통합보안관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구*

김석훈** · 김은수*** · 송정길****

요 약

최근 다변화된 침입에 대하여 대처하기가 어렵고, 시스템 환경에 적합한 시스템 개발과 대규모 네트워크에 대한 효율적인 침입 탐지 및 대응 구조를 갖고 있지 않는 등 단일 보안 관리의 문제점이 대두되고 있다. 그래서 대규모화 되어가는 네트워크에서 다양한 침입을 차단하기 위해서는 분산화된 보안제어시스템들의 필요성이 요구되고 있고, 다양한 보안시스템의 통합관리와 각 시스템들의 침입탐지 및 대응에 대한 모델이 필요하게 되었다. 본 논문에서는 광범위한 네트워크 자원을 관리하는 PBNM 구조를 개선하고 보안시스템의 침입탐지 및 대응에 적합한 새로운 모델을 제시하였다. 또한 제시된 모델을 통합보안관리시스템에 적용시킴으로써 효과적인 침입탐지 및 대응을 위한 보안 정책 모델를 기반으로 통합보안관리시스템을 설계하였다.

Security Policy Model for the Intrusion Detection and Response on Enterprise Security Management System*

Seok-Hun Kim** · Eun-Soo Kim*** · Jung-Gil Song****

ABSTRACT

Recently It,s difficult to deal with about variety of attack. And Simple Security management have a problem. It is that they don,t develop System measuring their system envoirment and have efficient attack detector, countermeasure organization about large network. Therefore, need model about enterprise management of various security system and intrusion detection of each systems and response. In this paper, improve PBNM structure that manage wide network resources and presented suitable model in intrusion detection and response of security system. Also, designed policy-based enterprise security management system for effective intrusion detection and response by applying presented model to enterprise security management system.

Key words : ESM, Security, Policy, Intrusion Detection, PBNM

---

* 본 연구는 '산업자원부 지역협력연구사업(과제번호 : R12-2003-004-02001-0) 지원으로 수행되었음'.

** 한남대학교 컴퓨터공학과
*** 한남대학교 교수학습지원센터
**** 한남대학교 정보통신 · 멀티미디어 공학부

1. 서 론

IT분야의 기술 발전으로 인하여 네트워크 상에 존재하는 논리적인 도메인들의 규모가 확대되었고, 인터넷의 활성화와 대규모 네트워크가 활발히 구축되면서 경제, 사회, 정치 분야에서 컴퓨터를 이용한 업무처리 및 정보 관리 등 인간 생활의 많은 부분이 컴퓨터시스템에 의존적으로 변형되었다. 더욱이 IT 분야의 급속한 발전과 사회 전반에 걸친 영향으로 인하여 여러 가지 문제점들이 발생하고 있는데 특히 컴퓨터 시스템에 대한 해커와 크래커 등의 침입이 아주 큰 문제로 대두되어 왔다. 또한 인터넷을 통한 개방된 네트워크 환경에서는 정보 보안에 취약한 상태이며, 이러한 이유로 정보보호서비스에 대한 요구의 증대와 정보보호기술 및 정보보호제품에 대한 수요가 점차 확대되고 있다[1, 2, 13].

최근 보안과 관련하여 IPv6의 제정과 함께 IPsec (IP Security Protocol)에 대한 심도 있는 연구가 진행되고 있으며 IETF(The Internet Engineering Task Force)의 IPSP(IP Security Policy) 워킹그룹에서 보안정책과 관련된 연구가 활발히 이루어지고 있다. IPSP 워킹그룹은 보안의 기술적 측면의 개발 뿐만아니라 Host 또는 Gateway를 포함하고 있는 도메인의 보호를 위하여 보안정책의 연구와 표준화를 진행 중이다[3, 4].

현재 시스템의 보안을 위하여 다양한 보안제품들이 상용화되었고 이를 탑재하여 운영 중인 시스템들이 상당수에 이른다. 예를 들어 초기 보안시스템의 상징인 방화벽(Firewall)과 침입탐지에서 차단기능까지 수행하는 IDS(Intrusion Detection System)가 대표적이다. 하지만 침입의 유형이 매우 다양화 되면서 침입에 대한 탐지 및 대응이 매우 복잡해지고 보안제품에 따라 기능 및 제어가 어려워지고 있다. 그로인해 다양한 보안솔루션에 대한 보안관리자들의 통합보안관리가 요구되었고 이러한 요구를 충족시키기 위한 다양한 보안솔루션의 통합관리가 중요한 과제로 대두되었다. 더불어 네트워크 자원에 대한 관리 및 운용과 관련하여 IETF에서는 정책기반 관리 모델을 제시하고 있는데 이는 네트워크와 관련된 장비 및 이에 준하는 솔루션들의 광범위한 관리를 위한 것이다[5, 6, 19].

본 논문에서는 광범위한 정책기반관리 모델을 변형하여 침입탐지 및 대응에 적합한 변형 모델을 제시하고 이를 통합보안관리(ESM)시스템과 연계시킴으로써 침입탐지 및 대응에 대한 정책기반의 통합보안관리시스템에 대해 기술하고자 한다. 본 논문의 2장에서는 통합보안관리 모델과 정책기반관리 모델에 대해 알아보고 3장에서 침입탐지 및 대응위한 보안정책 모델의 적용과정 및 비율산출을 정의하고 비율산출에 따른 신규정책 수립 모델의 생성과정을 기술하며 4장에서는 논문에서 제시한 SPB-ESM 시스템의 모듈별 설계와 모델적용에 대하여 언급한다. 마지막으로 5장에서는 결론 및 향후 연구방향에 대하여 논한다.

2. 관련 연구

2.1 정책기반의 네트워크 관리 (PBNM: Policy-Based Network Management)

PBNM(정책 기반의 네트워크 관리)은 네트워크에서 제공되는 정보보호 및 네트워크 자원(NE : Network Element) 제어를 위해 관리정책(Management Policy)을 정의하고, 이를 기반으로 네트워크 및 서비스를 일관된 정책에 따라 자동으로 관리하는 기술이다.

IETF의 정책 프레임워크 규격에서는 PBNM 시스템의 기능적 컴포넌트로 정책관리도구(Policy Management Tool : PMT), 정책 저장장치

(Policy Repository : PR), 정책 결정장치(Policy Consumer : PC), 정책수행 대상장치(Policy Target: PT)로 구분한다[3, 5, 13, 17].

- 정책관리도구(PMT : Policy Management Tool)

시스템운영자에 의해 통신망 동작을 모니터링하는 정책 기반의 통신망 관리 운영 상태 감시 혹은 관리를 위한 작업과 관련하여, 규칙을 변환 및 검증, 정책규칙 자료 검색, 그래픽으로 표시된 정책규칙을 특정한 정보로 변환하는 등의 기능을 수행한다.

- 정책저장(PR : Policy Repository)

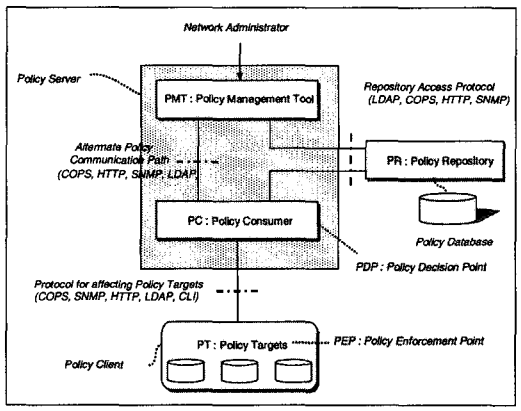
정책 저장소(Policy Repository)는 수립된 정책 규칙을 정책데이터베이스에 저장하게 되며 객체지향 측면에 입각하여 중앙 혹은 지역적으로 분산된 형태로 저장 및 관리한다.

- 정책결정(PC : Policy Consumer)

PDP(Policy Decision Point) 또는 정책서버라고도하며, 정책 규칙 및 각종 네트워크 정보를 관리한다. 또한 정책저장소(PR)의 정보가 추가, 삭제, 갱신되었다는 사실을 인지하여 정책저장소로부터 정책정보를 검색하여 해당 정책을 정책 클라이언트로 전송한다.

- 정책수행 대상(PT : Policy Target)

PEP(Policy Enforcement Point) 또는 정책 클라이언트라고도 하며 수립된 정책을 실제로 수행한다. PEP는 정책관리에서 수립된 정책과 정책결정에 의해 수신된 정책 규칙정보를 정책 클라이언트가 상주하는 시스템에 적합한 형태로 저장하여 이를 수행한다. 그리고 정책수행 결과를 정책서버에 알리거나 또는 동적으로 처리되는 중요한 정보를 보고하는 기능을 수행한다.



(그림 1) PBNM Framework

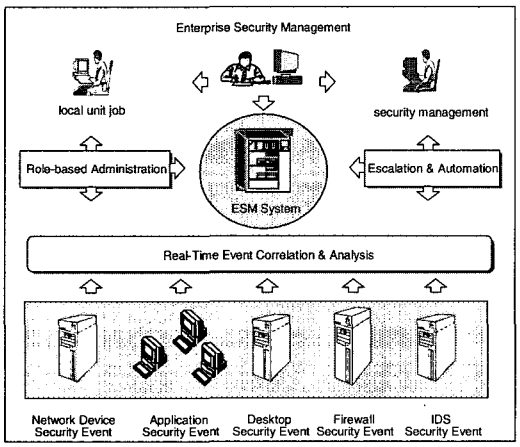
2.2 통합보안관리(ESM: Enterprise Security Management)

통합보안관리(Enterprise Security Management : ESM) 기술은 침입탐지 시스템(IDS), 가상사설망(VPN) 시스템 등 다양한 종류의 보안 시스템들을 상호 연동하여 각 기능을 통합 관리하는 중앙집중식 관리체계이다[11, 12]. 이러한 ESM 시스템은 과거 각각의 제품에 대한 모니터링 기능의 구현이었지만 보안 프로토콜의 표준화를 통해 타사 제품을 포함한 이기종 보안 시스템에 대한 모니터링 기능을 가지도록 발전하고 있다. 또한 ESM 시스템에서는 수집된 자료를 분석하여 보안사건에 대한 리포팅 기능과 함께 각 보안시스템에 대한 세부 정책관리 기능이 가능한 단계로 발전할 것으로 예상된다[15, 16].

통합보안관리를 위한 보안 표준 프로토콜로는 체크포인트사의 Firewall-1/VPN을 중심으로 컨텐츠 보안, 인증 및 권한 관리, 침입탐지시스템, 사건 분석 및 리포팅, 디렉토리 서버분야의 프레임워크 파트너를 구성하는 OPSEC과 IETF의 침입탐지시스템 상호연동 메시지 표준을 구축하고 있는 IDWG 워킹그룹이 대표적이다[11, 12].

이와같은 ESM의 의의는 관리의 효율성 차원에서 살펴 볼 수 있는데 가트너 그룹이 조사한

TCO(Total Cost of Ownership) 모델에 따르면 기업 IT 비용의 2/3에서 3/4정도가 인력을 배치 및 관리 그리고 유지 등의 비용으로 지출된다고 한다. ESM은 이처럼 수많은 관리자가 해야 할 반복적이고 단순한 업무들을 자동화하고 단순화함으로써 전체적인 비용 절감 효과를 가져 올 수 있다. 또한 분산되어 있는 기업 IT 환경에서 전사적인 차원의 관리가 가능하기 때문에 일관되고 효율적인 보안 관리를 가능케 한다[17, 18].



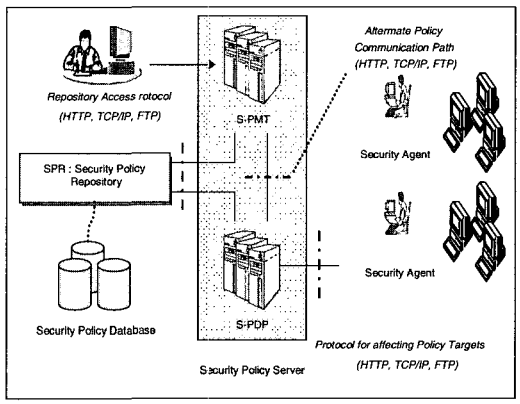
(그림 2) ESM 시스템

IDMEF 메시지 타입은 크게 Alert와 Heartbeat의 두 가지 형태로 구성된다. Alert는 침입정보를 생성한 IDS의 이름, 침입정보를 발생시킨 이벤트, 공격의 개시시스템과 목표시스템에 대한 정보 등을 포함한다. Heartbeat는 분석모듈이 관리모듈에게 상태정보를 제공할 때 사용된다.

3. SPB-ESM 시스템 침입탐지 및 대응 모델

3.1 SPB-ESM 시스템의 개요

본 논문에서 제안하고자하는 SPB-ESM(Security-Policy-Based Enterprise Security Management) 시스템은 앞에서 언급한 PBNM 구조에 근거하여 구조를 설계 변경하였다. 상위 PMT와 관련하여 침입탐지 및 대응과 관련된 S-PMT로 설계하며 해당 Viewer를 통해 제어하게 된다. 또한 PDP는 정책수립을 위한 S-PDP로 설계하고 정책저장소인 PR은 S-PR로 침입탐지 및 대응과 관련된 정책정보를 데이터베이스에 저장하게 된다. 마지막으로 정책수행을 담당하는 PEP는 보안을 필요로 하는 호스트 및 네트워크 상에 존재하는 시스템에 보안에이전트로 구현되며 정책수립과 연계하여 보안정책에 따른 정책수행을 담당한다. 이와같이 PBNM 구조를 변경하여 시스템을 설계한 것은 광범위한 네트워크 자원의 관리보다는 보안의 핵심인 침입-대응에 적합한 시스템을 구현하기 위한 것이다. 다음은 본 논문에서 제안하는 침입-대응에 적합한 SPB-ESM 시스템 구성도이다.



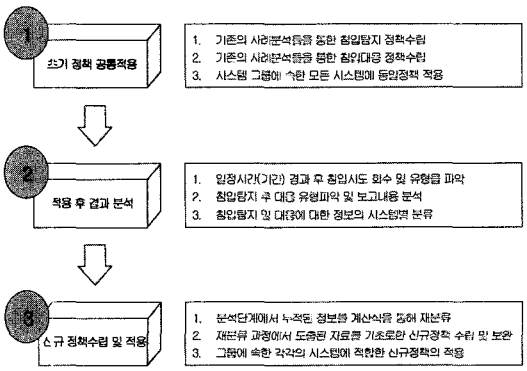
(그림 3) SPB-ESM 시스템

SPB-ESM 시스템은 침입-대응에 적합한 보안시스템의 관리 즉, 보안정책의 결정, 모니터링, 적절한 대응과 같은 작업을 수행한다. 또한 침입에 대한 대응을 담당하는 보안에이전트를 보안을 요구하는 시스템에 탑재함으로써 보다 효과적인 관리와 대응이 가능하도록 하였다.

3.2 침입탐지 및 대응 위한 보안정책 적용과정

SPB-ESM 시스템의 침입탐지 및 대응모델은 통합보안관리 시스템의 정책 결정에 효율성, 편의성 및 보안성 향상을 목적으로 하며, 통합보안관리 시스템에 종속되는 시스템들 간의 상호연동이 가능하도록 구성한다. 본 논문에서 제시하고자 하는 침입탐지 및 대응위한 보안정책 모델은 기존의 IT 보안정책 수립 등과 같은 광범위한 정책규칙을 적용시키는 것이 아니라 침입탐지 및 대응과 관련하여 호스트 또는 네트워크 기반의 보안정책 수립을 목적으로 한다.

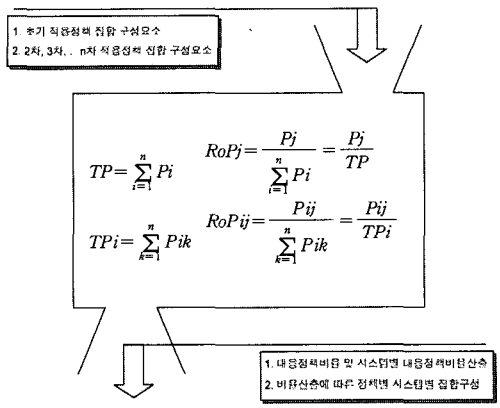
침입탐지 및 대응 모델을 정의하기 위해서는 다양한 형태의 침입탐지 및 차단 유형들로부터 추출된 분석정보를 정책수립에 필요한 정보유형으로 변환, 분류하고 이를 분석하는 과정을 거쳐야 한다. 다음 (그림 4)는 침입탐지 및 대응을 위한 보안정책 모델의 적용 과정을 도식화한 것이다.



(그림 4) 보안정책 모델의 적용 과정

3.3 보안정책 적용 및 분석 모델

시스템에 침입하는 침입유형 및 침입에 대한 대응 유형이 매우 다양하여 각각에 대한 개별적 접근 및 해석이 서로 상이하고 구현절차 또한 복잡해진다. 이러한 문제를 해결하기 위해서는 수집된 정보를 분석하고 정량화된 구조로 분류하는 작업이 먼저 선행되어야한다. 따라서 초기 적용된 보안정책의 시스템 적용 후 발생한 적용범위에 따라 비율을 산출하고 산출된 비율을 비교분석하여 새로운 정책수립을 한다. 다음 (그림 5)는 초기 보안정책의 시스템 적용 후 보안정책과 시스템별 보안정책의 비율산출과정이다.



(그림 5) 보안정책의 비율산출

- 초기 통합보안관리 영역에 속한 단위별 시스템에 적용되는 정책의 정의

초기 보안정책의 적용에 있어서 시스템에 대한 정확한 환경분석 또는 시스템의 특징을 파악할 수 없기 때문에 일반적인 침입탐지 및 대응과 관련된 정보들을 분석하여 초기 보안정책을 결정한다. 이때 초기 보안정책의 그룹을 Pi 라 가정하고 다음과 같이 정의한다.

P : 정책종류 P_i : 시스템별 정책종류, i : 시스템종류

$P = \{ P_1, P_2, P_3, P_4, P_5, \ldots, P_{n-1}, P_n \}$,

$P_i = \{ P_1, P_2, P_3, P_4, P_5, \ldots, P_{n-1}, P_n \}$

- 시스템 적용 후 비율 산출

비율산출은 두 가지로 분류하여 산출하게 되는데 초기 모든 시스템에 적용된 정책 P에 대한 비율을 산출하고 시스템별로 적용된 정책에 대

한 비율을 산출한다. 이러한 비율산출은 정책별로 가장 많이 적용된 정책을 파악하고 시스템별 정책비율 산출을 통해 해당 시스템에 적합한 정책을 찾아내는데 목적이 있다.

$$TP = \sum_{i=1}^{n} Pi \qquad RoPj = \frac{Pj}{\sum_{i=1}^{n} Pi} = \frac{Pj}{TP}$$

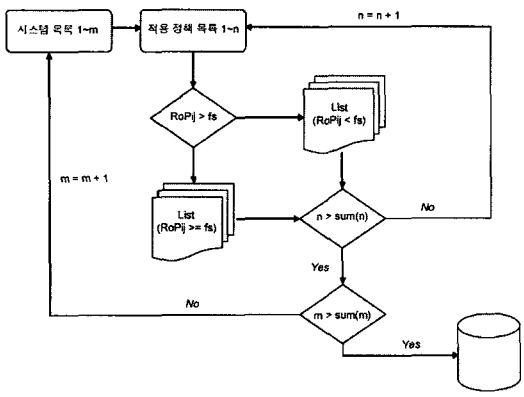
〔정책별 비율 산출〕

$$TPi = \sum_{k=1}^{n} Pik \qquad RoPij = \frac{Pij}{\sum_{k=1}^{n} Pik} = \frac{Pij}{TPi}$$

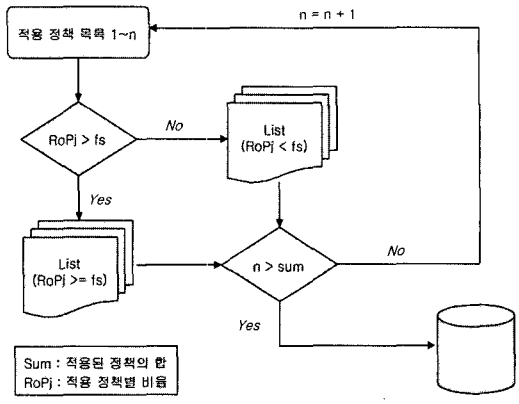
〔시스템별 정책비율 산출〕

3.4 신규 보안정책 도출과정 및 분류

초기 보안정책의 시스템적용 후 각각의 비율 산출 수식에 의해 도출된 비율을 이용하여 각각의 시스템에 적용할 새로운 보안정책을 수립하게 된다. 이때 적용 정책별 비율그룹과 시스템별 비율그룹 그리고 기준치를 적용한 정책별 비율그룹과 시스템별 비율그룹으로 분류하여 각각의 상호 관계를 통해 새로운 보안정책을 수립한다. 다음 (그림 6)은 정책별 비율 산출과정과 시스템별 비율산출 과정에 대한 흐름도이다.



〔정책별 비율산출과정〕



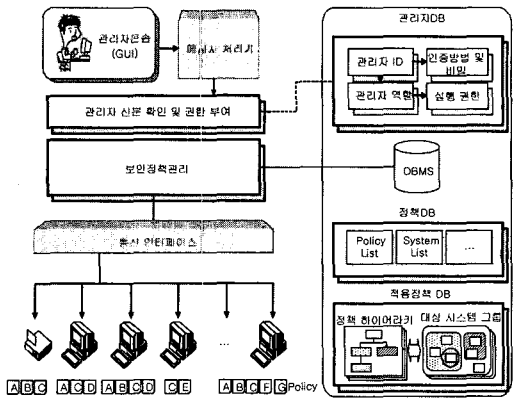
〔시스템별 비율산출 과정〕

(그림 6) 정책별, 시스템별 정책비율산출 과정

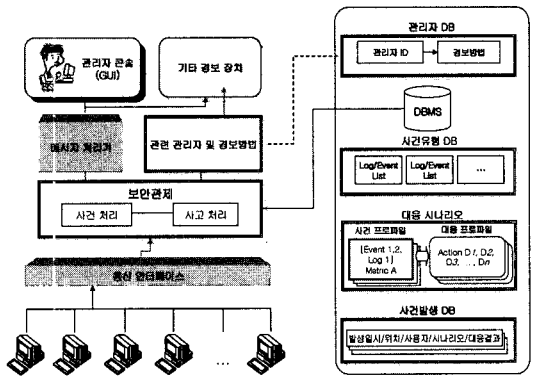
4. SPB-ESM 시스템의 모듈별 설계

4.1 SPB-ESM 시스템에 필요한 모듈 설계

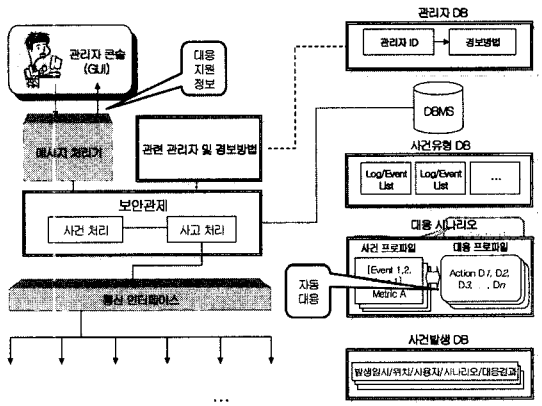
본 논문에서 제안하는 시스템은 단위별 시스템의 보안정책을 수립하는 정책설정및 관리모듈, 시스템의 보안상태를 감시하는 모니터링 모듈, 침입이 발생했을 경우 대응하는 대응모듈, 침입의 유형분석 및 경고기능을 하는 분석 및 경고 모듈로 크게 4가지로 분류가 된다. (그림 7)은 시스템의 구성에 필요한 4가지 모듈을 설계한 것이다.



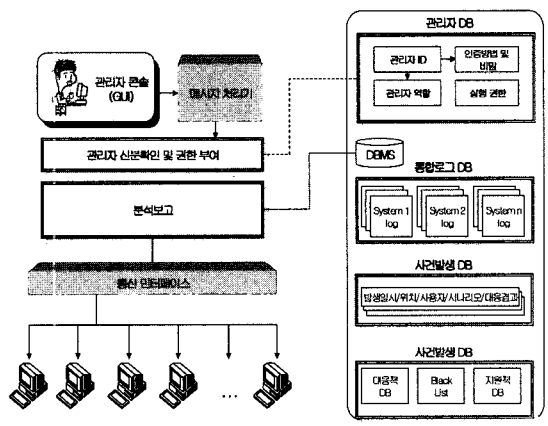
〔보안정책 모듈〕



〔모니터링 모듈〕



〔보안대응 모듈〕

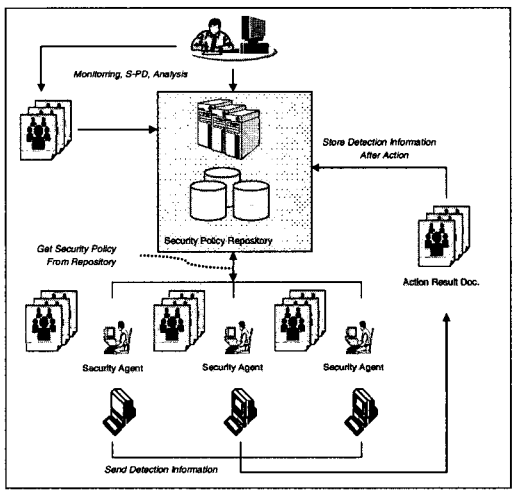


〔분석 및 경보 모듈〕

(그림 7) 제안 시스템의 4가지 모듈

4.2 전체 시스템 구성

SPB-ESM 시스템의 구성은 시스템에 종속되어있는 보안대상 시스템들의 모니터링과 대응방안을 수립한 보안서버를 주축으로 한다. 이때 SPB-ESM 시스템에 종속된 시스템들은 각각 수립된 정책에 따른 개별적 탐지 및 대응을 할 수 있는 에이전트를 갖고 있으며 이들 에이전트들은 탐지 및 대응 결과를 다시 보안서버에 회신하게 된다. 관리자는 보안서버에 상주하여 에이전트로부터 회신된 자료를 분석하고 침입탐지 및 대응 정책의 수립과 갱신을 담당한다. 관리자의 정책수립과 갱신과정에서 유형분류 및 상호관계의 변형이 가능하며 이러한 갱신사항은 정책의 수립에서부터 정책수행에 이르기까지 광범위한 영향을 미치게 된다.



(그림 8) 침입탐지 및 대응 모델을 적용한 SPB-ESM 시스템

5. 결론 및 향후 연구방향

본 논문에서 제안하는 SPB-ESM 시스템은 PBNM 구조의 변경과 통합보안관리시스템에 종

속되어있는 보안시스템들에 에이전트를 상주시킴으로써 침입탐지 및 대응에 적합한 모델을 제시하였다. 광범위한 네트워크 장비의 관리보다는 침입탐지 및 보안에 중점을 두어 설계함으로써 보안을 필요로 하는 시스템들의 침입대응효과를 높이도록 하였다. 또한 종속된 시스템들의 서로 다른 시스템 환경을 고려하여 보안정책을 수립함으로써 해당시스템에 적합한 보안정책을 적용시킬 수 있고 보안에이전트를 통한 분산대응으로 관리시스템에 대한 집중화를 억제시키도록 하였다. 마지막으로 SPB-ESM 시스템은 보안에이전트를 통한 종속된 보안시스템들의 자체 대응과 최상위 관리자에 의한 원격대응을 병행시킴으로써 통합보안관리시스템의 응용모델을 제시하였다.

향후 연구방향으로는 통합보안관리시스템에 종속된 이기종간의 침입탐지 및 대응 모델로의 확장된 연구와 실시간 분석을 통한 다양한 대응모델에 대한 연구가 필요하다.

참 고 문 헌

[1] N. Freed and S. Kille, "Network Services Monitoring MIB", RFC2248, Janualry 1998.

[2] A Study on the Development of Countermeasure Technologies against Hacking and Intrusion in Computer Network Systems, KISA final development report, January 1999.

[3] "Policy-based Network Management", Network computer Magazine, Dec. 1999.

[4] "Policy-Based Management", TM Forum University Workshops, May, 2001.

[5] Guidelines on Firewalls and Firewall Policy, NIST SP800-41, 2002.

[6] Judy Novak, Stephen Northcutt, "Network Intrusion Detection", New Riders Publishing, 2003.

[7] Earl Carter, "Cisco Secure Intrusion Detection System", Sicso Press, 2001.

[8] CISCO NETWORK MANAGEMENT CISCOWORKS,

[9] IBM Security management, http://www-306.ibm.com/software/tivoli/solutions/security/.

[10] Strassner, J., E. Ellesson, B. Moore and A. Westerinen, "Policy Core Information Model Version 1 Specification", RFC3060, 2001. 2.

[11] Deron Powell, "Enterprise Security Management (ESM) : Centralizing Management of Your Security Policy", SANS Institute, December 2000.

[12] Randy Heffner, "Enterprise Application Security Integration", IT Trends 2002, December 2001.

[13] 정연서, "대규모 네트워크를 위한 통합 침입탐지시스템 설계", 한국컴퓨터산업교육학회 논문지, Vol. 3, No. 7, July, 2002. 7.

[14] 이동영, 방기홍, 홍승선, 김동수, "이종의 caldql 차단시스템 관리를 위한 웹기반의 통합 보안 관리시스템 개발", 한국정보보호센타 정보보호 우수 논문 공모전 응용기술분야, '99 정보보호 우수논문집, pp.153-180, Dec. 1999.

[15] 황윤철, 현정식, 이상호, "정책기반 보안관리 모델을 위한 프로토타입과 정책 협상 메커니즘", 정보보호학회논문지, 제13권, 제1호, 2003. 2.

[16] 신역성, 장종수, " 정책 기반의 정보보호 시스템 관리기술", 정보보호학회지, 제13권, 제1호, 2003. 2.

[17] 이영석, 나중찬, "통합 보안 관리를 위한 이

기종 보안 시스템 연동", 한국정보보호학회지, 제13권, 제1호, 2003. 2.
[18] 이영석, "ESM 자료조사" ETRI 기술문서, 2002. 12.
[19] 오승희 외, "최신 네트워크 보안 기술 동향 분석", 한국정보과학회 추계학술 발표 논문지, 제30권, 제2호, 2003. 10.
[20] 정영서 외, "네트워크 정보보호 시스템 발전 방향", SK Telecommunications Review, 제13권, 제2호, 2003. 2.

김 석 훈

2001년 배재대학교 정보통신공학과(공학사)
2003년 한남대학교 대학원 컴퓨터공학과 (공학석사)
2003년~현재 한남대학교 대학원 컴퓨터공학과 박사과정 재학중
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 모바일 컴퓨팅, 정보보호

김 은 수

1994년 서울산업대학교 시각디자인과(이학사)
1997년 서울산업대학교 대학원 시각디자인과(이학석사)
2004년 한남대학교 대학원 컴퓨터공학과(공학박사)
2004년~현재 한남대학교 교수 학습지원센터 강의전담교수
관심분야 : 웹디자인, 멀티미디어디자인, 정보보호

송 정 길

1966년 한남대학교 수학과 (이학사)
1982년 홍익대학교 대학원 전자계산학과(이학석사)
1988년 중앙대학교 대학원 전자계산학과(이학박사)
1990년~1991년 University of illinois 객원교수
1979년~현재 한남대학교 컴퓨터공학과 정교수
관심분야 : 멀티미디어문서처리(XML), 객체지향 모델링 및 방법론(UML), 분산시스템, 정보보호