이종의 보안시스템 관리를 위한 정책 기반의 통합보안관리시스템의 계층적 정책모델에 관한 연구

이 동 영[†] · 김 동 수[††] · 정 태 명[†††]

요 약

정보통신과 컴퓨터기술의 발전으로 인하여 불법침입으로 인한 정보 파괴, 서비스거부공격 그리고 컴퓨터 바이러스 등에 의한 역기능이 날로 증가하고 있는 추세이다. 또한, 이러한 공격들로부터 네트워크를 보호하기 위해서 침입차단시스템(일명 : 방화벽), 침입탐지시스템, 접근제어시스템 등 많은 보안제품들이 개발 및 적용되고 있다. 그러나 이러한 보안 제품들에 대한 관리를 위해서는 많은 작업과 비용이 소요된다. 따라서, 이들 보안제품들에 대한 효율적인 관리와 일관된 보안 정책을 적용할 수 있는 정책 기반의 통합보안관리시스템의 정책모델이 필요하게 되었다. 본 논문에서는 정책계층의 개념을 기반으로 상위계층의 추상적이고 개념적인 정책을 보다 구체적인 형태의 정책으로 정제(refinement)하는 정책기반의 통합보안관리시스템의 계층적 정책모델을 제시하였다. 정책의 정형화된 표현을 위해서 Z-Notation을 적용하였으며, 이는 수학적 논리와 집합이론을 기반으로 스키마형태로 표현된다.

A Study of Hierarchical Policy Model of Policy-based Integrated Security Management for managing Heterogeneous Security Systems

Dong Young Lee[†] · Dong Soo Kim[††] · Tai Myoung Chung[†††]

ABSTRACT

With a remarkable growth and expansion of Internet, the security issues emerged from intrusions and attacks such as computer viruses, denial of services and hackings to destroy information have been considered as serious threats for Internet and the private networks. To protect networks from those attacks, many vendors have developed various security systems such as firewalls, intrusion detection systems, and access control systems. However, managing those systems individually requires too much work and high cost. Thus, in order to manage integrated security management and establish consistent security management for various security products, the policy model of PN-ISMS (Policy Based Integrated Security Management System) has become very important. In this paper, present the hierarchical policy model which explore the refinement of high-level/conceptual policies into a number of more specific policies to form a policy hierarchy. A formal method of policy description was used as the basis of the mode in order to achieve precision and generality. Z-Notation was chosen for this propose. The Z-Notation is mathematical notation for expressing and communicating the specifications of computer programs. Z uses conventional notations of logic and set theory organized into expressions called schemas.

키워드 : Integrated Security Management, PBNM(Policy-based Network Management), Hierarchical Policy Model

1. 서 론

정보통신과 컴퓨터기술의 발전으로 인하여 불법침입으로 인한 정보 파괴와 컴퓨터 바이러스 등에 의한 역기능이 날로 증가하고 인터넷과 같이 범 세계적인 네트워크로 연결되어 있는 정보 시스템에 대한 위협 역시 급속히 증가하고 있는 추세이다. 이러한 이유로 비밀성, 신뢰성 등의 정보보호서비스에 대한 요구가 증대되어 정보보호기술 및 정보보호제품에 대한 수요가 점차 확대되어 가고있다[1].

그러나 최근 네트워크나 시스템에 대한 크래킹(cracking)이나 잘못된 조작 등에 의한 피해 사례는 대표적인 정보 보호 시스템인 침입차단시스템(일명 : 방화벽)이 설치된 네트워크 도메인에서도 많이 발생하고 있다. 이는 지금까지 침입차단시스템만으로 자신의 네트워크를 안전하게 관리할 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

† 정 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학부
†† 준 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학부
††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터공학부 교수
논문접수 : 2001년 8월 4일, 심사완료 : 2001년 9월 26일

보안 관리를 위해서 관리자는 보안 시스템들이 설치된 네트워크 환경에 대한 사전에 전문적인 보안 지식을 갖고 있어야 하며, 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. 이에 복잡하고 다양한 방식의 보안관리 및 통신망 관리체계의 집중화, 자동화된 관리체계로의 전환, 그리고 이종간의 보안 시스템들에 대한 통합적인 관리를 위한 정책 관리가 요구되고 있다[10, 11].

정책 관리의 과정은 다양한 추상적인 계층으로 표현할 수 있다. 계층적 정책 모델의 특징은 상위 계층의 정책들이 하위 계층 정책의 서브셋(subset) 들에 의해서 정확하게 표현이 되었는지 그리고 제안된 정책의 목적과 정책 적용 대상들이 완벽하게 지원이 가능한지를 정책 계층의 모델을 통해서 분석이 가능하다.

따라서, 이를 위해서 상위 계층의 정책, 정제된 하위 계층의 정책, 그리고 이들의 동작과 최종적인 구현 절차 등 이들의 관계에 대해서 정형화된 표현이 필요하다. 즉, 관리자로부터의 개념적이고 추상적인 정책을 해당보안시스템이 이를 수행하기 위한 정책으로의 전환을 위한 정형화된 정책의 정제, 정책의 분류, 그리고 정책의 표현방식에 대한 정형화된 모델의 정립이 필요하게 되었다.

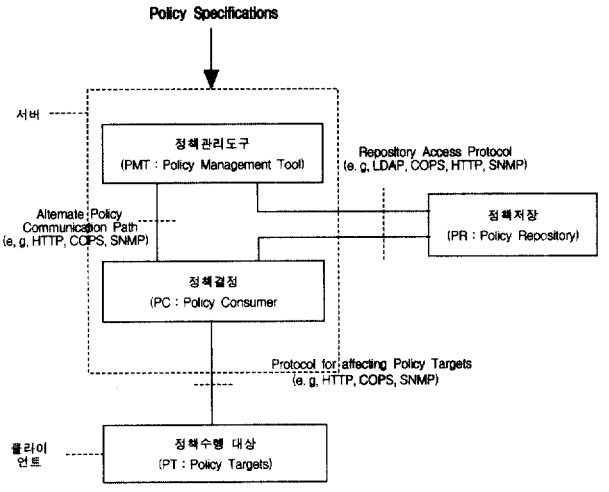
본 논문의 구성을 살펴보면, 2장에서는 정책기반의 네트워크관리(PBNM : Policy-based Network Management)의 개념과 기존의 정책 모델에 대한 연구에 대해서 살펴보고, 3장에서는 정책 기반의 통합보안관리시스템(Policy Based Integrated Security Management System)의 정책 모델을 제시하고 마지막으로 4장에서는 결론 및 향후계획에 대해서 언급하고자 한다.

2. 관련 연구

2.1 PBNM의 개요

정책 기반 통신 시스템은 IETF 표준화 문서중 "Policy Framework"에 기능이 정립되어 있다[2, 3]. 정책 기반의 네트워크 관리[4]는 네트워크에서 제공하는 QoS[5], 정보보안 및 자원을 공통된 형태로 제공하고, 이를 효율적으로 관리하는 데 있다. 이에 정책 기반의 네트워크 관리 시스템은 정책 규칙(Policy Rule)을 제정하고, 정책에 따라 네트워크를 운영하기 위해서는 통신망 구성장치를 실시간으로 모니터링하여, 동적으로 변화되는 정보를 신속하게 정책 기반 관리 시스템에게 전송해야 한다.

IETF의 정책 프레임워크 규격에서는 기능적 컴포넌트로 정책관리 도구(Policy Management Tool), 정책정보 저장(Policy Repository), 정책 결정(Policy Consumer), 정책수행 대상장치(Policy Target의 4개의 기능 블록으로 구성되어 있다. (그림 1)는 정책 기반 관리시스템의 프레임워크를 나타낸 것이며, 각 블록별 상세 내용은 다음과 같다.



(그림 1) 정책기반 관리시스템의 프레임워크

- 정책관리도구(PMT : Policy Management Tool)
  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. 이때, 규칙은 추상적 또는 인간이 이해하기 쉬운 형태에서 정책데이터베이스가 이해할 수 있는 정책정보모델의 구문으로 변환되어 데이터베이스에 저장된다.
- 정책결정(PC : Policy Consumer)
  PDP(Policy Decision Point) 또는 정책서버라고도하며, 정책데이터베이스내의 정보가 변했다는 것을 인지하여 정책데이터베이스로부터 정책정보를 검색하고, 정책을 정책 클라이언트가 받아들일 수 있는 형태나 구문으로 변환한 후 정책 클라이언트로 전송한다.
- 정책저장(PR : Policy Repository)
  정책 저장소(Policy Repository)는 정책 규칙을 데이터베이스로 객체지향 개념에 입각하여 중앙 혹은 지역적으로 분산형태로 저장 및 관리를 담당한다.
- 정책수행 대상(PT : Policy Target)
  PEP(Policy Enforcement Point) 또는 정책 클라이언트라고도 하며, 정책결정으로부터 전송된 정책 규칙정보를 자체 시스템에서 적합한 형태로 저장하여 이를 수행한다. 수행된 결과를 정책기반 서버에 보고하거나 혹은 동적으로 처리되는 중요한 정보를 보고하는 기능을 수행한다. 또한, 동

적인 네트워크 상태를 모니터링하는 정책결정과 함께 정책 서버를 구성한다.

2.2 PBNM의 정책 모델

2.2.1 IETF의 정책 모델

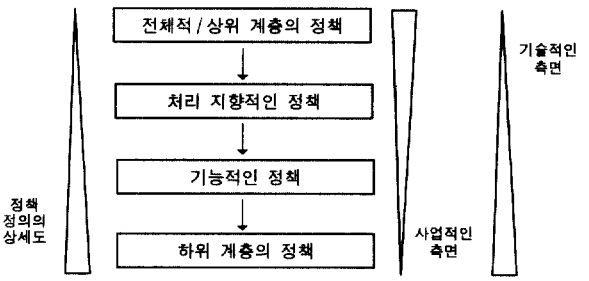
IETF 정책핵심 정보모델에서 객체 클래스는 정책 정보와 정책을 제어하기 위한 구조 클래스와 구조 클래스간의 관계를 특정지우는 연산 클래스로 계층화하여 정의하였다. 정책 규칙은 우선 순위를 가지면, 정책 그룹과 규칙에 따라 7개의 정책으로 구분하여 단계적인 정책 기반의 정보모델을 제시하였다[3].

- 동기정책(Motivation Policies) :
  동기 혹은 계기가 되는 정책으로 정책의 목적이 어떻게 성취되는가에 상관없이 단지 정책의 대상이 된다. 구성정책과 사용정책들은 동기정책의 한 종류로 정의된다. 예를 들면 오전 8시부터 오후 3시까지의 행위에 대해서는 백업 파일 시간표를 작성한다.
- 구성정책(Configuration Policies) :
  관리대상 객체(예를 들면, 네트워크 서비스)에 대한 일반적인 장치를 정의한다. 대표적인 예로 네트워크 포워딩(forwarding) 서비스 또는 네트워크 프린트 사용에 대한 정책설정 등이 있다.
- 설정정책(Installation Policies) :
  설정을 실행하는 메커니즘에 대한 구성뿐만 아니라 구성요소나 시스템에 대해서 설치해야 할지 혹은 하지 말아야와 설치를 하는 경우에는 무엇을 어떻게 해야 할 것인가에 대해서 정의한다. 예를 들면 구성요소 A를 설치하기 위해서는 먼저 구성요소 B와 구성요소 C가 성공적으로 설치가 되어 있어야한다.
- 오류와 이벤트정책(Error and Event Policies) :
  설치된 장비가 오전 8시부터 오후 9시 사이에 결함이 있는 경우, 시스템 관리자 또는 Help desk 에 연락한다.
- 사용정책(Usage Policies) :
  정의된 "usage"데이터를 기반으로 관리대상 객체의 구성과 선택을 제어한다. 구성 정책들은 "usage policies"에 의해서 변경이나 재적용이 가능하다. 예를 들면, 사용자가 "gold" 서비스 그룹의 회원으로 승인을 받은 후 네트워크 포워딩 서비스의 단계를 높여준다.
- 보안정책(Security Policies) :
  해당 자원에 대한 사용자의 접근을 허가/금지, 인증 메커니즘의 적용, 그리고 감사(auditing)와 계정(accounting)관리에 관한 정책을 말한다.
- 서비스 정책(Service Policies) :
  네트워크와 다른 서비스들에 대한 정책을 말한다. 예를 들면, 광역의 기간망의 인터페이스는 큐잉타입(queuing type)을 정의해한다.

2.2.2 Rene Wies의 정책 모델

Rene Wies는 관리자로부터의 집합적이고 추상적인 상위 계층의 정책으로부터 관리 대상 객체(MO)에 대한 하위 계층의 정책으로의 변환을 위해서 다양한 정책을 분류하고 전이(transformation)과정을 통해서 구체적인 정책으로 정제하였다. 그리고 정제한 정책을 탬플릿(template)하여 최종 목적인 관리대상 시스템에 대해서 정책을 적용시키는 4단계의 계층적 정책 구조를 제안하였다. (그림 2)는 Rene Wies가 제안한 분산시스템 관리를 위한 계층적 정책 구조를 나타낸 것이며 각 계층별 상세 내용은 다음과 같다[6, 7].

- 전체적/상위 계층의 정책(Corporation/High-Level Policies) :
  전체적인 목적과 직접적인 관련이 있으며, 태스크(Task)의 조정과 제공된 서비스의 특징을 정의하며, 정책의 전체적인 목적과 직접적인 관련이 있다.
- 처리 지향적인 정책(Process Oriented Policies) :
  관리 플랫폼(management platform)들과 응용들의 적용과 사용 방법에 대해서 정의한다.
- 기능적인 정책(Functional Policies) :
  관리 서비스의 사용에 대해서 정의한다.
- 하위 계층의 정책(Low-Level Policies) :
  관리대상 객체(MO : Managed Objects) 계층의 동작에 대한 정책을 정의한다.

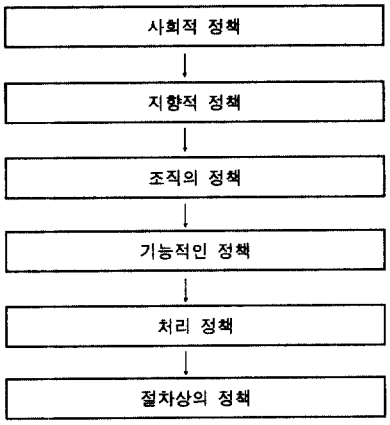


(그림 2) Rene Wies의 계층적 정책모델

2.2.3 Masullo & Calo의 정책 모델

Masullo & Calo[8]의 정책 모델은 6계층의 정책 모델로 구성된다. 사회적 정책(Societal Policy), 지향적 정책(Directional Policies), 조직 정책(Organizational Policy), 그리고 기능적 정책(Functional Policy) 등 상위 계층은 개념적이고 추상적인 정책을 규정하며, 사람의 언어로 정의되고 인간에 의해서 해석된다. 이에 반하여 기능적 정책(Functional Policy), 처리정책(Process Policy), 그리고 절차상의 정책(Procedural Policy) 등 하위 계층은 구체적이고 시스템에 의존적인 정책으로 구성된다. (그림 3)은 Masullo와 Calo의 계층적 정책 모델을 나타낸 것이며, 각 계층별 상세 내용은 다음과 같다.

- 사회적 정책(Social Policy) :
  사회적인 법률이나 지켜야 할 규정 등에 대해서 정의.(예 : 성공을 위한 가장 우선적으로 지켜야 할 윤리적인 규범 등)
- 지향적 정책(Directional Policy) :
  추상적인 형태를 유지하며, 조직적이고 종합적인 목적에 대한 정책이 수행되어야 할 방향을 설정한다.(예; 최종 목적의 등급 혹은 특징)



(그림 3) Masullo와 Calo의 계층적 정책 모델

- 조직적인 정책(Organizational Policy) :
  상위의 계층의 추상적이고 집합적인 정책을 이해가 쉽도록 구체화시키며, 계획의 수립과 접근 방향의 정형화 그리고 계약상의 협의 또는 프로그램의 등급 등 정책의 목적에 대해서 규정한다.
- 기능적인 정책(Functional Policy) :
  상위 계층에서 개념적인 정책을 실용적인 방법으로 표현하기 위해서 대응시키는 과정을 수행하며, 상위 정책인 조직의 정책을 인식하고 이를 보다 정형화된 형태로 표현한다. 예를 들면, 무결성에 대한 요구사항과 네트워크 시스템의 구성에 대한 규정 또는 작업량의 측정 등이 있다.
- 처리 정책(Process Policy) :
  상위 계층의 추상적이고 개념적인 정책을 처리과 정을 통해서 번역하는 기능을 수행한다. 각 계층별로 분할된 정책은 구조화된 언어인 Pseudo코드, 매크로(macros), 이진 구성법으로 표현, 그리고 데이터베이스 스키마(schemas) 등으로 표현된다. 즉, 처리 정책 계층에서는 시스템을 지원하기 위한 인코딩이 행해진다.
- 절차상의 정책(Procedural Policy) :
  인코딩된 정책에 대한 해석이 완료되며, 컴퓨터가 이해할 수 있는 형태의 언어로 작성된다. 즉, 추상적인 형태의 최상위의 정책은 관리 대상 시스템을 지원하는 소프트웨어 형태로 표현된다.

앞서 언급한 'Rene Wies'와 'Masullo와 Calo'가 제안한 정책모델은, 추상적인 개념의 상위 정책을 단계별로 시스템에 의존적인 정책으로의 정제시키는 특징을 갖고 있으며, 이는 광범위한 분산관리 시스템을 적용하기에 적합한 모델이다. 그러나 Masullo와 Calo의 모델은 상위 정책의 정제과정이 복잡하고 각 계층별 모델에 대한 상세한 내용은 정의되지 않은 단점을 갖고 있다. IETF의 정책모델은 분산시스템에서 QoS (Quality of Service)와 정보보안과 관련한 7단계의 정책모델을 제시하고 있으나 아직 표준화가 진행 단계에 있으며, 정보보안과 관련한 정책의 표현에 문제가 있어서 이를 해결하기 위한 표준화 연구가 진행되고 있는 상태이다.

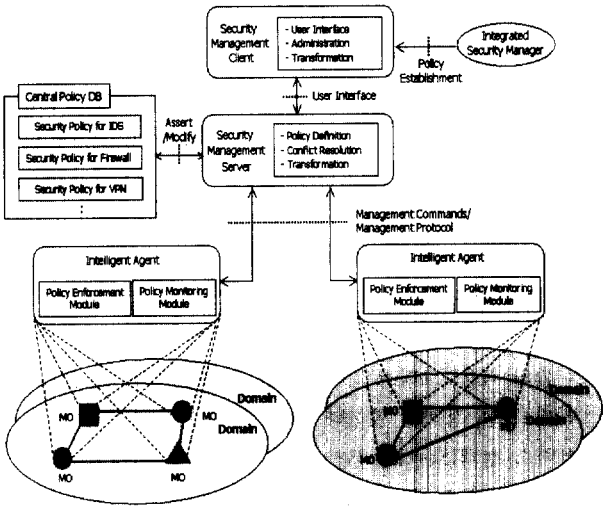
이에 본문에서는 보안관리의 측면에서 이종의 보안관리시스템에 대한 정책기반의 통합보안관리시스템(PB-ISMS : Policy Based-Integrated Security Management System) 개발에 적합한 5단계의 계층적 정책모델을 제시하고, 이들 각 계층별 정책의 상세 내용과 이를 구현하기 위한 정책 프레임워크, 정책의 분류 및 정형화 그리고 Z-Notation을 이용한 보안정책의 표현을 등에 대해서 언급하고자 한다.

3. PB-ISMS의 정책 모델

3.1 PB-ISMS의 개요

정책기반의 통합보안관리시스템(PB-ISMS : PB-ISMS : Policy Based-Integrated Security Management System)은 이종의 분산환경에서 다양한 보안 관련 시스템을 중앙 관리 즉, 정책을 설정하고 모니터링하는 기능을 수행하며, 보안 관리자에게 네트워크 보안 상태의 전체적인 뷰(View)를 제공한다.

또한, 보안 정책에 대해서 전문적인 지식이 부족한 사용자의 추상적인 정책 설정 요구에 대해서 보안관리서버에서 이를 수행하며, 추가로 보안시스템에 대해서 통합 관리를 하고자 할 경우에는 기존의 보안 시스템들의 재구현이나 수정이 필요 없이 그에 해당하는 에이전트[12]를 추가함으로써 이들을 수용할 수 있는 확장성을 갖고 있다. (그림 4)는 본 논문



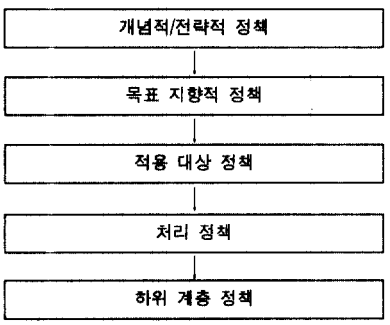
(그림 4) PB-ISMS의 전체 구조

에서 제시하는 분산 도메인 환경에서 다양한 관리객체(MO : Managed Object) 즉, 침입차단시스템(일명 : 방화벽), 침입탐지시스템(IDS : Intrusion Detection System), 그리고 가상사설망(VPN : Virtual Private Network)시스템 등을 통합관리하는 PB-ISMS의 전체구조를 나타낸 것이다.

3.2 PB-ISMS의 계층적 정책 모델

정책 관리의 과정은 다양한 추상적인 계층으로 표현할 수 있다. 계층적 정책 모델의 특징은 상위 계층의 정책들이 하위 계층 정책의 서브셋(subset) 들에 의해서 정확하게 표현이 되었는지 그리고 제안된 정책의 목적과 정책 적용 대상들이 완벽하게 지원이 가능한지를 정책 계층의 모델을 통해서 분석이 가능하다. 이를 위해서 상위 계층의 정책, 정제된 하위 계층의 정책, 그리고 이들의 동작과 최종적인 구현 절차 등 이들의 관계에 대해서 정형화된 표현이 필요하다[6-8, 12].

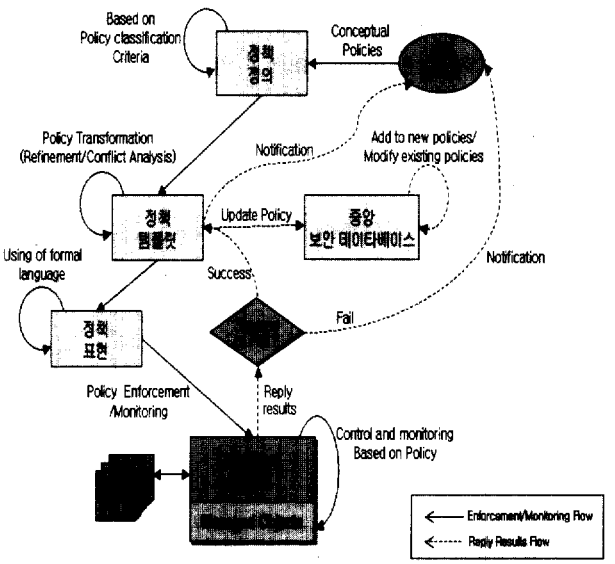
PB-ISMS의 계층적 정책모델은 상위 3계층은 개념적이고 추상적인 의미의 정책을 나타내고, 하위 2계층은 해당 정책을 실행하는 에이전트와 관리대상 객체(MO : Managed Object)들 즉, 보안시스템들이 이해할 수 있는 형태의 정책을 표현한다. (그림 5)는 정책기반의 통합보안관리시스템(PB-ISMS : Policy Based Integrated Security Management System)의 계층적 정책 모델을 나타낸 것이며, 각 계층별 상세 내용은 다음과 같다.



(그림 5) PB-ISMS의 계층적 정책모델

- 개념적/전략적 정책(Conceptual/Strategic Policies) :
  관리자로부터의 개념적이고 추상적인 정책 단계
- 목표 지향적 정책(Goal-Oriented Policies) :
  보안 시스템에 대한 정책의 기능과 행위에 대한 정책. 예를 들면, 정책에 대한 허가, 거부, 인증, 그리고 정책의 위임 등.
- 목적 대상 시스템 정책(Target Policies) :
  정책의 적용 대상이 되는 시스템들이나 관리 대상 도메인 등에 대한 정책.
- 처리 정책(Process Policies) :
  최종 정책을 수행하는 해당 보안시스템을 관리하는 에이전트 시스템에 대한 정책. 이때 정책은 에이전트 시스템이 이해할 수 있는 형태로 표현되어야 하며, SNMP나 OSI(open system interconnection) 시스템 관리 기능 등이 이에 해당된다.
- 하위 계층 정책(Low_Level Policies) :
  관리대상 객체(MO : Managed Object)에 대한 기능과 자원 관리에 대한 정책.

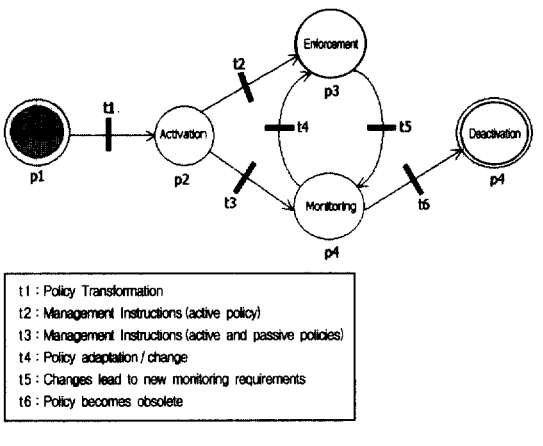
(그림 6)은 앞서 언급한 계층적 정책 모델을 기반한 PB-ISMS의 계층적 정책 프레임워크를 나타낸 것이다. 정책의 정의와 정책 템플릿그리고 정책의 표현에 대한 상세한 내용은 다음절에서 각각 설명하고, PB-ISMS의 에이전트와 중앙 정책을 다루는 정책 데이타베이스에 대한 내용은 본 논문의 범위에 벗어나서 다루지 않기로 하겠다.



(그림 6) PB-ISMS 계층적 정책 프레임워크

3.2.1 정책의 라이프사이클

정책의 라이프사이클(life-cycle)은 다양한 상태의 변화로 전이된다. (그림 7)은 PB-ISMS의 정책의 라이프사이클을 Petri Net[13, 14]으로 표현한 것이다.

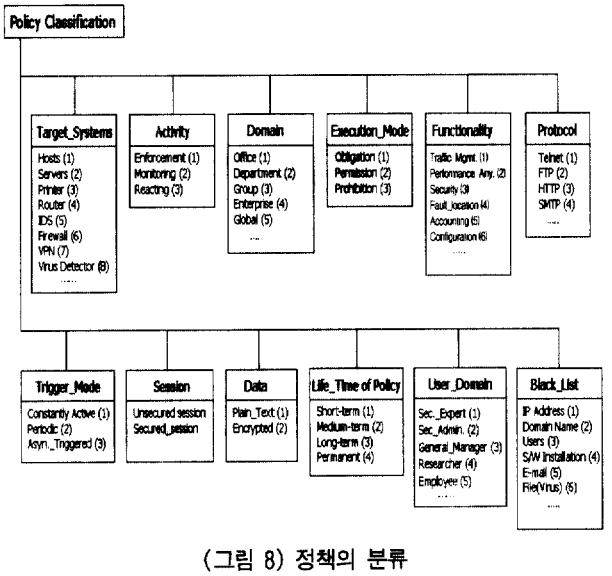


(그림 7) 정책의 라이프사이클

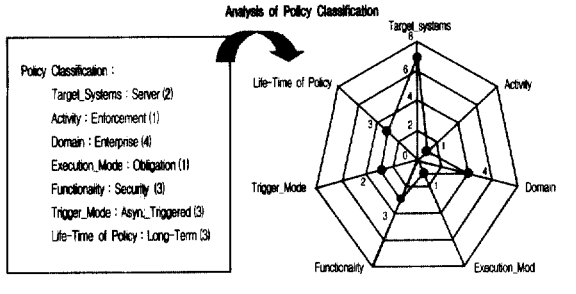
PB-ISMS의 정책의 라이프사이클의 동작을 살펴보면, 우선 p1은 개념적이고 추상적인 정책을 정의(definition)하고 이들에 대한 정제 과정을 거쳐서 정책을 적용할 수 있는 활동(activation) 상태인 p2로 전이된다. 활동 상태의 정책에 따라서 정책의 적용(enforcement)상태인 p3와 모니터링(monitoring) 상태 p4로 전이된다. 이후 모니터링 상태에서 정책의 변경사항이 발생할 경우 새로운 모니터링의 요구 사항을 변경하고 이를 수행한 후 정책이 종료된다.

3.2.2 정책의 분류

관리자로부터의 개념적인 정책을 보다 이해하기 쉽게 표현하고 이를 통해서 정책을 실행하기 상세한 정보로의 전환과 정책 템플릿을 정의하기 위한 정책간의 동질성과 이질성의 구분이 선행되어야 한다. 이를 위하여 정책에 대한 분류가 필요하다. (그림 7)은 PB-ISMS에서 발생할 수 있는 개념적 정책에 대한 분류를 나타낸 것이다.



(그림 8) 정책의 분류



(그림 9) 정책 분류의 적용 예

(그림 9)는 개념적 정책 "서버에 접근하기 위한 패스워드의 설정시 대·소문자를 혼합해서 6자 이상이거나 대·소문자의 혼합이 아닌 경우에는 적어도 8자 이상이어야 한다."는 패스워드 설정에 관한 정책에 대한 정책을 분류하고 이를 분석한 예를 나타낸 것이다.

3.2.3 정책의 템플릿

관리자로부터의 개념적인 정책에 대한 분류와 이를 기반으로 보다 상세한 정책의 표현을 위해서 정책을 정제하고 정책의 충돌을 분석하는 과정을 통해서 정책의 템플릿(template)을 표현한다. (그림 10)은 (그림 9)의 정책 분류를 기반으로 작성한 정책의 템플릿을 나타낸 것이다.

```
POLICY TEMPLATE : workstationPsswordPolicy
        Author(s) : D. Y. Lee
        CreationDate : 08/06/2001
        StatusOfRefinement : completed/applicable
        DerivedFromParentPolicy : generalAccessPolicy
        ManagementScenario : systems management
        ManagementFunctionality : security management
        Service : data processing and authentication service
        LifeTime : long term, until changed
        SubjectCharacteristics/Domain : system administrator
        TargetCharacteristics/Domain : all workstations
        TriggerMode : asyn.Triggered
        TriggerCharacteristics/Domain : triggered by exec passwd
```

(그림 10) 정책 템플릿 적용 예

3.2.4 정책의 표현

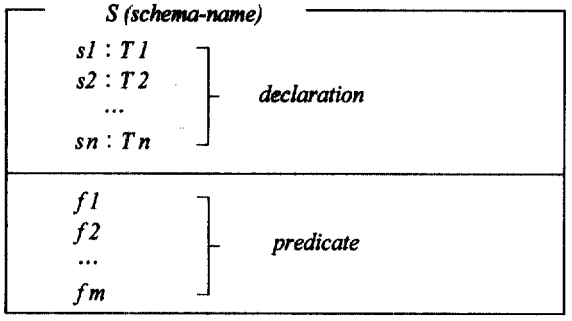
정책기반의 네트워크 관리에 있어서 정책의 표현을 위한 언어의 개발은 아주 중요한 문제로 대두되고 있다. 지금까지 정책을 표현하는 언어는 다양하게 연구가 진행되고 있다[15]. 최근 이러한 정책의 규칙은 QoS(Quality of Service)관리에서 블록화된 그래픽 구조로 표현이 가능하나, IETF에서는 정보보안을 위한 기능으로 세부적으로 표현이 어려운 관계로 정보보안 정책규칙을 위한 별도의 언어를 대상으로 표준화 연구 진행 중에 있다.

본 논문에서는 소프트웨어 설계와 정의에 사용되는 Z-Notation[16-18]이라는 언어를 사용하였다. Z-Notation은 1980년대 영국 옥스포트 대학의 'Computing Laboratory'에서 개발되기 시작해서 1999년 8월에 ISO에서 Draft화된 컴퓨터 프로그램의 정의를 상호전달하고 표현하기 위하여 수학적으로 표현한 형식화된 언어이다.

Z-Notation은 Set이론과 수학적 논리를 기반으로 구성되어 있으며, 표현하고자 하는 대상과 이들의 특징을 선언 - 술어(declaration - predicate) 패턴의 스키마(schema)로 표현할 수 있다. Z의 표현 스키마는 아래와 같은 수평적 형태(horizontally form)와

$$S \triangleq [s1 : T1 ; s1 : T2 ; \cdots ; sn : Tn \mid f1 \wedge f2 \wedge \cdots \wedge fn]$$

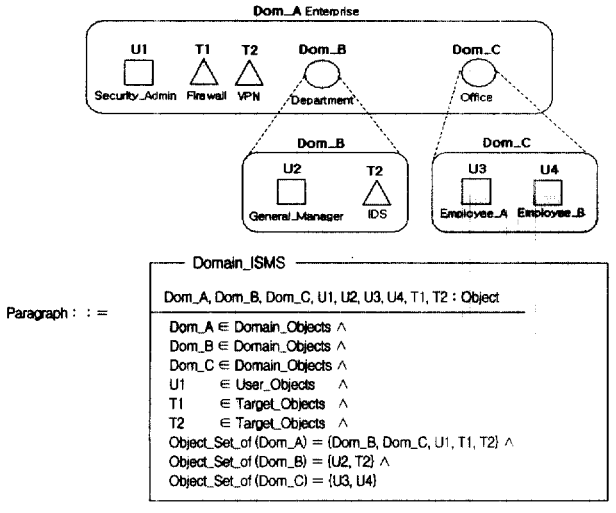
일반적으로 많이 사용하는 수직적 형태(vertical form)로 표현할 수 있으며,



$si : Ti\,(i = 1 \cdots n)$는 서명(signature)이고, 제안된 술어(predicate) 스키마 $fi\,(i = 1 \cdots m)$의 논리곱을 나타낸 것이다. $si\,(i = 1 \cdots n)$의 집합을 변수라고 하며, $Ti\,(i = 1 \cdots n)$은 타입을 의미한다. 그리고 각 각의 fi는 선언 부분의 순서에 해당하는 계산식을 나타낸 것이다. 본 논문에서는 수직적 형태의 스키마를 이용해서 정책을 표현하였다.

Z-Notation의 특징을 살펴보면, 우선 자연어를 사용하며, 일반적으로 제기된 문제에 대해서 해결책을 발견하고, 규정에 맞는 설계가 되었는지를 증명하기 위해서 수학적 방법을 사용한다. 현실 세계에서는 객체들에 대한 수학적 요소를 연결시키기 위해서 자연어를 사용한다. 이는 변수들에 대한 적절한 네이밍(naming)과 주석을 통해서 실현할 수 있으며, 정확하게 정의된 규정은 사용자로 명확한 의미를 해설할 수 있게 도와준다.

또한, Z-Notation은 정제의 특징을 갖고 있다. 설계모델의 구성과 요구된 행위를 인지하기 위해서 간단한 수학적 데이터 타입을 사용해서 시스템을 개발한다. 이들에 대한 정제 과정을 통해서 설계의 적절성을 파악하고, 시스템 구현을 용이하게 할 수 있다. (그림 11)와 (그림 12)는 Z-Notation을 이용한 보안정책의 표현의 예를 나타낸 것이다.



(그림 11) PB-ISMS의 관리도메인 정책 표현

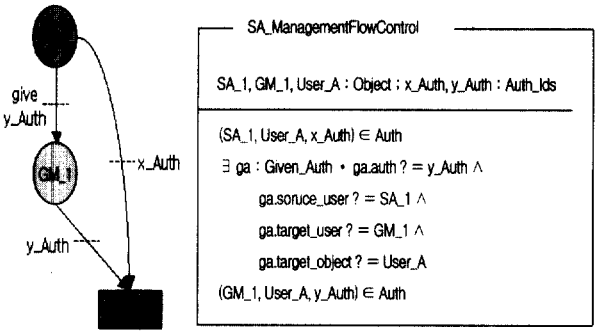
● 관리 도메인

PN-ISMS의 관리 영역인 상위 도메인(Domain) Dom_A와 하위 도메인 Dom_B, Dom_C의 구성과 이들의 사용자와 목표객체에 대한 전체적인 구성에 대해서 Z-Notation으로 표현한 것이다.

● 정책의 위임(obligation)

보안관리자(SA : security administrator)의 역할에 대한 정책은 우선 보안관리자들의 등급을 분류하고, 이들 등급에 따란 역할을 구별한다. 역할 정책의 경우, 목표 객체들에게 대한 인증의 권한을 갖게 되는 것을 의미하다. 따라서 보안관리자는 한 기관에서 하나 이상의 역할을 갖는 경우도 있다. 이때 상위의 관리자의 역할을 하위 관리자에게 권한을 부여할 수도 있다.

(그림 12)는 상위관리자(SA)가 하위 관리자(GM : General_Manager에게 User_A에 대한 인증의 권한을 부여한 것을 표현한 것이다.



(그림 12) SA가 GM에게 권한을 부여하는 정책 표현

본 논문에서 지시한 정책기반의 통합보안관리시스템(PB-ISMS : Policy-based Integrated Security Management System)의 구조와 계층적 정책모델을 제안하였다. 이는 2장에서 언급한 기존의 추상적이고 개념적인 형태의 정책모델을 보안정책 관리의 측면에서 이종의 보안관리시스템을 통합관리 시스템에 적합한 계층적 모델과 프레임워크를 제시하였다. 그리고 제시된 모델을 기반으로 실제 환경에 적용하기 위해서 다양한 정책을 분류하고 이를 정형화하였다. 또한, 현재 정책기반 네트워크 모델의 가장 큰 해결과제에 하나인 보안정책의 표현에 어려움을 본 논문에서는 Z-Notation이라는 형식화된 언어를 사용하여 표현함으로 이를 해결하고자 하였다.

4. 결론 및 향후계획

최근 이종의 분산환경에서는 복잡하고 다양한 방식의 보안관리 및 통신망 관리체계의 집중화, 자동화된 관리체계로의 전환, 그리고 이종간의 보안 시스템들에 대한 효율적이고 통합적인 관리를 위한 정책 관리가 요구되고 있다. 따라서 관리자로부터의 추상적인 정책을 해당보안시스템이 이를 수행하

기 위한 정책으로의 전환을 위한 정형화된 정책의 정제, 정책의 분류, 그리고 정책의 표현방식에 대한 정형화된 모델이 필요하게 되었다. 이에 본문에서는 정책기반의 통합보안관리 시스템(PB-ISMS : Policy Based - Integrated Security Management System)의 계층적 정책모델과 이를 구현하는 방법론을 제안하였다.

본 논문에서 제안한 PB-ISMS의 계층적 정책모델은 상위 3계층은 개념적이고 추상적인 의미의 정책을 나타내고, 하위 2계층은 해당 정책을 실행하는 에이전트와 관리대상 객체(MO : Managed Object)들 즉, 보안시스템들이 이해할 수 있는 형태의 정책으로 5계층으로 구성되어 있다. 3계층에 해당되는 즉, 관리자의 개념적인 정책에 대해서 정책을 분류하고 보다 구체적인 정책 템플릿을 작성하였다. 그리고 이를 기반으로 수학적 기반의 소프트웨어 설계 및 정의에 적합한 Z-Notation을 이용하여 보안 정책을 표현하였다.

그리고 향후 계획으로는 다양한 정책간의 충돌 발생하였을 경우, 이를 분석하고 검출하는 알고리즘의 개발과 제안된 모델을 기반으로 PB-ISMS을 구현하여 실제 네트워크 환경에서의 성능에 대한 검정 및 보완작업이 병행되어야겠다.

참 고 문 헌

[1] C. Pfleeger, 'Security in Computing Second Edition', Prentice Hall, 1997.

[2] M. Stevens, "Policy Framework," Internet Draft, draft-oeft-policy-framework-00.txt, Sep. 1999.

[3] B. Moore, et., "Policy Core Information Model-Version 1 Specification," Internet Draft, draft-policy-core-info-model-06.txt, IETF, May. 2000.

[4] Susan Hinrichs, "Policy-Based Management : Bridging the Gap," Computer Security Applications Conference, 15th Annual, pp.209-218., 1999.

[5] Raju Rajan, Diesh Verma, Sanjay Kamat, Eyal Felstaine, Shai Herzog, "A Policy Framework for Integrated and Differentiated Services in the Internet," Journal of IEEE Network, Sep./Oct., 1999.

[6] Rene Wies, "Using a Classification of Management Policies for Policy Specification and Policy Transformation," Integrated Network Management IV, pp.44-56, 1995.

[7] 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.

[8] 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

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

[10] 이동영, 김동수, 홍승선, 정태명, "웹 기반의 방화벽 통합보안관리 시스템 개발", 한국정보처리학회논문지, 제7권 10호, pp.3171-3181, 2000.

[11] 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.

[12] Jonathan D. Moffett and Morris S. Sloman, "Policy Hierarchies for Distributed Systems Management," IEEE Journal on Selected Areas in Communication, Vol.11, No.9, pp.1404-1414, 1993.

[13] James L. Peterson, "Petri Net Theory and The Modeling of Systems," Prentice-Hall, 1981.

[14] Kurt Jensen, "Coloured Petri Nets : Basic Concepts, Analysis Methods and Practical Use," Volume 1, Springer-Verlag, 1992.

[15] Gary N. Stone, Bert Lundy, and Geoffrey G. Xie, U.S Department of Defence, "Network Policy Languages : A Survey and a New Approach," Journal of IEEE Network January/February 2001.

[16] Spivey, J. M., 'The Z Notation - A Reference Manual', Prentice-Hall, second edition, 1992.

[17] Jim Woodcock, Jim Davies, 'Using Z : Specification, Refinement, and Proof', Published by Prentice-Hall, 1996.

[18] ISO Panel JTC1/SC22/WG19(Rapporteur Group for Z), Final Committee Draft, CD 13568.2, "Z Notation," August 24, 1999.

이 동 영

e-mail : dylee@rtlab.skku.ac.kr

1993년 동아대학교 전자공학(학사)

1998년 성균관대학교 정보공학(석사)

1993년~1997년 기아자동차 중앙기술연구소 연구원

현 재 성균관대학교 전기전자및컴퓨터공학부 박사수료

관심분야 : 네트워크 보안, 시스템보안, 네트워크 관리

김 동 수

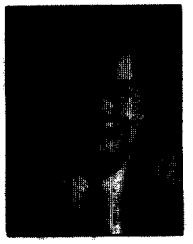
e-mail : dskim@rtlab.skku.ac.kr

1998년 성균관대학교 정보공학(학사)

2000년 성균관대학교 정보공학(석사)

현 재 성균관대학교 전기전자및컴퓨터공학부 박사과정

관심분야 : 네트워크 관리, 네트워크 보안, 시스템 보안



정 태 명

e-mail : tmchung@ece.skku.ac.kr

1981년 연세대학교 전기공학(학사)

1984년 University of Illinois Chicago, 전자계산학과 학사

1987년 University of Illinois Chicago, 컴퓨터공학과 석사

1995년 Purdue University, 컴퓨터공학 박사

1985년~1987년 Waldner and Co. , System Engineer

1987년~1990년 Bolt Bernek and Newman Labs., Staff Scientist

현 재 성균관대학교 전기전자및컴퓨터공학부 부교수

관심분야 : 실시간시스템, 네트워크관리, 네트워크 보안, 시스템 보안, 전자상거래.