Regular paper

Journal of the KIECS. pp. 737-746, vol. 12, no. 5, Oct. 31 2017, t. 85, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.5.737

WB(Water-Bubble) 기반의 강한 보안성을 갖는 탄력적 네트워크 구간에 관한 연구

서우석*

A Study on WB(Water-Bubble) Based Highly Secure Flexible Network Section

Woo-Seok Seo*

요 약

2017년 통합보안(IS, Integrated Security), 융합 보안(CS, Convergence Security) 등과 같은 새로운 보안시장의 변화 속에서 운영과 관리 차원의 다양한 보안 패러다임이 제시되고 있다. 이러한 솔루션과 기술은 현존하는 네트워크 인프라의 변경과 유동적인 다차원적인 변화를 이끌어 내기보다는 보안성을 높이는 1차원적인 방어에 모든 보안 역량이 집중되어짐으로써 예상치 못한 침해와 장애를 지속적으로 내제하고 있는 네트워크 인프라를 유지해 오고 있다. 따라서 WB(Water-Bubble)이라는 새로운 아이디어를 네트워크 인프라에 접목하고 실험과 구현 기반의 분석을 진행함으로써 유사패턴 공격과 집중화 트래픽 공격을 방어할 수 있는 탄력적 네트워크 구간을 제안하고 개발할 수 있는 기회이기도 한다. 또한 본 논문에서 제안하는 WB 기반의 강한 보안성을 갖는 탄력적 네트워크 구간에 관한 연구기법은 공격의 최종 목적지로 예상되는 네트워크 영역을 울림 형태의 탄력적 영역변화를 갖는 네트워크 구간(구역)으로 유동성과 비예측성, 상호 접점비율에 따른 비 영역 확장성 등의 3대 주요 제한 및 보안 기준을 바탕으로 네트워크 구간 보안성 확보를 위한 연구 자료를 제공하고자 한다.

ABSTRACT

In 2017, amid changes in the security market such as integrated security (IS) and convergence security (CS), a variety of security paradigms in terms of operation and management have been suggested. Rather than changing existing network infrastructure and bringing about fluid, multi-dimensional changes, these solutions and technologies focus entire security capacity on a primary protection, leading to network infrastructure suffering from unexpected inherent violations and problems in a continued manner. Therefore, it is time to propose and develop a flexible network section that can protect from attacks of similar pattern and concentrated traffic attacks by applying a new concept of WB (Water-Bubble) to network infrastructure and analyzing on the basis of experiment and installation. Methodology of the WB-based highly secure flexible network section proposed in this study is expected to provide materials for studies on how to achieve network section security taking into account three major limitations and security standards: fluidity, unpredictability, and non-area scalability by contact point ratio, by changing a network area predicted to be the final target of attack into resonant network section (area) with flexible area changes.

키워드

Network Security, Logical Buffer Layer, Flexible Network
네트워크 보안, 논리적 버퍼 구간, 탄력적 네트워크

* 교신저자 : Security Consulting(Freelancer)

・접 수 일 : 2017. 07. 21
・수정완료일 : 2017. 08. 13
・게재확정일 : 2017. 10. 18

・Received : July 21, 2017, Revised : Aug 13, 2017, Accepted : Oct 18, 2017

・Corresponding Author : Woo-Seok Seo
Dept. Security Consulting, Gyeonggi-do R&D laboratory
Email : ssws2000@nate.com

Ⅰ. Introduction

With the consistent interests in information protection and the advancement in various technologies, computer problems and infringements through first-dimensional access have been reduced. The tendencies of attacks, however, started to adopt advance technologies just as defensive systems do. As the methods of attach and defense coexist, there are resources available to the public online. As to attacking tendencies, consistent attacks reveal and induce a problem of the object. Further, sophisticated attacking scenarios are prepared and demonstrated in advance to thoroughly materialize the attacking process. It is not that the advancement of defensive methods is in proportion to that of the attacking, black-hacking methods. It is certain, however, that as attacking techniques become ever more various, the information is available to the public mainly through the public networks. Hence, this study is to reconsider the current condition of the security markets being neglected as a physical network infrastructure, induce the new concept of Spring-AREA and suggest the virtual reality just as if one network is separated and operated as two different ones, and re-separate the network area for mutual exchange in order to secure a higher level of security and efficiency. As to the contents of this study, Chapter 2 analyzes actual cases of network infra infringement and the current condition of security technologies and network-based security products and solutions, home and abroad. Chapter 3 explains the composition of a WB(Water-Bubble) based elastic network of a higher level of security. Chapter 4 presents the experiment result of the suggested elastic network infra operation. Lastly, Chapter 5 presents the conclusion and issues for the future study.

Ⅱ. Related Researches

2.1 Actual Cases of Network Infra Infringement

On July 7, 2009, hundreds of thousands of PCs became 'zombie' computers with the third illegal attacking resources and attacked the major national network computing networks including governmental agencies and administration offices. Since then, other critical attacks have continued for the more than 4 years up to the year of 2017. While the infringement was limited to paralyzing the business affairs in the past, the effect is becoming more critical and complicated. Currently, efforts are united to solve critical infringements and the results are shared by promotion agencies to instill consciousness of information security. Accordingly, all companies are actively taking the lead of responding such infringements, which shows the advancing awareness in line with the advancement of security technology. Table 1 shows the reported cases of hacking incidents presented by Korea Internet & Security Agency, the infringement report agency, and the reports of malicious code attacks to wire and wireless network infrastructures from May 2016 up to the present[1]. Fortunately, the social influence of such critical infringements resulted in reflection effects of reducing the infringement rates. Now, how long this reflection effects could last is an important matter that would enhance the awareness of security.

Table 1. Reported hacking incidents and malicious code infections of each month (sample)

Month (2016)	Hacking Incidents	Malicious Code Infections
May	1,534	2,138
June	2,174	2,394
July	1,937	1,638
Aug	2,173	1,472
Sep	1,273	1,339
Oct	1,608	1,419
Nov	1,586	2,059
Dec	1,444	2,462

Table 2. Types and classification of network security technologies

Class	Description
Hardware	Physical security technology for network environments e.g. key encryption security, biometrics, etc
Software	VPN, IDS, IPS, Filtering, Scanner, Finder, Firewall, Web-Firewall, USB Security, LOG-Monitoring, Database Security, etc
Converge nce	CS(Convergence Security) that combines the hardware and software security technologies

2.2 Classification of Network Security Technologies

The security method suggested and experimented in this study forms 'Spring-AREA' between two different network infra areas for IP band conversion as a way of defensive mechanism.. Hence, the security technology over various types of networks as shown in Table 2 is divided to the three fundamental technologies - hardware, software, and convergence - to examine the definitions, usages, and objectives[2]. The physical type 1-dimensional security technology that adopts visual effects and confirmation advanced into the 3-dimensional security technology of logical information security rapidly. In the process, though, the procedure to maintain and manage the main infrastructure was omitted while the general system was developing. Hence, the area of network security is classified as one of various security technologies and categories rather than one portion of the specialized security markets such as information security or personal information security. It is necessary to separate as an area of security in the future[3].

The term, 'convergence,' is recognized as combining various heterogeneous networks from the basic set of signal information to large-scale network backbones for information exchange, and its use has become common. When used wrongly, however, it might seem to be a way of information presentation through one single network. In short, convergence means a future information technology that includes all behavioristic elements such as planning, management, and operation as well as technologies used to form a network[4].

2.3 Current Condition of Security Products and Solutions Home and Abroad

While the domestic information security markets are rapidly changing, there might be critical attacks that would not be detected only by domestic security technologies. Hence, it is necessary to introduce attacking and defensive methods from abroad, analyze them, and combine them with common domestic technologies to enhance the security level. Table 3 shows the objective situations such as trends in the security markets, home and abroad, available security products and solutions, market shares and ranks, and degree of integration[5-9].

Table 3. Network-based security products and solutions

Class	Domestic	Abroad
Trend	Convergence Security Market	Unified Security Market
Rank	Basic Infra Security Devices	Domestically, grades from "C" to "E"; Rather than new solutions such as Hybrid-Security, stability is focused on in realization of security products and solutions
Integ ration	High ~ Middle	Middle ~ Low
Mar ket	Market Size: 1 trillion; Growth Rate of Security Industry Per Year: 14.3	Entry into the Integrated Security Market

This study includes, as the basic data, investigation of the characteristics of the security markets that security agencies participate in, experiments and analysis of a higher level of security through the elastic network infrastructure suggested in this study.

Ⅲ. WB(Water-Bubble) Based Elastic Network Sections of a Higher Level of Security

The forms of networks being currently operated may be academically classified to LAN(Local Area Network), MAN(Metropolitan Area Network), and WAN(Wide Area Network). They also may be classified in terms of network-based composition and specific topology to Star, Bus, Ring, Mesh, and so forth. This study adopts the logical WB(Water-Bubble) based elastic Spring-AREA in actual environments that reflect all types of networks stated above. As an IP band internally divided and heterogeneous but externally represented as a physical form of fixed network infrastructure, this study suggests a defensive mechanism that causes no transformation of the network infrastructure.

3.1 Composition of WB(Water-Bubble) as a Layer of Logical Buffering

The term, 'logic,' in the definition is the key to understanding Spring-AREA of WB(Water-Bubble), which is the core technology suggested in this study. While general logics prove elements that virtual reality or visual methods would be unable to, the logic stated in this study designs a new composition of logic for the network with the existing physical network remaining and reset multiple IP bands with the designed access area as a buffering layer. The vertical kinetics when a small drop of water falls on the surface is represented horizontally as shown in Figure 1. In the Expression, however, the movement is divided to sub-areas with arithmetic and objective numbers with the exchange among areas as an intersection form of multiple networks.

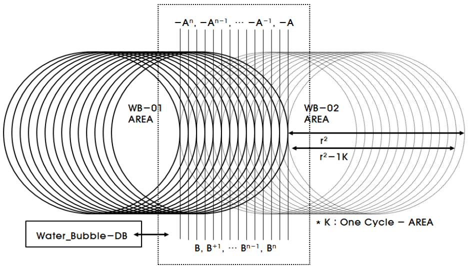

Fig. 1 Composition of WB(Water-Bubble) as a layer of logical buffering

One important factor in the transforming process of representing a physical reality into a logical expression is how the boundary of contacts could be formed since it could affect the area of the buffering area. The expression of the physical network area divisible into logical sub-areas should be separated as shown in Figure 2 and Figure 3 to confirm Spring-AREA.

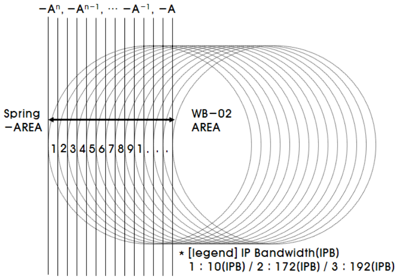
$-A^n, -A^{n-1}, \cdots -A^{-1}, -A$
Spring
-AREA
WB-02
AREA
1 2 3 4 5 6 7 8 9 1 . . .
* [legend] IP Bandwidth(IPB)
1 : 10(IPB) / 2 : 172(IPB) / 3 : 192(IPB)

Fig. 2 Composition of WB-02 area of WB(Water-Bubble)

Each step of Spring-AREA that belongs to the buffering area goes through mapping to a three-layered round structure as in 10, 172, and 192, each private IP band. Hence, The totaling of IP bands to be provided and mapped depends on into how many network pieces the buffering layer, Spring-AREA, will be divided into. The proper, standardized quantity of division determined in an experiment should be presented. Spring-AREA suggested in this study consists of heterogeneous buffering layers, which will be mapped into each network area, and the total number is limited to 10.

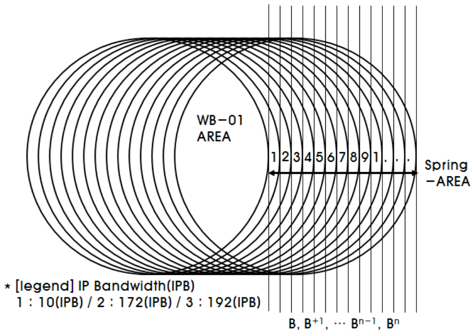
WB-01
AREA
1 2 3 4 5 6 7 8 9 1 . . .
Spring
-AREA
* [legend] IP Bandwidth(IPB)
1 : 10(IPB) / 2 : 172(IPB) / 3 : 192(IPB)
$B, B^{+1}, \cdots B^{n-1}, B^n$

Fig. 3 Composition of WB-01 area of WB(Water-Bubble)

3.2 Composition of and Limitations to Elastic Network Areas

To generate a buffering layer for WB-01 AREA and WB-02 AREA, the two heterogeneous network areas, different physical networks are formed and new Spring-AREA is created. In this process, the limited section for the final composition of an elastic network is reflected as in Table 4. When a limited area is separated on the basis of WB-01 AREA, the entire section of Spring-AREA from WB-02 AREA B to B+9 is reflected as the -A Spring-AREA network mapping area of WB-01 AREA. Except this area, a certain section of Spring-AREA that can be operated in the limited condition of sequence area mapping is in inverse proportion.

Table 4. Composition of and limitations to elastic network areas

Class	AREA		Limited Section
	WB-01	WB-02	
Limit ations	-A	B, B+1, B+2, B+3, B+4, B+5, B+6, B+7, B+8, B+9	ALL
	-A-1	B, B+1, B+2, B+3, B+4, B+5, B+6, B+7, B+8	9
	-A-2	B, B+1, B+2, B+3, B+4, B+5, B+6, B+7	8
	-A-3	B, B+1, B+2, B+3, B+4, B+5, B+6	7
	-A-4	B, B+1, B+2, B+3, B+4, B+5	6
	-A-5	B, B+1, B+2, B+3, B+4	5
	-A-6	B, B+1, B+2, B+3	4
	-A-7	B, B+1, B+2	3
	-A-8(9)	B, B+1(B)	2(1)

Basically, as for a network composition by means of an elastic buffering layer, the areas that would be overlapped when the two networks completely coincide are limited rather than the two heterogeneous network areas are combined. Thus, the applicable area is 1/2 of original Spring-AREA. For the linkage of two sections of Spring-AREA, the study suggests the Spring-AREA Mapping algorithm as shown in Figure 4 as a lower implementation class. Rather than a technical foundation to develop a separate analysis algorithm, this is a step of standardizing the environments to connect two heterogeneous physical networks.

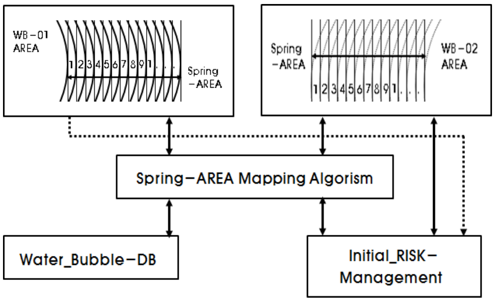

Fig. 4 Mapping & RISK management of WB(Water-Bubble)

3.3 Rates of Securing Flexibility in the Network Sections

The plan to form an elastic network has been already suggested, and based on it, the rates of flexibility of WB-01 AREA and WB-02 AREA are presented in Table 5 for the standardization for effective Spring-AREA operation. The values shown in the table are the basis for which band of IP would be used and what form of process and procedure would be used in creating a separate logical network for the buffering layer of Spring-AREA. In this study, 10, 172, and 192 of the private IP bands that exist from 1 to 3 go through the roofing in the consecutive order, but the way of selection may be a random type. Since the table structure involves a key to generate Spring-AREA, various forms could be suggested flexibly. Although the encryption key in case of a third party's access to the network is also formed differently, a key that could be blocked may be used in case of infringement attempts intended for selection and analysis.

Ⅳ. WB(Water-Bubble) Based Elastic Network Sections of a High Level of Security

4.1 Experiment Environments

A third party's channels of attack are divided to three in terms of orientation as shown in Figure 5 #1 WB-02 AREA, #2 WB-01 AREA, and the two physical networks are logically changed into Spring-AREA, which involves an area that can be possibly attacked. In this experiment, the intent is not to calculate the infringement possibilities and estimates with various attacks tried and to suggest a defensive method to block accesses without permission. In other words, for Spring-AREA, the buffering layer created while the physical network was logically changed, when the area was exposed to a simple access rather than a type of attacks without a policy of channel forwarding permission, it was viewed as an area that could be attacked. In addition, the accessibility depending on the security settings to defend a single network and the accessibility in the suggested final experiment environment were comparatively and objectively assessed in terms of time and number of attempts.

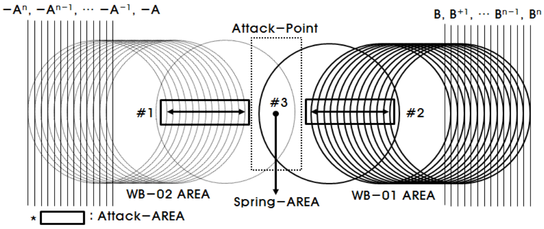
$-A^n, -A^{n-1}, \cdots -A^{-1}, -A$
$B, B^{+1}, \cdots B^{n-1}, B^n$
Attack-Point
#1
#3
#2
WB-02 AREA
Spring-AREA
WB-01 AREA
★ ▭ : Attack-AREA

Fig. 5 Experiment environments

4.2 Analysis of Rates of Securing WB(Water-Bubble) Sections

As one of the results from the access control experiment, the rates of accessible areas of WB(Water-Bubble) were determined based on the area combination as shown in Table 6.. This shows the compositions of Spring-AREA accessible depending on the access attempts. The areas with values gained in the certain conditions were counted in the rates of accessibility. Hence, the experiment result of the first access control over WB-01 AREA ∪ WB-02 AREA will be expanded to the future study, in which the range of access control is to be minimized for the highest and optimal level of security in Spring-AREA.

Table 5. Rates of securing flexibility in the network section

WB-01 AREA WB-02 AREA	-A	-A-1	-A-2	-A-3	-A-4	-A-5	-A-6	-A-7	-A-8	-A-9
B+9	NON	1	2	3	1	2	3	1	2	3
B+8	NON	NON	1	2	3	1	2	3	1	2
B+7	NON	NON	NON	1	2	3	1	2	3	1
B+6	NON	NON	NON	NON	1	2	3	1	2	3
B+5	NON	NON	NON	NON	NON	1	2	3	1	2
B+4	NON	NON	NON	NON	NON	NON	1	2	3	1
B+3	NON	NON	NON	NON	NON	NON	NON	1	2	3
B+2	NON	NON	NON	NON	NON	NON	NON	NON	1	2
B+1	NON	NON	NON	NON	NON	NON	NON	NON	NON	1
B	NON	NON	NON	NON	NON	NON	NON	NON	NON	NON

Table 6. Analysis of rates of securing elastic sections

Class	AREA	SUM	WB-01 AREA ∪ WB-02 AREA
Combination of Sections	10 Bands	22	-A-1(B+9), -A-2(B+8), -A-3(B+7), -A-4(B+6), -A-5(B+5), -A-6(B+4), -A-7(B+3), -A-8(B+2), -A-9(B+1), -A-4(B+9), -A-5(B+8), -A-6(B+7), -A-7(B+9), -A-7(B+6), -A-8(B+8), -A-8(B+5), -A-9(B+7), -A-9(B+4)
	172 Bands	15	-A-2(B+9), -A-3(B+8), -A-4(B+7), -A-5(B+9), -A-5(B+6), -A-6(B+8), -A-6(B+5), -A-7(B+7), -A-7(B+4), -A-8(B+9), -A-8(B+6), -A-8(B+3), -A-9(B+8), -A-9(B+5), -A-9(B+2)
	192 Bands	14	-A-3(B+9), -A-4(B+8), -A-5(B+7), -A-6(B+9), -A-6(B+6), -A-7(B+8), -A-7(B+5), -A-8(B+7), -A-8(B+4), -A-9(B+9), -A-9(B+6), -A-9(B+3)

4.3 Determination and Analysis of an Algorithm for the Operation of Elastic Network Sections

For the algorithm for the operation of elastic network sections, WB-01 AREA=Elastic Network#1 and WB-01 AREA=Elastic Network #2 are suggested. How to represent heterogeneous networks with the minimal algorithm operation process and how to apply and operate the process flow are presented in a format of algorithm to determine the direction of the virtual simulation.

```
* WB-01 AREA=Elastic Network #1
  START
     Roof(-A, -A-1, -A-2, -A-3, -A-4, -A-5, -A-6, -A-7, -A-8, -A-9)
     Load(Water_Bubble-DB)
     RUN=Spring-AREA Mapping
     RUN=Initial_RISK-Management
      Select= {Spring_AREA || detail_AREA}
      Operation_line="select"
      Breakup=traffic_rate .and. attack_rate
  END
```

```
* WB-02 AREA=Elastic Network #2
  START
     Roof(B, B+1, B+2, B+3, B+4, B+5, B+6, B+7, B+8, B+9)
     Load(Water_Bubble-DB)
     RUN=Spring-AREA Mapping
     RUN=Initial_RISK-Management
      Select= {Spring_AREA || detail_AREA}
      Operation_line="select"
      Breakup=traffic_rate .and. attack_rate
  END
```

The range of Roof in each algorithm was set to the total area, and the divided Spring-AREA was examined thoroughly to calculate the accurate interval function.

Table 7. Result of applying the WB(Water-Bubble) based elastic network sections

Class	SUM	Sucess Rate[%]	WB-01 AREA ∩ WB-02 AREA
Combination of Secured Sections	22	18.48	-A-4(B+6), -A-4(B+9) -A-5(B+5), -A-5(B+8) -A-6(B+4), -A-6(B+7) -A-7(B+3), -A-7(B+9), -A-7(B+6) -A-8(B+2), -A-8(B+8), -A-8(B+5) -A-9(B+1), -A-9(B+7), -A-9(B+4)
	15	11.85	-A-5(B+9), -A-5(B+6) -A-6(B+8), -A-6(B+5) -A-7(B+7), -A-7(B+4) -A-8(B+9), -A-8(B+6), -A-8(B+3) -A-9(B+8), -A-9(B+5), -A-9(B+2)
	14	12.04	-A-6(B+9), -A-6(B+6) -A-7(B+8), -A-7(B+5) -A-8(B+7), -A-8(B+4) -A-9(B+9), -A-9(B+6), -A-9(B+3)

4.4 Result of Applying the WB (Water-Bubble) Based Elastic Network Sections

The initial rates of accessibility to the sections were determined based on the analysis of rates of securing elastic sections. However, whether the resulting values drew out the proper rates for each IP band was not certain. Hence, the second application of the WB(Water-Bubble) based elastic network sections as shown in Table 7 was analyzed to enhance the accuracy based on the objective figures.

The second analysis was not merely to support the result of the first analysis. Rather, the two results are combined to apply and embody the suggested method to perfection.

Ⅴ. Conclusion

Based on the composition and operation of objective values such as a series of Spring-AREA Mapping algorithms, limitations, and adjustment rates to readjust the existing physical network infra areas into an elastic, echoing, transformative network infrastructure, this study suggests a method to provide services in a stable network infrastructure as well as prevent attacks such as external pattern attacks and generation of physical loads as full as possible. As for the logical Spring-AREAs - WB-01 AREA and WB-02 AREA, the most important with regard to the suggested method, the limits of elastic operation are determined and the Sucess Rate(%) of embodying multi-dimensional layer networks is also calculated so that the possible combinations of converting physical networks into logical IP bands can be confirmed through the experiment. The future study will suggest and embody the method in a virtualized, logical experiment environments. In reflection of the limitations when it comes to the higher efficiency of objective operation and a higher level of security, it is necessary for the future study to apply the method in various actual environments of low physical efficiency and weakness in terms of defense as well as secure transparency of the process by reconfirming the results.

References

[1] J. Shin, “Economic Analysis on Effects of Cyber Information Security in Korea: Focused on Estimation of National Loss,” *J. of the Korean Institute of Information Security and Cryptology*, vol. 23 no. 1, 2013, pp. 89-96.

[2] S. Paik, S. Kim, and H. Park, “Design and Implementation of Network Access Control for Security of Company Network,” *Journal of the Institute of Electronics Engineers of Korea*, vol. 47, no. 12, 2010, pp. 90-96.

[3] K. Kim, Y. Park, S. Ro, and B. Kim, “Design of Infringement Accidents Preventing System Using DNS Information Retrieval Integration Method,” *J. of the Korea Institute of Information and Communication Engineering*, vol. 16 no. 9, 2012, pp. 1955-1962.

[4] M. C. Park, Y. S. Park, Y. R. Choi, “A Study on the Active Traceback Scheme Responding to a Security Incident,” *J. of the Korea Society of Computer and Information*, vol. 10, no. 1, 2005, pp. 27-34.

[5] D. Kim, Y. Jeong, G. Yun, H. Yoo, S. Cho, G. Kim, J. Lee, H. Kim, T. Lee, J. Lim, and D. Won, “Threat Analysis based Software Security Testing for preventing the Attacks to Incapacitate Security Features of Information Security Systems,” *Korea Institute of Information Security and Cryptology*, vol. 22 no. 5, 2012, pp. 1191-1204.

[6] J. Ko, H. Kwak, J. Wang, H. Kwon, and K. Chung, “An Improved Signature Hashing Algorithm for High Performance Network Intrusion Prevention System,” *Korea Institute of Information Security and Cryptology*, vol. 16C no. 4, 2009, pp. 449-460.

[7] J. Hoon, “A Study on The Vulnerabilities and Problems of Security Program,” *J. of Convergence Security*, vol. 12 no. 6, 2012, pp. 77-84.

[8] Y. Lee, “A Design and Analysis of Multiple Intrusion Detection Model,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2016, pp. 619-626.

[9] K. Kim, D. Wang, and S. Han, “Home Security System Based on IoT,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 8, 2016, pp. 743~750.

저자 소개

서우석(Woo-Seok Seo)

Received his M.S. and Ph.D degrees in Computer engineering from University of Soongsil, Korea, in 2013. His research interests include Network Security, Network Infra Design, Computer Network Algorithms, and Network Protocol.