Graph Neural Network을 활용하여 홈페이지 보안을 강화하는 기법 연구

조세현*, 양재승
경북대학교
*csh831219, yjs9433@knu.ac.kr

A study on enhancing security on the homepage by using Graph Neural Network

Cho Sehyun*, Yang Jaeseung
Kyungpook University

Abstract

Although the homepage is one of the important online media used in various ways such as promotion and information provision by companies and institutions, the homepage is the main target for hackers. In order to prevent this, we want to prevent it through a web firewall. Although known vulnerabilities can be prevented in advance such as a web firewall, it is true that hackers are vulnerable to new methods devised. In this paper, before uploading a file to an existing bulletin board, we propose a method for judging whether a file is malicious by pre-verifying the uploaded file through the Graph Neural Network, one ofthe deep learning methods. In this way, it is possible to detect files containing malicious behaviors that were not previously detected through a web firewall.

Ⅰ. Introduction

Public relations in companies and institutions is important to grow the institution and to secure the trust of the corporation from consumers. There are various means of publicity, but in the 21st century, online publicity is also important[1]. Among online public relations methods, the website is an important means of connecting companies and institutions. Although such a homepage is an important means, it is true that many companies are insufficient in managing the homepage for budgetary reasons. Security management during website management incurs additional costs, so many companies consider it a burden to invest budget in security. Efforts are being made to strengthen website security through firewall equipment. There are several ways to strengthen the security of the website, and the first line of defense strategy is adhered to through the web firewall [2]. In this way, security can be strengthened firstly. However, many existing web firewalls have signatures that are not registered as policy-based web firewalls. It cannot detect malicious files. In this paper, instead of a signature-based web firewall, we propose an intelligent web firewall using the deep learning method. Among the deep learning methods, Graph Neural Network (GNN) is used to detect malicious files and register them in the policy of the web firewall. We would like to propose a method to utilize it for detection. Chapter 2 introduces the operation methods and disadvantages of existing web firewalls, and suggests ways to solve them. Through this, we will derive the result of detecting files that perform malicious actions that were not detected by existing web firewalls. Chapter 3 will discuss the results of the experiment, and Chapter 4 will discuss future research directions.

Ⅱ. Body

The firewall is installed between networks with different levels of trust based on predefined security rules to prevent traffic from a low-reliability network from flowing into a relatively high-reliability network [3]. There are four main types of firewalls [4]. First, as the earliest method, there is a packet filtering method that operates at the network layer and the transport layer. While this has the advantage of being faster than other methods, it does not block malicious actions in the packet. Second, there is an application method, which can operate up to the application of the 7th layer, which is the highest layer of the OSI layer, and checks and controls even the data area in the packet. This allows higher security settings than the packet filtering method, but may cause overload on the network. The third is a circuit gateway method and refers to a firewall that performs access control between layers 5 (session layer) to layer 7 (application layer) in the OSI layer structure. The advantage is that the internal IP can be hidden, but it is cumbersome to modify all applications used for circuit gateway recognition. The fourth is a hybrid method that mixes packet filtering and application methods. It combines the advantages of packet filtering and application, and has the advantage of not only packet level control but also user control of application services.

It can be divided into Among firewalls, there are also web firewalls designed to specialize in web attacks [5]. Unlike general network firewalls, this is a solution developed specifically for web application security. In order to prevent malicious behavior of the web (SQL Injection, Cross-Site Scripting (XSS), etc.), a web firewall is additionally introduced and used. Most of the existing web firewalls try to block malicious behavior based on policy [6]. However, hackers continuously try to infiltrate various methods to bypass the web

firewall [7]. For example, if character encoding is performed twice (double encoding) to bypass the policy registered in the web firewall, the policy may not be filtered. Therefore, in this paper, we would like to propose a scheme that can be checked when uploading using a Graph Neural Network (GNN) rather than a policy-based firewall. As shown in Figure 1, we want to add a module that checks whether the request does not contain malicious behavior in front of the module that receives and processes requests within the web server.

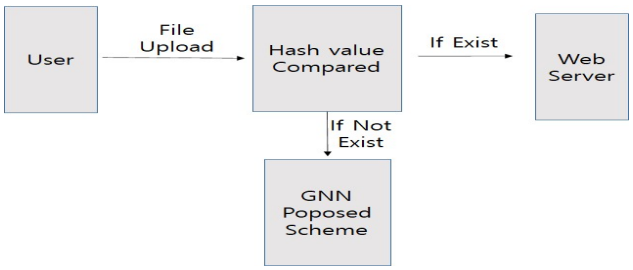

Figure 1. The proposed Scheme

III. Result

To utilize the method proposed in this paper, Google Cloud Platform (GCP) was used. A GPU card is required to use the Graph Neural Network (GNN), so four NVIDIA Tesla K80s provided by GCP were utilized. For CPU, 16 CPUs were used, 32GB RAM, and 100G hard disk were used. Experimental data was tested through datasets published on Github. Through the proposed technique, it was confirmed that although it took time, the attacker applied various techniques to bypass the web firewall, such as SQL Injection or Cross-Site Scripting, to detect it. Although it takes the user to learn the Graph Neural Network (GNN) for initial learning, it was confirmed that the detection rate to block malicious behaviors increased from 0% initially to 38% over time.

IV. Conclusion

It is no exaggeration to say that firewalls go with the history of the Internet [8]. As the number of Internet users increases, the importance of security is emphasized, and the importance of web firewalls has increased accordingly. From the attacker's point of view, there is a lot of data when it passes through the firewall, so the effort to bypass it and infiltrate continues [9]. However, existing firewalls based on policy cannot respond to these threats. Through the previously proposed method, it was confirmed that there is a possibility to respond to the threat of a new type of attacker that is not based on policy, although it is a limited situation. If the method proposed in this paper is trained by securing multiple datasets and optimized, it will be another means of increasing security in the real-world operation.

References

[1] Hansen, Anders, and David Machin. 2018. Media and Communication Research Methods. Macmillan International Higher Education

[2] Goutam, A., Tiwari, V. (2019). Vulnerability assessment and penetration testing to enhance the security of web application. 2019 4th International Conference on Information Systems and Computer Networks (ISCON),pp. 601-605

[3] Urshila Ravindran1, Raghu Vamsi Potukuchi. A Review on Web Application Vulnerability Assessment and Penetration Testing. International Information and Engineering Technology Association, Review of Computer Engineering Studies. Vol. 9, No. 1, March, 2022, pp. 1-22

[4] Chapman, D. B. and Zwicky, E. D. 1995. Building Internet Firewalls. O'Reilly & Associates, Inc.

[5] Balduzzi, M., Gimenez, C. T., Balzarotti, D., and Kirda, E. 2011. Automated discovery of parameter pollution vulnerabilities in web applications. In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS'11)

[6] R. Bebawy, H. Sabry, S. El-Kassas, Y. Hanna, Y. Youssef, "Nedgty: Web Services Firewall", Proc. of 2005 IEEE International Conference on Web Services (ICWS'05), 2005. (Pubitemid 44460253)

[7] Sid Ansari et al., "SQL Injection in Oracle: An exploration of vulnerabilities", International Journal on Computer Science and Engineering (IJCSE), pp. 522-531, April 2012.

[8] M. M. Ayachit and H. Xu, "A Petri Net-Based XML Firewall Security Model for Web Services Invocation", Proc. of the International Conference on Communication, Network, and Information Security (CNIS 2006, MIT, Cambridge, Massachusetts, USA, 2006.

[9] C. Kruegel and G. Vigna, "Anomaly detection of web-based attacks", 10th ACM Conference on Computer and Communication Security (CCS 03), pp. 251261, October 2003.(http//www.nist.gov/aes).