情 報 保 護 學 會 誌
第 13 券 第 1 號, 2003. 2

정책 기반의 정보보호 시스템 관리기술

신 영 석*, 장 종 수**

요 약

정보통신 기술의 발전과 인터넷의 사용자 증가로 인해 인터넷은 사회 각 분야에 다양하게 활용되고 있으나, 해킹 및 사이버테러에 대한 역기능이 증가되고 있는 실정이다. 최근 이를 위한 정보보호 시스템과 정보보호 관리기술이 연구 개발되고 있다. 본 고에서는 인터넷에 구축되어 있는 다양한 방화벽, 침입탐지 시스템 등의 정보보호 시스템을 효율적으로 관리하기 위해 인터넷에서 정책 기반의 정보보호 시스템에 대한 관리기술과 이들의 분산 시스템에서 보안정책의 정보공유 기술을 살펴본다.

Ⅰ. 서 론

인터넷 서비스의 폭발적인 증가로 인해 네트워크는 복잡해지고 있으며, 네트워크 구성장치(NE, Network Element)도 다양한 기능으로 확장되고 있다. 이러한 네트워크의 기술 발전과 서비스 확산으로 인터넷은 사회 각 분야에 다양하게 활용될 뿐 만 아니라, 해킹과 사이버테러에 대한 역기능이 증가되는 추세이다.

최근 인터넷에서 해킹은 악의적 사용자에 의한 독창적인 새로운 침입 사례는 네트워크 보안관리에 어려움을 더욱 증대시키고 있다. 이에 대응하기 위한 방화벽, 침입탐지 시스템, IPSec(IP Security), VPN, SSL(Secured Socket Layer), S-HTTP 등의 여러 정보보호 시스템과 프로토콜이 개발되어 네트워크에 구축되고 있다. 그러나 동시 다발적이며 광범위한 인터넷을 대상으로 정보보호 시스템과 NE를 일사불란하게 가동하여 운영하기란 쉬운 일이 아니다. 즉 네트워크 관리 측면에서 통신 사업자와 사설망의 관리 범주, 정보보호 시스템 간의 상호 호환적인 접속 및 제어관리에 많은 어려움이 뒤따른다. 따라서 네트워크 관리 서비스에서 SNMP, CMIP 등의 접속 프로토콜로 NE의 네트워크 관리정보(MIB, Management Information Base)를 공유하는 차원과 같은 방식으로 각 NE 간에 보안관련 정보(PIB, Policy Information Base)를 공유하며, 이를 기반으로 보안 정책(policy)을 수립하여 네트워크와 정보보호를 관리하는 방향으로 연구되고 있다[6,13,18].

본 논문에서는 정보보호 시스템에 대한 관리 기능을 네트워크 관리 측면에서 검토하고, 이들을 효과적으로 관리하기 위한 정책 기반의 정보보호 시스템과 기술을 살펴보기로 한다. 제2장은 OSI 참조모델에 따른 계층별 정보보안 시스템에 대한 기능과 정책 기반의 네트워크 관리기술을 살펴보며, 제3장에서는 정책 기반의 정보보호 시스템에 대한 시스템 구성을 살펴본다. 제4장에서는 보안정책 정보를 공유하는 방안과 네트워크 구조를 검토하며, 제5장에서는 결론과 향후 연구방향을 제시한다.

Ⅱ. 정보보안 시스템의 관리기술

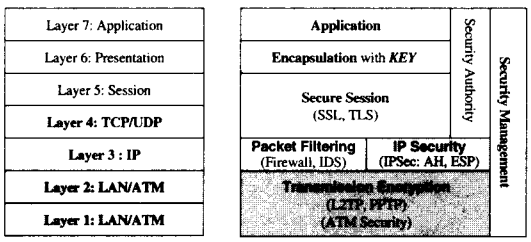
1. 계층별 정보보호 기능

네트워크에서 정보보호 기능은 응용 서비스에서 별도의 키(key)에 의한 암호화로 정보를 보호하거나 특정 호스트 혹은 응용 서비스 사용에 따른 액세스 레벨의 정보보호로 인식될 수 있다. 그러나 네트

* 호남대학교 정보통신공학부 (ysshin@honam.ac.kr)
** 한국전자통신연구원 정보보호기술연구본부 (jsjang@etri.re.kr)

워크를 구성하는 시스템, 이들 간의 전송선로를 비롯하여 상위계층의 응용 서비스에 접속하는 경우에 다양하게 계층별로 그림 1과 같이 기능적으로 구분할 수 있다. 물리계층과 링크계층에 적용되는 LAN, ATM, Gigabit 네트워크에서 연결 경로에 따라 ATMSec(ATM Security)와 같은 L2TP(Layer 2 Tunneling Protocol), PPTP(Point-to-Point Tunneling Protocol)가 적용되거나, 특정 포트에 허락된 MAC 주소를 사용도록 규정할 수 있다. 계층 3은 인터넷 프로토콜과 소스 코드 개방으로 패킷 스니퍼(packet sniffer)이 가능하다. 따라서 이를 위해 IPSec 혹은 IPv6에서 별도의 패킷 레벨에서 정보보호 기능을 제공하고 있으며, 패킷 필터링에 의해 네트워크 차원에서 접속을 허락하거나 차단하는 기능을 제공한다.

상위계층에서는 응용 서비스의 세션에 의한 SSL/TLS(Transport Layer Security), 서비스 제공에 따른 별도의 키 관리 및 배분과 암호화 등의 기능이 제공된다. 한편 키 관리와 정보보호의 공유를 위해서는 일련의 공통된 구조 모델과 인증 및 접속 프로토콜에 의한 별도의 네트워크 관리 기능이 요구된다.



〔그림 1〕 계층별 정보보호 기능 적용 개념도

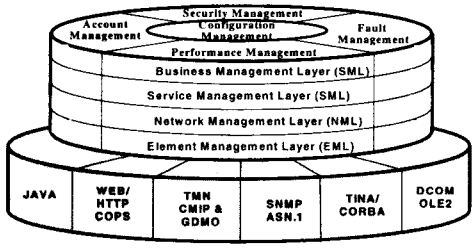
2. 네트워크 관리기술

공중통신망의 네트워크 관리에 대한 구조 모델은 그림 2와 같이 TMN(Telecommunication Management Network)으로 정립되며, 관리 기능은 FCAPS (Fault, Configuration, Accounting, Performance, Security) 영역(area)으로 요약된다.

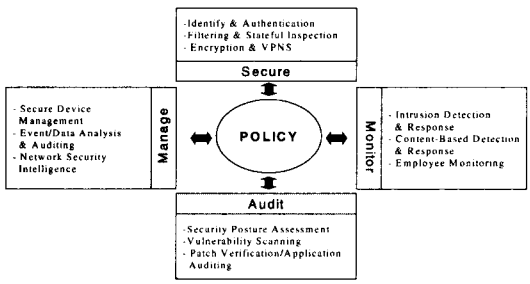
네트워크 관리 구조에서 실제 기능을 수행하는 엔티티(entity) 간의 접속은 관리자(manager)와 에이전트(agent) 혹은 서버와 클라이언트 모델로 2-tier 구조로 구성된다. 에이전트 기능이나 지역적인 구축 환경에 따라 프록시가 설정됨에 따라 3-tier 구조로 구성될 수 있다. 에이전트는 관리자가 요구하면 해당 관리정보를 제공하며, 이들 간에 정보 표현의 통일성과 효율적인 정보 전송 및 공유를 위해 별도의 프로토콜과 정보 모델 그리고 분산 시스템 기술이 요구된다.

초기 네트워크는 안정된 네트워크의 운용 및 유지와 네트워크 구성장비의 결합 및 복구에 최우선의 목표였다. 따라서 네트워크의 구성관리와 운용 상태의 모니터링을 위한 관리에 많은 투자와 이를 위한 NMC가 구축되고 있다. 그러나 정보통신 기술의 발전과 멀티미디어 서비스 출현, 시스템 안정화에 따라 이제는 성능과 보안관리 기능에 중점을 두어 네트워크를 관리하고 있다.

보안관리는 사용자가 네트워크 서비스와 상위계층에서 응용 서비스간의 액세스, 네트워크 디바이스 액세스 제한으로 구분된다. 이는 계층별로 이루어지지만, 해당 NE 기능에 의해 제한되어 접속된다. 기능적으로 다양하고 손쉽게 NE를 제어관리 하며, 항시 예고치 못한 정보보호를 위해서 NE 및 분산된 정보보호 시스템을 통합적인 정보보호 관리를 위해서는 중앙 집중적으로 일정한 정책 기반으로 일관성 있게 보안관리를 해야 한다. 이러한 네트워크 관리 정책은 그림 3과 같이 네트워크의 모니터링(monitor)과 감시(audit), 정보보호(secure), 관리(manage) 측면으로 기능을 실행하는 차원으로 보안정책 기능을 도출할 수 있다.



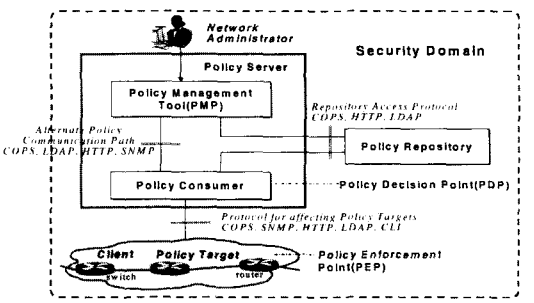
〔그림 2〕 TMN 기능 구조와 요소기술



〔그림 3〕 정보보호 관리에서 보안정책의 기능 구분

3. 정책 기반의 정보보호 시스템

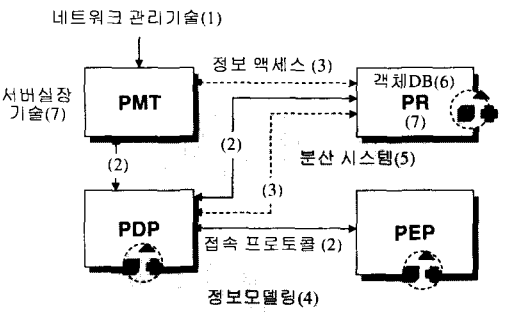
정책 기반의 통신 시스템 관리(Policy-Based Network Management: PBNM) 모델은 IETF 표준화 문서에 정립되어 있다[6,7]. 정책 기반의 네트워크 관리는 네트워크에서 제공하는 정보보호 및 통신 자원(resource) 제어를 위한 정보를 모니터링하여, 수립된 정책에 근거로 NE를 효율적으로 관리하는 데 있다. 정책 기반의 정보보호 관리를 위해서 NE는 네트워크 정보 혹은 정보보호 및 보안정책(PIB) 등의 정보를 SNMP, HTTP, COPS(Common Open Policy Service), LDAP(Light Directory Access Protocol) 등의 프로토콜을 사용하여, 정책을 관리하는 정책 서버에 정보를 전달한다. 정책관리 시스템은 수집된 정보를 분석하여 운영자가 수립하는 정책 규칙(policy rules)에 따라 수행하도록 세부 명령을 내리면 된다.



〔그림 4〕 정책 기반의 통신시스템 구성

PBNM의 기능 구조는 NE를 실시간으로 모니터링하여, 동적으로 변화되는 정보를 신속하게 정책 서버에 전송해야 한다. 이를 위해서 PBNM 시스템은 그림 4와 같이 기능적으로 정책관리 도구(Policy Management Tool: PMT), 정책 저장장치(Policy Repository: PR), 정책 결정장치(policy consumer), 정책수행 대상장치(policy target)로 구분한다. 통신망 사업자 관점으로 볼 때, 운영자에 의해 정책을 관리하고 통신망 동작을 모니터링하는 운영자 시스템(PMT), 정책 규칙 및 각종 네트워크 정보를 관리하는 PDP(Policy Decision Point), 실제 정책을 수행하는 PEP(Policy Enforcement Point)로 구분한다.

정책 기반의 통신 시스템은 컴포넌트 간에 원활한 정보교환과 제어를 위해 그림 5와 같은 요소기술이 요구된다. 세부 요소기술로는 컴포넌트 간의 접속 프로토콜, PDP, PEP, PR에서 운영되는 네트워크 관리정보에 대한 정보모델링, PR의 정책 객체를 액세스하는 접속 프로토콜, 네트워크 관리기술, 이들 컴포넌트의 객체를 한데 묶는 분산 시스템 기술로 구분된다. PBNM 시스템의 접속 프로토콜로는 SNMPv3, CLI, COPS-PR, HTTP 등이 있으며, 정보 액세스를 위해서는 LDAP, COPS-PR, HTTP, SQL과 분산 시스템으로는 CORBA(Common Object Request Broker Architecture), DCOM 등의 기술을 들 수 있다.



〔그림 5〕 정책 기반의 정보보호 시스템의 요소기술

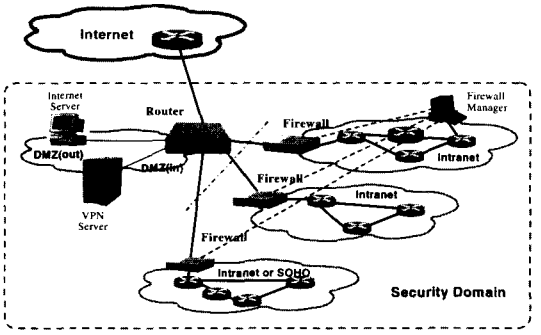
III. 정책 기반의 정보보호 관리 시스템

1. 정보보호 시스템

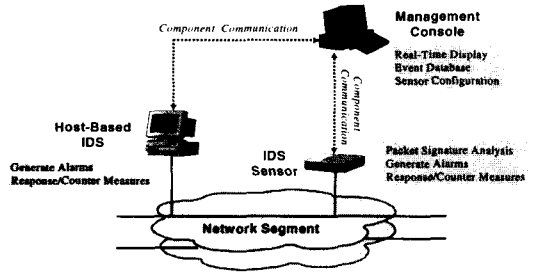
네트워크 기반의 정보보호 시스템을 구분하며, 패킷 필터링을 이용하여 액세스를 제어하는 방화벽, 네트워크에 해커 등이 침입을 탐지하고 이를 제어하는 IDS(Intrusion Detection System)와 관련 네트워크 센서 시스템, 정보보호 기능을 제공하는 NE, 정책 관리 시스템으로 구분된다. 기능적으로 종단 간에 보안연결을 수행하는 VPN, IPSec, 키 관리, NAT 등의 기능으로 구분된다.

네트워크에서 정보를 보호하는 시스템 구축 단계로 방화벽, 키를 이용한 암호화를 이용한 액세스 제어를 목적으로 한 1단계가 있다. 침입 탐지 시스템을 구축하여 외부로부터 해킹 및 정보보호 관리하거나 별도의 연결에는 VPN, IPSec 및 디지털 인증을 통한 개별적 정보의 보호를 관리하는 2단계, 그리고 3단계는 정책 기반으로 1, 2 단계를 통합하여 관리하는 구조로서 여러 벤더에서 제품 개발단계로 제시하고 있다[19]. 따라서 초기 단계에는 지역적으로 정보보호 영역에서 그림 6과 그림 7과 같은 대규모

네트워크에서는 지역적으로 대규모 네트워크에서 각 장치를 관리하는 관리 서버 혹은 PMT(manager)에 의해 통제되어 기능별로 수행된다. 그러나 이러한 서버들의 중복 투자와 서로 다른 서버로 인해 통합적인 정보보호 관리가 어렵게 된다. 이를 위해 중앙 집중적으로 개별화된 시스템 관리를 탈피하여 통합된 관리를 위해 정책 기반의 네트워크 관리가 요구된다.



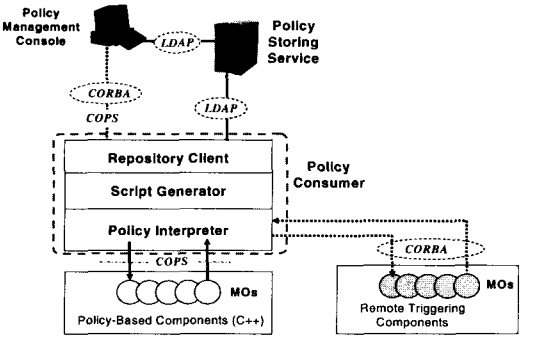
〔그림 6〕 방화벽 구성도



〔그림 7〕 침입탐지 시스템 구성도

2. 정책 기반의 보안관리 시스템

정보보호는 사설망 혹은 공중 통신망에서 부분적으로 지역화(grouping, regional)되어 관리된다. 이들 지역화된 영역에서 정보보호 시스템과 NE들은 수립된 보안정책에 따라 응용 서비스와 패킷을 제어 관리한다. 문제는 기존의 네트워크에서 정보보호 시스템, NE들 간에 네트워크 관리정보와 보안정책 정보를 효율적으로 교환하고 공유하는 프로토콜과 분산 시스템 그리고 이들 기능을 지원하는 서버가 요구된다. 또한 중앙집중식으로 수립된 하이 레벨(High-Level)의 보안정책을 서로 다른 정보보호 시스템에 맞게 해석하여 이를 NE 디바이스에 적용하여 운영해야 한다. 그림 8에서 볼 수 있듯이 보안정책은 객체로서 정책 레포지토리에 데이터베이스로 저장된다. PDP와 PEP는 보안정책을 상호 간에 LDAP 프로토콜을 이용하여 정보를 공유하며, 해당 디바이스에 적용도록 PDP에서 기능을 제공한다. 최근 많은 벤더들이 DEN으로 제공되는 구조로 상용 시스템으로 개발되고 있다. 그러나 정보보호 시스템과 NE인 PDP와 PEP의 접속은 장기적으로 PIB 객체를 직접 액세스가 가능하도록 분산 시스템 환경인 CORBA을 적용하거나, 정책 객체를 클라이언트-서버 모델로 손쉽게 교환이 가능하도록 COPS를 적용하는 2개의 구조로 구분되어 연구개발 되고 있다. 이러한 개발 전략은 현재 상용제품은 벤더들 간의 컨소시엄을 구성하여 정책 기반의 네트워크 관리 플랫폼을 구성하여 제공하고 있다.



〔그림 8〕 정책 기반의 정보보호 관리시스템 구성

IV. 보안정책의 정보공유 구조와 모델

1. 보안정책 정보공유 구조

1.1 WBEM 기반의 정보공유

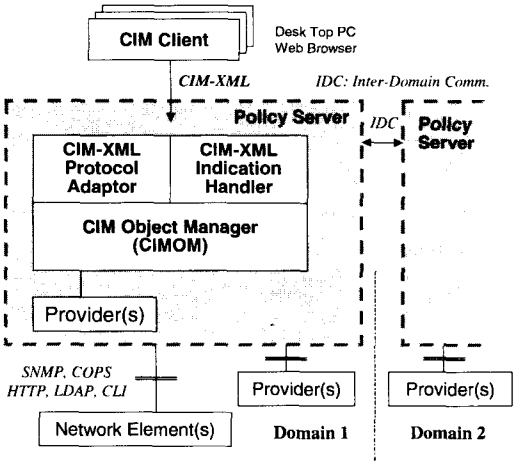
WBEM(Web-Based Enterprise Management)는 인터넷 상에서 상이한 네트워크 관리 프로토콜과 NE 환경을 극복하기위해 개발되었다. 네트워크 관리자가 데스크 탑 PC 상에서 웹 브라우저를 이용해 호환성이 없는 시스템이나 네트워크 및 애플리케이션을 관리할 수 있는 표준규격 개발을 목표로 한다. '96년 7월에 Microsoft, Cisco, Compaq, Intel 및 BMC 소프트웨어 등이 구성한 컨소시엄(DMTF)에서 WBEM 관련 표준화 작업을 수행 중이다.

WBEM의 표준은 SNMP, DMI, CMI를 사용하여 기존의 NE의 데이터 수집 에이전트와 웹 서버와 접속을 함으로서 네트워크 관리 정보를 효과적으

로 수집하여, 관리자가 웹 브라우저 근간의 GUI 환경에서 원격으로 네트워크를 관리할 수 있는 플랫폼을 제공한다. 따라서 그림 9와 같이 보안정책 서버는 NE에 존재하는 네트워크 운영관리 정보(CIM, Common Information Model)를 중앙집중식으로 수집하며, 관련 정보를 HTTP 프로토콜로 NE에게 제공한다. 그러나 실제 NE의 CIM 정보를 웹에서 볼 수 있도록 해당 네트워크 관리정보를 XML (xmlCIM) 형태로 제공한다.

WBEM 방식에 의한 정보공유는 중앙집중식으로 NE의 에이전트와 웹 서버(정책서버) 간에 다양한 접속 프로토콜에 의해 수집된 보안정책 정보를 XML 형태로 변환하여 이를 공유하도록 한다. 따라서 서버는 CIM 클라이언트에 의해 요구된 메시지에 따라 정보를 전송하면 된다. 또한 그림 9와 같이 서버에는 CIMOM(CIM Object Manager)이 상주하여 해당 정보를 일관성 있게 관리해야 한다. NE는 CIM schema의 정보를 수시로 혹은 Event에 따라 서버에 전송해야 한다.

WBEM 방식은 NE 측면에서는 HTTP를 사용함에 따라 구현이 용이하지만, 중앙 집중식의 서버에 의존성 높아 시스템 장애에 따른 이중화 대책이 별도로 요구된다.



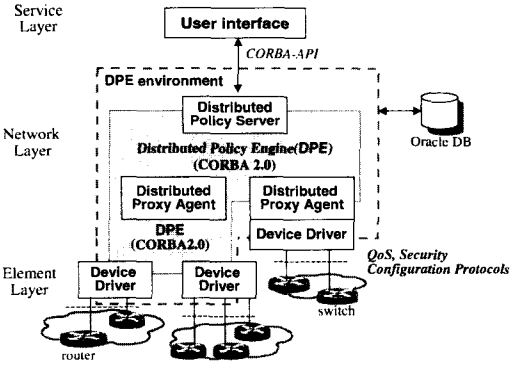
〔그림 9〕 WBEM 기반 정보공유 시스템의 기능 블록 구성

1.2 CORBA 기반의 정보공유

보안정책이나 관련 네트워크 정보를 공유하는 데 있어서 여러 벤더의 NE와 정책 서버 간의 연결, 국한된 관리영역, 다양한 접속 프로토콜이 문제된다. 이로서 PEP와 PDP의 보안정책 객체와 이들 정보간에 접속 프로토콜이 상이하여, 이를 위한 별도의 프로토콜 변환 모듈(프록시)과 여러 인터페이스에 따른 다양한 NE를 접속하기에 한계성이 노출되었다. 한편 네트워크 정보는 객체 지향 기반으로 설계되었지만, 접속 프로토콜과 시스템 운영 소프트웨어는 메시지 기반으로 운용됨에 따라 객체 지향 시스템의 성능을 발휘하지 못하는 실정이다.

TINA-C(Telecommunication Information Network Architecture-Consortium)와 ITU-T TMN에서는 네트워크를 객체화로 모델링하고 있으며, 분산 시스템 환경에서 NE와 운용 관리 시스템 간의 분산 시스템 환경을 제공하여 네트워크 관리를 통합하고 있다. DMTF도 WBEM과 DEN에 대한 보안 관련 정보를 객체화하여 구현 레벨의 표준 규격을 개발하고 있다. 이로서 NE와 관리 시스템 간의 분산 시스템 환경에서 객체화된 네트워크 정보를 공유하는 방향으로 관리되고 있다.

분산 시스템의 미들웨어인 CORBA는 OMG(Object Management Group)에서 제정한 표준화 규격으로 서로 다른 운영체제나 프로그램 언어로 구현된 모듈 간에 상호 간의 운용이 가능하게 하는 일종의 소프트웨어 버스(bus)이다. '96년 CORBA 2.0 규격이 발표되면서 급속히 분산 컴퓨팅을 위한 응용 프로그램의 개발이 용이하여 하드웨어, 운영체제, 프로그램 언어와 무관하게 분산객체 간에 통신이 가능해졌다.



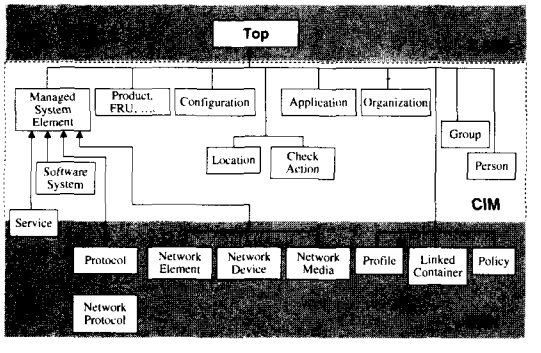
〔그림 10〕 CORBA 기반의 보안정책 관리 시스템

PBNM 시스템도 같은 맥락으로 볼 수 있다. 그림 10과 같이 정책 서버, PMT, PDP, PEP에서 CORBA 환경을 기반으로 객체를 공유할 수 있도록 설계되었다. 특히 Orchestream은 CORBA 2.0

규격을 기반으로 DPE2(Distributed Policy Engine 2)라는 분산 시스템 환경을 자체 개발하여, 이를 정책 서버와 PDP, PEP에 실장 하였다. 기존의 NE인 라우터, 방화벽, IDS, 스위치 등에 직접 실장을 하지 못하는 경우에는 별도의 디바이스 드라이버(프록시)를 두어 DPE2 환경과 연동하도록 하였다.

1.3 DEN 기반의 정보공유

DEN(Directory Enable Network)은 DMTF에서 디렉토리 안에 네트워크 요소 및 서비스를 표시하기 위한 표준 정보모델 개발을 목표로 한다. 따라서 DEN은 디렉토리와 네트워크가 통합되어, 네트워크 구성요소를 쉽게 디렉토리로 파악할 수 있다. 즉 사용자와 서버 혹은 프린터 등의 컴퓨팅 리소스뿐만이 아니라 네트워크 장치, 서비스 및 응용 프로그래밍을 비롯한 IP 주소, QoS(Quality of Service), 보안 등의 정책에 관련된 정보를 디렉토리 구조로서 저장 및 관리할 수 있게 한다. 이로서 디렉토리가 디렉토리 내의 모든 요소 간의 관계에 대한 정보를 수용한다는데 이점이 있다.



〔그림 11〕 DEN 시스템 구성도

'97년 Microsoft와 Cisco에 의해 주장된 DEN에 적용한 LDAP은 X.500 디렉토리 서비스가 너무 방대하며, 복잡하고 구현하기 어려운 면을 해결한 디렉토리 접속 서비스 표준규격을 IETF에서 제정하였다. DEN를 네트워크 자원을 디렉토리 구조로서 LDAP을 이용하여 표현함에 따라 데스크탑 PC에서도 적용이 가능하여 보안정책 정보를 공유할 수 있다. 그러나 DEN으로 적용하기위해서는 네트워크 자원과 정보에 대한 별도의 정보모델이 요구된다.

현재 DMTF에서는 DEN를 위한 보안정책 정보모델을 개발하고 있으며, 디렉토리 서비스를 위한 객체 Class와 관련 Attribute를 별도로 정의한다. 그림 11은 X.500, CIM과 DEN의 정보모델에서 10개의 기본 클래스를 보였다.

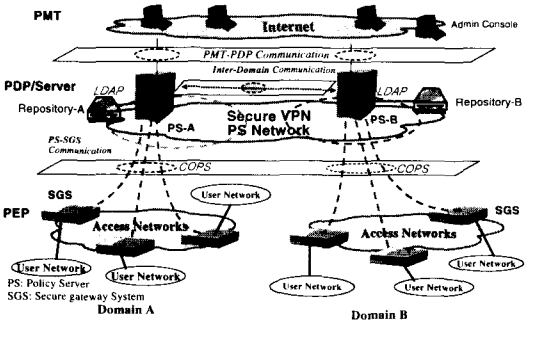
2. 정보공유 구조 및 모델

2.1 정보공유를 위한 구조

정책 기반의 시스템에서 보안정책과 QoS 정책 정보를 공유하는 데 PEP와 PDP, 서로 다른 관리 영역에서의 정책 서버 간의 접속, 중앙집중식 정책 서버 접속으로 구분된다. 또한 관리영역 측면에서는 동일 영역의 PEP와 PDP 레벨, 서로 다른 영역에서의 정책 서버 레벨로 구분된다.

서비스 사업자나 통신사업자 측면에서 동일영역에서는 동일한 분산 시스템 환경이나 PDP 혹은 정책 서버에 접속된 클라이언트 간에 정보공유가 가능하다. 그러나 다른 영역인 경우, 사업자에 따른 보안정책 혹은 QoS 관련 정보를 공유하기 위해서는 기존의 분산처리 환경보다는 라우팅 프로토콜처럼 별도의 프로토콜(IDIP, AN-IDP 등)이나 분산 시스템 게이트웨이 등이 요구된다.

현재 사업자 혹은 상용 시스템 간의 상호 호환성 문제로 PDP와 PEP 간에 접속은 PBNM 소프트웨어 개발회사와 네트워크 구성장치 벤더들 간의 컨소시엄 형태로 해결하고 있으나, 앞으로 이들 간의 정보모델과 접속 프로토콜에 대한 표준화가 조속히 확정되어야 할 것으로 전망된다. 그러나 여러 NE를 적용하는 경우에는 그림 12와 같이 일정 영역에서 정책정보를 수집하여 이를 관장하는 정책 서버와 다른 영역의 정책서버와 정보공유를 위한 간단한 메시지 기반의 프로토콜이 요구된다.



〔그림 12〕 정책 기반의 정보보호 관리 시스템 구조

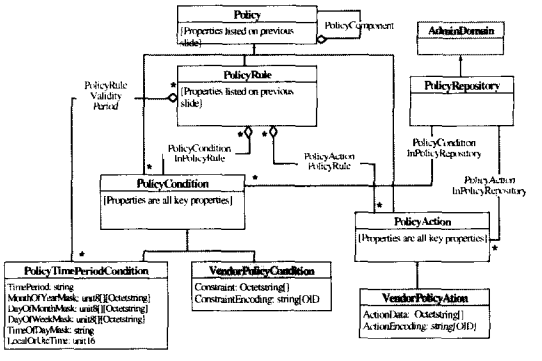
2.2 보안정책 정보모델링

정보보호 시스템에서 보안객체, 보안정책 및 네트워크 정보를 비롯한 정보모델은 종전의 SNMP 프로토콜을 적용한 경우 MIB를 이용함에 따라, ASN.1 혹은 GDMO(Guideline for the Definition of Managed Objects), GRM(General Relationship Model) 방식에 의한 모델을 사용하고 있다. 그러나 객체지향 설계 기술과 분산 시스템의 기술의 발전으로 객체 기반의 정보모델이 OMG, TINA, ITU-T, IETF, DMTF, Paraley 등의 표준화 연구기관에서 정착되었다. 한편 인터넷의 보급으로 데스크 탑 PC에서 웹 브라우저를 이용하여 네트워크를 관리함에 따라, 웹 서버에 네트워크 관리정보가 HTML 형태로 제공되는 것이 보다 편리해지고 있다. 따라서 객체화된 네트워크 관리정보를 웹 브라우저로 표현을 위해 변환 프로토콜이 필요함에 따라 이를 보다 유통성 있게 표현하고자, XML로 모델링하는 연구가 DMTF에서 진행되고 있다. 현재 DMTF의 CIM 정보모델 버전 2.6에서는 796개의 Class와 Properties를 개발 중에 있으며, 그림 13은 보안정책 정보모델을 보이고 있다.

PEP에서 보안 네트워크 관리를 위해서 DMTF 혹은 IETF에서 정의된 정책 정보모델을 구현한 경우, PEP 에이전트는 해당 보안정보를 정책 서버로 전송한다. 현재 보안정책 정보모델을 표준화 기관에서 연구를 수행하고 있지만, 보안정보모델과 관련 접속 프로토콜은 벤더들의 정책 기반 관리 시스템을 비공개로 벤더들 간의 공유한 정보모델과 접속 프로토콜을 사용하고 있다. PEP에 해당되는 라우터, 스위치, 방화벽, IDS 등의 NE들도 일부 PBNM 개발회사와 컨소시엄 혹은 협력지원 그룹으로서 몇 개의 제품만 기능이 수용되도록 개발하여 상용모델을 출시하고 있다.

앞장에서 언급한 바와 같이 현재 보안정책 정보공유를 위한 모델로 WBEM과 DEN 구조는 손쉽게 기존의 NE를 기반으로 수용이 가능하여 활발한 연구와 제품 개발이 이루어지고 있다. 그러나 통신 사업자의 마인드에 따라 분산 시스템 기술의 확산과 객체지향 설계에 따른 NE의 원활한 관리를 위해서는 CORBA와 같은 분산 시스템으로 정보를 공유하는 것이 최종 목표가 될 수 있다. 그러나 당분간 상호 시스템이 혼용되어 사용도록 PEP와 PDP 간은 기존 접속 프로토콜을 제공하는 구조를 보인다. 그러나 Cisco의 Post Office, DARPA의 SLSS (Survivability of Large Scale Systems) 프로젝트인 IDIP(Intruder Detection and Isolation Protocol), FTN(Fault Tolerant Network)의 AN-IDR(Active Network-Intrusion Detection & Response)과 접속도 가능하도록 정책서버의 기능 확장성과 별도의 디바이스 접속을 위해서는 디바이스 프록시 구조 등이 검토되어야 한다.

정책 서버와 관리자용 클라이언트 간에는 웹 기반 혹은 GUI 기반의 응용 소프트웨어로 분산 시스템 환경이나 인터넷을 통하여 접속된다. 그러나 이러한 연결 접속에서 네트워크 관리정보 수집 및 관리를 위해서는 별도의 계층 2에서 L2TP 레벨의 보안 연결과 세션에 대한 IPSec, SSL 등의 보안이 요구된다.



〔그림 13〕 보안정책 정보모델링

V. 결 론

인터넷에서 네트워크 자원과 정보보호를 보다 체계적이고 효율적으로 관리하기 위해서는 네트워크 관리영역(domain)을 지역적으로 구분하여 계층화하며, 일관성 있는 네트워크 운영관리 전략에 근거한 통합적 관리로 정책 기반의 네트워크 관리기술로 발전되고 있다. 이러한 통신환경에서 네트워크 관리정보는 MIB로 정립이 되어 SNMP 관리자에 의해 관리되고 있다. 그러나 정보보호 및 보안정책 기반의 정보모델(PIB)은 IETF와 DMTF 표준화 기관에서 정책 기반의 핵심 정보모델(PCIM)과 확장된 정보모델(PCIM-E)의 표준화 규격을 제정하고 있으며[8], 일부 상용제품에서는 이를 수용하여 출시하고 있다. 그러나 근본적으로 다양한 정보보호 시스템을 수용하는 보안정책의 정보모델의 확장과 이들의 정보공유를 위한 프로토콜, 정책 표현방식 및 정책규칙 기술 언어 등에 신속한 표준화가 요구되고

있다.

현재 정책 기반의 정보보호 시스템은 벤더의 폐쇄적인 제품 개발과 일부 컨소시엄으로 협력하여 일부 NE 간에 호환성을 보이고 있으며, 보안정책에 대한 정보모델은 표준화와 벤더들의 자체 개발된 모델을 실장하여 네트워크에 구축되고 있다. 이는 결국 인터넷 상에서 정보보호를 위해 일사분란하게 시스템 상호간에 호환성 있고, 정보공유가 가능한 네트워크 구성 및 관리에 귀속된다. 보다 개방적 다양한 정보보호 시스템에 수용 가능한 정보모델과 접속 프로토콜을 비롯한 정보보호 관리모델 및 규격 제시로 시스템 간의 적극적인 보안정책 기반의 네트워크 관리가 요구된다.

앞으로 인터넷의 폭발적인 사용 증가와 다방면에 활용됨에 따라 정보보호를 위한 보안정책 등의 정보모델의 표준화와 접속 프로토콜 및 상호 호환성 있는 보안 플랫폼의 API(Application Program Interface) 제정이 필요하다. 또한 네트워크 관리 기능의 FCAPS와 보안관리가 통합적으로 구성할 수 있는 플랫폼 기술이 요구된다.

참 고 문 헌

[1] Dinesh C. Verna, *"Policy-Based Networking: Architecture and Algorithm"*, New Rider, 2001.

[2] Paris Flegkas, Panos Trimintzios, et al., *"A Policy-based Quality of Service Management System for IP DiffServ Networks"*, IEEE Network, March/April 2002.

[3] Theo Dimitrakos, et al., *"Policy-Driven Access Control over a Distributed Firewall Architecture"*, Proceeding of POLICY'02, March 2002.

[4] Morris Slomon and Emil Lupu, *"Security and Management Policy Specification"*, IEEE Network, March/April 2002.

[5] N. Dulay, E. Lupu, M. Slomon and N. Damianou, *"A Policy Deployment Model for Ponder Language"*, Proceeding of DSOM-2001, Oct 2002.

[6] M. Stevens, *"Policy Framework"*, Internet Draft, draft-ietf-policy-framewok-05.txt, September 1999.

[7] B. Moore, et al., *"Policy Core Information Model-Version 1 Specification"*, IETF RFC 3060, Feb 2000.

[8] B. Moore, et al., *"Policy Core Information Model (PCIM) Extensions"*, IETF RFC 3460, Jan 2003.

[9] Thi Mai Trang Nguyen, Nadia Boukhatem, *"COPS-SLS: A Service Level Negotiation Protocol for the Internet"*, IEEE Comm. Magazine, May 2002.

[10] Edgard Jamhour, *"Distributed Security Management Using LDAP Directories"*, Proceeding of INFORCOM'02, 2002.

[11] Andreas Polyrakis and Raouf Boutaba, *"The Meta-Policy Information Base"*, IEEE Network, March/April 2002.

[12] P. Martinez, M. Brunner and J. Quittek, *"Using the Script MIB for Policy-Based Configuration Management"*, Proceeding of INFORCOM'02, 2002.

[13] DMTF Document, *"CIM Core Policy Model"*, Version 2.0, DMTF, May 2000.

[14] 손승원, "Active Security 기술발전 방향", Sigcom Review, Vol 1, No 1, Dec 2000.

[15] 김기영, 장종수, 신영석, "분산시스템 기반의 보안정책 정보공유 기술", 정보통신, 제19권 제8호, 한국통신학회, 2002.

[16] IETF Policy Framework WG, *http://www.ietf.org/html.charters/policy-charter.htm*, 2002.

[17] Orchestream, *http://www.orchestream.com*, 2002.

[18] DMTF, *http://www.dmtf.org*, 2003.

[19] IETF, *http://www.ietf.org/html.charters_/policy- charter.html*, 2002.

[20] Check Point, *http://www.checkpoint.com*, 2002.

[21] Cisco, *http://www.cisco.com/networkers*, 2003.

〈著 者 紹 介〉

신 영 석(SHIN, Young Seok)

1982년 : 전북대학교 공과대학 전자공학과 학사
1984년 : 전북대학교 대학원 전자공학과 석사
1993년 : 전북대학교 대학원 전자공학과 박사
1984년~1998년 2월 : 한국전자통신연구원 선임연구원
1993년~1994년 : 일본 NTT 통신망연구소 객원연구원
1998년 3월~현재 : 호남대학교 정보통신공학부 조교수

장 종 수(JANG, Jong Soo)

1984년 : 경북대학교 공과대학 전자공학과 학사
1986년 : 경북대학교 대학원 전자공학과 석사
2000년 : 충북대학교 대학원 컴퓨터공학과 박사
1989년 7월~현재 : 한국전자통신연구원 책임연구원. 정보보호연구본부 보안게이트웨이연구팀 팀장