보안 라우터와 보안 관리 시스템과의 경보 전달 인터페이스 설계 및 구현

이호균°, 김정녀
한국전자통신연구원 보안운영체제연구팀
{hglee°, jnkim, }@etri.re.kr

Design and Implementation of the Alert Transport Interface between Secure Router and Management System

Ho Gyun Lee°, Jeong Nyeo Kim
ETRI Secure OS Research Team

요 약

본 논문에서는 가까운 미래에 시장에서 요구하게 될 여러 보안 장비 형상 중에서 라우터 장비 자체 내에 침입 탐지, 서비스 거부 공격 대응, VPN 서비스 등과 같은 보안 기능을 구현하는 프로젝트의 일부로 보안 라우터와 보안 관리 장비 간 경보 전달 인터페이스의 설계 및 구현 과정을 보이고 있다.

1. 서론

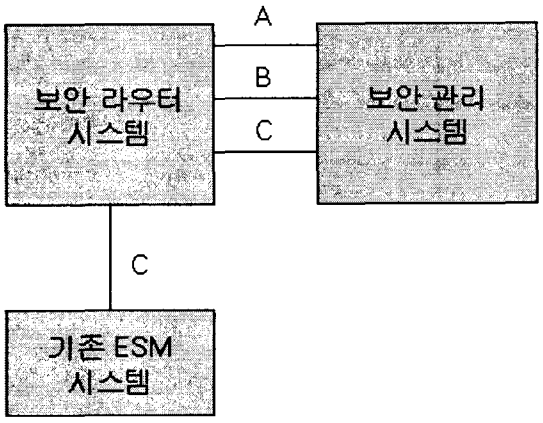
2003년 1월25일과 1988년11월2일은 컴퓨터 보안 특히 네트워크 보안 담당자들에게는 매우 의미가 깊은 날이다. 전자는 대한민국에서 전문가 뿐 만이 아니라 일반인들까지도 서비스 거부 공격 (DoS)이 무엇이고 어떤 파괴력을 가진 것인지 인식하게 되는 계기가 된 날이다. 후자는 DoS 공격의 원조 격인 인터넷 웜이 미국에서 처음으로 네트워크에서 확산, 실제 피해를 입힌 날이다. 이것이 계기가 되서 정부 기관과 학계를 중심으로 인터넷 정보전에 대한 연구가 시작되었다. 서비스 거부 공격이란 컴퓨터가 정상적인 작업을 처리하기 위해서 필요한 여러 가지 자원들, 즉 네트워크 대역폭이나 TCP/IP 스택 처리를 위해서 필요한 캐쉬, 메모리, 버퍼들을 향해서 과도한 서비스 요청을 보냄으로써 서비스가 불가능한 상태로 만드는 공격을 지칭한다[1]. 서비스 거부 공격을 위시해서 최근 빈번하게 발생하고 있는 침입 사고를 막기 위해 여러 가지 기법, 장비들이 제안 되고 있다. 보안 관련 장비에는 전통적으로 가장 많이 알려진 파이어월, 근래 도입이 많이 되고 있는 IDS, IDS 를 개선한 IPS, 그리고 1.25 대란을 계기로 해서 효용도가 널리 알려진 L7 Swtich 장비, QoS 장비 등이 있다. 그리고 보안 장비는 아니지만 기본적으로 패킷과 메시지 자체의 암호화를 제공하는 VPN 장비를 추가할 수 있다. 현재 장비 업체의 개발 추세는 각 제품군에 속하는 하나의 전용 장비를 개발하는 것이 아니라, 라우터 기반 IDS 장비, 파이어 월 기반 바이러스월과 같이 여러 보안 기능을 원 세트로 제공하는 통합 장비 개발을 진행하는 추세이다.

본 논문에서는 가까운 미래에 시장에서 요구하게 될 여러 보안 장비 형상 중에서 인터넷 망의 가장 기본에 속하는 라우터 장비 내에 필요한 보안 기능을 구현하는 프로젝트의 일부로 보안 라우터와 보안 관리 장비간의 경보, 구성 정보 전달 인터페이스에 대한 설계 및 구현 과정을 보이고 있다.

2. 보안 라우터와 관리 시스템의 구성

보안 라우터와 관리 시스템간의 구성은 그림 1과 같다. 보안 라우터는 침입 탐지 기능과 트래픽 제어 기능, VPN 기능, F/W 기능이 구현되어 있는데 이

중 침입 탐지 기능에서 탐지한 경보들의 전송 인터페이스로 IAP, IDXP를 사용한다[2]. 그리고 각 기능 블록들의 상태와 시스템의 구성 정보, 네트워크 상태 정보들의 전송을 위해 SNMP 프로토콜을 사용하고 있다. 그리고 보안 관리 시스템이 라우터 시스템을 제어하기 위해서 정책 기반 관리 기능을 구현하고 관련된 모든 메시지 통신은 COPS 프로토콜을 사용하고 있다. 본 논문에서는 경보 전달, 네트워크 관리 메시지 전달에 해당하는 IAP, IDXP, SNMP 의 구현 기술을 그 대상으로 하고 있다.



[그림 1] 보안라우터와 관리시스템 간 인터페이스

A : 정책 전달용 인터페이스 : COPS
B : 경보 전달용 인터페이스 : IAP, IDXP
C : 네트워크 관리용 인터페이스 : SNMP

3. 경보 전달 및 네트워크 관리 인터페이스

1) 경보 전달

보안 라우터 시스템은 경보 전달을 위해서 IAP와 IDXP를 적용하고 있다. 경보 전달 표준으로는 IAP와 IDXP가 제안, 개발 되어 왔는데, 현재 IDWG에서 Alert 전송 프로토콜로 IAP가 아닌 IDXP를 선택함으로써(50th IETF Meeting) IAP에 대한 연구 및 개발은 거의 이루어지고 있지 않다. IDXP는 침입 탐지 시스템 간의 데이터를 교환하기 위한 응용 계층 프로토콜로 일종의 BEEP 프로파일이다. BEEP는 연결 기반 통신, 비 동기 통신 등을 지원하는 일반적인 응용 프로토콜 프레임워크이다. IDXP는 연결 기반 프로토콜 상에서 상호 인증, 무결성 및 기밀성을 지원하며 IDMEF 메시지, 구조화되지 않은 텍스트, 바이너리 데이터 등을 교환할 수 있다. BEEP 보안 프로파일은 IDXP에 필요한 보안 속성 값들의 집합을 제공하기 위해 사용된다.

IDXP 모델은 접속 준비, 데이터 전송, 신뢰 모델로 구성된다. 먼저 접속 준비 단계에서는 종단 지점이 쌍으로 존재하며, 이 두 종단 지점은 하나 또는 다수의 BEEP 채널을 포함하고 하나의 BEEP 세션을 이용해서 통신한다. 데이터 전송에서 두 침입 탐지 시스템은 BEEP 채널을 포함한 하나의 BEEP 세션을 통해서 통신한다. BEEP 보안 프로파일은 IDXP 종단 지점 간의 종단 간 보안을 수립하는데 사용되며 성공적인 협상 이후에 IDXP 종단 지점이 신뢰할 수 있음을 보증한다. IDXP 프로파일은 침입 탐지 시스템 간의 정보 교환에 대한 메커니즘을 제공한다.

IDXP는 아직까지 프로토콜 자체에 대한 표준화 작업이 계속 이루어지고 있으며 구현 또한 미비한 실정이다. 2002년 8월에 처음으로 구현 결과물이 http://rr.codefactory.se/를 통해 릴리즈 되었다. 또 다른 IDXP 구현 프로젝트로 libidxp라는 것이 있다[4].

2) 네트워크 관리 메시지 전달

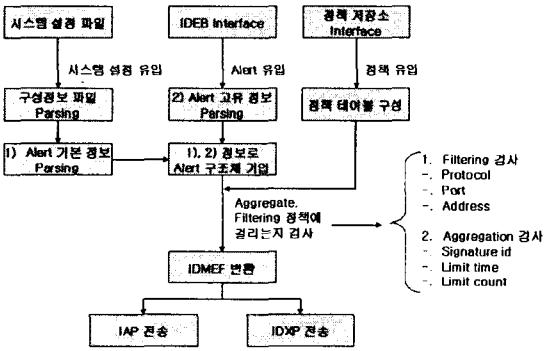
SNMP(Simple Network Management Protocol)[5]는 네트웍 관리 및 네트웍 장치와 그들의 동작을 감시, 제어하는 프로토콜이다. SNMP는 관리 정보의 정의를 위한 공통구조와 식별기법을 기술한 관리정보구조(SMI : Structure of Management Information)를 통해서, 망에서 피 관리 대상들의 집합체인 MIB (Management Information Base)으로 정의된 정보를 이용한다. SNMP는 간편성으로 인해서 망 장치 관리로 많이 배포되어서 사용 중이다[6]. 보안 라우터에서는 시스템 상태 정보와 구성 정보들의 전달을 위해서 SNMP를 사용하고 있다.

4. 구 현

1) 경보 전달 블록

경보 전달 블록은 그 기능에 따라서 부분으로 구성된다. 첫 번째로 커널 내부에 존재하는 침입탐지블록과의 인터페이스 부분이 있다. 여기는 Proc 파일을 통해서 경보 정보를 수신하고 필요한 정보로 파싱 하는 역할을 한다. 두 번째로 SRS 시스템 설정과 Rule 정책을 파싱하는 부분이 있다. 이 부분은 파일 또는 GDBM DB로 저장되어 있는 구성 정보들을 파싱 해서 이 정보들을 경보 데이터의 IDMEF 변환 시에 포함시킨다[3]. 세 번째로 정책관리유닛과의 인터페이스가 있다. 여기서는 정책관리유닛이 보내는 차단 정책과 축약 정책을 자체자료구조에 변환, 유지하면서 경보 데이터를 전송할 때마다 정책을 적용 가부를 판단하게 된다.

차단 정책에는 프로토콜, 송신 주소, 수신 주소, 송신 포트, 수신 포트가 사용된다. 예를 들어 송신 포트가 80 포트인 모든 경보 데이터는 전달하지 않는다. 등의 정책이 있을 수 있다. 축약 정책에는 경보 ID, 상한 시간, 상한 개수가 사용된다. 사용 조합은 경보 ID가 100 인 경보가 1000 ms 이내에 1000 개의 이상의 경보를 발생할 경우 이는 1개로 축약해서 보내라는 정책이 있을 수 있다.



[그림 2] 경보 전달 플로우

2) 구성 정보 관리 블록

구성 정보 관리 블록은 시스템 구성 정보, 시스템 커널 모듈 상태 정보, 시스템 응용 계층 모듈 상태 정보를 관리 한다. 커널 모듈 상태 정보로는 IDS, F/W, VPN, T/M, 접근 제어 등이 있다 각 모듈들은 기능은 On, Off 가 가능하다. 구성 정보 관리 블록은 기능의 On, Off 정보를 설정, 질의할 수 있는 기능을 수행한다. 표 1은 SRS 전용의 MIB 정의 예제를 보이고 있다.

[표 1] SRS 전용 MIB 정의

sysID.0	SRS-1
sysVersion.0	0.1
sysDescr.0	SRS-TEST-SYS
sysManufacturer.0	COMPANY
sysOperStatus.0	up(1)
sysUptime.0	NULL
fwOperStatus.0	up(1)
idsOperStatus.0	up(1)
vpnOperStatus.0	up(1)
acOperStatus.0	up(1)
tmOperStatus.0	up(1)
Policyblk.0	up(1)
Alertblk.0	up(1)
Nodeblk.0	up(1)
Iapproto.0	up(1)
Idxpproto.0	down(2)
copsproto.0	up(1)

구성 정보 관리 블록의 커널 상태 수집을 위해서 각 커널 모듈은 미리 지정된 Proc 파일 시스템에 자신의 상태 정보를 기록하도록 하였다. 기본값은 Not Setting으로 시작해서 모듈 초기화에 성공하면 Up 상태로 천이하고 사용자의 요구에 의해서 해당 커널의 작동을 중단 시키면 다시 Down 상태로 천이하게 된다. 그리고 IAP, IDXP 프로토콜 동작 상태와 경보 관리, 정책 관리 데몬의 상태 정보 수집을 위해서 리눅스 오픈소스에서 libproc 을 이용, SNMP 데몬에서 바로 다른 데몬의 상태를 감시할 수 있도록 구현하였다.

5. 결 론

본 논문에서는 보안 라우터와 관리 시스템간의 인터페이스 요구 사항을 검토하고, 이를 바탕으로 경보, 구성 정보 전달 인터페이스 시스템을 설계, 구현하였다. 본 프로젝트는 진행 중인 프로젝트로서 최종적인 목표는 억세스급의 (10Gbps) 보안 라우터

구현을 목표로 한다. 따라서 라우터의 기본 기능에 보안 기능을 추가함으로써 생기는 성능 저하를 최소화 하는 것이 주요 과제 중의 하나이다. 추후 과제로는 구현된 인터페이스 시스템 상에서 관리 시스템과 주고 받는 메시지의 구성과 내부 시스템 배치를 최적화함으로써 라우터의 성능 저하를 최소화하는 방안를 연구하고자 한다.

참고문헌

[1] S.Gilson, "The Strange Tale of theDenial of Service Attack Against GRC.COM," http://grc.com/dos/grcdos.htm, Mar. 2002

[2] B. Feinstein, G. Matthews, J. White, "The Intrusion Detection Exchange Protocol (IDXP)", draft-ietf-idwg-beep-idxp-07, October 22, 2002

[3] D. Curry, H. Debar, Merrill Lynch, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition", draft-ietf-idwg-idmef-xml-10.txt, January 30, 2003

[4] libidxp - An IDXP/BEEP Protocol Implementation, http://idxp.codefactory.se/

[5] J. Case, D. Harrington, R. Presuhn, B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2262, January 1998

[6] NET-SNMP Home Page, http://www.net-snmp.org/