Final Paper

Hector Gomez
Old Dominion University
4/16/2024
CYSE 368
Sterile Geeks VR
Spring 2024

Table of contents:

At the beginning of this year, I was blessed with an incredible opportunity to gain an internship within my specific field of interest, cybersecurity. I had been searching for an internship for a few years, ever since I first became interested in the major of cybersecurity. However, I was having a difficult time finding an internship that was a good fit for me. So, when I was finally presented with the opportunity to take on an internship, I jumped at the chance without hesitation. I decided to do this internship with Sterile Geeks VR, primarily because the brothers of my organization led me to meet one of the workers of the company, who was also a part of my organization. It was an instant click between us, which was a huge plus for me. Additionally, when he was covering what we would be doing during the internship, I found it to be very interesting and similar to what I was looking for in an internship. Once I received the internship, I was very excited for a few reasons. Firstly, I wanted to extend my knowledge of what I had already learned from my major in cybersecurity. Secondly, I wanted to see how much I knew and how I could incorporate my knowledge into this internship. Lastly, I wanted to gain experience in what I could be doing once I graduated. This was particularly important to me as I was coming up on graduation, and I wanted to be as prepared as possible to succeed in my chosen field. I have always wanted to be a cybersecurity professional, and I believe that everything I have done in school for the past six years has been in service of that goal. I never wanted to go a different route or not pursue higher education. Receiving this internship and completing it for something that I love, which is cybersecurity, is one of my long-term goals. This internship has been an incredible learning experience for me, and I am grateful for the opportunity to have taken it on. Throughout this paper, I will detail everything that I have done and learned through creating a VR headset system. I started by creating a technical blueprint and finished off by starting to create firewalls for security measures within a VR headset. As part of my internship, I was tasked with creating a PowerPoint presentation that provided a detailed overview of the security system for a VR headset. The presentation had to be informative and concise, while also taking into account the technical nature of the device and the complexity of its security requirements. Over several months, my co-interns and I worked tirelessly to ensure that we had all the necessary information and details required to create a robust security system for the VR headset. We knew that any mistakes or oversights could have serious consequences, so we approached the task with the utmost care

and attention to detail. To ensure that we were on track, we had weekly meetings where we presented our progress to our boss. The security portion of our presentation was particularly challenging, as it required us to delve into the minutiae of the VR headset's security requirements. We had to consider everything from firewalls to protective measures, and we had to ensure that our presentation covered all the necessary information clearly and concisely. In the end, we were able to create a 20-page document that provided a comprehensive overview of the security system for the VR headset. We were proud of our work, and we knew that it would help ensure that the device was safe and operating efficiently.

I am interning for Sterile Geeks VR which is a company based in Jacksonville, Florida. Sterile Geeks VR is a MedTech startup based in Jacksonville, Florida that specializes in providing software development solutions for the healthcare industry. The company was originally founded in 2017 as a virtual reality healthcare software design firm, but in May 2018, Sterile Geeks VR pivoted its focus solely towards Augmented Reality (AR) based solutions to cater to the needs of a wider range of industries within the healthcare sector. With over 50 years of combined experience, Sterile Geeks VR is committed to delivering long-term solutions that prioritize the needs of its clients. The company's mantra is to prioritize trust by avoiding shortcuts or seeking out quick profit opportunities. As a service-disabled veteran-owned company, Sterile Geeks VR is dedicated to being a reliable solutions provider that supports the completion of the mission, regardless of size. The company primarily serves the healthcare and IT/Cybersecurity sectors, providing a range of services such as XR software development and management, healthcare education and training consulting, project-based custom development, and cloud software security solutions. Sterile Geeks VR's extensive industry knowledge and processes enable it to provide seamless contract performance for its clients. It's worth noting that Sterile Geeks VR CEO, Scotty Jones, was one of 241 veteran entrepreneurs globally to be selected to attend the first cohort of 2022. A partnership of WeWork and Bunker Labs, Veterans in Residence is a six-month business incubator that provides veteran and military family member entrepreneurs with a community of peers, business support, and workspace. Overall, Sterile Geeks VR is a reputable and reliable partner for healthcare organizations looking for innovative solutions to improve their operations. The

company's dedication to its clients and its commitment to excellence make it a standout player in the healthcare software development space.

Upon receiving notification about the available internship position, I immediately contacted the CEO and another worker at the company. I expressed my interest in applying for the internship and my willingness to offer my services in the cybersecurity department. I sent out an email to both of them and received a prompt response, which was not only engaging but also very encouraging. They expressed their excitement and interest in having me on board, which gave me a lot of confidence in taking the next step. As I had no prior experience in this field, I was upfront about it while communicating with them. However, they were very supportive and told me that I would only need to do a lot of research to keep up with my co-interns. This was a huge relief for me as I knew that I could put in the effort required to learn and grow in this field. Before starting the internship, I took the time to research the company and visited its website to understand its mission and vision. I also kept in touch with the manager and asked for guidance on how to be successful throughout the internship process. This helped me to prepare myself better for the upcoming tasks. As the start date for the internship drew closer, we received more information about the project and the tasks we were required to complete. We were tasked with creating a technical blueprint for a VR headset, which was a challenging yet exciting task. I was determined to put in my best effort and learn as much as I could during my time at the company. Before commencing the internship, all the interns were required to attend a virtual meeting on Zoom to discuss the details of the program, including the nature of the work that we would be doing and how the internship would be conducted. As I reside in Virginia, it was made clear that the entirety of the internship would be conducted online. During the interview process, our manager emphasized that each intern should dedicate at least two hours per day to working on the technical blueprint. Additionally, he informed us that we would be meeting every Saturday via Zoom to discuss our progress and review what we had accomplished during the week. This was incredibly motivating for me, as it demonstrated that the company was invested in our success and was committed to ensuring that we were on the right track. Overall, my initial impressions of the internship left me feeling enthusiastic and eager to begin working for this esteemed organization.

The management environment during my internship was truly remarkable. I must admit that I was a bit apprehensive before starting the program, as I had expected to receive a lot of hand-holding and oversight. After all, we were tasked with performing important work that would greatly benefit healthcare workers. However, during our initial meeting, the manager made it clear that they would not be coddling us or holding our hands throughout the process. At first, this made me a bit nervous, as I had no prior experience in the field. But at the same time, I was also excited because I knew that if I was going to learn and grow, I would need to do so independently. Throughout the internship, we were given a great deal of autonomy. We were expected to work independently and manage our projects and timelines. Of course, if we had questions or needed guidance, the managers were always available to help us out. But they never did the work for us or held our hands every step of the way. This approach helped me to develop my skills and feel more confident in my abilities. I knew that I was being prepared for the real world, where I would be expected to perform tasks on my own without a lot of hand-holding. Looking back on the experience, I can confidently say that this was one of the most professional and insightful internships I have ever experienced. I learned quickly and was able to complete my tasks with ease, thanks to the skills I developed during the program. I know that I will carry these skills with me as I move forward in my career, and I am grateful for the opportunity to have learned so much during my time with this organization.

As part of our assignment, we were tasked with creating a comprehensive technical blueprint for a security system that would be implemented in a mixed-reality environment. Our primary goal was to ensure that the CIA Triad principles, which include Confidentiality, Integrity, and Availability, were being upheld at all times. This was essential to keep everything safe and secure while accessing highly sensitive data such as patient information or personal identifiers. We also emphasized the importance of cybersecurity and user engagement when interacting with VR headsets. To develop the technical blueprint, we started by identifying and creating a detailed plan for various sections that would go into our role. These sections included Privacy and Data Security, Technical Skills and Tools, Specifics of Authentication Options, VR/MR Specifics/Features, and more. We

understood that the success of the assignment would depend on how detailed we were in each of these sections. To ensure that we were covering all bases, we conducted extensive research on User interface, Accessibility, Risk Management and Assessment, Incident response plan, and other critical areas. We discovered that while the details could vary depending on the security of the system, they were all equally important in helping us develop a more secure system. Some of the essential details we discovered include the importance of making the application user-friendly to provide ease of access while maintaining a strong sense of security. We also ensured that within the system settings, there would be dedicated accessibility options for users to customize their experience to their liking. We also followed a rigorous process that involved Risk Identification, Risk Analysis, Risk Prioritization, Risk Mitigation Strategies, Implementation and Testing, and Monitoring/Reviewing after the risk has been dealt with. We understood that this process was critical to identifying potential risks and developing effective strategies to mitigate them. Finally, we created an Incident Identification plan that emphasized the need to identify any security-related incidents through various methods such as security monitoring, user reports, and system alerts. This plan would enable us to respond quickly and effectively to any security incidents and minimize the impact on the system and its users. Overall, our technical blueprint is detailed and comprehensive, covering all the critical areas necessary to develop a secure security system for a mixed reality environment. As we move forward with our security process, we are being more specific in our approach to ensure that the system is secure. With every passing day, the technical blueprint is getting longer, and we are beginning to visualize how the system will look once it's fully operational. In our latest update, we have added a few more sections to the blueprint, including Emergency Shutdown Procedure, User Content and Data Ownership, and Headset Startup/First-time User Experience. Regarding the Emergency Shutdown Procedure, we have implemented User Alerting in the form of on-screen notifications. This means that whenever an emergency shutdown is imminent, users will be prompted with a notification on their screen, alerting them of the shutdown. Additionally, we have incorporated User Guidance, which will guide users on how to properly shut down the headset to save their progress. Users will also be kept informed of when the servers will be back up, so they know when they can resume their work. When it comes to User Authentication for VR

headsets, we have employed various methods, such as passwords, PINs, biometric authentication (e.g., fingerprint or facial recognition), or even more advanced methods like iris scanning. This ensures that only authorized users can access the device and its content, making it more secure. Furthermore, we require users to provide their Username, Email, and Password. This information will be kept protected and inaccessible to others, ensuring the safety of the system. Additionally, when users first use the system, they will be greeted with a user-friendly mixed-reality screen, making it easy for them to navigate through the system. As we continue to work on the technical blueprint, we are also focused on presenting the information clearly and concisely. Therefore, we have added more details regarding the system security for the VR headset, ensuring that users are aware of the measures put in place to secure their content and data. The security of sensitive user data stored on VR headsets or transmitted between the headset and connected devices is of utmost importance. Encryption is a fundamental aspect of safeguarding user data, and encryption algorithms such as AES (Advanced Encryption Standard) may be used to secure data, including user profiles, payment information, and communication with external servers. Another critical aspect of ensuring the security of VR headsets is implementing secure boots to ensure that only trusted software components are loaded during the boot process. This helps prevent unauthorized or malicious software from running on the device, thereby protecting the integrity of the VR headset's operating system and firmware. During a recent internship, our team was tasked with building three firewalls for different cases within the VR headset. Though we had no previous experience in building firewalls or incorporating them into VR headsets, we eventually found some information and used Python to try some coding that we found online to see how it would work. After running the code successfully, we realized that we were stuck on how to incorporate it and what to do with it. However, our manager provided us with some valuable insights on how to implement the firewalls, and we gained a better understanding of the process. As we continued our research, we found that there are several options for implementing firewalls for VR headsets, including network traffic filtering, access control, and intrusion detection and prevention. Though this part of the internship was initially challenging, we have gained more information regarding firewalls and how to incorporate them into VR headsets. The implementation of network traffic filtering is a crucial aspect of maintaining the

security and integrity of any network. This process is typically carried out through the use of devices such as firewalls and routers, which are responsible for governing the flow of data within the network. The primary function of these devices is to block any unauthorized access attempts and prevent malicious data from entering or leaving the network. To achieve this, access control lists (ACLs) or filters are used to manage internet traffic and ensure that only authorized users can access the network. This level of access control provides an additional layer of protection, as the network can be effectively sealed off from unwanted access or configured to allow only limited access to specific servers or applications. Intrusion detection and prevention are two broad terms that describe application security practices used to mitigate attacks and block new threats. These practices are critical in preventing unauthorized access to sensitive information and ensuring that any potential security breaches are detected and addressed promptly. When it comes to creating a VR headset that is safe and secure for use by healthcare professionals, it is essential to incorporate these security measures into the design and development process. The VR headset will be used to store and transmit sensitive patient data, so all data must be kept confidential and secure. Our team of interns worked tirelessly to ensure that the VR headset was designed with the highest level of security in mind. We followed the best practices for network traffic filtering and access control and implemented intrusion detection and prevention mechanisms to ensure that any potential security threats were addressed proactively. Ultimately, a secure VR headset is vital for healthcare professionals as it ensures that their patient data remains confidential and secure. Our team is proud to have contributed to this important project and to have helped create a VR headset that is both safe and viable for use in the healthcare industry.

Before starting this internship, my knowledge and skills in the field of cybersecurity were limited. However, I was able to secure the internship based on my strong personal qualities and background knowledge from previous classes that I had taken. As I began the internship, I realized that attention to detail and carefulness were crucial aspects of the job. Given the sensitive nature of the information that we were working with, it became clear that even the smallest detail could make a significant difference in the overall outcome. Through this internship, I have been able to develop a comprehensive understanding of the

importance of these little details and how they can have a major impact on cybersecurity. As a result, my focus and approach towards cybersecurity have shifted, and I am now more detail-oriented and meticulous in my work.

During my VR headset project, I realized that my knowledge of the subject was broad but not detailed enough to tackle the project effectively. However, as the internship progressed, I was able to delve deep into the technicalities of the project and gain a more in-depth knowledge of my major. I must admit that my basic understanding of cybersecurity was limited before the internship, but the experience helped me go beyond the surface and understand the concepts on a more profound level. I was able to explore the details and technicalities of cybersecurity, which helped me develop a more comprehensive understanding of the subject matter. Overall, the internship was a great learning experience that helped me broaden my horizons and gain valuable knowledge on cybersecurity.

The internship fulfilled every outcome that I set in my introduction. I was able to expand my knowledge within things I already learned through my major. I applied the things I already knew to the internship which allowed me to be successful during my internship. My third outcome was a goal I set for the future and I would say it was fulfilled because now I know how to do something that I didn't before and I can apply it to my next career if needed. The most exciting part of the internship was when we finished the PowerPoint and technical blueprint because it was very thrilling to know something was accomplished and it was correct. I would the most discouraging part of the internship was when we started the firewalls and we were very lost on how to do it. The most challenging part refers back to the creation of firewalls because it was something that dealt with coding and none of us had experience with it. The main preparation that I would give to someone looking to be an intern is just to be confident with what you already know and apply it the best way you can. If you can do that then you will have a great outcome with the internship and possibly a job after you graduate.

In conclusion, I received an internship opportunity in cybersecurity with Sterile Geeks VR. I was very excited about the opportunity to learn more about cybersecurity and gain experience in the cybersecurity field. As part of the internship, we were tasked with creating a security system for a VR headset. I worked a ton of hours with my co-interns to ensure that we had all the necessary information and details required to create a robust security system. We presented our progress to our boss weekly and were able to create a 20-page document that provided a comprehensive overview of the security system for the VR headset. This internship has given me everything I needed to feel more confident for the future, especially for my future career. I feel as though I am prepared enough now to be successful in my future.