Innovation to the Future of Cyberwarfare

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Huy Huynh

Spring, 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, Department of Computer Science

Innovation to the Future of Cyberwarfare

CS4991 Capstone Report, 2022

Huy Huynh
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
hth5cf@virginia.edu

ABSTRACT

Cyberspace is a complex environment without an adequate means for envisioning it. With the increasing rates of cyberattacks and cyberwarfare, a method of planning is needed to defend against attacks. This is the main goal of Project IKE, a tool for visualizing cyberspace. Attacks and defenses can be mapped out digitally through this software; then artificial intelligence can be used to advise users how to go about an attack.

I interned at Two Six Technologies in the summer of 2021 and helped the company work on Project IKE, a tool to visualize cyberspace. I worked with the CORE team on the backend of Project IKE, making valuable contributions to the project with the help of a senior developer. Project IKE is still being updated and potential changes, such as a stronger implementation of artificial intelligence and better graphic user interface could make it even better.

1. INTRODUCTION

The rate of cyberattacks have been increasing during the last decade. They began as small attacks on individuals and transformed into more large-scale attacks on big organizations. The first large-scale ransomware attack was called the WannaCry attack, took place on May 17th, 2017. It targeted old Windows computers and stole their data for ransom (Gregory, 2021). More recent and larger scale cyberattack was the ransomware attack on the Colonial Pipeline, the largest American oil pipeline system, on May 7th, 2021. This attack halted the distribution of gas and led to higher gas prices and gas outages around the United States. In addition, Colonial paid the ransomware of $4.4 million in bitcoin, which can further incentivize even more large scale attacks (Turton, 2021).

Later the same month on May 30th, 2021, another large scale ransomware attack on JBS Foods, a worldwide meat producer, occurred. This stopped the slaughterhouse operations around the world and led to JBS Foods paying the ransomware of $11 million in bitcoin (Nair, 2021).

With cyberwarfare growing at an alarming rate, actions have to be taken in order to fight against these attacks. Since cybersecurity is still an underdeveloped idea, there are not many surefire solutions that can truly protect or at least mitigate these cyberattacks.

2. RELATED WORKS

There has been apathy for the topic of cybersecurity from the government in the past. Some mitigation procedures were attempted, but all seemed to fail. Congressional reports were used to voice concern about potential deficiencies in their cybersecurity and to prompt further action to fix those issues. In a 2019 Congressional report on the US Federal Government, the Committee on Homeland Security and Governmental Affairs investigated eight agencies within the government and found a long list of vulnerabilities. In many cases, the agencies even lacked government certification that their systems were in proper working order (Senate, 2019). It was recommended that these agencies check their systems and fix the listed vulnerabilities. However, two years later, the Committee on Homeland Security and

Government Affairs investigated the same eight agencies and they identified many of the same issues they found (Senate, 2021).

From these studies, it is clear that the US government has a lack of care for the cybersecurity of their systems. On May 12, 2021, President Joe Biden issued an executive order to improve the nation's cybersecurity. The executive order aimed at modernizing cybersecurity defenses in the country by having open channels for sharing information on cybersecurity and enforcing cybersecurity requirements on organizations to prevent further damages.

Federal agencies are also expected to modernize their technology environment and security practices (The United States Government, 2021). The executive order also called for updating authentication and encryption frequently and executing planned timelines for implementing and monitoring each federal agency and its technology environment (The United States Government, 2021). Because this executive order was so recent, it is hard to tell if it even had any substantial impact because the JBS Foods attack took place 18 days after. Even so, these methods were very indirect in solving the situation of cyberattacks.

This is where Project IKE can play a key role, since it is a very direct method of dealing with these attackers. Its visualization allows people to see what is happening directly and it can track down the origin of the attack, potentially stopping those attacks for good.

3. SYSTEM DESIGN

The purpose of Project IKE is to be able to visualize cyberspace. The application can be launched onto a browser and accessed through there. It consists of a user interface with many options including ways to create cyber missions and find specific information through their database. I was with the CORE team and we mainly worked on the backend functions of IKE. During my internship, I helped complete three tasks with Project IKE: 1) upgrade the whole project from Java 8 to Java 11; 2) created a custom flag when using Exodus, an extensible database project; and 3) implemented an API rate limiter using Flask.

In order to upgrade from Java 8 to Java 11, almost everything in the program itself needed to be updated and modified, from the XML files to Dockerfiles. My senior developer helped guide me through the upgrading process, as it would optimize the system better and allow for more feature implementation. First, a custom JDK 11 runtime was created and uploaded to the online server, where the program can call and run. A custom runtime was made to save storage, since the full runtime had extra functions that were not used within IKE. Since the XML and Dockerfiles were connected to the previous JDK 8 on the server, I had to change where they downloaded the runtime from to the new JDK 11 runtime on the server.

There were many errors when upgrading Luna and Maven, two other softwares involved in the upgrading process. My senior and I had to troubleshoot many of the errors and had to reinstall a different version of Maven in order to get it working with Java 11. When everything seemed to be building correctly with Java 11 and IKE launched properly onto the browser, the changes were pushed. Then another team that deals with the databases would have to upgrade their systems as well in order to fully upgrade the whole project to Java 11.

I worked with Exodus, a database software, and was given the task to create a custom flag. This custom flag when running a command will retrieve all the column information of a specific field in the table. This involved learning a library that implemented custom flags and being able to use an SQL query to obtain the column information from the database. In this library, I created a new function which was called whenever the custom flag was implemented. The function then connected to the database and ran an SQL query that obtained the column information needed from a specific field depending on the parameters of the command. The data was placed into a dictionary and was returned when it was called. When the Exodus command was run with the custom flag, the dictionary of the column information was shown in the console.

Lastly, an API rate limiter was implemented on the project. This rate limiter basically limits how many times someone can access the site. I implemented this through the Flask-limiter library. My senior had already started on creating a login system involving API tokens and my task was to be able to limit user access to the site. Within the Flask-limiter library, I created a limiter object and gave it a limit of once per day. After 1 accessed the site and tried to go back into it, it gave a 429, too many requests error, which showed that it was successfully implemented.

4. RESULTS

The changes to Project IKE helped optimize and start a new pathway for more features to be implemented into the IKE system. Project IKE greatly benefits from the Java 11 upgrade. Java 8, 9, and 10, will no longer be supported within the next couple of years, so it makes sense to move to Java 11 early to avoid the hassle of moving to it later. Java 11 also provides better performance and optimization, more security fixes, and allows for more use of third-party libraries, since modern ones require a more recent version of Java.

The custom flag added to retrieve column information from the database was also helpful to Project IKE. This change allows users to obtain column information without going to the database directly. This custom flag will make it easier for people to access information from a specific table through a parameter along with the custom flag.

With the implementation of the API rate limiter users are now limited to how many times they can access the site. This allows for more security to the site as it prevents malicious attacks from taking place and prevents suspicious activity of accessing the site more than a certain number of times. More control over the traffic of usage can be beneficial as well because if the system is accessed too many times at once, then performance on the system can suffer. This was mainly a prototype to a future API rate limiter and can be built upon further by specifying a specific limiting rate in the future.

5. CONCLUSION

Cyberwarfare is a problem that is growing at an exponential rate. The government has had a lack of successful actions to deal with the issue of cyberwarfare, and Project IKE can be an answer to that. With an AI to help guide how to approach a certain cyber battle and a visualization of cyberspace, this project has the potential to give a massive advantage in cyberwarfare. This project reveals the existing problem of cybersecurity and can solve it by directly dealing with the attackers through its visualization. As long as the development of this project continues, it can be a very powerful tool to use in the future.

6. FUTURE WORK

The project is currently developing to have a fully functioning AI that takes a question about the current state of warfare and returns an answer of the next steps based on the current data. Over time, the project could also be more optimized with its database searches and page redirects.

Since the government also plays a part in how they want the project to go, they might ask for more requirements as well, meaning the project will have to prioritize those requests as well. There is a lot of potential with this project since it is still new and in development, and hopefully it will be able to make a positive impact in the future.

REFERENCES

[1] Gregory, J. (2021, September 1). What has changed since the 2017 WannaCry ransomware attack? Security Intelligence. Retrieved October 4, 2021, from https://securityintelligence.com/articles/what-haschanged-since-wannacry-ransomware-attack/.

[2] Nair, A., & Reese, C. (2021, June 10). *Meatpacker JBS says it paid equivalent of $11 mln in Ransomware attack*. Reuters. Retrieved October 17, 2021, from

https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/. [3] Senate., Portman, R., & Carper, T., Federal Cybersecurity: America's DATA AT RISK: Staff report (2019). Committee on Homeland Security and Governmental Affairs.

[3] Senate., Portman, R., & Peters, G., Federal Cybersecurity: America's data still at risk: Staff report (2021). Committee on Homeland Security and Governmental Affairs.

[4] The United States Government. (2021, May 12). *Executive order on improving the nation's cybersecurity*. The White House. Retrieved October 17, 2021, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[5] Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg. Retrieved October 4, 2021, from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-usingcompromised-password.