디지털산업정보학회 논문지 제16권 제3호-2020년 9월
http://dx.doi.org/10.17662/ksdim.2020.16.3.037

A situation-Flexible and Action-Oriented Cyber Response Mechanism against Intelligent Cyber Attack[*]

Kim Namuk[**] · Eom Jungho[***]

지능형 사이버공격 대비 상황 탄력적 / 실행 중심의 사이버 대응 메커니즘

김 남 욱 · 엄 정 호

〈Abstract〉

The In the 4th industrial revolution, cyber space will evolve into hyper-connectivity, super-convergence, and super-intelligence due to the development of advanced information and communication technologies, which will connect the nation's core infrastructure into a single network. As applying the 4th industrial revolution technology to the cyber attack technique, it is evolving in an intelligent and sophisticate method. In order to response intelligent cyber attacks, it is difficult to guarantee self-defense in cyberspace by policy-oriented, preplanned-centric and hierarchical cyber response strategies. Therefore, this research aims to propose a situation-flexible & action-oriented cyber response mechanism that can respond flexibly by selecting the most optimal smart security solution according to changes in the cyber attack steps. The proposed cyber response mechanism operates the smart security solutions according to the action-oriented detailed strategies. In addition, artificial intelligence-based decision-making systems are used to select the smart security technology with the best responsiveness.

Key Words : Cyber Response Mechanism, Intelligent Cyber Attack, Smart Security Solution, Action-Oriented Strategy

Ⅰ. Introduction

The cyberspace in the 4th industrial revolution era will evolve into a hyper-connection, super-intelligence, and super-convergence space that is connected various objects & equipment and national critical infrastructures to a single network. On the other hand, due to the numerous systems connected to the evolving cyberspace, new vulnerabilities are increasing exponentially and are easily exposed to

[*] This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019R1F1A1041782).

[**] SKKU Computer Engineering Doctorial Course
[***] Daejeon Univ. Military Studies Professor(Co-author)

cyber attacks. And, it is emerging as an important security domain because the national critical infrastructure is controlled by a control system applied the 4th industrial revolution technology including AI. The cyber attacks are changing to an intelligent cyber attack in the 4th industrial revolution era. Cyber attack technology using artificial intelligence algorithms can have an intelligent cyber attack function that enables self-learning and decision attack paths and autonomous selection[1].

Advanced countries are aggressively revising or strengthening their national cyber security strategy offensively, judging that intelligent cyber attacks are the biggest threat among various security threats in the 4th industrial revolution era. In order to effectively respond to the intelligent and sophisticate cyber attacks, it is necessary to implement a situation-flexible and action-oriented cyber response mechanism utilizing smart cyber security technology.

In this research, we design a situation-flexible and action-oriented cyber response mechanism and propose an action-oriented detailed strategy based on smart cyber security technology according to changes of the cyber attack step. In this paper, we will explain evolution of cyberspace and cyber attack & defense technology in section 2, and describe the detailed cyber response strategies in section 3. Lastly, we explain the proposed cyber response mechanism in section 4, and describe how to apply the proposed mechanism to defense the APT attack And we conclude in section 5.

Ⅱ. Evolution of cyberspace, cyber attack and defense technology

The 4th industrial revolutionary technology is evolving at a rapid pace that has never been experienced before, causing disruptive technological innovations in all industries and changing the function of the system to a new concept. In particular, advanced information and communication technologies based on computers and the Internet fuse real world into cyberspace through various technologies such as 5G, mobile, IoT(Internet of Things), cloud computing, big data, artificial intelligence, virtual reality and augmented reality, 3D printing, robots, and drones, etc. A typical example is a cyber-physical system that is an automated and intelligent system in which all objects are connected to the IoT and communicate in real time so that the cyber space and the physical space interact with each other[1-3].

AI(Artificial Intelligence), which is the core technology of the 4th industrial revolution technology, is applied to cyber attack and defense technology through various AI algorithms. Cyber attack technology has a multi-level and randomly unpredictable attack pattern according to the changes of the cyberspace environment and the target system. The cyber defense technology has a situation-aware security algorithm that analyzes and learns the path and target step by step in the cyber attack to prevent it from intruding the final attack target[3].

2.1 Evolution of cyberspace

Cyberspace will be a hyper-connected, super-convergent, and super-intelligent space that connects all things in the world by combining advanced ICT such as AI and IoT with highly developed science and technology. In other words, the boundaries will disappear in all areas such as the physical, biological, and virtual worlds, creating a new space that is different from the composition and function of the previous cyberspace. Cyberspace in the future will have the following characteristics[2, 3].

First, all objects, systems, and humans will be connected to each other in real time to transmit data or information, and it will be a hyper-connected space that is not limited by distance and time. In the 4th industrial revolution era, the development of advanced ICT enables hyper-logical connection, so data will be transmitted in real time without time delay. In other words, the concept of physical distance will disappear, creating simultaneity as if everyone is sharing the same information at the same time, and in the same place.

Second, the boundary between cyberspace and physical space will be broken and fused in real time, it will become a super-convergent space interlocked as if working together in the same space. Assets in cyberspace are virtually created cyber assets and physical assets that are connected and controlled by a control communication network. And, humans in cyberspace include accounts that computers can recognize, cyber robots that are programmed to perform a given task, and people as physical beings affected by cyber humans in cyberspace. It is the cyber physics system that enables all these humans and objects to communicate with each other in real time in the same space.

Finally, it will be a super-intelligent space that analyzes the situation and solves problems on its own with technologies such as big data and artificial intelligence based on huge data generated from various objects, systems, and networks. Intelligent services can be provided by finding certain patterns and knowledge hidden in huge data. Previously, most of the system components were controlled by humans or controlled by another control system, but the super-intelligent cyberspace has many smart systems that they are possible to select an operation method suitable for the situation and to analyze and autonomously handle the problem when problem is occurring.

2.2 Evolution of cyber attack and cyber defense technology

Among the 4th industrial revolution technologies, AI is the most effective technology for cyber attack and defense technology. AI is capable of learning, analyzing, judging, and predicting functions, so it can analyze and predict cyberspace situations, analyze and judge cyber attack and defense procedures, and predict paths of attack and defense. In terms of cyber attacks, AI predicts changes in the cyberspace environment, finds the weakest points, and sets the cyber attack path. In terms of cyber defense, AI recognizes the progress of cyber attacks and learns cyber attack techniques and respond to the optimal cyber security technology[3].

Cyber attack technology is evolving into a pattern of intelligent cyber attack applied with the

4th industrial revolution technology, such as a target-centric attack method that selects only a specific user of software and executes the infected malicious code, and a method that evades and attacks a security system. Cyber attack technology is evolving into autonomous malware that collects and analyzes the information of cyberspace and the target system's specification, and establishes a cyber attack procedure to conduct attacks without external control by using various algorithms of AI. And, it is advancing into a pattern of malicious code capable of adapting to the ever-changing cyberspace environment and self-evolving and mutating so as not to be detected by security systems or programs installed in the target system. Zero-day attacks targeting only new security vulnerabilities in devices that utilize the 4th industrial revolution technologies such as intelligent CCTV, AI speakers, and IoT-combined systems are increasing. Recently, a cyber attack technique has been developed that attempts to illegally access a network and leak data after planting malicious code in a drone and flying the target system area[4-6].

The existing cyber security technology was able to find and patch system vulnerabilities one by one or respond only to known cyber attack methods. Therefore, the ability to defend against internal threats or newly generated cyber attacks is insufficient. In other words, without knowing who, when, how, and where cyber attacks will occur, security managers were passively defending against cyber attacks. Since existing cyber security solutions are not possible to defend against intelligent cyber attacks using AI algorithms, active and intelligent cyber security solutions using AI algorithms have also been developed for cyber defense technologies[7, 8].

In the 4th industrial revolution era, the aspect of cyber security technology is building an active integrated cyber response management structure capable of responding to intelligent cyber attacks in real time in order to realize the safety, reliability, and rapid resilience of hyper-connected platforms based on IoT and 5G. Vulnerability analysis tools to secure system safety are developing into intelligent vulnerability analysis technology that automatically detects and analyzes security vulnerabilities occurring in the system, and automatically generates security patches. The cyber self-mutation technology currently being developed by ETRI [9] is a technology that prevents cyber attacks through periodic modification of the system's network address, software, and data. In other words, even if the target network address is stolen, it is a technology that protects the target because the network address has already been changed to another address when attempting to attack with that address. The intrusion detection system is able to collect normal network packets and various abnormal network packets by applying AI to the packet collection tool[7]. And, by applying various machine learning algorithms, it is possible to determine whether packets are generated in real time based on the learned knowledge. The recently developed detection technology utilizes non-supervised learning-based machine learning techniques, such as the human immune system, to learn normal behavior through the data flow of all systems and to judge abnormal behavior that deviates from it. The intelligent enterprise security management system can collect and analyze various data generated from security systems by using big data on a platform. In addition, it can be applied to security control by intensively analyzing high-risk events through machine learning-based supervised and unsupervised learning.

Ⅲ. The detailed strategies for a situation-flexible and action-oriented cyber response mechanism

As explained in Chapter 2 above, it is difficult to defend with current security solutions, because cyberspace becomes more complex and cyber attacks become intelligent due to the 4th industrial revolution technology. So, it is necessary to propose the cyber response mechanism based on smart security solutions.

3.1 Requirements for a situation-flexible and action-oriented cyber response mechanism

The following describes the requirements for establishing a situation-flexible and action-oriented cyber response mechanism that can effectively respond to intelligent cyber attacks[1, 2, 10].

First, a policy-oriented cyber response strategy is excluded. In the era of rapid development of ICT and science technology, the policy-oriented strategy is not appropriate because cyber attack methods and technologies are radically changing. In particular, cyber response strategies not based on cyber security technology(system) cannot be applied in practice.

Second, the preplanned-centric cyber response strategy is excluded. As the cyber attack technique is sophisticate & intelligent and the attack method or path cannot be predicted, it is difficult to defend the cyber attack according to the preplanned response procedure. In particular, scenario-based responses are not appropriate when a cyber attack agent upgrades or changes itself during a long-term attack.

Third, it should be a situation-based response switch strategy that can apply cyber security technology in accordance with the changes of cyberspace environment and cyber attack step. As mentioned above, the progress of cyber attacks are not sequential as before, but cyber attacks are changed according to the target system and cyberspace environment. Therefore, it is necessary to autonomously select and apply the security technology(systems and programs) that can defend the cyber attack as much as possible.

Finally, the cyber response mechanism should operate on action-oriented detailed strategies. Just as military strategies are established in conjunction with operations, tactics, and maneuvering, cyber response mechanism must be practically implemented in connection with cyber security technology. In other words, cyber security technology must be selected and deployed according to the action-oriented detailed response strategy, and it must have the ability to respond to cyber attack. To do this, it needs to install the best cyber security system(program) and keep the security functions up to date.

3.2 Types of action-oriented detailed strategies

The action-oriented detailed strategies of proposed mechanism were established by deriving concepts applicable to cyber response mechanism from the strategies, operation, and tactics used in security / military strategy and cyber / information warfare. The detailed response strategies of proposed mechanism are as follows.

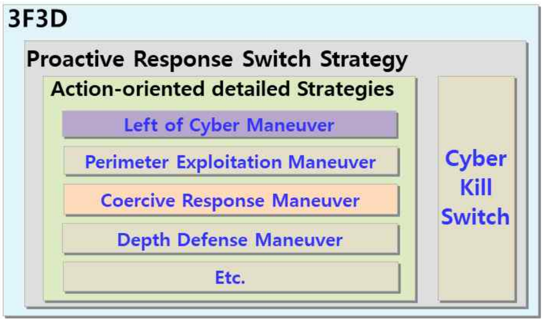
First, the most basic concept of the proposed cyber response mechanism is 3F3D[11]. The concept of 3F (First detection, First decision, and First Action) is to detect attack indicators before cyber attack occurs, decide firstly whether to act or not, and then firstly take action. 3D (Deep watch, Deep control, and Deep protection) is a concept that must be able to monitor core assets, to control core assets, and to protect core assets from intrusion. It prevents cyber attacks proactively, actively detects intrusions, and protects them from attacking as much of the core assets as possible. To enable 3F3D strategy, it is necessary to support smart security solutions that can automatically identify and block vulnerabilities, analyze incoming packets in real time to determine intrusion, and intelligently block attack progress.

Second, the core strategy of the proposed mechanism is a proactive response switch strategy. This is a strategy that proactively defends by selecting or adapting the most suitable cyber security solutions by modifying or switching action-oriented detailed strategies that can respond to sophisticate attack techniques when an intelligent cyber attack proceeds according to changes of the cyberspace and the target system environment.

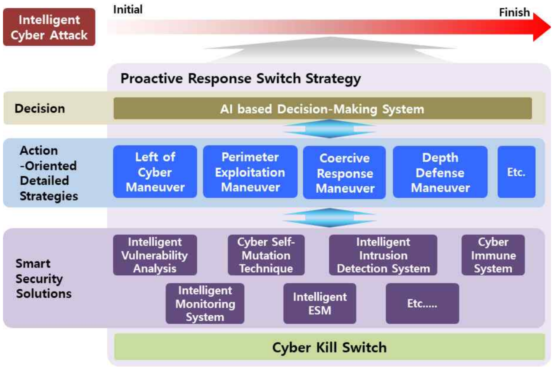
Third, cyber kill switch is a strategy to shut down the system as quickly and completely as possible without keeping safety mechanisms in the following major crisis situations. First case, there are indicators of cyber attack, but the cyber attack is not detected and the system continues to malfunction or become paralyzed. The second case, when the cyber attack has intruded in the depth, but there is no defense. This strategy must be carefully determined as it will damage the system at the same time it is executed.

Lastly, these are action-oriented detailed strategies for implementing the proposed cyber response mechanism. The left of cyber maneuver is a strategy that predicts the possibility of an attack and the attack method by collecting and analyzing abnormal indicators before a full-scale cyber attack starts[12]. The perimeter exploitive maneuver is to block cyber attacks from the point of entry from the outside to the inside and find malicious code that has already entered the inside. The coercive response maneuver is to prevent cyber attacks that could not be blocked from perimeter exploitive maneuver from intruding to the depth by actively blocking malicious packets and dynamically changing the network configuration. The depth defensive maneuver is to prevent account takeover of core systems, leakage of confidential data, and paralysis of core servers[13].

The following figure shows the composition of a situation-flexible and action-oriented cyber response mechanism.


3F3D
Proactive Response Switch Strategy
Action-oriented detailed Strategies
Left of Cyber Maneuver
Perimeter Exploitation Maneuver
Coercive Response Maneuver
Depth Defense Maneuver
Etc.
Cyber Kill Switch

<Figure 1> The composition of proposed cyber response mechanism


Intelligent Cyber Attack
Initial
Finish
Proactive Response Switch Strategy
Decision
AI based Decision-Making System
Action -Oriented Detailed Strategies
Left of Cyber Maneuver
Perimeter Exploitation Maneuver
Coercive Response Maneuver
Depth Defense Maneuver
Etc.
Smart Security Solutions
Intelligent Vulnerability Analysis
Cyber Self-Mutation Technique
Intelligent Intrusion Detection System
Cyber Immune System
Intelligent Monitoring System
Intelligent ESM
Etc.....
Cyber Kill Switch

<Figure 2> The situation-flexible and action-oriented cyber response mechanism

Ⅳ. A situation-flexible and action-oriented cyber response mechanism

The proposed cyber response mechanism is a mechanism that selects action-oriented maneuvering strategies according to the progress of intelligent and sophisticated cyber attacks, and flexibly applies smart security solutions to defend them. Intelligent cyber attacks do not rely on sequential attack procedures and use appropriate cyber attack techniques in according to changes in the cyber-space and cyber attack, so it is impossible to preemptively respond by policy and preplanned-oriented cyber response strategies. And, since intelligent cyber attacks are carried out in an instant, it is impossible with existing human-controlled cyber security solutions. Therefore, it is necessary to make it possible to select an smart security solution that can detect and block cyber attack techniques that are applied to each attack step without time delay by AI-based decision-making systems. The following figure shows the model of a situation-flexible and action-oriented cyber response mechanism.

The framework of a situation-flexible and action-oriented cyber response mechanism has the following functions.

First, when smart security solutions warn to find the indicators of an intelligent cyber attack, left of cyber maneuver is selected in order not to intrude inside through an AI based decision system. Then, depending on the nature of the indicators of cyber attacks, smart security solutions are selected to prepare for defense or to change information of internal systems.

Second, when a cyber attack intrudes to the inside, it analyzes the cyber attack step, technique, route, etc. using the data collected through the previous security systems, and then applies the most appropriate detailed strategies to operate the smart security solution. For example, perimeter exploitation maneuver or coercive response maneuver is selected. At this time, not only one detailed strategy is selected, but several strategies may be selected according to the cyber attack step. And, multiple smart security solutions can be selected, and each security solution can expand the scope of monitoring and detection. As the cyber attack progresses, it can either switch to a attack technique that bypasses the security solution or choose another attack technique due to information changes of the internal system. In this case, based on the data analysis results collected by the smart security solution, it is necessary to select strategies that can respond to the converted cyber attack technique through the AI based decision-making system.

Third, if there is a possibility that the cyber attack may intrude the core system, select a depth defense maneuver to operate the security systems installed at the front line. Multiple detailed strategies and security solutions can be selected depending on the situation.

Lastly, if indicators of a cyber attack is detected, but the intention and path of the cyber attack are not identified, or if the cyber attack cannot be defended with action-oriented detailed strategies and security solutions, the target system is forcibly terminated by using a cyber kill switch. At this time, the damage may occur to the target system, but it is less than the damage caused by the cyber attack, so it is used as a last means as a final action-oriented defense strategy.

Ⅴ. Example

An APT attack occurs, the mechanism to defend each attack step by applying the proposed model is as follows. The outline of APT attacks is shown in the following table[14, 15].

<table 1> The Outline of APT

<table>
<tr><th>Title</th><th>Contents</th></tr>
<tr><td>Type</td><td>APT</td></tr>
<tr><td>Goal</td><td>Data Leakage</td></tr>
<tr><td>Target</td><td>Server</td></tr>
<tr><td>Procedure</td><td>- <b>Pre-Reconnaissance</b>
· (R1| R2| R3| R4)
· (R5| R6| R7)
- <b>First Penetration</b>
· (P1 & P2) | (P5 & P2) | (P3 & P4)
- <b>Concealment / Information Gathering / Hidden Communication</b>
· (S1 | S2 | S3 | S4 | S5) & (G1 | G2 | G3 | G4 | G5) & ((S1 | S2 | S3 | S4) & (C1 | C2))
- <b>Privilege Escalation</b>
· (A1 | A2 | A3 | A4 | A5)
- <b>Data Leakage</b></td></tr>
</table>

The attack method used in each attack step of the attack procedure is shown in the following table.

<table 2> The Attack Method in Each Attack Step

Step	Contents
Reconnaissance	R1 : Port Scanning R2 : Vulnerability Scanning R3 : Service Scanning R4 : Host Scanning R5 : Search Engine R6 : Crawler R7 : Social Network
Penetration	P1 : Spear-phishing email with malicious link P2 : Drive-by Download P3 : Spear-phishing email with malicious attachment P4 : Malicious cod installation through software vulnerability P5 : Water Hole attack
Concealment & Information Gathering & Hidden Communication	S1 : Logic bomb S2 : Rootkits S3 : Binary packing S4 : Polymorphic malware S5 : Fileless malware G1 : Port Scanning G2 : Vulnerability Scanning G3 : Service Scanning

	G4 : Host Scanning G5 : Directory Guess G6 : Backdoor G7 : C&C Communication (Using FTP, HTTP, SMTP/POP3, etc) C1 : Network Fast Flux C2 : Encrypted Communication C3 : Anonymous Communication C4 : Covert Communication
Privilege Escalation	A1 : Dictionary / Brute force attack A2 : Key Logging A3 : Screen Capture A4 : Man-in-the Browser A5 : Directory/File Search

In the pre-reconnaissance step, R1 to R4 are likely to be detected by security programs, so they are not used much now. So, if R5 or R7 is used to collect the target information, the proposed model applies the left of cyber maneuver strategy and uses the same method to monitor the collected words and focused search targets. In the infiltration step, if P1 and P2 are used to infect the target network or system, a perimeter exploitation maneuver strategy is applied to operate a vaccine program or a security program that filters e-mails of unknown origin intelligent monitoring system. In the concealment & information gathering & hidden communication step, all of the concealment, information gathering, and hidden communication must be successful. only one of them needs to be blocked in order not to proceed to the next attack step. If fileless malware that has been widely used recently, is used, a coercive response maneuver strategy is applied and a motion-based detection tool in intelligent intrusion detection system is used to detect it. If the attacker uses the key logging(A2) method in the privilege escalation step, we have to apply the depth defense manuever strategy to prevent it with a security program capable of real-time monitoring function exclusively for key logging. Finally, if it is determined that there is a possibility of information leakage without preventing and blocking the attack in the APT attack step, the cyber kill switch is activated to stop all system operations.

The existing cyber attack response strategy monitors and detects from the beginning to the end of the cyber attack through an installed security system(program). When several security systems(programs) operate at the same time within the internal network, the operating speed of the internal system decreases or a collision between security systems(programs) occurs. In order to compensate for these shortcomings and to preemptively defense intelligent cyber attacks from invading to the depths, the security system(program) is activated only when the cyber attack step or internal network layer is defended, and countermeasures are initiated, so it does not affect the internal system normally.

Ⅵ. Conclusion

In the 4th industrial revolution era, cyberspace will become a security domain that poses a great threat to national and social security due to sophisticated and intelligent cyber attacks. An advanced cyber response mechanism is needed to protect the key core infrastructure of the nation and society from these intelligent cyber attacks. It is difficult to preemptively block intelligent cyber attacks with the existing policy and preplanned-oriented cyber response strategies. We proposed a situation-flexible and action-oriented cyber response mechanism that can actively respond to the cyberspace and cyber attack situations. In accordance with the proactive cyber response switch strategy, the action-oriented detailed strategy was selected according to the cyber attack situation and the smart security solution was applied. Once indicators of cyber attacks are detected or cyber attacks are in progress, it selects action-oriented detailed strategies that can most effectively respond cyber attacks according to cyberspace and cyber attack situations. Then, depending on the detailed strategy, a smart security solution that can defend the attack is activated.

The proposed cyber response mechanism has the advantage of selecting the appropriate detailed strategy and operating the smart security solutions whenever a different cyber attack technique is used or the cyberspace situation changes as the cyber attack progresses.

Reference

[1] Shin, H.G. and Eom, J.H., "Establishment of Cyber Security Strategy according to the change of cyberspace environment," Journal of Security Engineering, Vol.14, No.4, 2017, pp.251-262.

[2] Kim, S.G., Cheon, S.P., and Eom, J.H., "A leading cyber warfare strategy according to the evo-lution of cyber technology after the fourth industrial revolution," International Journal of Ad-vanced Computer Research, Vol 9(40), 2018, pp.72-80.

[3] Hur, C.H., Kim, S.P., Kim Y.S., and Eom, J.H., "Changes of Cyber-Attacks Techniques and Patterns after the Fourth Industrial Revolution," The 5th International Conference on Future Inter-net of Things and Cloud Workshops 2017, pp.69-74.

[4] Eom, J.H., "Modeling of Cyber Attack Intentions Analysis reflecting Domestic / International Situations," International Journal of Grid and Distributed Computing Vol.11, No.1, 2018, pp.13-16.

[5] Eom, J.H, Kim, N.U., and Chung, T.M., Introduction on cyber war in the 4th industrial revolution era, Hongneung, Seoul, 2020, p.81-94.

[6] 7 cyber attacks in 2020, https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35227

[7] Lee, D.S, "The Trends of Next Generation Cyber Security Technology," Weekly Technology Trends, No.1916, 2019, pp.2-15.

[8] Kook, K.H. and Kong, B.C., "The Trend of Security technology development using artificial intelligence," Weekly Technology Trends, No.1913, 2019, pp.2-15.

[9] ETRI, Promotes network self-defense technology development, http://www.koit.co.kr/news/articleView.html?idxno=68307

[10] Chang, N.S., "Cybersecurity Threats, Counter Strategies and South Korea's Cyber Strategy," Journal of National Security and Strategy Vo.19, No.2, 2019, pp.1-33.

[11] Kim, K.S. and Shin, J.H., "Concept of operating unmanned ground combat system according to the aspect of future war," Defense & Technology, No.479, 2019, pp.62-75.

[12] Herbert C. Kemp., "Left of Launch: Countering Theater Ballistic Missiles," Atlantic Council, Washington, 2017.

[13] Scott D. Applegate., "the principle of maneuver in cyber operations," the 4th International Conference on Cyber Conflict 2012, IEEE, 2012, pp.1-13.

[14] Kim, N.U. and Eom, J.H., "Attack Path and Intention Recognition System for detecting APT Attack," Journal of the Korea Society of Digital Industry and Information Management, Vol.16, No.1, 2020, pp.69-80.

[15] Eom, J.H., Park, S.H., and Chung, T.M., "A Study on an Extended Cyber Attack Tree for an Analysis of Network Vulnerability," Journal of the Korea Society of Digital Industry and Information Management, Vol.6, No.3, 2010, pp.49-57.

■ 저자소개 ■

김 남 욱
(Kim, Nam Uk)

2012년 3월~ 현재
성균관대학교 컴퓨터공학과
박사과정
2012년 2월 성균관대학교 컴퓨터공학과(석사)
2009년 2월 성균관대학교 컴퓨터공학과(학사)

관심분야 : 네트워크/시스템 보안, 프로그래밍 언어
E-mail : nukim8275@gmail.com

엄 정 호
(Eom, Jung Ho)

2011년 3월~ 현재 대전대학교
군사학과&안전융합학부 부교수
2011년 2월 성균관대학교 정보통신공학부 BK21
연구교수
2008년 2월 성균관대학교 컴퓨터공학과(박사)
2003년 2월 성균관대학교 컴퓨터공학과(석사)
1994년 2월 공군사관학교 항공공학과(학사)

관심분야 : 네트워크/시스템 보안, 사이버전, 접근제어, 내부자보안
E-mail : eomhun@gmail.com

논문접수일 : 2020년 8월 27일
수 정 일 : 2020년 9월 3일
게재확정일 : 2020년 9월 9일