계층적 구조의 보안 정책 모델과 연동 방식 설계

준회원 황 윤 철*, 정회원 이 용 주**, 이 종 태**, 이 상 호*

Design of Hierarchical Security Policy Model and its Working Mechanism

Yoon-Cheol Hwang* *Associate Member*

Yong-Ju Lee**, Jong-Tae Lee**, Sang-Ho Lee* *Regular Members*

요 약

인터넷 서비스의 다양화와 네트워크의 대형화로 인하여 서브 도메인(Subdomain) 및 도메인을 포함한 인터넷 전체에 걸쳐 적용할 수 있는 계층적 구조의 보안 정책 모델의 정의와 이 모델을 기반으로 하는 보안 정책 프로토콜의 표준화가 요구되고 있다. 이 논문에서는 기존 보안 정책 서버 구조를 기존의 Internet-Draft 문서를 통해 분석하고 그것을 바탕으로 계층적 보안 정책 구조를 제시한 후 보안 정책 연동 프로토콜을 설계한다. 이를 위해 보안정책 프로토콜을 확장하여 그룹개념을 위한 질의와 레코드를 확장 설계하고 계층적 보안 모델에서 효과적인 보안정책 상속 및 수정을 위한 갱신 레코드를 정의한다. 또한 동일한 정책 속성을 갖는 호스트들의 모임을 그룹으로 정의하고, 이 개념을 기반으로 효율적인 연동 메커니즘을 설계한다.

ABSTRACT

Definition of hierarchical security policy model applicable to Internet including domain and subdomain and standardization of security policy protocol based on this model are strongly needed, by reason of diversity of Internet services and largeness of network. In this paper, we analysis existing security server through draft documents, propose hierarchical security policy based on this existing structure and design a working mechanism for security policy. To do it, we design expanded security policy protocol including group query and group record and define modification record for efficient security policy inheritance and renewal. We define hosts with the same properties as group and design a working mechanism based on this concept.

Ⅰ. 서 론

인터넷은 전세계를 대상으로 구축된 네트워크로서 네트워크에 연결된 대부분의 호스트 컴퓨터 시스템들은 운영체제는 Unix,통신 프로토콜로는 개방형 구조인 TCP/ IP(Transmission Control Protocol /Internet Protocol)를 주로 사용하기 때문에 정보 보안에 취약한 상태이다.

또한, 상용화 서비스의 확산으로 중요한 정보들이 인터넷상에서 상호 교환되는 특성이 있어, 악의적인 검색, 수정 및 파괴의 가능성에 항상 노출되어 있다. 이러한 문제점을 해결하여 안전한 이용을 보장하기 위해서는 인터넷 보안에 대한 관련 연구가 필수적이라 할 수 있다[1]. 기존의 보안 관련 연구의 주요 분야는 인터넷상의 통신 및 시스템들을 안전하게 보호하기 위하여 보안 위협 요인들을 분석하고 제공되어야 하는 보안 서비스들을 정의하여 이를 위한 메커니즘들을 개발하는 것이 대부분이었다. 이러한 연구는 단편적인 기술적 측면의 연구에 불과하고 포괄적인 보호를 제공하지 못하기 때문에

* 충북대학교 컴퓨터과학과 ** 한국 전자 통신 연구원
논문번호: K01087-0228, 접수일자: 2001년 2월 28일

인터넷의 전체적인 보호를 위한 주요 요소인 보안 정책(Security Policy)에 관한 연구가 최근 들어 진행되고 있다.

보안 정책을 구현함에 있어서의 특징 중의 하나는 보호 대상인 각 정보보호 시스템에 필요한 정보보호 서비스에 부합되는 정책 기술을 사용할 수 있으나, 시스템들의 상호호환성을 위해 보안 정책 시스템의 구현과 개체들 사이의 통신 프로토콜 등을 표준화하여야 한다는 점이다. 전 세계를 하나의 도메인으로 본다면 이 하나의 보안 도메인에서 구현된 정보보호 정책 기술은 서로 호환이 가능해야 하는 것은 당연하다. 실제 정보보호 시스템에 적용되는 보안 정책은 하위 보안 도메인인 정부나 업체 단위로 구성될 수 있지만 이들의 검색, 교환, 접근을 위한 프로토콜은 표준화되어야 한다.

IPSec(Internet Protocol Security)기반으로 인터넷 정보보호 방식을 설계하는 과정에서, 대상 네트워크의 규모가 확대됨에 따라 보안 정책 설정이 복잡해지고 네트워크 구성요소와 환경이 다양해짐으로써 각 시스템에 대한 보안 정책 설정 및 제어가 어려워진다. 따라서 보안 정책 모델을 개발함에 앞서 대형화 되어가는 네트워크의 추세를 고려한 보안 정책 모델에 대한 이론적인 분석과 각 모델의 장단점 분석, 범용성 및 확장성에 대한 구조적이며 체계적인 사전 연구가 필요하다. 이 논문에서는 보안 정책에 대한 이론적 분석을 바탕으로 세계적인 관련 연구 동향을 분석하며 향후 발전 방향을 예측하여 서브 도메인(Subdomain) 및 도메인을 포함한 인터넷 전체에 걸쳐 적용할 수 있는 계층적 구조의 보안 정책 모델을 설계하고 이 모델을 기반으로 하는 보안 정책 메커니즘을 제안한다.

Ⅱ. 관련 연구

2.1 연구 동향

인터넷 보안 정책 기술은 인터넷상에서 정보보호 기능을 구현할 때 적용하는 정책들에 대한 검색, 접근제어, 분배, 처리하는 기술이며, 전세계적으로도 현재까지는 활발한 연구가 이루어지지 않고 있는 실정이다. 정보보호 정책 기술은 각 정보보호 시스템 단위로 필요한 정보보호 서비스에 부합되는 정책 기술을 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 형태로SPS(Security Policy System) ,SPP(Security Policy Protocol), SPSL (Security Policy Specification Language) 등의 세부 주제들을 중심으로 정보보호 정책 기술에 관련된 프레임워크를 이론적으로 연구하고 있다[2][3].

보안 정책(Security Policy)에 관련한 주요 연구 동향을 살펴보면 다음과 같다. 최근 IPv6의 제정과 함께 IPSec에 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 보안 기술적인 측면의 개발뿐만 아니라 자신의 호스트 또는 게이트웨이를 포함한 도메인을 보호하기 위한 보안 정책의 연구를 활발히 진행 중이며 Internet -Draft에 대한 표준화를 진행 중이다. NIST에서도 1997년 'Internet Secur- ity Policy : A Technical Guide' 를 초안 문서로 발표한 상태이다[4].

IPSec은 인터넷상에서 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 보안 정책은 방화벽(Firewall)과 같이 자신의 호스트 또는 도메인을 보호하기 위한 수준에 지나지 않는다. 인터넷 정보보호 정책 기술은 인터넷상에서 정보보호 기능을 구현할 때 적용하는 정책들에 대한 검색, 접근제어, 분배, 처리하는 기술이며, 전세계적으로도 현재까지는 구체적인 연구가 이루어지고 있지 않다. 정보보호 정책 기술은 각 정보보호 시스템 단위로 필요한 정보보호 서비스에 부합되는 정책 기술을 채택하여 사용할 수 있으나, 정보보호 정책 기술을 운영하는 시스템들의 상호호환성을 위해 정보보호 정책 시스템의 구현과 객체들 사이의 통신 프로토콜 등이 표준화되어야 한다. 각 기업체들은 표준을 따르는 자신들만의 VPN장비, 방화벽, 라우터 등에서 적용될 수 있는 보안 정책에 대하여 국부적으로 연구하고 있다.

현재 운영중인 대부분의 보안 정책은 자신의 호스트 또는 도메인을 보호하기 위한 목적으로 한 수준에 지나지 않으나, 다른 도메인간 또는 서브 도메인 내에서 안전한 정보 통신을 위하여 상호 교환 및 공유를 수행하는 보안 정책으로의 확장이 이루어짐으로써 체계적인 인터넷 정보 보안이 가능해질

것이다. 국내의 현실은 보안 정책에 대한 연구보다는 보안 기술 측면의 연구에 편중되어 있고 외국의 연구 결과에 의존하고 있다. 보안 정책 기술이 정보 보호 서비스를 제공할 때 없어서는 안 될 중요한 기술임에도 불구하고, 정책 기술에 대한 명확한 정의조차 되지 않은 상태이다[5][6]. 그러나 보안 정책 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.

이 논문에서는 기존 보안 정책 서버 구조를 Internet-Draft 문서를 통해 분석하고 그것을 바탕으로 계층적 보안 정책 구조를 제시한 후 보안 정책 연동 프로토콜과 보안 정책 데이터베이스 구조를 설계를 이용하여[7] 동일한 정책 속성을 갖는 호스트들의 모임을 그룹으로 정의하고, 이 개념을 기반으로 효율적인 연동 메커니즘을 설계한다. 특히, 계층적 구조를 이용하여 보안 정책 구조를 설계할 때 각 계층의 상속은 분산 환경에서 상속이 이루어진다는 가정 하에 보안 정책 프로토콜을 설계한다.

2.2 관련 연구

보안 정책 모델에 접근하는 방법으로는 평평한 구조 방법과 계층적 구조 방법이 있다. 기존에 발표된 보안정책 메커니즘은 평평한 구조에서 제안된 것이다. 이와 같은 구조에서 설계된 보안정책 메커니즘은 단순한 하나의 보안정책 시스템과 다른 보안정책 시스템의 보안정책 협상을 의미한다. 다음은 이와 같은 환경에서 안전한 통신을 위해 보안서비스를 제공하는 과정에서 SPS의 동작 과정이다. 그림 1에서 SG_A와 SG_B는 모두 ESP를 이용하여 수신 패킷을 인증 해야 하는 정책을 가지고 있다. 즉, PC_A와 PC_B는 SA협상을 시작하려 PC_A가 패킷을 송신하면 SG_B는 모든 수신 패킷에 대해 ESP인증을 요구하고 PC_A는 PC_B에 대한 SA를 아직 가지고 있지 않으므로, 협상 자체가 불가능하다.

SPS는 이러한 문제를 해결할 수 있는 메커니즘을 제공한다. 보안 도메인 Foo와 Foo'의 네트워크 관리자는 각각의 도메인 정책을 유지하는 master file을 가지고 있다. 보안 도메인은 하나의 호스트만을 포함할 수도 있고, 여러 개의 PS와 SG로 구성되는 네트워크가 될 수 도 있다.

1) master file은 syntax error을 없애기 위해 먼저 parse하고 검증한다.

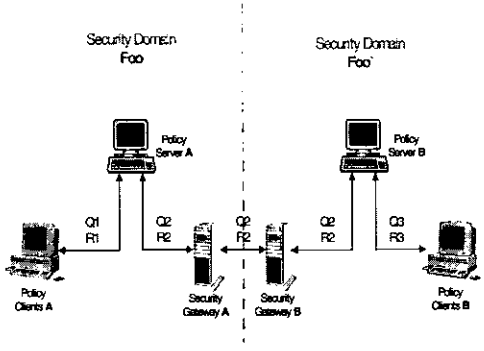


그림 1. 보안정책 시스템 동작과정

2) master file내의 정책들은 decorrelation process를 사용하여 decorrlated된다.
3) PS_A와 PS_B는 각각의 보안 도메인 내의 SPS 데이터베이스로부터 정책을 로딩하고, policy request를 기다린다. 커널에서 키 관리 프로토콜로 보내진 메시지는 policy request 메시지를 시작하도록 해준다.
4) PC_A는 PS_A에게 Q1을 보내다. PS_A는 query와 매치 되는 cache내의 policy record를 검색한다. 만약 필요한 정책이 없으며, PS_A는 PC_B로 Q2를 보낸다.
5) SG_A와 SG_B는 중간에서 Q2를 가로챈다. PS_B는 Q2를 검증해 보고, 적당한 정책 정보가 있는지 데이터베이스를 검색한다.
6) PS_B는 먼저 Q2내에 있는 정책 정보와 local policy를 merge한다. 그리고, 원래의 query 정보와 PC_B와 PC_A가 안전하게 통신을 하기 위해 필요한 정보를 이용하여 R2를 생성하여 PS_A에게 보낸다.
7) PS_B는 Q3을 생성하여 PC_B에게 보내고, PC_B는 R3를 생성하여 PS_B에게 보낸다. R3는 PS_B에서 merge되고 PS_B는 PC_B가 자신에 의해 인증 되었다는 정보를 추가하여 R2를 생성하여 이를 PS_A에게 보낸다.
8) R2내에서 merge된 정책은PS_A로 리턴되고, PS_A는 R2에서 받은 외부 정책을 local policy에 merge시키고, 이를 cache 한다.

Ⅲ. 계층적 보안 모델 설계

3.1 계층 구조의 개요

엔터프라이즈 환경에서의 보안 정책은 도메인 내에서 또는 자사 제품들을 사용한 도메인간 보안 정

책 협상을 통하여 안전한 통신을 제공하고 있다. 이러한 국부적인 보안 정책에서 벗어나 전체 네트워크 환경을 제공할 수 있는 보안 정책 모델이 필요하다[8]. 평평한 구조 접근 방법은 전체 보안 정책 공간의 효율적인 사용이 가능하고 인터넷 환경에서 보안 정책 복제로 능률을 유지할 수는 있다. 그러나 분산된 보안 정책 변화에 따른 갱신의 어려움이 존재한다. 계층적 구조는 중앙 집중 방식이 아닌 분산 방식으로 보안 정책 변화에 따른 갱신이 쉽다. 또한 같은 도메인 내 정책 협상을 하지 않아도 된다는 장점이 있다. 따라서, 엔터프라이즈 네트워크, 더 나아가 글로벌 네트워크 환경에서 적합한 보안 정책 모델의 접근 방법은 계층적 구조의 보안 정책 모델이 적합할 것이다. 이와 같은 장점을 수용하는 계층적 모델을 도입하기 위해 보안 정책을 수행하는 하나의 큰 영역을 계층구조로 나누었을 때 가장 상위 도메인이 보안 게이트웨이와 인접해 있고 보안 게이트웨이는 인터넷 등과 같은 공중망과 접해있다고 보았을 때 [그림 2]와 같다.

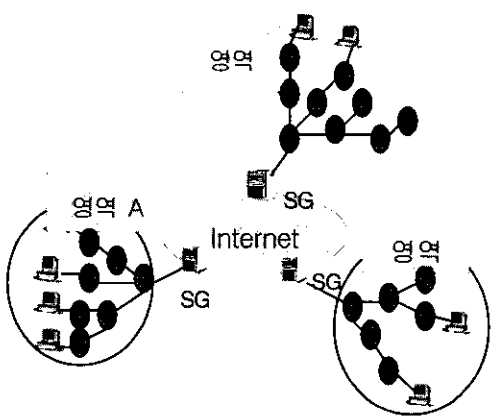


그림 2. 계층적 모델의 전체 구조도

영역 A를 대상으로 분리하여 계층화 모델을 살펴보면 다음과 같다. 각각의 도메인은 논리적으로 [그림 3]과 같이 세 가지 레벨로 분류할 수 있다. 분류 기준을 보면 다음과 같으며 중위 도메인 레벨은 하나 이상의 깊이를 가질 수 있다[9].

- 최상위 도메인 레벨 : 논리적 혹은 물리적으로 분리된 영역 안에서 가장 최상의 도메인으로서 외부 영역으로 통하는 보안 게이트웨이와 인접해 있다. 상위 도메인 레벨에도 하나 이상의 보안 정책서버가 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 보안 정책 적용 시기도 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 [7]에서 설계한 형태를 따르겠다.

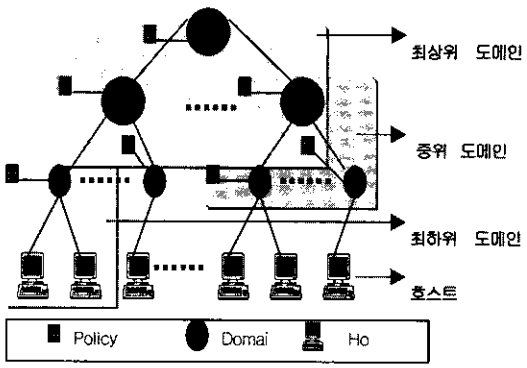


그림 3. 논리적인 도메인 레벨의 분류

- 중위 도메인 레벨 : 최상위 레벨의 보안 정책을 상속한 중위레벨로서 바로 호스트를 관리하지 않고 하위 도메인을 상속한다. 중위 도메인 또한 하나 이상의 정책서버를 가지며 이는 하나 이상의 SPS를 소유한다. 중위 도메인이 상속해준 하나 이상의 하위 도메인을 도메인 특성에 맞게 보안 정책을 적용하며 관리 한다. 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 하나 이상의 정책서버와 이에 해당하는 하나 이상의 SPS를 소유한다. 자신의 도메인 안에 있는 호스트가 다른 영역 혹은 같은 도메인 내의 호스트와 보안 정책 협상을 하기를 원할 경우 보안정책 서버의 역할을 한다.

3.2 보안 정책 모델의 특징

계층적 구조는 평면 구조에서 발생되는 분산된 보안 정책 갱신의 어려움을 해결할 수 있다. 즉 보안 정책의 수정 혹은 갱신이 쉽고 관리가 용이하다. 서로 신뢰하는 도메인간 혹은 신뢰된 도메인 안에

서는 정책협상이 불필요하고 확장된 통신망, 즉 글로벌 네트워크 환경에서 체계적인 보안 정책의 관리가 용이하다[10].

계층모델에서 정책은 자신의 상위 도메인으로부터 상속하여 자신의 도메인에 맞게 적용한다. 최상위 도메인의 정책을 상속한 중위 도메인은 각각의 특성에 맞게 서로 다른 도메인 정책을 적용하기 위해 허용되는 한 수정 및 변경이 가능하다. 상위 도메인은 가장 광범위하게 적용이 가능한 정책을 정의하고 각 중위 도메인은 이를 자신의 도메인에 맞게 추가하여 지역 정책 데이터베이스에 저장한다. 하위 도메인은 중위 도메인의 정책을 상속하여 자신의 도메인에 맞는 정책을 수립하여 지역 정책 데이터베이스에 저장한다. 여기에서 분산환경에서 상속에 관해서는 구현상의 문제이므로, 언급하지 않도록 하겠다. 또한 수정 및 갱신을 하기 위한 관리가 쉽다. 보안 도메인에서 수정 및 갱신이 일어나면 그 하위의 레벨의 도메인에 영향을 미친다.

Ⅳ. 보안정책 프로토콜 설계

계층적 구조의 보안정책 모델에서 정책 서버와 클라이언트는 SPP를 이용하여 정보를 교환한다. 이러한 프로토콜은 정책 정보가 클라이언트/서버에 의해 변경, 처리, 보호되는 방법과 변경되는 정책 정보, 그 정보를 인코딩 하는데 사용되는 형식 등을 정의한다. 메시지 포맷에 대한 내용은 다름과 같다[11].

4.1 메시지 타입

메시지 타입은 다음과 같이 6가지로 정의된다.

- Query message : 정책 정보를 요구
- Reply message : 특정 policy query에 대한 응답인 policy records
- Policy message : 정책 서버로부터 보안 정책을 업로드/다운로드할 때 사용되는 정책 정보
- Policy Acknowledgement message :policy message에 대한 ACK 메시지
- Transfer message : 서버들 사이에서 bulk policy information을 교환하는데 이용
- Keep Alive message : 서버의 상태를 SG나 다른 디바이스에 공지하는데 이용

SPP메시지는 보안 메커니즘을 이용하여 인증되어야 한다. 물론, 자신이 메시지에 대한 인증과 무결성을 제공할 수 있는 기본적인 보안 메커니즘을 제공하고, 특히 이종 도메인으로 이동할 경우에는 디지털 서명을 이용한다. 이 경우, SPP 서명 페이로드에 서명을 포함하여 전송되는데, 서명 검증에 사용되는 비밀키와 관련된 공개키의 억세스를 위한 인증서가 필요하다. SPP에서 인증서를 액세스하는 메커니즘의 제공은 범위 밖이지만, 다른 메커니즘의 대용으로 간단히 사용할 수 있는 간단한 인증 패칭 메커니즘을 적용한다.

4.2 SPP 페이로드

정책 정보를 요청(request)하기 위해 사용하는 질의 페이로드는 호스트나 SG, 그리고 정책 서버가 SPP 메시지 내의 질의 페이로드를 생성하여 정책 정보를 가진 정책 서버에게 전달한다. 레코드 페이로드는 정책 정보를 가지고 있는 필드이다. 서명 페이로드는 서명 페이로드를 제외한 SPP 메시지 전체에 대해 디지털 서명을 계산한 값을 가지는 페이로드이다. SPP 메시지의 무결성을 검증하는데 이용된다[12].

4.3 정책 질의

보안 게이트웨이 질의는 기본적인 질의로서 특정 수신측 주소 내에서 관련된 SG를 찾는 동적 메커니즘을 제공한다. 이러한 질의 내에는 통신의 송신측 호스트 또한 포함되어야 한다. 즉, 송신측과 수신측 사이의 SG를 찾는 질의이다. COMSEC 질의는 특정한 성질을 가지는 통신인지를 조사할 수 있도록 해주는 동적 메커니즘을 제공한다. 특정 성질을 통신 파라메터로 셀렉터(src/dst address, protocol, src/dst port 등)를 의미한다. CERT 질의는 공개키 인증서를 발송하거나 취득하는 메커니즘은 SPP의 범위가 아니지만, 이러한 외부 메커니즘이 제공되지 않을 경우, SPP는 인증서를 요청할 수 있도록 인증서 요청 질의를 제공한다. 그룹 정보 질의는 호스트로부터 정책 협상 요청을 받은 최하위 도메인은 협상을 하고자 하는 상대 호스트가 어떤 그룹에 속해있는지 알아보기 위해 최상위 도메인에게 그룹정보 질의를 전달하고 이에 대한 응답으로서 그룹정보 레코드를 반환 받는다[13]. 그룹정보 질의는 계층적 보안 모델의 장점을 살리도록 확장 설계된 것으로서 비슷한 속성을 갖거나 비슷한 보안등급을 갖는 호스트나 도메인을 그룹으로 묶어 장점을 계층구조의 장점을 살릴 수 있다.

4.4 정책 레코드

보안 게이트웨이 레코드는 호스트나 호스트 그룹을 보호하는 주/부 보안 게이트웨이의 인터페이스를 IP 주소 형태로 포함하고 있다. 즉, SG의 질의에 리스트 되어 있는 송신측 주소와 수신측 주소 사이에 IP 데이터그램의 도달하기 위해 이동하는 각 지점에서의 주 SG와 부 SG에 대한 정보를 가지고 있다. 만약, IP 데이터그램이 다중 게이트웨이를 이동한다면, 보안 게이트웨이 레코드는 각 게이트웨이에 대해 각각 정보를 가지고 있어야 한다. 부 보안 게이트웨이 리스트는 선택적이다.COMSEC 레코드는 원하는 통신이 특정 셀렉터 값을 가질 수 있는지 나타낸다. 보안협상 레코드는 레코드 내의 소스 주소와 목적지 주소간의 특정 SA를 규정짓는 셀렉터와 보안협상 애트리뷰트 (Attribute)를 포함하고 있는 필드이다.

정책 서버 레코드는 특정 정책 서버가 인증하는 노드(호스트, SG, 다른 정책서버) 리스트를 포함하고 있는 필드이다. 즉, 정책 서버의 보안 도메인 멤버를 나타낸다. CERT 레코드는 SPP에서 공개키 발송을 대신하는 메커니즘으로 공개키 인증서를 하나 가지는 레코드를 말한다.

갱신 레코드는 수정 혹은 갱신이 필요할 때 자신의 정책을 상속받은 하위 도메인에게 전달하는 데이터이다. 갱신 레코드는 계층구조에서 효율적으로 보안정책을 갱신 및 수정할 수 있도록 기존의 보안 정책 프로토콜의 정책 레코드를 확장 설계하였다. 그룹 정보 레코드는 정책 협상을 요청 받은 최하위 도메인이 최상위 도메인에게 그룹정보 질의를 던졌을 때 최상위 도메인은 이에 대한 응답으로 그룹정보 레코드를 전달한다. 그룹정보 레코드에는 협상을 원하는 상대 호스트가 어떤 그룹에 속해 있는지 그룹 아이디와 그룹 주소를 전달한다.

V. 보안정책 협상 메커니즘

이 논문에서 설계한 계층적 구조의 보안정책 모델에서 호스트가 다른 호스트와 보안정책 협상을 하기 위해서는 관리 영역에 따라 크게 각 호스트가 다른 영역에 존재해서 [그림 4]의 2와 같이 보안 게이트웨이를 거쳐야 하는 경우와 같은 영역에 존재해서 보안 게이트웨이를 거치지 않는 경우로 분류할 수 있다.

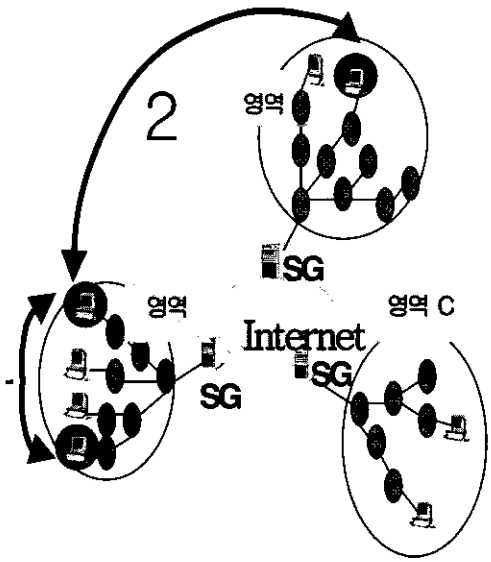


그림 4. 계층구조의 협상 메커니즘에 대한 동작도

5.1 메커니즘 1에 대한 상세 시나리오

[그림 4]에서 본 두 가지 경우의 보안 협상 메커니즘 중 1에 해당하는 경로에는 최상위 도메인 내에 있으나 중위 도메인과 최하위 도메인을 달리하는 도메인에 존재하는 호스트와의 보안 정책을 협상하고자 한다. 이때 보안 정책 협상을 하기 위해 외부 보안 게이트웨이는 거칠 필요가 없으며 계층구조의 보안정책 모델 내에 존재하므로 그룹정보를 이용하여 그룹간의 정책 정보를 확인할 필요 없이 직접 호스트간의 정책 협상을 한다. 이 과정을 시퀀스 다이어그램으로 그려보면 [그림 5]와 같다.

[그림 5]에 표현된 시퀀스 다이어그램을 단계적으로 설명하면,

1) 마스터파일은 표현상의 에러를 없애기 위해 먼저 파싱하고 검증한다.
2) 마스터 파일내의 정책들은 비연관성 처리를 사용하여 연관성을 제거한다.
3) PS_A와 PS_B는 각각의 보안 도메인 내의 SPS 데이터베이스로부터 정책을 로딩하고, 정책 요청을 기다린다. 커널에서 키관리 프로토콜로 보내진 메시지는 정책요청 메시지를 시작하도록 해준다.
4) PC_A는 PS_A에게 Q1을 보낸다.
5) PS_A는 Q1을 분석하여 자신의 관리하에 있는 호스트인가를 검색한다. 검색 결과에 따라 두 가지 경우가 발생한다.
   A. 자신의 도메인 내에 속한 호스트 일 경우 단계8로 진행 한다.

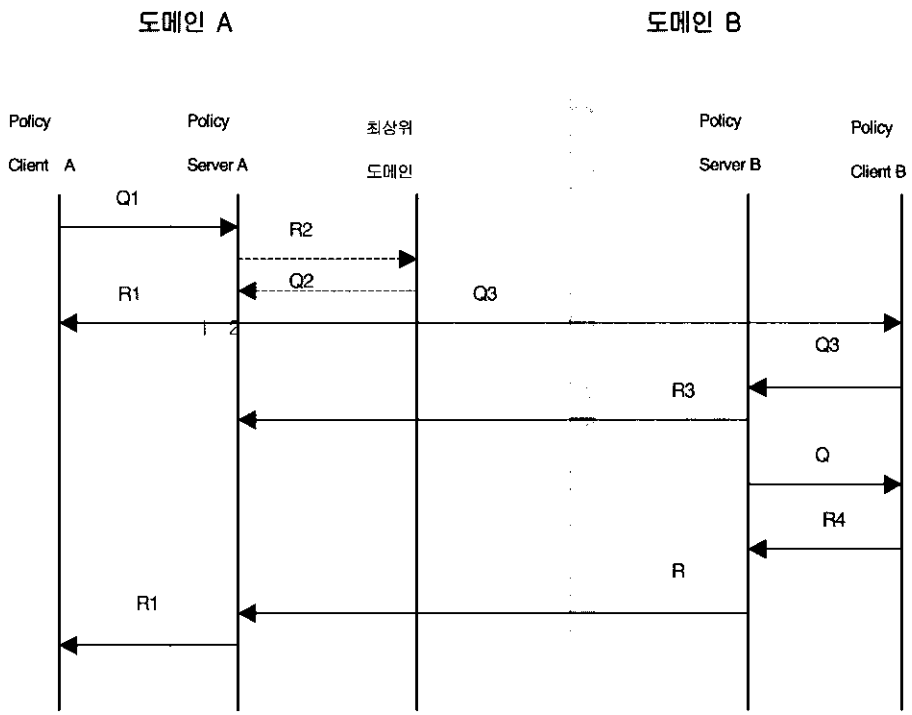


그림 5. 메커니즘 1에 대한 시퀀스 다이어그램

B. 자신의 도메인 내에 속한 호스트가 아닐 경우 정책 협상을 하고자 하는 PC_A가 어떤 도메인 내에 속한 호스트 인가를 확인하고 그룹 정책을 적용하기 위하여 최상위 도메인에게 그룹정보 질의(Q2)를 전달한다. 이어 단계 6으로 진행한다.

6) 최상위 도메인은 PS_A가 요청한 그룹정보 질의를 분석하여 해당 호스트가 어떤 그룹에 속해있는지 도메인 이름과 주소 등의 정보가 들어있는 그룹 정보 테이블을 검색하여 그룹 정보 레코드(R2)를 전달한다.

7) PS_A는 전달받은 R2에서 도메인의 이름으로 관계 정보를 검색하였을 때 다음의 두가지 경우가 발생한다.

A. 그룹 관계정보가 이상이 없을 경우 다음의 단계 8로 진행한다.

B. 그룹 관계 정보가 접근을 금지하는 영역에 있을 경우 협상이 불가능하므로 정책 협상을 중지하고 불가하다는 R1을 전송한다.

8) PS_A는 질의와 매치되는 캐쉬 내의 정책 레코드를 검색한다. 만약 필요한 정책이 없으면, PS_A는 PC_B로 Q3를 보낸다.

9) PC_B는 Q3를 검증해 보고, 적당한 정책 정보가 있는지 데이터베이스를 검색하기 위해 PS_B에게 전달한다.

10) PS_B는 먼저 Q3내에 있는 정책 정보와 지역정책을 병합한다. 그리고, 원래의 질의 정보와 PC_B와 PC_A가 안전하게 통신을 하기 위해 필요한 정보를 이용하여 R2를 생성하여 PS_A에게 보낸다.

11) PS_B는 Q4을 생성하여 PC_B에게 보내고, PC_B는 R4를 생성하여 PS_B에게 보낸다.

12) R3는 PS_B에서 병합되고 PS_B는 PC_B가 자신에 의해 인증 되었다는 정보를 추가하여 R3를 생성하여 이를 PS_A에게 보낸다.

13) R3내에서 병합된 정책은 PS_A로 리턴되고, PS_A는 R3에서 받은 외부 정책을 지역 정책에 병합시키고,이를 캐쉬 한다.

5.2 메커니즘 2에 대한 상세 시나리오

[그림 4]에서 본 두 가지 경로의 보안 협상 메커니즘 중 2에 해당하는 경로에는 최상위 도메인을 벗어나 다른 영역에 속한 호스트와 정책을 협상하고자 한다. 이때 보안 정책 협상을 하기 위해 보안 게이트웨이를 거쳐야 하며 계층 구조의 보안정책 모델에서 최상위 도메인의 영역을 벗어나는 것은 계층 구조의 보안정책 모델의 범위를 벗어나므로

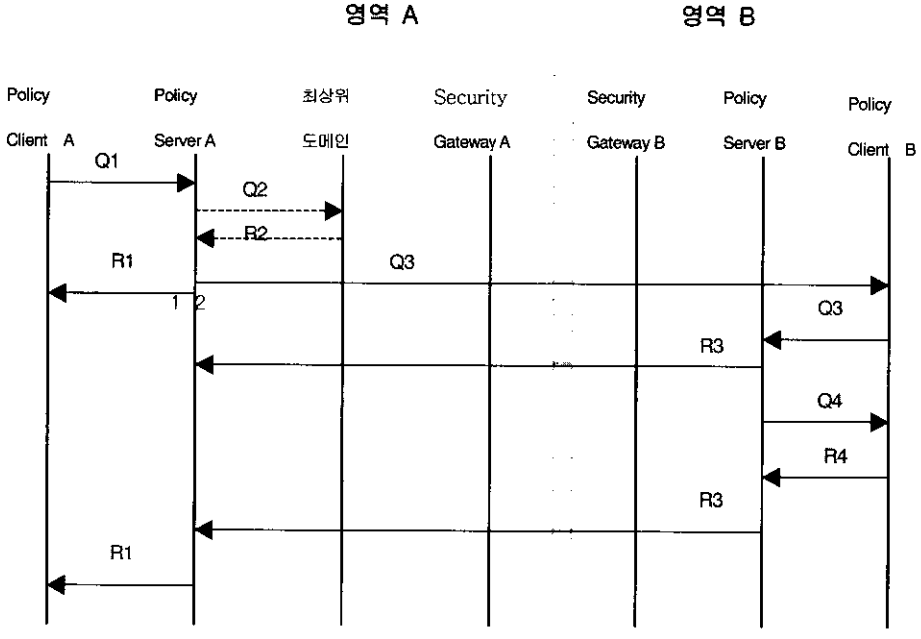


그림 6. 메커니즘 2에 대한 시퀀스 다이어그램

최상위 도메인이 영역 B의 그룹정보를 가지고 있거나, 가지고 있지 않는 경우 계층 구조의 보안정책 모델에 적용 받지 않고 일반 정책 모델에서의 보안 정책 협상 메커니즘과 같이 정책 협상을 하게 된다. 보안 정책 협상을 하기 위해 보안 게이트웨이를 거쳐야 하며 그룹정보를 이용하여 그룹간의 정책 정보를 확인한 후 호스트간의 정책 협상을 한다. 이 과정을 시퀀스 다이어그램으로 그려보면 [그림 6]과 같으며 동작과정은 앞서 설명한 시퀀스 다이어그램에서와 동일하므로 생략하도록 한다.

Ⅵ. 기존 연구와의 비교

기존의 IP 보안 시스템은 각기 다른 보안 영역의 통신 상대와 통신하거나 다른 보안 영역을 거쳐서 통신하는 경우에, 정책에 대한 중앙 집중적인 관리나 정책 정보의 일반화 없이 각 보안 영역에 따라 자신의 지역 정책을 적용한다. 따라서 기존 IP 보안 서비스를 사용하여 종단 노드들간에 IP 패킷을 교환할 때 보안 영역들 간의 정책 요구사항이 서로 다르고, 망의 복잡한 토폴로지로 인하여 패킷이 양방향으로 같은 경로를 따라 전송되고 같은 정책을 사용하여 보호되는지 보장할 수 없으며, 동적인 SA들을 관리할 필요성과 같은 문제점들이 발생한다. 또한 인트라넷 환경이 발달된 현재 그룹개념이나 도메인의 개념에 따라 보안정책의 도입이 어렵고 각각의 안전 등급에 따른 차별적인 관리와 보호가 어렵다. 또한 분산환경에서 이와 같은 보안정책이 적용될 경우 비효율적이며 세분화된 보안 서비스를 제공하기 어렵다.

계층적 보안모델을 기반으로 설계된 보안정책 메커니즘은 엔터프라이즈와 같은 기업 환경에서 적절히 사용될 수 있도록 계층화하여 모델화 하였으며, 계층간의 안전 등급에 따라 차별화 된 보안정책을 적용할 수 있고 최상의 도메인의 보안정책에 따라 효율적인 보안정책 관리가 용이하며, 보안정책에 관한 수정과 갱신이 용이하도록 설계하였다.

그러나 이러한 계층적 보안 구조가 가지는 보안 취약성을 두 가지 관점으로 살펴보면, 계층적 보안 구조 관점에서는, 대규모 분산환경에서 많은 보안 정책 서버들을 관리해야 되고, 계층적인 구조를 갖기 때문에 중간 노드(서브 도메인의 보안 정책 시스템)의 문제 발생은 서브 도메인과의 안전한 통신을 저해할 수 있다는 것이고, 보안 정책 시스템 관점에서는, 보안 정책 시스템의 붕괴는 안전한 통신을 위한 네트워크 전체의 붕괴를 의미하며, 보안 정책 시스템 또한 하나의 시스템에 불과하므로 보안 시스템의 취약성과 일맥 상통한다는 점이다. 이에 대하여 중간 노드의 문제 발생을 복구 또는 해결할 수 있는 대책이 요구된다. 또한 그룹 개념을 엔터프라

이즈 네트워크를 대상으로 적절하게 적용함으로써 네트워크 전체의 보안성을 향상시킬 수 있으며, 각 호스트간의 보안 정책 협상을 효율적으로 지원 할 수 있으며 표 1과 같다.

Ⅶ. 결 론

최근 인터넷에 접속하는 사용자의 수가 폭발적으로 증가하면서 인터넷을 통해 제공되는 서비스가 다양해지고, 이에 따라 인터넷을 통해 안전하게 데이터를 제공하고자 하는 요청이 증가하게 되었다. 이에 대응하기 위해 인터넷 구조와 인터넷 표준화 단체인 The Internet Engineering Task Force(IETF)의 차세대 인터넷 프로토콜 작업반(IPNG-WG : IPNG Working Group)에서는 주소지정능력을 향상시키고 데이터 보안을 지원하는 확장 헤더를 정의함으로써 기존의 인터넷 프로토콜 버전 4인 IPv4를 대체할 새로운 인터넷 프로토콜 버전 6(IPv6) [RFC-188 3]를 정의하였다.

표 1. 기존구조와의 비교

비교항목	평평한구조의 보안정책	계층적 구조의 보안 정책
관리의 용이성	중앙집중적인 관리로 대규모일수록 비효율적인 관리	분산된 관리로 그룹별 관리가 용이
정책협상 메카니즘의 효율성	일률적인 협상 메커니즘의 사용으로 비효율적	그룹개념의 사용으로 효율적
보안 서비스의 다양화	중앙 집중적인 서비스 제공으로 불가능	보안등급별 다양화된 서비스 제공 가능
엔터프라이즈 환경에서의 효율성	비효율적	적당하며 효율적
취약점	보안등급의 세분화가 없으므로 보안 정책 시스템의 붕괴가 쉬움	중간 노드붕괴로 인한 네트 워크의 붕괴

IP보안 서비스를 사용할 때, 종단 노드들간의 보안 서비스 품질을 보장하기 위해서는 위와 같은 문제점들이 해결되어야 한다. 이를 위해, IP 보안 정책을 지원하는 정책 시스템 구조, 정책 시스템이 사용하는 데이터 모델, 정책 정보의 기술을 위한 언어, 정책 정보를 교환하기 위한 프로토콜 등이 정의되어질 필요가 있다.

이 논문에서는 인터넷에서 서로 다른 보안 정책을 사용함으로 발생할 수 있는 문제점을 정책 협상 시스템을 이용해 해결하고자, 기존의 평평한 구조에서 발생되는 분산된 보안 정책 갱신의 어려움을 해결하고, 확장된 통신망, 즉 글로벌 네트워 환경에서 체계적인 보안 정책의 관리가 용이한 구조인 계층 구조를 설계하고 IP 보안정책을 지원하는 보안정책 시스템 구조를 바탕으로 보안 정책 정보를 교환하기 위한 프로토콜 등을 확장 설계하였다. 또한 그룹 개념을 정의하여 실제 호스트간의 보안 정책 협상이 보다 효과적으로 수행되도록 협상 메커니즘을 정의하였으며, 이를 위한 질의와 레코드를 확장 설계하고 계층적 보안 모델에서 효과적인 보안정책 상속 및 수정을 위한 갱신 레코드를 정의하였다. 또한 계층적 보안 정책 모델에 맞게 설계된 보안 정책 데이터베이스 구조 설계를 이용하여 동일한 정책 속성을 갖는 호스트들의 모임을 그룹으로 정의하고, 이 개념을 기반으로 효율적인 연동 메커니즘을 설계하였다. 그러나 대부분 개념적 관점에서 계층적 보안 정책 모델을 설계하였으며 이에 대한 효율성 및 타당성에 대한 검증을 수행하지 못하였다. 향후 이 모델을 구현하여 그 효율성과 타당성을 분석하는 연구와 분산구조에서의 효율적인 객체상속 방안에 대한 연구, 무선 환경으로의 적용 방안에 관한 연구가 필요하다.

참 고 문 헌

[1] 조은경, 최은심, 권영회, 양태연, 인소란, IP보안 정책 연구, 한국 정보 처리 학회 추계 학술발표 논문집, 제6권 2호,1999.

[2] M.Stevens, W.Weiss, Policy Framework, Internetdraft, draft-ietf-policy-framework-00.txt, 1999. 9.

[3] Y. Snir, Y. Ramberg, QoS Policy Schema, InternetDraft, draft-ietf-policy-qos-schema-01.txt, 2000.9.

[4] 윤혁중, 김학범, 이홍섭, IETF 정보 보호 표준화 동향, 한국통신보호학회지, 제10권 2호, 2000.6.

[5] 임채훈, 강명희, 인터넷 보안 : 가상사설망, 방화벽 그리고 침입탐지시스템, 한국통신학회지 Vol.17 No.3

[6] IBM,Internet Security Policy :A Technical Guide, 1997.

[7] 윤여웅, 엄남경, 김건우, 이상호,계층적 보안 모델에서의 데이터베이스설계, 한국정보처리학회 논문지 투고중,2001
[8] Fred Halsall, Data Computer Networks And Open Systems Fourth Edition, Addison Wesley, 1999
[9] Paul Albitz, Cricket Liu, DNS와BIND, 한빛미디어, 1999
[10] S.Kent, R.Atkinson, Security Architecture for the Internet Protocol, RFC2401, Nov. 1998.
[11] 이용주, 엄남경, 이지인, 이상호, 김건우, 보안정책에서의 계층적 연동 방식 설계, 한국정보과학회 충청지부 추계학술대회 논문집, p36-40, 2000.
[12] 엄남경, 이상호, 김건우, 이종태, 손승원, 안전한 통신을 위한 계층적 구조의 보안정책 적용 방안, 한국통신정보보호학회 충청지부 학술대회 논문집, 2000
[13] 엄남경, 황윤철, 이상호, 이종태, 손승원, 계층적 보안 정책을 위한 데이터베이스 구조설계, 한국정보과학회 충청지부 추계학술대회논문집, p41-46, 2000.

황 윤 철(Hwang Yoon Cheol)

1994년 : 한남대학교 전자계산공학과 졸업 (공학사)
1996년 : 한남대학교 대학원 전자계산공학과 졸업 (MS)
1999년~현재 : 충북대학교 대학원 전자계산학과 박사과정수료
<주관심 분야> 보안정책,네트워크 보안, IDS, Active Network

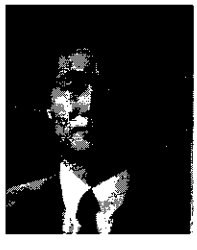
이 용 주(Lee Young Ju)

1999년 2월 : 청주대학교 정보통신공학과 졸업
2000년 2월 : 충북대학교 전자계산학과 졸업
2000년 1월~현재 : 한국전자통신연구원
<주관심 분야> 미들웨어보안, 인터넷정보보호, 액티브네트워크

이 종 태(Lee Jong Tae)

1984년 2월 : 서울대학교 물리교육학과 졸업
1991년 10월 : Indiana University 물리학과 박사
1992년 1월~현재 : 한국전자통신연구원 책임연구원
<주관심 분야> 통신정보보호, 인터넷보안, 양자암호

이 상 호(Lee Sang Ho)



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