안전한 네트워크 구성을 위한 정책기반 보안 프레임워크

정회원 박 상 길*, 장 종 수*, 손 승 원*, 노 봉 남**

A Policy-based Secure Framework for Constructing Secure Networking

Sang-Kil Park*, Jong-Soo Jang*, Seung-Won Son*, Bong-Nam Noh** *Regular Members*

요 약

인터넷의 지속적인 보급/발전과 인터넷을 이용한 다양한 서비스의 증대를 통해 네트워크를 통한 보안취약점 공격과 정보획득을 위한 사이버테러 시도가 증가하고 있는 추세이다. 이는 침입탐지시스템의 적용환경에도 많은 영향을 끼치게 되었다. 일반적인 네트워크 기반 침입탐지 시스템은 네트워크 디바이스를 통해 유입되는 패킷에 대하여 시그너춰 기반 침입 탐지 모듈을 통하여 침입을 탐지하게 된다. 현재까지의 네트워크상의 정보보호는 주로 보안 호스트, 특정 보안 시스템에 대한 지역적인 정보보호였으나 전세계에 연결된 인터넷 시스템들의 침해에 대한 방어능력이 취약한 상태이다. 특정 도메인에 국한하여 서브 네트워크 상에 적용되었던 보안을 네트워크 전체에 확장시킬 수 있는 보안 메커니즘이 제공되어야 한다. 본 논문에서는 이를 해결하기 위해 DARPA의 과제를 분석하고, 그 분석을 통한 침입탐지관련 기술을 살펴본다. 또한, 상기에 지적한 보안 문제점들을 해결하기 위해 Policy 기반으로 보안집행이 수행되는 정보보호 서비스 구조를 설계하고, 각 모듈별 제공 기능에 대하여 살펴본다. 보안정책의 집행은 AS내의 네트워크 유입지점인 게이트웨이 장치에 설치된 침입탐지시스템을 통해 수행되며, 추가되는 정책정보가 중앙의 보안제어서버를 통하여 실시간으로 반영되어 처리된다. 이를 통하여 관리도메인에 대한 집중적인 보안정책의 설계 및 집행이 수행된다.

ABSTRACT

Cyber-terror trials are increased in nowadays and these attacks are commonly using security vulnerability and information gathering method by variable services grew by the continuous development of Internet Technology. IDS's application environment is affected by this increasing Cyber Terror. General Network based IDS detects intrusion by signature based Intrusion Detection module about inflowing packet through network devices. Up to now security in networks is commonly secure host, an regional issue adopted in special security system but these system is vulnerable intrusion about the attack in globally connected Internet systems. Security mechanism should be produced to expand the security in whole networks. In this paper, we analyzer the DARPA's program and study Intrusion Detection related Technology. We design policy security framework for policy enforcing in whole network and look at the modules's function. Enforcement of security policy is acted by Intrusion Detection system on gateway system which is located in network packet's inflow point. Additional security policy is operated on-line. We can design and execute central security policy in managed domain in this method.

keyword : Network security, IDS, PBNM, Security Framework

* 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 (wideideal@etri.re.kr), ** 전남대학교 전산학과 정보보호연구실
논문번호 : 020199-0429, 접수일자 : 2002년 4월 29일)

Ⅰ. 서 론

인터넷의 활성화에 힘입어 전세계의 인터넷 이용자수는 기하급수적으로 늘어났으며, 지금도 E-business, 기업의 홍보, 사이버 교육등의 분야에 인터넷이 이용되고 있다. 인터넷은 정보의 바다로서 필요한 정보를 쉽게 검색하여 사용할 수 있는 반면, 공개되어 있음으로 네트워크를 통하여 누군가 항상 접속이 가능하다. 본래의 목적인 정보의 창의적이며 효율적인 이용에 반하여, 불순한 의도를 갖는 공격자나 script kids에 의한 침입시도나 침입의 결과가 전세계에 걸쳐서 기하급수적으로 증가하고 있다. 이에 대하여 미국의 경우는 사이버 테러를 국가 안보의 중대한 위협요소로 규정하고 범정부적 대응체계를 준비하는 차원으로서 국가기반보호협의회(NIAC), 정보기반보호센터(NIPC), 분야별 정보공유 및 분석센터(ISAC), 정보기반보호연구소(IIIP)등을 설치하여 인터넷 보안에 관한 민·관 합동회의등을 통하여 대응책을 마련하려 하고 있다[1]. 일본의 경우에는 2000년 1월부터 사이버 테러를 실시간으로 탐지하고 경보를 전파할 수 있는 기술등을 본격적으로 개발하고 있으며, 유럽은 유럽전기 통신표준협회(ETSI : European Telecommunications Standard Institute)를 중심으로 유럽 및 전세계 차원의 정보기반 구조의 구축을 위한 정보보호를 포함한 각종 기준과 표준 정책등을 개발하고 있다. 이러한 사이버테러에 대한 각 정보의 대응에는 정보보호 차원의 법령 제정 과 일반 인터넷 사용자에 대한 교육 및 홍보, 침입의 조기 탐지 및 대응으로 연결되는 조기 경보대응 시스템의 개발, 주요 시스템에 대한 취약성 분석을 통한 보안성 강화와 같은 분야의 연구개발에 집중되고 있다.

본 논문에서는 이렇게 급증하는 사이버테러의 조기대응을 위한 네트워크 보안 기술과 관련하여 미국방성의 연구동향, IETF의 연구동향에 대하여 살펴보고, 광역망 차원에서 침입탐지 조기 대응 및 네트워킹 시스템을 보호하기 위한 정책기반의 보안제어구조를 기술하고 이와 관련된 시스템의 프로토타입을 제시하며, 실제 사이버테러가 발생하였을 경우 대응체계에 대하여 살펴본다.

Ⅱ. 관련 연구

1. DARPA의 침입탐지 대응

미국방성(DoD)의 DARPA(Defense Advanced Research Project Agency)소속인 ITO(Information Technology Office)는 외부 공격자에 의해 시스템에 대한 어떤 공격이 성공할지라도 군 정보시스템의 중요 서비스 및 기능에 대한 최소한의 성능을 지속시키기 위하여 (그림 1)과 같이 외부 인터넷을 통한 침입에 대응하기 위한 정보 생존 프로그램(Information Survivability)을 시작하였다[7].

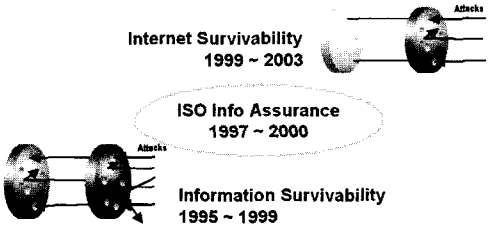


그림 1. DARPA Secure Networking Project

(1) 정보생존성(Information Survivability)프로그램

ITO에 의해서 1996년부터 1999년까지 진행되었으며, 보호대상에 대하여 외부로부터의 침입을 방어하는 시스템을 기반으로 하여 Local machine 위주의 침입탐지를 주로 수행하였다. 세부 주제로서 고신뢰 네트워킹(HCN : High Confidence Networking), 고신뢰 컴퓨팅 시스템(HCC : High Confidence Systems), Wrapper와 구성(W&C : Wrapper and composition), 대규모 시스템의 생존(SLSS : Survivability of Large Scale Systems)으로 구분되어 프로젝트가 추진되었다. HCN은 네트워크를 혼란시키거나 위태롭게 하는 공격에 대해 강력한 방법을 생성하고, 현재의 기술과 새로운 네트워크 기술등에 방어 메커니즘을 삽입하는 기술 개발, HCS는 모듈식의 보안 서비스 및 메커니즘의 제공과 분산 컴퓨팅을 위한 높은 신뢰성 제공, W&C는 Wrapper를 통한 구성으로 안전한 컴포넌트의 형성과 플러그인 Wrapper 기능의 제공과 자동 생성되는 Wrapper의 제공, SLSS는 모니터링 및 탐침, 침입탐지 및 대응 프로토콜 등에 대한 표준 인터페이스를 정의하고 이를 산업표준으로 채택하는 것을 목표로 한다. 상기와 같이 진행된 주요 결과물로서 EMERALD, NetSTAT, GrIDS, AAFID등과 같은 호스트 및 네트워크 기반 침입탐지 시스템을 개발하였다[4][5][6].

(2) 정보보증(Information Assurance)프로그램

ISO에 의해서 1997년부터 2000년까지 진행하였으며, 주로 ITO에서 가발되어진 프로젝트를 이관하여 운영하였다. 세부주제로서 시스템 보안관리(MSS : Manage System Security), 공격방지(PA : Prevent Attack), 탐지 및 대응(DR : Detect and Respond), 구조 및 통합(A&I : Architecture and Integration)으로 구분되어 프로젝트가 추진되었다. MSS는 정보생존성을 바탕으로 방화벽 등 보안 장치를 이용한 보안시스템의 관리를 위한 기술의 개발 및 통합, PA는 정보생존성을 바탕으로 동적인 방화벽 구성, 프로토콜의 보안성 제고 등의 기술 개발, DR은 정보생존성을 바탕으로 정보보증을 위한 보안프레임워크의 기술개발 및 통합, A&I는 정보보증을 위한 보안 API 및 보안프레임워크의 기술개발 및 통합을 목표로 한다. 상기와 같이 진행된 주요 결과물로서 정보생존성 프로그램에서 수행 중이던 프로젝트의 연장선상의 연구로서 CIDF, EMERALD, GrIDS, IDIP, Boundary Controller등이 연구되었으며, 침입탐지 시스템간의 정보 공유를 통한 Coordinated Attack 탐지, IDIP 프로토콜들을 통한 침입자 추적, 침입에 대한 라우터, 방화벽 등의 네트워크 장비를 통한 적극적인 대응기술을 개발하였다.

침입탐지 시스템간의 상호운용성을 확보하기 위하여 1997년 1월 CIDF 작업반이 결성되었으며 이는 미국방성 프로젝트의 지원아래 추진되었고, 1998년 SRI, UC Davis등에서 침입탐지 시스템을 복잡한 대규모의 네트워크 환경에 적용하도록 침입탐지 시스템 설계와 구현을 위한 방법으로서 논의되었다. CIDF는 (그림 2)과 같이 대규모의 네트워크에서 이기종의 침입탐지 시스템간의 정보교환 및 상호운영, 침입탐지 컴포넌트의 재사용에 대한 명세서를 규정하고 있다. 이는 이종의 침입탐지 시스템들이 정보를 교류하고, 이러한 정보를 이용하여 침입 탐지 및 대응을 효율적으로 하기 위한 침입과 관련된 정보를 표현하기 위한 프레임워크로서 이용된다.

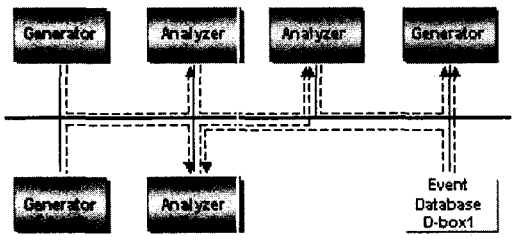


그림 2. CIDF Model

(3) 계층적 생존성(Inherent Survivability) 프로그램

연구되었던 많은 토픽들이 2000년부터 ITO에서 새로 시작된 Inherent Survivability 프로그램의 연장선에서 연구가 진행되고 있다. 2000년부터 ITO에서 추진중인 Inherent Survivability는 동일 Domain 내의 침입에 대한 탐지를 수행하며, 침입에 대한 적극적인 방어책으로서 침입탐지 및 대응을 제공하는 침입감내시스템을 개발하며 능동보안(Active Network)기술과의 융합을 통한 기술제공, 라우터, 스위치 등의 구성정보에 대해 동적인 변경을 통한 재구성 기술의 적용, DDoS 공격에 대응하기 위한 기술을 추진하고 있다.

2. IETF IDWG의 침입탐지 및 대응

IETF IDWG는 DARPA ISO의 정보보증(Information Assurance) 프로그램에서 기획, 추진되었던 CIDF에 근거를 두고 1998년 12월 구성되었다. IETF IDWG는 (그림 3)과 같이 침입탐지 시스템과 관리시스템간 정보공유를 위하여 데이터 포맷 및 교환 절차를 정의한다. 이들 연구는 이종의 침입탐지시스템들이 서로 상호 동작하도록 하는데 기본적인 목적을 가지고 있으며, 침입탐지 시스템을 구성하는 요소들이 지닐 수 있는 가능한 모든 역할을 블록별로 정의하고 있다[8][9]. 현재 IETF IDWG에서 논의되고 있는 세부 주제는 다음과 같다.

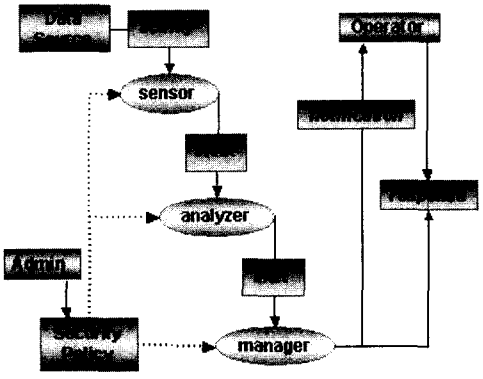


그림 3. IETF IDWG의 Model

(1) IDMEF(Intrusion Detection Message Exchange Format)

침입탐지 시스템, 대응 시스템, 관리시스템이 필요로 하는 정보를 교환하기 위한 절차와 데이터 포맷을 정의하기 위한 것이다. 요구사항은 일반요구사항, 메시지 포맷 요구사항, 통신 메커니즘 요구사항,

메시지 내용 및 의미 요구사항, Alert 정의 및 정의 절차 요구사항으로 구분된다.

(2) Tunnel(BEEP 프로토콜 기반)

BEEP(Block Extensible Exchange Protocol) peer들이 응용 프로그램 수준 tunnel을 생성할 수 있는 메커니즘을 제공한다. BEEP는 연결 지향적, 비동기 대화를 지원하는 일반적인 응용프로그램 프레임워크이다. 응용프로그램 수준 tunnel은 방화벽을 경유해서 BEEP 서비스를 제공하기 위해서만 사용된다. 이 문서는 TUNNEL 프로파일의 사용예와 메시지의 의미를 기술한다.

(3) IDXP(Intrusion Detection eXchange Protocol)

침입탐지 구성요소간 데이터를 교환하기 위한 응용프로그램 수준 프로토콜로서 일종의 BEEP 프로파일이다. IDXP는 연결 지향적 프로토콜 상에서 상호인증, 무결성 및 기밀성을 지원하며 IDMEF 메시지, 구조화되지 않은 텍스트, 바이너리 데이터 등을 교환한다. IDXP 모델은 접속준비, 데이터 전송, 신뢰모델로 구성된다. 중간 경유지의 Proxy는 항상 비신뢰 상태이며, 최종 단말구성요소만이 신뢰대상이 된다. IDXP 프로파일은 침입탐지 구성요소간의 정보교환에 관한 메커니즘을 제공한다.

IETF IDWG에서는 이와 더불어 침입탐지 엔진이 관리자에게 전달하는 경보메시지에 대해 XML 등을 이용한 침입탐지 관련 정보의 암호화 등을 제공한다. 이러한 제안에 대하여 현재 IDMEF에 관련된 library가 구현되어 제공되고 있고[15], IAP, IDXP등의 프로토콜을 적용한 시스템이 구현되고 있다. 대표적인 IAP 적용 시스템으로는 Global Guard[10]을 들 수 있다.

Ⅲ. 정책기반 보안프레임 워크의 구성

오늘날 빈번히 발생되고 있는 사이버테러에 대한 대응을 위한 필수 기술로서 침입 예방, 탐지, 제거 및 피해복구기술등이 거론된다. 기존의 보안장비는 방화벽, 침입탐지시스템 등의 단일 제품으로 제공되어 왔으나 사이버테러에 대한 효율적인 대응을 위해 최근에 제품들간의 상호정보교환이 가능한 통합보안관리 솔루션(ESM : Enterprise Security Management)을 개발 및 시판하고 있다. 이러한 제품들은 CheckPoint社의 OPSEC(Open Platform for Security)에서 정의하고 있는 SNMP 프로파일을 주로 이용하고 있다. 네트워크 보안제어시스템은 발생하는 공격에 대해 실시간 처리 및 대응기능과 분산시스템의 기능을 가져야 한다. 이러한 요구사항을 위해 IETF에서는 중앙 집중적인 보안정책 관리가 가능한 네트워크 구조로서 Policy Framework를 적용하고 보안정책관리 및 제어를 정책서버를 통하여 할당 관리하면, 관리되는 네트워크가 동일한 정책하에서 운용되어진다.

1. 정책기반 망 관리

PBNM(Policy Based Network Management) 시스템은 정규규칙을 제정하고, 정책에 따라 통신망을 운영하기 위해서 통신망 장치를 실시간으로 모니터링 하여, 동적으로 변화되는 정보를 신속하게 PBNM 시스템에게 전송해야 한다. 이를 위해서 IETF의 정책 프레임워크 규격에서는 기능적 컴포넌트로 정책관리도구(PMT), 정책저장장치(Policy Repository), 정책결정부(PDP), 정책수행대상장치(Policy Target)로 (그림 4)와 같은 기능으로 분류된다[11][12]. 또한 벤더의 시스템을 통신망 관점으로 볼 때, 운영자에 의하여 정책을 관리하고 통신망 동작을 모니터링하는 운영자 시스템, 정책규칙 및 각종 통신망 정보를 관리하는 서버(PDP : Policy Decision Point), 라우터 등의 통신망 구성장치(PEP : Policy Enforcement Point)로 구분한다.

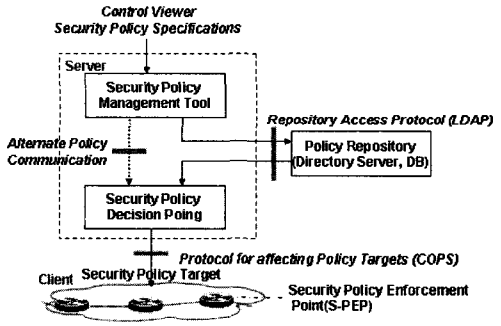


그림 4. IETF의 정책기반 망 관리구조

망 관리에 관한 정책은 정책 저장소(Policy Repository)에 저장되며, 망 내부의 분산되어 있는 정책 결정부(PDP)에 의해 실시간으로 검색된다. 정책 데이터는 Policy Condition과 Action으로 구성되며, 효율적인 보안정책의 적용을 위해 Policy Rule과 Group등의 데이터 스키마를 제공한다. 일반적인 정규규칙은 IF (condition) THEN (action) 형태로 구성되며, 여러 개의 정책규칙을 사용하여 또 다른

정책규칙을 생성할 수 있다. 표준화 동향은 다음과 같다.

(1) DMTF(Distributed Management Task Force)

관리 객체를 정의하는 CIM(Common Information Model), 관리 객체간의 접속 절차인 DMI(Desk-top Management Interface)를 표준화 문서로 제시하고 있다[13]. CIM 규격을 Schema 형태로 제공하며, CIM Schema 작성을 위한 MOF editor를 개발하여 제공하고 있다.

(2) IETF

IETF에서는 프로토콜에 대한 표준화를 Policy Framework과 IP Policy, QoS WG을 구성하여 표준화 연구를 수행하고 있다[8]. IETF 표준화 연구는 정책 프레임워크를 근간으로 접속 프로토콜, 정책 정보모델, QoS 제어를 위한 방식으로 구분하여 연구되고 있으며, 정책 정보모델을 정보보호와 QoS 제어를 위한 Core 모델을 연구한 후 각 특성에 맞는 정보모델을 확장방향으로 표준화를 수행하고 있다.

2. 정책전달 프로토콜

PBNM은 네트워크 환경에서 동적으로 네트워크의 운영방침을 적용하여 효율적인 네트워크를 운영하는 데 그 목적이 있다. 이러한 정책을 전달하기 위해 기존의 망관리 프로토콜인 SNMP(Simple Network Management Protocol)와 실제 정책 전달을 위하여 설계된 COPS(Common Open Policy Service)를 사용한다[8][14]. COPS 프로토콜은 정책서버(PDP)와 클라이언트(PEP) 사이의 정책정보 전달을 위한 TCP 기반의 간단한 질의/응답 프로토콜이다. COPS는 TCP connection을 이용하며, 모든 COPS 메시지는 common header로 시작하고, Header는 8비트, Op Code는 10개의 operation 정의가 가능하다. COPS는 (그림 5)와 같은 구조를 가지고 망에 적용된다.

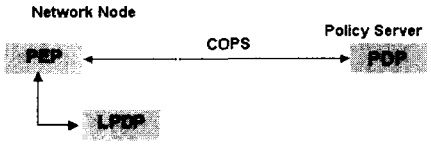


그림 5. COPS 기본구조

COPS프로토콜은 그 자체를 수정하지 않고 다양한 클라이언트 타입을 지원할 수 있는 확장성을 갖는데, IntServ 망에서 신호 프로토콜인 RSVP를 지원하기 위한 COPS-RSVP, DiffServ 망에서 provisioning을 위한 COPS-PR이 현재 제안되어 있다.

3. 정책기반 보안프레임워크

보안정책 규칙은 보안 정책 시스템의 핵심으로서 개체들 사이에서 상호 운용성을 나타내며 Condition / Action으로서 표현되어 진다. 본 논문에서 제안하는 계층적 구조를 갖는 보안정책모델은 (그림 6)과 같다.

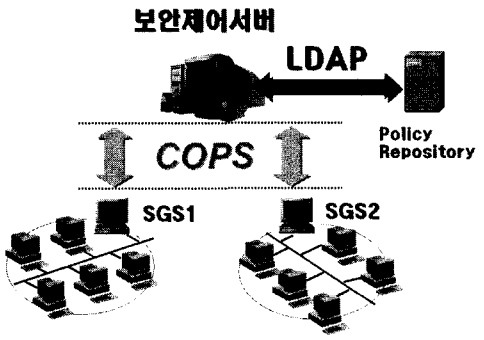


그림 6. 정책기반 보안프레임워크

정책기반 보안프레임워크는 계층적인 구조이며 적어도 2개의 계층으로 구성된다. 하나의 계층은 관리계층이며 PMT의 기능과 정책결정부(PDP)의 기능을 담당하는 보안제어 서버로서의 역할을 담당하게 된다. 다른 하나의 계층은 실행계층으로서 네트워크의 접속점에 위치하게 되며, 해킹 트래픽 탐지 및 대응을 위한 침입탐지시스템 기반의 보안게이트웨이 시스템(SGS : Security Gateway System)이다. 보안제어서버와 SGS 간의 정책의 전달은 COPS 프로토콜을 통하여 전달되며, 정책저장소(PR)와 PMT 간의 정책자료의 전달은 LDAP을 이용한다. SGS와 보안제어서버와의 구성관리는 SNMP를 이용하여 운용된다.

보안제어서버의 PMT는 SGS에서 적용할 Policy를 생성하고 LDAP 프로토콜을 이용하여 정책저장소에 저장한다. 보안제어서버의 정책결정부는 정책저장소에 저장된 정책을 읽어와서 SGS가 이해할 수 있는 데이터 스키마 형태로 변환 후 SGS 내부에서 정책집행부(PEP)기능을 수행하는 CP-A에 전달하면, CP-A는 추가되는 침입탐지 패턴 정보등을

SGS내부의 DB에 update한 후, Analyzer에게 통보하여 추가된 침입패턴에 대한 침입탐지를 수행하게 된다. 이때 PMT가 정의하는 정책(Policy)에 관한 정보는 DMTF에서 추진중인 CIM 모델을 이용하여 모델링을 하고, 이 정책정보는 LDIF형식으로 변환된 후 LDAP 프로토콜을 이용하여 정책저장소(PR)에 저장된다. 보안제어서버의 정책결정부(PDP)는 관리대상인 SGS에 적용하고자 하는 정책을 LDAP 프로토콜을 이용하여 PR에 조회한 후 해당 정책 데이터를 ASN.1 형식의 PIB로 변환 후 SGS에 전송한다. SGS 내부에서 PEP기능을 수행하는 CP-A는 PIB를 해독하여 SGS내부에서 침입탐지 패턴용 DB에 맞는 스키마로 변환하여 저장한다. 그후 CP-A는 침입탐지 기능을 수행하는 Sensor/Analyzer에게 새롭게 갱신된 보안정책을 적용하여 침입탐지기능을 수행하도록 signal을 전달하다. 이러한 기법을 통해 관리대상에 대하여 통일된 보안정책의 수행이 가능하며, 새로운 유형의 Attack이 발견되는 경우 정책서버의 정책 추가를 통하여 적용할 관리대상에 on-line상 업데이트 한다.

(1) 보안제어서버

보안제어서버는 침입탐지 정책의 구성에 관해 관리자에 의한 요구를 받고 이를 정책으로 생성하여 관리대상인 SGS에 집행한다. 보안제어서브는 SGS로부터 이벤트 로그 데이터를 수신하여 데이터베이스에 저장 후 통계 정보를 주기적으로 생성한다. 이렇게 생성된 정보는 관리자의 콘솔에 실시간 갱신된다. 이 정보를 기반으로 SGS에서 침입이라고 단정하기 어려운 이벤트에 대하여 High-level Analyzer(HA)를 통하여 침입을 탐지하게 된다. 보안제어서버의 HA는 이벤트로그 데이터와 SGS의 경보메시지를 가공하여 알려지지 않은 공격이나 협동공격(Coordinate Attack)에 대한 침입탐지를 수행하게 된다.

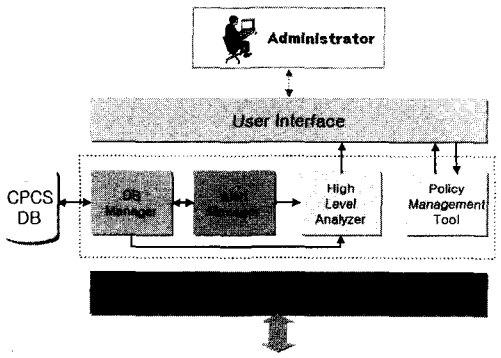


그림 7. 보안제어서버의 기능 블록도

보안제어서버의 세부기능은 (그림 7)과 같으며 다음과 같은 구성요소로서 운용된다.

- 관리자(Admin) : 보안프레임워크 전체에 대한 관리의 책임이 있으며, 침입에 관련된 경보를 사용자 인터페이스를 통하여 수신하며, 그에 적절한 대응을 취하도록 지시
- 사용자 인터페이스(UI) : 관리자로부터 모든 요청 메시지 등을 처리하며, 경보 관리자로부터 발생되는 보안 경보메시지를 관리자에 전달
- 데이터베이스 관리자 : 보안제어서버 데이트베이스 뿐만 아니라, UI관련 테이블, SGS 테이블, 정책 테이블, 시스템 로그 등을 제어(필요할 경우 이벤트 로그 프로파일 테이블, 경보 로그 프로파일 테이블, TCP 세션 테이블과 UDP/ICMP 패킷 정보 테이블 등을 제어)
- 경보관리자(AM) : SGSs로부터의 침입경보메시지를 수신하여 HA에 전달 및 침입경보메시지 가공
- 상위수준 분석기(HA) : Coordinated 공격의 탐지와 Anomaly탐지를 위한 보안제어서버의 핵심기능으로서, 보안제어서버상의 시스템의 침입도 탐지하며, 데이터베이스에서 경보데이터와 TCP session 정보 등을 이용하여 네트워크 전반에 걸친 공격을 탐지
- 정책관리도구(PMT) : SGSs에서 사용되는 패턴과 차단 등에 관련된 정책을 정의하고 집행을 결정한다. 관리자로부터 망 전체에 대한 정책을 전달받아 관리대상 객체인 SGSs에 적용
- COPS server : COPS 프로토콜을 통하여 정책을 송수신 하는 기능

(2) 보안게이트웨이 시스템

SGS는 네트워크의 유입지점에서 게이트웨이 역할을 수행하며 네트워크 기반 침입탐지 역할을 수행하는 Sensor/Analyzer를 탑재하고, COPS Client를 통하여 수신된 정책정보에 의하여 침입을 탐지한다. 탐지된 각각의 침입에 대하여 CP-A는 SGS의 데이터베이스에 경보메시지를 저장하고, SGS의 구성정보를 참조하여 보안제어서버에서 어느 SGS인지 확인 가능한 정보를 첨부(sgs_id 필드)하여 경보메시지를 생성 후 COPS 프로토콜을 통하여 보안제어서버에 전달한다. 현재의 보안게이트웨이 시스템은 Linux 서버에 Etherenet Interface 2장 또는 ATM

Interface 2장을 적용하여 Linux Router로서 동작하도록 되어 있다.

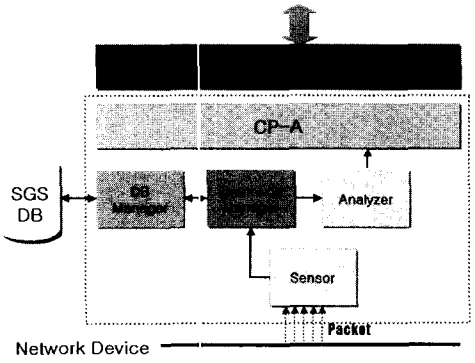


그림 8. 보안게이트웨이 시스템의 기능 블록도

SGS가 침입을 탐지하는 방법은 네트워크 기반 침입탐지를 수행하며 Misuse 방법을 주로 사용한다. 새로운 유형의 공격에 대한 패턴의 정의가 필요할 경우 보안제어서버의 정책관리도구에서 정책을 정의하고 정책결정부를 통해 변환후 COPS client에 전달하면 CP-A는 PIB형태로 수신된 정책정보를 SGS의 관계형 데이터베이스의 스키마에 맞게 변환 후 Analyzer에게 패턴정보의 업데이트 메시지를 전송한다. 이 시그널이 수신되면 Analyzer가 데이터베이스에서 바뀐 패턴정보를 저장하는 테이블을 조회하여 메모리에 업로드하여 시스템을 재 구동하지 않고 메모리 상에 추가된 패턴정보를 Analyzer의 정책으로 적용하여 새로이 적용되어진 패턴에 의해 공격에 대하여 유연하게 대응한다. SGS는 (그림 8)에서 보는 것처럼 크게 5가지의 구성요소로 구분된다.

- COPS Client : 보안제어서버와의 정책 송수신 및 Alert Data등의 전송경로로 사용
- CP-A : SGS의 데이터베이스 관리자와 SGS 내의 PEP 기능의 수행 및 L-PDP(local)기능 수행. 중앙 보안제어서버로부터 침입탐지 정책을 수신하여 SGS 시스템에 맞도록 변환 및 데이터베이스 저장 기능을 수행
- Sensor/Analyzer : 네트워크로부터의 패킷의 유입시 패킷을 수집, 축약, 캡춰한 후 정해진 보안정책에 의해 침입을 탐지한다. Sensor로부터 생성된 이벤트로그 데이터는 이벤트로그 관리자에 의해 데이터베이스에 저장되며, 일정기간마다 ftp 경로를 통하여 보안제어서버에 전송된다. Analyzer는 이벤트로그 데이터에 대하여 지속적이며 반복적으로 적용할 보안정책을 매칭하여 침입을 판정
- 이벤트 로그 관리자 : 축약된 이벤트 로그 데이터를 주기별로 압축하여 보안제어서버의 경보관리자에 전송하여 off-line 침입탐지
- 데이터베이스 관리자 : 보안정책 및 SGS 구성관리, 이벤트 로그, 경보데이터 등을 테이블 단위로 관리

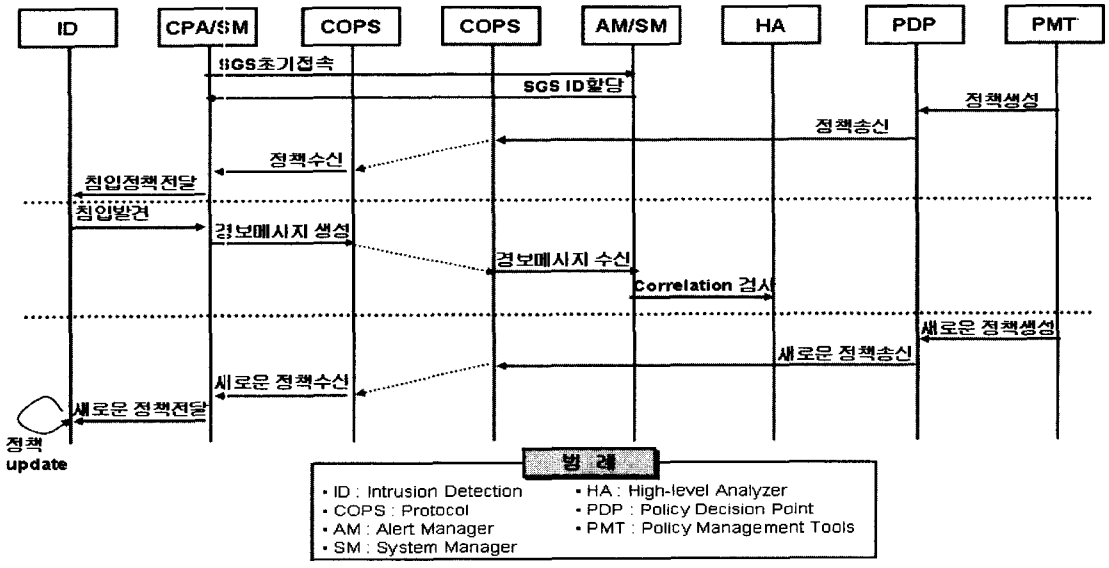


그림 9. 정책기반 보안프레임워크의 흐름도

(3) 정책기반 보안프레임워크의 운영

시스템이 운영되는 절차는 다음과 같다. 먼저 중앙보안제어서버와 보안게이트웨이 시스템은 서로 다른 도메인에 물리적으로 연결된 상태에 있음을 가정한다.

(그림 9)에서 첫 번째 단계는 SGS 시스템이 CPCS의 관리대상으로 운영되기 위한 첫 번째 단계로서 정책을 수신하는 과정을 나타낸다. 두 번째 단계는 침입을 발견하였을 경우 경보메시지를 전달하고, 망의 보안위협도를 점검하는 과정을 나타낸다. 세 번째 단계는 새로운 정책이 PMT에 의해 정의될 경우 말단인 게이트웨이 시스템에 적용되는 과정을 나타낸다.

Ⅳ. 테스트 베드의 구조 및 공격에 대한 대응

Ⅲ장에서 설계되었던 보안제어서버와 다수의 SGS 시스템을 관리도메인에 적용하였을 경우 실제 어떤 결과와 효력을 나타내는지 살펴보고자 한다. 본 시스템을 테스트 베드 상에서 실험하고자 (그림 10)과 같은 네트워크를 구성하여 적용하였다.

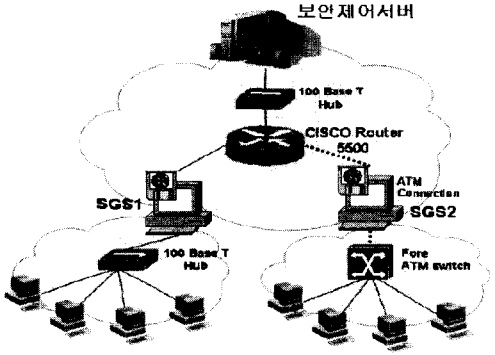


그림 10. 테스트베드 프레임워크 구성

1. 테스트베드의 구조

각 서비스 Zone에 연결된 Edge에 SGS 시스템이 각각 설치되며, 각 SGS는 중앙의 보안제어서버에 의한 정책을 수신하여 집행한다. 본 테스트베드에서는 하나의 Ethernet과 하나의 ATM망을 이용하여 구성하였다.

2. 공격에 대한 대응

중앙의 보안제어서버는 각 Zone마다 별개의 보안정책을 전달 할 수 있으며, 이를 통해 네트워크 이용성향에 따라 보안정책을 유연하게 적용할 수 있다. (그림11)은 보안제어서버에 연결된 관리대상인 SGS 시스템에 대해 침입탐지 정책이 전송되어 가능한 식별자를 통하여 네트워크의 성격에 따라 별개의 정책을 적용할 수 있다. 공격에 대한 탐지 및 대응에 대하여 실험하고자 nmap과 nessus를 이용하여 Smurf Attack을 시도하였다. 중앙의 보안제어 서버상에서 침입탐지 정책을 정의할 때 공격의 피해 심각성에 따라 Impact를 분류하여 적용한다. (그림 12)는 공격유형별 심각성에 따른 경보데이터를 Impact Level에 다라 1, 2, 3 구분하여 보인다.

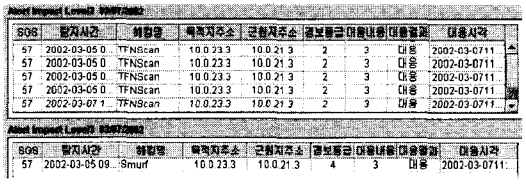


그림 12. 공격의 심각성(Impact)에 따른 경보의 분류

보안프레임워크에 정책기반네트워크 관리개념을 접목시키는 가장 중요한 이슈는 관리대상에 대하여 전체가 동일한 정책하에 침입을 탐지하며, 침입을 차단할 수 있는 기능을 제공하게 되는 것이다. 또한 SGS에서는 네트워크 기반의 침입탐지 패턴에 의해 misuse 탐지를 수행하며, 중앙보안제어서버의 HA는 SGSs들에 의해 확실히 침입으로 판명되지는 않지만, Alert Message와 TCP Session Log, Alert Traffic Data, Impact Level별 count 값등의 Data를 사용하여 traffic양의 증대와 같은 경우와 근원지 주소, 목적지 주소등의 정보와 동일 시간대의 접속이

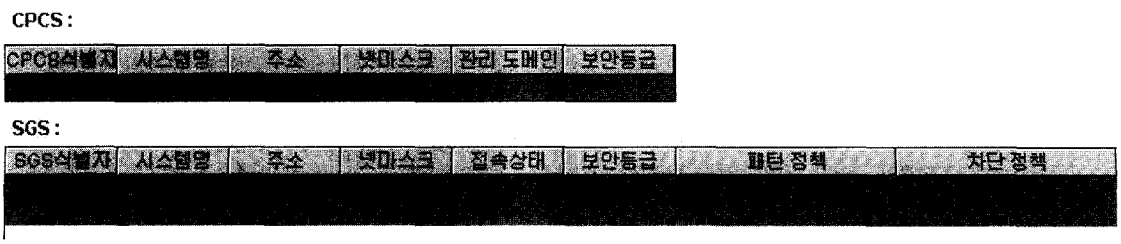


그림 11. 관리자 뷰어에서의 연결된 관리 SGS 대상 정보

갑자기 증가하는 등의 parameter를 이용하여 네트워크상의 잠재적인 불량 사용자/호스트를 기록하고, 정해진 임계치(Threshold)를 넘어서는 보안위협에 대하여 보안수준에 따른 경계경보를 관리자에게 제시하여 네트워크의 안전한 관리를 가능하게 한다. 본 논문에서는 2개의 계층구조로서 보안프레임워크를 구성하였으나, 보안제어서버를 제어하는 최상위 보안제어서버를 통하여 WAN 영역에서도 일괄된 보안정책하에 네트워크를 통하여 유입되고 유출되는 네트워크 패킷에 대하여 침입탐지를 원활히 수행가능하다.

V. 결론 및 향후계획.

네트워크 기반 침입탐지시스템 기술의 핵심은 유입되는 패킷을 유실하지 않고 캡춰링하여, 시도되는 공격에 대하여 적절한 대응을 하는 것이다. 그러나, 네트워크에 유입되는 패킷이 처리할 수 있는 능력보다 많을 경우 네트워크 기반 침입탐지 시스템이 원활히 동작하리라 보장하기는 힘들다. 특히 Gigabit Ethernet등에서 본 시스템을 적용하기 위해서는 본 논문의 내용중 여러 부분이 수정되어야 하지만, 특히 SGS의 Sensor와 관련하여 multi-sensor 구동, Sensor 기능의 Embedded화하는 하드웨어 수준의 패킷의 캡춰링 기술이 해결되어야 한다. 이러한 추가적인 기술을 프레임워크에 적용한다면 기가 이더넷과 백본망에서도 정책기반 네트워크 침입탐지를 원활히 수행하는 프레임워크로 동작할 것이다.

또한 현재는 정의/구현되어 있지 않지만, SGS 시스템에 적용될 여러 컴포넌트에 대해 MIB를 정의하여 보안제어서버상에서 SNMP 프로토콜을 이용하여 구성정보와 상태정보를 얻거나 설정하는 방법이 고려되어야 하며, SGS로부터 보안제어서버로의 경보메시지를 전달할 때 IETF IDWG에서 표준화하고 있는 IDXP와 "IDMEF XML DTD & Data Model"을 지원하는 library의 제공으로 효율적이며 안전한 데이터의 전송을 제공하여야 할 것이다.

참 고 문 헌

[1] CIAO, National Plan for Information Systems Protection. Version 1.0 : An Invitation to a Dialogue. 2000.1

[2] S. Northcutt, M. Cooper, M. Fearnow, K. Fredrick, *Intrusion signature and Analysis.* New Riders. 2001.

[3] Edward G. Amoroso, *Intrusion Detection : An Introduction Internet Surveillance, Correlation, Traps, Trace Back and Response.* Intrusion.Net Books. 2001

[4] Rebecca Gurley Bace, *Intrusion Detection,* Macmillan Technical Publishing. 2000

[5] S. Northcutt, Judy Novak. *Network Intrusion Detection : An analyst's Handbook*^{2nd} *Edition,* New Rider

[6] Terry Escamilla, *Intrusion Detection : Network Security Beyond the Firewall.* Willey computing Publishing.

[7] http://www.darpa.mil/ ITO 및 ISO 문서

[8] http://www.ietf.org/ IDWG 및 Policy Framework 문서

[9] http://www.kisa.or.kr/ IETF IDWG 기술표준동향

[10] J.Betser, A.Walther. GloblaGuard : Creating the IETF-IDWG Intrusion Alert Protocol(IAP), DISCEXII vol 1, 2001

[11] Dinesh C, Verma. *Policy-Based Networking.* New Riders

[12] 안개일, 정책기반 네트워크 관리구조에서 PCIM 정책 전달 방안, NCS 2001

[13] DMTF Specification, white paper CIM Core Policy Model for CIM schema release 2.4, 2000.5.12 http://www.dmtf.org

[14] 윤승용, 보안정책 전달을 위한 COPS-SECURITY 프로토콜, 추계 정보과학회 학술대회, 2001.10

[15] libidmef package library, http:// www.siliconde fense.com/idwg/libidmef

박 상 길(Sang-Kil Park Kim) 정회원

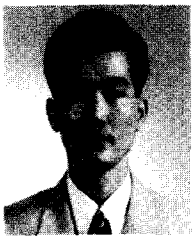
1995년 2월 : 조선대학교 컴퓨터 공학과 공학사

2000년 8월 : 전남대학교 전산학과 이학석사

2000년 7월~현재 : 한국전자통신연구원 연구원 (보안게이트웨이연구팀)

<주관심 분야> 네트워크 보안, 이동코드 보안, 신경망등

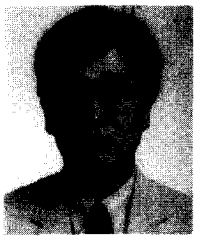
장 종 수(Jong-Soo Jang) 정회원



1984년 2월 : 경북대학교 전자공학과 공학사
1986년 2월 : 경북대학교 전자공학과 공학석사
2000년 2월 : 충북대학교 컴퓨터공학과 공학박사

1989년 7월~현재 : 한국전자통신연구원 책임연구원 (보안게이트웨이연구팀)
<주관심 분야> 네트워크 보안, PBNM, 능동네트워크

손 승 원(Seung-Won Son) 정회원



1984년 2월 : 경북대학교 전자공학과 공학사
1994년 2월 : 연세대학교 전자공학과 공학석사
1999년 2월 : 충북대학교컴퓨터 공학과 공학박사

1991년 8월~현재 : 한국전자 통신연구원 (네트워크보안연구부)
<주관심 분야> 네트워크 보안, 능동네트워크, 생체 인식

노 봉 남(Bong-Nam Noh) 정회원

1978년 2월 : 전남대학교 수학교육과 이학사
1982년 2월 : 한국과학기술원 전산통계학과 이학석사
1994년 2월 : 전북대학교 전산통계학과 이학박사

1983년~현재 : 전남대학교 컴퓨터정보학부 교수
<주관심 분야> 객체지향시스템, 통신망관리, 정보보안, 시스템 및 네트워크 보안 등