이종의 보안시스템 관리를 위한 보안정책 관리에 관한 연구

이동영*, 박현주**
*명지전문대 정보통신과,
**(주)엠큐릭스 기술연구소
e-mail:dylee@mjc.ac.kr*, hjpark@mcurix.com**

A Study on the Security Policy Management for managing Heterogeneous Security Systems

DongYoung Lee*, Hyun-Ju Park**
*Dept of Information & Communication, MyongJi College
**Institute of Technology, Mcurix Company

요 약

이종의 분산환경에서 다양한 보안시스템에 대한 효율적인 보안 관리를 위해서 관리자는 보안 시스템들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야하며, 개방형 네트워크 환경의 경우 새로운 보안시스템이 추가되면 새로운 보안 정책과 기술을 적용해야 한다. 이는 전산망 운영 기관의 보안 관리 비용을 가중시키며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오히려 보안 문제를 야기시키는 역기능을 초래할 수 있다. 이에 본 논문에서는 관리대상 보안 시스템들에 대한 효율성, 편의성 및 보안성 향상을 목적으로 하며, 보안 시스템들 간의 상호연동이 가능하도록 보안정책의 일반화 프로세스를 제시하고자 한다.

1. 서론

최근 네트워크나 시스템에 대한 크래킹(cracking)이나 잘못된 조작 등에 의한 피해 사례는 정보보호시스템이 설치된 네트워크 도메인에서도 많이 발생하고 있다. 이는 지금까지 정보보호시스템들만으로 자신의 네트워크를 안전하게 관리 할 수 있다고 믿고 있는 일부 보안 관리자들을 당혹스럽게 만드는 일임에는 틀림없다. 따라서, 보안 관리자는 자신이 관리하고자 하는 네트워크의 환경과 자료의 중요도에 따라 보안정책을 수립하고 이에 맞는 다양한 보안제품을 설치, 운영하여야 한다.

이종의 분산환경에서 다양한 보안시스템에 대한 효율적인 보안 관리를 위해서 관리자는 보안 시스템들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야하며, 개방형 네트워크 환경의 경우 새로운 보안시스템이 추가되면 새로운 보안 정책과 기술을 적용해야 한다. 이는 전산망 운영 기관의 보안 관리 비용을 가중시키며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오히려 보안 문제를 야기시키는 역기능을 초래할 수 있다. 그리고, 보안 제품의 개발과 공급이 다수의 공급자에 의해서 공급되므로 서로 상이한 특성을 갖는 보안 시스템들로 구성된 보안 관리 구조의 효율적인 운용과 유지에 상당한 어려움이 있다[1-3]. 이에 복잡하고 다양한 방식의 보안관리 및 통신망 관리체계의 집중화, 자동화된 관리체계로의 전환, 그리고 이종간의 보안 시스템들에 대한 통합적인 관리를 위한 정책 관리가 요구되고 있다.

그러나, 이러한 통합보안관리시스템은 다양한 보안 제품군들이 갖고 있는 기능적 공통점을 일반화하여 보안정책에 반영하기 보다는 단순히 UI(User Interface)의 통합만을 제공하여 관리 작업을 한 곳에 집중시켜 오히려 관리자의 부담을 가중시키고 있다. 그리고, 보안 제품군들이 갖고 있는 특정 파라미터를 통한 보안정책 설정이나, 통합관리를 위한 보안 제품간의 연동성에 보다 중점을 둠으로써 보안관리를 보다 복잡하게 만드는 경향이 있다. 이와 같은 통합보안관리시스템이 보다 광범위한 네트워크에 적용될 경우, 보안관리의 복잡도를 증가시킴으로써 관리의 어려움은 더욱 심각해 질 것이다.

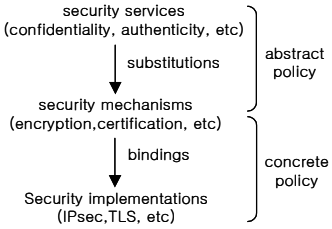
이에 본 논문에서는 대규모 네트워크상에 분산 설치되어 있는 다수의 보안 제품들을 통합관리하기 위하여 관리대상 보안 시스템들에 대한 보안관리의 효율성, 편의성 및 보안성 향상을 목적으로 하며, 보안 시스템들 간의 상호연동이 가능하도록 보안정책의 일반화 프로세스를 제시하고자 한다.

2. 연구내용

2.1 정책 모델

현재 네트워크 보안관리구조는 침입탐지시스템, 침입차단시스템, 가상사설망 등과 같은 공격의 근원지를 찾아내고 차단하는 기능을 가진 하부조직에 속하는 보안 시스템들을 중앙 집중적으로 통합 관리하는 방향으로 지속적인 연구가 진행되고 있다[4-6].

최근 연구활동으로는 통합 보안정책의 동적관리를 위한 MSME(Multidimensional Security Policy Management for Dynamic Coalitions)가 있다. MSME 시스템은 SAL(Security Abstraction Layer)에 기반하고 있으며, MSME SAL은 ISO 보안구조(ISO 7498-2)의 일부분과 ISO 7498-2에서 정의되지 않은 서비스와 메커니즘을 추가적으로 포함하고 있다. 추가적으로 포함된 것으로는 coalition members와 steganography mechanism 사이의 통신서비스를 들 수 있다. SAL에서 정책 관리자들은 특정한 보안을 독립적으로 이행함으로써, 상위레벨 보안서비스에 관하여 판단과 계획을 세울 수 있다.

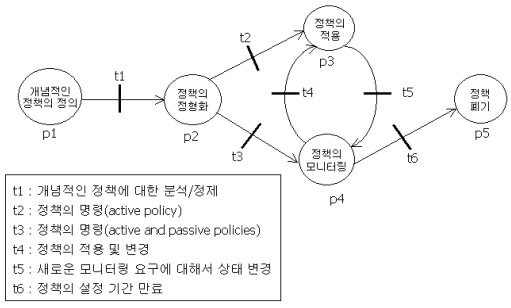


〈그림 1〉 정책의 추상화

<그림 1>은 MSME에 대한 추상적인 개념을 도시한 것이다. MSME 시스템은 어떠한 보안 메커니즘으로 보안서비스를 제공할 것인지를 결정하고, 결정된 보안 메커니즘의 구현 기술을 결정하여 동적으로 연결 구성함으로써 보안정책을 동적으로 구성 관리할 수 있다.

2.2 정책의 라이프사이클

정책의 라이프사이클은 다양한 상태의 변화로 전이된다. PB-ISMS의 정책의 라이프사이클의 동작을 살펴보면, <그럼 2>에서 p1은 개념적이고 추상적인 정책을 정의하고, 이들에 대한 정제를 거쳐서 정책을 적용할 수 있는 활동 상태인 p2로 전이된다.

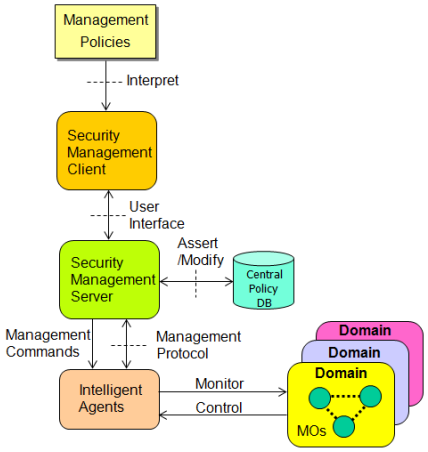


〈그림 2〉 정책의 라이프사이클

그리고 활동 상태의 정책에 따라서 정책의 적용 상태 p3와 정책의 모니터링 p4 상태로 전이된다. 이후 정책의 모니터링 p4 상태에서 정책의 변경사항이 발생할 경우 이를 정책의 적용 p3상태로 이동하고 그와 반대로 정책의 적용 p3상태에서 새로운 정책의 모니터링 p4상태의 요구사항을 변경될 수 있다. 이를 설정된 정책의 기간이 만료되면 정책 폐기 p5상태가 된다. <그림 2>는 통합보안시스템의 정책 라이프사이클을 표현한 것이다[4].

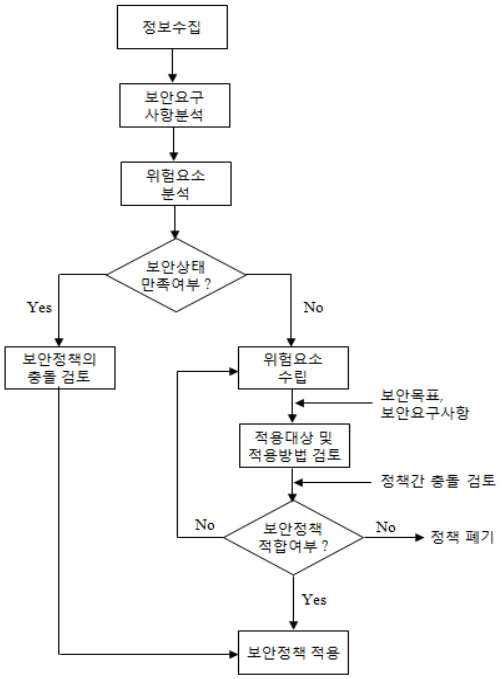
2.3 정책의 일반화 프로세스

본 논문에서는 보안시스템을 통합관리하기 위한 시스템을 기반으로 적용하여 보안관리시스템의 개념적인 구조는 <그림 3>과 같다.



〈그림 3〉 보안관리시스템의 구조

<그림 3>과 같은 관리시스템의 경우 관리대상 보안 제품들 마다 독립적으로 보유하고 있는 특정 파라미터를 통하여 보안정책을 설정하는 것이 아니라, 보안 제품들의 기능적 공통점을 일반화하여 보안정책에 반영하고, 보호대상 네트워크로부터 수집된 보안 관련 정보에 대한 분석 결과를 일반화된 보안정책의 설정과정에 반영함으로써 보안 제품들 간의 연동성과 보안정책관리의 효율성을 향상시킬 수 있는 보안정책관리 모델이다.



<그림 4>보안정책 일반화 프로세스

그리고, 보안정책 일반화 과정을 통하여 보안정책의 중복 및 충돌현상을 미연에 방지할 수 있기 때문에 보안정책의 무결성을 향상시킬 수 있다. <그림 4>는 보안정책의 일반화 과정을 나타낸 것이다. 보안정책 일반화 프로세스를 통해서 관리대상 보안 시스템들에 대한 보안관리의 효율성, 편의성 및 보안성 향상을 목적으로 하며, 보안 시스템들 간의 상호연동이 가능하도록 보안정책을 구성할 수 있다.

3. 연구 결과 및 향후 계획

클라우드 컴퓨팅의 개방성은 사용자에게 많은 편리함을 제공함과 동시에 클라우드 서버에 저장된 정보에 대한 유출은 시급히 해결해야할 문제이다. 이에 본 논문에서는 클라우드 환경에서 내부정보 유출 환경을 살펴보고 클라우트서버로부터의 사용자 명령어를 수집 및 로그(Log)파일로 생성하고 이를 분석하여 내부 정보 유출을 판단하고 이를 보호하기 위한 명령어 감사시스템 구조를 제안하였다. 현재 리눅스 서버를 대상으로 프로토타입(prototype)으로 구현을 진행하고 있다. 향후 계획으로는 프로토타입으로 개발된 시스템에 대한 성능 평가 및 다른 OS로의 확장이 요구된다.

참고문헌

[1]. J. Zao, L. Sanchez, et el, “Domain based Internet security policy management,” DARPA Information Survivability Conference and Exposition, 2000, DISCEX ’00, Proceedings, Vol.1, pp.41-53, Jan., 1999.

[2]. L. Lewis, “Implementing policy in enterprise networks,” IEEE Communications Magazine, Vol.34, Iss.1, pp.50-55, Jan., 1996.

[3] D. Y. Lee, D. S. Kim, K. H. Pang, H. S. Kim, T. M. Chung, "A Design of Scalable SNMP Agent for Managing Heterogeneous Security Systems", NOMS(Network Operations and Management Symposium)2000, pp.293-294. April 2000.

[4] Rene Wies, "Policy Definition and Classification : Aspects, Criteria, and Examples, Proceeding of IFIP/IEEE International Workshop on Distributed Systems : Operations & Management, Toulouse, France, Oct. 1994.

[5] Miriam J. Maullo and Seraphin B. Calo, "Policy Management : An Architecture and Approach"Systems Management", Proceedings of the IEEE First International Workshop on , pp. 13-26, 1993

[6] 이동영, 김동수, 방기홍, 김홍선, 정태명, "SNMP를 이용한 웹 기반의 통합 보안관리 시스템", KNOM(Korea Network and Operations Management) Review 논문지, Vol. 2. pp. 1167-1171, 1999.