情報保護學會論文誌
第13券 第1號, 2003. 2

정책기반 보안관리 모델을 위한 프로토타입과 정책 협상 메커니즘

황 윤 철*, 현 정 식*, 이 상 호**

Prototype Design and Security Association Mechanism for Policy-based on Security Management Model

yoon-cheol hwang*, jeung-sik hyun*, sang-ho lee**

요 약

인터넷 서비스가 대중화되면서부터 네트워크상의 통신 및 시스템을 안전하게 보호하기 위한 네트워크 보안 관리가 시급한 문제로 부상되고 있다. 이에 따라 침입탐지 시스템, 침입차단 시스템, VPN과 같은 보안 장비들이 급속히 사용화 되고 있는 실정이다. 그러나 이들 보안 장비들은 단일환경, 단일 시스템에서 제각기 독립적으로 기능하기 때문에 보안 대상이 매우 제한적이며, 벤더별로 상이한 구조로 인해 상호 유기적인 통합기능을 제공하지 못하고 있는 실정이다. 따라서 이 논문에서는 일관성 있고 체계적인 보안정책을 네트워크를 대상으로 적절하게 적용할 수 있는 계층적 구조의 정책기반 보안관리 모델을 제시하고, 각기 다른 보안 영역에 따라 다르게 정의된 보안 정책들에 대한 관리와 협상을 용이하게 하는 정책 협상 메커니즘과 프로토타입을 제시한다. 이 연구 결과는 다양한 환경의 네트워크에서 보안정책 서버 및 보안 기술의 개발에 지침으로 활용이 가능하며, 또한 네트워크 전체의 보안성을 향상시킬 수 있으며, 각 호스트간의 보안 정책 협상을 효율적으로 지원할 수 있다.

ABSTRACT

With the Internet winning a huge popularity, there rise urgent problems which are related to Network Security Managements such as Protecting Network and Communication from un-authorized user. Accordingly, Using Security equipments have been common lately such as Intrusion Detection Systems, Firewalls, and VPNs. Those systems, however, operate in individual system which are independent to one another. Their usage are so limited according to their vendors that they can not provide a corporate Security Solution. In this paper, we present a Hierarchical Security Management Model which can be applicable to a Network Security Policies consistently. We also propose a Policy Negotiation Mechanism and a Prototype which help us to manage Security Policies and Negotiations easier. The results of this research also can be one of the useful guides to developing a Security Policy Server or Security Techniques which can be useful in different environments. This study also shows that it is also possible to improve a Security Characteristics as a whole network and also to support Policy Associations among hosts using our mechanisms.

Keyword : *Security Policy, Hierarchical Security Management Model, Security Association, Mechanism, Prototype*

* 충북대학교 컴퓨터과학과 네트워크 보안 연구실(dolpin98,jshyun@netsec.cbnu.ac.kr)
** 충북대학교 전기전자 및 컴퓨터공학부 및 컴퓨터 정보 통신 연구소(shlee@chungbuk.ac.kr)

Ⅰ. 서 론

인터넷은 전세계적으로 구축되어 있는 개방된 구조의 네트워크로서 프로토콜로 TCP/IP (Transm ission Control Protocol/Internet Protocol)를 주로 사용하기 때문에 정보 보안에 취약한 상태이고, 상용화 서비스의 확산으로 중요한 정보들이 인터넷을 통하여 상호 교환되는 특성을 가지고 있어, 악의적으로 검색, 수정 및 파괴될 가능성에 항상 노출되어 있다. 이러한 문제점을 해결하기 위하여 안전한 이용을 보장하는 인터넷 보안에 관련된 연구가 필수적이라 할 수 있다.

보안 정책(Security Policy)에 관련한 주요 연구 동향을 살펴보면, 최근 IPv6의 제정과 함께 IPsec(IP Security Protocol)에 대한 심도 있는 연구가 진행되고 있으며 주로 인터넷 기술을 담당하는 기관인 IETF(The Internet Engineering Task Force)의 IPSP(IP Security Policy) working group에서 연구하고 있다. 이 워킹 그룹은 보안 기술적인 측면의 개발뿐만 아니라 자신의 호스트 또는 게이트웨이(Gateway)를 포함한 도메인(Domain)을 보호하기 위한 보안 정책의 연구도 활발히 진행중이며 inter-draft에 대한 표준화가 진행 중이다. 또한, NIST에서는 1997년에 "Internet Security Policy : A Technical Guide"라는 초안 문서로 보안정책을 발표했다.[1,2]

보안 정책을 구현함에 있어서 유의할 점은 각 정보보호 시스템의 정보보호 서비스에 부합되는 정책 기술을 사용할 수 있게 하여야 하며, 시스템들의 상호호환성을 위해 보안 정책 시스템의 구현과 개체들 사이의 통신 프로토콜 등을 표준화하여야 한다는 것이다. 또한 전 세계적으로 분포되어 있는 네트워크를 어떠한 기준으로 그룹화하여 계층적으로 구성할 것인가도 고려해야 한다. IPsec기반 인터넷 정보보호를 설계하는 과정에서, 구조 설계의 대상인 네트워크의 규모가 확대됨에 따라 Security Association 설정이 복잡해지고 네트워크 구성요소와 환경이 다양해짐에 따라 각 시스템에 대한 보안정책 설정 및 제어가 어려워진다. 따라서 정책기반 보안관리 모델을 개발함에 앞서 대형화되어가는 네트워크 차원의 보안정책 모델에 대한 이론적인 분석과 각 모델의 장단점 분석, 범용성 및 확장성에 대한 구조적이며 체계적인 사전 연구와 각 정보보호 시스템의 정책 제어를 위한 데이터 구조의 정의 및 구현에 관한 연구가 필요하고 이를 실제로 구현하여 연동시키는 프로그램의 개발이 필요하다.

이러한 현실적 요구를 바탕으로 이 논문에서는 기존의 보안정책 설정 및 제어 기술을 분석하고, 보안 영역의 특성을 고려한 계층적 구조의 정책기반 보안관리 모델을 제안하고, 다양한 네트워크 환경에서 활용이 용이한 정책 상속 메커니즘과 프로토타입을 개발한다. 이 논문의 구성을 살펴보면 2장에서는 기존의 보안 정책 구조를 분석해 보고, 이를 바탕으로 3장에서는 계층적 구조의 정책기반 보안관리 모델을 제시한다. 4장과 5장에서는 3장에서 제시한 모델을 근간으로 프로토타입과 정책협상 메커니즘을 기술하고, 6장에서 결론을 맺는다.

Ⅱ. 보안 정책 프레임 워크

보안 정책 시스템의 목적은 전체적으로 네트워크를 관리하고 제어하는 것이며 이는 네트워크 운영이 네트워크를 운영하는 조직의 비즈니스 목표와 일치하기 때문이다. 보안 정책 프레임워크는 IP 네트워크의 운영적인 특성들을 제어하기 위한 대체 방안을 나타낸다. 전통적인 네트워크 관리 방법과 달리, 보안 정책 프레임워크 내에서 개발된 시스템들은 단일 소프트웨어 어플리케이션 내로 제어 기능들을 집중화함으로써 보안 정책을 구현하는 대신에 규정된 규칙들의 저장을 집중화함으로써 구현한다. 이 프레임워크 하에서 설계된 보안 정책 시스템은 개별적인 디바이스를 형성하는 것으로부터 전체적으로 네트워크에 대한 보안 정책을 설정하는 것으로 포커스를 이동시키고 네트워크 보안 정책을 통하여 디바이스 행위들을 제어한다.[3,4]

보안 정책 규칙은 보안 정책 시스템들의 핵심이다. 보안 정책 규칙들은 일반적/추상적이거나 명세적/구체적이다. 보안 정책 규칙들은 디바이스와 개발자에 독립적으로 의도되는 condition과 action의 쌍으로 표현하고, 네트워크 내에 개발된 어느 보안 정책 시스템에 참여하고 있는 엔티티들 사이에서 상호 운용점(The Point of Interoperability)으로 제공된다. 상호운용성의 주요 포인터로 보안 정책 규칙을 만들기 위해서 정보 모델은 보안 정책 규칙들의 병합, 보안 정책 규칙들에 의해 제어되고 있는 디바이스들의 특성, 관리되고 있는 객체들 사이의 상호관계와 상호작용 등을 기술한다. 보안 정책 규칙에 의해 제어되고 있는 디바이스들의 특성에 따라 보안 정책 규칙들의 병합은 'Policy Framework LDAP Core Schema'에서 기술된다.

이것은 보안 정책 규칙에 대한 저장 구조와 형식뿐만 아니라 보안 정책 규칙들에 의해 제어되고 있는 장치들을 특성화시키는 데이터들을 정의한다. 관리되고 있는 다른 객체들 사이에서 의미와 상호관계를 획득하는데 사용되는 디바이스들의 다른 특징들은 보안 정책 규칙에서 표현된 condition와 action들이 어떻게 해석되는지를 정의한다. 또한 디바이스 기능들에 대해 어떤 효과를 미치는지를 정의한다. 이러한 것들은 "Policy Framework Core Information Models"에 정의되어 있다. 이 문서는 스키마와 의미 정의에 대한 것들을 제공하며 완전한 보안 정책 시스템을 실현하기 위해 요구되는 기능적 요구 사항들을 열거한다. 규칙들의 표현을 구성하는 보안 정책 시스템은 적어도 사용자가 보안 정책 규칙을 정의하고 갱신할 수 있도록 하는 기능, 보안 정책 규칙을 저장하고 검색하는 기능, 보안 정책 규칙을 해석하고 구현하고 시행하는 능력을 증명해야 한다. 보안 정책 시스템의 기능적인 요소들을 리스트로서 정리하여 보면 아래와 같다.[5,8~10]

- 보안 정책 관리 도구

엔티티들(예, 사람, 어플리케이션)이 보안 정책 규칙을 정의하고 갱신하고 선택적으로 그들의 배치를 감시할 수 있도록 한다. 예를 들어 그래픽 또는 명령어 라인/스크립트 인터페이스이다.

- 보안 정책 저장소(repository)

보안 정책 규칙의 지속적인 저장과 검색을 위한 것이다. 저장소는 단순히 데이터를 저장하고 데이터에 대해 처리하거나 활동하지 않는다.

- 보안 정책 소비자(consumer)

보안 정책 대상에 의해 사용 가능한 형태로 보안 정책규칙을 얻고 보안 정책 규칙을 배치시키고 선택적으로 보안 정책 규칙을 해석하는 책임이 있다.

- 보안 정책 대상(target)

보안 정책 규칙에 의해 구술되는 행위의 기능적인 요소이다. 보안 정책 대상은 보안 정책 규칙에 의해 가리키는 action을 수행한다.

보안 정책 소비자 소프트웨어가 실행되는 목적은 보안 정책 규칙을 획득하고 선택적으로 번역하고 배치하는 것이다. 기능적으로, 규칙을 해석하는 것은 규칙의 구현과는 분리된다. 이것은 condition의 평가와 action의 실행이다. 단일 소프트웨어 또는 디바이스 엔티티가 보안 정책 규칙의 획득 및 배치에 책임이 있음에도 불구하고 보안 정책 소비자는 기능적으로 보안 정책 규칙의 대상들로부터 구별될 수 있다.

보안 정책 규칙은 condition들 내에 시간 참조를 포함한다. 어떤 보안 정책 대상은 시간을 포함하는 condition들을 평가할 수 없다. 그 경우에 보안 정책 소비자는 보안 정책 규칙을 분해하고 자신과 보안 정책 대상 사이의 결정 프로세스를 분배한다.[6]

물리적인 디바이스는 보안 정책 대상이 있지 않는 네트워크에서 보안 정책에 영향을 미친다. 그러한 상황에서, 보안 정책 소비자와 보안 정책 대상 기능들은 소프트웨어 어플리케이션에서 병합되고 실현된다면 물리적인 디바이스가 보안 정책 소비자와 보안 정책 대상이 실현되었을 때 소프트웨어에 의해 조작된다.

라우팅 기능은 수행하나 저장소에 저장된 표준화된 보안 정책 표현을 해석할 수 없는 능력을 가진 라우터는 다른 예다. 한 조직이 게임 서버를 가지고 있고 정상적인 작업 시간 외 주기에서 이러한 서버에 접근하는 것을 제한하기를 원한다고 가정한다. 서버로의 접근을 지배하는 보안 정책 규칙은 두 방법으로 쓰여질 수 있다.

- time condition을 명세하고 서버로의 접근을 가능하게 하거나 불가능하게 할 수 있는 Action을 명세할 수 있다.
- 동일한 time condition을 명세했으나 action은 보안 정책이 배치된 디바이스에서 특정 지시를 포함한다.

보안 정책 소비자와 보안 정책 대상사이에 차이를 인식하는 목적은 보안 정책 규칙 의미를 쉽게 이해하도록 하며 표준 보안 정책 표현에 대한 빌딩 블록을 쉽게 개발하려는 것이다. 보안 정책 규칙을 설계하려는 노력에서, 사람들은 동일한 규칙 내에 두 개의 독특한 주체들을 함축하는 규칙을 종종 표현하는데, 이런 규칙들은 이치에 맞지 않은 규칙이거나 디바이스 특정 규칙들의 개발을 유도하는 규칙 중에 하나이다.[3]

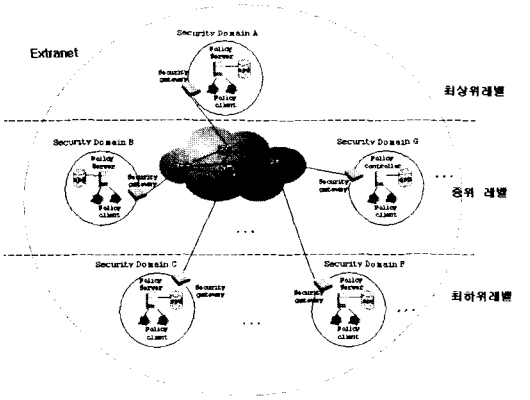
Ⅲ. 계층적 구조의 정책기반 보안 관리 모델

보안 도메인이란 동일한 보안 정책을 공유하는 통신 개체나 자원, 즉 특정 security gateway에 의해 보

호되어지는 네트워크 범위로서 특정 보안 도메인 내에 포함될 수 있다. 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.[11] 이러한 난점을 개선하기 위해 [그림 4]와 같은 계층적 모델을 제시한다. 제시한 계층적 모델은 기존의 네트워크들을 정책의 상호 연관성과 포함관계를 고려하여 세분화하고, 세분화된 영역을 조직단위로 계층화 시켰다. 이런 구조는 도메인 내 정책 협상을 하지 않아도 되며 ,정책 정보 분배를 단순화하고, 갱신 및 수정의 관리가 용이하며 정책의 충돌 발생 문제를 해소해 준다는 장점을 가진다.[12] 계층적 구조의 정책기반 네트워크 보안 관리 모델의 각 레벨에서 수행하는 일들을 기술하면 다음과 같다.

- 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 date*를 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.

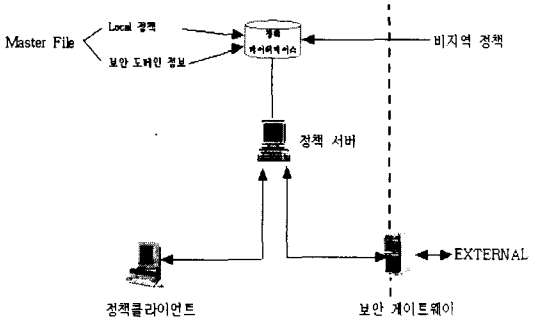


[그림 1] 계층적 구조의 정책기반 네트워크 보안 관리 모델

이러한 계층적 구조의 정책 기반 네트워크 보안관리 모델에서 계층 설정은 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.

3.1 계층적 구조의 정책기반 네트워크 보안 관리 모델의 구성요소

일관적이고 체계적인 정책 관리를 하기 위해 제안한 계층적 구조의 네트워크 보안 관리 모델의 시스템 구성도를 살펴보면 [그림 2]와 같다.[1,2,7]



〔그림 2〕 계층적 구조의 네트워크 보안 관리 모델의 시스템 구성도

3.1.1 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.

3.1.2 정책 클라이언트

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

3.1.3 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.

3.1.4 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.[4,5] 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 파일로부터 오는 정보와 함께 놓이고, 캐쉬 DB을 포함한다.
   - 캐쉬 DB : 다른 보안 영역들로부터 수신된 지역 및 비지역 외부 정책들을 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 계층

정보로 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.

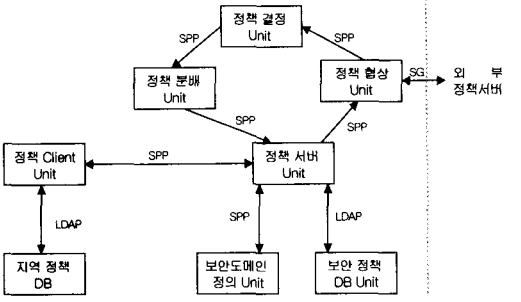
이중 캐쉬 DB는 캐쉬 된 항목이 만기가 된 후에 지역 DB 정책 정보로 캐쉬 된 정책 정보를 복귀하는 것이 불가능하기 때문에, 지역 DB와 캐쉬 된 DB는 개별적인 정책들의 집합을 유지해야 한다.

Ⅳ. 프로토타입

앞장에서 설계한 모델이 두 endpoint간 정책협상을 통해 안전한 통신을 하기 위한 프로토타입을 제시하면 아래 그림6과 같다. 이 프로토타입은 크게 정책 클라이언트 Unit과 정책 서버 Unit으로 나눌 수 있고, 정책 서버 Unit에서는 보안정책서버와 게이트웨이 기능을 담당하고 노드간의 연동을 위한 프로토콜을 제공한다. 정책 클라이언트 Unit에서는 정책서버에 정책을 요구하고, 전송 받은 정책을 집행하는 기능을 담당한다. [그림 3]에서 볼 수 있듯이 정책서버 Unit은 정책 분배 Unit, 정책결정 Unit, 정책협상 Unit, 보안 도메인 정의 Unit, 보안정책 Database Unit으로 구성되어 있다.

정책 클라이언트 Unit은 모든 정책 클라이언트에 탑재되며, 자체적인 지역정책을 저장할 수 있는 Database을 가지고 있다. 정책 분배 Unit, 정책결정 Unit, 정책협상 Unit, 보안 도메인 정의 Unit, 보안정책 Database Unit은 정책 서버에 탑재되어 각각의 기능을 담당하고, 보안 게이트웨이를 통해 모든 외부 네트워크 노드들간의 통신을 하게 된다.

정책 클라이언트 Unit과 정책 서버 Unit는 각 클라이언트와 서버에서 다른 Unit들간의 연동을 제어하며, 정책서버에 있는 정책 협상 Unit은 새로운 정책을 협상하기 위한 Unit으로 보안정책 프로토콜을 이용하여 다른 보안 도메인의 정책 서버와 로컬 정책에 따르는 정책 협상 기능을 제공하며, 정책 결정 Unit은 정책 협상을 통해 생성된 정책중 실제로 실행시킬 정책을 결정하는 기능을 제공하고, 정책 분배 Unit은 정책 클라이언트와 정책 서버에 존재하는 데이터베이스의 일관성을 유지하는 기능을 담당한다.



[그림 3] 계층적 구조의 네트워크 보안 관리 모델의 프로토타입

Ⅴ. 정책 협상 메커니즘

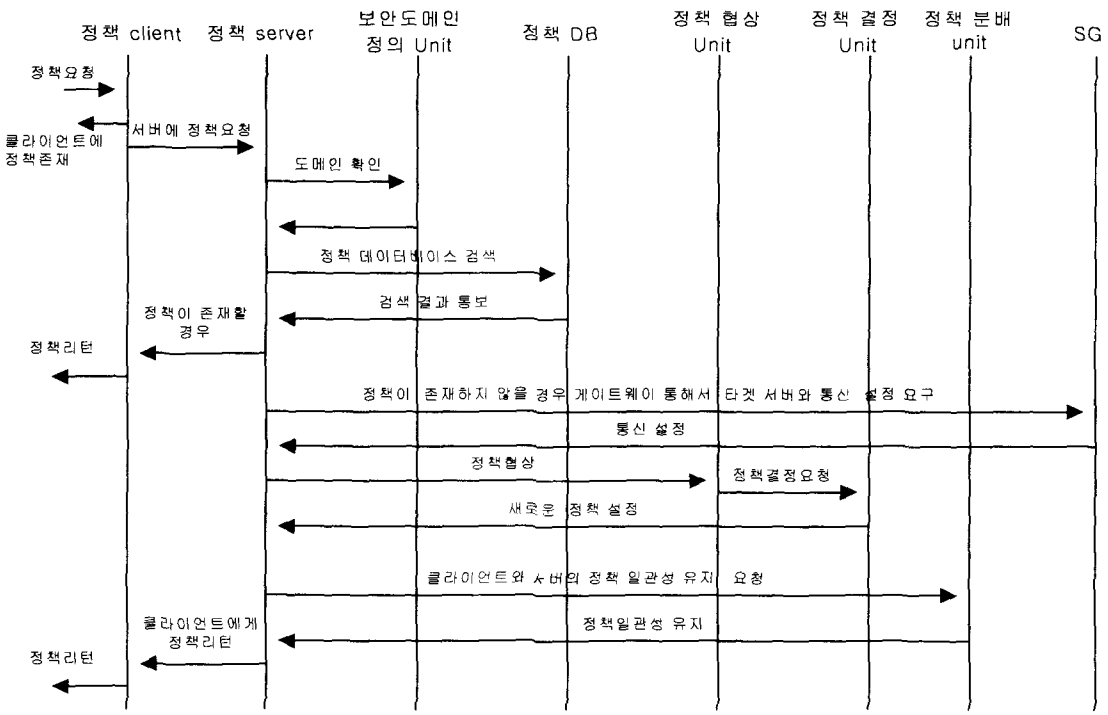
계층적 구조의 네트워크 보안 관리 모델의 프로토타입을 이용한 정책 협상 과정을 살펴보면, 두 endpoint 간의 안전한 통신 채널을 설정하고자 하는 경우, 먼저 정책 클라이언트에게 보안 정책을 요구한다. 정책 클라이언트는 자체 보안정책 데이터베이스를 검색하여 해당하는 보안 정책이 있을 경우 이를 리턴하고 만일 해당하는 정책이 없으면 보안정책 서버에게 정책 프로토콜을 이용하여 새로운 보안 정책을 요구한다. 보안정책 서버는 정책 클라이언트로부터 요구받은 보안정책을 자신의 정책 데이터베이스(캐시, 지역 데이터베이스)에서 검색하고 이에 대한 결과를 정책 클라이언트에게 리턴 한다. 만약 해당하는 보안정책이 존재하지 않으면, 통신하고자하는 endpoint의 정책 서버와 새로운 보안 정책 설정을 위해 보안정책 프로토콜을 이용해 목적지 정책 클라이언트의 정책 서버에게 새로운 정책 협상을 요구한다.

정책 협상을 요구받은 목적지 보안정책 서버는 통신하고자 하는 endpoint의 정책 클라이언트가 자신의 도메인 안에 있는지 확인한 후, 정책협상을 하게 된다. 정책 협상이 완료되면, 양 보안정책 서버에는 새로운 정책이 설정되고 이를 기반으로 정책 클라이언트 간에 안전한 통신을 하기 위한 통신 채널이 설정된다.

이런 일련의 과정을 시퀀스 다이어그램으로 표현하면 아래 [그림 4]와 같다.

Ⅵ. 결 론

기존의 보안 시스템은 각 보안 영역과 구현 제품에 따라 각각 다른 보안 정책을 내부적으로 정의하여 사용하였다. 따라서 각기 다른 보안 영역의 통신 상대와 통신하거나 다른 보안 영역을 거쳐 통신하는



〔그림 4〕 계층적 구조의 네트워크 보안 관리 모델 정책 협상 메커니즘

경우에 보안 영역간의 정책 요구사항이 다르고, 양방향의 통신이 같은 경로에서 같은 정책을 사용하는지를 보장할 수 없었다. 이를 해결하기 위해서는 보안정책에 따라 다르게 정의된 정책 정보들에 대한 중앙 집중적인 관리와 협상을 용이하게 하는 정책 기반의 보안 관리 모델이 정의되어야 한다. 이 논문에서는 계층적 구조의 정책 기반 보안관리 모델을 위한 구성요소로서 기존의 IETF에서 정의하고 있는 보안정책 시스템의 구성요소들을 이용하고, 추가적으로 우리 계층적 구조의 보안정책 모델에서 필요한 계층 DB를 추가하여 정의하였으며, 이 모델이 두 endpoint 간 정책협상을 통해 안전한 통신을 하기 위해 크게 정책 클라이언트 Unit과 정책 서버 Unit로 구성된 프로토타입을 설계하고, 계층화된 도메인간의 정책 협상 메커니즘을 제시했다.

계층적 구조의 정책기반 보안관리 모델에 관한 연구를 통하여 얻어진 메커니즘이나 모델들은 현재 완전히 구현되어 있지 않고 알고리즘의 수준까지 연구되었기 때문에 향후 이를 보완하여 완벽한 프로그램을 구현하는 연구가 필요하고, 실제로 이를 다양한 네트워크 환경 특히 모바일 환경에 적용하기 위한 연구가 필요하다.

참 고 문 헌

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

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

[3] 조은경, 최은심, 권영희, 양태연, 인소란, IP보안 정책 연구, 한국정보처리학회 추계학회발표논문집, 제6권, 제2호, 1999.

[4] 엄남경, 이상호, 김건우, 이종태, 손승원, "안전한 통신을 위한 계층적 구조의 보안정책 적용 방안", 한국통신정보보호학회 충청지부 학술대회 논문집, 2000.11

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

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

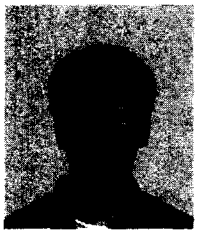
[7] 니츠 편저, 인터넷 보안 기술. I, 도서출판 동서 2000.

[8] 신영석, 정책기반의 보안 네트워크 구조, NETSECKR-

2001, April, 2001.
[9] Dinech C. Verma, "Policy-based Networking", New Riders, November, 2001.
[10] Dave Kosiur, "Understanding Policy-based Network", Wiley, 2001.
[11] 연현정, 이동석, 나재훈, 이상호, "정책상속을 이용한 계층화된 정책관리 모델의 설계",한국정보처리 학회추계학술발표논문집, 2001.10
[12] 김주옥, 배수정, 황윤철, 이상호, "계층적 구조의 정책기반 보안관리 모델을 위한 프로토타입의 설계", 한국통신학회추계학술발표대회논문집, 2001. 11

〈著者紹介〉

황 윤 철 (yoon-cheol hwang) 학생회원
1994년 : 한남대학교 전자계산공학과 졸업(공학사)
1996년 : 한남대학교 대학원 전자계산공학과 졸업(MS)
1999년~현재 : 충북대학교 대학원 전자계산학과 박사과정수료
<관심분야> 네트워크 보안, 정보보호, IDS, ITS등



현 정 식 (jeung-sik hyun) 학생회원
1999년 : 청주대학교 컴퓨터정보공학과 졸업
2001년 : 청주대학교 전자계산학과 졸업(MS)
2001년~현재 : 충북대학교 전자계산학과 박사과정
<관심분야> 네트워크 보안, P2P, 그리드 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 컴퓨터공학부 교수
<관심분야> Protocol Engineering, Network Security, Network Management, Network Architecture