논문 03-28-1B-11 한국통신학회논문지 '03-1 Vol 28 No 1B

대규모 네트워크 망에서 효율적인 보안정책관리를 위한 정책기반 보안관리모델

준회원 황 윤 철*, 엄 남 경*, 정회원 이 상 호**

Policy-Based Security Management Model for Efficient Security Policy Management in Large-Scale Network

Yoon-cheol Hwang*, Nam-Kyeong Um*, Sang-ho Lee** *Regular Members*

요 약

정보보호 기술이 부분적, 폐쇄적, 개별적 개발에서 개방적, 광역적, 통합적으로 변모해 감에 따라 각각의 보안 시스템을 구조적으로 통일하고 분산된 관리 방법을 일원화하기 위한 연구의 필요성이 증대되었다 그러나 아직까지는 각각의 보안시스템을 하나로 통합시켜 관리할 수 있는 공통된 프레임워크가 존재하지 않는다 따라서 이 논문에서는 각각의 보안 시스템을 체계적으로 관리하고 분산된 관리 방법을 일원화 할 수 있는 정책기반 네트워크 보안 관리 모델을 제시한다

ABSTRACT

As Information Security Technology has become rather transparent, wide, and integrated than in part, exclusive, and separated, A necessity of the study about integrating the separated distributed security systems into one module, has grown However, there is no integrated framework which can manage all separate security systems as one integrated one yet. Accordingly, we propose a new policy based network administrative model in this paper which can integrate individual security systems and distributed control way into one effectively

I. 서 론

인터넷을 구성하는 논리적인 도메인들의 규모가 확대됨에 따라 개체들간 Security Association 설정이 복잡해지고, 다양한 특성을 갖는 각 도메인들의 구성요소와 환경 등의 요인으로 각 시스템에 대한 보안정책 설정 및 제어가 어려운 문제로 등장하고 있다. 보안 정책은 조직의 정보와 자산에 접근하기 위해 사용자들이 지켜야 하는 규칙을 정의한 형식문으로 조직의 정보와 자산을 보호하기 위해 필요한 요구사항을 사용자와 운영자, 관리자에게 알려주기 위해 사용하고, 정의된 보안 정책에 따라 컴퓨터 시스템과 네트워크를 취득, 구성, 감사하기 위한 기본 지침을 제공하는데 그 목적이 있다[6][7] 국내의 현실은 보안의 정책적인 연구보다는 기술적인 연구에 편중되어 있고 외국의 연구 결과에 의존하고 있다. 보안 정책 관련 시스템을 외국으로부터 수입하여 사용하는데 한계가 있으며, 국내 실정에 맞고 국내의 보안 도메인 내에서 상호호환이 가능하며 나아가 전 세계와의 호환도 가능한 기술 연구와 시스템 개발이 시급히 요구된다[3][4][5] 이러한 현실적 요구를 바탕으로 이 논문에서는 정책 기반 네트워크 보안 관리의 모델에 대한 구조와 상호 작용 및 기능에 대해 서술하고, 이를 보다 효율적으로 관리하기 위해 기존의 네트워크들을 정책의 상호 연관성과 포함관계를 고려하여 세분화하고, 세분화된 영역을 조직단위로 한 계층화된 정책 기반 네트워크 보안 관리 모델을 제시한다 논문의 구성을 살펴보면,

* 충북대학교 대학원 전자계산학과 ** 충북대학교 전기전자 및 컴퓨터공학부
논문번호 020355-0813, 접수일자 2002년 8월 13일

2장에서는 기존에 산재해 있는 네트워크 망들을 어떻게 계층화시킬 것인지를 기술하고, 3장에서는 계층적 구조를 이용한 네트워크 보안 관리 모델을 제시하며, 4장에서는 그 구성요소에 대하여 기술한 후 5장에서 결론을 맺는다.

Ⅱ. 네트워크의 계층화

일관된 정책을 적용하는 정책 기반 네트워크 보안 관리 모델을 보다 더 체계적으로 관리하고 확장성을 뛰어나게 하기 위해서 이 논문에서는 기존에 존재하는 네트워크들을 일정한 기준에 의해 세분화하고, 세분화한 영역의 네트워크를 계층화 시켜서 각각의 계층마다 필요한 정책들을 별도로 관리하는 모델을 설계한다. 기존의 네트워크들을 세분화하는 기준은 동종의 조직 및 그룹의 부서 단위로 세분화하는 것을 의미하는 것으로, 이 세분화된 도메인은 다음의 [그림1]과 같이 조직의 본사와 지사, 계열사 간의 상관관계를 고려하여 계층화시킨다. 아래의 [그림1]에서는 H그룹 본사 도메인을 최상위에 위치시키고, 자동차 도메인, 전자 도메인, 건설회사 도메인을 본사 도메인의 하위에 위치시킨다. 또한, H그룹 자동차회사 도메인은 영업소, 공장, A/S 도메인으로 나뉘어지고 그 하위에 각각의 호스트들이 위치한다. 나머지 본사 도메인의 하위 도메인들 역시 이와 같은 형태로 도메인이 구성된다.

앞의 [그림1]에서 동종의 조직을 본사와 지사, 계열사, 하청 업체간의 상관관계를 고려하여 계층화했는데, 각 계층의 도메인은 그 회사의 부서 및 팀에 부여되는 역할에 의해서 다시 계층적으로 구성된다. 즉, 최상위에 위치한 도메인인 H그룹 본사와 중간 위치의 도메인인 H 자동차, H전자, H건설 도메인 그리고, 최하위에 위치한 도메인인 지사 및 하청 도메인은 각각 회사의 운영 방침에 의해서 부서 및 팀이 분류되는데, 이는 최상위에 위치한 도메인이나 최하위에 위치한 도메인이나 모든 조직에서 유사하게 나타난다.

[그림1]의 중간 위치의 도메인 중에서 H자동차 도메인의 내부 조직도를 업무의 역할계층으로 표현하면 다음 [그림2]와 같이 표현할 수 있다.

각각의 역할에 그에 정당한 책임과 권한, 자격이 있는 사용자를 배치할 수 있는데, [그림2]에서 총괄은 회사의 사장을, sub총괄에는 이사진을, 또한 각 부서에는 부서장을, 마지막으로 가장 말단에는 해당 담당자가 이에 배치된다. 위의 [그림2]은 최상위에 위치한 도메인인 그룹본사 도메인과 최하위에 위치한 도메인인 지사, 하청업체 도메인에서도 유사하게 나타난다. 하지만 계열사의 회사 특성에 따라서 부서나 직책, 업무는 가변적일 수 있다. 다시 말해서, [그림2]은 자동차회사 뿐만 아니라 다른 회사에서도 거의 비슷하게 나타나지만, 자동차회사에는 업무상 꼭 필요한 부서일지라도, 전자회사나 건설회사에서는 해당 부서가 필요 없을 수 있다. 이러한 역할계층에서 역할은 사용자 및 접근권한의 모음으로 트랜잭션 형태의 접근권한이 시스템 관리자에 의해서 일괄적으로 부여된다. 시스템 관리자는 기업이나 조직에서 수행할 업무 기능에 따라 역할을 생성하여 역할에 접근권한을 부여하고, 사용자를 책임과 자격에 따라 역할에 배정하게 되는 것이다. 이런 시스템에서는 접근권한이 역할에 부여되므로 시스템이 변경될 때, 필요에 따라 쉽게 새로운 접근권한을 역할

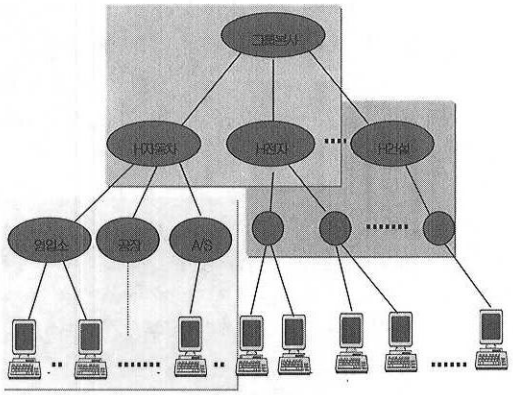

그림 1. .조직(그룹) 단위로 계층화한 도메인 예

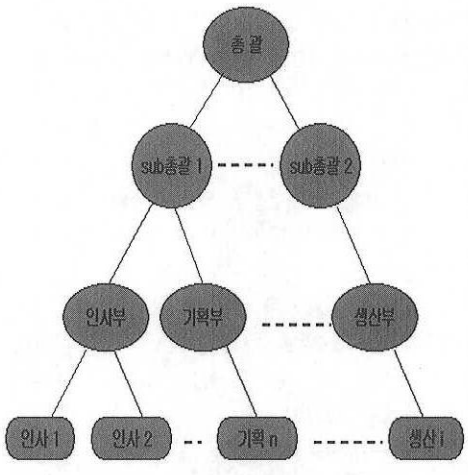

그림 2. H자동차회사의 역할 계층

에 부여하거나 삭제할 수 있고, 조직의 요구에 따른 접근 제어 정책의 관리를 용이하게 한다. 이러한 역할간의 계층관계는 접근권한의 상속이 이루어질 수 있도록 유지되어야 하고, 역할의 특성에 따라 상호 배타적 역할을 설정하거나, 역할간의 관계에 따라 임무분리를 요하는 보안정책이 규정되어야 한다. 역할의 접근권한과 상속방법 및 역할의 배정의 표현이 모호한 문제점을 해결하기 위해 역할의 상속속성에 따라 역할의 계층을 분류하는 부분순서관계(Partial Ordering relation)에 따라 계층화된 도메인을 구성하도록 한다

이렇게 [그림2]과 같이 조직 단위로 계층화를 시킴으로써, 계층화된 도메인에서 최상위의 도메인인 그룹 본사 도메인에서 생성한 일반적이고, 포괄적인 정책은 하위의 서브 도메인인 계열사, 지사 도메인으로 전달되면서 상세화 되고 정제된다. 다시 말해서 세분화된 도메인들 사이에서 정책을 생성해서 배포하는 본사의 도메인을 최상위 레벨에 배치하고, 정책을 상위 레벨에서 전달받는 도메인 중에서 정책을 하위 도메인에 전달하는 역할을 하는 지사 도메인들을 중위 레벨에 그리고 정책을 전달받아서 실제로 정책을 실행하는 계열사나 하청업체 도메인들을 최하위 레벨에 배치하여 계층적 구조를 형성한다. 각 레벨간 정책의 포함관계는 다음과 같이 최상위 레벨의 정책은 일반화(generalization)되어서 중위 레벨의 정책에 포함되고, 중위 레벨 또한 하위 레벨의 정책에 포함된다. 반대로, 상세화(specialization)된 하위 레벨은 일반화된 상위 두 레벨의 정책을 모두 포함하고, 중위 레벨 역시 가장 일반화된 최상위 레벨의 정책을 모두 포함한다. 이렇게 세분화된 각각의 도메인들을 구성하고 있는 요소들을 조직단위 기준으로 계층화시키면 아래 [그림 3]과 같은 구조가 생성된다. 이 논문에서 제시한 기준 이외에 여러 가지 다른 기준(IP주소, 사이트 등)으로 네트워크를 세분화하는 경우에도 계층적으로 구성한 최종 결과는 [그림3]과 같다. 세분화된 각 도메인 내부의 레벨들에서 수행되는 작업들을 기술하면 아래와 같다.

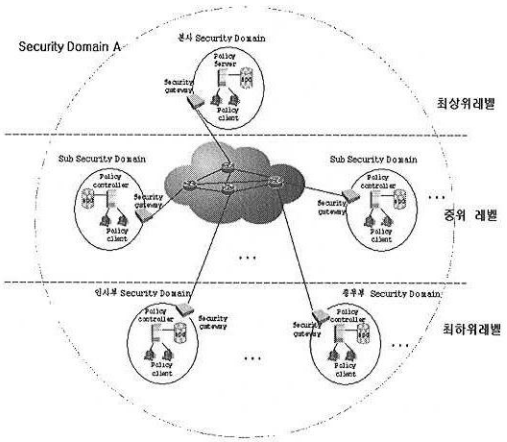

그림 3. 세분화된 한 도메인 내부의 계층 구조

- 최상위 레벨 : 조직의 목표를 정의하고 그것을 달성하기 위한 정책 설정, 정책을 입안하고 실행할 수 있는 정책들을 생성, 배포하고 최종적으로 생성된 정책을 저장, 정책에 적합한 정책규칙 생성
- 중위 레벨 : 최상위 레벨의 정책을 받아서 정책의 목표를 달성하기 위한 전략을 기술하고 자신의 레벨에서 발생되는 변동사항을 최상위 레벨에게 통보하는 역할을 하며 최상위 레벨의 정책을 최하위 레벨에게 전달.
- 최하위 레벨 : 최상위나 중위레벨의 정책을 받아서 정책을 상세화 시켜 실제적인 정책을 실행하며, 실행한 결과나 변동사항을 상위레벨에게 통보하는 역할. Domain내 계층화된 네트워크에서의 상속

[그림 3]의 구조를 살펴보면, 최상위 레벨에서만 정책을 관리하고 저장하기 위한 정책서버를 두고 그 하위 레벨에는 정책의 변동이나 제어를 하기 위해 정책제어기를 두어서 정책 규칙의 변경이나 적용을 담당하게 한다. 각 레벨에다 정책 서버를 두는 것은 자원의 낭비와 일관적인 정책을 적용하는데 있어 많은 오버헤드를 유발하기 때문에 최상위 레벨에게만 정책서버를 배치하고 있다.

Ⅲ. 계층적 구조의 정책 기반 네트워크 보안 관리 모델

보안 도메인이란 동일한 보안 정책을 공유하는 통신 개체나 자원, 즉 특정 security gateway에 의해 보호되어지는 네트워크 범위로서 특정 보안 도메인 내에 포함될 수 있다.[3][4][5] 이러한 보안 도메인들은 flat 구조로서 보안 정책 공간의 효율적인

사용이 가능하며 인터넷 환경에서 보안 정책의 복제로 능률을 유지할 수 있으나, 분산된 보안 정책의 변화에 따른 갱신의 어려움이 존재한다. 이러한 난점을 개선하기 위해 [그림 4]와 같은 계층적 모델을 제시한다. 제시한 계층적 모델은 도메인 내 정책 협상을 하지 않아도 되며 ,정책 정보 분배를 단순화하고, 갱신 및 수정의 관리가 용이하며 정책의 충돌 발생 문제를 해소해 준다는 장점을 가진다. 계층적 구조의 정책기반 네트워크 보안 관리 모델의 각 레벨에서 수행하는 일들을 기술하면 다음과 같다.[9]

- 최상위 도메인 레벨 : 논리적 혹은 물리적으로 분리된 영역 안에서 가장 최상의 도메인으로서 외부 영역으로 통하는 보안 게이트웨이와 인접해 있다. 최상위 도메인 레벨에도 하나의 보안 정책 서버를 두며, 중위 도메인 레벨을 관리하며 최상위 도메인 레벨이 관리하는 중위 도메인 레벨은 각각의 도메인 특성에 따라 다른 등급의 보안 정책을 적용할 수도 있고 보안 정책 적용시기도 각각 다르게 적용할 수 있다. 또한 최상위 도메인의 정책 서버는 자신의 정책을 상속한 중위 도메인 레벨의 상태를 KeepAlive message를 이용하여 주기적으로 점검한다. 또한 정책상의 수정이 필요한 경우 modification record를 전달하여 각각의 도메인 별로 modified date를 관리한다. 최상위 도메인 레벨에서의 정책 서버가 가져야 하는 데이터 구조에 대해서는 다음절에서 언급하겠다.
- 중위 도메인 레벨 : 최상위 레벨의 보안 정책을 상속한 중위레벨로서 바로 호스트를 관리하지 않고 하위 도메인으로 상속한다. 중위 도메인 또한 하나의 정책서버를 가지며, 중위 도메인이 상속해주는 하나 이상의 하위 도메인을 도메인 특성에 맞게 보안 정책을 적용하며 관리한다. 중위 도메인도 자신의 정책을 상속한 하위 도메인의 상태를 관리하며 방법은 최상위 도메인 레벨과 같다.
- 최하위 도메인 레벨 : 중위 도메인의 정책을 상속한 가장 하위 도메인으로서 하나이상의 호스트에 관한 정책을 관리하며 하나의 정책서버를 가지며, 자신의 도메인 안에 있는 호스트가 다른 영역 혹은 같은 도메인 내의 호스트와 보안 정책 협상을 하기를 원할 경우 보안 정책 서버의 역할을 한다.

또한, 각 레벨에 위치한 정책 서버들은 다음과 같은 기능을 제공하여야 한다.

1) 시행점에 위치한 종단 노드들이 자신의 영역에 적용된 정책을 알 수 있도록 해야 한다.
2) 클라이언트 노드가 응용에 관련 있는 정책을 질의하고 발견할 수 있는 프로토콜을 제공해야 한다.
3) 정책 교환과 질의 정보를 위한 메커니즘을 제공해야 한다.
4) 정책 협상을 제공해야 한다.
5) 정책 결정이 제공되어야 한다.
6) 정책 시행점에 대해 동적으로 정책 정보의 변경이 제공되어야 한다.
7) 실패한 정책에 대해 종단 노드에게 오류 정보를 제공해야 한다.
8) 각 도메인이 가지는 보안 레벨과 사용자인가 등급에 대한 정보를 제공해야 한다.

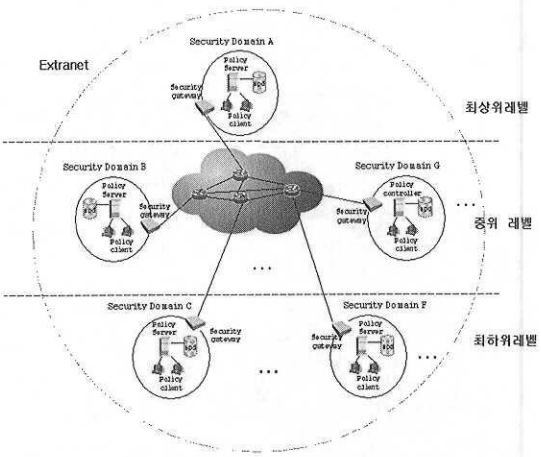

그림 4. 계층적 구조의 정책기반 네트워크 보안 관리 모델

이러한 계층적 구조의 정책 기반 네트워크 보안 관리는 이종 도메인이 아닌 동종 도메인간에 성립될 수 있으며, 초기 계층화 설계시 human 관리자가 각 master file에서 보유하고 있는 식별 ID에 의해 각 도메인을 최상위 레벨, 중위 레벨, 하위 레벨로 설정한다고 가정한다. 그러나 human 관리자가 업무 수준 정책과 보안, 혹은 도메인 명세 지식을 모두 깊이 이해하기에 어려움이 있으며, 또한 human operator에 의해 전송된 transformation의 일관성과 정확도를 체크하는 일도 쉽지 않다. 이런 제반적인 문제점들은 향후 지속적인 연구가 필요하다.

Ⅳ. 계층적 구조의 정책기반 네트워크 보안 관리 모델의 구성요소

일관적이고 체계적인 정책 관리를 하기 위해 제안한 계층적 구조의 네트워크 보안 관리 모델의 시스템 구성도를 살펴보면 [그림5]와 같다.[1][2]

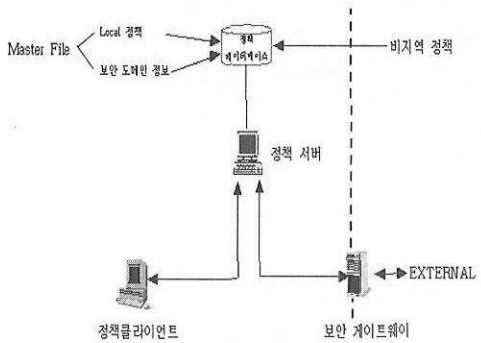

그림 5. 계층적 구조의 네트워크 보안 관리 모델의 시스템 구성도

가. 정책 서버

계층 구조를 이용하여 정책 클라이언트와 다른 정책 서버들로부터 Query 메시지를 수신하여 그것을 처리하고 적절한 정책 정보를 요청자에게 제공한다. 이때, 정책 서버는 요청자에 대한 접근 제한 규칙에 근거하여 정책 정보를 제공한다, 또한 정책 서버는 수신된 지역 및 비지역 정보를 가지고 정책 DB를 유지한다.

나. 정책 클라이언트

계층구조를 이용하여 정책 정보를 요청하는 메시지를 생성하고, 정책 서버로부터 Reply 메시지를 수신하며 응용에 의해 요구되는 적절한 포맷으로 reply 메시지를 응용에게 전달한다.

다. master file

특정 보안 영역의 지역 정책들과 그 보안 영역에 관한 특정 정보들을 포함한다. 지역 정책 정보는 정책 DB로부터의 비지역 정책들 (보안 영역의 경계 밖의 정책들)과 결합되며, 정보의 저장을 위한 특별한 포맷을 가지고있지 않다. 마스터 파일에 포함되는 특정 정보들은 다음과 같다.

- 인증서 (Certificate) : Maintainer 정보에 의해 참조되는 하나 이상의 인증서를 가리킴(이 인증서에서 발견되는 public key에 대응되는 private key는 마스터 파일에 포함된 정보에 서명하기 위해 사용되고, public key 정보의 무결성과 출처의 확실성(authenticity)를 증명하기 위해 사용된다.)
- 유지자(Maintainer): 특정 마스터 파일 내의 정책 정보를 생성, 삭제 및 수정하는 권한이 있는 엔티티를 정의
- 정책 서버 :특정 보안 영역에 대한 주와 부 정책 서버의 신원을 기술
- 노드 : 첨부된 정책들을 갖는 인터페이스 집합을 지정(보안 영역 내에는 최소한 하나의 노드가 있어야 한다.)
- 게이트웨이 : 특정 보안 영역의 정책을 실행하는 호스트와 연관된 인터페이스 집합을 지정
- 영역 : 영역에 속한 노드들, 보안 게이트웨어들 및 정책 서버들에 의해 보안 영역을 정의
- 정책 : 정책들의 순서화된 집합

마스터 파일은 보안 영역의 일부인 노드들의 리스트, 보안 영역을 보호하는 SG들의 리스트, SG에 의해 실행되는 정책 규칙들과 노드에서 실행되는 정책 규칙들의 리스트를 포함한다. 또한 누가 보안 영역을 책임지고 있는지를 가리키는 정보와 마스터 파일 내의 정보의 무결성과 인증을 검증하기 위해 사용될 수 있는 public key에 대한 포인터를 포함해야 한다.

라. 데이터베이스

계층적 구조 보안 관리 모델에서는 모든 보안 영역은 그 영역에 대한 정책 정보를 포함하는 DB를 유지해야 한다. 보안 영역들은 작게는 호스트이거나 크게는 여러 개의 망이 될 수 있다.[10] 정책 DB는 지역 정책 DB, 계층DB의 2가지 논리적인 DB로 구성된다. 이 2가지 DB들을 따로 구현할 필요가 없으나, 그들 각각에 포함된 정보는 존재해야 한다.

1) 지역 정책 DB. 어떤 보안 영역에 대한 모든 정책들을 포함, 보안 영역의 마스터 파 일로부터 오는 정보와 함께 놓이고, 캐쉬 DB를 포함한다.

   - 캐쉬 DB 다른 보안 영역들로부터 수신된 지역 및 비지역 외부 정책 들을 포함, 정책들은 정책 결정처리를 통해 병합된다.

2) 계층 DB: 계층화된 도메인의 상위와 하위의 리스트들을 가지고 있으며, 오직 최상위 root 서버만이 모든 도메인의 리스트를 가진다. 보안영역과 계층정보로 이루어진다.
   - 보안 영역 보안 영역의 일부인 모든 호스트, 보안 게이트웨이, 그리고 정책 서버들의 리스트를 포함한다.
   - 계층 정보 : 각 레벨별 계층정보 및 정책 제어기의 정보를 가지고 있다

이중 캐쉬 DB는 캐쉬 된 항목이 만기가 된 후에 지역 DB 정책 정보로 캐쉬 된 정책 정보를 복귀하는 것이 불가능하기 때문에, 지역 DB와 캐쉬 된 DB는 개별적인 정책들의 집합을 유지해야 한다.

V. 결 론

일관된 정책을 적용하는 정책 기반 네트워크 보안 관리 모델을 보다 더 체계적으로 관리 하고 확장성을 뛰어나게 하기 위해서 이 논문에서는 계층적 구조를 이용하여 표현하였다 계층적 구조를 이용한 정책 기반 네트워크 보안 관리 모델은 각 도메인간의 통신과 관련된 상호작용을 세분화하였기 때문에 이해하기 쉽고, 상하 계층간 표준 인터페이스를 정의하여 이 표준에 따른 경우 각 업체에서 만든 어떤 시스템과도 상호 호환이 가능하며, 각 계층의 성능 향상 및 개선이 쉽고, 이러한 이점들 때문에 기술혁신을 가속화 할 수 있다는 장점을 가지고 있다 그래서 이 논문에서는 계층적 구조의 정책 기반 네트워크 보안 관리 모델을 최상위, 중위, 최하위 레벨로 나누어 각각의 레벨에서 수행해야 될 일들을 기술하였고, 계층적 구조의 정책기반 네트워크 보안 관리 모델의 구성 요소들을 정책서버, 정책 클라이언트, Master File, 데이터베이스로 구성하여 각각의 기능과 구성요소들을 기술하였다. 이 모델에 대한 효율성 검증을 위해서 모델상에서 이루어지는 정책협상 메커니즘과 알고리즘들에 대한 연구와 구현이 필요하고, 실제로 이를 다양한 네트워크 환경 특히 모바일 환경에 적용하기 위한 연구가 필요하다.

참 고 문 헌

[1] Policy Framework, draft-ietf-policy-frame work 00 txt, Internet Draft, September 1999.

[2] Policy Framework Core Information Model, draft-ietf-policy-core-info-schema-02.txt, Internet Draft, February 1999

[3] Wang ChangKun, "Policy-based Network Management," Communication Techno logy Proceeding, 2000

[4] Dinech C Verma, "Policy-based NetworkI ng", New Riders, November, 2001

[5] Dave Kosiur, "Understanding Policy-based Net work", Wiley, 2001.

[6] 신영석, 정책기반의 보안 네트워크 구조, NET SEC -KR2001, April, 2001

[7] 니츠 편저, 인터넷 보안 기술. I, 도서출판 동서 2000.

[8] 조은경, 최은심, 권영희, 양태연, 인소란, IP 보안 정책 연구, 한국정보처리학회 추계학회발표논문집, 제6권 제2호, 1999

[9] 엄남경, 이상호, 김건우, 이종태, 손승원, 안전한 통신을 위한 계층적 구조의 보안정책 적용 방안, 한국통신정보보호학회 충청지부 학술대회 논문집, 2000

[10] 엄남경, 황윤철, 이상호, 이종태, 손승원, 계층적 보안 정책을 위한 데이터베이스 구조 설계, 한국정보과학회 충청지부 추계학술대회 논문집, 2000

황 윤 철(yoon-cheol hwang) 준회원

1994년: 한남대학교 전자계산공학과 졸업(공학사)

1996년: 한남대학교 대학원 전자계산공학과졸업(MS)

1999년~현재· 충북대학교 대학원 전자계산학과 박사 과정수료

<주관심 분야> 네트워크 보안, 정보보호, IDS, ITS 등

엄 남 경(Nang-kyeong Um) 준회원

1999년: 충북대학교 컴퓨터과학과 졸업(이학사)
2001년: 충북대학교 대학원 전자계산학과 졸업(MS)
2001년~현재: 충북대학교 대학원 전자계산학과 박사 과정

<주관심 분야> 통신 프로토콜, 개방형 네트워크, 네트워크 보안

이 상 호(sang-ho lee) 정회원

1976년: 숭실대학교 전자계산학과 졸업
1981년: 숭실대학교 대학원 전자계산학과 졸업(MS)
1989년: 숭실대학교 대학원 전자계산학과 졸업(PHD)

1976년 1월~1979년 5월: 한국전력 전자계산소
1981년 6월~현재: 충북대학교 전기전자 및 컴퓨터 공학부 교수

<주관심 분야> Protocol Engineering, Network Security, Network Management, Network Architecture