역할기반 접근통제 모델을 이용한 SNMPv3 보안관리기능 설계*

Design of Security Management Function for SNMPv3 using Role-Based Access Control Model

이형효 [1], 이동익 [1], 노봉남 [2]
[1] 광주과학기술원 정보통신공학과, [2] 전남대학교 컴퓨터정보학부
{hlee, dilee}@kjist.ac.kr, bongnam@chonnam.ac.kr

요 약

SNMP 통신망 관리프레임워크를 제시한 SNMPv3는 데이터 인증, 암호기능 및 재사용 방지, 세분화된 접근통제 등 개선된 보안서비스를 제공함으로써, 이전 SNMP 버전에서 제공되지 않았던 안전한 통신망 관리를 위한 기반기술을 제공하고 있다. 그러나, 이와 같은 SNMPv3의 개선된 보안서비스에도 불구하고 통신망에 대한 보안관리정보가 여러 시스템에 분산되어 있는 특성으로 인해 통신망을 운용하는 기관의 일관성있는 보안정책의 기술과 실행에 문제점이 있다. 본 논문에서는 SNMPv3가 제공하지 못하는 보안정책기반의 중앙집중형 보안관리기능과 효과적인 통신망 관리권한 부여를 위한 역할기반 보안관리모델을 제시한다. 제시된 모델은 보안관리자에 의해 기술된 보안관리정책과 통신망 관리자에게 부여된 관리권한을 관리역할에 따라 배정함으로써 효과적인 통신망 관리권한 관리기능과 함께 보안정책기반의 보안관리기능을 수행할 수 있게 한다.

1. 서 론

본래 OSI(Open System Interconnect) CMIP(Common Management Information Protocol)의 개발까지 잠정적인 통신망 관리 프로토콜로 개발되었던 SNMP(Simple Network Management Protocol)는 사용의 편리성과 함께 지속적인 기능향상에 의해, 현재는 단순한 네트워크부터 이종의 네트워크 구성요소들로 이루어진 복잡한 대규모 네트워크 관리까지 통신망 관리의 핵심 프로토콜로서 자리잡아 가고 있다[1,2]. SNMP는 1989년 IETF(Internet Engineering Task Force)에 의해 TCP/IP기반의 인터넷 표준 통신망 관리 프로토콜로 채택된 후, 서브네트워크 단위의 통신망 관리를 위한 RMON(Remote Monitoring) 기능 보완(1991년), 1993년 SNMP 버전 2(SNMPv2) 표준 제정, 1996년 RMON2 정의 등 지속적인 기능의 확장과 보완이 이루어지고 있다[3]. 그리고 1998년 SNMP에 대한 구조 및 문서에 대한 모듈화와 보안기능이 추가된 SNMPv3가 발표되었다[4].

SNMP는 통신망 관리 프로토콜뿐만 아니라, 통신망 구성요소의 기술(description)과 관리정보 스키마 명세를 위한 규칙들(SMI: Structure of Management Information), 그리고 통신망 구성요소들의 관리정보 저장소인 관리정보베이스(MIB: Management Information Base)로 구성된다. SNMP를 이용한 일반적인 통신망 관리시스템은 관리시스템(management system)-관리대상시스템(managed system)으로 이루어진 2 계층 구조를 가지며, SNMP 프로토콜에서 제공되는 프리미티브들을 이용해 통신망에 대한 구성관리(CM: Configuration Management), 장애관리(FM: Fault Management), 성능관리(PM: Performance Management), 보안

* 본 연구는 교육부 두뇌한국 21 정보기술사업단의 지원금에 의한 것입니다.

관리(SM: Security Management), 과금관리(AM: Accounting Management) 기능을 수행한다.

한편, 최근 인터넷을 통한 정보의 불법 감청과 변경, 파괴 등의 보안침해사례와 적법한 사용자에 의한 권한남용이 증가함에 따라 보안의 중요성이 대두되고 있으며, 각 시스템의 취약성 및 보안요구사항이 분석되고 그에 따른 보안기능이 구현되고 있다. 통신망의 경우, 통신망 관리시스템에 의해 관리되는 관리정보 역시 통신망의 정상적인 동작을 위해 관리정보를 안전하게 관리하는 보안기능이 필수적이다. SNMP가 제공하는 보안기능을 살펴보면 초기 SNMP 버전(SNMPv1)에서는 커뮤니티(community) 개념을 이용한 매우 단순한 인증 메커니즘만을 제공하였을 뿐, 정보의 비밀성(privacy)이나 무결성(integrity)을 보장하기 위한 보안서비스는 제공하지 못하였다. 따라서, SNMP의 전반적 기능과 보안기능 보완을 위한 SNMPv2 표준제정 작업이 1993년경부터 진행되었으나, 보안기능에 대한 새로운 표준안 제정에는 실패하였고, 단지 SNMPv1의 커뮤니티 개념에 기반한 SNMPv2C만이 1996년에 발표되었다[1,3]. 그리고, 1998년 SNMP에 대한 전반적인 보안기능이 추가된 SNMPv3가 발표되었다.

본 논문에서는 SNMPv3에 추가된 보안기능과 보안모듈 구성에 대해 살펴보고, 보안관리 측면의 SNMPv3 보안기능의 문제점을 분석한다. 그리고, 통신망 보안의 중앙관리를 위한 보안관리정책의 필요성, 수립된 보안관리정책을 효과적으로 실행하기 위한 역할기반 보안관리모델에 대해 기술한다.

2. SNMPv3 보안모델 구조 및 특성

이 장에서는 통신망 관리 보안위협(threat)과 대응기술에 대해 살펴보고, SNMPv1과 SNMPv2의 커뮤니티 기반 보안기능, 그리고 SNMPv3의 보안모델의 구성과 특징, 문제점에 대해 기술한다.

2.1 통신망 및 통신망 관리시스템 보안

통신망을 대상으로 일반 시스템과 같은 비밀성, 무결성, 가용성(availability)에 대한 보안위협이 가능하며, 특성에 따라 수동적 위협(passive threats)과 능동적 위협(active threats)으로 구분된다. 수동적 위협으로는 전송중인 데이터의 내용을 불법적으로 도청하는 행위(eavesdropping)와 시간대별 통신량과 통신패턴 등을 이용한 통신 트래픽 분석행위(traffic analysis) 등이 있다. 수동적 위협이 데이터의 전송을 차단하거나 전송중인 데이터의 내용을 변화시키지 않는데 비해, 능동적 위협은 데이터의 전송 차단(interruption), 데이터의 변경(modification)과 위조(fabrication) 등 보다 적극적인 보안위협을 포함한다. 이 밖에도 데이터 스트림 순서의 변경, 재사용(replay), 정당한 사용자로의 위장(masquerade) 위협들도 능동적 위협에 포함된다. 수동적 위협은 위협에 대한 탐지는 어려운데 반해 암호기술이나 가짜 데이터 전송을 통해 도청이나 트래픽 분석 공격에 비교적 쉽게 대응할 수 있는 특징이 있다. 그러나, 능동적 위협에 대한 대응은 통신에 참여하는 모든 구성요소에 대한 완전한 보안이 요구되는 어려움이 있다.

그리고, 통신망 관리시스템에 대한 주요 위협으로는 사용자 위장(user masquerade), 통신망 관리자 위장(network manager masquerade), 관리자와 대행자간 방해 위협 등이 있다[5]. 따라서, 다양한 보안위협으로부터 통신망과 통신망 시스템을 보호하기 위하여 보안관련 정보의 안전한 관리, 주요 정보 및 자원에 대한 접근통제(access control), 그리고 암호 알고리즘 지정과 키분배 및 관리 등의 보안서비스가 필수적이다[4].

본 논문에서는 SNMP 환경에서 사용되는 관리자(SNMP 매니저)-대행자(SNMP 에이전트)를 각각 관리시스템과 관리대상시스템으로, 통신망의 관리기능을 수행하는 사용자를 통신망 관리자로 사용한다.

2.2 SNMPv1 보안서비스 특성

SNMP를 이용한 통신망 관리구조는 분산 응용의 한 종류이며, 일반적인 하나의 관리시스템(SNMP 매니저)이 여러 개의 관리대상 시스템(SNMP 에이전트)을 관리하는 구조로 볼 수 있다. 그러나, 위와 같은 통신망 관리구조는 하나의 관리대상 시스템에 여러 관리시스템이 결합된 구조로 간주될 수 있다[6]. 이에 따르면, 각 관리대상 시스템은 지역 MIB의

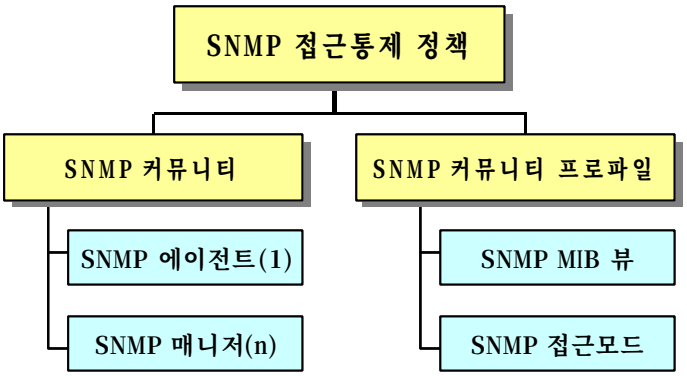


그림 1: SNMPv1 접근통제 정책 구성

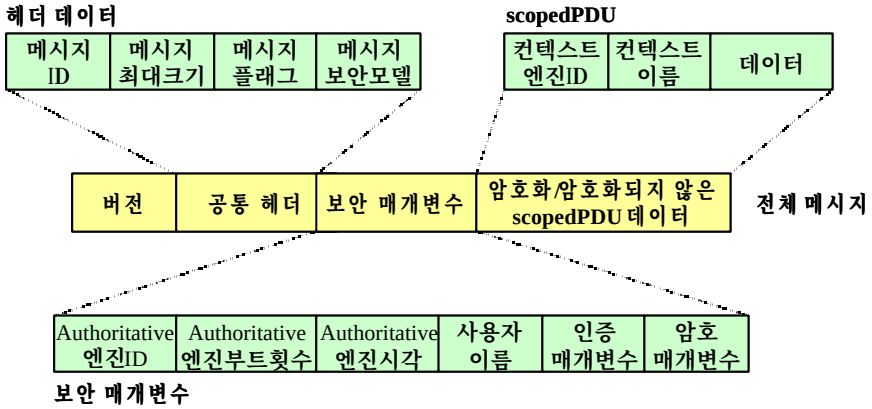


그림 2: SNMPv3 메시지 구조

관리기능 외에 지역 MIB에 접근할 수 있는 관리시스템의 인증 서비스와 관리시스템들에 대해 서로 다른 접근권한 부여하는 접근통제 정책 등을 결정한다.

2.2.1 인증 서비스(authentication service)

SNMP 통신망 관리에서 인증은 관리대상 시스템으로 전달된 메시지가 정당한 관리시스템으로부터 전달된 것인지를 확인하는 서비스이며, 이를 위해 RFC 1157[6]에서는 커뮤니티 이름을 이용한 매우 단순한 인증 서비스를 제시하였다. 이 방식은 관리시스템으로부터 전달된 SNMP 메시지에 포함된 커뮤니티 이름이 관리대상 시스템의 커뮤니티 이름과 동일한 지 판단함으로써 인증기능을 수행한다. 그러나, 이 방법은 보안측면에서 완전하지 못한 특성으로 주로 'GET', 'TRAP' 연산에 대하여 제한적으로 사용되고 있다.

2.2.2 접근통제 정책(access policy)

관리대상 시스템은 커뮤니티를 이용하여 임의의 관리시스템 그룹에 대한 지역 MIB 접근을 제한할 수 있게 되었다. 그리고 하나 이상의 커뮤니티를 지정함으로써, 관리시스템 그룹들과 각 관리시스템 그룹에 속한 관리시스템이 접근할 수 있는 지역 MIB를 지정할 수 있는 접근통제 정책의 기술이 가능하다. 이러한 접근통제 정책의 특성은 MIB에 포함된 관리객체의 집합인 SNMP MIB 뷰(view)와 'READ-ONLY', 'READ-WRITE'로 정의되는 SNMP 접근모드(access mode)에 의해 기술된다. 이때 SNMP MIB 뷰와 SNMP 접근모드를 SNMP 커뮤니티 프로파일(community profile)이라 하며, SNMP 접근모드는 각 커뮤니티마다 지정된다. 정리하면, SNMPv1의 보안특성은 커뮤니티 기반의 인증, MIB 뷰와 그에 대한 접근모드로 구성된 커뮤니티 프로파일과 커뮤니티의 조합으로 기술되는 접근통제 정책이다. SNMPv2 역시 커뮤니티 기반의 SNMPv1과 유사한 보안특성을 제공한다(그림 1).

SNMPv1의 보안서비스는 전송중인 데이터의 비밀성을 해치는 수동적 보안위협이나, 데이터의 내용을 변화시거나 위조하는 등의 능동적 보안위협에 대한 대응기능을 제공하지 못하는 단점을 가진다.

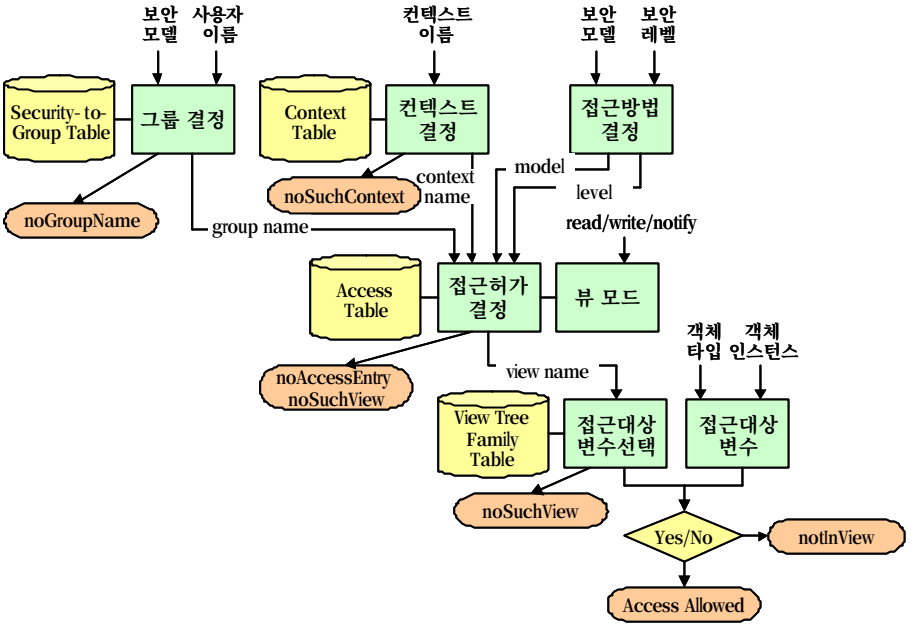


그림 3: VACM 처리 절차

2.3 SNMPv3 보안서비스

SNMPv3 개발의 주요 목적중의 하나는 SNMP를 이용한 통신망 관리의 보안기능을 향상시키는 것으로, 강화된 데이터 출처 인증(data origin authentication), 데이터의 암호화, 데이터 스트림 변경방지, MIB에 대한 접근통제 기능들이 추가되었다. SNMPv3 보안서비스는 비인가된 사용자에 의한 데이터의 변경(무결성 침해), 도청(비밀성 침해), 재사용 공격에 대응하는 기능을 제공하는 사용자기반 보안모델과 인가된 사용자의 MIB 접근을 통제기능을 제공하는 뷰기반 접근통제 모델에 의해 제공된다. SNMPv3 메시지는 보안서비스 등의 매개변수 전송을 위해 설계되었으며, 그 구조는 그림 2와 같다. 메시지의 Authoritative 엔진은 SNMP 명령을 처리하거나 통지(notification)를 발생시키는 SNMP 엔진을 의미하며, 일반적으로 SNMP 에이전트 기능을 수행하는 엔진을 나타낸다.

2.3.1 사용자기반 보안모델

사용자기반 보안모델(USM: User-based Security Model)[10]에서는 데이터 출처 인증, 데이터 암호화,데이터 스트림 변경방지 기능을 위한 보안서비스를 제공한다. 데이터출처 인증을 위해 HMAC-MD5-96이나 HMAC-SHA-96 알고리즘이 사용되고, 데이터 암호화에는 CBC-DES 암호 알고리즘이 이용된다[4,12]. 데이터 스트림 변경방지 기능을 제공하는 timeliness 모듈은 SNMP 엔진 ID(snmpEngineID), 부트횟수(snmpEngineBoots), 엔진시각(snmpEngineTime) 값을 이용한다.

2.3.2 뷰기반 접근통제

뷰기반 접근통제 모델 모델(VACM: View-based Access Control Model)[11] 은 사용자 이름과 보안모델로 구성되는 그룹, 보안 레벨(noAuthNoPriv, authNoPriv, authPriv), 컨텍스트, MIB 뷰, 뷰 모드(read/write/notify)를 입력으로 사용자가 접근하려는 관리정보에 대한 접근통제 기능을 수행한다. 뷰기반 접근통제 수행절차와 각 과정별로 사용되는 테이블은 그림 3과 같다[2]. 관리시스템으로부터 그림 2와 같은 구조를 갖는 SNMPv3 메시지가 전달되면, VACM은 헤더 데이터에 포함된 보안모델과 보안레벨, 보안 매개변수에 저장된 사용자 이름, scopedPDU에 명시된 컨텍스트 이름, PDU(‘GET’, ‘SET’, ‘NOTIFY’) 종류에 따른 뷰 모드, 접근대상 객체에 대한 정보를 추출한 후 접근허용 여부를 결정한다. 이 과정에서 사용되는 테이블들로는 사용자 이름과 보안모델에 의해 그룹을 결정하는

‘vacmSecurityToGroupTable’, 컨텍스트를 관리하는 ‘vacmContextTable’, 그룹, 컨텍스트, 보안모델과 레벨에 의해 뷰 이름을 결정하는 ‘vacmAccessTable’, 그리고 접근대상 객체가 접근이 허용된 MIB 뷰에 포함여부를 나타내는 ‘vacmViewTreeFamilyTable’이 있다.

2.4 SNMPv3 보안특성 분석

사용자기반 보안모델과 뷰기반 접근통제 모델에 기반한 SNMPv3의 보안서비스는 보안서비스를 거의 제공하지 않았던 이전 SNMP 버전에 비해 인증과 암호화를 이용한 매우 강화되고 MIB 뷰기반의 세부화된(fine-grained) 접근통제 기능을 제공하는 특징을 가진다. SNMPv3에서 제공되는 보안서비스 특징을 기술하면 다음과 같다.

- 인증-암호화-접근통제를 이용한 여러 강도의 보안서비스 제공
  SNMP를 이용한 통신망 관리시스템의 사용자가 접근하는 관리정보의 보안 중요도에 따라 인증과 데이터 암호화 여부를 선택할 수 있으며(vacmAccessTable의 vacmAccessSecurity-Level 필드 이용), 보안측면에서 보호가 필요한 관리정보에 ‘READ’, ‘WRITE’, ‘NOTIFY’ 뷰에 대한 접근통제기능을 설정할 수 있다.
- 사용자 그룹기반의 접근통제
  SNMPv3의 사용자기반 보안모듈의 실제 동작은 인증된 사용자가 보안모델 정보와 함께 vacmSecurityToGroupTable을 통해 그룹으로 매핑되어 접근통제가 수행되는 사용자 그룹기반의 접근통제 기능을 제공한다.
- 세분화된 접근통제 명세기능
  SNMPv1의 접근통제 정책이 MIB 트리에서 공통 관리정보(ancestor)를 포함한 MIB 서브트리단위로 접근통제를 명세하는데 비해, SNMPv3에서는 공통 관리정보에 속한 MIB 서브트리에 대해 매스킹(vacmViewTreeFamilyTable의 vacmViewTreeFamilyMask, vacmView-TreeFamilyType 필드 이용)을 통해 세분화된 접근통제 기능을 간략히 기술할 수 있는 장점을 제공한다.

그러나, SNMPv3에서 제공하는 보안서비스는 지금까지 기술된 장점 외에, 보안관리 측면에서 다음과 같은 문제점을 가지고 있다.

2.4.1 인증 및 암호화를 위한 패스워드 관리 문제

SNMPv3 사용자기반 보안모델은 인증과 데이터 암호화 과정에서 관리시스템과 관리대상시스템이 공유하는 인증용 패스워드, 암호용 패스워드로부터 각각 생성된 인증키, 암호키를 사용한다. 이를 위하여, 통신망 관리시스템의 초기화 단계에서 관리시스템과 관리대상시스템에는 동일한 인증용, 암호용 패스워드를 설정하는 과정이 필요하며, 관리기능 수행 중의 인증키 또는 암호키의 변경은 이미 설정된 인증키와 암호키를 이용하여 새로운 값(usmUserTable의 usmUserAuthKey, usmUserPrivKeyChange 필드)으로 ‘SET’ SNMP 연산을 통해 이루어진다.

따라서, 초기화 과정의 인증키, 암호키 설정은 현재의 SNMPv3 표준안에 정의되지 않기 때문에 사용자기반 보안모듈을 구현하는 시스템마다 인증 및 암호화 패스워드 설정이나 관리방식이나 절차가 달라질 수 있는 문제점이 있다. 이 문제점은 관리시스템과 관리대상시스템의 사용되는 인증키, 암호키의 대칭성으로 발생된 것으로, 비대칭형 인증, 암호 알고리즘을 채택함으로써 보완이 가능하나, 본 논문에서는 이 문제에 대한 해결방안은 다루지 않는다.

2.4.2 중앙집중방식의 보안관리기능 부재

SNMPv3 보안서비스의 다른 문제점은 통신망 관리자에 의해 결정된 보안정책을 통신망 관리에 적용하고 관리할 수 있는 중앙집중방식의 보안관리기능이 제공되지 않는 점이다. 예를 들어 그림 4 와 같이 두 개의 관리시스템에 의해 통신망 관리기능이 수행되는 환경을 가정할 때, 관리시스템 A에 의해 관리되는 관리영역 A의 경우, 관리대상시스템 1, 2, 3, 4의 각 지역 MIB에 관리자 A1, A2,

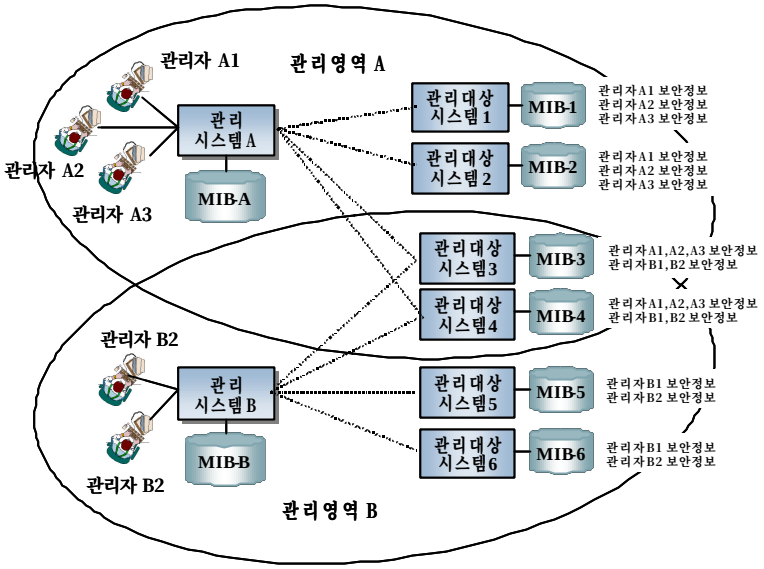


그림 4: 통신망 관리자기반 통신망 관리구조 예

A3의 인증키와 암호키 정보가 저장, 관리되어야 한다. 뷰기반 접근통제모델에서 비록 사용자 그룹이 정의되지만, 사용자기반 보안모델에서 인증과 암호화 과정은 사용자 단위로 이루어지므로 통신망 관리자에 대한 보안정보가 모든 관리대상시스템에 중복, 저장되는 문제점을 가진다. 따라서, 통신망 관리자 정보의 추가, 삭제, 변경 등의 결과가 모든 관리대상시스템의 MIB에 반영되어야 한다.

그리고, 통신망 관리자별 인증키/암호키 정보, 통신망 관리자 그룹, 통신망 관리자 그룹별 접근가능 MIB 뷰 정보 등 통신망통신망 보안관리정보가 관리시스템과 관리정보시스템의 MIB에 분산 저장, 관리되어 통신망에 대한 일관된 보안정책의 명세, 변경된 정책의 반영, 그리고 현재 통신망 보안정보 파악에 대한 중앙집중방식의 보안관리가 불가능한 문제점이 있다. 예를 들어, 관리영역 A와 관리영역 B에 동시에 포함된 관리대상시스템 3, 4의 경우, 통신망 관리자 A, B에 부여된 관리권한에 충돌이 발생할 경우, 통신망 관리의 일관성이나 무결성이 침해될 수 있다.

마지막으로, 통신망 관리자 그룹간 관계(relationship)를 정의하는 기능을 제공하지 않아서 관리대상시스템의 계층적 관리가 불가능한 문제점이 있다. 대규모 기업의 통신망을 고려할 때, 통신망 구성요소가 수행하는 기능의 중요도에 따라 관리대상시스템을 그룹화하고 각 그룹에 대해 관리자 또는 관리자 그룹을 배정할 수 있다. 이런 경우, 일반적으로 중요한 통신망 구성요소 관리기능을

수행할 수 있는 통신망 관리자(상위 통신망 관리자)는 중요도가 낮은 통신망 구성요소를 관리하는 통신망 관리자(하위 통신망 관리자)의 관리권한을 부여받는다. 따라서, 관리자간 또는 관리자 그룹간 계층관계를 표현할 수 있다면, 하위 통신망 관리자의 권한이 상위 통신망 관리자에게 묵시적으로 상속되는 특성을 표현할 수 있게 되어 통신망 관리권한 부여를 단순화할 수 있다.

지금까지 살펴본 SNMPv3의 보안관리기능 문제를 정리하면 다음과 같다.

- 관리대상시스템 MIB에 통신망 관리자 보안정보의 중복 저장
- 통신망 보안관리정보의 중앙집중방식의 관리기능 부족
- 통신망 관리자간, 관리자 그룹간 계층구조 미지원으로 인한 효과적 권한부여 관리의 어려움

이와 같은 보안관리 문제점은 상업환경의 보안모델로서 최근 그 사용이 확대되고 있는 역할기반 접근통제(RBAC: Role-Based Access Control) 모델에 의해 제공되는 보안기능에 의해 해결될 수 있다.

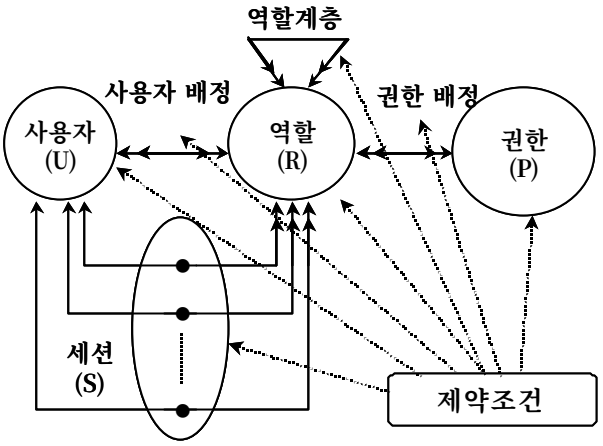


그림 5: RBAC 모델 구성요소

3. 역할기반 보안관리

RBAC 모델은 사용자 대신 역할에 권한을 부여하고 역할간 상속관계를 이용한 효과적 권한부여 관리 특성으로 인해 많은 사용자로 구성된 기업환경에 적용이 확산되고 있다. 지금까지 살펴본 SNMPv3 보안관리기능의 문제점들은 RBAC 모델이 제공하는 보안특성을 이용하여 해결될 수 있다.

이 장에서는 SNMPv3의 보안관리기능 보완을 위해 RBAC 모델의 주요 보안특성을 간략히 살펴보고, RBAC 모델을 이용한 역할기반 보안관리(RSM: Role-Based Security Management) 모델의 구성과 동작에 대하여 기술한다.

3.1 RBAC 모델의 보안특성

RBAC 모델의 가장 큰 특징은 권한을 부여하는 단위가 사용자 대신 사용자가 수행하는 기능에 따라 분류에 역할이라는 점이다[13,14]. 따라서, 사용자는 보호대상 정보나 자원에 대한 접근권한을 얻기 위해서는 해당 접근권한이 배정된 역할의 구성원이 되어야 한다. 권한부여 및 관리 단위가 사용자가 아닌 역할이라는 이 특성은 많은 사용자로 구성된 시스템의 효율적 권한관리를 가능하게 한다. 또한, 역할간 계층구조를 통해 하위 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한상속(permission inheritance) 특징을 제공한다. 권한상속 특성을 이용하여 계층구조를 가진 역할들에 대한 권한부여를 효과적으로 실행할 수 있다(그림 5).

RBAC 모델은 보안 관리자가 관리기능을 통해 모델 구성요소의 구성정보를 변경함으로써 다양한 보안특성을 모델링이 가능하며, 구성요소 관리를 통한 보안특성의 통제가 가능한 특징이 있다.

3.2 역할기반 보안관리 모델

역할기반 보안관리 모델은 다수의 통신망 관리자들의 관리연산 수행에 의해 관리정보의 일관성과 일치성이 침해될 수 있는 SNMPv3 보안서비스를 보완하는 기능을 수행한다. 또한, 다수의 통신망 관리자에 의해 통신망이 운용, 관리되는 환경에서 통신망 전반에 적용되는 일관된 보안정책의 수립과 실행을 가능하게 하는 기능을 제공한다.

3.2.1 구성요소

역할기반 보안관리모델은 보안관리자, 보안관리정책, 보안관리 MIB, 보안관리 MIB 전송 프로그램, 보안관리시스템으로 구성된다.(그림 6)

보안관리정책은 보안관리자에 의해 기술되며, 통신망 관리자와 역할간 배정, 역할간 계층구조, 각 역할이 수행되는 관리시스템 혹은 관리대상시스템, 각 역할에 배정된 'READ', 'WRITE', 'NOTIFY' 뷰 이름 등의 정보를 포함하고 있다. 보안관리정책은 텍스트 형태로 기술되며, 보안관리테이블 변환기에 의해 MIB 테이블로 변환된 후 보안관리 MIB에 저장된다.

보안관리 MIB은 보안관리자에 의해서만

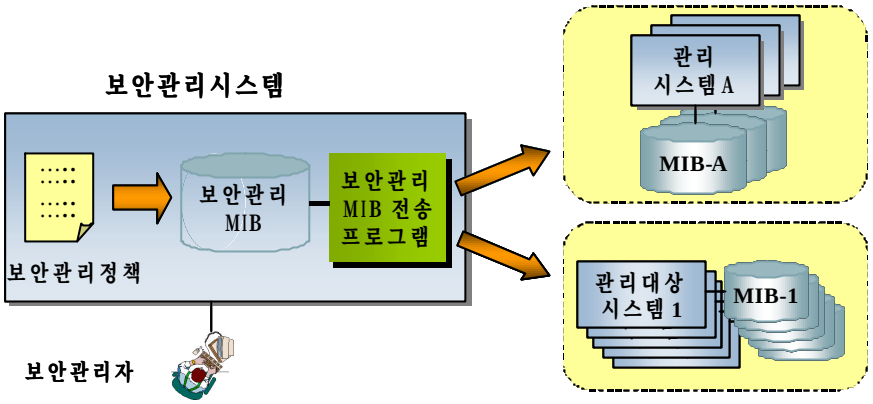


그림 6: 역할기반 보안관리모델 구성요소

접근이 가능하도록 별도의 인증 메커니즘에 의해 보호된다. 보안관리 MIB에는 보안관리 정책에 의해 기술된 관리정책이 관리시스템이나 관리대상시스템에 전송되어 사용될 수 있는 보안관리 MIB 테이블들이 저장된다. 이와 같은 보안관리정책의 기술과 보안관리 MIB 테이블의 생성은 통신망 관리시스템 초기화 과정과 통신망 운용 중 변경된 보안관리정책의 적용과정때 이루어진다. 보안관리 MIB 테이블들은 테이블의 기능에 따라 관리시스템이나 관리대상시스템 MIB로 전송되어 통신망 관리정보에 대한 역할기반 접근통제 실행에 사용된다.

보안관리 MIB 전송 프로그램은 보안관리 MIB 테이블에 따라 해당 관리시스템이나 관리대상시스템으로 전송하는 기능을 수행한다. 보안관리시스템은 관리시스템 중에서 지정되며, 보안관리자의 인증, 보안정책화일의 저장과 관리, 보안관리 MIB의 관리, 보안관리 MIB 테이블의 전송기능을 제공한다.

3.2.2 동작절차

보안관리자는 SNMPv3에 의해 관리되는 통신망의 관리시스템, 관리대상시스템, 통신망 관리자, 통신망 관리자에 부여된 관리권한을 분석한 후 통신망 관리자 역할 과 역할간 계층구조, 역할에 부여될 관리권한, 역할이 수행될 시스템을 결정하여 보안관리정책을 기술한다. 통신망 관리자 역할에 부여되는 관리권한을 통신망 구성요소의 중요도, 통신망 구성요소의 기능적 특징 및 관리부서 등에 의해 배정함으로써 통신망 관리권한의 통제와 관리부하를 경감할 수 있다.

기술된 보안관리정책은 변환기에 의해 보안관리 MIB 테이블로 변환되고, 변환된 보안관리 MIB 테이블들은 보안관리 MIB 전송 프로그램에 의해 관리시스템과 관리대상시스템으로 전송된다. 보안관리 MIB 테이블의 생성과 전송은 통신망 관리시스템의 초기화나 보안관리정책의 변경때 수행된다.

이와 같이 역할기반 보안관리모델은 보안관리자가 통신망 전반에 대한 효과적인 보안관리정책의 기술하고 보안관리정책을 반영한 보안관리 MIB 테이블을 관리시스템과 관리대상시스템에 적용함으로써, 일관된 보안정책의 실행과 중앙집중방식의 보안관리기능을 제공한다.

3.3 보안관리 MIB 테이블

보안관리자에 의해 기술된 보안관리정책은 통신망 관리시스템과 관리대상시스템에 의해 처리되기 위해 그림 7과 같은 관리정보 MIB 테이블들로 변환된 후 보안관리 MIB에 저장, 관리된다.

통신망 관리에 사용되는 역할에 배정된 통신망 관리자 정보는 'rsmUserToRoleTable'에, 역할간 상속관계는 'rsmRoleHierarchyTable'에 각각 저정된다. 그리고, 'rsmRoleAccessTable'은 사용자기반 보안모델의 'usmAccessTable'과 유사하며, 각 역할에 배정된 'READ', 'WRITE', 'NOTIFY' 뷰 이름에 대한 접근통제 정보를 제공한다.

'rsmRoleToEngineTable'은 보안관리시스템에 저장된 역할정보가 통신망 운용관리때 저장되어 사용되는 관리시스템 또는 관리대상

rsmUserToRoleTable

Object	Type	Access
rsmUserName	SnmpAdminString	read-create
rsmRoleName	SnmpAdminString	read-create

rsmRoleHierarchyTable

Object	Type	Access
rsmJuniorRoleName	SnmpAdminString	read-create
rsmSeniorRoleName	SnmpAdminString	read-create

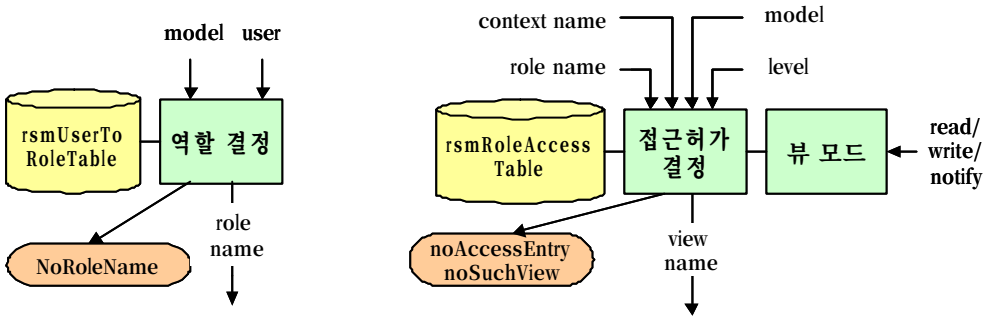
rsmRoleToEngineTable

Object	Type	Access
rsmRoleName	SnmpAdminString	read-create
rsmEngineID	SnmpEngineID	read-create
rsmRoleType	INTEGER	read-create

rsmRoleAccessTable

Object	Type	Access
rsmRoleName	SnmpAdminString	not-accessible
rsmAccessContextPrefix	SnmpAdminString	not-accessible
rsmAccessSecurityModel	SnmpSecurityModel	not-accessible
rsmAccessContextMatch	INTEGER	read-create
rsmAccessReadViewName	SnmpAdminString	read-create
rsmAccessWriteViewName	SnmpAdminString	read-create
rsmAccessNotifyViewName	SnmpAdminString	read-create
rsmAccessStorageType	StorageType	read-create
rsmAccessStatus	RowStatus	read-create

그림 7: 보안관리 MIB 테이블



(a) 관리시스템 변경 (b) 관리대상시스템 변경

그림 8: 역할기반 보안관리모델의 접근통제 절차

시스템 정보를 표현하고 있다. ‘rsmRoleType’ 필드는 해당 역할정보가 저장되는 시스템의 종류(관리시스템, 관리대상시스템)를 구분하며, 관리시스템인 경우 인증된 통신망 관리자의 역할을 결정하기 위해 필요한 ‘rsmUserToRoleTable’ 정보를 전송한다. 그리고, 관리대상시스템인 경우에는 연산을 요청한 역할의 하위역할을 판단하기 위한 ‘rsmRoleHierarchyTable’과 각 역할의 접근권한 정보를 가진 ‘rsmRoleAccessTable’ 정보가 함께 전송된다.

3.4 관리대상시스템의 접근통제 절차

역할기반 보안관리모델을 적용한 통신망 관리시스템에서 역할기반의 접근통제를 실행하기 위해 관리시스템과 관리대상시스템의 수정이 필요하다.

먼저, 관리시스템의 경우 사용자기반 보안모델에서는 인증된 사용자 정보가 관리대상시스템으로 전송되어 뷰기반 접근통제 절차에 사용되었으나, 역할기반 보안관리모듈을 적용한 경우, 사용자 정보대신 역할 정보가 관리대상시스템으로 전송되는 특징이 있다(그림 8의 a).

한편, 관리대상시스템에서의 접근통제 절차는 뷰기반 접근통제 절차(그림 3)와 유사하지만, “접근허가 결정” 과정과 그 때 사용되는 MIB 테이블이 차이가 있다(그림 8의 b).

역할기반 보안관리모델이 적용된 “접근허가 결정” 알고리즘은 그림 9와 같다. 역할기반 접근통제 절차는 뷰기반 접근통제 절차와 매우 유사하며, 뷰기반 접근통제 모델과 같이 접근통제 결정을 위해 보안모델, 보안레벨, 컨텍스트, 연산의 종류와 접근대상 관리정보가 주어진다. 그리고, 접근통제 알고리즘에서 호출되는 ‘IsAccessAllowed’ 함수는 뷰기반 접근통제 모델에서 ‘vacmAccessTable’과 ‘vacmViewTree-FamilyTable’에 기반한 접근통제 함수를 의미한다.

```
Algorithm IsAccessAllowedInRSM
Input

    role: SnmpAdminString
    context: SnmpAdminString
    model: SnmpSecurityModel
    level: SnmpSecurityLevel
    op: ' READ' , ' WRITE' , ' NOTIFY'
    oid: OBJECT IDENTIFIER
Output

    TRUE: access allowed
    FALSE: access denied
Begin

    if (IsAccessAllowed(role, model, level, context, op, oid) == FALSE) then
        role_list ← GetJuniorRoles(role);
        for each role r in role_list do
            if (IsAccessAllowed(r, model, level, context, op, oid) == TRUE) then
                return TRUE;
        done
    else
        return TRUE;
    endif;
    return FALSE;
End
```

그림 9: 역할기반 접근통제 알고리즘

역할기반 접근통제와 뷰기반 접근통제 절차의 차이점은 사용자 이름 대신 역할이 입력으로 주어지며, 입력으로 주어진 역할이 관리정보에 대한 접근권한이 허용되지 않은 경우, 관리대상시스템 MIB에 저장된 'rsmRoleHierarchyTable'을 이용하여 해당 역할의 하위 역할들을 계산(GetJuniorRoles())한 뒤, 각 역할에 대한 접근허가 여부를 점검하는 점이다.

4. 결 론

SNMP 통신망 관리프레임워크를 제시한 SNMPv3는 인증과 데이터 암호기능, 데이터 재사용 방지기능을 제공하는 사용자기반 보안모듈과 사용자그룹 기반의 뷰기반 접근통제 모델을 통해 융통적이며 매우 강화된 보안서비스를 제시함으로써, 이전 SNMP 버전들이 제공하지 못했던 안전한 통신망 관리를 위한 기반기술을 제공하였다. 그러나, 이와 같은 SNMPv3의 개선된 보안서비스에도 불구하고 통신망 보안관리정보가 여러 시스템에 분산되어 있는 특성으로 인해 통신망을 운용하는 기관의 보안정책을 종합적으로 관리하고 통제하는 데 문제점이 있다.

본 논문에서는 SNMPv3가 제공하지 못하는 보안관리기능을 중앙집중방식으로 관리하기 위한 역할기반 보안관리모델을 제시하였다. 제시된 보안관리모델은 보안관리자에 의해 기술된 보안관리정책과 보안관리 MIB 테이블을 보안관리시스템에서 중앙관리하고, 보안관리 MIB 테이블을 관리시스템과 관리대상시스템에 전송하는 구조를 가진다. 또한, 보안관리자는 통신망 관리자들의 수행기능에 따라 역할단위로 분류하고 역할간 계층구조를 통해 보안관리권한을 효과적으로 배정하고 관리하게 된다.

향후 제안된 역할기반 보안관리모델에 대한 보완연구와 함께 보안관리 MIB 테이블들을 관리시스템과 관리대상시스템에 안전하게 전송하는 프로그램 설계 및 구현에 대한 연구가 필요하다.

[참고문헌]

[1] William Stallings, *SNMP, SNMPv2 and RMON, 2nd Ed.*, Addison-Wesley, 1996.

[2] Mani Subramanian, *Network Management: Principles and Practice*, Addison-Wesley, 2000.

[3] RFC1901, Introduction to Community-based SNMPv2. SNMPv2 Working Group, January 1996.

[4] William Stallings, *SNMP, SNMPv2, SNMPv3 and RMON1 and 2*, 3rd Ed., Addison-Wesley, 1999

[5] Warwick Ford, *Computer Communications Security: Principles, Standard Protocols and Techniques*, Prentice-Hall, 1994.

[6] RFC 1157, Simple Network Management Protocol (SNMP), May 1990.

[7] RFC 2571, An Architecture for Describing SNMP Management Frameworks, May, 1999.

[8] RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol(SNMP), May 1999.

[9] RFC 2573, SNMP Applications, April 1999.

[10] RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999.

[11] RFC 2575, View-based Security Model (VACM) for the Simple Network Management Protocol(SNMP), April 1999

[12] William Stallings. *Cryptography and Network Security: Principles and Practice, 2nd Ed.*, Prentice-Hall, 1999.

[13] Ravi S. Sanhdu, Pierangela Samarati, "Access Control: Principle and Practice," *IEEE Computer*, September 1994, pp.40-48.

[14] David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn, "Role-Based Access Control(RBAC): Features and Motivations," *Proceedings of the 11th Annual Computer Security Applications Conferences*, December 1995, pp. 241-248.

이 형 효

1987 전남대학교 전산학과 졸업
1989 KAIST 전산학과 석사
2000 전남대학교 전산학과 박사
1990-1992 삼보컴퓨터 기술연구소
1993-1997 한국통신 연구개발원
1995 정보처리기술사(전자계산조직응용)
2000-현재 광주과학기술원 BK21 정보기술사업단 Post-Doc.
<관심분야> 정보보안, 보안모델, 통신망관리 등

이 동 익

1985 영남대학교 전기공학과 졸업
1989 Osaka Univ. 전자공학과 석사
1993 Osaka Univ. 전자공학과 박사
1990-1995 Osaka Univ. 전자공학과 Research Associate
1993-1994 Univ. of Illinois at Urbana-Champaign Visiting Assistant Professor
1995-현재 광주과학기술원 정보통신공학과 부교수
<관심분야> 에이전트 시스템 및 보안, 비동기회로 설계/CAD, Petri net 이론 등

노 봉 남

1978 전남대학교 수학교육과 졸업
1982 KAIST 전산학과 석사
1994 전북대학교 전산통계학과 박사
1983-현재 전남대학교컴퓨터정보부 부교수
<관심분야> 객체지향시스템, 통신망관리, 정보보안, 멀티미디어와 정보사회