Regular paper | Journal of the KIECS. pp. 1155-1160, vol. 13, no. 6, Dec. 31 2018, t. 92, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.6.1155

서비스 기반 정보시스템의 안정성 증대를 위한 보안정책 최적화 균형모듈에 관한 연구

서우석*

A Study on the Optimized Balance Module of Security Policy to Enhance Stability in the Service-Based Information System

Woo-Seok Seo*

요 약

2018년 현재 보안시장은 새로운 변화와 기술들로 인해 보안분야의 진보적인 발전과 혁신이 필요한 시점으로 도래되고 있다. 이는 빠른 서비스 기반의 정보시스템과 서비스 플랫폼의 비약적인 발전을 말하기도 한다. 따라서 본 논문에서는 다양한 서비스가 존재하는 온라인 상에서 특정한 서비스를 선정하는 기준이 아닌 다수의 서비스를 운영하고 보안성을 확보하는 과정을 대상으로 정보시스템들이 운영하는 플랫폼에 대한 관리자의 접근권한을 보호하고 서비스 제공부터 파기까지의 일련의 흐름 속에서 불법적인 침해와 접근이 가능한 영역과 해당 영역에 대한 보안을 위해 최적화 균형모듈을 전체 서비스 플랫폼에 최대 4가지 분류로 제한하고 제한된 보안영역에 대해서는 각각 또 다시 하위 보안정책과 기술 적용을 함으로써 정보시스템의 안전성과 보안성을 제공하고 확대하기 위한 기법과 이를 적용하는 과정을 제안한다.

ABSTRACT

Presently in 2018, the security market is requiring progressive development and innovation in the area of security on account of new changes and technologies. This means the rapid and prompt development of the service platforms and service-based information systems. Here, this study is going to examine the process of operating a number of services and obtaining security, not the criteria for selecting particular service in online environment where the various services exist. Within a series of flows to protect the manager's authority about the platforms operated by information systems, and to provide and destroy services, this author limits the entire service platforms of the optimized balance module into four categories maximum for the security of the area apt for illegal invasion and access, and the proper area. Also, about the area with limited security, this researcher again applies subordinate security policy and technology respectively. This author here will suggest a method to provide and to extend safety and security for the information system and also propose the process of applying it as well.

키워드

Availability, Balance Module, Information Security, Optimization, Security Policy, Stability
균형 모듈, 정보 보안, 최적화, 보안 정책, 안정성

* 교신저자 : Security Consulting(Freelancer)
• 접 수 일 : 2018. 07. 26
• 수정완료일 : 2018. 10. 05
• 게재확정일 : 2018. 12. 15
• Received : Jul. 26, 2018, Revised : Oct. 05, 2018, Accepted : Dec. 15, 2018
• Corresponding Author : Woo-Seok Seo
Dept. Security Consulting, Gyeonggi-do R&D laboratory
Email : ssws2000@nate.com

Ⅰ. 서 론

21세기 통신분야 인프라를 기반으로 하는 서비스 정보시스템의 활용과 방향은 그 영역의 범주가 측정이 불가능할 정도의 영역인 가운데 많은 정보의 생성으로부터 가공 그리고 최종 파기 또는 저장에 이르는 절차적인 흐름이 발생하고 있다. 이러한 일련의 과정속에서 각 단계별 정보에 대한 서비스와 검증 그리고 제공 등의 안정성을 확보하고 이를 보존하기 위한 방안으로 본 논문과 같은 정보보안의 안전성 확보를 위한 다양한 정책과 기법들이 제시되고 있는 상황이다[1-2].

따라서 본 연구과정도 서비스를 기반으로 하는 정보시스템에게 있을 수 있는 정보 침해에 대한 적절한 방어와 사전 점검 등 검증을 위한 기술적 제안으로 보안정책에 대한 최적화 균형모듈에 관한 연구를 제안하고 있다. 물론 현재 신기술로써 시장에서 많은 변화와 발전을 보이는 IoT(: Internet of Thins), ICT(: Information and Communications Technologies)와 같은 기술에 대한 접근점과 접근에 따른 보안성 확보와 연계를 위한 접점도 확인해야 할 과제이기도 하다[3]. 따라서 본 논문에서는 소규모 기업으로부터 대규모 기업 및 기관에 이르기까지 모든 정보보안 정책 기본으로 제시가 가능한 조건의 모듈로 구성하기 위해 정보보안의 주요 핵심 사항 중에 하나인 가용성 기반의 정보보안 최적화 균형모듈에 관한 연구기법을 제안하고자 한다[4-5]. 이와 같이 제안되어지는 논문상의 기술 및 정책적 제안에 대한 기술을 1장에서는 연구방향과 목적 그리고 시장상황 등을 언급하고 연구를 위한 전반적인 개요를 기술하고자 하며, 2장에서는 관련연구로써 온라인 서비스 제공 정보시스템에 대한 운영현황 및 현행 적용중인 보안정책 등에 대한 상황을 기술하고 3장에서는 정보시스템의 안정성 증대를 위한 보안정책 최적화 균형모듈 제안을 위한 구성환경과 균형모듈 기준을 제시하고자 한다. 또한 4장에서는 정보시스템 플랫폼 보안정책 적용에 따른 최적화 균형모듈 설계의 보안수준 검증을 위한 내용을 제시하고 마지막으로 결론을 도출하는 과정으로 연구방향과 논문의 내용을 제시하고자 한다.

Ⅱ. 관련연구

제안하고 논증 및 검증하고자 하는 본 논문의 기초자료로써 활용되어질 관련연구 과정에서 제시하고 있는 연구목적의 결과를 반영하고 현실에서 활용하게 될 기업과 기관이 보유한 서비스 기반 정보시스템의 운영 탬플릿에 대한 안전성을 확보하고 또한 최적화 보안정책 부문 가용성을 반영하고 이로 인해 발생 가능한 취약점과 정보보안의 침해를 제거함으로써 연구하는 목적과 방향에 맞는 최종 결론을 도출하기 위한 기초자료를 확보하는 중요 연구자료 들을 기술하고자 한다[6-8].

2.1 온라인 서비스 제공 정보시스템 운영현황

공중망을 통한 온라인 주요 서비스 범주를 구성한다면, 표 1과 같이 금융, 산업, 물류, 교육, 통신과 같이 구분이 가능하다. 물론 이외의 다양한 산업형태와 시장이 있으나, 본 논문에서는 해당 범주를 기준으로 하는 최적화 보안정책을 구현하기 위한 균형 모듈을 제시하고자 한다[9]. 이외의 추가적인 연구 또한 향후 지속적인 데이터의 부적합 및 적합 결과에 대한 표준화를 통해 대상을 확대함으로써 가능할 것이며, 본 논문에서는 주어진 범주에 따른 정보보안의 정책을 적용하고 구현 가능한 서비스로 다시 분류함으로써 제공되는 서비스의 플랫폼에 따른 최대 안정성과 가용성 확보를 가진 균형 모듈 보안정책 현황을 도식 가능하다[10].

표 1. 온라인 정보운영과 활용을 위한 서비스 제공형태의 정보시스템 현황
Table 1. Information system in the form of providing service for online information operation and utilization

Classification	Operating system	Service provided
Finance	Transaction system	Company-specific specialization services
Industry	Internal ERP system	Integrated internal management of enterprises
Logistics	Logistics management system	RFID, NFC
Education	Personnel management system	internal institutional management services
Communication	Communication linkage system	ommunication records management

2.2 주요 취약점 침해와 공격형태의 변화

네트워크와 시스템을 중심으로 공격과 침해의 종류는 이미 대외적으로 공개되고 오픈 소스를 활용한 변형된 공격까지도 많은 부분에서 방어를 위한 정책에 이미 포함되어진 상태이지만, 아직까지도 지속적인 공격의 형태와 침해의 종류는 표 2와 같이 발전되고 있다. 따라서 이러한 공격에 대한 정의와 형태를 파악하고 정의된 조건을 두고 제안하는 보안정책의 균형 모듈 범주로 재 분할하고 재 정의함으로써 접근된 침해의 방어와 공격을 1:1 대칭시킴으로써 자동화된 접근과 방어가 가능하다[11-12].

표 2. 네트워크 경로 접근 및 시스템 취약점 종류
Table 2. Network path access and system vulnerability types

Classification	Type of Infringement
Network	Zerbo, Klez, MITM, SSL Strip, Syn Flooding, DoS, DDoS, Session hijacking
System	Spyware, Adware

2.3 정보보안 대비 침해 공격과의 대립과 일반적 보안정책의 방향

정보보안 대비 침해공격의 종류는 무수히 많으나 이러한 공격에 대한 일반적인 방어 정책과 보안을 위한 물리적이고 논리적인 방어 기능 또는 기기들 그리고 소프트웨어는 표 3과 같이 서비스를 기반으로 하는 정보시스템을 기준으로 네트워크 접근 공격에 대한 방어기기들을 일상적인 네트워크 인프라 구성 기기들로써도 충분히 침해를 제어 가능할 것으로 판단하기도 한다. 그러나 불규칙하고 불특정한 접근 침해는 예측을 벗어나는 패턴을 보이고 있어서 이러한 패턴의 형태까지도 표준화된 방어 정책의 데이터베이스로 활용 가능한 균형 모듈 방어기법을 제안하는 것이다.

표 3. 정보시스템 접속을 위한 네트워크 경로 기반의 공격현황
Table 3. Network path based attacks for information system access

division	Network defense devices	Used
Information system	Switch	Access list function with router function Switch operation
	Router	Application of security functions such as utilization of private IP band for router network area separation
	Firewall	Perform firewall self packet security
	WEB Firewall	Illegal access defense of web fire
	Filtering	Filter defense to prevent packet and information distortion
	UTM	Comprehensive security management that combines multiple security solutions together to reduce costs and minimize management complexity
	Etc	Operate other security equipment

III. 정보시스템의 안정성 증대를 위한 보안정책 최적화 균형모듈 제안

대외 및 대내를 대상으로 하는 기업마다 보유한 정보시스템의 경우 최초 정보를 생성하고 이를 라이프사이클에 준하는 과정에 맞추어 관리하는 경우와 이관된 정보를 활용하는 단계, 단순 연계되는 상태 등 다양한 구성현황을 보이고 있으나, 이러한 구성현황들에 제한되지 않고 표준화된 정책으로 정보보안을 위한 표준 모듈로 제안이 가능한 카테고리를 구성하는 균형모듈을 적절하게 제안하는 부분이 가장 큰 본 논문의 결과를 극대화할 수 있는 방안으로써 이를 모색하고자 한다.

3.1 정보시스템 서비스 플랫폼 보안영역 분류와 구성환경

정보시스템을 활용하기 위한 두 가지 접근 형태인 네트워크와 시스템 인프라를 축으로 하여, 4가지 환경과 연계방안을 제시하고 이를 정보보안을 구성하는

제안하는 균형모듈의 4가지 축으로 구성한다. 우선 네트워크와 시스템으로 물리적인 환경을 4가지 일체의 환경 구성 인자를 대상으로 하는 균형모듈의 범주를 선정하고 네트워크와 시스템 범주를 활용하고 연계 및 상호 호환성을 그리고 가용성을 극대화 하는 단계인 연결과 연계 그리고 정보의 생성과 파기까지의 라이프사이클의 호환성을 또 다른 균형모듈의 두 가지 범주로 총 4가지 확정 영역으로 구성을 표 4와 같이 제시한다.

표 4. 정보시스템 서비스 플랫폼의 4가지 보안영역 분류
Table 4. Classification of 4 security areas of information system service platform

Classification	Security Platform Area
Network Security Policy and Configuration	Steps to define all the functions and technologies of the policy and configuration steps for network security
System Security Policy and Configuration	Steps to define all the functions and technologies of the policy and configuration steps for system security
Other information system linkage information Security Policy and Configuration	Defining all the functions and technologies of the policy and setting-up phase for network and system-linked security
Information, General Data and Personal Data Security Policy and Configuration	Defining all the functions and technologies of the policy and the setting process for security from the information generated from the network and the system to the destruction

3.2 정보시스템 서비스 기반의 안정성 증대 보안정책 균형모듈 기준

대외 또는 대내 기업의 특정한 성과 또는 결과와 행위의 실체를 확인하기 위한 서비스 기반의 정보시스템의 운영에 있어서 정보보안의 안전성을 확보한 가운데 가용성과의 적절한 대칭 비율을 보존하는 가운데에 보안정책의 균형모듈을 그림 1과 같이 4가지 방향성을 가진 표준화 보안정책 모듈 중 하나인 System Security Policy and Configuration 환경에 대한 서비스 기반의 안정성 증대 보안정책 균형모듈 기준의 적용환경을 제시하고 있으며, 이는 다른 3가지 환경 조건에도 동일하게 구성하고 환경을 제시 가능하다.

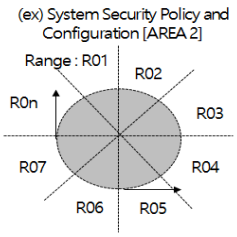

그림 1. 서비스 기반의 안정성 증대 보안정책 균형모듈 기준 적용환경
Fig. 1 Service-based stability enhancement Security policy balance module standard application environment

특정한 한 범주의 정보보안 균형모듈의 일부를 구성하는 부분에 있어서 대분류의 보안 정책을 기준으로 하위에는 그 범주를 R01로부터 Rn(n은 정수)까지 그 한계를 두지 않고 제안이 가능하지만, 본 논문에서 최종 제안하는 균형모듈을 향후 지속적으로 적용함으로써 최적화된 결과가 도출될 수 있는 조건의 범주를 확인하고 향후 개선 방안으로 제시하고자 한다.

Ⅳ. 네트워크 기반의 공개 정보자산과 접근권한에 따른 보안성 검증

제안하고 연구하는 과정인 서비스 기반 정보시스템의 안전성 증대를 위한 보안정책 최적화 균형모듈에 관한 연구에서는 균형모듈과 가용성에 중점을 두고 정보보안의 수준 등급이 상향조정됨에 따른 가용성의 현저한 저하가 발생하는 등의 서비스 불균형을 배제하고 최적의 비율과 환경을 구축하기 위한 설계와 기준이 검증되어야 한다.

4.1 보안정책 기반의 최적화 균형모듈 구성 검증

정보보안을 위한 적극적인 침해 방어 방법으로는 그 범주가 정해진 경우보다는 쓰임과 기능에 따라 기술의 한계는 끝이없는 상황이다. 다만 해당 기술들을 정책적으로는 기술의 기능에 따른 분류 정도는 이루어지고 있으나, 공격과 침해에 따라 자동화된 균형모듈을 이용한 실시간 방어 구성환경을 적용하는 경우

는 많지 않다. 단순히 외부 망으로부터 최초 연결되는 부분의 라우터를 기반으로 라우터 만의 방어정책 설정, 이후 방화벽, 웹방화벽 등 방어를 위한 기기마다 솔루션 마다의 각각의 보안정책을 중복 또는 교차 하는 등의 정책적 균형모듈화하여, 적용하지는 않고 있으며, 중복이 되든 단일 방어가 되든 각 기기와 솔루션마다의 성과만을 확인하고 방어를 완수한 것으로 판단하는 경우가 가장 기본적인 침해방어 전략 또는 정책으로 확인되기도 한다.

따라서 이러한 다수의 방어전략과 정책 및 기능을 4가지의 환경설정 영역으로 구성하고 이를 다시 각 정책별 구성영영의 성격을 별도로 정의함으로써 다수의 방어와 침해전략을 다시 적용하는 등의 다단계 방어와 순환방어를 기본으로 하는 균형모듈을 제시하고 구현한다. 최종 순환된 균형 모듈의 검증은 특화된 공격과 침해의 시나리오를 구성함으로써 공격과 방어를 통한 환경 값으로 그 검증이 가능하다. 다만, 다수의 시나리오 환경에 대한 적용은 향후 개선 방안으로 지속적인 연구가 필요한 상황이다.

4.2 정보시스템 구동에 따른 보안수준 향상을 위한 구현

네트워크 보안 정책 환경설정 부문과 시스템 보안 정책과 환경설정 그리고 주변 연계 시스템 등과의 정보 연결, 최초 생성으로부터 최종 파기까지 서비스 기반의 정보시스템이 보유하는 다양한 형태의 정보와 데이터베이스로 4가지 대분류를 두고 각 카테고리마다 방어와 침해에 관한 공격적 성향과 방법 등을 인식하고 이를 방어하기 위한 상호 4가지 영역의 균형적 방어 비율 값을 책정함으로써 정보보안의 모듈을 구성한다. 이러한 정책적 분류는 다소 많은 부분의 정보보안이 필요한 상황에서 활용 가능하고 안전성과 가용성 확보에 주된 기준과 보안수준을 향상하는 구현으로 진보 가능하다.

4.3 보안수준 검증에 따른 보안정책 균형모듈 기준 지표

서비스 기반 정보시스템을 운영하는 플랫폼에 대한 관리자의 권한 또는 사용자의 활용에 대한 접근권한을 보호하고 서비스 제공에 따라 생성되고 최종 파기되는 정보에 대한 기존 보안척도 지표에 대해 객관적인 정량적 안전성 증대 수치 값과 하나의 정보시스템 서비스 보안을 위해 적용한 보안기술과 정책에 대한 최적화 균형모듈을 그림 2와 같이 전체 서비스 플랫폼에 최대 4가지 분류로 제한하고 제한된 보안영역에 대해서는 각각 최소한 2개 이상의 보안정책과 기술을 적용하여 전체 정보시스템 운영에 따른 안전성과 보안성을 제공한다.

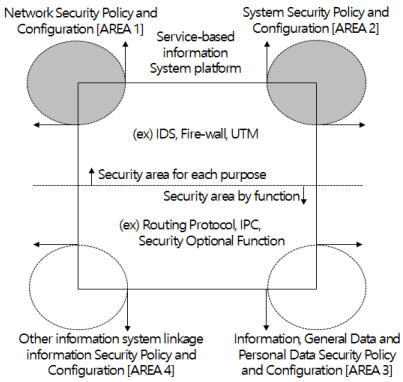

그림 2. 서비스 기반 정보시스템 플랫폼 보안정책 적용에 따른 최적화 균형모듈 설계
Fig. 2 Design of optimization balance module according to application of service-based information system platform security policy

V. 결 론

본 연구논문에서는 네트워크 통신기반의 다양한 서비스 플랫폼을 제공하고 이를 활용하는 다수의 사용자들을 위한 정보시스템의 정보보안 안전성을 확보함으로써 해당 시스템에 정보가 생성되면서부터 최종 파기 또는 저장되어지는 순간까지의 과정 속에서 보안정책의 최적화 균형 모델을 제안하는데, 목적을 두고 연구를 지속적으로 추진했다. 모든 기업과 기관에서 통신 기반의 환경을 모두 공개하고 있지는 않으나 공통적으로 확인 가능한 정도의 수준과 배경을 기준으로 연구과정을 진행했다. 따라서 본 논문이 표현하고 그 결과를 도출함으로써 제시하고자 하는 목적인 안전성 확보 기준의 정보시스템 서비스 플랫폼에는 반드시 정보보안을 위한 최적화된 균형모듈을 적용함으로써 극대화 할 수 있음을 제시하고 있다.

본 논문의 연구결과를 바탕으로 이후 연구과정은

일반적인 통신환경에서 서비스를 제공하는 기업과 기관들을 대상으로 실제 운영하는 환경에 일부 반영하고 이에 따른 적용 결과에 대한 표준편차를 확보하는데, 2차적인 목표를 두고자 한다. 추가적인 연구 방향으로는 서비스 분야에서 요구되어지는 정보보안의 주요 요소인 가용성을 준수하는 범주에서의 정보보안의 안전성 확보라는 주제까지 확대연구가 이루어져야 한다.

References

[1] J. Hom, S. Heon, and T. Mhung, "A Sudy on an Extended Cyber Attack Tree for an Analysis of Network Vulnerability," *J. of the Korea Society of Digital Industry and Information Management*, vol. 6, no. 3, Sept. 2010, pp. 49-57.

[2] J. Jang, D. Mim, and C. Jhoi, "Study on Hybird Type Cloud System," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, June 2016, pp. 611-618.

[3] S. Park and N. Kim, "A Verification Csae Study about the Authentication of a Network using AAA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 2, Apr. 2017, pp. 295-300.

[4] J. Song, B. Kim, and H. Kim, "A Design of A Modbus Application Protocol for Multiple SCU Connections," *J. of the Korea Academia-Industrial cooperation Society*, vol. 19, no. 4, Apr. 2018, pp. 642-649.

[5] H. Choi and Y. Cho, "Analysis of Security Threats from Increased Usage of Mobile App Services," *J. of the Korea Society of Digital Industry and Information Management*, vol. 14, no. 1, Mar. 2018, pp. 45-55.

[6] I. Kim, H. Lim, D. Ji, and J. Park, "A Efficient Network Security Management Model in Industrial Control System Environments," *J. of the Korea Academia-Industrial cooperation Society*, vol. 19, no. 4, Apr. 2018, pp. 664-673.

[7] B. Cha, S. Park, and J. Kim, "Prototype Design of Hornet Cloud using Virtual Honeypot Technique," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 8, Aug. 2015, pp.891-900.

[8] Y. Shin, S. Han, I. Jae, and J. Lee, "A Study on the Linkage between Intelligent Security Techno.logy based on Spatial Information and other Technologies for Demonstration of Convergence Technology," *J. of the Korea Academia-Industrial cooperation Society*, vol. 19, no. 1, Jan. 2018, pp. 622-632.

[9] K. Kim, D. Wang, and S. Ban, "Home Security System Based on IoT," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 1, Feb. 2017, pp. 147-154.

[10] Y. Hee, Y. Seo, and W. Kim, "Hardware Implementation for High-Speed Generation of Computer Generated Hologram," *J. of the Korea Society of Digital Industry and Information Management*, vol. 9, no. 1, Mar. 2013, pp. 129-139.

[11] J. Lee and J. Lee, "Efficient Hierarchical Mobility Management Scheme for Mobile Content Centric Networking," *J. of the Korea Academia-Industrial cooperation Society*, vol. 19, no. 2, Feb. 2018, pp. 37-41.

[12] S. Jung, D. Kum, and S. Choi, "Channel Grade Method of multi-mode mobile device for avoiding Interference at WPAN," *J. of the Korea Society of Digital Industry and Information Management*, vol. 11, no. 3, Sept. 2015, pp. 91-98.

저자 소개

서우석(Woo-Seok Seo)

2006년 숭실대학교 정보과학대학원 정보통신융합학과 (공학석사)
2013년 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
2006년 ~ 2012년 서울특별시용산구시설관리공단 전산총괄
2012년 ~ 2017년 주식회사 이지서티 보안사업본부 본부장(이사), 개인정보보호센터 센터장(이사)
2017년 ~ 현재 시큐리티 컨설팅(Freelancer)
※ 관심분야 : 4차 산업, ICT, IOT, 정보경영, 정보보안, 개인정보, 비식별화, 정보화 전략기획(ISP), 정보화 관리체계, 실태점검, 빅데이터, 인공지능(AI), PIMS, ISMS 인증