2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

정책상속을 이용한 계층화된 정책 관리모델의 설계

연현정*, 이동석*, 나재훈**, 이상호*
*충북대학교 전자계산학과
**한국전자통신 연구원
e-mail:{yonnolbu, xman21}@cnlab.chungbuk.ac.kr
shlee@chungbuk.ac.kr

Design of A Hierarchy Policy Management Model Using Policy Inheritance

Hyun-Jeong Yeon*, Dong-Seok Lee*, Jae-Hoon Na**, Sang-Ho Lee*
*Dept of Computer Science, Chung-buk University
**Electronics and Telecommunications Research Institute

요 약

최근 인터넷 이용의 확산으로 도메인의 크기와 규모가 방대해짐에 따라 정보시스템의 관리는 더욱더 복잡해졌다. 또한, 개별적인 네트워크 기술의 개발과 운용으로 인해 시스템간의 정보 공유와 정보 보안 정책의 일관성과 정책 표현 기법의 공동화가 어렵게 되자, 체계적이고 일관된 네트워크 보안과 정책 적용에 대한 요구가 증대 되었다. 이러한 정책적용과 관리상의 문제점들을 해결하기 위해 이 논문에서는 유연성을 갖추면서, 일관된 정책을 집행할 수 있는 정책관리의 구조와 속성을 설계하고 정책상속을 이용한 계층화된 정책 관리모델을 제안한다.

1. 서 론

최근 인터넷 이용의 확산은 수많은 도메인 그룹들을 만들어내고 있으며, 도메인의 크기와 규모가 방대해짐에 따라서 분산 시스템의 관리는 점차 복잡해지고 있다. 그리고 전자상거래와 VPN서비스 등을 지원하기 위한 네트워크 보안 기술들은 인터넷에서 빠르게 전개되고 있는 실정이다.

특히, 초기 기업환경에서 보안 게이트웨이들을 설치하여 데이터에 대한 보안과 인증, 접근제어를 수행하였고, IP 보안 프로토콜 과 전송 레벨 보안프로콜(TLS/SSL)들은 인터넷 트래픽에서 end-to-end 와 hop-to-hop의 기밀성, 무결성, 인증보호를 제공하기 위해 사용되었다. 그러나 이러한 보안 장치들은 자신의 영역에 맞는 보안정책들을 적용하여 네트워크 망을 보안 도메인으로 세분화 시켰다. 이것은 인터넷에 대한 안전성은 증대시켰지만 관리 문제를 더욱 복잡하게 하였다.[1]

이 논문에서는 이러한 문제점들을 해결하기 위해 유연하고, 일관된 정책을 집행할 수 있는 정책관리의 구조와 속성을 제시하고, 이 정책관리 구조를 이용하여 논리적 도메인 계층화 관리모델을 설계하고자 한다. 논문구성은 2장에서 프레임워크 관리에 대해 기술하고, 3장에서 정책 속성 및 계층화 방법, 4장에서 정책상속 개념을 적용한 계층화된 정책관리 모델을 설계하고, 5장에서 결론 및 향후 연구방향을 제시한다.

2. 프레임워크 관리

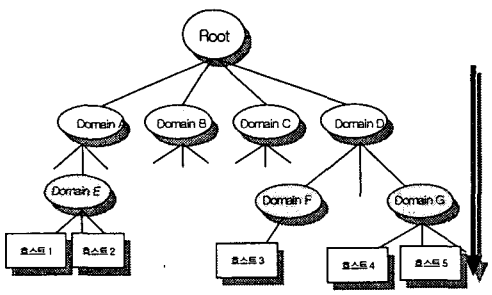
분산 정보 시스템의 관리는 한 사람이나 자동화된 엔터티로 중앙집중화 할 수 없기 때문에, 관리자를 분산시켜야 한다. 따라서 시스템 관리는 파티션으로 체계화시키고, 다중레벨에서의 다중 관리자는 서로간의 책임의 경계를 명확히 해야 한다. 왜냐하

면 다중 관리자가 정책을 집행하게 되는 경우 책임의 한계가 명확하지 않으면 정책협상에서 그만큼 정책충돌의 가능성이 높아지고, 일관된 정책을 집행하기 어려워지기 때문이다. 이렇게 책임의 경계를 명확히 하고 시스템 관리를 부분화함으로써 기존의 물리적 네트워크 연결방법과, 분산된 어플리케이션이나 계층적 관리 구조를 적용할 수 있게 된다.

이러한 구조에서는 서로 다른 기능과 서로 다른 상황에 맞는 동작들을 갖게 되지만 같은 객체에 대해서는 모두 책임을 갖게 되는 것이다. 예를 들어 같은 워크테이션 컴퓨터의 유지에 대해 사용자와 엔지니어는 다른 관리책임을 갖게 되는 것이다. 도메인은 정책관리를 명세화하기 위해 필요한 객체들을 그룹화함으로써, 관리 책임에 대한 구분을 분명히 할 수 있는 프레임워크를 제공해야 한다.[2][3]

도메인은 관리할 수 있는 객체들의 집합이며, 도메인 또한 다른 도메인의 멤버가 될 수 있고, 이런 경우 상위도메인에 대해 서브 도메인이라고 한다. 서브 도메인은 상위 도메인에게서 상속받은 정책들을 능동 수용하여 서브그룹들에게 각기 다른 정책을 적용시킬 수도 있고, 서로 다른 관리자에게 책임을 할당할 수도 있다. 서브도메인은 간접적으로 상위도메인의 멤버가 될 수 있으며 관리되는 객체는 직·간접적으로 상위 다중도메인의 멤버가 된다.

도메인에 대한 요구사항을 도식화하면 [그림1]과 같다. 이 정책 프레임워크 모델에서는 정책 상속을 위해 평면적인 도메인 구조보다는 계층적 도메인 구조를 사용한다.



[그림1 논리적 도메인 계층도]

[그림1]에서 계층적 보안 정책 시스템 모델을 살펴보면, 도메인 간의 보안 정책 설정은 실질적인 통신이 시작되기 전에 보안정책 협상(Security Association: SA)의 단계가 요구된다. 즉,'Domain A'와 Domain B'는 보안 정책 시스템으로부터 'Root'의 보안 정책을 상속받으며, 이때 'Domain A'와 'Domain B'는 자신의 도메인 환경에 맞는 정책을 능동 수용하게 된다. 동일한 방법으로 'Domain C'와 'Domain D'는 보안정책을 상속받는다. 정책의 구조 및 상속에 필요한 속성과, 액션들은 4장에서 자세하게 기술한다.

3. 보안정책 관리 구조

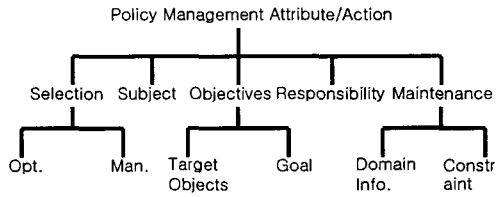
분산된 도메인의 각각의 정책 관리자는 일관성을 유지시키면서 유연성을 갖는 정책을 수행하기 위해서 필요한 기능들 즉, 도메인내의 활동을 모니터링하고, 정책을 결정, 실행, 추가, 삭제하는 기능 등을 가져야 한다.

3.1 정책 구조 개념과 속성

기업환경에서 정책관리자가 자사의 환경에 맞는 정책을 처음 생성하기 위해서는 조직의 목표를 세우고, 목표달성을 위해 정책을 결정하고 이를 수행해야 한다. 이 과정에서 정책관리자는 생성된 정책을 해석하고 정책충돌 가능성이 있는 요소들을 해결해야 하고, 생성된 정책은 조직의 목표를 이루기 위한 계획이 되는 것이며 관리자는 형식적인 것과 비형식적인 정책을 명세화해야 한다.

일관적인 정책만을 고수하다 보면 상속 가능한 정책 구조에는 부적합한 정책이 된다 .왜냐하면 관리자 콤포넌트 위주로 코드화된다면 이 정책은 유연성을 갖지 못하여 다른 환경에 재사용 될 수가 없게 되기 때문이다.

따라서 정책을 관리자 콤포넌트화 시키지 않고, 정책을 표현, 결정, 조작할 수 있는 정책구조가 요구된다. [그림2]은 분산 시스템에서의 계층화된 정책 속성과 액션구조를 변형한 결과이다.[6]



[그림2 정책 관리 속성/액션]

- Selection : Opt.(Optional)과 Man.(Mandatory)의 한쌍으로 구성되어 상위도메인에서 하위도메인으

로 정책을 상속시킬 때 사용되며, 하위도메인에서의 능동적 수용의 공간을 제공하고자 할 때는 Opt., 강제적으로 정책을 집행하려 할 때는 Man.을 선택한다. 이것은 정책을 상속시킬 때 계층적 구조의 최상위 도메인에서 정책의 일관성을 유지하면서도 유연성을 갖게 한다.

- Subject : 정책을 집행하는 주체로서 Policy Objective를 수행하기 위해서 누가 인증하고, 누가 의무를 갖는지에 대해 나타낸다.
- Objectives : 정책의 목표로서 Target Objects와 Goal의 한쌍으로 구성되어지며 Policy Goal은 High-level Goal 이나 Procedure로 표현된다.
- Responsibility: 정책협상시 책임의 한계와 관리 책임자를 나타낸다. 특히 도메인 내에서의 정책 상속시 관리되는 도메인내의 책임자를 분명히 명시한다.
- Maintenance : Domain Info.와 Constraint의 한쌍으로 Domain Info는 자신의 도메인 정보와 정책이 도메인에서 상속될 때 자신의 위치에서 상·하위 도메인의 정보를 유지하는데 사용되며, 이것은 신뢰된 도메인간에는 정책협상을 하지 않도록 하면서 도메인 계층화를 유지한다. Constraint는 정책의 응용성을 제한하는 것으로 일반적으로 시스템의 특성이나, 확장 등에 제한을 두어, 시스템의 안정성 확보하기 위해 사용된다.

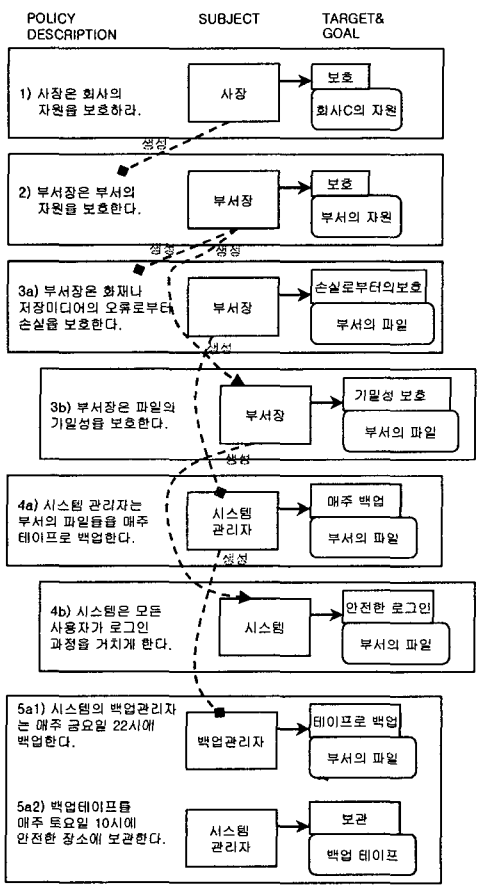
3.2 정책 계층화

정책을 계층화시킬 때 추상적인 개념의 상위레벨 정책을 기초로 하여, 이를 상속받는 하위레벨 정책은 상위레벨 정책보다 정교화, 세밀화 되는 정책생성 과정을 거치게 된다.

[그림3 정책관리 동작]

[그림3]은 정책관리 동작은 주체가 정책 명세서 대로 목표을 성취하기 위해서 대상에 동작을 취하는 과정이다.[6]

[그림4]는 [그림3]의 정책관리 동작 구조를 이용하여 하위레벨로 갈수록 정책생성이 세분화 되는 과정을 설명한 것이다. 상위레벨 정책은 하위레벨 계층으로 파티션 될수록 정책이 세분화되고, [그림4]에서 최상위 레벨 정책 1은 단지 회사의 자산을 보호하라는 추상적인 개념에서 시작하여 하위레벨 정책으로 계층화 될 수록 정책목적(policy objective)을 이루기 위한 액션들을 명확히 세분화한다. 상위레벨의 정책의 목표(Goal)는 하위레벨의 목표로 계층화 될 수록 하나 이상으로 세분화 되는데, 정책 4a는 정책 3a와 같은 대상을 갖지만, 목표는 '손실로 부터의 보호'에서 '매주 백업'으로 더욱 세분화된 정책을 생성할 수 있다. 또한 각 단계별 정책의 목표와 대상은 상위레벨의 목적과는 상당히 다를 수 있는데, 정책 3b에서의 목표는 '기밀성 보호' 이고, 정책 4b에서의 목표는 '안전한 로그인'이다. 이들 두 정책의 Subject(3b의 subject = 부서장, 4b의 subject = 시스템)나 대상(3b의 대상 = 부서의 파일, 4b의 대상 = 부서의 파일)들은 상위레벨의 목적 수행하기 위하여 다른 목표와 다른 주체를 갖을 수 있다.[6]



[그림4 정책 계층화]

이것은 상위 레벨의 정책이 정의 및 변동된다면, 하위레벨에서의 정책도 생성되고 변동될 수 있도록 하는 유연성을 갖는 것을 보여준다.

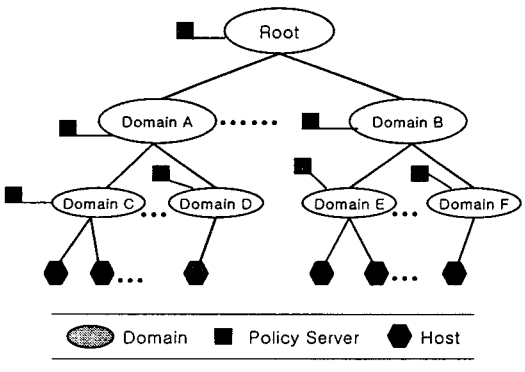
4. 정책 상속을 이용한 계층화된 정책 관리 모델

정책을 상속개념을 이용하여 도메인을 계층화시킬 경우, 계층화 진행 중에 초기 정책협상 과정을 거치게 되므로, 계층화 형성 단계 이후에서는 정책협상 과정은 불필요하다고 가정한다. 예를 들어 기업환경에서 동종업계간에 한번 신뢰된 도메인 구축은 도메인의 정책이 변동되기 전까지 유효하게 되어, 협상 과정을 생략할 수 있다. [그림2]의 정책관리 속성/액션 구조를 기반으로 [그림4]의 정책 계층화 방법을 각각의 도메인에 적용하면 [그림5]과 같다.

정책서버는 자신의 도메인 정보 및 정책을 관리 및 협상하는 역할을 하며, 최상위 도메인의 경우는 서브 도메인들의 정보를 관리한다.

[그림5]에서 초기 도메인 계층화 형성시,'도메인 A'가 '도메인 Root'의 정책을 상속하려고 할 때 '도메인 Root' 정책의 일부분(정책관리 속성/액션 구조에서 Selection<opt>부분의 정책)을 자신의 도메인 환경에 맞게 정책을 수정한 후에 정책을 설정한다. 각각의 '도메인 C, D, E, F'도 같은 방법으로 정책을 상속받는다.

기업 환경의 경우 지사 '도메인 A,B'가 본사 '도메인 Root' 정책을 따르면서 자사의 환경에 맞게 정책으로 수정 후 능동 수용 할 수 있다.



[그림5 정책상속의 도메인 계층화]

중위 도메인 레벨이나 최하위 도메인 레벨에서의 정책, 추가, 삭제, 수정 등의 변동은 '도메인 Root'의 승인을 취득한 후에 각각의 도메인에서 적용하게 된다.

5. 결론

방화벽, VPN같은 기존의 네트워크 보안기술들은 자신의 도메인을 보호하기 위해서 다른 도메인과의 통신에 대해서는 폐쇄적으로 운영되어 왔다. 이런 네트워크 보안기술들은 보안장치들을 이용하여 보안 도메인을 형성하였고, 네트워크 망을 각각의 정책이 적용된 보안 도메인으로 세분화 시켰다. 이로 인해 통합 도메인 관리의 어려움을 낳았고, 이 문제를 해결하기 위해서는 각각의 도메인 내에서 정책집행의 유연성과 도메인 통합관리를 위한 일관성 있는 모델을 필요로 한다. 따라서 이 논문에서는 구성 요소들 간의 연관성을 기반으로 도메인을 그룹화하고, 그룹화된 도메인을 정책 상속 개념을 이용하여 계층화시킬 수 있는 방법을 제시하였다. 이 논문의 모델을 구현하기 위해서 정책관리 속성과 액션의 관계를 명확히 하고, 다중 레벨에서의 정책충돌의 배제에 관한 연구와 계층별 제어 필드 필요한 계층별 제어 필드들에 대한 연구가 필요하다.

참고문헌

[1] John Zao, Luis Sanchez, Matthew Condell, Charles Lynn, Matthew Fredette, Pamela Helinek, Pajesh Krishnan, Alden Jackson, David Mankins, Marla Shepard, Stephen Kent, "Domain Based Internet Security Policy Management",DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00 Proceedings, vol.1, 1999

[2] M.S. Sloman. B.J. Varley, J.D. Moffett, K.P. Twidle, "Domain Management and Accounting in an International Cellular Network", Integrated Network Management 3th. 1993

[3] Dave Kosiur, "Understanding Policy-based Network", Wiley, 2001.

[4] Policy Framework, draft-ietf-policy-framework00.txt, Internet Draft, September 1999.

[5] Internet Draft, RFC 2026. October, 1999.

[6] Jonathan D.Moffett, "Policy Hierarchies for Distributed Systems Management", IEEE JSAC Special Issue on Network Management, vol 11, No.0 Dec.1993