정책 기반의 보안 시스템을 위한 보안정책 정보모델링

김도수*, 손선영**, 김진오**신영석*
*호남대학교 정보통신공학과, **ETRI 정보보호연구본부
e-mail: dskim@honam.ac.kr

A Policy-Based Secure Policy Information Modeling for Secure System

Do Soo Kim*, Sun Kyoung Shon**, Jino Kim**, Young Seok Shin*
*Dept of Information & Comm Eng, Honam University
**Information Security Research Division, ETRI

요 약

인터넷 사용의 급증으로 통신망 관리와 정보보호 시스템에 대한 연구 개발이 급속히 이루어지고 있으며, 정보보호를 위한 시스템이 개별적으로 구축하고 있다. 구축된 정보보호 시스템은 사설망과 WAN에서 독립적인 시스템으로 운영관리 되고 있는바, 사설망과 공중망 간의 통합적인 정보보호 관련 정보공유의 부재 및 상호 호환성이 없는 실정으로 사이버 테러와 효율적인 정보보호 관리에 능동적인 대처를 하지 못하고 있다. 본 논문에서는 정책 기반의 방화벽, IDS, 라우터 등의 정보보호 시스템에서 보안정책 정보를 공유하여, 보안 시스템을 손쉽게 제어관리 가능한 보안정책 정보모델을 제시하였으며, UML를 사용하여 보안정책 객체들 간의 접속과 정보공유 모델을 확인하였다.

1. 서 론

인터넷 사용이 급증함에 따라 인터넷 관련 시스템과 기술이 비약적인 발전을 해왔다. 그러나 인터넷 사용만큼 정보보호와 통신망 관리가 다소 소홀한 점이 지적되고 있다. 따라서 통신망을 관리하는 측면에서 통신 사업자의 주요 운영정책(policy)과 동적으로 변화되는 통신망의 상태에 따라 이를 효율적으로 관리하는 방안이 모색된다.

인터넷은 서설망과 WAN이 통합되어 구축되어 운영되는 바, QoS(Quality of Service)와 정보보호 관리기능은 구축 현황에 따라 국한된 영역에서 관련 시스템을 적용하여 운영하고 있다. 정보보호 기술의 적용방법으로 패킷 필터링, 세션 계층의 정보 암호화와 네트워크 계층의 패킷 암호화로 분리하여 운영하고 있다. 트래픽과 서비스 집중을 이용한 해킹으로 전체 통합 통신망을 대상으로 정보보호 관리 기능을 효율적으로 운영하는 데 역부족인 결과를 초래하였다. 이로서 국부적인 지역적 관리의 한계성을 탈피하며, 특정한 정책에 기반을 두어 이를 통신망 전체에 통신망 운영관리 정책을 배포하여 통신망을 관리하는 방식으로 변화되고 있다.[2]

정책 기반의 통신망 관리(PBNM, Policy Based Network Management) 기법은 IETF와 DMTF, Parlay 그룹 등의 표준화 기관을 중심으로 표준화 규격이 활발하게 진행되고 있다[2,3,4,7,11]. 통신망에서 QoS와 정보보호 관리서비스를 정책 기반의 통신망 관리 대상 서비스로 설정하여, Cisco를 비롯한 여러 회사에서 상용제품을 개발하고 있다

본 논문에서는 WAN과 사설망에서 개별화된 정보보호 시스템을 통합하여, 정책 기반으로 효율적인 정보보호 통신망 운영을 위해 보안정책 객체에 대한 정보모델을 제시한다. 초기단계로는 기존의 라우터 및 방화벽 등의 통신망 장치에 정책 기반의 핵심이 되는 보안객체를 모델링하며, 추후 다양한 NE에 적용하도록 모델링 방향을 검토하였다

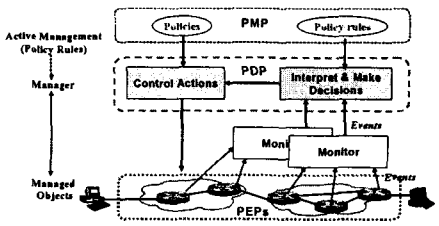
2. 정책 기반의 통신망 관리

2.1 PBNM 시스템

정책 기반의 통신망 관리는 통신망에서 제공하는 QoS, 정보보호 및 자원을 공통된 형태로 제공하며, 이를 효율적으로 관리하는 데 있다. 정책 기반의 관리를 위해서는 (그림 1)과 같이 통신망 구성장치(Network Element, NE)의 MIB 혹은 PIB(Policy Information Base) 을 SNMP, COPS(Common Open Policy Service), LDAP 을 사용하여, NE를 모니터링하여 정책을 관장하는 관리 시스템에 전달한다. 정책관리 시스템은 수집된 정보를 분석하

여 운영자가 내리는 policy rule에 따라 수행하도록 명령을 내리면 된다.

PBNM 시스템은 policy rule을 제정하고, 정책에 따라 통신망을 운영하기 위해서는 통신망 구성장치를 실시간으로 모니터링하여, 동적으로 변화되는 정보를 신속하게 정책 서버에게 전송해야 한다. IETF은 표준화 규격 작성을 위해 (그림 2)와 같은 컴포넌트로 정책관리 도구(PMT, Policy Management Tool), 정책저장장치(Policy Repository), 정책결정장치(PDP, Policy Decision Point, 일명 서버), 정책수행 NE(PEP, Policy Enforcement Point)로 분류한다.



(그림 1) PBNM 네트워크 시스템 구성

2.2 정보보호 시스템 기능 및 표준화 활동

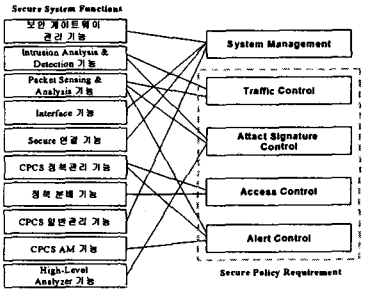
PBNM 시스템은 라우터 및 스위치를 비롯한 인터넷을 구성하는 모든 NE가 대상이 된다. 즉 VPN 시스템, 방화벽, 게이트웨이, IDS, IPSec 시스템, 보안정책 서버, 호스트 등으로 볼 수 있다. 이들은 운용자가 PMT에서 보안정책을 설정하면, 보안정책 서버에 저장된다. 이때 보안정책을 해당 PEP에서 운용되는 PIB로 변환하여 디바이스 레벨의 정보로 저장한다. 각각의 PEP는 해당되는 디바이스 레벨의 보안 정책을 전송 받아 수행한다.

(그림 2)는 정보보호 시스템이 가지는 정보보호 관리 기능을 포괄적으로 나타내었으며, 보안정책 정보모델링을 설계하는 경우, (그림 2)의 관리기능을 충분히 표현 가능한 보안정책 객체로 정보 모델링을 해야 한다. 정보모델링은 PEP와 PDP의 접속 프로토콜에 따라 Schema가 LDAP, XML(HTTP 접속), PCIM 객체(COPS) 형태로 변경되어 적용될 수 있다.

정책 기반 관련 시스템 기능 정립 및 프로토콜에 대한 표준화를 위해 IETF에서는 policy WG을 구성하여 RFC 3060, 3198, 3460을 비롯한 많은 규격을 작성하였으며, 지속적으로 표준화 연구를 수행하고 있다.

DMTF는 정책 기반의 네트워크 관리에 관련된 CIM ver 2.7 표준안을 제시하고 있으며, XML 기반의 xmlCIM을 정의하여, WBEM을 위한 표준안을 작성하고 있다[7]. 한편 상용제품 개발회사에서는 정책 기반의 서버와 운영자 시스템 간의 객체지향 분산 시스템 환경인 OMG CORBA을 구축하여 정책 객체를 공유하는 방안과 자체회사의 GUI 기반으로 제품 개발이 진행되고 있다.

Parlay 그룹은 3GPP, ETSI와 협력하여 기존 통신망에서 제3의 서비스 사업자의 출현을 위해 통신망 관리 서비스 혹은 응용 서비스를 정책 기반으로 관리하도록 정책관리 서비스를 위한 API로서 SCF(Service Capability Feature)을 제시하고 있다[11].

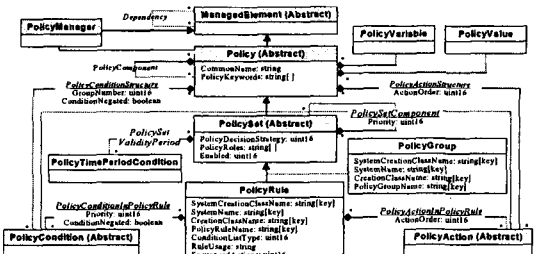


(그림 2) 정보보호 시스템 기능에 따른 주요기능 추출

3. 보안정책 정보모델링

본 연구는 보안객체를 DMTF CIM Ver 2.8 pre와 IETF PCIM/E(RFC 3060, 3460)를 근거하여, 라우터, 방화벽, 스위치, IDS에 적용 가능하도록 보안정책 객체를 모델링 하였다[3,4,7].

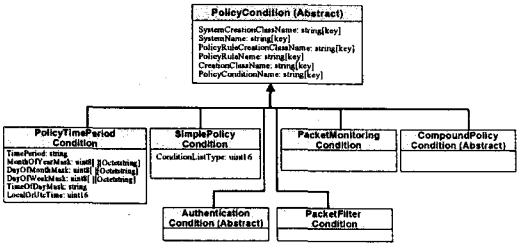
정책 기반의 보안정책(policy) 객체는 policySet을 근간으로 policyCondition, policyAction, policyVariable, policyValue로 구성된다. 그러나 통신망 구성장치를 단순히 운영자가 Rule에 의한 관리보다는 정보보호를 위해서는 통신망에서 운용되는 패킷을 객체로 인식해야 함에 따라 collection과 ManagedSystemElement 객체를 구성하였다. 또한 기존의 Policy Rule 재사용하기 위한 policySet에 PolicyGroup와 PolicyRule를 추가하여(PolicyRule에는 AlertControlRule, AccessControlRule, TrafficControlRule, AttackSignature- Rule로 구성), policy 객체와 dependency를 가지도록 하였다. policyCodition은 policyTimePeriodCondition과 제조회사에서 독자적으로 정의한 vendorPolicyCondition 객체로 상호 의존 관계(dependency)를 가진다. policyRepository는 policySet 객체와 연관되어 정책서버에 객체 정보를 저장한다.



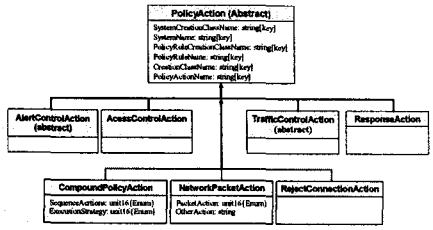
(그림 3) 보안정책 정보모델: PolicySet

보안정책 객체는 독립된 시스템에서 상호간 정보교환이 이루어지며, 이를 위해서 객체 지향 미들웨어가 요구된

다. 따라서 분산 시스템의 미들웨어 환경에서 객체에 대한 생성, 소멸, 접속보안, 관리 등의 기능이 수행된다. 그러나 PMT에서 운영자에 의해 직접 통신망 구성장치의 보안정보객체를 관리해야하는 관계로 별도로 보안정책 객체관리를 위한 policyManager 객체가 요구된다[11].



(그림 4) 보안정책 정보모델: PolicyCodition



(그림 5) 보안정책 정보모델: PolicyAction

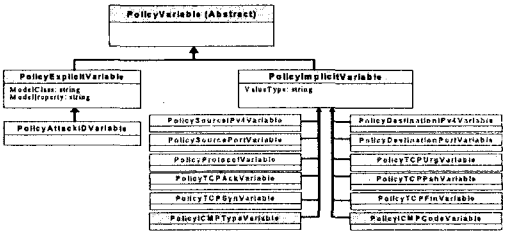
policy rule은 운영자에 의해서 간단한 rule을 비롯하여 rule 속에서 다른 rule을 사용함에 따라(예: {**If** *parent-condition*(PolicyFilter), **then** *parent rule's action*(PolicyAction) **(else) If** *ConA*, **then ActA**; **(else) If** *CondB* **then** *ActB*; **(else) If** *True*, **then** *default Action*}) policyVariable를 (그림 6)과 같이 적용 보안 시스템에 맞게 다양하게 모델화 되어야 한다.

PolicyRule에서 AlertControlRule, AttackSignatureRule, AccessControlRule, TrafficControlRule을 구성하며, PolicyCondition에 PCIM-E의 정보모델인 PolicyTimePeriodCondition, SimplePolicyCondition, CompoundCondition 외에 PacketMonitoringCondition을 두어을 구성하여 각각의 패킷에 따른 조건을 부여하였다. CompoundCondition은 AlertControlCondition, AccessControlCondition, TrafficControlCondition으로 모델링하였다. 또한 PolicyAction에 ResponseAction과 TrafficControlAction(아래에 ExportAction, RateLimitAction), AccessControlAction, AlertControl- Action(아래에 AlertSuppressAction, AlertAggregationAction, AlertIgnoreAction)을 정의하였다.

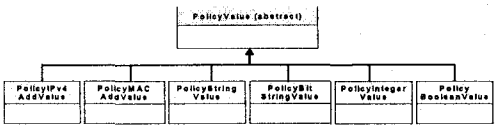
policyVariable은 기존의 보안 시스템에 적용 가능하도록 IPv4 레벨의 IP 주소와 포트번호 등을 정의하였으며, TCP 6 Flags(policyTCPUrg/Ack/Psh/Rst/Syn/FineVariable)와 ICMP의Code 및 Type(policyICMPCode/TypeVariable)를 (그림 5)와 같이 정의하였다.

policyValue 클래스는 policy rule을 표시하는 string, integer 등의 데이터 type을 정의할 수 없는 별도의 특별한 데이터 표현 방식과 값을 객체화 하였다. 즉 MAC과 IP 주소를 비롯한 카운터, 버퍼처리 알고리즘 등을 예로 들 수 있다.

(그림 6)에서 볼 수 있듯이 클래스로는 policyIPv4-AddrValue, policyMACAddrValue, policyStringValue, policyBitStringValue, policyIntegerValue, policyBoolean-Value 등으로 구성된다.



(그림 5) policyVariable 클래스



(그림 6) policyValue 서브클래스

4. 보안정책 관계 객체와 개발환경

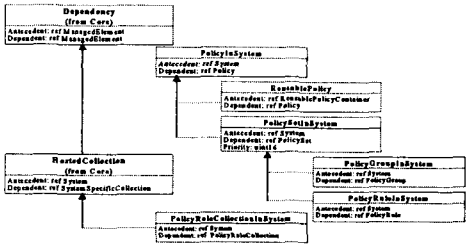
4.1 보안정책 클래스

본 보안정책 정보모델링에서는 DMTF에서 제시한 ManagedElement 클래스에서 ManagedSystemElement 부분을 제외하였다. 따라서 보안정책 객체를 구현하는 데는 DMTF CIM의 ManagedElement 객체를 그대로 수용하도록 함으로서 같은 객체 컴포넌트로 적용하였다. 또한 세부적으로 완벽한 클래스 정의보다는, 클래스를 분류하여 속성을 설정하고, 추후 세부적인 오퍼레이션을 설정하는 방향으로 유도하였다.

Policy 클래스 속성으로는 CommonName: string, PolicyKeywords: string[ ]으로 정의하였으며, policyRule은 CreationClassName: string[key], PolicyRuleName: string[key], Enable: uint16, ConditionListType: uint16, RuleUsage: string, Priority: uint16, Mandatory: boolean, SequencedAction: uint16, ExecutionStrategy: uint16으로 정의하였다.

4.2 연관관계

객체지향 정보모델에서 상호 객체 간에 접속하여 메시지를 전송하는 관계 객체는 dependency, generalization, association, aggregation으로 구분된다. 보안정책 관계객체는 기본적으로 상호 객체 간의 관계를 구현 레벨로 객체로 (그림 8)과 같이 정립하여 객체 간의 상호관계를 객체화하여 모델링 하였다. 이로서 객체 간의 상호 접속에 대한 접속에 따른 관계를 분명히 하였다.

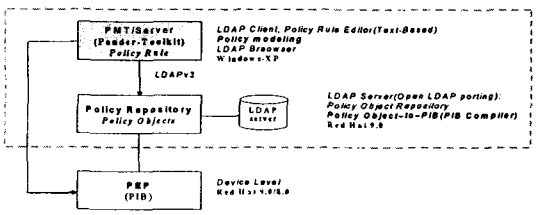


(그림 7) Association 객체

4.3 객체 모델링 환경

보안정책 정보모델링은 DMTF CIM 모델링을 위해 MOF(MicroSoft Object Formatter)를 사용하여 보안정책 객체를 정의하여 DMTF 모델과 대비하였다. 보안정책 객체는 UML 도구인 Rational ROSE를 사용하였으며, 클래스 다이어그램과 협력/시퀀스 다이어그램을 기반으로 설계하였다. 특히 MOF를 활용하여 ManagedElement 객체 컴포넌트 수용과 객체 간의 상속성 유지하였으며, 정의된 클래스에 따른 syntax, 클래스 계위 및 instantiate 등을 확인하였으며, UML을 이용하여 속성과 오퍼레이션, 상호연관 등의 클래스가 정상적으로 정립되었는지를 확인 하였다.

정의된 보안정책 객체를 실제 시스템에 적용 환경으로 Ponder MP(Management Platform) ver 1.4.1을 활용하여, 보안정책(policy rule)에 따른 제시된 보안정책 객체와 연동 기능을 확인하였다. 그러나 Ponder MT가 수행 파일로 제공됨에 따라, 일부 보안정책 모델은 Ponder API을 활용하여 보안정책을 수정하여 정보를 LDAP 서버에 저장하였다[2]. 또한 PEP 기능을 최소한의 라우터 기능으로 에뮬레이션하여 PDP에서 정책 레포지터리 기능을 수행하는 LDAP 서버에서 보안정책을 분배 받도록 하였다. Ponder MT는 Windows NT 환경에서 운용하였으며, LDAPv3 프로토콜은 openLDAP(ver 2.1)을 포팅하였으며, PDP와 PEP는 리눅스 시스템(Red Hat 9.0)으로 본 기능을 수행하였다.



(그림 8) 보안정책 정보모델 검증을 위한 적용 환경

5. 결 론

본 논문에서는 정책 기반의 정보보호 관리 시스템에 적용되는 보안정보 객체에 대한 기능 정립으로 DMTF와 IETF에서 제안하는 객체 모델링 방식을 도입하여, 초기 단계로 보안정책 객체의 핵심 객체를 모델링 하였다. 보안정책객체는 PolicySet를 비롯하여 (그림 3)과 같이 5개 객체(PolicyCondition, PolicyAction, PolicyVariable, PolicyValue)로 구분하였으며, 실제 타켓 시스템의 manageElement는 CIM 컴포넌트를 그대로 수용하였다. policy rule의 다양한 표현을 위해서는 PCIM을 기반으로 policyVariable과 policyValue 객체는 해킹을 모니터링하도록 개별 패킷의 모니터링을 위해 시간 및 로그 정보를 수용하여 IETF와 다르게 정의하였다. 또한 IDS에서 요구하는 패킷을 객체화 하기위한 filterEntryBase 객체를 세부적으로 정의하였다.

앞으로 연구사항은 분산 시스템의 타켓에서 객체간의 상호작용과 수집된 보안정보 객체가 policy rule에 따라 능동적으로 보안정책 객체와 연동되며, 이를 위한 알고리즘 연구가 요구된다(현재 Ponder Toolkit에 제공)[1,5]. 또한 보안정책 객체에서 확장된 객체와 세부 오퍼레이션에 대한 연구가 필요하다.

참고문헌

[1] Morris Sloman, et al. "*Using CIM to Realize Policy validation within the Ponder Framework*", GMC-2003, July 2003.

[2] Emil Lupu, et al. "*Security and Management Policy Specification*", IEEE Network, Vol 16, No 2, March 2002.

[3] B. Moore, et al., "*Policy Core Information Model-Version 1 Specification*", RFC 3060, IETF, Feb 2001.

[4] B. Moore, et al., , "PCIM-Extension", IETF, RFC 3460, Jan 2003.

[5] Nicodemos Damianou, et al., "*Ponder: A Language for Specifying Security and Management Policies for Distributed Systems*", Version 2.3, Imperial College Report DoC 2000/1, Oct 2000.

[6] Y. Snir, "*Policy QoS Information Model*", IETF, *draft-ietf-policy-qos-info-model-04.txt*, Nov 2002

[7] DMTF Document, "*CIM Core Policy Model*", Version 1.1, DMTF, May 2000.

[8] 손승원, "Active Security 기술발전 방향", Sigcom Review, Vol 1, No 1, 2000.12.

[9] 장종수, 김기영, 신영석, "정책 기반의 정보보안 및 QoS 관리기술", 한국통신학회, 정보통신 제18권 9호, 2001.9.

[10] 장종수, 신영석, "정책 기반의 정보보호 시스템 관리 기술", 한국정보보호학회, 제13권 제1호, 2003.2.

[11] The Parlay group, "Policy Management SCF", ETSI ES 202 915-13 Ver 1.1.1, Jan 2003.

[12] openLDAP Foundation, "*open LDAP 2.1 Administrator's Guide*", Jan 2003.