論文
3-3-9

직무기반 보안모델을 이용한 SNMPv3 보안관리 강화 (Enhance Security Management for SNMPv3 using Task-Based Privacy Model)

양 기 철* 오 승 훈** 신 성 권*** 김 민 수**** 권 오 범*****
(Gi-Chul Yang) (Sung-Hun Oh) (Seong-Kwon Shin) (Min-Su Kim) (O-Beom Kwon)

요 약

SNMP 관리 영역이 네트워크에서 시스템, 요금데이터 등 다양한 영역으로 확대되고, 보다 중요한 데이터를 전송하는 수단으로 사용된다. SNMPv3는 사용자그룹기반의 view기반 보안모델을 통한 보안강화 기능을 제공한다. 그러나, view기반보안모델을 이용한 보안관리는 데이터 접근목적에 연관된 접근제어 기능이 없고, 다양한 사용자그룹 생성에 따른 관리의 복잡성이 증대되는 문제가 있다. 따라서, 이러한 관리의 복잡성 문제를 해결하고, 보안강화를 하기 위한 직무기반 보안모델을 통한 접근강화 방법을 제안한다. 제안된 직무기반 보안관리는 관리대상에 따라 네트워크관리자 직무, 시스템 관리자 또는 계정관리자 등의 직무로 구분하여 직무를 통한 접근을 제한하여 관리의 복잡성을 해소하고 , 직무와 목적간 관계를 확인하여 보다 강화된 보안기능을 제공한다.

ABSTRACT

Today, management object using SNMP is not only covered network but also more privacy object like personal or billing data. To enforce security management, view-based access control model is introduced in SNMPv3. However, they are not designed to enforce more privacy object such as purpose and increase complexity of user management. Task-based access control can provide enhanced security service using purpose binding and leverage the complexity of user management using purpose of task.

1. 서론

SNMP (Simple Network Management Protocol)을 이용한 네트워크 관리 환경이 증대되고, 그 활용도 네트워크관리에서 시스템관리, 응용프로그램관리 등 관리 영역이 확대되고 있다. 또한, SNMP를 이용하여 과금 기본데이타를 수집하거나, 네트워크 서비스를 제한하는 기능 등 다양한 영역으로 관리대상을

* 정회원: 동해대학교 정보통신공학과 교수
** 정회원:동해대학교 정보통신공학과 교수
*** 정회원: 동해대학교 정보통신공학과 교수
**** 정회원: 동해대학교 정보통신공학과 교수
***** 정회원: 동해대학교 정보통신공학과 교수
2001년 교내연구과제지원으로 수행된 것임
논문접수 : 2002. 2. 15.
심사완료 : 2002. 3. 9.

넓혀가고 있는 추세에 따라 SNMP 관리의 중요성이 증대되고 있다. 그러나, SNMP에서는 제한적인 보안 기능만 제공함으로 다양한 보안 취약점 및 위협에 노출되어 있는 실정이다. 이에 따라 IETF는 몇 년 동안 보안과 관리 기능을 보완하는 작업이 계속되어 왔다[1,2,3]. 1세대 SNMPv1의 community 기반의 보안기능[4], 2세대 SNMPv2의 party 기반 보안기능을 제공하였고, 3세대인 SNMPv3에서 보안과 관리 부분에 대한 프레임워크가 확정[5]되어 사용자 기반의 보안모델(User-based Security Model: USM)[6]과 view기반의 접근모델(View-based Security Model: VACM)[7]을 기본으로 정의하고, 다양한 보안모델을 적용할 수 있도록 모듈화 된 아키텍처 형태로 보안 서비스를 제공하게 되어 보다 향상된 보안기능을 제공하게 되었다.

본 논문에서는 SNMPv3에서 제공되는 보안기능과 동작에 대해 알아보고, VACM보안모델에서 문제점과 이를 극복하기 위한 직무기반 보안모델을 도입하여 강화된 보안 관리 방안에 대해 기술한다.

2. SNMP 보안 기능

SNMP는 다른 네트워크 프로토콜과 마찬가지로 다양한 보안 위협에 노출되어 있다. 따라서, SNMP 기반으로 중요 데이터를 처리하는 경우 위협은 더욱 증대된다. 본 장에서는 SNMP에서 보안 위협을 살펴보고, SNMP 버전 별로 보안기능을 알아본다.

2.1 SNMP 보안 위협사항

2.1.1 정보의 변조

승인되지 않은 실체가 비 정상적인 방법으로 SNMP메시지를 생성하여 객체에 거짓 값을 전달하는 위협이다. 예로 관리자community이름으로 관리대상정보에 거짓 값을 set함으로 정보의 변조 발생.

2.1.2 가장

권한을 가지고 있는 사용자인 것처럼 속여서 인가되지 않은 조작을 행하는 위협사항으로 권한을 가진 SNMP community를 이용하여 관리대상시스템에 대한 직접적인 조작을 하는 위협.

2.1.3 도청

관리시스템과 관리대상시스템 사이 메시지를 도청하여 필요한 정보를 유출하는 위협으로 관리상 중요 데이터를 획득, 분석하여 정보를 유출하는 위협.

2.1.4 메시지 흐름 변조

SNMP는 UDP기반의 트랜스포트를 사용함으로 기본적으로 메시지에 대한 지연, 재구성, 재현에 의한 메시지 흐름 변조 위협을 가지고 있다. 메시지를 도청하여 이에 대한 전달을 지연하거나, 재구성하거나 또는 새로운 메시지를 재현하여 전달 할 수 있는 위협.

2.1.5 서비스 거부

SNMP 관리자 포트(UDP162)에 대한 광범위한 서비스 거부 공격이다. 관리시스템의 열려있는 포트에 대한 지속적인 데이터 전송을 통하여 해당 관리자가 정상적인 관리대상시스템으로부터 전송되는 데이터를 수신하지 못하여 결과적으로 서비스가 중단되도록 하는 위협.

2.1.6 트래픽 분석

SNMP 트래픽을 분석하여 주요 정보를 획득하는 위협으로 트래픽 분석을 통한 정보는 분석의 정도에 따라 상당한 위협사항으로 존재 가능.

2.2 SNMPv1 보안 기능

SNMPv1에서는 SNMP 실체 간 SNMP 메시지를 SNMPv1 PDU로 Encapsulation하여 전송한다. SNMPv1에서는 하나 이상의 인증 scheme을 통한 인증 개념을 도입하였으나, 최종적으로는 커뮤니티 스트링 (Community String) 기반의 미미한 인증기능과 SNMP MIB view라 불리는 접근제어 방식을 도입했다. 따라서 전달되는 메시지에 대한 암호화나 인증기능이 없으므로 메시지 지연이나 재현등에 대한 보호는 불가능하고 관리대상정보에 대한 단순 인증과 접근제어만 제공한다.

2.2.1 인증서비스

인증된 관리자에게만 제한적으로 MIB (Management Information Base)에 대한 접근을 허용하기 위해 모든 SNMPv1 메시지(get, put request)에 포함된 community 이름을 패스워드와 같은 기능으로 인증서비스를 제공.

2.2.2 접근정책

각 관리자에 따라 다른 접근권한을 제공하기 위하여 MIB 객체의 서브 셋을 구성하여 각 community별로 별도의 MIB view를 제공하는 SNMP MIB view를 제공하고, 각 community별로 {READ-ONLY, READ-WRITE} 셋을 정의하여 SNMP community profile을 구성하여 접근을 제한.

2.3 SNMPv2 보안 기능

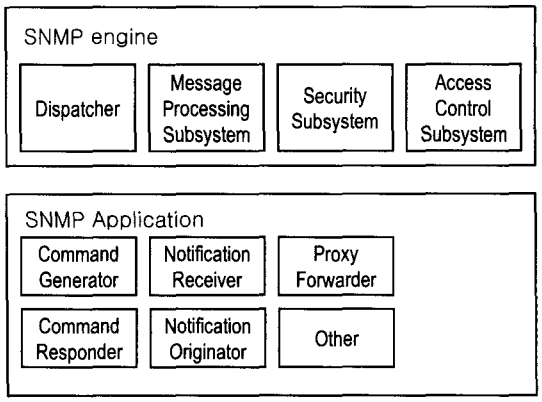
데이터 정의 언어의 튜닝, 확장 64비트 카운터를 이용하고, 관리 프로토콜에서 효율성과 성능향상을 위한 동작 (get-bulk operation), 향상된 에러처리와 이벤트 알림 기능을 추가하였지만 보안과 관리를 표준에 포함되지 않은 관계로 인증, 암호, 접근제어와 원격지 구성관리를 만족하지 못하고 있다.

SNMPv2c [8]는 community기반으로 별도의 보안 기능이 없고, SNMPv2u [9,10]및 SNMPv2*는 보안 기능을 포함하고 있었으나 승인되지 못함.

2.4 SNMPv3 보안 기능

데이터 정의 언어, 관리정보 정의, 관리프로토콜은 기존 SNMPv2와 동일하고 SNMPv3에서는 추가적으로 보안과 관리에 대한 기능이 SNMP관리 프레임워크를 표현하는 아키텍처[11], SNMP 메시지 프로세싱 과 분배 [12], SNMPv3 어플리케이션 [13], 사용자 기반 보안모델, View기반 보안모델이 추가적으로 정의 됨.

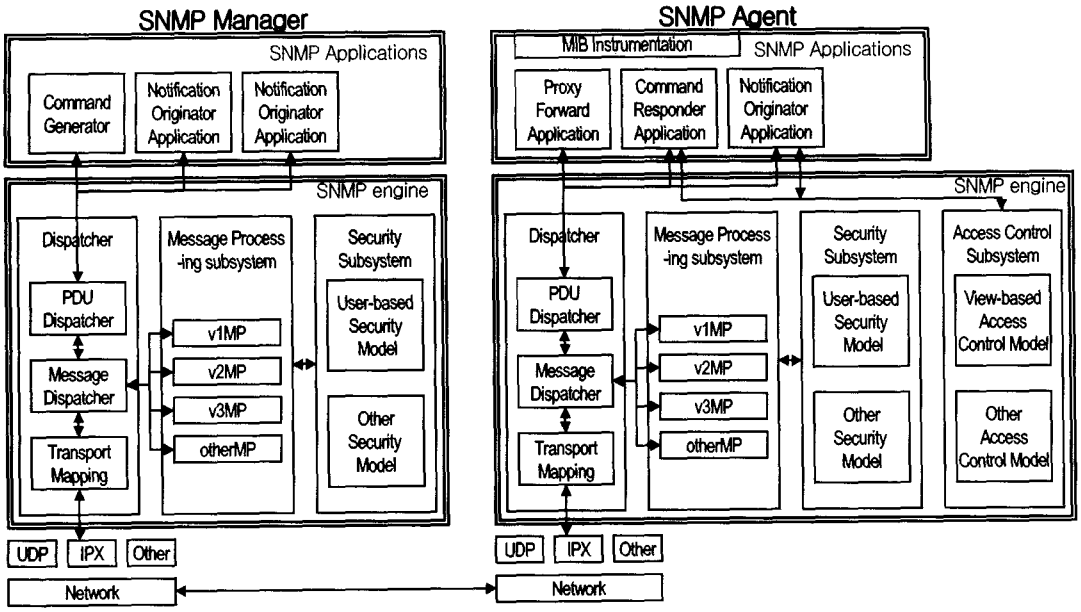
SNMP프레임워크를 표현하는 아키텍처는 [그림 1]과 같은 SNMP 실체를 가짐.



[그림1] SNMP 프레임워크 아키텍처
[Fig.1] SNMP Frame Architecture

SNMPv3 아키텍처의 모듈화 된 구성은 광범위한 운영환경에 적용할 수 있도록 하고, 아키텍처의 일부분만 개선하고 표준화 할 수 있도록 하며, 대체 보안 모델을 적용할 수 있도록 구성됨.

[그림 2]는 정형적인 SNMP 관리자와 에이전트의 블럭다이어그램이다. SNMP 관리자의 보안 서브시스템에서은 모든 전송메시지에 대해 인증과 암호화 기능을 수행한다. SNMP 에이전트에 있는 접근제어 서브시스템은 관리객체를 read하거나 setting 하기 위한 MIB에 대한 접근 권한을 승인하는 기능을 수행한다. 이러한 서비스는 기본적으로 PDU에 포함된 내용에 의해 동작한다. 보안기능은 Security 서브시스템과 Access Control 서브시스템으로 구성되어 독립적으로 구성되어 동작하며 Security 서브시스템은 메 시지 수준에서 암호화 및 인증기능을 제공하며, Access Control 서브시스템은 보안 강화 메커니즘으로 Protocol Data Unit (PDU)수준에서 관리 대상시스템에 대한 접근은 제한하는 기능을 수행한다. 두 개의 보안 시스템을 별도로 구성하여 향후 표준화 작업이 보완작업에 융통성을 제공한다. 현재는 2 가지 보안 서브 시스템인 사용자 기반 보안모델(USM)과 view기반 보안모델(VACM)이 제안되어 있다.



[그림2] SNMP관리자와 관리대상 블럭다이어그램
[Fig.2] Block diagrams for SNMP Manager and Agent

3. 기존 보안모델과 문제점

3.1 사용자 기반 보안모델

사용자 기반 보안모델(USM:User Based Security Model)은 메시지 수준(message level)에서 보안기능을 제공하며 제공하는 보안서비스와 동작절차는 다음과 같다.

3.1.1 데이터 신뢰성과 발신자 확인

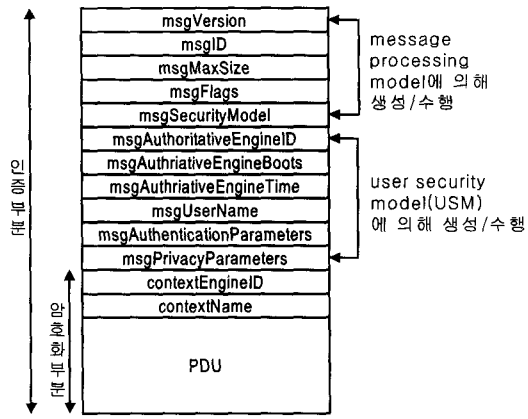
전달메시지에 대한 HMAC-MD5-96 또는 HMAC-SHA-96 해쉬함수를 적용함으로 데이터가 중간에 변조되거나 파괴여부를 확인하고, 데이터의 발신자가 정당한 발신자여부를 확인.[14]

3.1.2 메지시 지연이나 재현 방지

SNMP EngineID가 인식된 이후 리부팅/초기화된 횟수를 기록하는 snmpEngineBoots, snmpEngineBoots 카운터가 마지막으로 증가된 시간부터 경과시간 인 snmpEngineTime, 원격지 엔진으로 부터 수신한 msgAutoritativeEngineTime의 가장 큰 값인 lastReceivedEngineTime 을 비휘발성 메모리에 저장하여 지연된 메시지나 재현된 메시지를 확인 및 방지.

3.1.3 메지지 암호화

전달되는 SNMP 메시지 payload에 대하여 Cipher Block Chaining-Data Encryption Standard (CBC-DES) Symmetric Encryption Protocol 을 이용하여 암호화하여 전송. [그림 3]



[그림3] SNMPv3 메시지 구조
[Fig.3] SNMPv3 Message Structure

3.2 View기반 접근제어 모델

접근제어는 PDU 수준에서 수행되는 보안 기능이며 관리대상에서 구현하는 접근제어 메커니즘이다 [15].

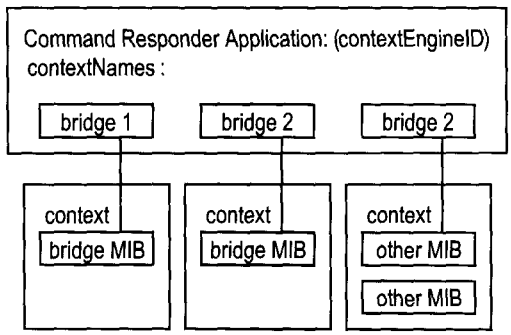
접근제어는 관리자가 관리대상의 로컬MIB에 접근을 허용할 지 여부를 결정하는 메커니즘으로 다양한 접근제어 메커니즘을 이용할 수 있다.[16] SNMPv3에서는 view-based access control (VACM)model을 정의하고 있다. VACM자체가 에이전트를 위한 접근제어정책을 정의한 MIB과 원격 구성할 수 있도록 구성된 MIB 정보를 이용하여 제어.

3.2.1 VACM구성요성

▪ group : SNMP관리객체를 접근할 수 있도록 (securityModel, securityName)으로 구성된다. securityName은 권한자를 의미하며 주어진 내 모든 권한자에 대한 접근권리는 동일하다. 그룹이름은 접근권한을 가지고 있는 관리자들을 분류하고 운용하는데 유용하게 사용.

▪ security level : 요청한 메시지의 보안레벨(예: read-only 또는 write)에 따라 암호화나 인증(noAuthPriv, authNoPriv, authPriv)을 요구할 수 있다.

▪ contexts : 로컬MIB에 있는 객체 인스탄스의 서브셋으로 다른 보안정책을 가지고 있는 객체를 집합시키는데 유용하다. 권한자나 context에 적용된 MIB view에 접근권한을 표현하여 접근을 제어 할 수 있다. 예로 contextName "bridge1"은 context "bridge MIB"을 포함하여 접근을 제어할 수 있다. VACM은 contextName에 의해 로컬에서 가용 한 context 리스트인 vacmContextTable을 정의하여 이용. [그림 4]



[그림4] Context Table 예
[Fig.4] Context Table Sample

▪ MIB view 와 view family

그룹에 대한 관리정보의 서브셋을 접근하도록 정의한다. context에 있는 관리객체타입의 특정한 인스턴스를 MIB view를 통하여 접근하도록 하는 기능이다. 관리객체타입은 트리 형태 네이밍 구조인 ISO의 OID(Object Identifiers)에 의해 구분.

▪ access policy

VACM은 그룹에 대한 접근을 권한자, security level, security model, MIB context, object instanace, type of access(read, write, notify)를 이용하여 결정.

3.2.2 접근제어 수행 절차

접근제어 요구는 SNMP 응용프로그램에 의해 시작되며 6개의 독립된 변수인 securityModel, securityName, contextName, securityLevel, viewType, varableName에 의해 접근제어 여부를 결정한다.

권리 권한자는 securityModel과 securityName의 조합이며 주어진 securityModel에서 권한자를 정의한다. 이 조합은 적어도 SNMPengine내 하나의 그룹에 속하고 vacmSecurityToGroupTable에서 해당되는 securityModel과 securityName에 해당되는 groupName을 제공한다.

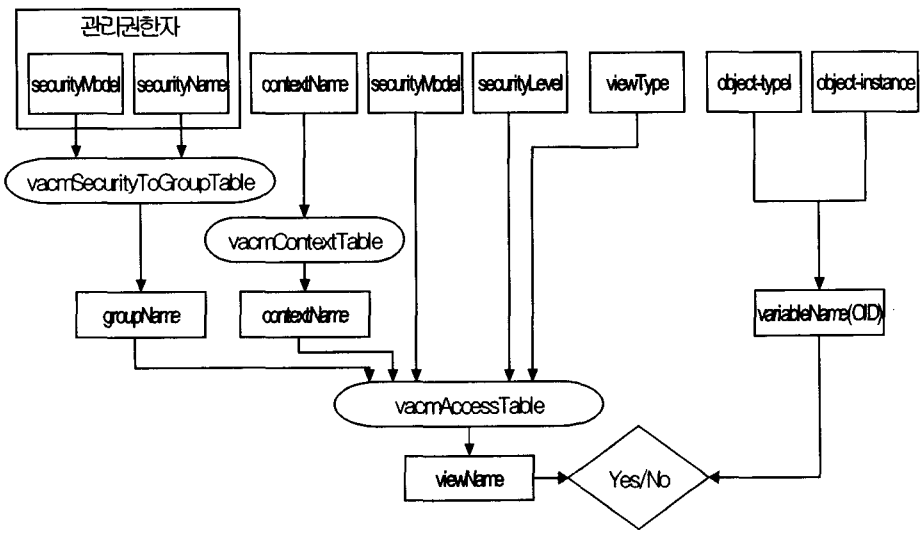
contextName은 관리객체가 있는 장소를 정의한다. vacnContextTable에는 contextName의 list가 존재한다.

securityModel과 securityLevel의 조합은 PDU의 보안 방법에 관한 것을 정의한다.

viewType은 접근 목적이 read, write 또는 notify 인지 정의한다. vacmAccessTable 에 선택된 엔트리는 각 동작 형태에 따라 하나의 MIB viewName을 가지고 있고, viewType은 특정한 viewName을 선택하는데 이용한다. 이 viewName으로 vacmViewTreeFamilyTable로 부터 적절한 MIB view을 선택한다.

variableName은 objectID로써 prefix는 특정 object-type를 구분하고 suffix는 특정객체 인스턴스를 구분한다.

object-instance는 정보의 특정 아이템 요구 시 사용한다. variableName은 retrived된 MIB view와 대응한다. 만약 variableName이 MIB view에 포함된 엘리먼트와 일치한다면 접근은 허용된다. [그림 5]



[그림5] VACM 동작 절차
[Fig.5] VACM Operation Procedure

3.3 기존 보안 모델의 문제점

view기반 보안모델은 사용자그룹에 따른 보안수준과 접근 가능한 mib 정보를 제한한다. 이러한 접근제어 수준은 과거 community 기반의 접근방법보다 보 다 향상된 보안 수준을 유지할 수도 있지만 기본적인 접근 주체는 그룹명에 기반하고 있기 때문에 다음과 같은 보안문제가 발생 할 수 있다.

- 그룹명 가장

높은 보안수준을 가지고 있는 사용자로 가장하거나 나 높은 수준의 사용자 그룹에 속하게 함으로써 필요한 정보를 접근 가능.

- 다양한 사용자 및 그룹 생성 필요

강화(세부화)된 보안정책을 구현하는 도메인에서 다양한 사용자/그룹 생성이 필요하고, 이에 따른 관리 문제가 발생 가능하다. 예로 특정 OID만 한정해서 접근이 필요한 사용자가 증가하면 이에 따라 관리해야 할 사용자명 증가.

- 다양한 viewTree 생성 필요

각 사용자그룹별 view 모드에 따른 view tree를 각각 유지하므로 테이블 관리의 복잡성이 증대.

이외에 관리자가 여러 관리 도메인을 관리하는 경우,

- 관리 도메인에 따른 중복저장

관리자가 다른 도메인에 있는 관리 대상을 접근하기 위해 관리 대상은 접근 테이블을 중복으로 유지해야 할 필요가 있다.

- 중앙집중 관리 방식의 관리 기능 부족

관리자 그룹간 관계가 정의되지 않아 발생하는 보안 침해가 발생 할 가능성이 있다.

여러 관리 도메인을 관리하는 경우 역할기반 접근 모델 이용하여 문제를 해결하려는 연구가 있었다[17]. 본 논문에서는 여러 관리 도메인 환경은 고려하지 않고, 단일 관리 도메인에서 직무(task)기반 접근 모델을 이용하여 상기 언급한 문제를 해결 할 수 있다.

3.4 연구방법

기존 보안모델에서 도출된 문제점을 해결하는 방안으로 직무기반 보안모델을 적용하여 보안을 강화하는 방법을 제안하고, 시뮬레이션을 통하여 제안된 방안의 동작을 확인한다.

4. 직무기반 보안모델

직무기반 보안모델은 데이타를 접근하는 목적 즉, 특정 목적을 가지고 획득한 데이타에 대해서 적절한 절차 없이 다른 목적을 가지고 사용하지 못하도록 하는 (purpose binding)과 데이타 프로세싱 필요성 (necessity of processing)을 가지고 접근을 제한하고 보안을 강화하는 보안모델이다. [18]

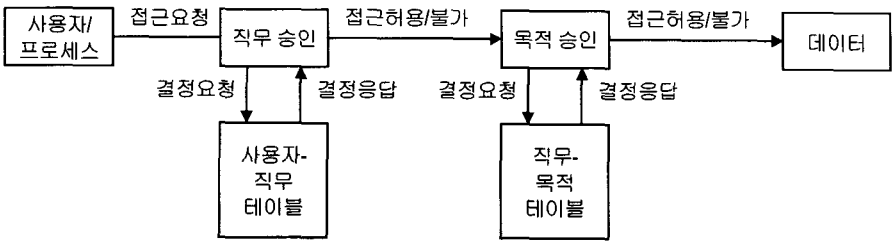
4.1 직무기반 모델 개요

잘 알려진 Bell Lapadula model은 보안 수준 (securitylevel)에 따른 접근만 제어한다. Mandatory Access Control (MAC) 정책은 객체가 가지고 있는 정보의 민감도와 주체에 대한 허가를 기반으로 접근 제어가 실행된다. 그러나, 정보의 민감도에 판단은 주체에 따라 서로 다를 수 있다. 즉, 어떠한 목적으로 사용되는 가에 따라 정보의 민감도는 달라진다.

이러한 이유로 직무 수행목적에 따라 특정 데이터를 접근하려는 사용자의 목적에 일치하는 데이터를 획득하는지 확인이 필요하다.

Discretionary Access Control (DAC)은 주체 또는 그룹의 식별자로 접근을 제한한다. 따라서 데이터에 대한 제어권(control over)을 가질 수 있는 접근권한에 대한 접근권한을 획득하게 되어 데이터가 다른 주체나 그룹에 의해 "owned" 되거나 "controlled by" 될 가능성이 있다. 따라서 접근제어가 사용자나 그룹에 의해 식별되지 않고 각 사용자가 현재 수행하고 있는 직무에 기반 한 접근제어를 할 필요가 있다.

Clark Wilson model이나 Role-based Access Control model은 사용자와 role기반으로 접근을 제한하여 보다 향상된 보안 model을 제시하지만 purpose binding 같이 직접적으로 보안문제를 해결하지는 못한다.



[그림6] 직무기반 보안모델 접근 절차
[Fig.6] Task-based Security Model Procedure

직무기반 보안모델에서 우선 사용자나 프로세스가 수행하는 직무(necessity of processing)에 따른 판단과 직무의 목적(purpose of binding)에 따른 판단을 하여 데이터에 대한 접근을 제어한다. [그림 6]

4.2 직무기반 보안관리 모델

직무 기반 보안관리 모델은 보안 관리 직무를 우선 구분한 후, 이에 따른 관리 주체를 선정하고, 접근하려는 OID에 따른 목적과 부합여부를 확인하여 접근을 제어하는 보안관리 모델이다.

4.2.1 구성요소

직무기반 접근제어를 위한 다음과 같은 구성 요소를 갖고 SNMPv3에서 보안을 강화한다.

- tacmRoleName : 사용자와 보안모델에 따른 역할 관계 테이블로 부터 사용자의 역할을 정의한다. 예로 sysadmin은 시스템관리자 역할로써 rolesysadmin 이라는 tacmRoleName으로 맵핑하고, netadmin은 네트워크 관리자 역할로써 rolenetadmin 이라는 tacmRoleName으로 맵핑.

- tacmTaskName : 주어진 역할(tacmRolename)에 따른 직무(task)를 정의한다. 예로 tcamRoleName이 roleSysAdmin 시스템관련 직무(task)만 수행하도록 정의.

- tacmPurposeName : 접근하는 목적에 따라 해당OID에 대한 접근을 허용하는 역할을 정의한다. 예로 MIB Tress 상에 account 목적으로 접근하려고 하는 경우에는 해당 MIB만 접근 가능하도록 테이블에 맵핑하여 접근을 제한.

- tacmAccessLevel : 해당하는 OID와 인스턴스를 read, write, notify 할 것 인지를 결정.

4.2.2 동작

- 보안관리자는 역할에 따라 사용자를 구분하여 역할을 할당한다. 역할과 사용자가 tacmUserToRoleTable에 있는 경우 tacmRoleName을 바인딩하여 접근을 허용하고, 해당하는 역할이 없거나 사용자가 없는 경우에는 noSuchName 이나 noSuchRoleName 에러 출력을 하고 접근은 거부된다.

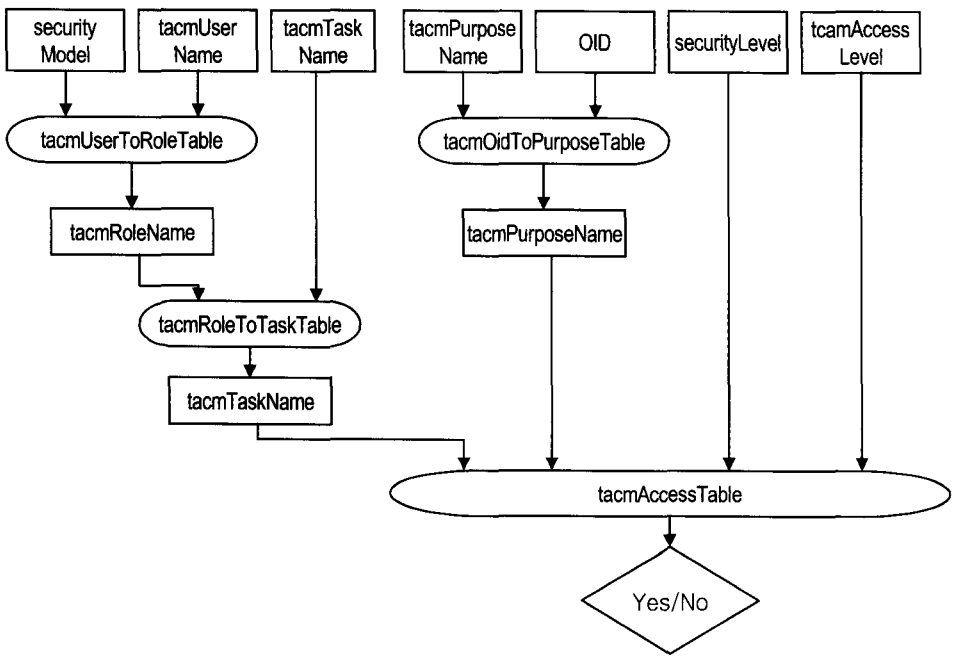
- 역할에 따른 직무 (supervisor, netadmin, sysadmin, system)를 정의한다. 역할이나 직무가 테이블상에 있는 경우 tacmTaskName을 바인딩하여 접근을 허용하고, 역할이나 직무가 없는 경우 noSuchName 이나 noSuchTaskName 에러를 출력하고 접근은 거부된다.

▪ 보안관리자는 해당하는 OID를 접근하는 목적(fault management, account management, performance management, security management, configuration management)을 정의하고, 이러한 목적에 의해 접근되는 MIBtree나 ODI를 정의한다. 해당하는 목적과 OID가 일치하면 접근은 허용되고, 해당하는 목적이나 OID가 tacmPurposeToOIDTable상에 없는 경우 noSuchPurpose, noSuchOID로 에러를 출력하고 접근을 거부한다.

▪ 역할(tacmRoleName), 직무(tacmTaskName), 목적(tacmPurpose)에 대한 접근이 허용된 이후 최종적으로 security level (인증과 암호화)과 접근권한(read, write, notify)이 tacmAccessTable에 존재하면 접근이 허용되고, 존재하지 않으면 에러를 출력하고 접근을 거부한다.[그림 7]

4.3 직무기반 보안모델 MIB 테이블

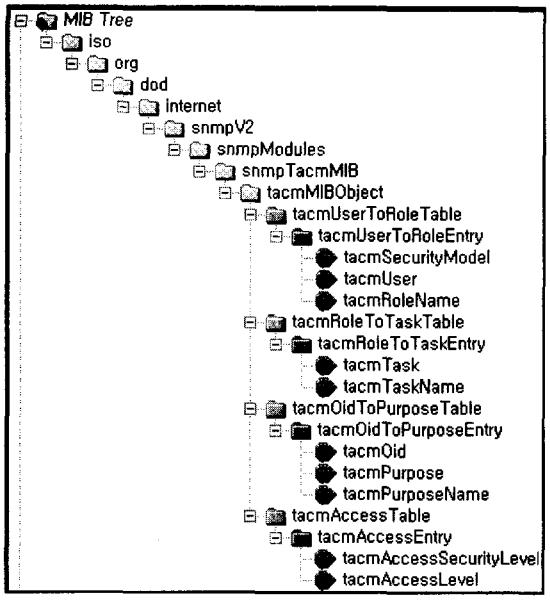
상기와 같은 보안관리 모델은 관리시스템과 관리대상시스템에 MIB 테이블로 구성하여 해당하는 MIB tree에 [표 1]과 같이 구성된다.



[그림7] 직무기반 보안모델 동작 절차
[Fig.7] TACM Operation Procedure

<표 1> TACM MIB Tree 시뮬레이션

<Table 1> TACM MIB Tree Simulation



구성된 MIB Tree 정보는 대상 Agent에 저장되고, Agent에 대한 접근과 보안은 직무기반으로 실행되어 진다.

5. 결론

SNMPv3에서는 기능의 모듈화와 view기반 보안 모델을 적용하여 보다 향상된 보안기능을 제공하고 있다. 그러나 표준화된 보안기능은 다양한 보안요구에 따른 다양한 사용자를 생성하여야 하고, 민감한 데이터처리에 부적합하다. 따라서, 본 논문에서 제안한 직무기반을 이용한 보안관리를 통해 기존에 제공하지 못하던 직무와 목적에 따른 보안 유지 기능을 제공함으로써 관리의 효율성을 증대하고, 민감한 데이터에 대한 접근 복잡도의 증가로 상대적으로 강화된 보안기능을 제공할 수 있다.

향후 제안된 직무기반 보안관리 모델에 대한 보완연구와 다른 보안관리 모델과 연동, 정책 기반 통합 보안 관리 환경에서 타 보안관리 시스템과 연동에 대한 연구가 필요하다.

※ 참고문헌

[1] William Stalling, SNMP, SNMPv2, SNMPv3 and RMON 1 and 2 3rd Edition, Addison Wesley, 1999.

[2] Wiliam Stalling, Network Security Essentials: applications and standards, Prentice Hall, 2000.

[3] David Zeltserman, A Pratical Guide to SNMPv3 and Network Mnagement, Prentice Hall, 1999.

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

[5] RFC 2571, An Archietecture for Describing SNMP Management Frameworks, May, 1999.

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

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

[8] RFC 1901, Introduction to Community-based SNMPv2, SNMPv2 working Group, January 1996.

[9] RFC 1909, An Administrative Infrastructure for SNMPv2, February 1996.

[10] RFC 1010, User-based Security Model for SNMPv2, February 1996.

[11] RFC 2271, An Architecture for Describing SNMP Management, January 1998.

[12] RFC 2272, Message Processing and Dispatching for the Simple Network Management Protocol(SNMP), January 1998.

[13] RFC 2273, SNMPv3 applications, January 1998.

[14] Willam Stallings, Cryptography and network Security: Principles amd Pratice 2nd Edition, Prentice Hall, 1999.

[15] Edward Amoroso, Fundamental of Computer security Technology, Prentice Hall, 1994.

[16] 심갑식, 데이터베이스 보안, 다성출판사, 2001

[17] 이형효, 이동익, 노봉남, "역할기반 접근통제 모델을 이용한 SNMPv3 보안관리기능 설계",KNOM Review, 제3권제2호, 한국통신학회 통신망운용관리회, 2000년 11월, pp28-38.

[18] Simone Fischer-Hubnet, Amon Ott, "From a Formal Privacy Model to its Implementation", National Information Systems Security Conference(NISSC98), 1998.

양 기 철

1985.2 동아대학교 대학원 전자공학과(공학사)
1987.2 동아대학교 대학원 전자공학과(공학석사)
2000.6 동아대학교 대학원 전자공학과(공학박사)
1995.3 - 현재 동해대학교 정보통신공학과 교수

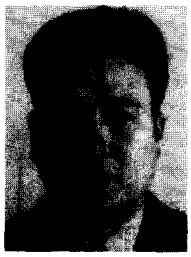
오 승 훈

1989 경일대학교 전기공학과 공학사
1991 영남대학교 대학원 전기공학과 공학석사
1997 영남대학교 대학원 전기공학과 공학박사
1994년 3월-현재 동해대학교 정보통신공학과 교수

신 성 권

1986년 2월 광운대 공과대학 전기공학과 졸 (학사)
1989년 2월 광운대 대학원 전기공학과 졸 (석사)
2000년 2월 광운대 대학원 전기공학과 졸 (박사)
2002년 현재 동해대학교 정보통신공학과 교수

김 민 수



1987.2 한양대학교 대학원 전자공학과(공학사)
1990.2 한양대학교 대학원 전자공학과(공학석사)
2000.2 한양대학교 대학원 전자통신공학과(공학박사 수료)
1990.10 - 2001.2 국방과학연구소 선임연구원
2001. 3 - 현재 동해대학교 정보통신공학과 교수

권 오 범

1983.2 청주대학교 대학원 전자공학과(공학사)
2000.2 서강대학교 대학원 정보통신공학과(공학석사)
1987.3 - 2000.6 (주)대한항공 시스템부 근무
2002.9 - 현재 동해대학교 정보통신공학과 교수