An implementation of log visualization system combined SCADA Honeypot

Jaehee Lee*, Jinhyeok Jeon**, Changyeob Lee***, Junbeom Lee****, Jaebin Cho*****

* Department of Information Security, Korea University, Seoul, Korea

** Department of Information Security, Sungkyunkwan University, Seoul, Korea

*** Department of Computer Science and Engineering, Sogang University, Seoul, Korea

****Department of Information and Telecommunications Engineering, University of Suwon, Suwon, Korea

*****Department of Convergence Security, Kyonggi University, Suwon, Korea

foodlook88@gmail.com, as26vl@gmail.com, howbest@ gmail.com, jb93lee@gmail.com, xxzchozxx@gmail.com

Abstract— **Recently, the leading trend and the biggest issue in global security is cyber terror. In case of Korea, on December 2014, a nuclear power plants' network was hacked into and its blueprint and manual was leaked. The case was a big threat not only to national security but also to the finance of Korea Hydro & Nuclear Power Co., LTD. However, despite this situation, there is not enough information about or detailed explanation on cyber terror. Identifying the cyber terrorists who commit a cyber terror is the best way to defend against the attack. So far, we thought that we successfully defended an attack by blocking the cyber terrorist's IP in the network firewall. However, when a certain attack fails, the cyber terrorist usually tries to find another way to attack. Especially, in case of cyber terror, a cyber terrorist uses very technical ways to attack and hack into computer network exploiting the fact that human beings can easily make mistakes. To increase the security, we do a profiling on cyber terrorist's attack techniques beforehand and set up concrete measures to deal with the attacks. This paper proposes a measure to implement a system to profile cyber terrorists, attack techniques on SCADA system, and discuss the practicality of such system by reviewing the result from actual implementation.**

Keywords-APT; Cyber Terror; APT; SCADA Security; SCADA Honeypot; SIEM

I. INTRODUCTION

Cyber Terror has become one of the biggest threat to the national security. On December 2014, KHNP (Korea Hydro & Nuclear Power Co. Ltd) which manages nuclear power plants had an accident in which their valuable data was leaked. The Cyber terrorist had been threatening KHNP through Twitter and disclosing the data. Citizens in Korea expressed their frustration at the fact that nuclear power plants' information assurance violated. In addition, there was public opinion that suggests the plants stop operating. According to Korea Defence Security Command's research, there has been over million number of attacks targeted on defence industry [1]. As such, number of cyber terror against national agency has been increasing every year. Identifying cyber terrorists and analyzing the attack technique is very important in establishing cyber-terror defence system. Honeypot is one of the ideal measure to identify cyber terrorists and analyse their purpose and behaviour pattern. Honeypot trick the cyber terrorists into attacking itself instead of the actual targeted IT system. If the Honeypot success its mission, it collects information such as the cyber terrorists' attack pattern or their IP address without losing the valuable data in IT system it protects. D3.js, which is a HTML5-based visualization tool used for visualizing the data collected by Honeypot. It helps analyst to see the log file by visualizing the file. For instance, it can show the attacks from specific IP address stage by stage. D3JS makes profiling on cyber terror much easier by providing this visualized analysis. Since September 2014, we have been working on a project that uses Honeypot in SCADA system and analyses collected log data, and we could get tangible results. Chapter 2 introduces related works that we referred to Chapter 3 presents the actual profiling system we implemented. Chapter 4 discusses about the result that we got from the profiling system. In addition, Chapter 5 discusses the practicality of this research and the future work.

II. RELATED WORK

A. Programmable Logic Controller Honeynet Project

PLC Honeynet was designed by Mattew Franz and Venkat Pothamsetty of CIAG(Cisco Critical Infrastructure Assurance Group). PLC Honeynet, which released on March 2004 provide following simulation services:

- PLC TCP/IP Stack
- Implementing Modbus/TCP Server
- Implementing FTP Server on PLC
- Searching Telnetd Server on PLC
- HTTP server

PLC Honeynet is made to implement software framework that simulates various industrial networks and devices and make decisions based on the output. Disso JP and their colleague setup an experimental but realistic Honeypot SCADA environment [2]. They then test the suitability of Honeypot in protecting SCADA systems and the efficiency of "anti-Honeypot" techniques. Their results show, that when used properly, a high interaction Honeypot can greatly

enhance SCADA system security, and in some cases better than any other security system.

B. Research on Log Visualization

ELVIS (Extensible Log Visualization) is one of the log visualization tool [3]. By using this tool, security officer can check the numerous log easily.

SnortView is also log visualization tool for Snort IDS [4]. Security officer can check the visualized security log for detecting false negative and false positive logs.

Risto at el researched comparative analysis of open-source log management solutions for network security [13]. They presented open-source solutions for log analysis is cost-effective and consume low resource. We also think same way. We decided to use open-source programs which are D3.js, Elastic search, Logstash, Kibana and Suricata.

After collecting attack log on SCADA by implementing Honeypot, it is also important to visualize the log. D3.js can make the collected data dynamically. Moreover, because it makes the data easy to understand by not only the experts but also executives, D3.js also can be useful in decision making processes.

C. Cyber Criminal Profiling on SCADA system

In the past, criminal acts were existed only in the physical world. However, due to the growth of IT technology, the criminal acts expanded their scope of activity to cyber world. Our society's critical infrastructures also can be a target for cyber terrorists because they consists of IT systems. Marc Rogers proposed the role of criminal profiling in the computer forensics process [5]. He anticipated that computer log files would be used as important evidential materials in cyber-criminal scenes.

Paulo at el researched a specialized Honeypots for SCADA systems [6]. They used Honeypot for profiling cyber threat to SCADA system. In Industrial Automation and Control System, this solution installed on DMZ zone. If attacker try to connect on PLC, he will connect to SCADA Honeypot system. In addition, their attacking logs are recorded on IDS. However, its logs are text-based. Therefore, it is hard to analyze its log. Not only this research, most of Honeypot systems record logs on text [7], [8], [9], [10], [11], [12].

For these reasons, we started to research on log visualization system for SCADA Honeypot.

III. CYBERTERROR PROFILING SYSTEM COMBINED SCADA HONEYPOT WITH SIEM

A. How to build

We used D3.js, ELK and Suricata IDS for visualizing security logs. We had implemented the log visualization solution beforehand using D3 for implement the system. The visualization solution is made of a structure in the Figure 1.

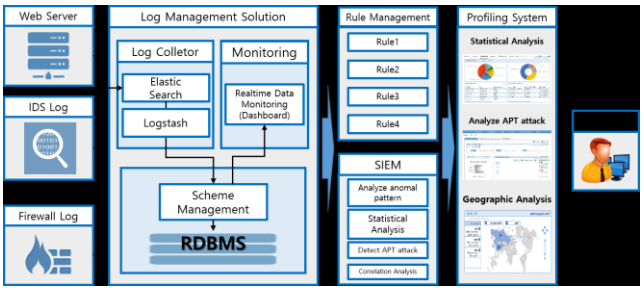


Figure 1. Diagram of profiling system

In Figure 1, it is the architecture of the solution, which we developed. It looks there is no difference with other Log visualization platform. However, it is based on open-source program and low-resource requirement. It can be useful when a server performance is limited.

B. Test environment

We actually exposed our profiling system to the public to get attack data. To expose it to the public, we gave separated official IP. The implemented system is like following in the Figure 2.

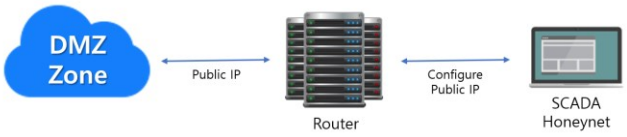


Figure 2. Test environment

C. Major Functions of Visualization System

We designed dashboard and used D3 library for visualizing security logs. Our dashboard design is in the figure 3 below. This dashboard show unified log statistics.

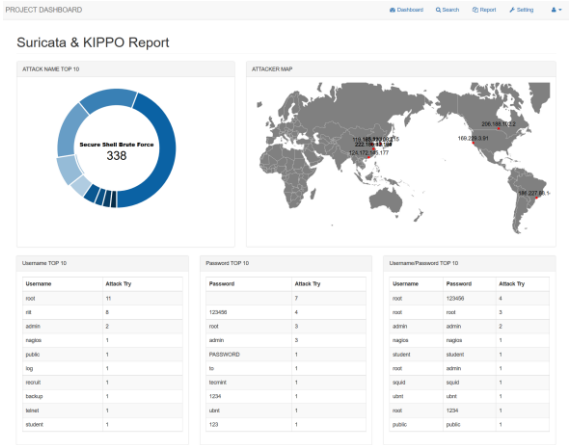


Figure 3. Dashboard design

In Figure 4, we can discover most common attack, real-time attack statistics, packet flow chart and most common tried password to our Honeynet system. Bot implements most of attacks. Nevertheless, it works well, so if we test our profiling system long time, we can get meaningful profiling result.

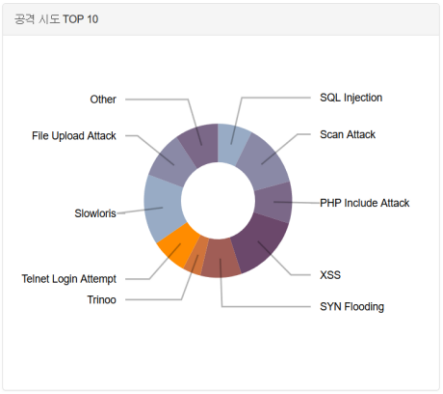


Figure 4. Most common attack Top 10

In figure 5, we analyse real-time security log pattern and visualized its log by bar graph.

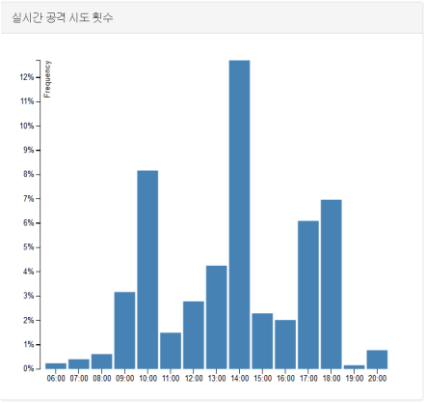


Figure 5. Real-time attack statistics chart

In figure 6, we analyse packet flow. If the packet goes through the security equipment, some packet are blocked. So if the packet as long as the inside, number of passed packet reduced. This chart shows the percentage of passed packet. In addition, we can guess the bypassing packet.

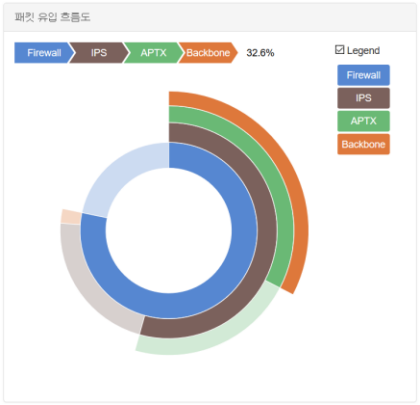


Figure 6. Packet flow chart

In figure 7, we analyse the Kippo SSH-Honeypot logs and visualize them on the table. We can check the most offensive IP and the most tried User ID for logging in.

Figure 7. Visualized Honeypot Logs

D. The Novelty of our system.

As research continues, diversity of log visualization increases. In addition, various security company use D3 component for visualizing security log. However, there is no research on combing SCADA Honeynet and log visualization platform. Previous research found that combine SCADA Honeypot and IDS for logging security events. We added additional function for visualizing security event more precisely. This platform can be used for analysing a pattern of hacker. This platform is built from open source program, so it is cost-effective. We can use it for profiling cyber threat on SCADA system.

IV. CONCLUSION

Through this study, we could learn what kind of action the cyber terrorists take when attempting an attack on SCADA system. In addition, we could verify profiling on cyber terrorists by visualizing the data. We have utilized the D3 component and other open source programs. For this reason, our profiling system is cost-effective. In Korea, research on cyber-profiling using Honeypot is not much fulfilled. If we provide our profiling system to each research institute, this will be of great assistance to our cyber security. Profiling on cyber terrorists can have more value when carried out by the entire nation, not just research agencies. Thus, national agencies should implement systems for profiling on cyber terrorists in their critical infrastructures and prepare security measures to protect its valuables from cyber terrors using the system. We will upload this profiling system on the github and get the user's feedback for the improvement of the system.

ACKNOWLEDGMENT

This research is sponsored by 'Best of the Best' education program in KITRI. In addition, we appreciate to our mentor Young-ok Kim.

REFERENCES

[1] Bodmer, Sean, et al. Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw Hill Professional, 2012.

[2] Disso, Jules Pagna, Ken Jones, and Susan Bailey. "A Plausible Solution to SCADA Security Honeypot Systems." Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on. IEEE, 2013.

[3] Humphries, Christopher, et al. "Elvis: Extensible log visualization." Proceedings of the Tenth Workshop on Visualization for Cyber Security. ACM, 2013.

[4] Koike, Hideki, and Kazuhiro Ohno. "SnortView: visualization system of snort logs." Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. ACM, 2004.

[5] Rogers, Marc. "The role of criminal profiling in the computer forensics process." Computers & Security 22.4 (2003):

[6] Simões, Paulo, et al. "Specialized Honeypots for SCADA Systems." Cyber Security: Analytics, Technology and Automation. Springer International Publishing, 2015. 251-269.

[7] Sochor, Tomas, and Matej Zuzcak. "Attractiveness Study of Honeypots and Honeynets in Internet Threat Detection." Computer Networks. Springer International Publishing, 2015. 69-81.

[8] Buza, Dániel István, et al. "CryPLH: Protecting smart energy systems from targeted attacks with a PLC honeypot." Smart Grid Security. Springer International Publishing, 2014. 181-192.

[9] Simões, Paulo, et al. "On the use of Honeypots for Detecting Cyber Attacks on Industrial Control Networks." proc of 12th European Conf. on Information Warfare and Security (ECIW 2013). 2013.

[10] Provos, Niels. "Honeyd-a virtual honeypot daemon." 10th DFN-CERT Workshop, Hamburg, Germany. Vol. 2. 2003.

[11] Valli, Craig. "SCADA forensics with Snort IDS." (2009).

[12] Wade, Susan Marie. "SCADA Honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats." (2011).

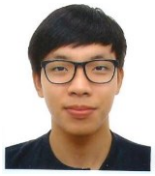
[13] Vaarandi, Risto, and Paweł Niziński. "Comparative Analysis of Open-Source Log Management Solutions for Security Monitoring and Network Forensics." Proceedings of the 2013 European Conference on Information Warfare and Security. 2013.

Jaehee Lee working on a Master's Degree in the Department of Information Security at the Graduate school of Information security, Korea University. His Research interests are in the areas of risk management and malicious code analysis. He is researching SCADA Honeynet recently. He takes 'Best of the Best' education program in KITRI.

Jinhyeok Jeon working on a Master's Degree in the Department of Information Security, Sungkyunkwan University. His Research interests are in the areas of security log analysis. He is researching analyzing APT recently. He takes 'Best of the Best' education program in KITRI.

Changyeob Lee working on a Bachelor's Degree in the Department of Computer Science and Engineering, Sogang University. His Research interests are in the areas of log analysis and visualization. He is researching SIEM solution recently. He takes 'Best of the Best' education program in KITRI.

Junbeom Lee working on a Bachelor's Degree in the Department of Information and Telecommunications Engineering, University of Suwon. His Research interests are in the areas of log analysis and visualization. He is researching log visualization recently. He takes 'Best of the Best' education program in KITRI.



Jaebin Cho working on a Bachelor's Degree in the Department of Convergence Security, Kyonggi University. His Research interests are in the areas of log analysis and visualization. He is researching log analysis recently. He takes 'Best of the Best' education program in KITRI.