https://doi.org/10.33778/kcsa.2022.22.1.093

제로 트러스트 환경을 위한 보안 정책 배포 방법에 대한 연구

한 성 화*, 이 후 기**

요 약

정보 서비스를 제공하기 위한 기술은 계속 발전하고 있으며, 정보 서비스는 IT융합 트렌드를 바탕으로 계속 확대되고 있다. 그러나 많은 기관에서 채택한 경계 기반 보안 모델은 보안 기술의 효율성을 높일 수 있지만, 내부에서 발생하는 보안 위협을 차단하는 것은 매우 어려운 단점이 있다. 이러한 문제점을 해결하기 위해 제로 트러스트 모델이 제안되었다. 제로 트러스트 모델은 사용자 및 단말 환경에 대한 인증, 실시간 모니터링 및 통제 기능을 요구한다. 정보 서비스의 운영 환경은 다양하므로, 보안 침해 사고가 다양한 시스템에 동시에 발생하였을 때 이에 효과적으로 대응할 수 있어야 한다. 본 연구에서는, 서로 다른 시스템으로 구성된 정보 서비스에 침해 사고가 발생하였을 때, 같은 보안 정책을 효과적으로 많은 시스템에 배포 할 수 있는 객체 참조 방식의 보안 정책 배포 시스템을 제안한다. 제안된 객체 참조형 보안 정책 배포 시스템은, 정보 서비스를 구성하는 시스템의 운영환경을 모두 지원 할 수 있음이 확인되었다. 또, 정책 배포 성능도, PC 보안 관리 시스템과 유사함이 확인되었기 때문에, 충분히 효과가 있다고 검증되었다. 다만, 본 연구는 보안 위협 대상을 사전 정의된 것으로 가정하였기 때문에, 보안 위협 별 침해 대상의 식별 방법에 대해서는 추가 연구가 필요하다.

Study on Security Policy Distribute Methodology for Zero Trust Environment

Sung-Hwa Han*, Hoo-Ki Lee**

ABSTRACT

Information service technology continues to develop, and information service continues to expand based on the IT convergence trend. The premeter-based security model chosen by many organizations can increase the effectiveness of security technologies. However, in the premeter-based security model, it is very difficult to deny security threats that occur from within. To solve this problem, a zero trust model has been proposed. The zero trust model requires authentication for user and terminal environments, device security environment verification, and real-time monitoring and control functions. The operating environment of the information service may vary. Information security management should be able to response effectively when security threats occur in various systems at the same time. In this study, we proposed a security policy distribution system in the object reference method that can effectively distribute security policies to many systems. It was confirmed that the object reference type security policy distribution system proposed in this study can support all of the operating environments of the system constituting the information service. Since the policy distribution performance was confirmed to be similar to that of other security systems, it was verified that it was sufficiently effective. However, since this study assumed that the security threat target was predefined, additional research is needed on the identification method of the breach target for each security threat.

Key words : Zero Trust, Security Policy Distribute, Security Event Monitoring, Real-time Response, Object-based Policy

접수일(2022년 2월 24일), 수정일(2022년 3월 23일), 게재 확정일(2022년 3월 31일)

* 동명대학교/정보보호학과(주저자)
** 건양대학교/사이버보안학과(교신저자)

1. 서 론

IT 융합 분야의 확대에 따라 정보 서비스는 계속증가하고 있다. 이러한 환경에서 보안 위협은 더욱 증가한다. 보안 위협은 외부에서도 발생하지만, 내부에서 더 많이 발생한다[1].

많은 기관에서 채택한 경계기반 보안 모델은, 외부에서 발생한 보안 위협 차단에는 효과적이지만 내부에서 발생하는 보안 위협을 차단하기에는 부족하다. 이러한 보안 환경의 문제점을 해결하기 위하여 제로 트러스트 모델(Zero Trust Model)이 제안되었다[2].

제로 트러스트 모델에서는 실시간 모니터링과 비인가 행위를 탐지한 경우 이를 실시간으로 차단할 수 있는 보안 기능을 요구하고 있다[3]. 그러므로 제로 트러스트 모델 기반 보안 관리 체계에서는 다양한 정보 시스템을 한꺼번에 제어할 수 있어야 한다. 그러나 정보 시스템의 종류는 매우 다양하므로, 같은 보안 정책을 동시에 배포하기에는 한계가 있다.

본 연구에서는, 제로 트러스트 모델 기반 보안 관리 체계에서 예상되는 여러 문제점 중, 동일 보안 정책을 이종 시스템에 배포해야 할 때 발생하는 문제점을 해결하기 위한 보안 정책 배포 모델을 제안한다. 제안하는 모델의 기능성 검증하기 위하여 실증 구현 후 기능을 실증 구현하고, 적절성을 평가한다. 또한 제안 모델의 실효성을 검증하기 위하여 성능 적절성을 평가한다.

2. 관련 연구

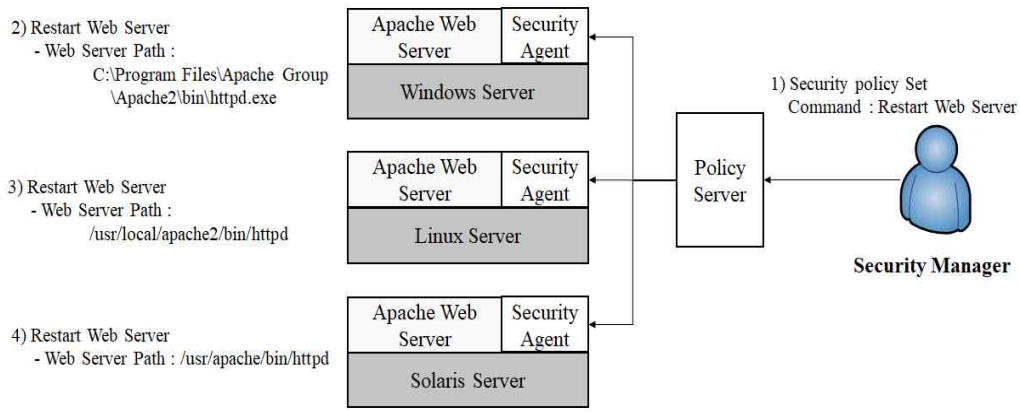
2.1 제로 트러스트 모델

많은 기관에서는 엔터프라이즈 환경에서 사용되는 다양한 정보 서비스를 보호하기 위하여 많은 보안 기술을 채택·적용하고 있으며, 보안 솔루션을 도입하여 운영한다.

이러한 보안 기술 및 솔루션은, 보안 솔루션의 운영 효율을 높이고 정보 서비스에 대한 부담을 최소화하기 위하여 경계 기반 보안 모델(Perimeter-based Security Model)을 채택하였다[4].

경계 기반 보안 모델 기반의 보안 관리 체계는 보안 기술과 솔루션의 운영 효율성이 높으며 외부에서 발생하는 보안 위협을 차단하기에는 적합하지만[5], 내부에서 발생하는 보안 위협을 차단하기에는 부적합하다[6]. 특히 최근 SmartWork나 Remote Home Work Process의 확대로 인해, 보안 위협은 더욱 증가하였다[7].

이러한 경계 기반 보안 모델의 한계점을 개선하기 위하여 제로 트러스트 모델이 제안되었다[8]. 제로 트러스트 모델은 Forrester의 John Kindervag가 2010년에 제안한 보안 모델이다. 제로 트러스트 모델에서는 사용자 인증 및 사용자 단말의 보안 환경 검증, 실시간 모니터링 및 비인가 행위 확인 시 즉시 통제 기능을 요구하고 있다[9].



(그림 1) 엔터프라이즈 환경의 정책 배포 환경

2.2 엔터프라이즈 환경의 보안 요구사항

엔터프라이즈 환경의 정보 서비스는 그 목적과 구성이 매우 다양하다. 정보 서비스의 목적이 같다고 할지라도, 해당 정보 서비스를 구성하는 시스템도 다양할 뿐만 아니라 Application 버전이나 종류도 매우 다양하다[10,11].

단일 시스템 및 동일 소프트웨어로 구성된 정보 서비스인 경우에는 단일 보안 정책의 배포만으로 보안 기능이 동작할 수 있다. 그러나 운영체제의 종류와 버전이 다르며, 각 정보 시스템에서 동작하는 Application의 종류와 버전이 서로 다를 수 있다. 이러한 경우에도 정보 서비스의 안전한 운영을 위해서는, 단일 보안 관리 행위만으로 다수의 정보 시스템에 보안 정책을 배포하여 적용할 수 있어야 한다[12]. (그림 1)은 대표적인 이종 정보 시스템으로 구성된 정보 서비스에서 동시에 발생하는 보안 위협에 대한 보안 정책을 설정할 때 발생되는 비효율적인 상황을 나타낸다. 만약 보안 위협 대상이 다수의 시스템일 때에는, 보안 관리자는 각 대상 시스템 마다 보안 정책을 설정해야 한다. 정보 시스템의 구성이 소규모일 경우에는 무관하지만, 클라우드 플랫폼과 같이 거대 시스템 인 경우에는 전체 시스템에 개별 보안 정책을 설정하는 것은 매우 어렵다.

이와 같이, 이종 정보 시스템으로 구성된 정보 서비스에 대한 보안 위협에 대응하기 위해서는, 보안 정책을 다수의 이종 정보 시스템에 동시에 적용할 수 있는 정책 관리 체계가 필요하다.

3. 보안 정책 배포 모델

3.1 이종 환경에 대한 보안 정책 배포 방안

본 연구에서는 이종 시스템으로 구성된 정보 서비스에 보안 정책을 배포를 할 수 있는 정책 배포 모델을 제안한다.

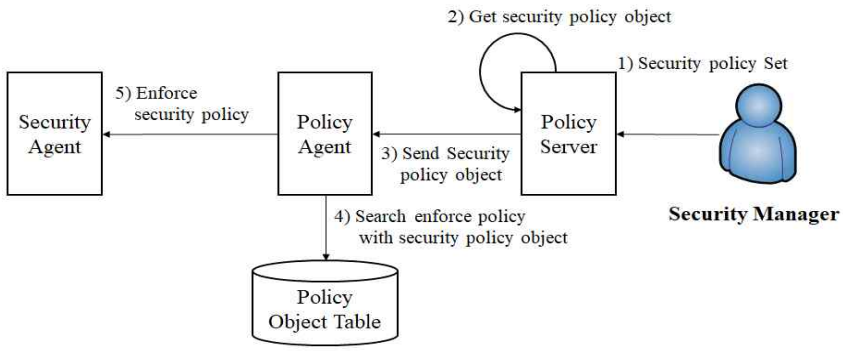
(그림 2)는 본 연구에서 제안하는 보안 정책 모델이다. 이 모델은 크게 4개의 컴포넌트로 구성된다.

Policy Server는 보안 관리자가 등록한 보안 정책에 대한 보안 정책 개체를 정보 시스템의 Policy Agent에 전달한다. Policy Agent는 보안 정책에 대한 개체를 수신한다. Policy Object Table은 보안 정책 개체에 대한 실제 적용할 보안 정책을 저장한다. Security Agent는 실제 적용할 보안 정책을 적용한다.

3.2 개체 기반 보안 정책 배포 시스템의 동작

본 연구에서 제안하는 개체 기반 보안 정책 배포 시스템은 보안 관리자에 의해 시작된다. 보안 관리자가 보안 정책을 설정하면 설정된 보안 정책이 등록되고 이에 대한 보안 정책 개체가 생성된다. 생성된 보안 정책 개체는 정보 서비스를 구성하는 Policy Agent에 전달된다. Policy Agent는 수신한 보안 정책 개체를 확인하여, 이를 Policy Agent가 동작하고 있는 정보 시스템에 적용할 수 있는 보안 정책으로 변환한다.

본 연구에서는 이종 시스템으로 구성된 정보 서비스에서는 보안 정책에 대한 객체를 생성하고, 생성된 객체를 각 정보 시스템에 배포한다. 각 정보 시스템에서는 보안 정책 객체를 수신한 후 이에 대한 정책을 Policy Object Table을 검색하여 산출 한 후 이를 보안 기능을 제공하는 Security Agent에 전달하여 적용한다.



(그림 2) 개체 기반 보안 정책 배포 모델

4. 정책 배포 시스템 검증

4.1 보안 정책 배포 기능 검증

4.1.1 정책 배포 기능 검증 방법 및 검증환경

본 연구에서 제안하는 개체 기반 보안 정책 배포 모델의 실효성을 확인하기 위한 기능 검증 환경은 3개(Windows 2017 Servere, CentOS 7.9, Ubuntu 18.04)의 운영체제에서 동작하는 Application 서비스에 대하여, 서비스 실행 제어에 대한 보안 정책을 배포하는 것을 시나리오로 선정하였다. 다수의 운영체제에서 동작하는 Application 서비스에 대한 보안 위협이 발생한 경우, 이를 제어하기 위한 보안 정책을 배포한다. 각 정보 시스템에서 동작하는 Policy Agent는 보안 정책 개체를 수신하여 각 시스템의 운영환경과 Application에 맞는 보안 정책을 찾아서 이를 적용하게 한다.

기능 검증 항목은, (표 1)과 같다.

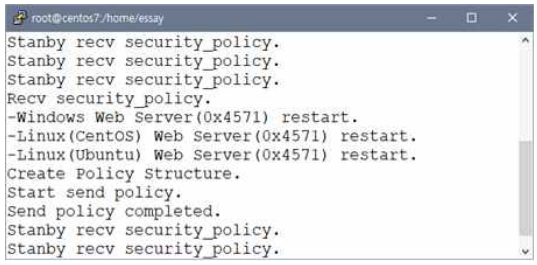
<표 1> 기능 검증 항목

기능 ID	검증 내용	검증 대상
Pos_Fnc_01	• 보안 정책에 대한 개체 생성 확인	Policy Server
Pos_Fnc_02	• 보안 정책 개체에 대해, 각 정보 시스템의 운영환경 및 Application에 대한 적용 보안 정책 도출	Policy Agent
Pos_Fnc_03	• 각 정보 시스템에서 적용 보안 정책이 정상 적용되었는지 확인	Security Agent
Neg_Fnc_01	• 전달된 보안 정책 개체가, 수신한 정보 시스템에 해당사항이 없을 때의 예외 처리	Policy Agent

4.1.2 검증 결과

■ Pos_Fnc_01

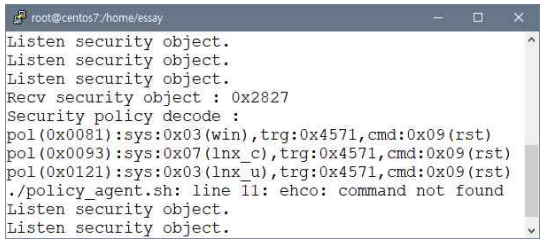
보안 관리자가 보안 위협에 대한 보안 정책을 설정한 경우, Policy Server는 (그림 3)과 같이 설정된 보안 정책을 바탕으로 보안 정책 개체를 생성한다.



(그림 3) 보안 정책 개체 생성 확인

■ Pos_Fnc_02

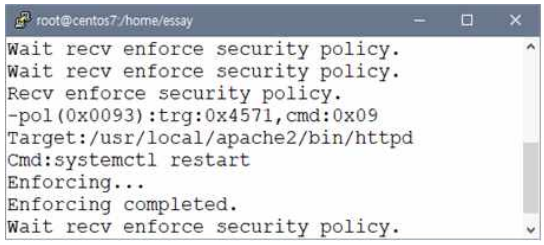
보안 정책 개체를 수신하면, 각 정보 시스템의 Policy Agent는 (그림 4)와 같이 운영환경과 동작중인 Application에 적합한 보안 정책을 도출한다.



(그림 4) 정책 보안 정책 도출 확인

■ Pos_Fnc_03

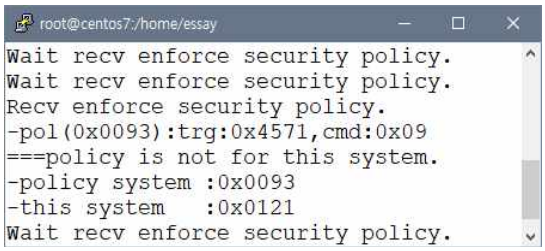
실제 보안 정책을 수신하면, Security Agent는 (그림 5)와 같이 보안 정책을 적용한다.



(그림 5) 실제 보안 정책 적용 확인

■ Neg_Fnc_01

전달된 보안 정책 개체가 해당 시스템에 해당 사항이 없는 경우에는, (그림 6)과 같이 전달된 보안 정책을 적용하지 않는다.



(그림 6) 실제 보안 정책 적용 예외 처리 확인

4.2 보안 정책 배포 성능 적합성 확인

4.2.1 정책 배포 성능 검증환경

본 연구에서 제안하는 개체 기반 정책 배포 모델의 성능 검증 환경은 Intel I-5 7500, 8Gbyte Memory, SSD 256G Storage의 시스템 4개로 구성된 정보 서비스 환경에서 수행하며, 검증 시나리오는 (표 2)와 같다.

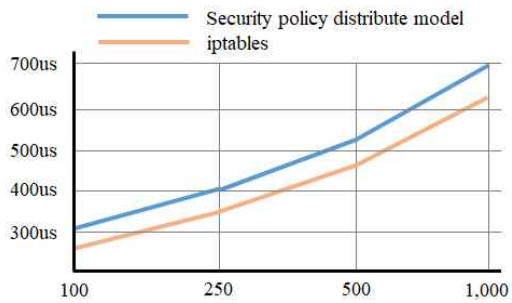
<표 2> 성능 검증 항목

기능 ID	검증 내용
Perf_01	• 100개, 250개, 500개, 1000개의 보안 정책 개체가 등록되어 있는 상황에서, 보안 정책을 등록하였을 때 등록할 보안 정책에 대한 보안 정책 개체 검색 속도 확인 • 동일 개수의 Host 방화벽(iptables) 정책 검색 속도와 비교하여 성능 적절성 확인

4.2.2 검증 결과

■ Perf_01

보안 정책을 등록할 때, 등록할 보안 정책에 해당하는 보안 정책 개체 검색 시간을 측정하고, 이를 방화벽 정책 검색 속도와 비교하였다.



(그림 7) 개체 기반 보안 정책 배포 모델 성능 측정

(그림 7)과 같이, 검색 속도는 Host 방화벽과 비교하였다. 그 결과 제안 모델의 성능은 iptables보다 성능이 낮지만, 사용자그 성능이 거의 유사한 것으로 확인되었다.

5. 결 론

엔터프라이즈 환경의 정보 서비스는 종류가 매우 많고, 정보 서비스도 매우 복잡하다. 이러한 환경에서 제로 트러스트 모델 기반의 보안 관리 체계를 수립하게 되면, 보안 위협 발생 시 실시간 통제기능이 요구된다.

본 연구는 서로 다른 운영환경 및 Application으로 구성된 다수의 정보 시스템으로 구성된 정보 서비스를 보호하기 위하여 필요한 보안 정책 배포 모델을 제안하였다.

본 연구에서 제안하는 개체 기반의 보안 정책 배포 모델은 Positive/Negative 기능 검증 결과, 엔터프라이즈 환경에서 발생하는 요구사항을 만족하며, 성능 또한 기존의 Host 방화벽과 큰 차이가 없어 충분히 실효적인 것으로 확인되었다.

다만, 본 연구는 보안 위협에 대한 보안 정책이 사전에 등록되어 있는 것을 전제하였다. 그러므로 보안 위협에 대한 각 정보 시스템 별 적용 보안 정책이 무엇진지를 생성하는 방법론에 대한 추가적인 연구가 필요하다.

참고문헌

[1] Kemp, M., “Barbarians inside the gates: addressing internal security threats”, Network Security, vol.6, pp.11-13, 2005.

[2] Kindervag, J., and Balaoura, S., “No more chewy centers: Introducing the zero trust model of information security.” Forrester Research, vol.3, 2010.

[3] Kerman, A., Borchert, O., Rose, S., and Tan, A. “Implementing a zero trust architecture”, National Institute of Standards and Technology, 2020.

[4] Saleem, Mubeen Begum and Venkata Sravya. "Issues with perimeter based network security and a better model to resolve them." European Journal of Molecular & Clinical Medicine, vol.7, no.9 pp.2437-2444, 2020.

[5] Rapuzzi Riccardo and Repetto Matteo, “Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter mode”, Future Generation Computer Systems, vo.85, pp.235-249, 2018.

[6] Ferretti, L., Magnanini, F., Andreolini, M., and Colajanni, M., “Survivable zero trust for cloud computing environments”, Computers & Security, vol, 110, 2021.

[7] Rhee, K., Won, D., Jang, S. W., Chae, S., and Park, S., “Threat modeling of a mobile device management system for secure smart work”, Electronic Commerce Research, vol.13, no.3, 243-256, 2013.

[8] Gilman, E., and Barth, D., “Zero trust networks.”, O'Reilly Media, Incorporated, 2017.

[9] Collier Zachary A. and Sarkis Joseph, “The zero trust supply chain: Managing supply chain risk in the absence of trust”, International Journal of Production Research, vol.59, no.11, pp.3430-3445, 2021.

[10] Aktas, Mehmet S. and Marlon Pierce, "High performance hybrid information service architecture." Concurrency and Computation: Practice and Experience, vol.22, no.15, pp.2095-2123, 2010.

[11] Leviakangas, Pekka, Jyrki Haajanen and Anna-Maija Alaruikka. "Information service architecture for international multimodal logistic corridor." IEEE Transactions on Intelligent Transportation Systems, vol.8, no.4, pp.565-574, 2007.

[12] Bodkin Ron, "Enterprise security aspects", AOSD'04 International Conference on Aspect-Oriented Software Development. 2004.

〔저자소개〕

한 성 화 (Sung-Hwa Han)
동명대학교 정보보호학과 교수
숭실대학교 공학박사
SW영향평가 전문위원
관심분야 : IT융합보안, 시스템보안, 인공지능, 악성코드 탐지, 제로트러스트 보안
email :shhan@tu.ac.kr

이 후 기 (Hoo-Ki Lee)
건양대학교 사이버보안학과 교수
숭실대학교 공학박사
KY 창업보육센터장, 정보보호영재교육원 부원장, 사이버미래혁신융합연구회 회장
관심분야 : 사이버보안 침해지표 연구, 제로트러스트 보안, 보안관제시스템
email : hk0038@konyang.ac.kr