계층적 구조 보안 정책 모델을 위한 데이터베이스 구조 설계

윤 여 웅[†]·황 윤 철[†]·엄 남 경[†]·김 건 우[††]·이 상 호[†††]

요 약

인터넷을 구성하는 논리적인 도메인들의 규모가 확대됨에 따라 개체들간 보안 정책 협상이 복잡해지고, 다양한 특성을 갖는 각 도메인들의 구성요소와 환경 등의 요인으로 각 시스템에 대한 보안정책 설정 및 제어가 어려운 문제로 등장하고 있다. 이 논문에서는 이러한 현실적인 문제점을 해결하기 위해 대상 네트워크를 계층적 구조로 구성한 후 그 결과를 바탕으로 안전한 통신을 위한 보안정책을 적용하기 위한 데이터베이스 스키마를 설계한다. 계층적 구조에서 서로 다른 도메인간에 보안정책은 보안정책 데이터 구조를 이용하여 효율적으로 데이터를 관리하고 보안정책 메커니즘을 이용하여 안전한 통신을 가능하게 한다.

Design of A Database Architecture for Hierarchical Security Policy Model

Yeo-wung Yun[†] · Yoon-Cheol Hwang[†] · Nam-Kyeong Um[†]
Kwun-Woo Kim[††] · Sang-Ho Lee[†††]

ABSTRACT

As enlarging a scale of logical domain organizing Internet, security policy association among entities become complicated. Establishment and control of security policies for each system is a hard problem to solve because of the environment and composite factors with variable properties. In this paper, to solve this actual problems, we organize a hierarchical structure of network and than we design the structure of database to apply security policies for secure communication. This enables efficient management of security data and association of security policy by using designed data structure between different domain in hierarchical structure which make secure communication possible.

키워드 : 보안 정책(Security Policy), 계층적 구조(Hierarchical Structure), 데이터베이스 구조(Database Structure)

1. 서 론

인터넷을 구성하는 논리적인 도메인들의 규모가 확대됨에 따라 개체들간 보안정책 설정이 복잡해지고, 다양한 특성을 갖는 각 도메인들의 구성요소와 환경 등의 요인으로 각 시스템에 대한 보안정책 설정 및 제어가 어려운 문제로 등장하고 있다. 본 논문에서는 이러한 현실적 문제들을 보완하기 위해 보안정책을 설정하고 제어하는 기술을 제안하고 기존의 보안정책이 가지는 서버 구조를 네트워크 차원에서 분석하고자 한다. 또한 보안 영역의 특성을 고려한 계층적 보안정책 모델의 개략적 구조와 보안정책 데이터베이스 구조를 제시하여, 인터넷상에서 활용이 용이한 계층적 보안 정책 및 프로토콜과 보안정책 데이터베이스 및 연동 메커니즘 개발을 지원하도록 한다.

기존의 보안관련 연구들은 인터넷상의 통신 및 시스템들을 안전하게 보호하기 위하여 보안위협 요인들을 분석하고 필요로 하는 보안 서비스들을 정의하여 이를 위한 메커니즘들을 개발하는 것이 대부분이었다. 이러한 연구는 단편적인 기술 측면의 연구에 불과하고 포괄적인 보호를 제공하지 못하기 때문에 인터넷의 전체적인 보호를 위한 주요 요소인 보안정책(Security Policy)에 관한 연구가 최근 들어 활발히 진행되고 있다.

국내의 현실은 보안정책에 대한 연구보다는 보안 기술 측면의 연구에 편중되어 있고 외국의 연구 결과에 의존하고 있다. 그러나 보안정책 관련 시스템을 외국으로부터 수입하여 사용하는데 한계가 있으며, 국내 실정에 맞고 국내의 보안 도메인 내에서 상호 호환이 가능하며 나아가 전 세계와의 호환도 가능한 기술 연구와 시스템 개발이 시급히 요구된다. 따라서, 본 논문에서는 기존의 관련 연구 동향과 보안정책 모델을 분석하여 보안정책 시스템을 계층적으로 구성 할 때, 시스템 효율성을 높이는데 필수적 역할을 수행하는 도메인간 호환성이 가능하도록 데이터베이스 스키마를 계층적 구조에 기반하여 설계하였다.

† 준 회 원 : 충북대학교 대학원 전자계산학과
†† 정 회 원 : 한국전자통신연구원
††† 종신회원 : 충북대학교 전기전자 및 컴퓨터공학부 교수
논문접수 : 2001년 2월 26일, 심사완료 : 2001년 9월 10일

2. 보안정책 연구 동향 및 분석

2.1 연구 동향

인터넷 보안 정책 기술은 인터넷상에서 정보보호 기능을 구현할 때 적용하는 정책들에 대한 검색, 접근제어, 분배 및 처리를 위한 기술이며 전세계적으로도 현재까지는 활발한 연구가 이루어지지 않고 있는 실정이다. 정보보호 정책 기술은 각 정보보호 시스템 단위로 필요한 정보보호 서비스에 부합되는 정책기술을 채택하여 사용할 수 있으나, 정보보호 정책기술을 운영하는 시스템들의 상호호환성을 위해 정보보호 정책 시스템의 구현과 객체들 사이의 통신 프로토콜 등이 표준화되어야 한다. 현재 IETF의 IPSec 워킹그룹(Working Group)과 ISPS 워킹그룹에서는 Internet-Draft 형태로 SPS(Security Policy System), SPP(Security Policy Protocol), SPSL(Security Policy Specification Language) 등의 세부 주제들을 중심으로 정보보호 정책기술에 관련된 프레임워크를 이론적으로 연구하고 있다.

보안정책에 관련한 주요연구 동향을 살펴보면 다음과 같다. 최근 IPv6의 제정과 함께 IPSec(IP Security Protocol)에 대한 연구가 진행되고 있으며 주로 인터넷 기술을 담당하는 기관인 IETF(The Internet Engineering Task Force)에서 IPSP(IP Security Policy)와 IPSec의 워킹그룹이 결성되었다. 이 워킹그룹들은 보안기술적인 측면의 개발뿐만 아니라 자신의 호스트 또는 게이트웨이를 포함한 도메인을 보호하기 위한 보안정책의 연구를 활발히 진행 중이며 Internet-Draft에 대한 표준화를 진행 중이다. NIST에서도 1997년 'Internet Security Policy : A Technical Guide'를 초안 문서로 발표한 상태이다[4].

IPSec은 인터넷 상에서 자원에 접근하고자 하는 요구에 대하여 어떤 것을 허가해주고 어떤 것을 거부할 것인지를 결정하는 정책으로 전자상거래 등과 같은 인터넷의 활용이 보편화될수록 선행되어야 할 핵심 과제이다. 그러나 현재 운영 중인 대부분의 보안정책은 방화벽(Firewall)과 같이 자신의 호스트 또는 도메인을 보호하기 위한 수준에 지나지 않는다. 따라서 각 기업체들은 국제표준에 입각해 자신들만의 VPN 장비, 방화벽, 라우터 등에서 적용될 수 있는 보안정책에 대하여 국부적으로 연구하고 있다.

현재 운영중인 대부분의 보안정책은 자신의 호스트 또는 도메인을 보호하기 위한 수준에 지나지 않으나, 다른 도메인간 또는 서브 도메인 내에서 안전한 정보통신을 위하여 상호 교환 및 공유를 수행하는 보안정책으로의 확장이 이루어짐으로써 체계적인 인터넷 정보보안이 가능해질 것이다. 국내의 현실은 보안정책에 대한 연구보다는 보안기술 측면의 연구에 편중되어 있고 외국의 연구 결과에 의존하고 있다. 보안정책 기술이 정보보호 서비스를 제공할 때 없어서는 안될 중요한 기술임에도 불구하고, 정책기술에 대한 명확한 정의조차 되지 않은 상태이다[6, 7]. 그러나 보안정책 관련 시스템을 외국으로부터 수입하여 사용하는데 한계가 있으며, 국내 실정에 맞고 국내의 보안도메인 내에서 상호 호환이 가능하며 나아가 전세계와의 호환도 가능한 기술 연구와 시스템 개발이 시급히 요구된다.

본 논문에서는 기존 보안정책 서버 구조를 Internet-Draft 문서를 통해 분석하고 그것을 바탕으로 계층적 보안정책 구조를 제시한 후 동일한정책 속성을 갖는 호스트들의 모임을 그룹으로 정의하고 이를 보안정책 데이터베이스 구조에 대한 설계에 이용한다.

2.2 기존의 보안정책 모델 분석

본 논문에서는 보안정책에 입각하여 계층적인 데이터베이스 설계 방법을 제시하기 위해 기존의 보안정책 모델을 라우터 기반 보안 정책 모델, Firewall 기반 보안정책 모델, VPN 기반 보안정책 모델로 나누어 분석하였다[2, 5].

- 라우터 기반 보안정책 모델

라우터 기반은 패킷 필터링 기능을 수행하며 오버헤드가 적어 수행 속도가 빠르다. 내용 체크가 불가능하며 저수준의 보안을 제공한다. 또한 검증이 어렵다. 그러나 확장성이 좋고 사용자에게 투명성을 제공한다.

- Firewall 기반 보안정책 모델

패킷 필터링 기능뿐만 아니라 Content Security 기능까지 지원한다. 어플리케이션 레벨에서의 보안 수준을 제공하기 때문에 처리 속도가 저하되는 단점이 있다. 확장성면에서는 각 도메인 내에서 정책 적용이 가능하며 자사 제품을 통한 도메인간 정책 협상이 가능하다. IBM Secureway Firewall의 경우, Security Policy Director를 통한 확장이 가능하고 디렉토리 내 사용자 정보유지에 LDAP V.3을 사용한다. 다양한 종점 시스템들을 지원하기 위해 TMA라는 관리 에이전트를 사용하고 자사 제품간 정책협상을 지원한다. CheckPoint Firewall-1은 정책명세시 INSPECT 언어를 사용한다. 또한 파이어월 기반 보안정책은 포괄적인 네트워크 환경에 적용 불가능하며 타사 제품간 정책협상을 고려하지 않는다. 현재는 OPSEC과 같은 Achitecture를 통한 통합관리 추세이다.

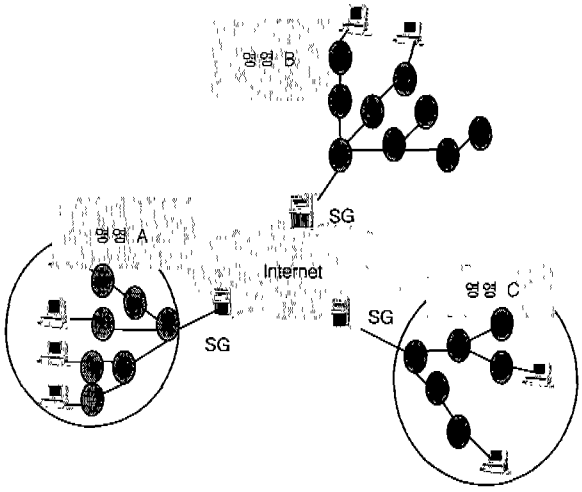
- VPN 기반 보안정책 모델

터널링을 통한 트래픽을 보호하기 위한 것으로 Firewall과 통합화되는 경향으로 상위 레벨의 보안기능을 지원한다. 인증과 기밀성을 제공하기 위해 다양한 보안파라미터들의 사이트간, 도메인간협상 일치가 요구된다. 상이한 VPN 프로토콜간 보안협상이 곤란한 점에서 확장성의 문제가 존재한다.

3. 계층적 보안 모델 구조

3.1 계층 구조의 개요

엔터프라이즈 환경에서의 보안정책은 도메인 내에서 또는 자사 제품들을 사용한 도메인간 보안정책 협상을 통하여 안전한 통신을 제공하고 있다. 이러한 국부적인 보안 정책에서 벗어나 전체 네트워크 환경에 적용될 수 있는 보안 정책 모델이 필요하다. 평평한 구조 접근 방법은 전체 보안 정책 공간의 효율적인 사용이 가능하고 인터넷 환경에서 보안정책 복제로 능률을 유지할 수는 있다. 그러나 분산된 보안정책 변화에 따른 갱신의 어려움이 존재한다. 계층적 구조는 중앙 집중 방식이 아닌 분산 방식으로 보안정책 변화에 따른 갱신이 쉽다. 또한 같은 도메인 내 정책협상을 하지 않아도 된다는 장점이 있다[10]. 이와 같은 장점을 수용하는 계층적 모델을 도입하기 위해 보안정책을 수행하는 하나의 큰 영역을 계층 구조로 구성하였을 때 가장 상위 도메인이 보안 게이트웨이와 인접해 있고 보안 게이트웨이는 인터넷 등과 같은 공중망과 접해있다고 보면, (그림 1)과 같다.



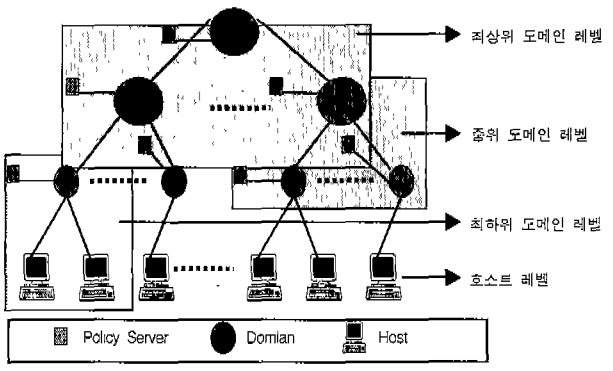
(그림 1) 계층적 모델의 전체 구조도

(그림 1)에서 보안정책 협상을 하기 위해 같은 영역안에서는 보안 게이트웨이를 거치지 않게 되고 다른 영역과는 보안 게이트웨이를 거쳐 보안정책 협상을 하게 된다. 전체 네트워크에 적용되는 계층 구조는 각각의 Global 영역에서 적용되는 방법과 세부적으로 나누어 보면 한 Local 영역안에서 적용되는 방법과 Global 영역에서 적용되는 방법은 같다. 따라서 한 영역의 계층화 모델을 세부적으로 나누어 체계화하고 그것을 확장하게 되면 Golbal Model이 됨을 알 수 있다. (그림 1)에서 Global 영역을 세부적으로 나눈 Local 영역중 영역 A를 대상으로 계층화 모델을 살펴보면 다음과 같다[5]. 각각의 도메인은 논리적으로 (그림 2)와 같이 세가지 레벨로 분류할 수 있다. 분류기준을 보면 다음과 같으며 중위 도메인 레벨은 하나 이상의 깊이를 가질 수 있다.

- **최상위 도메인 레벨** : 논리적 혹은 물리적으로 분리된 영역 안에서 가장 최상의 도메인으로서 외부 영역으로 통하는 보안 게이트웨이와 인접해 있다. 상위 도메인 레벨에도 하나 이상의 보안정책 서버가 존재하며 하나 이상의 SPS를 소유한다. 최상위 도메인 레벨은 중위 도메인 레벨을 관리하며 최상위 도메인 레벨이 관리하는 중위 도메인 레벨은 각각의 도메인 특성에 따라 다른 등급의 보안정책을 적용할 수도 있고 보안정책 적용시기도 각각 다르게 적용할 수 있다. 또한 최상위 도메인 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. 상위 도메인 레벨에서의 SPS가 가져야 하는 데이터 구조에 대해서는 참고문헌[8]에서 설계한 형태를 따르겠다.

- **중위 도메인 레벨** : 최상위 레벨의 보안정책을 상속한 중위레벨로서 바로 호스트를 관리하지 않고 최상위 도메인을 상속한다. 중위 도메인 또한 하나 이상의 정책서버를 가지며 이는 하나 이상의 SPS를 소유한다. 중위 도메인이 상속해준 하나 이상의 하위 도메인을 도메인 특성에 맞게 보안정책을 적용하며 관리한다. 중위 도메인도 자신의 정책을 상속한 하위 도메인의 상태를 관리하며 방법은 최상위 도메인 레벨과 같다.

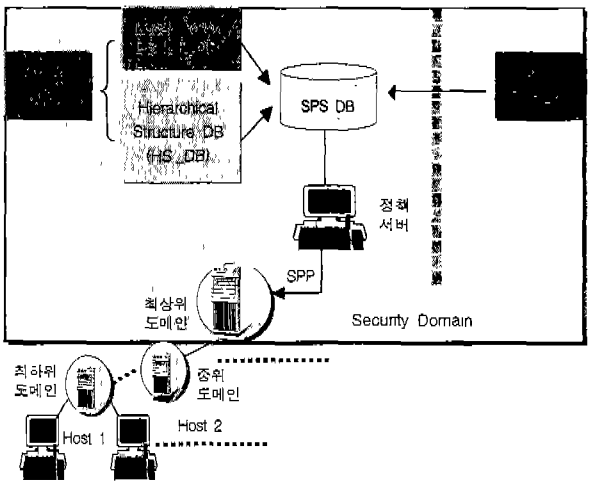
- **최하위 도메인 레벨** : 중위 도메인의 정책을 상속한 가장 하위 도메인으로서 하나 이상의 호스트에 관한 정책을 관리하며 하나 이상의 정책서버와 이에 해당하는 하나 이상의 SPS를 소유한다. 자신의 도메인 안에 있는 호스트가 다른 영역 혹은 같은 도메인 내의 호스트와 보안정책 협상을 원할 경우 보안정책 서버의 역할을 한다.



(그림 2) 논리적인 도메인 레벨의 분류

3.2 보안정책 시스템

계층 구조를 가지는 보안정책 모델에서 하나의 도메인이 소유하는 보안정책 서버는 하나 이상의 보안정책 시스템을 소유한다. 이러한 보안정책 시스템의 내부 구조를 살펴보기 위해 최상위, 중위, 최하위 도메인으로 나누도록 한다. 이 중 최상위 도메인을 예로 들어 하나의 도메인이 가지는 보안 영역을 알아보면 다음과 같이 나타난다.



(그림 3) 보안도메인 데이터베이스 정보 및 동작

각각의 요소들을 설명하면 다음과 같다.

- **정책 서버** : 도메인이나 호스트가 다른 정책 서버들로부터 정책정보 요청을 받아서 요청자의 접근 권한에 따라 정책정보를 제공한다.
- **도메인 및 호스트** : 정책 서버에게 정책정보를 요청하고 이를 수신하여 적절한 응용에 전달한다.
- **마스터 파일** : 특정 보안 영역의 지역 정책 정보와 그룹 정보 및 계층 영역, 보안 영역에 관한 정보가 저장된다. 여기서는 정책이 가지는 연관성을 제거하여 사용하므로 저장된 정보의 순서가 중요하다.
- **SPS DB** : 보안 정책 시스템이 정책정보를 유지하는 데이터베이스이며, 지역 정책 데이터베이스, 캐쉬 데이터베이스 계층적 구조의 데이터베이스로 구성된다. 캐쉬 데이터베이스는 보안정책 시스템을 통해 지역(local) 정책과 비지역(non-local) 정책들을 포함한다. HD_DB는 유지하는 계층의 정보 및 보안 영역의 부분들인 호스트, 보안 게이트웨이 등의 목록을 포함한다.

4. 보안 정책 데이터베이스 구조 설계

계층 구조를 가지는 보안정책 모델에 맞게 보안정책 서버를 확장할 경우, 가장 중요한 것은 최상위 도메인의 정보로부터 하위 단계로 관리 정보를 상속하여 최하위 도메인에서 관리하는 정보의 양이 단계적으로 축소되어야 한다는 점이다. 앞서 설계한 계층구조를 갖는 보안정책 모델에 맞추어 최상위, 중위, 최하위 도메인으로 분류하여 각 계층의 데이터베이스와 그들의 필드를 설계했다[5].

4.1 보안 정책 서버

보안 정책을 계층적으로 유지하기 위한 정책서버가 가져야 할 요구사항은 다음과 같다[2].

1) 각각의 도메인 영역에서 갖는 마스터 파일은 서명, 권한자, 영역 정보 외에 계층 관리 정보 및 그룹화 정보를 가져야 한다.
2) SPS 데이터베이스에서 지역 정책 데이터베이스, 계층 구조 데이터베이스 스키마는 계층적으로 관리되도록 구성되어야 한다.
3) 효과적인 제어를 위해서는 최상위 도메인의 정보를 하위 도메인으로 상속받도록 하여 상위 도메인과 하위 도메인간 체계적인 관리가 가능하도록 해야 한다.
4) 계층적 구조 데이터베이스의 경우, 계층 관리 테이블과 보안 영역 테이블을 따로 두어 관리해야 한다.

보안정책 서버가 관리해야 하는 관련 데이터 정보로는 크게 마스터 파일과 SPS 데이터베이스로 나뉜다. SPS 데이터베이스는 앞에서 설명한 바와 같이 지역정책 데이터베이스, 캐쉬 데이터베이스, 계층적 구조 데이터베이스로 구성된다. 또한 보안정책 서버에서 서버 자체를 관리하기 위한 정보는 계층별로 다르게 구분하여 구성할 필요가 없다. 다만 정책 서버를 식별할 수 있는 정보 및 날짜 등의 정보는 공통적으로 계층에 관계없이 가지고 있어야 한다. 서버 자체 관리를 위해 가지고 있어야 하는 데이터베이스 내의 정보는 정책 서버 정보, Signature(Digital Signature)이다. 각각에 대해 세부적으로 정의하면 다음과 같다.

- **마스터파일**

특정한 데이터 포맷을 규정하고 있지는 않지만, 정책정보를 정의할 수 있는 벤더에 독립적인 언어인 Security Policy System Language(SPSL)를 정의하고 있다. 마스터파일이 기본적으로 저장하고 있어야 하는 데이터 정보로는 사용자 서명시에 필요한 인증부분, 정책을 관리할 수 있는 권한자, 서버를 식별할 수 있는 ID, 영역 및 요소들의 정보 등을 가지고 있어야 한다.

- **지역정책 데이터베이스**

마스터 파일에서 도메인을 위한 모든 정책을 포함하고 있다. 모든 정책 서버와 정책 클라이언트는 자신의 지역 정책을 포함하는 데이터베이스를 유지해야 한다. 정책 서버의 정책은 보안 도메인 내의 모든 멤버에게 적용되므로, 서버 자

체의 SPD와 지역 정책 데이터베이스를 분리하여 운영하여야 한다. 정책 클라이언트는 SPD와 같으며, 미리 설정된 형태로 정책이 유지된다. 지역 정책 데이터베이스는 마스터파일 내에 있는 정책 정보를 이용하여 설정된 것으로, clause section과 action section으로 구성된다. clause section에서는 특정 통신에 대해 규정하고 있고, action section에서는 그 통신에서 행하여지는 처리에 대해 설명하고 있다. 각 엔트리들은 고유 식별자, 소멸시간, 단일 정책 절로 구성된다. SPP에서는 clause부와 action부로 나누어지는데, clause부는 통신 보안 레코드에서 인코딩 되고, action부는 SA 레코드에서 인코딩 된다. 지역 정책 데이터베이스내의 정책들은 연관성을 없애야 한다. 비연관 정책들은 실행 처리에 영향을 주지 않고, 정책의 효과적인 레코딩과 조직화가 가능하며, 외부 정책의 캐쉬기능 또한 용이하게 한다.

- **캐쉬 데이터베이스**

모든 정책 서버와 클라이언트는 병합된 지역 또는 외부 정책 데이터의 캐쉬를 유지하여야 한다. 외부 정책은 정책 서버나 클라이언트에 미리 설정되어 있지 않는 정책으로 이는 SPS 교환에 의해서만 획득될 수 있다. 외부 정책과 지역 정책 데이터베이스는 정책 결과 처리에 의해 병합된다. 이렇게 병합된 정책은 지역 정책과 논리적으로 분리되어 유지되어야 하며, 다음부터는 동일한 정책 정보에 대한 질의/응답으로 이용될 수 있다. 각 entry들은 고유 식별자, 소멸시간, 단일 정책절로 구성된다. SPP에서는 정책 서버 Assertion과 인증부로 나누어지는데, 정책서버 Assertion은 정책서버 내에서 인코딩 되고, 인증은 인증 레코드에서 인코딩 된다. 정책 서버와 클라이언트는 정책을 무한적으로 캐쉬 할 수 없다. 캐쉬 된 정책은 경고 없이 변경되는 외부 정책 때문에 캐쉬 될 수 있는 최대 시간을 소멸 시간으로 설정하고, 이를 포함하여야 한다. 물론, 캐쉬 데이터베이스 내의 정책도 비연관성이 없어야 한다.

- **계층 구조 데이터베이스**

각 보안도메인의 계층을 표시해주는 정보와 도메인간의 신용 정도를 증명하는 정보를 포함하고 있다. 또한 각 보안도메인에 대해서 보호되는 노드들의 정보를 리스트로 가지고 있다. 보안도메인의 경계에서 정책을 실행하는 각 SG의 식별자 리스트와 보안도메인의 멤버가 되는 노드들의 식별자를 가지고 있는 엔트리 등이 정책도메인이 인증된 것임을 증명하는 정보이다. 정책 서버는 정책 정보를 제공하는 호스트들이 인증 되었는지 판단할 때 이 정보를 이용한다. 또한, 정책정보의 수신처가 신뢰된 체인에 위배되지 않으며 SPP 교환에 참여하는지 확인할 때에도 이용한다.

- **정책 서버 정보**

보안정책들을 관리할 수 있는 정책 서버가 가지는 애트리뷰트를 정의한다. Pol_Serv_Name은 애트리뷰트의 주요키이며 이것은 정책 서버 객체들을 유일하게 식별한다. Name은 정책 서버가 위치했을 때 네트워크 엔티티를 식별하는 유효 고정 DNS 이름이다. 각 Alias 애트리뷰트는 정책 서버의 DNS 이름을 선택적으로 명세한다.

〈표 1〉 정책 서버의 DB 구조

Attribute	Value	Type
Pol_Serv_Name	<Policy_Server_Name>	필수
Char_Set	<Char_Set>	선택
Free_Form	<Free_Form>	선택
Name	<Dns_Name>	필수
Alias	<Dns_Name>	선택
IP_Addr	<IP_Address>	필수
Mnt_By	<Mntner_Name>리스트	필수
Changed	<Mnt_Name><Date>	필수
Signature	Signature 참조	필수

- **Signature**

객체가 수정되었을 때 모든 서명 애트리뷰트는 모든 서명이 유효하기 위해서 재계산되거나 객체로부터 제거되어야 한다. 애트리뷰트는 다음의 구문을 갖는다.

```
signature :
< mntner-name >< cert-name >< signature-alg >< signature-data >
```

<mntner-name>과 <cert-name>은 이 mntner가 객체를 서명하고 인증서가 사용되었다는 것을 식별한다. mntner이란 정책을 수행하기 위해 객체를 생성하고, 삭제하고, 다른 객체로 대치시키기 위해 명세하는 것으로, 정책을 표시하기 전에 mntner 객체를 생성하는 것이 필요하다. <signature-alg>은 서명을 생성하는데 사용된 알고리즘이다. 현재 다음의 서명 알고리즘이 정의되었는데 "rsa-pkcs1", "dsa-sha1"이다[5].

<signature-data>는 특정 알고리즘을 사용하여 생성된 서명의 16진수 스트링이다.

예) signature :
XYZ-IR-MNT XYZ-X509-CERT rsa-pkcs1 \f2
8889abce34daaaaebc2347. \f2

4.2 최상위 도메인의 데이터베이스

(그림 2)와 같은 계층구조를 갖는 보안정책 모델에서 최상위 계층의 도메인의 정책 서버가 유지하는 데이터베이스와 각 요소별 필드들은 다음과 같다.

- **마스터 파일**

[기본적인 요소]

- Certificate : 서명을 위한 인증서
- Maintainer : 정책정보 생성/삭제/수정할 수 있는 권한

을 가진 엔티티.

- Policy-Server : 서버의 ID.
- Elements : 정책을 가질 수 있는 인터페이스의 집합.
- Domain : Node(Security Gateway, 정책 서버 등을 모두 포함하는 관리 영역의 개념.
- Group_Domain : 같은 정책으로 구성된 단위별 그룹화 영역정보
- Level_Mnt : 계층에 대한 관리 정보.
- Policy

[세부적인 요소]

기본적인 요소의 필드 중 Group_Domain은 같은 정책을 사용하는 영역별로 그룹화시키는 정보를 저장하는 필드이다. 최상위 도메인이 가지는 그룹정보는 다음과 같이 구성한다.

- group_Name : 그룹명
- group_src : 소스 그룹 주소
- group_des : 목적지 그룹 주소
- direction : 방향
- trust_level : 신뢰도의 정도를 나타냄.
- policy_Name : 그룹간에 적용되는 정책
- action : 취해지는 행동
- mnt_Name : 그룹 관리자명
- group_Date : 그룹 지정일자
- address_Group : 해당 정책을 사용하는 호스트.

기본적인 요소의 필드 중 Level_Mnt는 계층에 대한 관리 정보를 나타내는 필드이다. 최상위 도메인이 가지는 계층 정보는 다음과 같다.

- level_ID : 보안영역을 위한 계층 식별자
- IP_Addr : 해당 계층 해당 도메인의 IP 주소
- down_Domain : 현재 도메인의 자식 도메인 열거

● 지역정책 데이터베이스

다음의 사항들은 최상위 도메인의 지역정책 데이터베이스가 가지는 필드이다. 하위 도메인 레벨에서는 이 필드들을 기본으로, 필요한 요소들을 상속받아 정책에 적용한다.

- Policy_Name : 정책 이름을 부여
- Group_Name : 그룹화된 영역정보
- sys_Name : DNS 이름
- Action : 해당정책의 행위여부(Permit/Deny)
- Cache_Expire : 캐쉬되는 최대 시간 표기
- Valid_Period : 시간 주기(time period)
- Dst_Addr : 정책이 적용되거나 적용되지 않는 IP_Address 또는 Address 범위들의 리스트를 명세
- Dst_Port : 목적지 주소의 포트
- Src_Addr : 정책을 요구하는 출발지 주소 명세
- Src_Port : 출발지 주소의 포트
- Xport_Proto : 특정 포트에 대해 서비스되는 트랜스포트 프로토콜 타입 명세
- Direction : 패킷이 정책과 관련된 도메인으로 들어가고 있거나(inbound) 도메인을 빠져 나가고 있는가를 (outbind) 명세화하는데 사용
- Ipv4/Ipv6 : Ipv4/Ipv6 구분 또는 변환 정보
- Changed : 정책이 변경된 일자를 기술한다.
- Exc_Proto : 인증 프로토콜 명세
- Set_Proto : 키설정 프로토콜 명세
- Mnt_Proto : 키관리 프로토콜 명세
- Cryp_Proto : 암호 프로토콜 명세
- Enc_Proto : 키교환 프로토콜 명세
- Mnt-by : 관리자 정보
- Signature : 관리자 서명

● 캐쉬 데이터베이스

지역 정책과 외부 정책의 병합된 부분이 그대로 저장된다.

● 계층 구조 데이터베이스

계층 구조를 관리하기 위한 데이터베이스이며, 자신이 관리할 수 있는 도메인에 속한 호스트들에 대한 정보가 들어있는 정보 테이블로서, 각 인덱스는 호스트에 대한 식별자가 된다. 각각의 중위 도메인에 관한 정보를 담고 있는 보안 영역 테이블과 상위 도메인 자체의 관리를 위한 관리 테이블 그리고 그룹 호스트 관리 테이블 등의 세개의 테이블을 가지고 있으며 내용은 다음과 같다.

[보안 영역 테이블]

보안 영역 테이블의 구조는 다음과 같다.

Ch_do_id	ch_do_addr	la_mod_dat	Nc	Pep	Pd	sta_do

- ch_do_id(child domain identifier) : 정보테이블의 인덱스
- ch_do_addr(child domain address) : 최상위 도메인으로부터 정책을 상속한 인덱스에 해당하는 중위 도메인의 주소 필드
- la_mod_dat(last modified date) : 해당 중위 도메인이 수정 혹은 갱신이 가장 최근에 이루어진 날짜를 기록하는 필드
- ne(never to be expired) : 해당 도메인의 정책이 만료하지 않는다는 기능 설정
- pep(Policy execution period) : 새로운 정책이 효력을 발생하여야 하는 기간을 나타내는 필드
- pd(policy degree(H, M, L)) : 해당 도메인이 정책상 어느 정도의 등급을 가져야 하는 중요도 정도를 나타내는 필드
- state of child domain : 자식 도메인의 상태를 나타내는 필드

[계층 관리 테이블]

계층 관리 테이블의 구조는 다음과 같다.

Num_do	adm_log _infor	la_mod _dat	num_do nor	sg_addr

- num_do(the number of domain to be managed) : 현재의 상위 도메인에서 정책을 상속한 중위 도메인의 수를 나타내는 필드
- adm_log_infor(administrator login information) : 관리자의 정보를 나타내는 필드
- la_mod_dat(last modified date) : 최상위 도메인 주체로 정책의 수정 혹은 갱신을 시행한 가장 최근 날짜를 기록하는 필드
- num_do_nor(the number of domain with normal state) : 현재의 상위 도메인에서 정책을 상속한 중위 도메인의 수중 정상 상태를 나타내는 도메인의 수를 나타내는 필드로서 이는 KeepAlive 메시지를 이용하여 중위 도메인의 상태를 체크 할 수 있다.
- sg_addr(security Gateway Address) : 최상위 도메인이 인접해 있는 보안 게이트웨이의 주소에 관한 필드

[그룹 내 호스트 관리 테이블]

그룹 내 호스트 관리 테이블의 구조는 다음과 같다.

gro_id	gro_man_ addr	lev_ gro	list_host	par_ addr	host_ addr	Last_mod_ date

- gro_id(Group Identifier) : 테이블의 인덱스로서 하나의 서브 네트워크인 그룹의 이름을 정의하는 필드
- gro_man_addr(address of group managed) : 그룹 이름에 해당하는 도메인의 주소를 나타내는 필드
- lev_gro(level of group) : 그룹 식별자(ID)에 속하는 도메인의 레벨을 나타내는 필드
- par_addr(address of group's parent) : 최하위 도메인인 경우 도메인을 상속한 중위 도메인의 주소를 정의하는 필드
- list_host(list of host) : 도메인내 속한 호스트의 리스트를 정의하는 필드
- host_addr(address of host) : 호스트들의 리스트에 해당하는 주소를 나타내는 필드
- last_mod_date(last modified date) : 수정이 발생한 가장 최근 날짜를 기록

이상은 최상위 도메인으로부터 정책을 상속받은 중위 도메인을 관리하기 위한 일반적인 테이블이다.

4.3 중위 도메인의 데이터베이스

(그림 2)와 같은 계층구조를 갖는 보안정책 모델에서 중위 계층의 도메인의 정책 서버가 유지하는 데이터베이스와 각 요소별 필드들은 다음과 같다.

- **마스터 파일**

[기본적인 요소]

중위 도메인이 가져야할 마스터 파일의 필드는 최상위 도메인이 가지는 필드와 같다. 하지만 도메인 영역의 레벨 정보를 가리키는 Level_Maintain과 Group_Domain 정보의 세부사항에는 변화가 있어야 한다.

[세부적인 요소]

기본적인 요소의 필드중 Group_Domain의 세부적인 요소는 최상위 도메인 영역과 같다. 또한 Level_Mnt는 계층에 대한 관리 정보를 나타내는 필드이다. 중위 도메인이 가지는 계층정보는 다음과 같다.

- level_ID : 보안 영역을 위한 계층 식별자
- IP_Addr : 해당 계층 도메인의 IP 주소
- up_Domain : 계층구조에서 현재 도메인의 부모 도메인 기술
- down_Dom_Hos : 계층구조에서 현재 도메인의 자식 도메인 열거지역정책 데이터베이스

- **지역 정책 데이터베이스**

중위 도메인의 지역 정책 데이터베이스가 가지는 필드이다. 이 정보는 자신의 상위 도메인으로부터 필요한 필드들을 상속받아 적용한다. 키 교환, 키 관리 등의 프로토콜과 관리자 서명 정보는 최상위 도메인에서 처리하므로 중위 도메인 레벨에서는 간주하지 않으며, 최하위 도메인 레벨에서는 중위 도메인 레벨의 정보를 상속받아 정책에 적용한다.

- **캐쉬 데이터베이스**

지역 정책과 외부 정책의 병합된 부분이 그대로 저장된다.

- **계층적 구조 데이터베이스**

계층 구조를 관리하기 위한 데이터베이스로서 자신에게 상속한 도메인을 관리하기 위한 정보가 들어있는 정보 테이블로서 인덱스는 각 도메인의 식별자가 된다. 관리를 위한 테이블을 다음과 같이 두개 가지고 있다.

[보안 영역 테이블]

보안 영역 테이블의 구조는 다음과 같다.

Ch_do_id	Ch_do_ addr	la_mod_ dat	ne	pep	pd	sta_do

각 요소의 세부적인 내용은 최상위 도메인의 보안영역 테이블의 기능과 동일하다.

[계층 관리 테이블]

계층 관리 테이블의 구조는 다음과 같다.

Num_do	adm_log_ infor	la_mod_ dat	num_do_ nor	pa_do_addr

요소중 num_do, adm_log_dat, la_mod_dat, num_do_ nor은 최상위 도메인의 보안영역 테이블의 기능과 동일하며, 추가적인 요소는 pa_do_addr이다.

- pa_do_addr(parent domain address) : 중위 도메인이 정책을 상속한 상위 도메인의 주소를 나타내는 필드

이상은 중위 도메인으로부터 정책을 상속받은 하위 도메인을 관리하기 위한 관리 테이블이다.

4.4 최하위 도메인의 데이터베이스

최하위 도메인은 하나 이상의 호스트를 관리하는 도메인으로서 하나 이상의 보안정책 서버와 보안정책 시스템, 이와 관련한 데이터베이스 등을 유지한다. 하나의 호스트가 다른 호스트와 정책을 협상하기 위해서는 최하위 도메인의 보안정책 시스템에게 보안정책 협상을 요청하여야 하며 최하위 도메인에서는 계층적 구조관리의 장점을 이용하여 그룹 정보를 검색한다. 그룹 정보는 신뢰된 그룹인지 접근을 금지하는 그룹인지 등의 정보를 유지하여 신뢰된 그룹이거나 보안정책이 필요하지 않는 그룹간에는 최소한의 정책 협상을 통한 정보의 전달이 이루어질 것이고 접근이 금지된 그룹간에는 정책협상을 하지 않고도 이에 대한 접근이 금지됨을 알 수 있다. 이와 같은 그룹간의 신뢰도 정보를 포함하고 있다.

계층구조를 갖는 보안정책 모델에서 최하위 계층 도메인의 정책 서버가 유지하는 데이터베이스와 각 요소별 필드들은 다음과 같다.

- **마스터 파일**

[기본적인 요소]

최하위 도메인이 가져야할 마스터 파일의 필드는 최상위 도메인이 가지는 필드와 같다. 하지만 도메인 영역의 레벨 정보를 가리키는 Level_Maintain과 Group_Domain 정보의 세부사항에는 변화가 있어야 한다.

[세부적인 요소]

기본적인 요소 중 최하위 도메인 레벨에서 Group_Domain이 가지는 세부요소는 group_Name, group_src, group_des, direction, trust_level, policy_Name, action, mnt_Name, mnt_Host, group_Date이며, 기본적인 요소 중 Level_Mnt은 계층에 대한 관리 정보를 나타내는 필드이다. 중위 도메인이 가지는 계층 정보는 level_ID, IP_Addr, up_Domain, down_Host이다.

- **지역 정책 데이터베이스**

최하위 도메인의 지역 정책 데이터베이스가 가지는 필드이다. 자신의 상위 도메인으로부터 보안정책 정보를 상속받아 영역내의 호스트에 적용하는데 사용한다.

- **캐쉬 데이터베이스**

지역 정책과 외부 정책의 병합된 부분이 그대로 저장된다.

- **계층 구조 데이터베이스**

계층 구조를 관리하기 위한 데이터베이스이며, 자신이 관리할 수 있는 도메인에 속한 호스트들에 대한 정보가 들어있는 정보 테이블로서, 각 인덱스는 호스트에 대한 식별자가 된다. 관리를 위한 두개의 테이블을 가지고 있다. 내용은 다음과 같다.

[보안 영역 테이블]

보안 영역 테이블의 구조는 다음과 같다.

Host_id	host_addr	la_mod_dat	Ne	pep	Pd	sta_host

각 요소중 상위 도메인에 추가된 요소들은 다음과 같다.

- host_id (host identifier) : 하위 도메인으로부터 정책을 상속한 호스트의 identifier로서 이 테이블의 인덱스가 된다.
- host_addr (host address) : 하위 도메인으로부터 정책을 상속한 id에 해당하는 호스트의 주소를 나타내는 필드
- sta_host(state of host) : 해당 호스트의 상태를 나타내는 필드로서 관리영역 안에 있는 호스트가 장애 등으로 통신이 불가능할 경우인 abnormal 상태와 정상인 normal 상태등을 나타낸다.

[계층 관리 테이블]

계층 관리 테이블의 구조는 다음과 같다.

num_host	adm_log_ infor	la_mod_ dat	num_host_ nor	pa_do_ addr

각 요소중 상위 도메인에 추가된 요소들은 다음과 같다.

- num_host(the number of host to be managed) : 현재의 하위 도메인이 관리하는 호스트의 수를 나타내는 필드
- num_host_nor(the number of domain with norma-l state) : 현재 이 도메인에서 정책을 상속한 하위 호스트 중 정상 상태를 나타내는 호스트의 수를 나타내는 필드로서 이는 KeepAlive 메시지를 이용하여 호스트의 상태를 체크 할 수 있다.
- pa_do_addr(address of parent domain) : 현제의 하위 도메인을 상속한 중위 도메인의 주소를 보관하는 필드

4.5 기존 데이터베이스와의 비교

기존의 IP 보안시스템에서 보안정책은 평평한 구조로 이루어지므로, 엔터프라이즈 환경에서의 중앙 집중적인 관리

로 인해 규모가 커질수록 효율성이 떨어지며, 정책협상에 대하여 일률적인 협상 메커니즘을 사용함으로서 다양한 보안 서비스를 바랄수 없었다[8, 9]. 따라서 분산된 관리로 그룹별 관리가 용이하고 보안 등급을 세분화시켜 다양화된 서비스 기능을 제공하기 위해서는 계층적 구조로 보안정책을 세우는 것이 바람직하다.

이를 위해 평평한 구조에서의 데이터베이스 스키마에 계층 개념을 추가하여 그룹화 기능과 상속기능이 가능하도록 하였고, 이를 저장할 수 있는 계층 구조 데이터베이스를 첨가하여 계층적 구조에 효율적으로 적용할 수 있는 스키마를 설계하였다. 그 비교 결과는 <표 2>와 같다.

5. 결 론

이 논문에서는 정책협상 시스템을 이용하여, 인터넷상에서 서로 다른 보안정책을 사용하면서 발생하는 문제점을 해결하고자 계층적 구조의 보안정책을 제안하고 이에 맞는 데이터베이스 구조를 제시한다. 즉, 기존의 평평한 구조에서는 분산 보안정책의 갱신이 어려웠으나, 확장된 통신망에서는 계층적 구조의 보안정책을 이용해 체계적인 보안정책의 관리가 용이하도록 한다. 여기서 제시하는 계층적 구조의 보안정책은 기존의 SPS와 SPP를 기반으로 주로 IP 보안정책을 지원하는 시스템 구조 및 서버 모델, 데이터베이스 스키마를 설계하였다. 또한 그룹 개념을 사용함으로서 호스트간의 보안정책협상이 효과적으로 수행 가능하여 분류된 각 그룹이 인트라넷으로 해석되고 처리될 수 있도록 제안하였다.

〈표 2〉 평평한 구조와 계층적 구조의 데이터베이스 스키마 비교

비 교 항 목		평평한 구조의 DB	계층적 구조의 DB
기능	상속기능 유무	×	○
	보안서명 유무	○	○
	보안영역설정 유무	○	○
DB 구성	마스터파일	○	○
	지역정책 DB	○	○
	캐쉬 DB	○	○
	보안영역 DB	○	○
	계층 구조 DB	×	○
관리의 용이성		규모가 커질수록 비효율	그룹별 관리 용이
보안서비스 다양화		중앙 집중적인 서비스제공으로 불가능	보안 등급별 다양화된 서비스제공 가능
엔터프라이즈환경에서의 효율성		비효율적	적당, 효율적

취약점으로는 다음과 같은 두 가지를 들 수 있다. 첫째, 많은 보안정책 서버들을 관리해야 하는 대규모 분산 환경에서 계층적인 구조는 중간 노드에서 발생하는 문제는 서브 도메인과의 안전한 통신을 저해할 수 있다. 이에 대하여 중간 노드의 문제 발생을 복구 또는 해결할 수 있는 대책이 요구된다. 둘째, 보안정책 시스템이 붕괴된다면 네트워크 전체가 안전한 통신 상태로부터 벗어날 수 있다. 그것은 보안 정책 시스템도 계층적 구조에 있는 하나의 시스템에 불과하므로 취약할 경우, 전체 네트워크에 문제가 발생한다는 것이다.

본 논문은 개념적 단계에서 기존의 방식과 계층적 구조 방식을 비교하였기 때문에 그 효율성을 비교하는데 있어 타당성이 부족하여 향후 연구 과제로 계층적 구조의 보안정책 모델에 대한 효율성을 검증하는 연구와 타당성을 분석하는 연구, 분산 구조에서의 효율적인 객체 상속방안에 대한 연구, 모바일 환경으로의 적용 방안에 관한 연구가 필요하다.

참 고 문 헌

[1] Fred Halsall, Data Communications, Computer Networks And Open Systems Fourth Edition, Addison Wesley, 1999.

[2] 엄남경, 이상호, 김건우, 이종태, 손승원, 안전한 통신을 위한 계층적 구조의 보안정책 적용방안, 한국통신정보보호학회 충청지부 학술대회논문집, 2000.

[3] 엄남경, 황윤철, 이상호, 이종태, 손승원, 계층적 보안정책을 위한 데이터베이스 구조 설계, 한국정보과학회 충청지부 추계학술대회논문집, pp.41-46, 2000.

[4] 이용주, 엄남경, 이지인, 이상호, 김건우, 보안 정책에서의 계층적 연동 방식 설계, 한국정보과학회 충청지부 추계학술대회논문집, pp.36-40, 2000.

[5] 이상호, 계층적 구조의 보안정책 모델에 관 한 연구, ETRI연구과제 최종보고서, 2000.

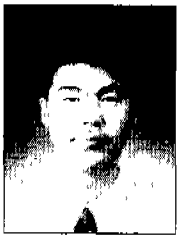
[6] R. Yavatkar, D. Pendarakis, R. Guerin, A Framework for Policy-based Admission Control, RFC2753, Jan. 2000.

[7] Hugh Mahon, Yoram Bernet, Shai Herzog, Requirement for a Policy Management System, Internet Draft, Oct. 22 1999.

[8] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC2401, Nov. 1998.

[9] L. A. Sanchez and M. N. Condell, Security Policy Protocol, Internet Draft, draft-ietf-ipsec-spp-00.txt, 1999.

[10] L. A. Sanchez and M. N. Condell, Security Policy System, Internet Draft, draft-ietf-ipsec-sps-00.txt, 1998.



윤 여 웅

e-mail : ywyun@center.kisa.or.kr

1996년 한남대학교 전자계산공학과 졸업 (공학사)

1998년 한남대학교 대학원 전자계산공학과 졸업(공학석사)

2000년~현재 충북대학교 대학원 전자계산학과 박사과정

관심분야 : 정보보호, 네트워크 보안, 인터넷

황 윤 철

e-mail : ychwang@cnlab.chungbuk.ac.kr

1994년 한남대학교 전자계산공학과 졸업 (공학사)

1996년 한남대학교 대학원 전자계산공학과 졸업(공학석사)

1999년~현재 충북대학교 대학원 전자계산학과 박사과정 수료

관심분야 : 네트워크 보안, 정보보호, 보안정책

엄 남 경

e-mail : family8@cnlab.chungbuk.ac.kr

1999년 충북대학교 컴퓨터과학과 졸업 (이학사)

1999년~현재 충북대학교 대학원 전자계산학과 석사과정중

관심분야 : 통신 프로토콜, 개방형 네트워크, 네트워크 보안

김 건 우

e-mail : kimgw@etri.re.kr

1998년 경북대학교 전자계산학과 졸업 (이학사)

2000년 경북대학교 컴퓨터과학과 졸업 (이학석사)

2000년~현재 한국전자통신연구원

관심분야 : 통신정보보호, 침입탐지 및 분석, 인터넷보안, HCI

이 상 호

e-mail : shlee@chungbuk.ac.kr

1976년 숭실대학교 전자계산학과 졸업 (공학사)

1981년 숭실대학교 대학원 전자계산학과 졸업(공학석사)

1989년 숭실대학교 대학원 전자계산학과 졸업(공학박사)

1976년~1979년 한국전력 전자계산소

1981년~현재 충북대학교 전기전자 및 컴퓨터공학부 교수

관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture