제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

XML을 이용한 SNMP 보안관리 기능 구현

*허용준 *홍충선 *이대영
*경희대학교 전자정보학부
e-mail: hyjeng@empal.com

Providing Security Management for SNMP using XML

*Yong Joon Heo *Choong Seon Hong *Dae Young Lee
*School of Electronics & Information, Kyung Hee University.

요약

현재 널리 사용되고 있는 네트웍 관리 프로토콜인 Simple Network Management Protocol(SNMP)은 시스템이나 네트웍 관리자로 하여금 원격으로 네트웍 장비를 모니터링하고 환경 설정 등의 운영을 하기 위하여 쓰이고 있다. 하지만 SNMP 의 메시지 핸들링 메소드들은 비인가 접근, 서비스 거부, 또는 불안정한 행동을 야기할 만한 취약점들을 갖고 있다. 이에 본 연구에서는 기존의 SNMP 프로토콜에 XML 보안알고리즘을 적용한 안전한 네트웍 관리 프로토콜을 설계하고자 한다.

1.서론

망 관리 표준 프로토콜인 SNMP(Simple Network Management Protocol)[1]는 기본적인 망 관리 용도 뿐만 아니라 원격 관리 구조의 형태를 가진 모든 모델에 적용하여 광범위하게 사용되고 있다. 하지만 IETF에 의해 1989년 제안되었던 SNMPv1 프로토콜은 처음부터 보안을 전제하고 작성된 프로토콜이 아니고, 또한 프로토콜 작성시 전제되었던 가정들은 더 이상 적용될 수 없는 것이 실정이다. 단순히 SNMPv1에서는 Community와 Community Name만을 가지고 인증 (Authentication) 서비스를 제공하였지만 그런 단순한 구조로서는 SNMP 메시지에 대한 보안 문제를 해결할 수 없었다. 따라서 Working 그룹에서는 보안 기능을 추가한 SNMPv2, SNMPv3[2]를 제시하였고 메시지 처리에 있어서 USM (User-based Security Model, SNMPv3)[4]을 제시하여 기본적인 보안 위협 문제는 해결하였지만 비인가 접근, 서비스 거부, 또는 불안정한 행동을 야기할 만한 취약점들을 안고 있다. 이런 취약점은 SNMPv3에서 추가되었던 USM(User-based Security Model)에서 고려하지 못한 부분에 의해 발생하는 것으로 침입자에 의한 서비스 거부와 매니저와 에이전트간의 트래픽 패턴을 침입자가 관찰할 수 있는 문제들에 기인한 것으로 여겨진다. 이에 본 연구에서는 SNMP 자체에서 제공해주는 약한 보안 기능을 개선하기 위해서 XML을 이용한 SNMP의 보안관리 기능을 구현하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 SNMP의 기본 구조와 XML Security Policy에 대해 설명하고, 3장에서 SNMP보안성 향상을 위한 구조를 소개한다. 그리고 마지막으로 4장에서 결론 및 향후 연구 방향을 제시한다.

* 본 연구는 한국과학재단 목적기초연구 (과제번호: R05-2001-000-00976-0)지원으로 수행되었음.

2,SNMPv3와 XML Security Policy의 기본 구조

2.1 SNMPv3 프로토콜에 대한 개요

RFC 2271에서 SNMP 구조에 대한 전반적인 내용을 정의하고 있는데, SNMPv3에서 manager와 agent간의 보

안요소와 이에 대한 구조를 설명하고 있다(그림1참조).

기본적으로 SNMP는 Structure of Management Information(SMI), Management Information Base (MIB), 그리고 프로토콜을 사용하여 네트워크의 요소들을 제어하거나 모니터할 수 있는 기능들을 제공한다.

그리고 SNMPv3의 기본 구조는 분산된 SNMP 엔터티(entity)의 상호작용으로 구현되는데, 각각의 엔터니들은 모듈로서 구현된다. 여기에서 각각의 엔터티들은 단일 SNMP 엔진을 갖고 있으며, 엔진들을 통해서 메시지를 주고 받거나, 메시지를 암호화□복호화□인증을 하며, 관리하려는 대상의 접근을 제어하는 기능을 한다.

각각의 엔터티들이 수행하는 역할들은 다음과 같다.

-Dispatcher : SNMP 엔진에서 버전이 다른 SNMP 메시지들을 유효하게 만들어준다.

-Message Processing Subsystem : 수신한 메시지에서 데이터를 추출하거나 전송할 메시지를 준비한다.

-Security Subsystem : 메시지의 인증, 비밀성과 같은 보안 서비스를 제공한다.

-Access Control Subsystem : 접근권한의 검사를 위해 사용하는 어플리케이션의 인가 서비스를 제공한다.

-Command Generator : SNMP 프로토콜의 Get, GetNext, GetBulk, Set request PUD메시지를 생성하고, 생성된 request메시지에 대한 response과정을 수행한다.

-Command Responder : request 메시지에 대한 response메시지를 생성한다.

-Notification Originator : 특별한 이벤트나 상태를 위해서 시스템을 모니터하고, 이러한 이벤트나 상태를 기초로 한 Trap/Inform 메시지를 생성한다.

-Notification Receiver : Notification 메시지를 기달리고, PDU가 Inform 메시지를 받은 경우 이에 대한 응답 메시지를 생성한다.

-Proxy Forwarder : SNMP 메시지를 전송한다.

SNMPv3 프로토콜은 위와 같은 SNMP 엔터티들을 통해서 메시지 송수신과 이벤트나 상태에 대한 모니터링 기능을 수행하게 된다.

2.2 XML 기반의 보안정책을 이용한 OSS 상호 작용

XML 은 DTD 가 고정되어 있지 않으므로, 다양한 논리적 구조를 표현할 수 있는 유연성을 갖고 있다. 본 절에서는 이러한 XML 의 장점이라 할 수 있는 유연성을 정책기반 보안기법에 접목함으로써, 조 직 간 뗌간의 네트워크 연결에서 보안성을 향상시키는 방안[8]에 대해서 살펴보도록 한다.

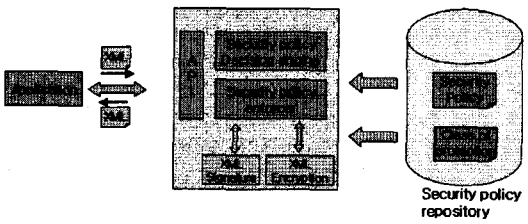


그림 1. XML Security Policy Module 의 기본구조

XML 보안정책의 기본구조는 Security policy decision engine과 Security policy enforcer로 구성되어 있는데, Security policy decision engine은 application으로부터 XML메시지를 받고, 전달받은 메시지의 분석을 바탕으로 security policy repository에 저장되어 있는 보안정책을 적용하게 된다. 그리고 메시지의 보안정책이 repository에 저장되어 있는 정책과 부합하면 보안정책의 CoP name을 뽑아낸다. Security policy enforcer는 XML 메시지와 CoP name을 전달 받고, repository로부터 정의된 CoP를 검색하여 적절한 policy를 적용함으로써 보안과정을 마치게 된다.

이러한 XML Policy based OSS interconnection은 service 공급자와 사용자간에 새로운 서비스 요구에 의하여 고안된 기법으로써, 많은 언어 가운데 XML이 사용된 이유는 XML이 구조화된 데이터를 표현하기에 가장 적합하기 때문으로 중앙 집중적인 관리, 유연성, XML 보안 표준과의 호환성, 적은 개발비용등과 같은 장점들을 가질 수 있다.

3. 제안하는 SNMP 보안구조

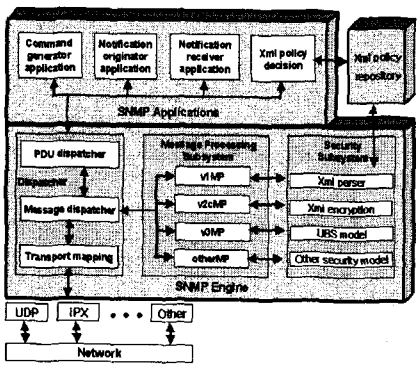
본 논문에서는 기존의 SNMP프로토콜의 보안성 향상을 위해 XML Policy based security를 이용하여 Device 영역과 네트워크 영역의 보안 기능을 강화하고자 한다. 제안하는 구조는 기존 SNMP프로토콜과의 호환성을 위해 기본구조에 XML의 Policy based security를 추가하였다.

본 제안에서 사용하는 entity들의 정의는 다음과 같다.

- XML policy repository : XML security 관련정보를

저장해두는 Policy Database server. XML policy repository의 정보를 통해서 XML policy decision에서 security policy를 결정하게 되고, 이를 받은 Agent의 XML policy enforcer에서 보안작업을 수행하게 된다.

- XML policy decision : XML policy repository에 저장되어 있는 security policy 중, 적용하고자 하는 security policy를 결정하고, 결정한 security policy를 PDU와 함께 Agent로 전달하게 된다.
- XML parser : SNMP PDU를 XML로 변환하는 작업을 수행한다. 여기에서 XML policy decision에서 생성된 PDU는 XML parser에서 XML로 변환할 필요가 없지만 다른 Application에서 생성된 PDU의 변환을 위해 필요한 Entity가 된다.
- XML encryption : Manager에서 XML로 변환한 PDU를 암호화 시키는 작업을 수행한다.
- XML decryption : Agent에서 XML로 암호화된 PDU를 복호화 시키는 작업을 수행한다.
- XML interpreter : Agent에서 Manager로부터 받은 PDU의 XML형식으로 변환된 정보를 다시 SNMP 메시지로 변환하여 Application으로 보내는 작업을 수행한다.
- XML Policy enforcer : Agent의 Application영역에 있는 Entity로서 XML 정책을 수행하고 Manager와 Agent 간의 보안 기능을 마침



(그림1) SNMP Manager

그리고 이러한 entity를 통해, 먼저 Manager에서의 security 기능 수행과정은 다음과 같다.

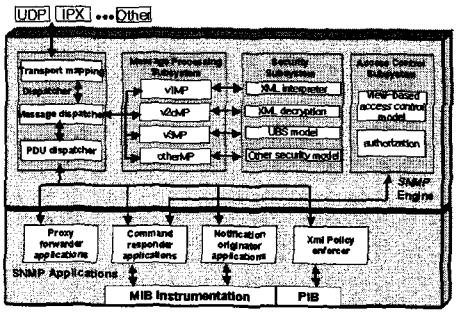
(MS1) application영역의 XML policy decision에서 적용할 보안 정책을 결정하여 dispatcher에게 보낸다.

(MS2) 이를 받은 dispatcher에서는 메시지의 SNMP version을 할당하기 위하여 Message Processing Subsystem으로 보내게 된다.

(MS3) Message Processing Subsystem에서는 보내고자 하는 메시지를 각각의 SNMP버전에 맞게 할당하여 메시지를 처리하고 Security Subsystem으로 메시지를 전달하여 보안기능을 추가한다.

(MS4) Security Subsystem에서는 먼저 PDU의 보안성 강화를 위하여 XML parser에서 XML policy repository에 정의된 정책에 의해 PDU를 XML로 변환하고 XML로 암호화 시킨다.

(MS5) XML로 PDU를 암호화시킨후 보내고자 하는 전체 메시지에 UBS model이나 기존의 SNMP 보안 모델을 적용하여 Manager에서의 보안 기능 수행과정을 마치게 된다.



(그림2) SNMP Agent

이에 대한 Agent에서의 security 기능 수행과정은 다음과 같다.

(AS1) 먼저 Access control subsystem에서 Manager의 인가과정을 수행한다.

(AS2) 인가과정을 마친후 Manager로부터 받은 메시지를 Security Subsystem에서 복호화 시키고, UBS model과 같은 기존의 SNMP 보안 모델을 적용한다.

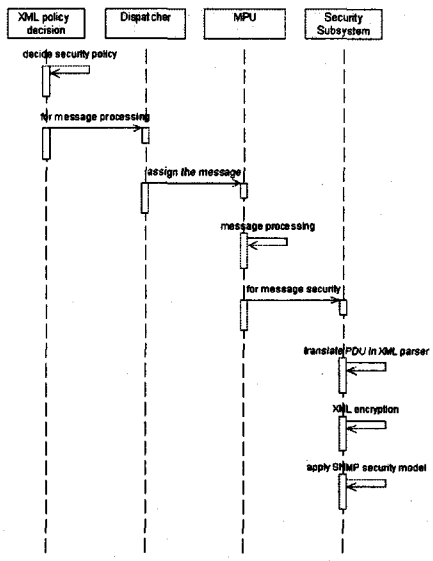
(AS3) 복호화된 전체 메시지에서 XML decryption에서 XML로 암호화된 PDU를 복호화 시킨다.

(AS4) 복호화된 PDU를 XML policy repository에 정의된 정책에 의해 XML interpreter에서 SNMP 메시지로 변환하여 Message processing Subsystem으로 보낸다.

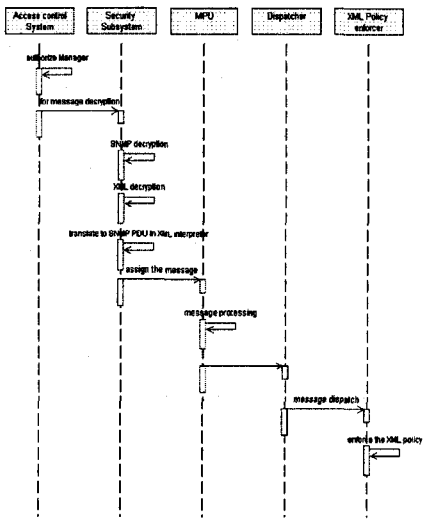
(AS5) Message processing Subsystem에서는 PDU에서 데이터를 뽑아내어 SNMP application에 있는 XML Policy enforcer로 보내게 된다.

(AS6) XML Policy enforcer에서 적합한 보안기능을 수행하게 되고 Agent에서의 보안 기능 수행과정을 마치게 된

다.



(그림3) Manager에서의 security sequence diagram



(그림4) Agent에서의 security sequence diagram

4. 결론 및 향후 연구과제

제안하는 보안구조는 기존의 SNMPv1,2 프로토콜의 취약점이라 할 수 있는 Modification of information, Masquerade(인가되지 않은 엔터티에 의해 Management operation이 수행될 수 있다.), Message stream modification, disclosure(공격자가 Manager와 Agent간에 주고받는 PDU를 분석하여 관리하려는 객체의 값을 알아낼 수 있다.-패스워드를 변경하는 set명령을 분석하여 공격자가 새로운 패스워드를 알아낼 수 있다.)와 같은 기본적인 SNMP 프로토콜의 보안성을 향상 시킬 수 있고, 또한 XML의 장점이라 할 수 있는 새로운 tag의 정의를 통하여 이를 policy based security 기능에 추가함으로써 Denial of service나 Traffic analysis와 같은 보안기능을 향상 시킬 수 있으리라 판단된다.

향후 연구과제로는 제안한 알고리즘의 시뮬레이션 결과를 토대로한 검증이 요구되고, SNMP 프로토콜에 적합한 SNMP MIB에 대한 보안 알고리즘 연구가 기대된다.

참 고 문 헌

[1] RFC 1157 "Simple Network Management Protocol "

[2] William Stallings "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2"

[3] RFC 1902 "Structure of Management Information for Version2 of the Simple Network Management Protocol(SNMPv2)"

[4] RFC 2574"User-based Security Model (USM) for version3 of the Simple Network Management Protocol (SNMPv3)"

[5] http://cert.org/, "CERT Advisory CA-2002- 03 Multiple Vulnerabilities in many Implementations of the SNMP"

[6] Oulu University Secure Programing Group

[7] William Stallings "SNMPv3: A Security ENhan - cement for SNMP"

[8] Kenichi Fukuda. etc."Security Policy Module for XML-based OSS Interconnection"