情 報 保 護 學 會 誌
第 13 券 第 1 號, 2003. 2

통합 보안 관리를 위한 이기종 보안 시스템 연동

이 영 석*, 나 중 찬*

요 약

보안 제품의 개발이 많아지면서 각 제품에 대한 통합의 필요성이 대두되고 있다. 예를 들어, 침입탐지 시스템에서 침입을 시도하는 노드를 판별한 경우, 실제 그 노드로부터의 접속을 차단할 수 있는 기능을 방화벽 시스템에서 제공하고 있기 때문에, 방화벽 시스템으로 접속 차단 명령을 보낼 수 있는 기능이 제공된다면 보다 자연스럽게 통합 관리가 이루어 질 수 있을 것이다. 그러나, 현재 보안 시장은 많은 종류의 보안 제품이 존재하기 때문에 이러한 통합이 쉽게 이루어지지는 않고 있다. 정보보호에 대한 관심이 높아지면서 많은 기업이 각종 보안시스템을 도입하고 있지만, 각 보안 시스템의 개별 관리에 중점을 두고 있어 이기종 보안 시스템 간의 연동에 기반한 통합 관리 차원의 필요성이 증가된다. 따라서, 국내외의 많은 보안 업체들이 이기종 보안 제품의 연동을 위한 방안들을 제시하고 있으며, IETF(Internet Engineering Task Force)를 중심으로 표준화 작업이 진행되고 있다. 본 논문에서는 국내외 각 보안 업체 혹은 보안 업체간 컨소시엄 형태로 제안된 이기종 보안 솔루션 연동 방식 및 공개 API(Application Programming Interface) 형식들을 분석하고, 표준화 동향에 대해 살펴본다.

Ⅰ. 서 론

대부분의 보안장비가 독자적 기술을 적용하여 개발되어 제품간 연동이 어려워지고 이를 운용하는 관리자는 기능 파악에만도 엄청난 노력을 들여야 하기 때문에 조직·장비·인력 소요가 증대되고 이는 결국 비용문제로 연결된다. 이와 같은 보안시스템에 대한 비효율적인 문제를 해결하기 위해 등장한 '통합보안관리(ESM, Enterprise Security Management)'가 최근 기업들로부터 호응을 얻고 있다. 이전에 전산시스템이나 네트워크가 방대해지면서 관리 효율을 높이기 위한 목적으로 서버관리시스템·네트워크 관리시스템 등 관리용 툴이 등장한 것과 마찬가지다[1].

초기에 ESM은 보안관제서비스업체가 고객사에 대한 관리 효율을 높이기 위해 자체 관제센터 용으로 개발하면서 시작됐다. 이 경우 단순히 보안제품에서 발생하는 로그를 직접 받아 모니터링하는 형태였으나 최근에는 여기에 검색엔진을 추가하면서 보안제품에서 발생하는 다양한 정보를 관리자가 선별할 수 있도록 제공하거나 각종 보안제품의 로그를 손쉽게 확인할 수 있도록 기능이 확장되었다[2].

보안관제 서비스는 정보보호 시스템을 원격지에서 관리하여 외부의 침입으로부터 보호하는 것을 의미했으나, 현재의 보안 관제 서비스는 서버와 네트워크 장비, 보안 시스템 등을 원격지에서 안전하게 관리하며 인가 받지 않은 외부 침입자를 실시간으로 탐지하여 원격 관제실에 경보를 보냄으로써 외부 침입에 즉각적인 대응 및 역추적을 할 수 있을 뿐만 아니라 이 기종간에 보안 관리를 할 수 있는 보안 통합 개념의 관제 시스템으로 발전하고 있다.

이러한 보안관제 서비스를 위한 선결과제는 각 고객 업체들마다 설치되어 있는 이기종의 보안 솔루션들을 통합해서 관리할 수 있는 통합 보안 솔루션인 ESM의 개발이다.

ESM은 침입차단시스템, IDS(Intrusion Detection System), VPN(Virtual Private Network) 등 다양한 종류의 보안 솔루션을 하나로 모은 통합 보안 관리 시스템으로 보안 관리보다는 통합 시스템 관리의 형태로 시스템 관리의 영역에서 먼저 출발하였다. 보안관리 측면에서의 통합 시스템 관리는

* 한국전자통신연구원 ({yslee, njc}@etri.re.kr)

Firewall, VPN, 바이러스 검사, 컨텐츠 필터링, URL 모니터링/필터링, 침입탐지 등 별개의 보안 구성 요소를 일관적인 전체로 결합하여, 인증과 감시, 허가에서 네트워크 관리에 이르기까지 모든 것들을 망라하는 통합관리로 연구되고 있다[3].

점차 도입이 확산되고 있는 ESM시스템은 통합관제시스템보다 대용량 네트워크와 이기종 보안시스템, 서버 장비를 보유하고 있는 기업을 대상으로 적용되고 있다. 향후 관리대상시스템이 기하급수적으로 늘어날 것으로 예상돼 안정성·확장성·비밀·편의성을 기반으로 한 통합보안관리 기능을 강화하는 유형으로 발전될 전망이다. 또한 현재까지 서버를 주요 대상으로 하는 통합보안관리 기능을 중점적으로 제공하고 있으나 대상 규모의 확장에 따라 앞으로는 일반적인 PC로까지 통합보안관리 대상 범위가 확장될 것으로 예상된다.

ESM의 기본적인 특성은 통합보안이라는 큰 틀 안에서 주요 기능이 '관제'와 '운영·관리'로 구분되며 365일 24시간 무정지 실시간 모니터링하는 것이다. 또한 이기종 보안시스템 외에 서버 및 네트워크 장비 등 각종 정보자산에 대한 확장적인 의미의 통합관제 기능이 요구된다. 즉 시스템 및 네트워크 관리영역까지 통합되는 기능을 갖고 있다는 것이다. 이외에도 다양한 보안솔루션을 통합적으로 지원하기 위해 필요한 '호환성'이 절대적인 기능으로 자리잡고 있다.

본 논문에서는 국내외의 많은 보안 업체들에서 이기종 보안 제품의 연동을 위해 제시된 방안들을 분석해 보고자 한다. 논문의 구성은 다음과 같다. 2장에서는 이기종 보안 제품 연동을 위해 국내외 각 보안 업체 혹은 보안 업체간 컨소시엄 형태로 제안된 공개 API 및 방안들을 살펴보고, 3장에서는 통합보안관리 표준화 동향에 대해 기술하고자 한다. 마지막으로 4장에서 결론을 맺는다.

II. 이기종 보안 제품 연동 방안

1. OPSEC

체크포인트(Check Point) 사에서 제안된 OPSEC (Open Platform for Security)은 확장 가능한 개방형 관리 프레임워크를 통하여 네트워크 보안의 모든 측면을 통합하고 관리하며, 제3의 응용으로 하여금 공개된 API를 통하여 OPSEC 프레임워크로 접속될 수 있도록 한다. 확장형 기업 정책 관리 및 정책 강화 프레임워크라 할 수 있는 OPSEC은 현재 OPSEC 협력 관계에 있는 250개 이상의 기업들이 안전한 엔터프라이즈 네트워킹을 위한 모든 요소들을 중앙 집중식으로 관리할 수 있게 하기 위해 중요한 역할을 하고 있다[4].

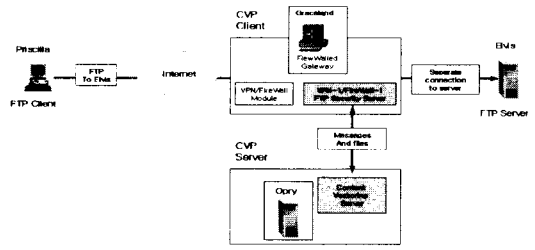
OPSEC은 보안 기능을 위한 몇 개의 프로토콜과 API의 집합으로 구성되어 있으며, 제공하는 SDK (Software Development Toolkit)을 이용하여 모든 제품들간의 통합이 가능하다. 현재 많은 업체의 제품들이 지원하고 있으며, OPSEC을 지원하는 제품은 아래와 같은 기능들을 이용하여 통합적인 보안 솔루션을 구성할 수 있다.

- CVP(Content Vectoring Protocol) API : 컨텐츠 보안
- SAM(Suspicious Activity Monitoring) API : 침입 탐지와 차단
- UFP(URL Filtering Protocol) API : 웹 자원 관리
- LEA(Log Export API): 리포팅과 이벤트 정보 분석
- ELA(Export Logging API): 이벤트와 보안 통합
- OMI(OPSEC Management Interface): 관리와 분석
- UAA(User Authority API): 사용자와 IP 주소의 연계
- SAA(Secure Authentication API): 인증의 통합

OPSEC은 OPSEC 전송 계층에서 제공되는 OPSEC API와 OPSEC 전송 계층 위에서 지원되는 API로 구분된다. OPSEC API는 일반 OPSEC 함수, 에러 처리 함수, 그리고 이벤트 API 함수로 구성된다. 위에 제시된 API 가운데 OPSEC CVP API와 SAM API를 통하여 이기종 보안 제품간의 연동이 어떻게 이루어지는 지를 살펴보도록 하며, 그외 API는 OPSEC SDK 관련 문서를 참고하기 바란다[4].

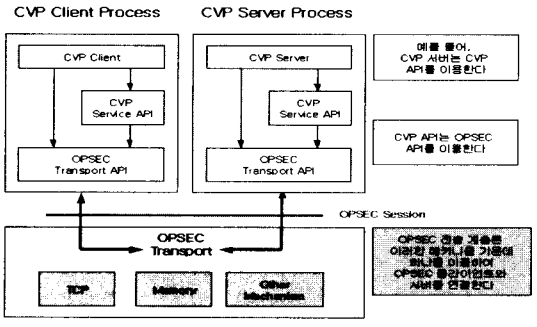
첫째, CVP(Content Vectoring Protocol) API는 제3의 Content Vectoring 서버가 다양한 프로토콜을 사용하여 전달되는 모든 파일들을 조사하는 것을 가능하게 하고, 그 결과로서 보호된 호스트의 취약성을 상당히 감소시키는 것을 목적으로 한

다. 체크포인트 사의 VPN-1/FireWall-1 제품을 통과하는 트래픽의 내용을 정책 설정에 따라서 제3의 응용 프로그램에게 전달하여 그 응용 프로그램의 응답 결과에 따라 트래픽에 대한 전달 허가/거부 및 내용(content)을 수정 한 후, 전달 등의 동작을 수행한다. 그림 1은 CVP 일반 프로그래밍 모델을 나타낸다. 우선, VPN-1/FireWall-1은 먼저 Content Vectoring 서버가 구동되는 지를 결정한다. 그런 다음, VPN-1/FireWall-1 보안 서버는 Content Vectoring 서버에게 조사되어야 할 파일을 전송한다. Content Vectoring 서버는 수신 파일과 해당 명령이 처리될 수 있는 지를 조사하고 VPN-1/FireWall-1 보안 서버로 조사 결과를 반환한다. VPN-1/FireWall-1 보안 서버는 조사 결과에 따라 파일 전송의 허용 여부를 결정하기 위해 해당 자원에 대해 적용된 규칙에 따라 행동한다.



〔그림 1〕 CVP 프로그래밍 모델

OPSEC 전송 계층(Transport Layer)은 TCP, Memory, 혹은 다른 메커니즘을 사용하여 OPSEC 서버와 클라이언트를 연결한다. 그림 2는 OPSEC API의 계층 구조를 보여준다. CVP 서버와 클라이언트에서 사용되는CVP API는 OPSEC Transport API를 기반으로 동작하게 된다.

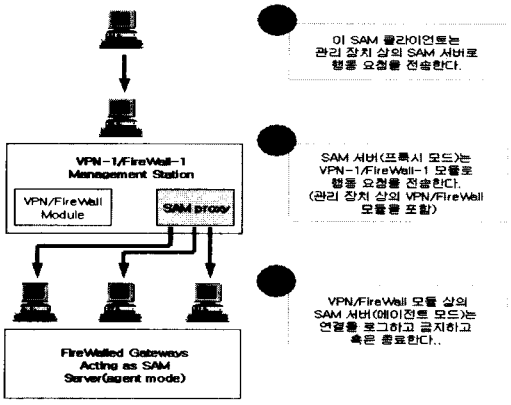


* Note : 클라이언트와 서버 프로세스는 같은 프로세스가 될 수 있다.

〔그림 2〕 OPSEC API 계층 구조

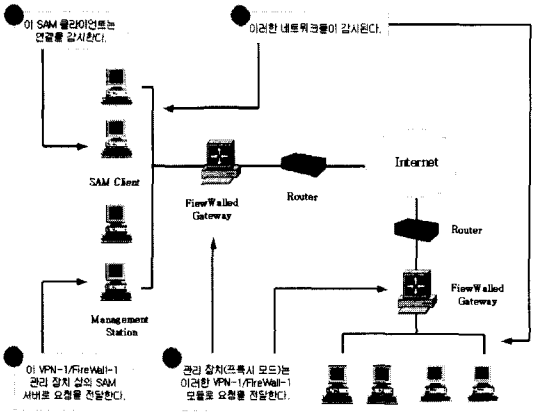
둘째, SAM(Suspicious Activity Monitoring) API는 네트워크 행위를 감시하는 제3의 응용들이 VPN-1/FireWall-1 시스템에게 어떤 연결을 로그하고, 금지하거나 블록킹하도록 요청하는 것을 가능하게 한다. 예를 들면, 모니터 응용 프로그램은 불법적인 명령어를 사용하거나 반복적으로 시스템에 접속 실패를 하는 사용자의 연결을 블록킹하도록 VPN-1/FireWall-1 에게 요청할 수 있다. SAM API는 SAM 클라이언트와 VPN-1/FireWall-1 사이에 통신을 구현한다.

SAM 클라이언트의 행동 요청은 하나 또는 그 이상의 VPN-1/FireWall-1 관리 장치 혹은 SAM 서버로서 동작하는 VPN-1/FireWall-1 모듈로 전달된다. SAM 서버는 에이전트 모드 혹은 프록시 모드로 동작할 수 있다. 에이전트 모드에서, SAM 서버는 자신의 VPN-1/FireWall-1 모듈을 통하여 주어진 연결을 로그하고, 금지하고 종료한다. 프록시 모드에서, SAM 서버는 SAM 서버로서 동작하는 다른 방화벽 기능을 갖는 호스트로 행동 요청을 전달한다. 이러한 과정이 그림 3에 보여진다. 그림에서 보듯이, 관리 장치 상에 있는 SAM 서버는 항상 프록시 모드로서 동작한다. 기본적으로, 관리 장치 상에 위치하지 않은 SAM 서버는 에이전트 모드로 동작한다



〔그림 3〕 프록시 모드/에이전트 모드의 SAM 서버

그림 4는 SAM 클라이언트가 두 개의 VPN-1/FireWall-1 모듈을 통하여 네트워크 연결 상태를 모니터하는 것을 보여준다. SAM 클라이언트가 이상 징후를 발견하면 SAM 서버로 연결 금지요청을 전송하고, SAM 서버는 VPN-1/FireWall-1로 요청을 전달하여 해당 연결을 금지하게 된다.



〔그림 4〕 SAM 프로그래밍 모델

이러한 과정들이SAM API 함수를 통해서 수행되며, SAM API는 세션 및 클라이언트 행위 함수와 이벤트 처리기로 구성된다. 아래 함수들은 SAM 클라이언트가OPSEC 세션을 초기화 하고, 특정 SAM 서버에 행동을 요청하기 위해 사용한다. 특히, AckEventHandler()는 VPN-1/FieWall-1이 SAM 클라이언트를 갱신하기 위해 호출한다.

- sam_new_session()
- sam_client_action()
- AckEventHandler()

미국에서 산업계 보안 표준으로 자리잡은 OPSEC API를 이용하여 통합보안관리를 개발하는 것은 체크포인트 사의 보안 솔루션 제품에 의존적일 수 밖에 없다. OPSEC API의 대부분이 체크포인트 사의 VPN-1/FireWall-1 제품에 기반하여 API를 정의하고 있기 때문이다. 또한, OPSEC 인증을 받기 위해서도 개발한 제3의 응용을 체크포인트 사에 제출하여 VPN-1/FireWall-1과의 통합 시험을 통과해야 하는 부담이 있다.

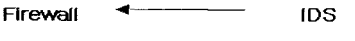
2. ASEN

ASEN(Adaptive Security for Enterprise Network)은 이기종 보안 제품 간의 연동을 위해 어울림정보기술에서 개발한 보안프레임워크이다[5]. 어울림정보기술은 SECUREWORKS 제품들과의 연동을 위한 ASEN API를 제공하므로, ASEN API를 이용하여 SECUREWORKS 제품군과 이기종 보안 제품들은 손쉽게 연동할 수 있다.

ASEN 프레임워크의 설계 목적은 다양한 보안제품으로 구성된 다수의 시스템을 모니터링하고, 상호 유동적으로 결합하여 작동할 수 있는 통신 모델과 제어 모델을 제시함으로써 불필요한 중복작업을 피하고, 보안 위협에 보다 능동적으로 대응할 수 있는 기반을 만드는 것이다. 이를 위해 ASEN은 다음의 사항들에 대해서 정의하고 있다.

- 상호 통신 방법의 정의, 제품간 또는 통합관리 서버와의 통신에 있어서 통신방법과 구조를 제안
- 상호 인증 방법의 정의, 통신에 있어서 신뢰성을 갖기 위한 상호인증 방법을 제시
- Security Device의 관리정보 표현방법 정의
- 보안정책 적용, 서로 다른 제품간의 보안정책을 설정하기 위해 어떠한 방법으로 보안정책을 표현하고 전송하는 가에 대하여 제시
- 통합관리에 필요한 기반 정보를 정의

ASEN은 Two-Tier 구조 혹은 Three-Tier 구조를 갖게 되는데, Two-Tier 구조는 두개의 ASEN 객체(object) 간에 상호 연동하여 작업을 수행하는 구조로 보안 제품 간의 연결과 보안 제품과 관리자 간의 연결로 나눌 수 있다. 그림 5의 보안 제품 간의 연결구조는 각 보안제품이 독립적으로 운영되면서 상호 연동을 통하여 보안기능을 수행하는 구조이다.



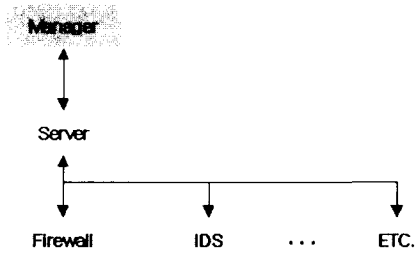
〔그림 5〕 보안 제품 간의 연결 구성도

Two-Tier 구조에서는 위 그림과 같이 각기 다른 보안제품이 직접 연결되어 있으며 특별한 이벤트 발생시 상호 정의된 규칙에 따라 동작할 수 있다. 예를 들어, 침입탐지시스템에서 침입이 탐지되었을 경우, 해당하는 출발지 주소에 대한 접속거부 등의 규칙을 방화벽에서 설정하도록 하는 것이다.

Three-Tier 구조에서는 그림 6과 같이 다수의 보안제품이 하나의 서버에 연결되어 있으며, 하나의 서버가 모든 통제를 하도록 구성되어져 있다. 통합보안관리를 수행하기 위해 서버는 데이터 수집, 저장 및 분석을 항상 수행하게 되며, 관리자는 필요한 경우 서버로 접속하여 그 상황과 결과를 모니터링할 수 있게 된다.

ASEN은 TCP를 기반으로 하여 상호통신을 수행하며, 통신 상의 보안을 유지하기 위해 암호화된 채널을 사용한다. 암호화된 채널은 SSL(Secure

Socket Layer) V3를 이용한다. SSL통신 시 사용되는 인증서 및 키는 수신자만 생성하여 관리한다. 접속자의 인증서 및 키는 선택적으로 사용할 수 있으며, SSL간의 상호 호환성에 문제가 있을 경우를 방지하기 위해 OpenSSL을 기준으로 하여 상호 호환성을 유지한다. 수신자 및 접속자는 ASEN 개체를 의미한다.



〔그림 6〕 Three-Tier Architecture 연결 구성도

ASEN 명령어 문법은 요청(Request)과 응답(Response)으로 구성되어 있으며 각 문법은 다음과 같은 형식을 갖는다. 요청은 명령자가 수행자에게 어떠한 요구를 하기 위한 명령으로 크게 METHOD, OBJECT, PARAMETER의 세 부분으로 나누어 진다. METHOD는 명령의 동작행위를 의미하며 OBJECT는 그 행위가 이루어질 대상을 지정한다. PARAMETER는 이 명령을 수행하기 위해 필요로 하는 추가정보 이다. METHOD는 아래 표 1과 같이 나누어진다.

〔표 1〕 METHOD 기능

METHOD	Description
GET	임의의 정보를 요청하는 명령어
SET	수정 명령어
DEL	삭제 명령어
ADD	생성 또는 입력 명령어
AUTH	사용자 인증

PARAMETER는 각 OBJECT마다 그 특성에 맞는 항목을 가진다. 하나의 요청은 다음과 같은 형식을 가진다.

〔METHOD〕〔OBJECT〕〔(PARAMETER=VALUE)...〕$

여기서 METHOD및 OBJECT는 반드시 하나의 명령에 하나만을 지정할 수 있으며 PARAMETER는 복수 개로 지정할 수 있으며 경우에 따라 생략도 가능하다. 하나의 명령은 중간에 LF(Line Feed) 문자를 포함하여 여러 라인으로 표현될 수 있으며 종료 문자인 '$'문자가 나타날 때까지의 모든 내용을 하나의 명령으로 인식한다. 요청을 전송한 뒤 처리자로부터 응답을 받기 전 까지는 어떠한 요청도 할 수 없다. 응답은 명령자가 내린 명령에 대한 결과값으로 수행자는 반드시 응답을 명령자에게 전달해야 한다. 응답은 다음과 같은 형식을 가진다.

〔RETURN CODE〕〔MESSAGE〕〔(PARAMETER=VALUE)...〕$

모든 응답은 반드시 RETRUN CODE와 MESSAGE를 가져야 하며 필요한 경우 PARAMETER를 포함할 수 있다. 예를 들어, RETRUN CODE와 MESSAGE에 추가적으로 PARAMETER를 가지는 응답은 다음과 같이 표현된다.

200 OK (STATUS=UP) (UPTIME=38573434)$

ASEN에서 사용되는 모든 명령어는 크게 인증(Authentication), 에이전트 식별(Agent Identification), 보안 객체(Security Object), 보안 정책(Security Policy), 로그(Log), 통계(Statistics), 상태(Status)로 나누어서 정의하고 있다. 이 중에서 에이전트 식별을 위한 ASEN 명령어를 살펴보면 다음과 같다.

- GET MIBINFO$
  기능 : 특정 보안 제품의 정보를 요청하는 명령
- GET MIB$
  기능 : 특정 보안 제품의 MIB(Managed Information Base) 요청하는 명령

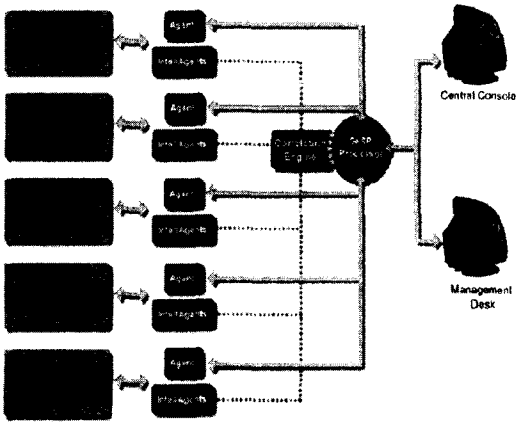
ASEN에서는 위와 같은 명령어들을 이용하여 각 보안 제품에 위치한 에이전트와 통합보안관리를 위한 관리자 사이에 SNMP(Simple Network Management Protocol) 형식의 확장된 API 집합을 정의하고 있다. 이러한 ASEN API를 사용함으로써 이기종 보안 제품 간의 연동이 가능하지만, 국내 보안 업계에서 아직까지 산업계 보안 표준으로 확립되지 못한 상태이다. 그러나, 국내 보안 업체 가운데 유일하게 이기종 보안 제품 연동을 위한 API를 공개하고, 통합보안관리 제품 개발에 적용하고 있다.

3. SNMP

국내외 많은 보안업체에서는 이기종 통합 보안 관리를 위하여 SNMP 기반의 API를 이용하고 있으며, 본 절에서는 eSecurity사의 OeSP(Open e-Security Platform)와 IBM Tivoli의 Risk Manager를 살펴보기로 한다.

첫째, eSecurity 사에서 개발한 통합보안관제 솔루션인 OeSP는 SNMP v1/v3를 이용하여 제3의 응용에서 사용할 수 API를 제공하고 있다[6]. 특히, 세계 최다의 에이전트(약 120개 : 어플리케이션과 장비간의 연동을 위함)를 지원하고, 제3의 응용에서 사용할 수 API 제공으로 손쉽게 에이전트 확장이 가능함을 장점으로 하고 있다. 그러나, 공개적으로 API를 제공하지 않아 어떤 형태로 지원되는지 파악할 수 없는 단점이 있다.

OeSP는 중앙집중형, 룰 베이스 에이전트로 작동하며, 이러한 에이전트들은 각 보안 장비들과 콘솔간에 통신을 지원하며 통신은 SNMP를 이용하여 엔터프라이즈 보안 관리 솔루션을 제공한다. 그림 8은 Open e-Security 플랫폼의 구조를 나타낸다.



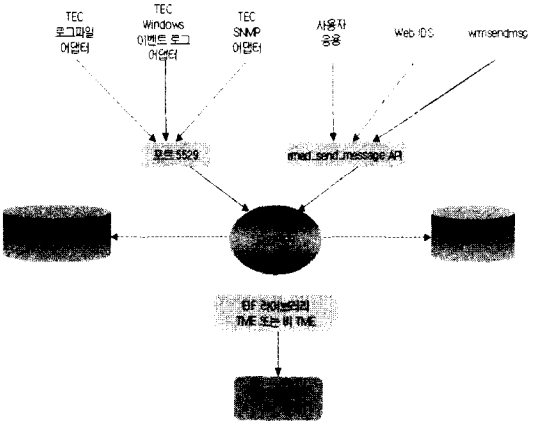
[그림 7] OeSP 구조

e-Security 플랫폼은 4개의 요소로 구성되어 진다. 다음과 같은 기능을 지원한다.

- Open e-Security Platform
  모든 보안 관련 장비를 하나의 GUI 콘솔에서 통합관리를 할 수 있도록 지원
- e-Security Agent
  각 장비와 콘솔간의 통신을 담당
- e-Security Administrator Workbench
  멀티 벤더의 장비들에 설치된 에이전트들을 룰 기반의 에이전트로 생성하고 서로간의 관계를 설정하고 관리하는 기능을 제공
- e-Security Management Desk
  침입에 대응하여 통보, 장애티켓발행, SLA관리와 관련된 워크플로우를 관리

둘째, IBM Tivoli Risk Manager는 침입 검출을 위한 관리 시스템으로서, 여러 가지의 포함된 센서 응용과 타사 센서(데이터의 소스가 되는 응용 또는 제품) 응용으로부터 침입 감지 경고를 받는 기능을 제공한다. 침입 검출 시스템은 실시간으로 서비스 거부 공격 또는 스캐닝 및 대량 공격의 침입을 발견하고 감시한다[7]. 또한, Risk Manager는 잘못된 경고와 실제 경고를 분리할 수 있도록 침입 검출 경고의 자동 처리를 제공한다.

그림 8은 Tivoli Risk Manger가 어댑터 혹은 응용으로부터 이벤트를 수집하여 TEC(Tivoli Enterprise Console) 서버로 전달하는 기능을 개략적으로 표현한다.



[그림 8] Tivoli 기능 개요

응용이나 센서가 Risk Manager에 보안 관련 이벤트를 전달하기 위해 사용 가능한 세가지 메커니즘을 제공한다.

- 표준 TEC
- TEC Event Integration Facility
- Risk Manager Event Integration Facility

첫째, 표준 TEC 어댑터로 작업하는 경우, Tivoli는 TEC 이벤트 어댑터에 대한 표준을 제공

한다. TEC 이벤트 어댑터는 정보를 수집하고 로컬 필터링을 수행하며 관련 이벤트를 TEC와 Risk Manager에 전달할 수 있는 형식으로 변환하는 소프트웨어 프로그램을 일컫는다. 여기서 어댑터는 센서가 작성한 데이터를 가져와서 그 데이터를 이벤트로 형식화하고 Risk Manager 이벤트 상관 서버에 이벤트를 보내는 응용을 의미한다. 이 어댑터는 기존 응용이 유용한 정보를 시스템 로그(Unix syslog 또는 Windows NT Event Log)로 라우트하거나 SNMP트랩을 생성하는 경우에 종종 사용된다. 예를 들어, TEC SNMP 어댑터는 SNMP 트랩을 수집하고 클래스 정의 명령문 파일의 규격에 따라 형식화하여 TEC 이벤트 서버로 보낸다.

둘째, TEC EIF(Event Integration Facility)를 사용하는 경우, TEC EIF는 이벤트를 TEC 서버로 보내기 위한 간단한 API 및 연관 라이브러리를 제공한다. Tivoli Endpoint에는 Tivoli 시스템에서 TEC 이벤트 서버로 이벤트를 보내기 위한 Tivoli *wpostemsg* 명령이 포함되며, Tivoli Endpoint는 비 Tivoli 시스템에서 TEC 이벤트 서버로 이벤트를 전달하기 위한 *postemsg* 명령이 포함된다.

셋째, Risk Manager EIF(Event Integration Facility)를 사용하는 경우, Risk Manager EIF는 이벤트를 이벤트 서버로 보낼 수 있는 확장 기능 세트를 제공한다. 이 기능은 C 및 C++ 프로그램을 위한 API, Perl 스크립트에서 Risk Manager EIF API로 직접 액세스하기 위한 모듈이 있는 Perl 지원, 명령행 기능을 포함한다.

SNMP 기반 API를 이용하여 이기종 보안 제품 연동을 위한 통합보안관리를 개발하는 것은 기존 SNMP 기반의 NMS와 ESM의 통합에서 동일한 프로토콜의 사용으로 효과를 발휘할 것이다. 그러나, SNMP 명령 자체의 제약성, 보안성, 그리고 표준화와 관련된 향후 확장성을 고려해 본다면 ESM 개발의 주요 방안으로 채택하기에 앞서 다양한 기능의 보강이 필요할 것이다.

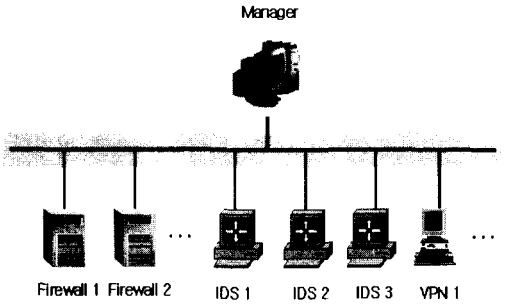
III. 표준화 동향

1. 국내 표준화 동향

1.1 ISTF

인터넷보안기술포럼(ISTF, Internet Security Technology Forum)은 인터넷 보안기술 분야의 민간 업체들이 중심이 되어 구성된 민간 포럼으로 인터넷 보안기술 관련 국제 표준화 활동에 공동 대응하고 시장수요를 반영한 표준 개발을 위해 2001년 창립되었다[8].

ISTF에서 제안된 통합 보안 시스템 구조는 그림 9와 같다. 관리 시스템(manager)이 ESM을 관장하고, 각 보안 장치인 Firewall, VPN, IDS가 네트워을 통해 연결되는 것을 가정하고 있다.



(그림 9) ESM에서 관리 시스템과 각 보안 장치과의 관계

ISTF의 주요 역할은 인터넷 보안기술 관련 최신 기술정보의 수집, 분석, 보급 및 활용을 촉진하고, 인터넷 보안기술 관련 국내 표준 개발하며, 인터넷 보안 관련 제품 상호운용성 항목 발굴 및 상호운용성 시험을 수행한다.

ISTF에서는 Firewall, VPN, IDS 등 여러 보안 업체의 보안 솔루션을 중앙에서 통합 관리할 수 있도록 로그형식 표준안 개정판을 2002년 12월에 발표하였다. 제안된 로그 표준은 각 보안 시스템에서 발생하는 이벤트를 전송하고 사용하는데 사용할 수 있는 표준화된 데이터 형식이다. 이 표준의 정의를 통해 상업적인 시스템, 공개용 시스템, 연구용 시스템 등을 설치하고 각각의 장단점에 따라 통합 운영이 가능하도록 구성할 수 있다.

우선, 방화벽 시스템 로그 형식 표준안을 살펴보면, 방화벽 시스템의 로그 형식에 대한 표준은 방화벽 시스템의 탐지 결과를 이용하고자 하는 보안 시스템 통합 관리시스템, 침입 분석 시스템 등의 보안 시스템이 방화벽 시스템에서 생성되는 로그를 통하여 연동이 가능하도록 방화벽 시스템의 로그 형식에 대한 표준을 정의하고 있다. 침입 탐지 시스템이나 가상사설망의 로그 형식에 대한 표준 역시 이와 유사하다.

Firewall, VPN, IDS 등 보안 시스템의 로그 형식을 체계적으로 정의하기 위하여, 우선 데이터 모델을 정의하였고 이에 따른 실제 구현 방법을 선택하여 정의하였다. 이를 위해서, 객체 지향 방법론 설계 언어인 UML(Unified Modeling Language)의 클래스 다이어그램을 사용하여 로그의 데이터 모델을 정의하였다. UML의 클래스 다이어그램은 확장성과 융통성을 보장할 수 있다. 또한, 로그 구현을 위하여 XML(eXtensible Markup Language)과 ; 으로 구분된 텍스트 형식으로 정의하도록 하였다. 확장성과 융통성이 필요한 경우에는 XML로 경제적인 표현법이 필요한 경우에는 ; 으로 구분된 텍스트 형식으로 표현할 수 있도록 하였다. 마지막으로, 침입 탐지 시스템의 로그와 호환성을 고려하고 국내에서 제작된 방화벽 시스템의 로그 자료를 함께 수집하여, 분석한 후 표준을 작성하였다.

ISTF에서는 방화벽, 침입탐지시스템, 가상사설망의 통합 관리를 위한 API 표준안을 제안할 예정이며, 우선 방화벽 통합 관리를 위한 API 표준안을 발표하였다.

ISTF에서 발표한 로그 형식 표준안 및 통합관리 API 표준안은 Firewall과 IDS를 개발한 업체들의 로그형식을 참조해 제정했기 때문에 곧바로 보안관제업체가 원격보안서비스에 활용할 수 있을 것으로 보인다. 제정된 VPN 및 ESM 표준은 아촵태전기통신협의체(APT) 산하의 ASTAP(APT STAndardization Program) 포럼에 제출, 일본·중국·호주 등 아시아·태평양 지역의 공통표준으로 채택을 추진 중에 있다.

1.2 SAINT

산업계 표준화 활동으로서, 국내 17개 정보보안 업체가 2001년 결성한 보안 컨소시엄인 세인트(SAINT, Security Alliance for Information Network & Technology)가 산업 표준 보안 아키텍처 구현과 보안 솔루션을 통합 관리할 수 있는 표준 API를 개발을 목적으로 결성되었다[9].

초기에 세인트는 PKI(Public Key Infrastructure)·PMI(Privilege Management Infrastructure)·ESMI 등 보안 인프라의 필요성이 높아짐에 따라 각사의 기술력 및 인프라를 활용한 원스톱 체제의 토털 보안 환경 구현에 적극 나설 예정이며, 이를 바탕으로 통신·금융·상거래 등 인터넷 환경의 중추적인 인프라 구축을 위한 산업 표준 아키텍처 개발에 주력하고자 했지만 활동 결과가 현재 거의 없는 상태이다. 그러나, 세인트는 단순 업무 차원의 전략적인 제휴에서 벗어나 보안제품 및 솔루션, 관리 콘솔 등 다양한 보안패키지 공동 개발을 통해 국내는 물론 아시아·태평양 지역의 시장 발전 및 기술 표준화에 적극 나설 계획을 갖고 있다.

1.3 VISTA

2001년 국내 6개의 보안 업체들이 보유하고 있는 전문 기술을 최고의 보안 서비스 및 솔루션 개발을 위해 비스타(VISTA, Vanguard of Information Security Technology Alliance)라는 공동 협의체를 결성하였고, 상호 제품의 연동, 공동 제품의 생산, 기술의 상호 전수를 목적으로 하였다[10]. 업계 내 상호 인적/물적/기술적/관리적 자원의 공유를 통한 효율적인 보안 조직의 구성이 필요해 짐에 따라서 비스타를 통한 통합 보안 및 토탈 솔루션을 고객에게 제공하고자 하였지만, 비스타는 현재 더 이상의 구체적인 진전이 없는 답보상태에 머물러 있다.

1.4 PISA

표준화 활동과 달리, 현대정보기술·한국IBM·리눅스시큐리티·에스큐브·인토스 등 시스템통합(SI) 및 정보보안 업체들이 결성한 정보보안업계 비즈니스 협의체인 피사(PISA, Pioneers of Information Security Alliance)가 2002년 결성되었다[11]. PISA 소속 7개사는 리눅스 기반 방화벽, 정보보호 컨설팅, 로그통합관리 솔루션 등 각사별 특화된 사업영역을 상호 보완하는 마케팅 활동을 통해 해외 정보보호 시장을 적극 개척한다는 전략이다. 특히 SI업체의 해외 금융기관 보안 프로젝트 및 보안 시스템 통합 프로젝트에 각 보안 업체들이 보유하고 있는 특화된 보안솔루션을 활용함으로써 해외시장 개척에 능동적으로 대처할 예정이다.

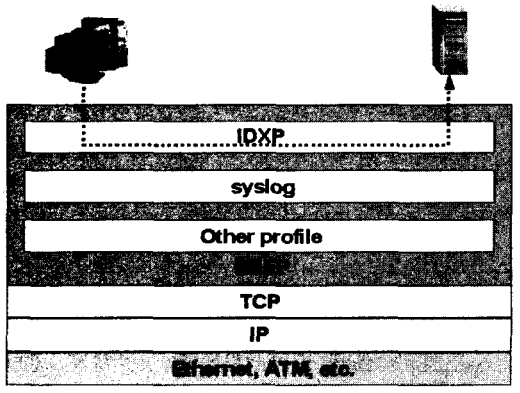
2. 국제 표준화 동향

이기종 보안 시스템 연동을 위한 국제 표준은 표준화 단체인 IETF(internet Engineering Task Force) IDWG(Intrusion Detection Working Group)에서 제안되고 있다. 지금까지는 이기종 보안 시스템간 연동 방안으로서, IDS에서 침입 탐지의 결과를 관리자로 통보하기 위해 IDS 로그 형식 표준안인 IDMEF(Intrusion Detection Message

Exchange Format)가 표준안으로 제안되었다[12-13]. IDMEF에서는 UML의 클래스 다이어그램을 사용하여 로그의 데이터 모델을 정의하였고, 데이터 모델을 실제 표현하는 방법으로 XML을 이용하였다.

IDMEF 기반의 XML 경보 데이터를 관리자로 통보하기 위한 프로토콜로서 IDWG에서는 BEEP (Block Extensible Exchange Protocol) 기반의 IDXP(Intrusion Detection Exchange Protocol)를 사용하고 있다. BEEP 프로토콜은 IDXP가 TCP/IP 상에서 사용될 수 있도록 해주는 기본 프로토콜이다. BEEP은 TCP 계층에서 동작하는 모든 프로토콜을 블록화하여 프로화일(profile) 형태로 제공하며 RFC3080, 3081에 기초하고 있다[14-15].

IDXP는 BEEP 상에서 상호 인증, 기밀성 등을 보장하는 프로토콜로서, BEEP 세션 형성 이후에 프로파일(TLS, SASL 등) 협상 그리고 IDXP 프로파일을 통해서 통신을 수행한다. 그림 10에서는 BEEP 상에서 IDXP를 이용하여 통신하는 경우를 보여준다[16].



[그림 10] BEEP 기반 IDXP

IV. 결 론

미국의 보안업계에 가장 널리 사용되고 있는 이기종 보안 시스템 연동을 위한 표준 프로토콜로는 산업계 표준인 체크포인트사의OPSEC과 IETF에서 표준화를 추진하고 있는 IDS와 관리자 사이의 전송 프로토콜인 IDXP(Intrusion Detection Exchange Protocol)와 메시지 형식을 정의한 IDMEF (Intrusion Detection Message Format) 등이 있으나, 아직까지는 완전히 국제표준으로 자리잡지 않은 상태이다.

많은 국내 개발업체도 ESM의 중앙관리모듈을 출시하면서 OPSEC을 지원하도록 하고 있으며, 자체표준을 제시하기 위한 움직임도 활발하다. 이기종 보안 솔루션간 상호 연동을 위한 보안 프로토콜 표준화문제가 ESM 상용화의 최대 현안으로 급부상함에 따라 프로토콜 표준화를 주도하고, 시장에 진출하기 위한 보안 업체간의 경쟁도 치열해지고 있는 실정이다.

따라서, 설치되어 운용되고 있는 다양한 보안 제품들의 상호 운용을 위해서는 각 보안 시스템들의 로그 표준화와 이들을 전달하고 관리하기 위한 보안 프로토콜의 제정이 시급하다. 또한, 단순한 통합적인 정보 수집이 아닌 보안 시스템들간의 연계된 동작이 이루어 질 수 있고 더 나아가 보안 제품군들만이 아닌 네트워크 관리 시스템들과의 협조와 데이터 교환 등 전체 관리 시스템들을 폭 넓게 통합관리 할 수 있는 프레임워크의 개발이 필요하다.

결과적으로, 향후 보안 관제 서비스 분야가 국내뿐만 아니라 세계 시장에서도 경쟁력을 가지고 성장하기 위해서는 국가 차원에서 이기종 보안 장비들을 동시에 관리할 수 있는 엔진 개발을 주도적으로 추진하는 것이 필요할 것이다.

참 고 문 헌

[1] 한국전자통신연구원, 주간기술동향 "ESM 기술 동향", 2001. 12.
[2] 시큐아이닷컴, 시큐아이ESM, http://www.secui.com
[3] 이글루시큐리티, 스파이더1, http://www.igloosec.co.kr
[4] Check Point Software, OPSEC SDK Documentation, http://www.opsec.com
[5] 어울림정보기술, ASEN Documentation, http://www.oulim.co.kr
[6] OeSP, eSecurity, http://www.esecurityinc.com/products/oesp.asp
[7] IBM, IBM Tivoli Users Guide, http://www.tivoli.com
[8] 인터넷보안기술포럼(ISTF), 로그형식표준안, http://www.istf.or.kr
[9] 마크로테크놀러지, http://www.macrotek.co.kr
[10] 정보보호뉴스, 2001. 12.
[11] 전자신문, 2002. 3.
[12] IETF, IDWG, Intrusion Detection Message

Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition, draft-ietf-idwg-idmef-xml-09.txt, 2002. 11.
[13] IETF, IDWG, Intrusion Detection Message Exchange Requirements, draft-ietf-idwg-requirements-10.txt, 2002. 10.
[14] IETF, RFC3080, The Blocks Extensible Exchange Protocol Core, 2001. 3.
[15] IRTF, RFC3081, Mapping the BEEP Core onto TCP, 2001. 3.
[16] IETF, IDWG, The Intrusion Detection Exchange Protocol (IDXP), draft-ietf-idwg-beep-idxp-07, 2002. 10.

〈著 者 紹 介〉

이 영 석(Young-seok Lee)

1992년 2월 : 충남대학교 컴퓨터공학과 학사
1994년 2월 : 충남대학교 컴퓨터공학과 석사
2002년 2월 : 충남대학교 컴퓨터공학과 박사
1994년~1997년 : LG정보통신(주)중앙연구소 주임연구원
2002년~현재 : 한국전자통신연구원 선임연구원
관심분야 : 가상사설망, 네트워크 보안, 이동컴퓨팅, 분산시스템

나 중 찬(Jung-chan Na)

1986년 2월 : 충남대학교 계산통계학과 학사
1989년 2월 : 숭실대학교 전자계산학과 석사
1998년 3월~현재 : 충남대학교 컴퓨터과학과 박사과정
1989년 2월~현재 : 한국전자통신연구원 능동보안기술연구팀 팀장
관심분야 : 네트워크 보안, 액티브 네트워크, 실시간 시스템