure-out various difficulties in understanding and running Linux systems and Python code. My skills with Linux systems have developed considerably after working on the project as I've become more comfortable working and operating different aspects of Linux in addition to learning more useful commands to help me navigate and function the system easier. Additionally, my Python coding skills have increased after working on the project as I have learned more about how the coding language works along with how to resolve various problems. Overall, the project has helped me to learn many coding aspects and become more comfortable using Linux systems which will become a beneficial skill to transfer in more cybersecurity focused aspects.

My second project contains more publicly open information with the Department of Defense and the use of their various security hardening tools. DISA is sector of the DoD that works to provide, operate, and assure command, control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders and other mission and coalition partners across the full spectrum of military operations (Department of Defense, n.d.). DISA utilizes various tools to achieve their goals such as Security Technical Implementation Guides (STIG) and Security Content Automation Protocols (SCAP) which were highly focused on in our second project. STIGs are configuration standards developed by DISA to make device hardware and software as secure as possible to safeguard the DoD IT network and related systems. STIG configurations are leveled into three categories of security compliance from settings at most risk (1), vulnerabilities that have the potential to be a cybersecurity issue (2), and settings that may lower defenses if left unchecked (3) (TITANIA, n.d.). In addition to the security provided by STIGs, DISA also uses SCAPs to further enhance the security of their systems. SCAPs are a method for using specific standards to help organizations automate vulnerability management and policy compliance evaluations (Sager, 2019). These along with a facet of other security tools used by DISA help the DoD in over $8 million of cost avoidance through security threats and save over 1,500 hours in man labor (NSWC Crane Corporate Communications, 2019).

These two specific tools were used in conjunction with my first project to harden and secure the Windows and Linux information systems used to develop the first project. In order to measure the level of security compliance, we used Evaluate-STIG (EVAL-STIG) scripts in Window's PowerShell and Linux Terminal to scan the systems and return a report of the level of security compliance in an individual category. We also used security answer-files to help meet these compliances in the case of a scan error or non-compliance issue. By implementing these security tools on the information systems used to accomplish the first project, the goal of fulfilling the main purpose of the first project while combining security and control tools can be attained.

My third project consisted of participating in a week-long, summer Gains in the Education of Mathematics and Science (GEMS) camp experience that introduces direct cybersecurity topics to local high schoolers in Maryland Public Schools. It is a US Army

sponsored summer enrichment program designed to expose science, technology, engineering, and mathematics (STEM) subjects and careers (Army Educational Outreach Program, 2024). My role includes learning and designing the lesson-plan and tools that will be used during the camp, restructuring any lesson pieces so the students can have a better experience learning cybersecurity topics, and to teach them in-person to help them understand assorted topics studied during the camp. Some core pieces of the plan include directly teaching the students about specific cybersecurity skills and tools, using test environments to give them an opportunity to develop their own understanding of cyber-related tools, and to gauge their understanding of cybersecurity before and after the program. Other concepts include learning about network threats, human factors of security threats, and the law and ethics related to cybersecurity. The goal is to help garner more interest into the cyberworld as there is an increasing number of jobs becoming available within the industry resulting in increased opportunities for careers given to people interested.

Additional Experiences

Along with my projects, I had the opportunity to participate in an internship collaboration. The collaboration opportunity was with a contracting group for the DoD that develops 3D models and simulations for various government needs. I was able to help in research efforts needed for the group and observe a team operation setting and learn how various roles come together and communicate to achieve a goal.

What's more, I was able to experience several events designed for interns similar to myself. One of these events was a tour of the Pentagon from Chester Maciag, the director of Cyber Technologies and Academic Outreach. Due to the vast size and needed clearances of the Pentagon, we were only able to explore particular parts, but I was able to gain a deeper understanding of the parts we could explore. I also had the opportunity to tour the Army Research Laboratory in both Adelphi and APG, MD. These tours helped me to acquire further understanding of the types of work these specific Army locations do and what they are looking to build upon in their future projects. Lastly, I was able to attend a tour of the cybersecurity division at Abeerdeen Proving Ground. The tour consisted of interacting and shadowing a software developer on the base to understand the roles and tasks of a cyber developer within the army. My additional experiences helped me to further expand upon developing a career path within cybersecurity and gain a broader perspective of the numerous technical careers and how they could relate to cybersecurity.

Skills & Knowledge

Throughout my internship, I had fewer chances to use my cybersecurity skills and knowledge than expected, however, I did still have the opportunity to express and build upon my skills when the opportunity came. Before my internship, I had more knowledge than experience within the cybersecurity field after having completed many classes related to cybersecurity and

achieving my CompTIA Security+ certification and AWS cloud practitioner certification. However, even with the many pieces of knowledge, I had not had the opportunity to make practical use of what I know and in a “real-world” environment. During the internship, I was able to build on particular pieces that are beneficial to my cyber career such as learning and operating multiple operating systems, learning to understand Python, develop an understanding of how cybersecurity can relate to many things even if it is not the focus, and re-hashing my understanding of various cybersecurity concepts and tools through teaching them. My on-the-job experience has helped me to understand how cybersecurity can be related to everything even if it is not the main focus due to practicing and analyzing various project situations and how cybersecurity can be used to benefit it.

ODU Preparedness

The ODU curriculum did prepare me for specific parts while also not preparing me for various other parts of the internship mostly due to the varying focuses of the internship and the skills of knowledge needed for each one. For instance, many of the beginner Linux and Python courses required helped me to navigate and be user friendly to applications making it easier to continue building upon what I know. However, the levels of coding expertise and pieces of mathematical knowledge of various aspects related to the projects are more centered toward computer science development rather than cybersecurity. This aspect is more related to the focuses of the internship rather than the readiness of ODU has provided me. For example, when developing a learning plan and skills related to cybersecurity for the GEMS camp, many aspects of my cyber knowledge was used and could be demonstrated to help younger students gain an understanding into cybersecurity. This project helped me immensely to reinforce various cyber aspects I have learned at ODU through relearning and teaching these concepts. In relation to cybersecurity, I would not be able to describe any new cyber concept or techniques that I have not already been exposed to at ODU from this internship.

Fulfillments

As stated previously, Griffiss Institute describes their objectives and what they hope to achieve with this program. Their first objective of developing early student interest in challenging DoD and national security problem sets was met but not as entirely as I would have hoped. I did have the opportunity to experience and practice implementing a couple of aspects of DoD security that did help my development in understanding its importance and tour various facilities to understand varying technical roles. However, I would have liked to experience more cybersecurity focused activities and get a deeper understanding of its impact compared to the intake of various other technical perspectives that are not a focus in my career path. Their next objective of enhancing the pipeline of cyber and electromagnetic spectrum students at the secondary school level does not directly apply to me. However, from my firsthand accounts, the Viceroy program is helping to enhance this pipeline to secondary school students through the

opportunities they are providing. Their third objective is to increase the number of cyber and EMS instructors at the secondary and collegiate levels. This is achieved through the ranging opportunities the program provides and the abundant locations to which they are expanding.

Furthermore, their fourth objective of honing student competencies in leadership, teamwork, and oral and written communications is achieved in my experience due to the many situations and opportunities to practice and improve my leadership, communication, and teamwork skills. To expand further, when trying to complete security and coding objectives, I would readily communicate with my other colleagues and mentors to understand and achieve the goal. Their fifth objective of reducing student financial barriers to increase retention and enhance geographic mobility is greatly met by the program. I have been able to witness in myself and many other Maven scholars to have the ability to take part in the opportunity due to Viceroy's ability to break down these barriers. The last main objective listed is to provide an exciting internship experience hosted by engaging and supportive mentors, leading to permanent employment with the DoD. This goal is met as it provided me an opportunity to learn from many different perspectives that can all have an aspect to help me in developing my cyber career. For example, in one of my main projects I had the opportunity to further develop my Linux skills that I will be able to transfer into my cyber career.

My personal goals for the program were less accomplished compared to the outlined goals of the Viceroy program. My goal of developing a core cybersecurity skill was not met as much as I would have hoped for. Many of my other colleagues were able to take part in projects more closely related to their career path such as developing a deeper understanding of machine learning and artificial intelligence which will directly affect cybersecurity. I more actively worked on projects that helped to develop softer skills of Linux and Python coding without directly using it for something that affects cybersecurity. Along with this, I was not able to meet as many people related to cybersecurity and gain more knowledgeable perspectives. Many of my colleagues taking part of the Viceroy program were split up and only brought together a few times during the entire time of the internship which hindered us from really developing a connection for the future. Additionally, many of the associates around me in any varying facility were not also developing a career in cybersecurity making it difficult achieve this goal through the program. In all, many of the objectives outlined by Griffiss Institute were more able to be achieved however, the goals I had developed and placed more emphasis on were not as successful.

Motivations, Discouragements, & Challenges

One of the most motivating aspects of the internship would be designing, planning, and teaching the GEMs camp cybersecurity topics. This experience has provided me the opportunity to re-learn familiar cybersecurity concepts and use fun practice tools and virtual environments to teach and inspire several topics to high school students. The opportunity to push and give kids that were in a similar position as me a potential understanding what they would have an interest in doing in their future was exciting to be a part of.

The most discouraging aspect of the internship was the lack of cybersecurity experience that I was expecting to have. Many of the particular skills that I have worked on during my time can be transferred to help develop my cyber career, however, I would have liked to participate in more cybersecurity focused activities that would've more directly help build my skills for the future.

My most challenging aspect during the internship was building and refining the ROS 1 & 2 code throughout the internship. Learning how the Linux system commands worked in relation to the code along with understanding Python code with my little experience was difficult for me. However, I was comfortable asking questions and asking for help to understand what to look and how to execute the goal.

Future Recommendations

My recommendation for future interns participating in the program and to have a valuable experience would be to come into the opportunity with an open-mind. Though I may have not gotten to fully meet my goals for learning more direct cybersecurity related tools and experiences, I had the opportunity to participate and experience many different fields within the DoD that could have sparked an interest into the field. Many people I have met during my time came into the internship from various backgrounds not fully related to cybersecurity but had the opportunity to learn more than just cybersecurity and potentially develop a passion for something else. Additionally, I'd also recommend that interns take the opportunity as a learning opportunity not just in the aspect of what they're doing currently but in how they are handling various situations, what they want for themselves in their future careers, and what they can do to build better skills and connections to achieve the goals they want in their career future. This experience helped me to reflect on each of these aspects and develop how I can improve myself and what I want for myself in my future career.

Conclusion

To summarize my internship experience, I was given an opportunity to acquire knowledge and develop various skills that can help me to further develop my soft cyber related skills. Coming into the internship, I was anticipating to further develop core skills related to cybersecurity and gain more knowledgeable perspectives and connections, however I was not able to fully meet these expectations as I had hoped. Though these expectations were not fully met, I was able to learn and experience several technical fields and gain a better understanding of how cybersecurity can be used in relation to these fields. Additionally, it helped me to understand what I want to achieve within my career and develop a track to achieve these goals.

My internship experience will influence the remainder of my college career in varying aspects. For instance, the types of cybersecurity of classes I take will be re-evaluated to understand its relation to my career-path goals. Furthermore, I will work to gain more insight

from my cyber-instructors and search for a mentor within the field to help me understand more about how to progress and succeed.

Lastly, my experience will impact my future professional career in many beneficial ways. As stated previously, it helped me to evaluate my career goals and the path to achieve this by asking professionals within my field questions on how to further succeed in my cybersecurity endeavors. In addition to this, I have gained more insight into choosing and developing my experiences and how to improve them by asking more questions in relation to the job tasks and how they align with what I am trying to achieve.

To conclude, my experience with the Griffiss Institute Viceroy Maven program has presented me with an amazing learning experience for developing my cyber career. This experience has brought me irreplaceable lessons that will only help me further develop my career goals and help me improve as a better career individual.

References

Army Educational Outreach Program. (2024, May 3). *Gems Adelphi*. Retrieved from AEOP Army Educational Outreach Program: https://www.usaeop.com/program/adelphi/

Department of Defense. (n.d.). *About DISA*. Retrieved July 20, 2024, from DISA Defense Information Systems Agency: https://www.disa.mil/About

Griffiss Institute. (2024, May 21). *Vicerory Powered by Griffiss Institute*. Retrieved July 14, 2024, from Viceroy Scholars: https://www.viceroyscholars.org/

Grinkewitz, J. (2022, April 15). *ODU Awarded $400,000 to Grow Diverse Cybersecurity Workforce Pipeline*. Retrieved from Old Dominion Univerisity : https://www.odu.edu/article/odu-awarded-400000-to-grow-diverse-cybersecurity-workforce-pipeline

NSWC Crane Corporate Communications. (2019, August 28). *NSWC Crane employee develops software tool to increase cybersecurity, cost avoidance over $8 million*. Retrieved from NAVSEA Naval Sea Systems Command: https://www.navsea.navy.mil/Media/News/Article/1946720/nswc-crane-employee-develops-software-tool-to-increase-cybersecurity-cost-avoid/

Open Robotics. (n.d.). *ROS - Robot Operating System*. Retrieved July 4, 2024, from ROS: https://www.ros.org/

Sager, T. (2019, September 18). *Secure Configurations and the Power of SCAP*. Retrieved from CIS Center for Internet Security: https://www.cisecurity.org/insights/blog/secure-configurations-and-the-power-of-scap

TITANIA. (n.d.). *DISA STIG compliance explained*. Retrieved 2024, from TITANIA: https://www.titania.com/resources/guides/disa-stig-compliance-explained