SNMP를 이용한 웹 기반의 통합보안관리 시스템
(Web-Based Integrated Security Management System using SNMP)

이동영* 김동수* 방기홍* 김홍선** 정태명*
*성균관대학교 전기전자 및 컴퓨터 공학부
**㈜ 시큐어소프트
{dylee, dskim, khpang,}@rtlab.skku.ac.kr, hskim@securesoft.co.kr, tmchung@ece.skku.ac.kr

요 약

정보통신과 컴퓨터기술의 발전으로 인하여 불법침입으로 인한 정보 파괴와 컴퓨터 바이러스 등에 의한 역기능이 날로 증가하고 있다. 이러한 이유로 비밀성, 신뢰성 등의 정보보호 서비스에 대한 요구가 증대되어 정보보호기술 및 정보보호제품에 대한 수요가 점차 확대되어 가고 있다. 이에 따라 이종간의 보안 시스템들에 대한 통합적인 관리가 요구되고 있으며, 본 논문에서는 이러한 요구를 수용하는 웹 기반의 통합 보안 관리 시스템을 제안하고자 한다. 제안된 웹 기반의 통합 보안 관리 시스템은 클라이언트, 엔진 그리고 에이전트로 구성되어 있으며 관리자는 관리하는 항목과 역할에 따라서 3가지 등급으로 구분된다. 각 모듈간의 통신채널은 안전한 데이터 전송을 보장하며 사용자 인터페이스는 단순하고 개념적인 보안 서비스를 통해 보안 정책에 대해서 전문적인 지식이 부족한 일반 사용자도 쉽게 보안 관리를 할 수 있는 기능을 제공한다.

1. 서 론

정보통신과 컴퓨터기술의 발전으로 인하여 불법침입으로 인한 정보 파괴와 컴퓨터 바이러스 등에 의한 역기능이 날로 증가하고 인터넷과 같이 범세계적인 네트워크로 연결되어 있는 정보 시스템에 대한 위협 역시 급속히 증가하고 있는 추세이다. 이러한 이유로 비밀성, 신뢰성 등의 정보보호서비스에 대한 요구가 증대되어 정보보호기술 및 정보보호제품에 대한 수요가 점차 확대되어 가고 있다[2][3].

그러나 최근 네트워크나 시스템에 대한 크래킹이나 잘못된 조작 등에 의한 피해 사례는 대표적인 정보 보호 제품인 방화벽과 같은 침입차단시스템이 설치된 네트워크에서도 많이 발생하고 있다. 이는 지금까지 침입차단시스템만으로 자신의 네트워크를 안전하게 관리 할 수 있다고 믿고 있는 일부 보안 관리자들을 당혹스럽게 만드는 일임에는 틀림없다. 따라서, 보안 관리자는 자신이 관리하고자 하는 네트워크의 환경과 자료의 중요도에 따라 보안정책을 수립하고 이에 맞는 다양한 보안제품을 설치, 운영하여야 한다.

효율적인 보안 관리를 위해서 관리자는 보안 제품들이 설치된 네트워크 환경에 대한 전문적인 보안 지식과 각각의 보안제품에 대한 특성을 파악하고 있어야 하며, 개방형 네트워크 환경의 경우 새로운 보안 제품이 추가되면 새로운 보안 정책과 기술을 적용해야 한다. 이로 인하여 전산망 운영자의 보안 관리 업무의 비능률적 수행과 전산망 운영 기관의 보안 관리 비용을 가중시키며 체계적이고 일괄적인 보안 정책 및 기술 구현을 불가능하게 하여 오히려 보안 문제를 야기시키는 역기능을 초래할 수 있다.

또한, 보안 제품의 개발과 공급이 다수에 의해서 공급되므로 서로 상이한 특성을 갖는 보안 제품들로 구성된 보안 시스템의 효율적인 운용과 보안 유지에 상당한 어려움이 있다. 이종간의 보안 제품들은 서로 독립된 관리체계와 메커니즘을 통해서 인터페이스를 운용하고 유지한다. 또한, 보안 제품들에 대한 통합된 관리를 제공하지 못할 뿐만 아니라 체계적인 보안정책의 수립에도 많은 어려움이 있다. 따라서 다양한 보안 제품을 수용하여 각 제품별로 독립적으로 운영되던 개별적인 특성을 통합하고 전문적인 보안 관리 지식이 부족한 관리자도 중앙에서 체계적이고 일괄적인 보안 정책을 제어 할

주요 서비스	기 능	보안 제품
유해 서비스 차단	유해 서비스에 대한 접근 및 침입부터의 패킷을 차단한다.	침입차단 및 탐지 시스템
취약점이 많은 서비스 차단	일반적으로 취약점이 많은 서비스에 대한 접근을 차단한다. (telnet, ftp 등)	침입차단시스템
원하지 않는 메일 차단	특정 호스트나 ID 로부터의 메일 차단한다.	침입차단시스템
Spam 메일 차단	Spam 메일 리스트를 이용한 메일 차단한다.	침입차단 및 탐지 시스템
서비스 거부 공격 차단	Smurf, Land, SYN flooding 등의 서비스를 탐지 및 보고한다.	침입탐지시스템
해킹 서비스 탐지	네트워크 상에서 수행되는 해킹 프로그램의 접근을 차단한다.	침입탐지시스템
취약점 점점	호스트 내에 점검 모듈이 해당 호스트를 점검 및 보고한다.	각 보안제품
홈페이지 검색	홈 페이지 내에 불건전 정보의 존재 여부를 검색한다.	각 보안제품
프록시 적용	프록시를 사용한 특정 서비스에 대해서 접근 차단한다.	침입차단시스템

표 1: 개념 적인 보안 서비스

수 있는 유연성, 확장성 및 안정성을 갖춘 통합적인 보안관리 시스템이 필요하게 되었다.

본 논문은 앞서 언급한 문제점과 요구를 수용하는 웹 기반의 통합보안관리시스템(WISMS: Web-Based Integrated Security Management System)을 제안하고자 한다. 먼저, 2 장에서는 WISMS 의 전체적인 구조와 관리대상 보안 제품들에 대해서 간략히 살펴보고 3 장에서는 웹 기반 관리 시스템의 특징과 WISMS 를 구성하는 클라이언트, 엔진 그리고 에이전트의 각 구성 요소들에 대한 세부 기능 및 동작 메커니즘과 WISMS 의 실험 환경의 구성요소와 동작에 대해서 설명한다. 마지막으로 4 장에서는 WISMS 의 설계 진행 상황을 살펴보고 향후 WISMS 구현 시 추가 진행되어져야 할 연구 방향에 대해서 언급하고자 한다.

2. WISMS 의 개요

정보 통신 기술의 급격한 발전은 사용자 환경의 관리를 점차 복잡하고 어렵게 만들고 있다. 더욱이 일반 통신 서비스 이용자가 통신 장비나 서비스 관련 정보를 이해한다는 것은 상당히 난해한 일이다. 따라서 통신환경의 상태를 쉽게 보여주고 문제 발생시 신속한 문제의 분석 및 해결 방안을 제시하는 시스템의 개발이 지속적으로 요구되어 왔다. 이를 해결하기 위한 방안으로 사용자 인터페이스 부분을 웹 기술을 기반으로 개발함으로써, 사용자의 위치에 관계없이 시스템에 대한 접근 권한만 있으면 어느 곳에서라도 서버에 접근하여 시스템 상황을 감시.관리 할 수 있다. 또한, 웹 기반의 사용자 인터페이스는 운용관리 시스템의 기종에 종속됨이 없이 인터넷에 연결할 수 있는 어떠한 시스템을 통해서든 관리가 가능하게하여 관리 시스템의 개발과 운용측면에서 유연성을 극대화 할 수 있는 장점을 가지고 있다.

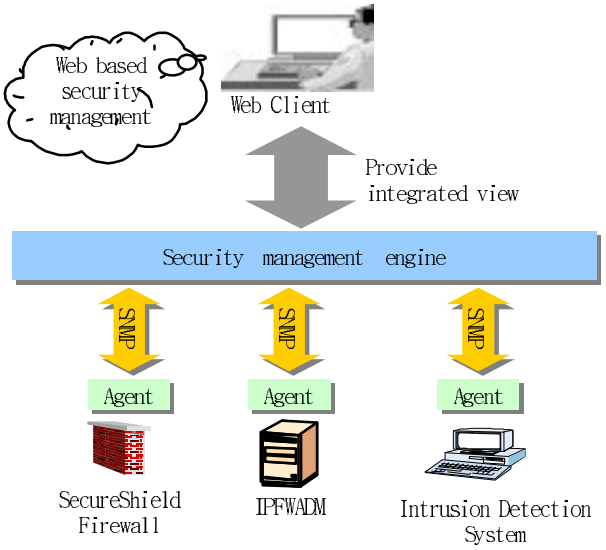

그림 1 : Overview of WISMS Environment

본 논문에서 제시한 WISMS 는 이러한 웹 인터페이스의 장점을 바탕으로 보안 정책에 대한 전문적인 지식이 부족한 일반 사용자도 쉽게 보안 관리를 할 수 있는 특징을 갖고 있다. 이를 위해서 표 1 은 WISMS 에서 제공하는 개념적인 보안 서비스를 나타낸 것이다.

2. 1 WISMS 의 적용환경 및 구조

WISMS 는 이종간의 네트워크 환경에서 네트워크 디바이스들과 응용 프로그램들을 관리하는 것뿐만 아니라 방화벽[3][4][24], 침입탐지시스템[1] 그리고 접근제어시스템과 같은 여러 여러 종류의 보안 제품들을 통합 관리하는 기능을 가진다. 그림 1 은 본 논문에서 제시한 WISMS 의 적용 환경을 나타낸 것이다.

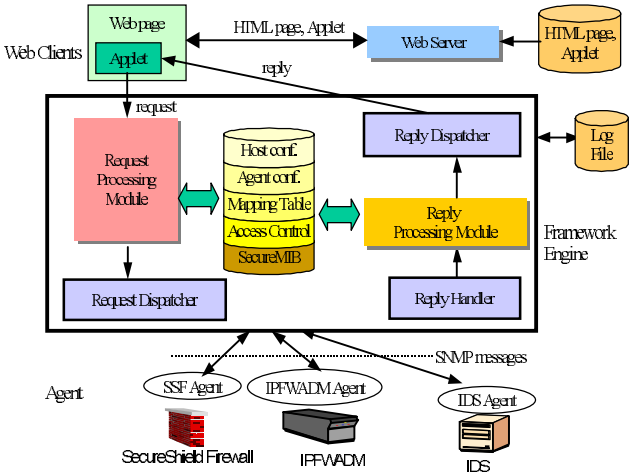

그림 2 : WISMS 의 전체 구조

WISMS 의 구조는 그림 2 와 같이 클라이언트, 엔진, 에이전트 등 3 개의 부분으로 구성되어 있다. 초기에 클라이언트는 HTTP 를 통해서 웹 서버에 접속하여 관리 프로그램의 웹 인터페이스를 구성하고 사용자의 명령을 받아 엔진에게 전달하는 자바 애플릿을 전송 받게 된다. 자바 애플릿은 실행과 동시에 엔진과 TCP/IP 연결을 설정하고 사용자로부터 요구를 받아 엔진에게 전달하는 기능을 담당한다. 엔진은 클라이언트로부터 요구 메시지를 수신하여 내부의 Request-Processing 모듈을 통해서 SNMP 메시지를 에이전트에게 전송한다. 에이전트는 전송된 SNMP 메시지를 분석하여 명령의 수행 결과나 응용 프로그램의 상태 정보를 엔진에게 전송하고, 엔진은 내부의 Reply Processing Module 을 통해서 에이전트가 보낸 메시지를 처리하게 된다. 엔진의 Reply Processing Module 은 에이전트에서 보낸 Trap 메시지를 해석하여 클라이언트 측에 알리는 기능도 수행한다.

2.2 관리 대상 보안 제품

WISMS 의 관리대상이 되는 보안 제품의 조사 및 분석은 침입차단시스템을 중심으로 수행하였으며 각 각의 보안 제품이 제공하는 기능의 설정을 위한 외부 인터페이스, 정책 설정 및 구성 방법의 분석을 중점으로 연구하였다.

특히 WISMS 의 프로토타입을 구현하기 위해서 소스코드에 접근이 용이한 보안 제품들을 관리 대상 보안 제품으로 선택하였다. 참고로 상용제품의 경우는 본 시스템의 공동 개발자인 국내 보안소프트 개발회사인 시큐어소프트의 SecureShied Ver.2.0 을 대상으로 하였다[25]. 표 2 는 관리 대상 보안 제품들의 특징을 나타낸 것이다.

보안제품명	특 징	개발자
SecureShield	패킷필터링과 프록시를 채용한 하이브리드 방식의 침입차단시스템	SecureSoft [25]
IDS	네트워크 기반의 실시간 침입탐지시스템	성균관대학교 실시간연구실
IPFWADM[26]	패킷필터링을 통한 침입차단시스템(공개S/W)	Jos Vos

표 2 : WISMS 의 관리대상 보안 제품

3. WISMS 의 설계

본 장에서는 WISMS 을 구현하기 위해 각 모듈 사이의 통신채널과 모듈 내부의 세부 동작 메커니즘, 구성요소 그리고 침입차단시스템의 공통적인 기능을 제어하기 위한 MIB 을 정의하고 실험 환경에 대해서 서술한다.

3. 1 WISMS 의 통신 채널

WISMS 의 통신 채널은 클라이언트-엔진간의 통신 채널과 엔진-에이전트간 통신 채널로 나눌 수 있으며 각각의 통신 채널을 안전한 정보 전송이 보장되어야 한다. WISMS 의 인터페이스는 그림 3 과 같다.

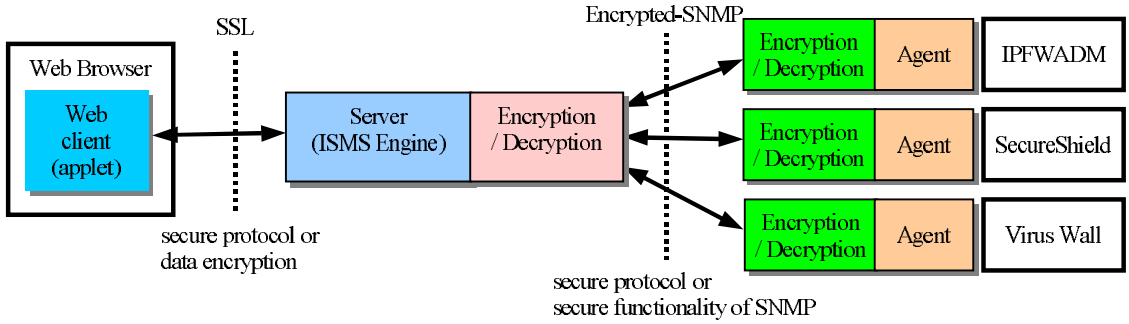

그림 3 : WISMS 의 인터페이스

● 클라이언트-엔진 통신 채널

클라이언트와 엔진 간의 통신은 HTTP 를 사용한다[6][19]. HTTP 는 응용 계층 에 속하며 그 기반을 TCP/IP 프로토콜에 두고 있다[23]. HTTP 의 연결을 통해서 클라이언트는 엔진에게 요구메시지를 보내며, 엔진은 에이전트로부터 수집한 보안제품의 상태정보 및 구성정보의 설정을 웹 브라우저를 통하여 사용자에게 보여준다[16].

안전한 통신을 위해서 WISMS 에서는 사용자 인증과 메시지에 대한 기밀성을 고려한다. 우선, 사용자 인증의 경우 간단한 보안 기법으로 기본 인증, IP 주소를 이용한 접근제어와 메시지 다이제스트 인증의 방법을 사용한다.

기본 인증은 사용자 ID 와 이에 대응하는 패스워드를 이용하는 방법이며, IP 주소를 이용한 접근 제어는 클라이언트의 고유 IP 주소를 이용해서 접근을 제어하는 방법이다. 마지막으로 메시지 다이제스트 인증은 MD5[3]와 같은 단 방향 함수로 다이제스트 하여 보내면 서버 즉, 엔진에 저장된 정보와 비교해서 클라이언트를 인증한다[18][24].

안전한 메시지 전송을 위해서 자바의 보안 기능을 사용하거나 SSL 을 사용한다. 웹 클라이언트 시스템 상에서는 불법적인 서버에 의하여 개인 정보가 노출되거나 외부 프로그램의 실행으로 인한 보안 구멍에 노출될 수 있다. 이러한 문제를 방지하기 위하여 WISMS 에서는 클라이언트에서 프로그램을 실행함으로써 엔진 프로그램의 안전성을 보장할 수 있는 자바를 사용한다. 이와 달리 웹 페이지 전송에는 SSL 을 사용하여 공개키 암호화 기술을 이용, 인터넷 어플리케이션들 간에 신뢰할 수 있는 통신 채널의 설정 및 암호화 통신을 수행한다[20].

● 엔진-에이전트 통신 채널

OSI 기반[8-15]의 연결 지향적(Connection-Oriented) 프로토콜인 CMIP[9]과 인터넷 표준 관리 프로토콜인 SNMP[5][16][21][22][23]의 적합성 비교를 통해서 엔진-에이전트간의 통신을 담당하는 프로토콜로 SNMP 를 설정하였다.

SNMP 는 CMIP/CMIS 에 비해서 구조가 간단하고 구현이 용이하다. 이미 구현된 소스코드가 공개되어 있으며, TCP/IP 기반 네트워크에서 널리 사용되어 기술이 검증되어 있다. 또한 네트워크 장비 제작사의 지원이 활발하며, 상대적으로 간단한 내용 전달에 적합하다[22].

불법적으로 엔진과 에이전트의 정보를 취득하거나 에이전트에게 요구 메시지를 보내는 등의 외부 위협 요소로부터 엔진과 에이전트 사이의 통신을 보호하기 위해서 SNMP 데이터 자체에 대한 기밀성 보장과 인증 메커니즘이 필요하다. 이를 위해서 엔진-에이전트간 인터페이스에 대칭 키를 분배하여 그림 3 과 같이 SNMP 메시지 자체를 암호화하여 송신하고 수신측에서는 복호화하는 과정을 통해서 안전한 통신 채널을 구성한다. 일반적으로 대칭키 암호화 알고리즘은 공개 키 암호화 알고리즘 보다 속도가 빠르며 WISMS 시스템에서 엔진과 에이전트는 물리적으로 근거리에 위치하여 통신 채널을 통한 원격 키 교환이 필요 없으므로 대칭키 암호화 알고리즘이 적당하다[20].

3.2 WISMS 의 구성요소

3.2.1 웹 클라이언트

웹 클라이언트는 호스트에 어떤 보안 제품이 설치가 되어있는지에 대한 정보가 없는 일반 사용자 관점에서 전체적인 통합 보안 관리시스템에 대

한 제어 기능을 수행하며 사용자에게 명령, 보안 정책, 보안 시스템의 위치 등의 정보를 통합적으로 수용할 수 있는 GUI 를 제공한다. 또한, 보안 관리의 이해와 정책 설정의 능력에 따라 다음과 같이 사용자의 등급을 분류한다.

- General Manager (GM)
  보안 관리에 대한 세부 지식이 없는 관리자로서 개념적인 보안 관리 기능만을 수행하며 토폴로지의 구성과 보안 제품 추가, 삭제 및 변경에 대한 설정 권한이 없다.
- Service Administrator (SA)
  GM 이 수행하는 보안 관리 기능을 수행함과 동시에 사용자와 서비스의 추가 및 삭제가 가능하며 세부적인 보안 정책을 설정한다.
- Security Expert(SE)
  네트워크 상의 보안 시스템으로부터 수집된 가공되지 않은 데이터에 대한 분석 기능과 보안 제품의 설정 및 Topology 를 구성한다

3. 2. 2 엔진

엔진은 웹 클라이언트로부터 받은 요구를 에이전트에게 요구하는 부분과 엔진에서 처리하는 부분으로 구별을 하며 해당 메시지를 생성하여 처리를 하고, 이 후 엔진 내부의 데이터베이스나 에이전트로부터 오는 응답을 처리하여 웹 클라이언트에게 응답 메시지를 돌려주는 기능을 한다. 엔진은 크게 Request Processing Module 과 Reply Processing Module 그리고 보안 데이터베이스로 나눈다.

- Request Processing Module
  웹 클라이언트와 통신하여 엔진 모듈로의 초기 접속을 설정하고 유지한다. 또한, 초기 클라이언트와의 접속 설정 시 Access Control Configuration Database 의 정보를 참조하여 클라이언트의 접근권한을 부여하는 기능을 포함한다. 그리고, 클라이언트로부터의 요구에 대해서 Mapping Table 을 참조하여 명령어 타입, 서비스 종류, 에이전트의 위치 정보 등을 분석하고 명령어 처리 대상 에이전트를 결정한다. 이 후 명령을 관리대상 객체 단위 query 로 전환하여 암호화된 SNMP 메시지를 해당 에이전트에게 전송하거나, 보안 데이터베이스를 검색하는 기능을 수행한다.
- Reply Processing Module
  Secure Database 로부터 추출한 정보나 에이전트로부터 전달된 암호화된 SNMP PDU 를 분석하여 보안 데이터베이스에 저장하고, 정보를 가공하여 클라이언트에게 웹을 통해서 제공하는 기능을 수행한다.
- 보안 데이터베이스
  엔진 내에 위치하는 보안 데이터베이스는 클라이언트로부터 요구되는 보안 관리 기능의 수행과 에이전트로부터 전달되는 보안 정보의 저장을 위하여 필요하다. 기능적인 관점에서 보안 데이터베이스는 5 개의 구성 요소로 이루어져 있으며, 클라이언트로부터 전달되는 보안 명령에 대해서 SNMP 메시지 생성을 수행하는 모듈에서 참조하는 Mapping Table, 클라이언트와의 접속 관리를 담당하는 Access Control Database, 보안 관리 정보를 저장 하는 SecureMIB, 네트워크 토폴로지에 대한 구성 정보를 저장하고 있는 Host Configuration Database, 그리고 에이전트(개별 보안 시스템)에 대한 구성 정보 관리를 위한 Agent Configuration Database 로 구성된다.

3. 2. 3 에이전트

엔진으로부터 받은 SNMP 명령을 받아 이를 해석하여 관리 대상 응용 프로그램에 이를 적용하고, SNMP 응답 메시지를 이용해서 엔진에게 결과를 전송하는 기능을 수행한다. 에이전트와 엔진 간의 메시지 전송 과정에서 모든 SNMP 메시지는 안전한 통신을 위해서 송신측에서 암호화되고 수신측에서 복호화하는 과정을 거치게 된다.

에이전트의 동작은 크게 수동적 동작과 능동적 동작으로 나누어 볼 수 있다[21][22]. 이 두 가지 동작에 대한 세부 구성을 보면 다음과 같다.

에이전트의 수동적 동작은 엔진으로부터 SNMP 요구 메시지를 받아 이 메시지가 관리 대상 응용 프로그램의 설정을 요구하는 메시지일 경우 이를 응용 프로그램에게 직접적으로 적용하고 그 결과를 엔진에게 통보한다. 이와 달리 정보를 요구하는 메시지일 경우는 이를 분별하여 응용프로그램에 관련된 여러 정보나 에이전트 자신의 관계된 정보를 SNMP 응답 메시지를 이용해서 엔진에게 통보한다.

에이전트의 능동적 동작은 자신이 관리하는 응용 프로그램의 상태 변화나 응용 프로그램 자체에서 발생한 오류 메시지 또는, 부가적인 이상 정보나 통지 사항이 있을 때 이와 관계된 정보를 SNMP Trap 메시지를 이용하여 엔진에게 전달하는 동작이다.

에이전트는 자신이 관리하는 응용프로그램의 소스코드 수정 및 재 컴파일 없이 전적으로 응용프로그램이 제공하는 외부 인터페이스(설정 파일, 설정 데몬, 혹은 설정 명령 프로세스)를 이용하여 정책을 적용할 수 있어야 한다. 에이전트가 MIB 값을 이용하여 WISMS 의 관리 대상인 제어 응용프로그램에 대한 정책의 설정 및 적용은 다음과 같은 방법을 통해서 할 수 있다.

- 응용 프로그램의 정책 설정 파일을 수정하여 적용하는 방법.
- 응용 프로그램과 특정 포트를 통해 직접 통신하는 방법.
- 응용 프로그램이 제공하는 정책 설정 명령 프로세스를 이용하는 방법.
- 위의 방법을 2 개 이상 동시에 제공하는 방법.

에이전트는 자신이 엔진으로부터 받은 MIB 값을 분석하여 위의 방법들 중 한가지를 이용하여 접근 제어 응용 프로그램의 정책을 설정 한다.

예를 들면, WISMS 의 관리대상 보안 제품의 하나인 SecureShield 의 경우 원격지에서의 제어를 위해 특정 포트상에 제어 데몬 프로세스가 있으며 또한, 지역적 설정을 위한 제어 명령 프로세스가 있다. 이 두 방법 중 에이전트는 효율성을 위해 제어 명령 프로세스의 호출을 이용한다. 즉, 에이전트가 받은 MIB 값에 따라 지역적 설정을 위한 제어 명령 프로세스를 적절히 호출하여 인자를 넘겨주는 방법을 사용한다

3. 3 WISMS 의 침입 차단 응용프로그램 공통 MIB

WISMS 에서 관리하는 각 응용 프로그램에 공통된 기능과 정보들을 위한 MIB 이며 크게 4 개의 부분으로 구성되어 있다. 그림 4 는 침입 차단 응용 프로그램 관리를 위한 MIB Tree 를 나타낸 것이며, 각 부분별 MIB 객체들의 기능에 대해서 간략히 소개하면 다음과 같다.

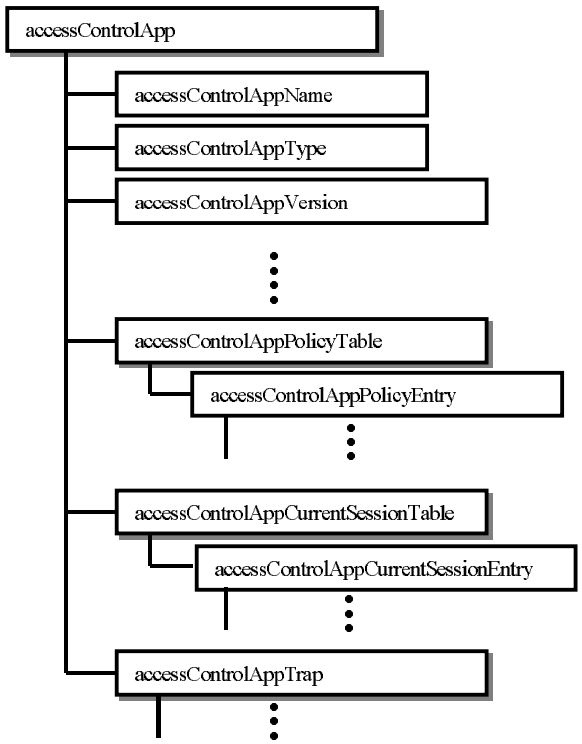

그림 4 : 침입차단 응용프로그램관리 MIB Tree

● 응용 프로그램 정보 MIB 객체 Group

침입 차단 응용 프로그램에 관계된 정적, 동적인 값들을 저장하고 제어하는데 사용되는 MIB 객체 들을 포함하는 Group 이다. 여기에 정의된 객체를 보면, 응용 프로그램의 이름, 응용 프로그램의 버전, 응용 프로그램이 설치된 날짜와 시간, 응용 프로그램의 실행 파일, 설정 파일에 관한 무결성 검사값, 응용 프로그램이 시작된 날짜와 시간, 응용 프로그램의 현재 상태, 프로세스 번호 등이 저장되게 된다. 이 MIB 객체들을 통해서 침입 차단 응용 프로그램 자체를 관리하고 현재 상태를 파악 할 수 있다.

● 응용 프로그램의 정책 테이블

침입 차단 응용프로그램의 접근 정책에 관한 정보가 저장되는 MIB 객체이다. 보통 침입차단 프로그램의 정책 설정 방법은 각 침입 차단 응용 프로그램마다 그 형식이 서로 상이하다. 그러나, 침입 차단 정책에는 근원지 주소, 목적지 주소, 포트 번호, 프로토콜 등의 설정 인자에 기반하여 접근 허용, 거부라는 공통적인 정책

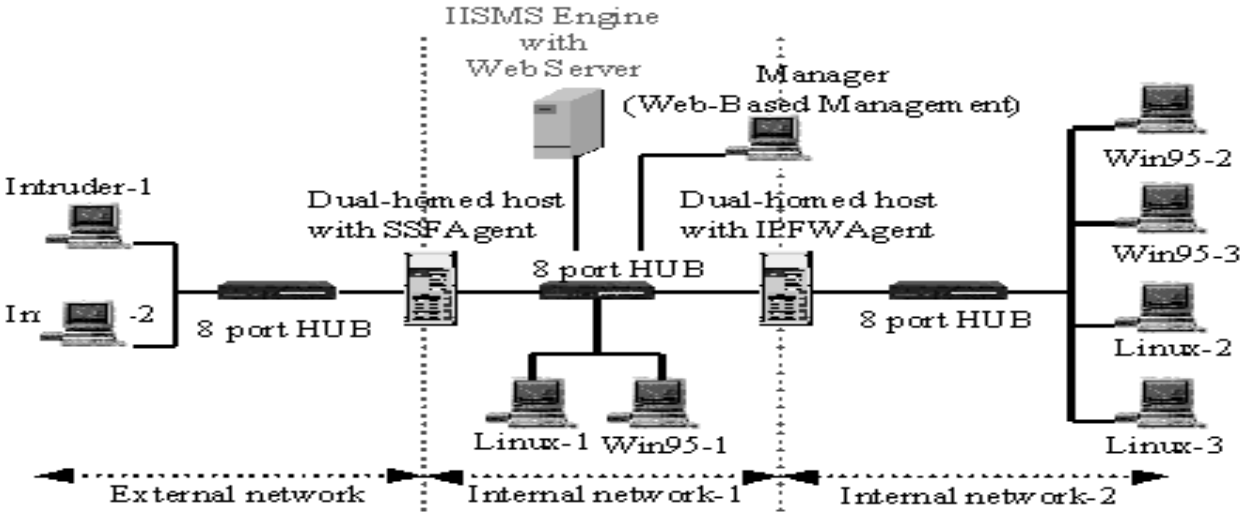

그림 5 : WISMS 의 실험 환경

형태가 존재한다. 이러한 공통적인 접근 정책 형태를 테이블 형식으로 구성하여 관리하는 것이 이 MIB 객체이다. 관리 에이전트가 관리 엔진에서 보내어진 SNMP 메시지 중 정책 설정을 위한 메시지를 수신하는 경우, 이 MIB 값이 변경되어 침입 차단 시스템의 정책이 수정된다.

- 관리 범위 내의 현재 세션 테이블

관리 대상 네트워크 상에서 침입 차단 응용 프로그램의 통제하에 있는 현재의 네트워크 세션에 관한 정보를 저장하는 MIB 객체이다. 이 MIB 을 통해서 정책 설정에 위반되는 세션의 연결 유무를 감시할 수 있으며, 병목현상이 나타나는 침입 차단점을 발견하여 네트워크 침입 차단 응용 프로그램의 갱신과 확장, 네트워크 구성 변경, 추가적인 침입 차단 시스템의 설치 등을 고려할 수도 있다. 그리고, 이 MIB 정보로부터 추출되는 통계적 자료에 근거한 의심스러운 세션의 파악과 이에 대한 접근 정책의 수정을 가할 수 있는 기초 자료를 제공한다. 기본적으로 이 MIB 테이블은 연결 지향 프로토콜에 대한 다양한 정보를 저장한다. 그러나, 일정한 타임아웃 설정에 의해 과거에 존재했던 비 연결 지향 프로토콜에 대한 정보를 설정한 시간 동안 저장하는 방법을 이용할 수 있다.

- Trap 메시지

침입 차단 응용 프로그램에서 발생하는 상태 변화나 오류 메시지가 있을 경우 이를 엔진에게 통보하기 위한 MIB 객체들이다. 이 MIB 에 정의된 Trap 메시지를 통해서 침입 차단 시스템의 이상 유무, 설정 변경, 관리자 접속, 응용 프로그램의 시작, 종료 등의 정보를 알 수 있다.

3.4 WISMS 의 실험 환경

다양한 보안 제품들을 효율적으로 관리, 제어하기 위해서는 우선 각 각의 보안 제품들에 대한 기능을 분석하고 이해해야 한다. 그림 5 는 본 논문에서 제안한 WISMS 의 프로토타입 개발을 위해서 실험적 네트워크를 구성한 것이다. 각 접근 제어 응용 프로그램을 위한 플랫폼으로 Linux, Solaris 를 사용하며, 내부와 외부 네트워크 상의 일반 호스트로 Window95 플랫폼을 사용한다.

각 접근 제어 응용 프로그램이 설치된 시스템은 Dual-homed host 이며, 각 각의 네트워크를 분리하는 역할도 동시에 수행한다. 이들 호스트에 의해서 내부 네트워크는 크게 두 개의 네트워크로 구분 할 수 있다. 외부 Dual-homed host 는 외부 네트워크 인터페이스에 공인된 IP 주소가 지정되어 있으며 인터넷과의 연결을 제공하게 된다. 내부 Dual-homed host 는 두 내부 네트워크 사이의 접근 제어를 담당한다.

WISMS 의 엔진은 1 차 내부 네트워크 상에 위치하며 2 개의 Dual-homed host 상에 설치된 에이전트와 SNMP 를 이용하여 메시지를 주고 받으며 중앙 집중적인 접근 제어 기능을 수행한다.

4. 결론 및 향후 계획

컴퓨터와 정보통신 기술의 발달은 전송 속도의 고속화, 대용량의 데이터 전송 등으로 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화 시켜주는 긍정적인 효과를 거두고 있는 반면, 개방 네트워크 구조인 인터넷의 확산으로 인한 컴퓨터 바이러스 및 정보 자원에 대한 침입 가능성은 날로 증대되고 있다. 따라서 다양한 보안제품을 적용한 보안 시스템의 필요성이 대두됨에 따라 본 논문에서는 서로 상이한 보안 제품으로 구성된 소프트웨어들을 통합적으로 관리하기 위한 다중보안기술을 수용하는 웹 기반의 통합 보안 관리 시스템(WISMS) 제안하였다.

본 논문에서 제안한 WISMS 의 개발 진행 현황을 살펴보면, 우선 클라이언트의 경우 관리자의 등급별 기능정의와 관리자에게 보여질 시스템 전체의 Topology, 보안정책에 대한 설정과 모니터링, 통계정보, Log 정보에 대한 사용자 view 를 설계하고 있으며, 엔진과 에이전트의 경우 세부적인 Secure Database 의 설계와 각 보안 제품들에 의존적인 기능별 MIB 정의 작업이 각각 진행 중에 있다.

그리고, 위에서 언급한 각 모듈들의 세부 구현을 통하여 플로토타입의 WISMS 를 개발하고 구현된 시스템에 대한 검증 작업을 통해서 도출된 문제를 해결하는 작업과 전체 시스템의 성능과 통합관리 시스템의 failure 에 따른 대응책에 대한 연구가 병행되어져야하겠다.

[참고 문헌]

[1] 이경하, 은유진, 임채호, 정태명, “네트워크 패킷을 기반으로 한 실시간 침입탐지시스템” 한국통신정보보호학회 종합학술발표회 논문집, vol.7 No.1, 1997

[2] 한국정보보호센타 정보보호뉴스 (통권 10 호), 1998

[3] C. Pfleeger, “Security in Computing Second Edition”, Prentice Hall, 1997

[4] D. Chapman and E. Zuicky, “Building Internet Firewells”, O’Relly & Associates. Inc. 1995

[5] D. Perkins and E. McGinnis, “Understanding SNMP MIBs", Prentice Hall , 1997

[6] F. Fielding, J. Gettys, J. Mogul, H. Frystyk and T. Berners-Lee, "Hypertext Transfer Protocol-HTTP/1.1", RFC2068, 1997

[7] F. Malek, and Panwar, “Network Management and Control vol.2”, Plenum Press , 1993

[8] ISO 7498-4: “Information Processing Systems – Open Systems Interconnection – Basic Reference Model Part 4 : Management Framework”, 1989

[9] ISO 9595: “Information Processing Systems – Open Systems Interconnection – Common Management Information Service Definition”, 1990

[10] ISO 9596: “Information Processing Systems – Open Systems Interconnection – Common Management Information Protocol” , 1991

[11] ITU-T Recommendation X.701 “Information Technology – Open Systems Interconnection – System Management Overview”, 1991

[12] ITU-T Recommendation X.711 “Common Management Information Protocol Specification for CCITT Applications”, Geneva, 1991

[13] ITU-T Recommendation X.720 ”Information Technology – Open Systems Interconnection – Structure of Management Information : Management Information Model”, 1991

[14] ITU-T Recommendation X.721 ”Information Technology – Open Systems Interconnection – Structure of Management Information : Definition of Management Information”, 1991

[15] ITU-T Recommendation X.722 ”Information Technology – Open Systems Interconnection – Structure of Management Information : Guidelines for the Definition of Managed Objects”, 1991

[16] J. Case, M. Febor, M. Schoffstall, and J. Davin, "A Simple Network Management Protocol (SNMP)", RFC1157, 1990

[17] M. Sloman, “Network and Distributed Systems Management”, Addison Wesley, 1994

[18] S. Garfinel and G. Spafford, “Web Security & Commerce”, O'Reilly &Associates, 1997

[19] T. Berners-Lee, R. Fielding and H. Nielson, "HyperText Transfer Protocol – HTTP/1.0", Internet Draft, 1995

[20] W. Stalling, “Cryptography and Network Security: Principles and Practice Second Edition”, Prentice-Hall, 1999
[21] W. Stallings, “SNMP, SNMPv2 and CMIP : The practical guide to network management standards”, Addison Wesley, 1993 1991
[22] W.Stallings, “SNMP, SNMPv2 and RMON : Practical Network Management Second Edition”, Addison Wesley, 1996
[23] W. Stevens, “TCP/IP Illustrated Volume.1”, Addison Wesley, 1994
[24] V. Ahuja, “Network & Internet Security”, Academic Press, 1996
[25] http://www.securesoft.co.kr
[26] http://www.xos.nl/linux/ipfwadm

이동영
1993 동아대학교 전자공학과 학사
1998 성균관대학교 정보공학 석사
현재 성균관대학교 전기 전자 및 컴퓨터공학부 박사과정
관심분야 : 네트워크 보안, 시스템 보안, 네트워크 관리,

방기홍
1998 년 성균관대학교 정보공학과 학사
현재 성균관대학교 전기 전자 및 컴퓨터공학과 석사 과정.
관심분야: 네트워크 관리, 네트워크 보안, JAVA 네트워킹.

김동수
1998 년 성균관대학교 정보공학과 학사.
현재 성균관대학교 전기 전자 및 컴퓨터공학과 석사 과정.
관심분야: 네트워크 관리, 네트워크 보안, 시스템 보안.

김홍선
1983 서울대학교 전자공학과 학사
1985 서울대학교 전자공학과 석사
1990 Purdue University, Electrical & Computer Engineering 박사
1990 년 - 1994 년 삼성전자 선임연구원
1994 년 - 1997 년 Twin Sun, Inc. 부사장.
현재 ㈜시큐어소프트 대표이사.

정태명
1981 년 연세대학교 전기공학과 학사
1984 년 University of Illinois Chicago, 전자계산학과 학사
1987 년 University of Illinois Chicago, 컴퓨터공학과 석사
1995 년 Purdue University, 컴퓨터공학 박사
1985 년-1987 년 Waldner and Co. , System Engineer.
1987 년-1990 년 Bolt Bernek and Newman Labs., Staff Scientist
현재 성균관대학교 교수
관심분야 : 실시간시스템, 네트워크 관리, 보안관리.