Risks, threats, and vulnerabilities within virtual reality technology

Ng Zheng Yao[1], Intan Farahana Binti Kamsin[2], Zety Marlia Zainal Abidin[3], Hemalata Vasudavan[4]
[1'2'3'4] Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[1]tp055535@mail.apu.edu.my, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

***Abstract*— Virtual Reality (VR) technology is becoming more and more popular in society not only as entertainment but for commercial uses as well. This research proposal touches on the importance of the security within the virtual reality (VR) technology field. It proposes a system that will provide additional insight to the vulnerabilities of the VR system that they are currently using. The methodology that will be used to conduct this research is the qualitative research method, interviews. It will be used to gather the required information and data from the interviewees.**

***Index Terms*— Cyber Security, Virtual Reality, Virtual Reality based Learning Environment, Vulnerability**

1. Introduction

As time passes, more and more innovations and technological advancements are made by researchers all throughout the world. They can range from something as simple as a automatic paper shredder to something as advanced as a machine that aids in completing difficult surgeries. In recent years, virtual reality (VR) has been the hot topic in many industries due to its immense potential. Many might think that the concept of VR be implemented in the entertainment industry, but there is actually so much more that it can be used for such as educations by revolutionizing the way we teach, retail by allowing the shoppers to try out what the clothes will look like on themselves in the comfort of their home and many more. VR might potentially put humanity into the next era. This is why the security of said technology should be without a doubt safe and verified.

2. Literature Review

2.1 Research Domain

2.1.1 Vulnerabilities Pertaining to Cyber Security

According to Rastogi & Nygard, security vulnerabilities tend to be forgotten until very late into the development of a software, because they are not considered to be one of the top priorities of a software developer [4]. It is also stated that software developers focus more on preventive measures rather than detection of breaches.

Based on the research conducted by Ezenwoye et al., there are a total of seven fundamental software product types of a system that can contain vulnerabilities [5]. These product types are Web Application, Utility, Server, Operating System, Browser, Framework, and Middleware. Vulnerabilities found in systems will always stem from these seven product types. They have also found that vulnerabilities vary across different types of software.

In the research from Decan et al., vulnerabilities tend to take a long time to be fixed because identification of the vulnerability in of it itself will take a long time [6]. As shown in the figure (Figure 1) below, the vulnerabilities are only discovered months into the release of the packages. This is because younger packages have not been able to reach the majority of the user base, hence not warranting much security-related attention.

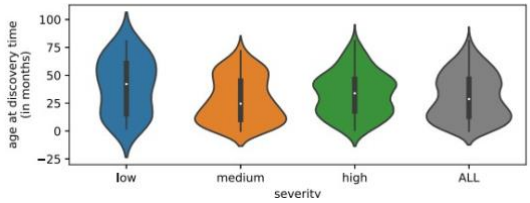

Figure 1Violine plots of package age at discovery time by vulnerability severity[6]

From the research conducted by Bhatt et al., discovering vulnerabilities is the topmost priority of software engineers [8]. It has stated that during the software development process, vulnerabilities may be accidentally implemented into the software. Later on, when these vulnerabilities are discovered, the software engineers will fix these vulnerabilities by doing minor tweaks to the source code of the software, known as patches.

After having read through all the various research, vulnerabilities are a common occurrence within all software. These vulnerabilities will be solved in due time when it is discovered. However, the discovery of these vulnerabilities tends to take a long time because software developers tend to focus on the prevention and mitigation of the vulnerabilities rather than focusing on the identification of these vulnerabilities.

2.1.2 Process of Identification of Vulnerabilities According to Votipka et al., there are 6 steps that will be used during the process of discovering vulnerabilities [7]. The first phase is information gathering where information is gathered to obtain an understanding of the program, the second phase is program understanding where the users will interact with the program to gain a better understanding of the program, the third phase is the attack surface phase where the points of manipulation and how the execution of the program can be influenced, the fourth phase is the exploration phase where a range of inputs is tested to see if the program can be exploited, the fifth phase is the vulnerability recognition phase where the first 4 phases is repeated until a vulnerability is found. In the case that a vulnerability is found, the user can move on to the final phase where they record the vulnerability into a report. The research has also stated that there are 4 external factors the vulnerability discovery experience, unverifying system knowledge, access to development process, and motivation as shown in the figure below (Figure 2).

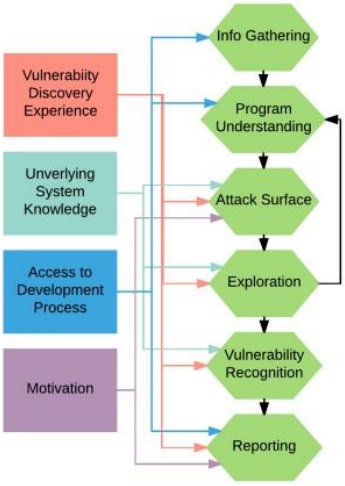

Figure 2 Vulnerability-finding process and influencing factors

Based on the research conducted by Bhatt et al., Vulnerability Discovery Models (VDMs) is one of the models used by software programmers to try to predict vulnerabilities within a software [8]. They function by quantifying trends in the vulnerability discovery process. There are two factors that impact the results provided by the model, the first factor is the number of installations of the software, and the second factor is the decreasing phenomenon of the number of undetected vulnerabilities with time. When plotted into a graph, this model tends to promote a discovery curve that is shaped like the letter "S". The result of the research shows that, VDMs shows great potential in aiding the software developer for further refinement of the software.

In the research from Croft et al., Software Vulnerability Prediction (SVP) is a process that helps decide the integrity of class modules with the use of data [9]. The data used by this process is previously recorded vulnerabilities within the software. With the use of this process, the development of future software can avoid the software vulnerabilities that has previously occurred. Data preparation is the most vital and difficult step within the entire process due to inconsistent factors such as natural infrequencies, inconsistent reporting, etc. According to the figure below, the four main steps of data preparation that determine the quality of the data prepared is the data requirement step, the data collection step, the data labelling step, and the data cleaning step.

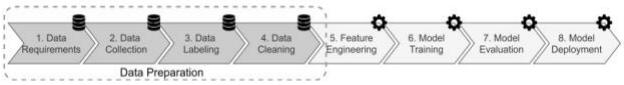

Figure 3Machine Learning Workflow [9]

From the research conducted by Ghaffarian & Shahriari, even though nature of the identification and analysis of vulnerabilities is unpredictable, professionals within the academic community and the software industry has studied and presented multiple approaches [10]. However, these approaches are inaccurate and can only provide an approximation. Example of these approaches are program analysis approaches, software penetration testing approaches, fuzz-testing approach, etc.

After having read through the various researches, the main factor that allows for the detection and prediction for vulnerabilities is previous records of vulnerabilities in different types of software itself. However, the preparation of the data itself is the most demanding task of all due to it directly affecting the overall results of the detection and prediction processes. This research will help in the creation of these databases allowing for high quality data preparation to be performed easily.

2.1.3 Security Within VR Technology

According to the results from the research conducted by Adams et al., although developers of VR software are aware of the privacy and security issues such as data collection or a breach of data of the users, however as of now nothing is done to try to solve these issues [11]. On the other hand, users expressed concern regarding the aforementioned issues especially if VR becomes more common in the future.

Based on the research conducted by Giaretta, VR as of now contains a lot of risks and threats that can be exploited by people with malicious intents [12]. There are a total three types of security threats that can affect VR technology, VR specific threats, generic threats and authentication threats. They have identified four VR specific attacks which tamper with the information provided to the user by the device. These attacks

are classified as Immersive Attacks. These attacks are targeted at changing what the user can see in hopes of trying to manipulate the physical action of the user. In terms of generic security threats that can affect VR technology, they have identified five threats, side-channel attacks, personal data leakage, denial-of-service, unauthorized access, and man-in the middle attack. As for the authentication security threats, they have identified three threats, hand-over-to unauthorized actor threat, brute force threat, and impersonation threat.

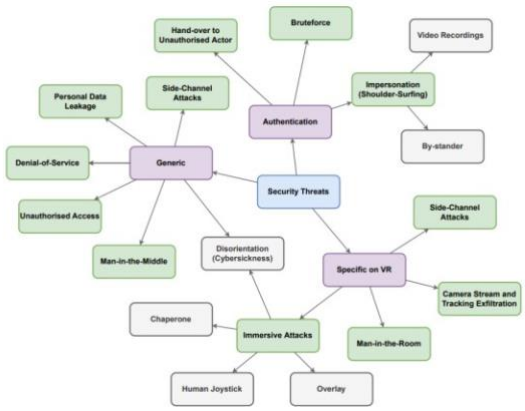

Figure 4 Security Issues in VR [12]

In the research from Gulhane, et al., Virtual Reality Learning Environment(VRLE) systems are mainly susceptible to three different types of threats, security threats, privacy threats, and safety threats [3].

After having read through all the various research, the security of VR systems leaves a lot to be desired. There is a lot of risks and threats that will compromise the integrity and performance of the VR system.

2.2 Similar Systems

2.2.1 Similar System 1- ManageEngine's EventLog Analyzer

ManageEngine's EventLog Analyzer is a software that is used to aid the user to manage event logs [14]. Depending on whether the system that it is installed on has local features used for log collection, there are two methods that it uses to collect logs, the agentless event log collection method, and the agent-based event log collection method. The agentless event log collection method is used when there are local features that allow for event log collection such as those of in Windows based devices. When this method is used, the software will work together with device to collect the event logs such as WMI, DCOM, and RPC. The agent-based event log collection method is used when there are no local features that can be used for log collection. The software comes with event log collecting agents. These agents are required to be installed on the system so that it may collect the log info and send it to the server. After collecting the event log data, the software has various functions that can be utilized to manage event log data such as event log analysis, filtering and parsing of event log data, etc. The event logs are automatically separated into different categories. These categories are as followed, the general event category, the security category, and the network category. The general event category contains event logs about general activities that are performed on a daily basis such as logins. The security category contains event logs pertaining to security events such as breaches. The network category contains event logs pertaining to the network such as frequently visited websites.

Figure 5 ManageEngine EventLog Analyzer logo

As shown in the figures (Figure 6, Figure 7, Figure 8)below, the interface of the software acts as the main hub. There are a total of 3 pages sections of the main page as indicated by the dots on top of the main page. The 3 sections are separated by the 3 aforementioned categories, the general event category, the network category, and the security category.
As shown in the figure(figure 6) below, the general events category main hub contains all the events that has happened, the devices that are connected to the eventlog analyzer. It also contains statistics that are related to events that have happened.

Figure 6 General events category Main Hub [14]

As shown in the figure(figure 7) below, the network events category main hub contains all the events that are related to network that has happened such as the number of attempted connections that has been denied and allowed. It also contains statistics that are related to the network such as the trends of the network traffic, what websites are frequently accessed and the changes of the interfaces of the device.

Figure 7 Network Category Main Hub [14]

As shown in the figure(figure 8) below, the security events category main hub contains all the events that are related to the cyber security of the devices such as the number of vulnerabilities detected, the number of treats detected, and the number of incidents that have happened. It also contains statistics regarding the network attacks that have been detected, any threats that have been recently identified, etc.

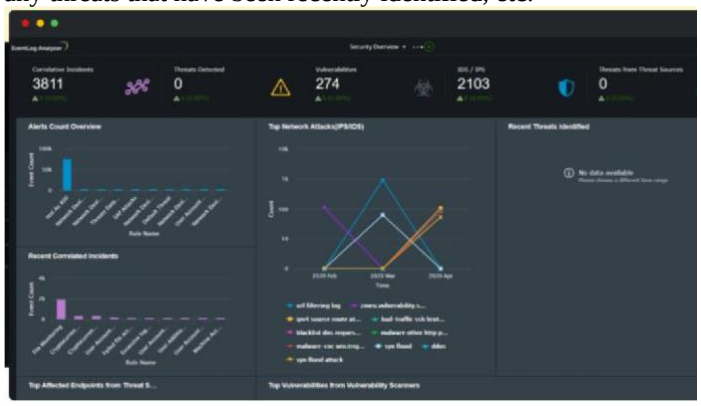

Figure 8Security Category Main Hub [14]

2.2.2 Similar System 2 -Graylog

Graylog is an software that acts as a log management and analytics tool. It provides value to various fields within the IT industry such as the cybersecurity field, the software development field, and the IT administration field. In terms of the cybersecurity field, it provides a platform for IT security teams to conduct their work as Graylog combines the concepts of Security Information and Event Management(SIEM), security analytics, and anomaly detection [13]. It has features such as threat detection, incident investigations, and threat hunting. As for the software development field, it provides a tool that allows for centralized log collection and analysis for software developers. For the IT administration field, Graylog combines monitoring, alerting and forensic features and place them all into one place. There are also additional auditing features that are provided by Graylog.

Figure 9 Graylog Logo

As shown in the figure(Figure 10) below, the dashboard of the graylog software contains event information such as failed authentication attempts, the IP address of those who have failed their authentication.

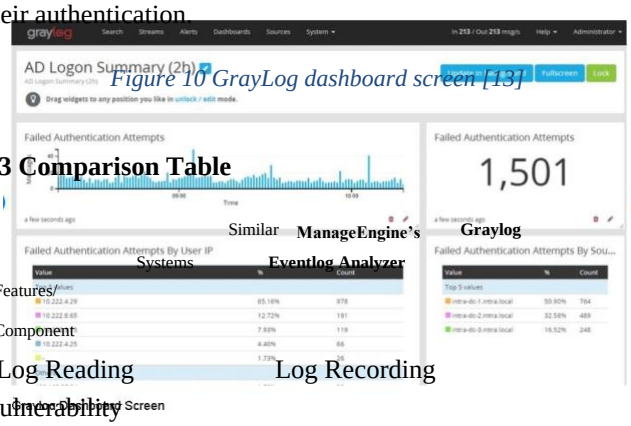

Figure 10 GrayLog dashboard screen [13]

2.3 Comparison Table

Features/ Component	Similar Systems	ManageEngine's Eventlog Analyzer	Graylog
Log Reading		✓	✓
Log Recording		✓	✓
Vulnerability Detection		✓	✓
Display Notifications		✓	✓
Auditing of Logs		✓	✓
Logs Type	General, Security, Network	General, Security, Network	
Devices	PC	PC	
VR Technology	Not Compatible	Not Compatible	

Table 1: Security Category Main Hub

The table (Table 1) above identifies the features and components of systems that are similar to the proposed system of the research. These features and components will be used within the proposed system of the research. These features and components are log reading, log recording, vulnerability detection, displaying of notifications, and auditing of logs. The proposed system also has to record logs of the security type, the network type that are related to VR technology. The proposed system also has to be able to function on the PC.

2.4 Conclusion

In conclusion, the similar systems although possess most of the required functions and components, there are still some missing requirements. That is why, in the proposed solution, a PC

application that is VR compatible will be created. It will have features similar to SIEM software where it can read logs, record logs, audit logs, detect vulnerabilities and display notifications when vulnerabilities have been detected

3.0 Problem Statement

According to Forbes in the year 2020, the effects of virtual reality (VR) in all fields of technology has revolutionized the work, education, and social lives of society [2]. However, VR has a lot of issues, for example, an issue that is distinct to ethical and privacy issues in VR is the permission requests for data collection or the use of microphones and cameras are frequently lacking [1]. The article published by Forbes has also mentioned, VR has been making great inroads into education with a large number of startups and established companies offering packaged experiences and services aimed at schools [2]. Examples of this is the emerging Virtual Reality based Learning Environments (VRLEs) such as vSocial for youth with learning disabilities. In spite of the optimistic future that lies in front of these platforms, the distribution of learning materials in real time poses an ethical, security and privacy risk [3]. The integrity and performance of VRLE systems can be jeopardized as well, as all VRLE systems are exposed to security attacks [3]. The confidentiality of VRLE systems is also vulnerable to threats to privacy such as packet sniffing and shoulder surfing [3]. VRLE systems allows for a better learning environment but at the same time exposes the privacy of the users without the user even noticing it most of the time.

4.0 Research Aims and Objectives

4.1 Aims

This project aims to propose effective solutions to provide the user with more insight on the security, and privacy issues that exist within the different types of VR software.

4.2 Objectives

- To evaluate the differences in terms of security within the different types of VR software
- To identify the common vulnerabilities that exist within all the different types of VR software
- To design a system that helps the user be aware of the dangers that might be happening when using VR technology

5.0 Research Significance

The findings from this research would be beneficial to the development and integration of VR technology into the everyday lives of society. This research provide transparency into what the VR software does. When implementing new innovations into the lives of people, the most common reaction of people would be to be afraid and wary of the side effects of the innovation. By providing transparency, people would be more open to the idea of implementing VR technology into the everyday lives of society in the future. If people are more open to the idea of VR technology, there would possibly be more funding allocated to the development of said technology. Implementing VR technology would be very beneficial for the economy of the world in various industries.

6.0 Methodology

6.1 Identify Target User

The respondents that will be targeted by the interview are people who are of the ages between 20 to 45 years old. These respondents should also have a good understanding of cyber security. This is because, they can provide the best information possible. Not only that, they will also be the ones that will be interacting with VR technology the most in the future when it is more integrated into society. Therefore, their opinion on the safety of VR technology is crucial to the research.

6.2 Sampling Method

The sampling method that is used within this research is the quota sampling method. This is because by using the quota sampling method, the answers provided by the participants can be organized by using the quotes. This allows for a clearer view of the types of answers that are provided by participants that match a certain criterion.

Through using the quota sampling method, the population will be separated into three different subsets with the use of 3 quotes. These subsets will be based on their age groups. These age group are as followed, the 20-30 age group, the 30-40 age group, and the 40-45 age group.

6.3 Sample Size

The interview will be conducted on a total of 30 respondents. These respondents will be of the three age groups, the 20 – 30 age group, 30-40 age group, and the 40-45 age group. This is so that the information obtained will not be so one sided, because people in different generations tend to have different viewpoints, therefore providing a higher variety of answers.

6.4 Data Collection Method

The method that is chosen to collect data is a structured interview. That is because the questions that are to be asked is descriptive in nature. By doing a structured interview, the questions can be answered to its fullest extent without bias. The information can also be compared with each other to obtain a better understanding of the topic.

The interviews will be conducted on a one-to-one basis to ensure that the interviewee will not be affected by other interviewees. The interviews will also have several spectators. These spectators will write down the answers provided by the interviewee. All of the interviews will be recorded with a camera as well to ensure that the spectators have not missed out on any vital information. The interview would consist of a list of 7 predetermined questions. The questions will be reviewed extensively so ensure their quality. These questions will be asked in the order that it is written in on all interviewees to ensure that there is no bias. The answers will be compared and analyzed after finishing all interviews. After that, an additional analysis will be performed to evaluate the feasibility and practicality of a log recording system specified for VR technology. The factors of the system that will be evaluated are the effectiveness, practicality, and sustainability.

7.0 Overview of the Proposed System

The diagram (Figure 11) below shows the main process of how the proposed system will function. During the logging process, the system will wait for any events that will happen when using the VR software. When an event happens within the VR software, the system will log all the necessary details of said event. The system will then scan its database to check if there is anything problematic with the event such as suspicious packets or data that is being transferred. If the system has discovered anything suspicious regarding the details of the event, the log will be flagged as suspicious. A notification will be send to the user shortly after.

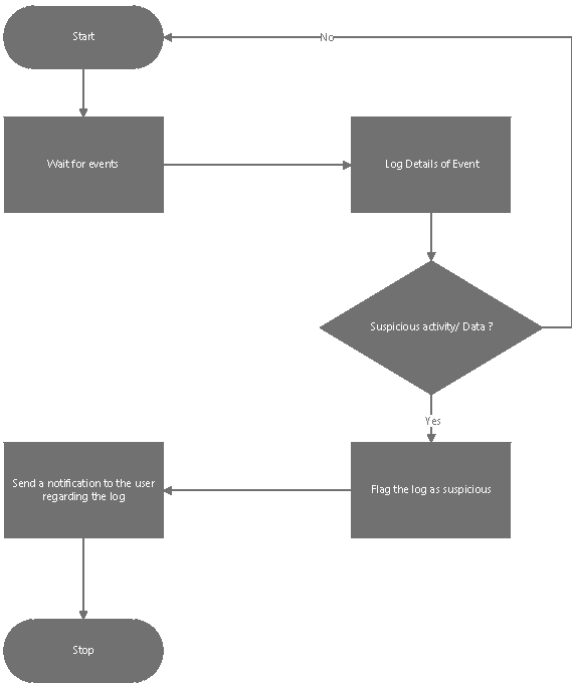

Figure 11Overview of Logging Process

The diagram below (Figure 12) shows the process of how the proposed system will function when the user views the suspicious log. When the user clicks on the notification, the system will display the full details of the log and why it is suspicious. From there, if the user deems the log to be not suspicious, the user can unflag the log with the click of a button.

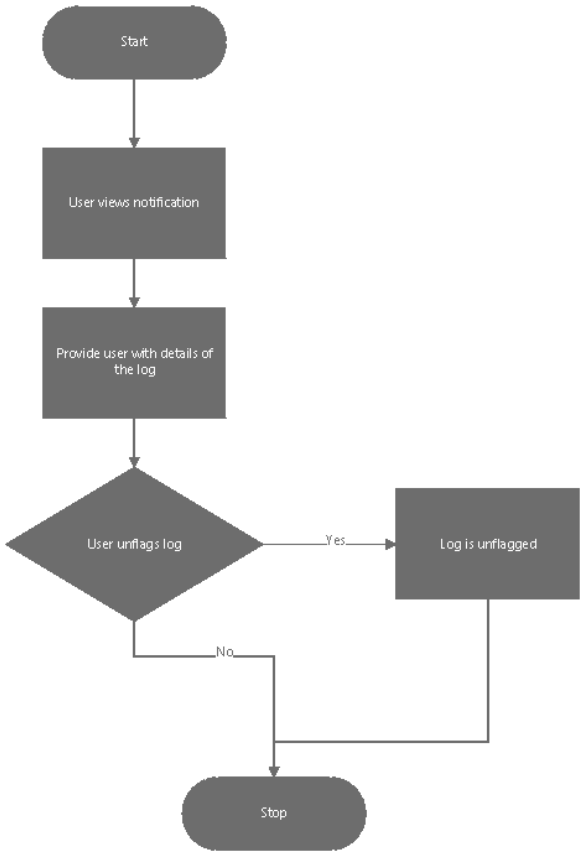

Figure 12 Overview of the system when the user views the notification

8.0 Conclusion

In conclusion, this research proposal proposes an informative system that provides VR technology users insight on potentially harmful events that may be affecting their security and privacy. By gaining insight on these events, the user will have a higher awareness on what is safe and not safe when using VR technology. This research is also beneficial to the development and integration of the VR technology as developers will be able to identify vulnerabilities within their software. In the future, this system can be upgraded to provide instructions on how to secure the VR system based on the vulnerability detected.

9.0 References

[1] Viswanathan, K., (2022). Security Considerations for Virtual Reality Systems. arXiv preprint arXiv:2201.02563.

[2] Marr, B. (2021, December 10). *The Future Of Virtual Reality (VR)*. Forbes. Retrieved March 25, 2022, from https://www.forbes.com/sites/bernardmarr/2020/12/18/the-future-ofvirtual-reality-vr/?sh=37b4c3227be8

[3] Gulhane, A., Vyas, A., Mitra, R., Oruche, R., Hoefer, G., Valluripally, S., Calyam, P., & Hoque, K. A. (2019). *Security, Privacy and Safety Risk Assessment for Virtual Reality Learning Environment Applications*. https://doi.org/10.1109/ccnc.2019.8651847

[4] Rastogi, A., & Nygard, K. (Eds.). (2019). *Software Engineering Principles and Security Vulnerabilities* (Vol. 58). International Society for Computers

[5] Ezenwoye, O., Liu, Y., & Patten, W. (2020). Classifying common security vulnerabilities by software type. In SEKE 2020 International Conference on Software Engineering and Knowledge - Proceedings of the 32nd

Engineering (pp. 61-64). (Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE; Vol. PartF162440). Knowledge Systems Institute Graduate School. https://doi.org/10.18293/SEKE2020-047and Their Applications(ISCA).

[6] Decan, A., Mens, T., & Constantinou, E. (2018). *On the impact of security vulnerabilities in the npm package dependency network* (A. Decan, T. Mens, & E. Constantinou, Eds.). https://doi.org/10.1145/3196398.3196401

[7] Votipka, D., Stevens, R., Redmiles, E., Hu, J., & Mazurek, M. (2018, May). Hackers vs. Testers: A Comparison of Software VulDiscovery Processes. *2018 IEEE Symposium on Security and Privacy* nerability

(SP). 2018 IEEE Symposium on Security and Privacy(SP), San Francisco, USA. https://doi.org/10.1109/sp.2018.00003

[8] Bhatt, N., Anand, A., Yadavalli, V. S. S., & Kumar, V. (2017). Modeling and Characterizing Software Vulnerabilities. *International Journal of Mathematical, Engineering and Management Sciences*, *2*(4), 288–299. https://doi.org/10.33889/ijmems.2017.2.4-022

[9] Croft, R., Xie, Y., & Babar, M. (2022). Data Preparation for Software Vulnerability Prediction: A Systematic Literature Review. *JOURNAL OF LATEX CLASS FILES*, *14*(8), 1–22. https://arxiv.org/pdf/2109.05740.pdf

[10] Ghaffarian, S. M., & Shahriari, H. R. (2018). Software Vulnerability Analysis and Discovery Using Machine-Learning and Data-Mining Techniques. *ACM Computing Surveys*, *50*(4), 1–36. https://doi.org/10.1145/3092566

[11] Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., & Elissa, M. (2018, August). Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. *Fourteenth Symposium on Usable Privacy and Security*, 427–442.

[12] Giaretta, A. (2022). Security and Privacy in Virtual Reality Survey. *arXiv E-Prints*. https://doi.org/10.48550/ARXIV.2205.00-- A Literature 208

[13] Graylog. (2022). *Graylog | Security*. Graylog | Security. Retrieved April 28, 2022, from https://www.graylog.org/products/security

[14] ManageEngine. (2022). *EventLog Analyzer - SIEM Log management software.* https://www.manageengine.com/products/eventlog/