Advanced Science and Technology Letters
Vol.136 (ITCS 2016), pp.157-160
http://dx.doi.org/10.14257/astl.2016.136.36

Architecture of Cyber Intelligence System for Cyber Attack & Defense Training

Yeon Seo[1], Yu-Hyun Kim[2], Keun-Seog Park[2], and Jung-Ho Eom[1*]

[1] Daejeon University,
62 Daehakro, Dong-Gu, Daejeon-si, 300-716, Republic of Korea
tjdus2243@naver.com, eomhun@gmail.com
[2] Airforce,
663, Gyeryongdae-ro, Gyeryong-si, Chungcheongnam-do, Republic of Korea
kimyh0106@airforce.mil.kr, pksm06@naver.com

Abstract. In this paper, we proposed architecture of cyber intelligence system for cyber-attack & defense training. In cyber training, the first process is exactly to acquire the cyber intelligence (data) related to cyber-attack and defense. The proposed cyber intelligence system is an optimized model for providing customized intelligence to trainees, for collecting and analyzing information (data) of cyber environment. When the cyber-attack training is performed, it must accurately identify data related to the target components. When the cyber-defense training is performed, it should be preceded to extract data related to cyber-attacks and detect signs of cyber-attack. The proposed system consists of 5 subsystems to efficiently collect, analyze, and propagate cyber intelligence.

Keywords: Cyber intelligence, Cyber training, Intelligence Process

1 Introduction

Cyber training is an essential element in the improvement of individuals and teams capabilities that is protected governmental, military, and commercial institutions from cyber-attacks. Nowadays, cyber training program provides intensive, practical and comprehensive training contents for red (attack) and blue(defense) teams. To proceed with this training, it should establish integrated training system that can be done cyber-attack and defense at the same time [1].

When cyber-attack and defense is executed in cyber training, it must firstly acquire data related to the offensive and defensive targets. Once the data is collected, it is needed to filter out enormous data and reproduced as validated data. The validated data are classified by data related to attack or defense, and the trainees should use these data in the training process. To manage the data required for the cyber training after collecting, analyzing, processing, and classifying the collected data will be a great help for achieving the cyber training goals [2].

* He is a correspondent-author of this paper.

ISSN: 2287-1233 ASTL

So, we propose cyber intelligence system that collect, analyze, manage, and provide needed data in order to achieve the goal of cyber-attack and defense training. Our proposed system is consisted of 5 subsystem; cyber intelligence circulation system, cyber intelligence fusion system, cyber intelligence support system, cyber intelligence management system, and cyber target management system.

In this paper, we will describe the framework of proposed system in section 2, and explain architecture of proposed system in section 3. We conclude in section 4.

2 The Framework of Proposed System

Cyber intelligence system should be able to extract only the data associated with a cyber-attack and defense through the analysis process of collected data. A cyber intelligence system must meet the following requirements to the above functions.

Firstly, it should have the fusion ability of data that can reproduce and share from vast collected data in cyberspace to use cyber-attack and defense. In other words, it requires data processing technology that can extract, analyze, product, and provide the effective data in the enormous data collected from cyberspace.

Secondly, it can support optimized intelligence because data collection target and method is different according to attack & defense and the provided data is different in accordance with the mission phase. When defensing cyber-attack, it should apprehend the type and importance of defensive targets system, the level of vulnerability and risk, mission and role of organization. When performing cyber-attack, it should acquire such data as environment of attack target, the type of network and system, security system, vulnerabilities, the main attack points, and so on.

Thirdly, it must include the management function of data to efficiently manage collected data and accurately provide a cyber-attack and defense. It must manage by classifying and listing collected data in accordance with the characteristics of intelligence to provide timely intelligence.

Finally, when doing cyber-attack, it should include a management function of target's intelligence could be recommended cyber target to comply with attack goal.

Fig. 1. The Framework of Cyber Intelligence System

Cyber intelligence system must collect, analyze, manage, and provide needed data in order to achieve the goal of cyber-attack and defense. It should be designed to reflect the requirements. It should include 5 subsystems such as cyber intelligence fusion system that can collect, process, and analyze data, cyber intelligence support system that can provide intelligence depending on mission, cyber intelligence management system that can classify and manage data based on types and importance of data, and cyber target management system that can timely provide target intelligence to achieve the goal of cyber-attack. The above figure shows the framework of cyber intelligence system [2,3,4].

3 Architecture of Proposed System

Cyber intelligence system must be architecture modules required functions of each system based on the framework. The following figure shows the architecture of proposed system.

Fig. 2. Architecture of Proposed System

Cyber intelligence circulation system is to reproduce the reliable intelligence through collection, analysis, and production of data produced in cyberspace. It should be executed the following steps; Planning and order, Data collection, Data processing, Analysis and production, Dissemination and management, and Consolidation and standardization.

Cyber intelligence fusion system performs the function to integrate data associated with the data of the different type from the data collected in the cyberspace. In other words, it is the processing system for processing into useful data after extracting data having the validity and reliability, through filtering and correlation analysis of raw data. It consists of 5 functions; Interpretation and transformations of raw data, data filtering, correlation analysis, Threat analysis, and Countermeasure recommendation.

Cyber intelligence support system is a system that provides the intelligence required to perform each mission step to the cyber-attack and defense. Cyber intelligence support is provided by each type of cyber-attack and defense. And it is provided optimized intelligence by each mission step. The process of cyber-attack is as follows; Data collection, Decision of main attack point, Selection of cyber weapons, Attack execution, deletion of attack trace, and Impact assessment. The process of cyber-defense is as follows; Watch and monitor, Indicator detection, Attack blocking, Impact assessment, and Recovery.

Cyber intelligence management system is to manage data related to cyber infrastructure as listing and classifying in according to the purpose of use to accurately and quickly provide data collected from cyberspace. It consists of 4 modules; Cyber infrastructure list, Cyber targets list, Cyber order of battle, and Pre-CTO(Cyber Tasking Order) [6].

Cyber target management system is to manage target system based on importance to maximize the effectiveness of cyber-attacks in order to achieve the goal of cyber-attacks. Cyber target can be determined based on the level of vulnerabilities by filtering the data related to the enemy information communication structure acquired by the cyber intelligence collection tool.

4 Conclusion

We need the specialized cyber intelligence system in order to effectively collect and efficiently manage the data in cyber training process.

So, we proposed the customized cyber intelligence collection, analysis, and management system. Cyber intelligence system should be able to extract only the data associated with a cyber-attack and defense through the analysis process of collected data. Our proposed system consists of 5 subsystem; Cyber intelligence circulation system, Cyber intelligence fusion system, Cyber intelligence support system, Cyber intelligence management system, and Cyber target management system.

References

1. https://www.sans.org/cybersecurity/ May 10 (2016)
2. Shin, J.H., Cheon, S.P., Eom, J.h.: The Role and Responsibility of Cyber Intelligence in Cyber Warfare, The proceedings of The 3rd International Conference on Information Technology and Computer Science, ASTL, Vol. 51, pp. 305--308 (2014)
3. Eom, J.-h.: Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace, International Journal of Software Engineering and Its Applications, Vol.8, No.9, pp. 137--146 (2014)
4. Gortney, W. E.: Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, (2014)
5. Dempsey, M. E.: Joint Intelligence, Joint Publication 2-0 (2013)
6. Eom, J.h., Kim, N.k., Chung, T.M.: Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare, The Proceedings of the 2012 International conference on Cyber Security, Cyber Warfare and Digital Forensic, pp. 295--299 (2012)

