제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

보안 시스템의 관리를 위한 망 토폴러지 맵 생성기의 설계

안개일, 백광호, 김기영, 장종수
네트워크보안연구부
한국전자통신연구원,
e-mail : {fogone, toobig, kykim, jsjang}@etri.re.kr

Design of Network Topology Map Generator for Management of Security System

Gaeil Ahn, Kwangho Baik, Kiyoung Kim, Jongsoo Jang
Network Security Department
Electronics and Telecommunications Research Institute

요 약

악의 있는 사용자로부터 네트워크와 시스템을 보호하기 위하여 침입 탐지 시스템이나 방화벽 같은 보안 시스템들이 제안되었다. 현재 보안 영역은 사용자 망에서 ISP 망으로 확대되고 있으며, 그에 비례하여 보안 시스템의 관리가 상대적으로 중요해졌다. 또한 보안 시스템에 적용하는 정책도 단순 정적 설정에서 현재의 보안 상황을 반영하여 정책을 재 수립하는 동적 설정으로 바뀌고 있기 때문에, 이를 위하여 관리자에게 망 상태를 주기적으로 보고하는 일도 또한 매우 의미 있는 일이 되었다. 본 논문에서는 SNMP (Simple Network Management Protocol) 프로토콜을 이용하여 보안 시스템의 설치 및 운용을 용이하게 할 수 있는 망 토폴러지 맵 생성기를 설계한다. 제안하는 망 토폴러지 맵 생성기는 탐색할 네트워크 도메인이 주어지면 자동적으로 네트워크 시스템과 보안 시스템을 발견하여 망 토폴러지를 생성하며 또한 망 상태를 주기적으로 수집하는 기능도 제공한다.

1. 서론

인터넷이 실험망에서 상업망으로 발전함에 따라서 보안 문제가 점점 심각한 문제로 대두되고 있다[1]. 이를 위하여 악의 있는 사용자로부터 네트워크와 시스템을 보호할 수 있는 침입 탐지 시스템이나 방화벽 같은 보안 시스템이 제안되었다[2]. 기존의 보안 시스템은 주로 사용자 망에서 설치되어 단독으로 동작했지만, 현재는 ESM (Enterprise Security/System Management)의 형태로 각기 다른 형태의 보안 시스템들이 서로 통합 관리되고 있는 추세이다[3]. 또한 그 보안 관심 영역이 사용자 망에서 ISP (Internet Service Provider) 망으로 확대되고 있으며, 다변화하는 악의 있는 사용자의 공격을 능동적으로 대처하기 위하여 보안 시스템에 적용하는 정책도 단순 정적 설정에서 현재의 보안 상황을 반영하여 정책을 재 수립하는 동적 설정으로 바뀌고 있다.

이처럼 관리해야 할 보안 영역이 확대되면 그에 비례하여 보안 관리 시스템의 관리가 매우 중요해 지며, 또한 보안 정책의 동적 설정을 위해서는 현재 보안 상태에 대한 정보 수집이 상대적으로 중요해 진다.

본 논문에서는 SNMP (Simple Network Management Protocol)[4]을 이용하여 보안 시스템의 설치 및 운용을 용이하게 할 수 있는 망 토폴러지 맵 생성기를 설계한다. 제안하는 망 토폴러지 맵 생성기는 탐색할 네트워크 도메인이 주어지면 자동적으로 네트워크 시스템과 보안 시스템을 발견하여 망 토폴러지를 생성하며 또한 망 상태를 주기적으로 수집하여 사용자에게 제공하는 기능을 제공한다.

본 논문의 구성은 다음과 같다. 먼저, 2 장에서는 망 토폴러지 맵 생성기에서 네트워크 시스템 및 보안 시스템의 발견 및 정보 획득을 위하여 사용되는 SNMP 프로토콜에 대하여 간단히 소개한다. 3 장에서는 망 토

폴러지 생성을 위하여 표준 MIB (Management Information Base) 정보를 분석하고 망 토폴러지 맵 생성기에서 제공하는 정보 및 구조를 자세히 설명한다. 마지막으로 4 장에서 결론을 맺는다.

2. SNMP 프로토콜 개요

ISO (International Standardization Organization)에서는 망 관리 (즉, 구성관리, 장애관리,성능관리, 보안관리, 계정관리)를 위해서 CMIP(Common Management Information Protocol)이란 프로토콜을 제안하였다. TCP/IP 환경에서는 그 CMIP 에 기반된 CMOT (CMip Over Tcp/Ip)와 SNMP (Simple Network Management Protocol) 그리고 특수 도구(예, ifconfig, ping, netstat, 등)로 망을 관리한다. 이중 SNMP 와 특수 도구가 가장 보편적으로 사용되고 있다.

SNMP 프로토콜은 전송 장비와 단말 장치들을 관리하기 위한 메니저와 에이전트간 프로토콜로써 UDP, IP, CLNS(OSI Connectionless Network Service), DDP (AppleTalk Datagram-Delivery Protocol), IPX (Novell Internet Packet Exchange) 상에서 실행된다. SNMP 프로토콜에서 관리 정보들은 트리 형태로 구성되며 MIB (Management Information Base) 객체로 불린다. 각 MIB 객체들마다 OID (Object Identifier)가 할당되어 유일하게 식별 된다. MIB 는 ASN.1 (Abstract Syntax Notation One) 표현 방식을 사용하여 SMI (Structure of Management Information)에 근거하여 기술된다. SMI 는 MIB 객체들을 기술하는데 필요한 규칙을 정의하고 있다.

SNMP 는 크게 세 개의 버전을 가지고 있다. 1988 년에 버전 1 이 제안되었고, 1993 년에 버전 2, 그리고 1997 년에 버전 3 이 마지막으로 제안되었다[5].

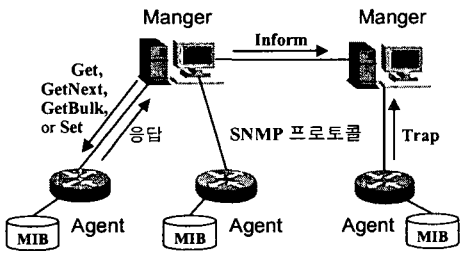

그림 1 SNMP 오퍼레이션

SNMP 버전 1 에서 정의된 오퍼레이션은 다음과 같다. (그림 1 참조)

- Get : 메니저가 관리되는 장치의 특정 MIB 정보를 검색할 때 사용되는 오퍼레이션
- GetNext : 메니저가 관리되는 장치의 특정 MIB 정보의 다음 MIB 정보를 검색할 때 사용되며, 이것은 메니저가 관리되는 장치의 모든 정보를 얻고 싶을 때 주로 사용되는 오퍼레이션
- Set : 메니저가 관리되는 장치를 구성하거나 제어하기 위하여 필요한 값을 설정할 때 사용되는 오퍼레이션
- Trap : 관리되는 장치가 어떠한 문제를 갖고 있을 때 메니저에게 알려주기 위하여 사용되는 오퍼레이션

SNMP 버전 2 는 버전 1 의 오퍼레이션을 포함하며 다음과 같은 추가적인 오퍼레이션을 정의하고 있다. (그림 1 참조)

- get-bulk : 확장된 Get 오퍼레이션으로서 메니저가 관리되는 장치의 여러 정보를 한번의 오퍼레이션으로 한꺼번에 얻고 싶을 때 사용되는 오퍼레이션
- Inform : 메니저가 다른 메니저에게 정보를 보내고 싶을 때 사용하는 오퍼레이션
- Improved Set: 테이블의 엔트리를 생성하거나 삭제할 수 있는 기능이 추가됨

SNMP 버전 3 는 다음과 같은 보안 기능이 추가 되었다.

- 인증(Authentication) 및 메시지 암호화 : 데이터 무결성과 발신자 인증을 제공하기 위하여 MD5 또는 SHA-1 과 함께 메시지 인증 코드인 HMAC 을 지원한다. 또한 CBC(Cipher Block Chaining)을 이용한 메시지 페이로드의 암호화도 지원한다.
- 접근 제어 (Access Control) : 메니저가 에이전트에 접근하여 해당 오퍼레이션을 실행할 자격과 권한이 있는지 확인하는 기능 지원

3. 망 토폴러지 맵 생성기 설계

3.1. 요구 분석

본 논문에서는 그림 2 에서 도시된 것과 같은 망 토폴러지에서 망 토폴러지 맵과 네트워크 트래픽 상태 정보 그리고 노드 구성 정보 등을 제공하기 위하여 SNMP MIB 정보를 이용 한다.

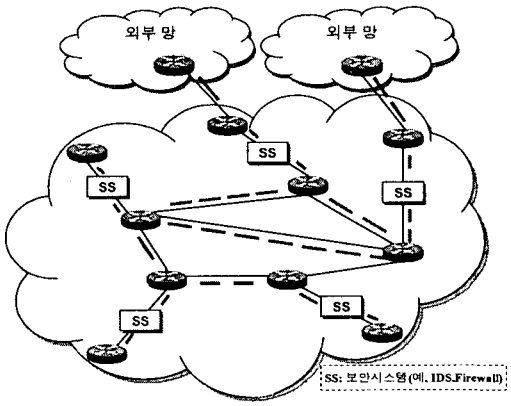

그림 2 망 토폴러지 예

SNMP 프로토콜을 선택한 이유는 거의 모든 네트워크 시스템이 SNMP 프로토콜을 지원하고 있으며,

또한 MIB 를 통하여 인터페이스 정보, 라우팅 정보, 그리고 구성 정보 등을 모두 제공하기 때문이다.

그림 2 와 같은 망 토폴러지를 자동 생성하기 위해 요구되는 사용자 입력 정보는 다음과 같다.

- 네트워크 도메인 주소 : 내부 망 및 외부망의 주소
- SNMP MIB 객체 식별자: 네트워크 시스템과 보안 시스템 탐색을 위해 시스템을 식별할 수 있는 MIB 객체 식별자
- 시스템 탐색 주기 시간
- 트래픽 정보 수집 주기 시간

또한 사용자가 입력한 정보를 바탕으로 망 토폴러지 맵과 망 상태 정보를 제공하기 위하여 망 토폴러지 맵 생성기가 생성해야 할 정보는 다음과 같다.

- 노드 정보 : 탐색된 시스템의 IP 주소
- 링크 정보 : 탐색된 시스템간의 링크 정보 (예, 인터페이스 타입, 링크 대역폭 등)
- 트래픽 정보: 트래픽의 수신 속도(bps)와 트래픽의 발신 속도(bps)

노드와 링크 그리고 트래픽 정보는 다음과 같은 SNMP MIB 정보를 이용함으로써 얻을 수 있다.

- 시스템 정보 : MIB 의 mib-2.system 에서 정의되어 있음
- 시스템 주소 정보 : MIB 의 mib-2.ip.ipAddrTable. ipAddrEntry 에서 정의되어 있음
- 인터페이스 정보 : MIB 의 mib-2.interfaces.ifTable. ifEntry 에서 정의되어 있음
- 라우팅 정보 : MIB 의 mib-2.ip.ipRouteTable. ipRouteEntry 에서 정의되어 있음

3.2. 망 토폴러지 맵 생성기 설계

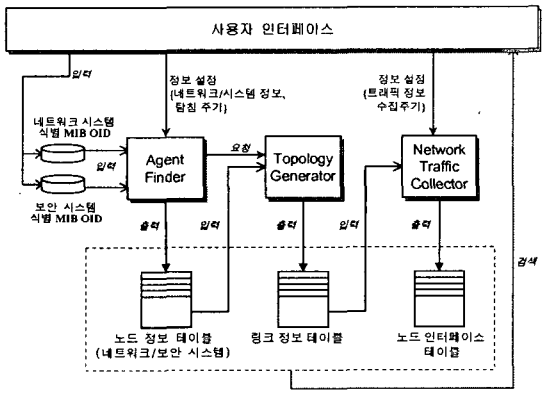

그림 3 망 토폴러지 맵 생성기의 구조

망 토폴러지 맵 생성기의 구조는 그림 3 에 도시되어 있다. 사용자는 네트워크 시스템을 식별하는 MIB 객체 식별자와 보안 시스템을 식별하는 MIB 객체 식별자 (즉, 보안 시스템을 위하여 새로 확장된 MIB 객체)를 등록한다. 또한 탐색할 네트워크 도메인과 탐색 주기 시간 그리고 트래픽 정보 수집 주기 등도 등록 한다.

본 논문에서 제안하는 망 토폴러지 맵 생성기는 네 개의 모듈로 구성되어 있다. 그 모듈들의 기능은 다음과 같다.

먼저, Agent-Finder 모듈은 주어진 네트워크 도메인에서 네트워크 시스템 및 보안 시스템의 자동 발견하는 것을 목적으로 하며, 사용자로부터 탐색할 네트워크 도메인 주소를 입력받아 네트워크 시스템 및 보안 시스템의 노드 정보 테이블을 출력한다. Topology-Generator 모듈은 네트워크 토폴러지 맵을 생성하는 것을 목적으로 하며, Agent-Finder 모듈이 생성한 노드 정보 테이블을 입력 받아 링크 정보 테이블을 출력한다. Network-Traffic-Collector 모듈은 네트워크 트래픽 상태를 주기적으로 수집하는 것을 목적으로 하며 Topology-Generator 모듈이 생성한 링크 정보 테이블을 입력 받아 노드 인터페이스 테이블을 생성한다. 마지막으로 MIB-Query 모듈은 네트워크 시스템 및 보안 시스템의 구성 정보를 제공하는 것을 목적으로 하며, 사용자로부터 노드의 주소와 MIB 객체 색별자를 입력 받으면 검색 후 MIB 정보를 응답한다.

Agent-Finder 모듈이 생성하는 노드 정보 테이블은 표 1 과 같이 구성된다.

표 1 노드 정보 테이블

필드 명	필드 타입	설명
address	String	노드 주소
location	Enumerate	노드 위치(내부망 또는 외부망)
type	Enumerate	노드 유형 (네트워크 시스템 또는 보안 시스템)

Topology-Generator 모듈이 생성하는 링크 정보 테이블은 표 2 와 같이 구성된다.

표 2 링크 정보 테이블

필드 명	필드 타입	설명
agentAddr_1	String	SNMP 에이전트 주소
ifAddr_1	String	인터페이스 주소
ifIndex_1	Integer	인터페이스 인덱스
agentAddr_2	String	SNMP 에이전트 주소
ifAddr_2	String	인터페이스 주소
ifIndex_2	Integer	인터페이스 인덱스

표 3 노드 인터페이스 테이블

필드 명	필드 타입	설명
agentAddr	String	SNMP 에이전트 주소
ifAddr	String	인터페이스 주소
ifIndex	Integer	인터페이스 인덱스
ifType	String	인터페이스 타입
ifSpeed	Integer	인터페이스 대역폭
inOctets	Integer	수신된 옥텍 수
avgInRate	Integer	평균 수신 속도(bps)
outOctets	Integer	발신된 옥텍 수
avgOutRate	Integer	평균 발신 속도(bps)

Network-Traffic-Collector 모듈이 생성하는 링크 정보 테이블은 표 3 과 같이 구성된다.

Topology-Generator 모듈이 하여 링크 정보 테이블을 생성하기 위하여 사용하는 알고리즘은 다음과 같다.

1) 노드 정보 테이블을 이용하여 노드 주소 정보를 수집한다. 즉, [노드 주소, 인터페이스 주소, 인터페이스 인덱스]로 구성된 임시 테이블인 노드 주소 정보 테이블을 만든다.
2) 노드 주소 정보 테이블에 새로운 노드의 주소를 추가할 시에, 그 노드의 주소가 이미 노드 주소 정보 테이블에 등록되어 있으면 중복된 주소이므로 등록하지 않는다.
3) 노드 주소 정보 테이블을 이용하여 라우트 정보를 수집한다. 즉, [노드 주소, 인터페이스 인덱스, 다음 노드의 주소]로 구성된 임시 테이블인 라우트 정보 테이블을 만든다.
4) 라우트 정보 테이블에 새로운 라우트 정보를 추가할 시에 그 정보에 의미 없는 주소 (예: 127.0.0.1, 0.0.0.0)를 포함하고 있으면 등록하지 않는다.
5) 두 임시 테이블 (즉, 노드 주소 정보 테이블과 라우트 정보 테이블)을 이용하여 링크 정보 테이블을 생성한다.

3.3. 현재 구현 상태

현재 토폴러지 맵 생성기를 구현하고 있다. 그림 4 는 토폴리지 맵 생성기의 구동 설정을 위한 사용자의 정보 입력 창이다.

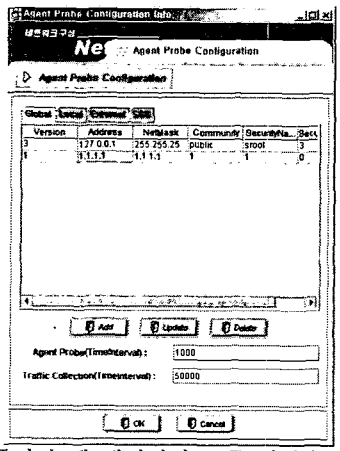

그림 4 토폴러지 맵 생성기의 구동 설정을 위한 사용자의 정보 입력 창

실제 구현에서는 네트워크 도메인을 로컬망, 공중망, 그리고 외부망으로 더 세분화 하였다. 그리고 보안 시스템은 본 저자의 연구팀에서 개발중인 SGS (Security Gateway System) 시스템만을 고려하였지만, 다른 보안 시스템도 쉽게 추가할 수 있다. SGS 시스템은 침입 탐지 및 대응을 지원하는 시스템으로서 독자적인 확장된 MIB 을 가지고 있다. 현재, 사용자 인터페이스는 Java 언어을 사용하여 프로그래밍하고 있으며, 데이터베이스는 Oracle 을 사용하고 있다. SNMP 프로그래밍을 위하여 카네기 멜론 대학과 캘리포니아 대학에서 만든 NET-SNMP 패키지[6]를 이용하였다. 이것은 이전에 UCD-SNMP 로 널리 알려졌으며 SNMP 응용을 개발하기 위해 필요한 SNMP 라이브러리와 MIB 확장에 필요한 툴들을 지원한다. 현재 버전 1,2,3 모두를 지원하고 있다.

4. 결론 및 향후 연구 과제

본 논문에서는 SNMP (Simple Network Management Protocol)을 이용하여 보안 시스템의 설치 및 운용을 용이하게 할 수 있는 망 토폴러지 맵 생성기를 설계하였다. 제안하는 망 토폴러지 맵 생성기는 탐색할 네트워크 도메인이 주어지면 자동적으로 네트워크 시스템과 보안 시스템을 발견하여 망 토폴러지를 생성하며 또한 망 상태를 주기적으로 수집하여 사용자에게 제공하는 기능을 제공한다.

본 논문에서 제안하는 망 토폴러지 맵 생성기를 이용함으로써 관리자는 네트워크 토폴러지가 어떻게 구성되어 있는지를 그리고 보안 시스템들이 어디에 위치하는지를 한눈에 쉽게 파악할 수 있으며, 또한 망 토폴러지 맵 생성기에서 제공되는 망 상태 정보를 이용함으로써 새로운 보안 시스템들을 어디에 위치 시킬지를 결정하는데 도움을 줄 수 있다.

향후 연구 과제는 SNMP 프로토콜을 사용하여 보안 시스템의 정책을 설정하는 일이다.

5. 참고 문헌

[1] Marchany, R.C. and Tront, J.G., "E-commerce security issues," Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), January 2001, pp. 2492 -2500

[2] Herve Debar, Mare Dacier, and Andreas Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks 31, 1999, 805-822

[3] Check Point, "OPSEC Framework," http://www.checkpoint.com/opsec/architect.htm.

[4] J. Case,M. Fedor,M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)", RFC 1157, May 1990

[5] William Stallings, "SNMPv3: A Security Enhancement for SNMP," IEEE Communications Surveys, Fourth Quarter 1998, Vol. 1 No. 1

[6] The Carnegie Mellon University and University of California, "NET-SNMP Tutorial," http://net-snmp.sourceforge.net/index.html