대규모 네트워크 환경을 위한 통합 침입탐지 시스템

정회원 안 정 모*, 조 진 성**, 정 병 수*

An Integrated Intrusion Detection System for a Large-scale Network Environment

Jeong-Mo Ahn* *Regular Members*, Jinsung Cho**, Byeong-Soo Jeong* *Regular Members*

요 약

최근 해마다 급증하는 보안 사고를 해결하기 위한 방안으로써, 침입탐지 시스템이 부각되고 있다. 하지만, 현재와 같은 대규모 네트워크 환경에서는 지역적인 침입탐지 시스템으로 다양한 형태의 침입을 탐지하는 데에 많은 문제점을 가지고 있다. 이에 침입탐지 구성 요소들을 분산시키거나 계층적으로 구성하기 위한 연구와 표준화된 통합 프로토콜의 개발 및 침입탐지 시스템들 간에 교환되는 메시지의 표준화된 형식을 정의하는 연구가 활발히 진행되고 있다. 본 논문에서는 이기종 침입탐지 시스템 간의 표준화된 침입탐지 정보 교환을 위하여 표준화된 메시지 형식 및 프로토콜을 사용하며, 통합된 침입탐지 정보들에 대한 상호 연관성 분석을 통하여 보다 효율적인 관리와 분석을 수행할 수 있는 통합 침입탐지 시스템을 설계 및 구현한다. 본 논문에서 제안한 시스템에서는 분산된 침입탐지 시스템들의 효율적인 운용을 위하여 정책 프로파일을 정의·교환하고, 이기종 시스템간의 상호 인증을 위하여 PKI를 이용한다. 이러한 설계를 기반으로 Snort로부터 수집한 침입탐지 데이터를 IDMEF 형식의 메시지로 변환하여 BEEP 기반의 IDXP 프로토콜을 사용하여 송수신하고 이를 다시 통합 판정이 가능한 정보로 변환하기 위한 통합 침입탐지 시스템의 프로토타입을 구현하여 성능을 분석한다.

Key Words : IDS, IDXP, IDMEF, Policy Profile

ABSTRACT

In order to solve the increasing security problems, IDSs(Intrusion Detection System) have appeared. However, local IDSs have a limit to detect various intrusions in a large-scale network environment. So there are a lot of researches in progress which organize the elements of IDS in a distributed or hierarchical manner. In this paper, we design a integrated IDS which exchanges messages between them through the standardized message format (IDMEF) and communication protocol (IDXP). We also propose a policy profile for an effective control of IDSs, and employ the PKI mechanism for mutual authentication. We implement a prototype system for the proposed IDSs communicating with Snort and analyze its performance.

Ⅰ. 서 론

최근 몇 년간 방화벽은 기업의 정보 보안을 유지하는데 있어, 합리적이고 효율적인 보안 솔루션으로 각광 받아 왔다. 하지만 해마다 급증하는 해킹과 보안 사고들에 대해, 관리자들은 더 이상 방화벽에 의지할 수만은 없는 상황에 이르렀다. 이에 따라, 오늘날 차세대 보안을 위한 방안으로 침입탐지 시스템이 주목받고 있다. 침입탐지 시스템은 방화벽이 해킹 되었을 경우 이에 따른 피해를 최소화하고 네트

* 경희대학교 컴퓨터공학과 (jmahn@dblab.khu.ac.kr, jeong@khu.ac.kr)
** 교신저자, 경희대학교 컴퓨터공학과 (chojs@khu.ac.kr)
논문번호 : 040094-0302, 접수일자 : 2004년 3월 2일

워크 관리자 부재 시에 시스템 자체적으로도 해킹 등에 대응할 수 있는 능력을 가짐으로써, 방화벽의 취약점을 효과적으로 보완할 수 있기 때문이다[1].

초기의 침입탐지 시스템에 대한 연구는 하나의 호스트에서 출발하였으나, 인터넷 보급률의 증가에 따라 그 영역을 네트워크로 확장시켰다. 그러나 이들 침입탐지 시스템들은 각각의 개별 호스트나 네트워크 장비에 적합하게 설계되고 적용됨으로써, 스스로 보안의 대상을 제한하고 시스템 자체적으로도 유연성의 한계를 가지게 되었다[11, 12]. 따라서 대규모 네트워크 환경에서 다양한 형태의 침입을 탐지하기 위해, 호스트 혹은 네트워크 기반에서의 감시 및 탐지는 물론, 개개의 시스템이 제공하는 침입탐지 정보의 광범위한 분석을 가능하게 하는 침입탐지 시스템의 개발이 요구되었으며, 이에 따른 고수준의 통신 프로토콜 및 표준화된 메시지 형식에 대한 정의가 필요하게 되었다[6, 18].

이러한 배경으로 DARPA(Defense Advanced Research Projects Agency)에서는 CIDF(Common Intrusion Detection Framework)라는 표준화된 침입탐지 프레임워크에 대한 연구를 시작하게 되었고[6], 최근에 이르러서는 IETF(Internet Engineering Task Force)에 IDWG(Intrusion Detection Working Group)가 결성되어 표준화된 통합 프로토콜의 개발 및 침입탐지 시스템들 간에 교환되는 메시지의 표준화된 형식을 정의하는 연구가 진행되고 있다[7, 8, 9]. 또한 여러 기관들로부터 분산 침입탐지 시스템에 대한 연구가 활발히 진행되고 있지만, 이들 연구의 초점은 침입탐지 요소들을 분산시키거나, 계층적으로 구성하여 탐지의 효율을 높이는 데에 국한되어 있다.

이에 본 논문에서는 침입탐지 기술의 기본적인 개념과 침입탐지 방법에 대해서 살펴보고, 현재 수행되고 있는 다양한 침입탐지 시스템 연구의 문제점을 분석하여 대규모 네트워크 환경을 위한 통합 침입탐지 시스템을 설계 및 구현한다. 본 논문에서 제안하는 통합 침입탐지 시스템은 대규모 네트워크 환경으로 확장이 가능하도록 IETF IDWG에서 제안한 침입탐지 시스템 모델을 기반으로 한다. 또한 이기종의 침입탐지 시스템 사이에 침입탐지 정보를 교환하기 위한 표준 메시지 형식으로 XML 기반의 IDMEF(Intrusion Detection Message eXchange Format)를 사용하고[7, 8], IDMEF 메시지 교환을 위한 프로토콜로써 IDWG에서 제안하고 있는 IDXP(Intrusion Detection eXchange Protocol)를 사용한다[9]. 그리고 본 논문에서 제안하는 통합 침입탐지 시스템은 대규모 네트워크 환경에서의 효율적인 메시지 제어를 위하여 구성 요소 사이에 정책 프로파일을 정의하고 교환하며, 침입탐지 구성 요소들 사이에 공개키 기반구조를 이용하여 상호 인증을 수행함으로써 대규모 네트워크 환경으로의 확장시 신뢰성을 보장한다. 또한 상호 연관성 분석 모듈은 확장 또는 교환이 용이한 구조를 가지며, 이를 통하여 최적의 상호 연관성 분석 기법을 적용함으로써 통합된 침입탐지 정보들의 효율적인 관리와 분석을 가능하도록 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 살펴보고, 3장에서 본 논문에서 제안하는 통합 침입탐지 시스템을 설계한다. 4장에서는 프로토타입의 구현을 통하여 성능 평가를 수행하고 5장에서 결론과 향후 연구 내용으로 끝을 맺는다.

Ⅱ. 관련연구

1. 침입탐지 시스템

침입탐지 시스템(Intrusion Detection System)은 정보시스템 또는 네트워크로부터 보안 관련 정보들을 수집·분석하여 침입 또는 오용을 탐지할 뿐 아니라 침입에 대한 적절한 대응행동을 수행하는 기능을 포함하고 있는 시스템으로 정의 되며[1], 그림 1과 같이 크게 데이터 수집 단계, 데이터의 가공 및 축약 단계, 침입 분석 및 탐지 단계, 그리고 보고 및 대응 단계인 4단계의 구성을 갖는다.

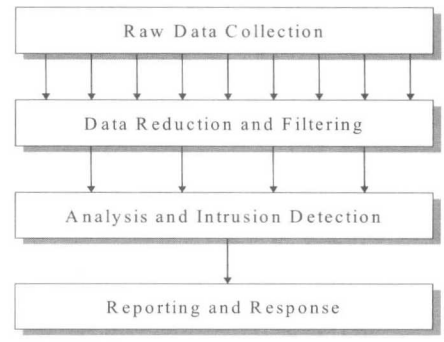


그림 1. 침입탐지 시스템의 구성

한편, 현재 침입탐지 시스템은 보안관리 인프라 구성을 위한 표준 구성요소로서 인식되어 가고 있지만, 침입탐지 시스템의 고속성, 확장성, 연동성과 같은 문제점들을 안고 있다. 이에 따라 분산 구조의 감사

정보 수집을 수행하며, 계층적인 분석 구조를 갖는 대규모 네트워크에서의 침입탐지 시스템에 대한 연구가 시작되었다. 대규모 네트워크상에서는 분산 구조의 감사 정보 수집을 통해 방대한 양의 감사 정보들이 생성되지만, 계층적 분석 구조는 이에 대한 축약을 효과적으로 수행함으로써 분석 효율을 증가시킬 수 있다는 장점을 갖는다. 이러한 형태의 침입탐지 모델을 바탕으로 진행되고 있는 연구에 대하여 살펴보면 다음과 같다.

EMERALD(Event Monitoring Enabling Response to Anomalous Live Disturbance)는 자원 객체에 따라 독립적인 코드 분석을 수행하고 리졸버(resolver)에서 종합 분석을 수행하며, 이를 계층적으로 구현한다. 그리고 스크립트 기반 메시지 인터페이스를 지원함으로써 호환성을 제공하도록 한다[2]. AAFID(Autonomous Agents For Intrusion Detection)는 기존의 침입탐지 시스템에 대하여, 계층적이고 분산된 에이전트의 구조를 가짐으로써 하나의 에이전트가 서비스를 중지해도 다른 에이전트들이 수행을 계속할 수 있도록 하며, 각 에이전트들이 독립적으로 수행되므로 전체의 시스템을 다시 시작해야 하는 번거로움을 해결한다. 또 각 계층에 있는 에이전트들은 수집한 정보를 간단하게 정리하여 상위 계층으로 전달하므로 침입자가 잘못된 데이터를 발생하려는 시도를 할 때 쉽게 감지할 수 있다[3].

GrIDS(Graph-Based Intrusion Detection System)는 호스트들의 행위와 호스트들 사이의 트래픽에 대한 정보를 수집하며, 이러한 정보를 행위 그래프로 수집하는 시스템이다[4]. GrIDS는 네트워크 관리자들로 하여금 사용자들이 호스트들의 특정 서비스를 사용하는 것에 대한 정책 기술을 허가하며, 이에 따른 행위 그래프의 특성들을 분석함으로써 기술된 정책의 위험성을 탐지하거나 보고한다. NetSTAT(Network-based State Transition Analysis Tool)는 STAT(State Transition Analysis Tool)의 도메인 독립적인 핵심 모듈을 사용하여 호스트와 네트워크 기반 공격의 상태천이를 분석할 수 있으며, 보호될 네트워크와 호스트를 구조적으로 표현할 수 있다[5].

이와 같이 다양한 침입탐지 시스템 모델들이 연구되었지만, 대규모 네트워크 환경에서 다양한 형태의 침입을 탐지하기 위해서는 각 시스템이 제공하는 침입탐지 정보의 통합 분석을 통하여 광범위한 분석을 가능하게 하는 통합 침입탐지 시스템이 개발되어야 했다. 이에 CIDF라는 표준화된 침입탐지 프레임워크에 대한 연구가 시작되었다. CIDF는 광범위한 환경에 전개된 침입탐지 시스템들이 서로의 위치를 알아내어 상호 통신할 수 있는 방법을 일치시키기 위해, 이들에 대한 기반 구조로써 침입탐지 컴포넌트의 재사용과 상호 운용을 목적으로 연구되었다[6]. CIDF는 이러한 상호 운용을 위하여 침입탐지 컴포넌트의 구조와 컴포넌트에 표현될 정보를 위한 언어 정의에 초점을 맞추어 연구되었다. CIDF는 메시지 패싱을 통하여 통신하는 분리된 컴포넌트들로 구성되며, 이들 컴포넌트들은 모두 표준 공통 형식으로 기술된 GIDOs의 형식에 맞춰 데이터를 교환한다[18].

2. IETF IDWG 표준화 동향

CIDF의 연구가 모태가 되어 IETF IDWG(Intrusion Detection Working Group)에서는 CIDF의 전반적인 내용을 포함하는 이기종 보안 시스템 연동을 위한 국제 표준을 제안하고 있다. 그림 2는 IETF IDWG에서 정의한 침입탐지 시스템 구성요소들과 그들의 관계를 나타낸다. 경보(alert)는 어떠한 이벤트가 탐지되었을 때, 분석기(analyzer)에서 관리기(manager)로 보내지는 메시지이다. 관리기는 침입탐지 시스템의 각 요소들을 관리하기 위한 침입탐지 구성요소로써, 경보를 받은 관리기는 관리자(administrator)가 설정한 보안정책(security policy)에 따라 운영자(operator)에게 통보하거나 사건에 적절한 대응을 취한다. 분석기와 관리기는 분리된 요소로써 TCP/IP 네트워크로 쌍방향 통신을 한다[7].

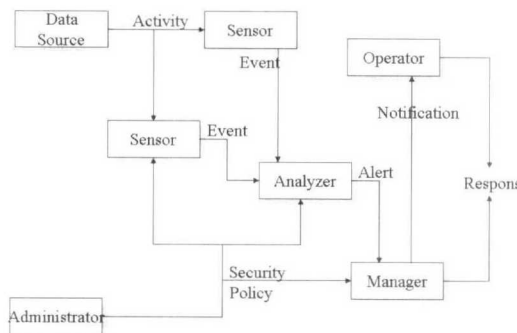


그림 2. IETF IDWG의 침입탐지 시스템 모델

IDWG에서는 침입탐지 및 대응 시스템, 그리고 그들과 함께 상호작용 하는데 필요한 관리 시스템을 위하여, 서로간의 정보를 공유하기 위한 교환 절차와 데이터 형식으로써 IDMEF를 정의하고 있다.

IDMEF는 자동화된 침입탐지 시스템이 스스로 의심스럽다고 생각되는 이벤트에 대해 경보를 보고하는데 사용할 수 있는 표준 데이터 형식이다[8].

또한 IDWG에서는 IDMEF 기반의 XML 경보 데이터를 관리기에게 전송하는 과정에서 BEEP(Block Extensible Exchange Protocol) 기반의 IDXP 프로토콜을 사용한다. IDXP는 상호 인증, 무결성, 기밀성을 제공하는 접속지향 프로토콜로써, 침입탐지 요소들 간에 IDMEF 메시지 및 텍스트와 이진 데이터를 교환하는데 사용된다[9]. IDXP는 그림 3과 같이 접속지향, 비동기적 상호 작용을 위한 어플리케이션 프로토콜 프레임워크인 BEEP 프로파일로 명시되어 있다. 따라서 인증, 기밀성과 같은 요소들은 다른 BEEP 프로파일의 사용을 통하여 제공되며, IDXP의 여러 기능들은 BEEP 프레임워크 내에서 제공된다[10].

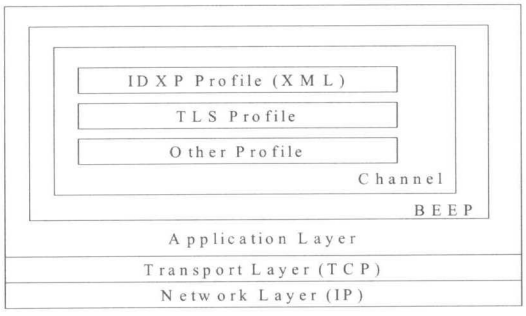


그림 3. BEEP 기반의 IDXP

Ⅲ. 제안하는 대규모 통합 침입탐지 시스템

1. 시스템 모델

본 논문에서는 그림 4와 같이 IETF IDWG의 침입탐지 시스템 모델에 기반하여 분산 침입탐지 시스템으로 확장한다. 이와 같이 침입탐지 구성 요소 사이에 상호 메시지 전송을 통하여 전체적인 표준 침입탐지 시스템 모델을 확장함으로써 대규모 네트워크 환경에서의 확장성과 가용성을 향상시킬 수 있다. 본 논문에서 제안하고 있는 대규모 환경에서의 통합 침입탐지 시스템의 전체적인 구조는 다음과 같다.

그림 4에서 보는 것과 같이 지역적인 침입탐지 시스템 내에서 각각의 침입탐지 구성 요소는 IETF IDWG에서 정의한 동작 방식을 따르며, 관리기는 분석기들의 정보를 바탕으로 침입탐지 결과를 통합 판정한다. 이때, 분석기는 센서로부터 수집된 데이터를 분석하여 경보를 발생하고 이를 IDMEF 형식의 표준화된 메시지로 변환하여 인접한 관리기에게 IDXP 프로토콜을 사용하여 전송한다. 이를 수신한 관리기는 수집된 네트워크 오용탐지와 비정상행위 탐지, 호스트 탐지 결과를 바탕으로 지역 네트워크 수준의 판정을 수행한다.

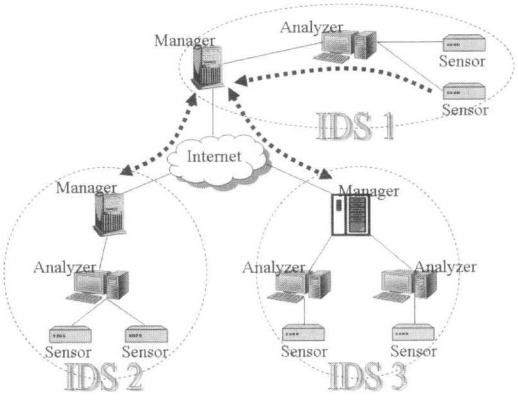


그림 4. 통합 침입탐지 시스템의 구조

또한, 본 논문에서는 지역적인 침입탐지 시스템을 대규모 네트워크 환경에 적합한 구조로 확장한다. 각 관리기는 지역적으로 판정된 침입탐지 정보를 표준화된 IDXP 프로토콜을 사용하여 이웃한 관리기들에게 전송함으로써, 전역 네트워크 수준의 통합 판정을 수행한다. 이러한 구조는 네트워크의 크기가 커지더라도 같은 메커니즘을 적용할 수 있고, 침입대응 및 복구기술과 연계되어 실시간에 이루어지는 침입을 탐지하고 그에 알맞은 대응 정책이 수행되도록 할 수 있다.

그리고, 본 논문에서 제안하고 있는 통합 침입탐지 시스템은 대규모 네트워크 환경에 분산되어 있는 침입탐지 구성 요소들이 수집한 침입탐지 경보에 대해 상호 연관성 분석을 수행하여 경보 메시지의 정확도를 높이고 중복되는 메시지를 제거함으로써 관리자의 관리를 용이하게 한다. 이때, 네트워크에 분산되어 있는 침입탐지 구성 요소에 상호 연관성 분석 엔진을 모듈화 함으로써, 침입탐지 구성 요소별로 적합한 상호 연관성 분석 알고리즘을 적용하며, 다른 모듈과 유기적인 관계를 가지고 동작하도록 설계한다[19, 20].

2. 고려사항

본 논문에서 제안하는 대규모 네트워크 환경을 위한 통합 침입탐지 시스템을 설계하기 위하여 다음과 같은 사항들을 고려해야 한다.

1) 표준화된 메시지 형식

본 논문에서는 대규모 네트워크 환경에서의 통합 침입탐지 시스템을 위한 모델로 3.1절에서 언급한 바와 같이 IETF IDWG의 침입탐지 시스템 모델을 기반으로 한다. 그러므로, 침입탐지 시스템 구성 요소 사이에 침입탐지 정보를 교환하기 위한 표준화된 메시지 형식이 필요하다. 이에 본 논문에서 제안하는 통합 침입탐지 시스템에서는 이기종의 침입탐지 시스템 간의 침입탐지 경보 교환을 위한 XML 기반의 IDMEF 메시지 형식을 사용함으로써, 플랫폼 독립적인 통합 침입탐지 시스템을 구축할 수 있다.

2) 표준화된 통신 프로토콜

대규모 네트워크 환경에 분산되어 있는 침입탐지 시스템으로부터 수집되는 침입탐지 정보를 관리기 사이에 통합하기 위해서는 표준화된 메시지 형식뿐만 아니라, 이들 메시지들의 기밀성과 무결성을 보장할 수 있는 통신 프로토콜도 지원되어야 한다. 이에 본 논문에서 제안하는 통합 침입탐지 시스템에서는 표준화된 메시지 형식의 교환을 위한 프로토콜로써 IDMEF와 함께 표준화로 제시되고 있는 IDXP를 사용하며, BEEP 보안 프로파일과 TLS 프로파일을 통해 기밀성과 메시지 무결성을 보장할 수 있다.

3) 유연성 있는 상호 연관성 분석 기법

대규모 네트워크 환경에서 수집되는 통합 침입탐지 시스템의 경보 메시지는 대량의 경보 메시지를 발생시키거나, 높은 오탐율을 보여 관리자가 이를 즉각 인지하지 못하도록 함으로써 신속한 대응을 어렵게 만들 수 있다. 따라서 본 논문에서 제안하는 통합 침입탐지 시스템에서는 경보 메시지에 대한 상호 연관성 분석을 통하여 탐지 메시지의 정확도를 높이고 중복되는 메시지를 제거한다. 또한 유연성 있는 상호 연관성 분석 모듈을 적재함으로써, 지역의 정책이나 시스템 환경에 맞는 최적의 분석 기법을 적용할 수 있다.

4) 정책 프로파일 정의

대규모 네트워크 환경에서 동작하는 통합 침입탐지 시스템에서는 분산되어 있는 각 침입탐지 구성 요소들이 효율적인 운용을 위하여 필요한 데이터만을 수집함으로써, 무의미한 경보 데이터의 전송을 미연에 방지하고 전체 네트워크에 발생하는 트래픽을 감소시키기 위한 방안이 마련되어야 한다. 이에 본 논문에서는 각 침입탐지 구성 요소들의 요구사항을 만족하는 행위들에 대하여 정책 프로파일로써 사전 정의하고, 각 침입탐지 구성 요소들은 상호 전달되는 정보의 내용이나 전달 방법을 협의하기 위하여 이를 사용한다. 본 논문에서 정의하는 정책 프로파일의 기술 방법은 IDMEF 메시지 데이터 모델의 XML DTD 정의 방법을 이용하며, 정책 프로파일의 내용은 정책 프로파일의 버전, 분석기의 정보, 관리기들에 대한 정보, 이벤트의 출발지 정보, 이벤트의 목적지 정보, 이벤트의 분류 정보, 경보 전송 주기, 이벤트의 평가 정보, 관리기의 상태 정보 등을 통합한다. 이에 대한 상세한 세부 내용은 부록 A에서 정의한다.

5) 침입탐지 시스템 사이의 상호 인증

경보 메시지는 대규모 네트워크 환경에 분산되어 있는 독립적인 침입탐지 시스템 사이에 사용되므로 이들 사이에 신원을 신뢰할 수 있어야 한다. 하지만 이러한 상호 인증은 인증 프로세스가 파괴되거나 구성에 실패할 수 있는 위험이 있기 때문에 기초적인 통신 메커니즘의 인증을 제한해서는 안 된다. 이를 위하여 본 논문에서 제안한 통합 침입탐지 시스템에서는 시스템의 부담을 줄이고 안전한 키 분배를 수행할 수 있는 공개키 인증서를 이용한 방식을 사용한다. 따라서 공인된 인증기관에 의해 신뢰된 침입탐지 구성 요소를 확장하여 대규모 네트워크 환경에서도 신뢰성이 보장되는 침입탐지 시스템을 운영할 수 있다.

3. 세부 모듈 설계

본 절에서는 통합 침입탐지 시스템을 위한 관리기와 분석기의 세부 모듈을 설계한다. 관리기는 그림 5에 보이는 것과 같이 여러 모듈로 구성되어 있다. 세부적으로 정책 프로파일 관리 모듈은 관리기 사이에 교환된 정책 프로파일을 관리한다. 또한 관리기가 관리하고 있는 정책 프로파일의 정보는 다른 관리기에 의한 정책 프로파일의 수신시 정책 프로파일의 버전을 비교하여 정책 프로파일 테이블을 갱신한다. PKI 인증 모듈은 대규모 네트워크 환경에서의 상호 인증을 지원한다. PKI 인증 모듈을 통하여 대규모 네트워크로의 확장시, 침입탐지 정보의 공유를 원하는 침입탐지 구성 요소와 상호 인증을 수행한다.

IDXP 통신 모듈은 관리기나 분석기가 IDXP 프로토콜을 사용하여 통신하기 위한 모듈이다. IDXP 통신 모듈은 BEEP 세션 개설 후에, 보안 프로파일을 협상함으로써 연결을 확립한다. 그리고 BEEP 세션

내부에 침입탐지 요소들 사이에 채널을 개설하기 위하여 IDXP 프로파일을 사용한다. 또한 IDXP 통신 모듈은 어플리케이션 계층 터널과 BEEP 보안 프로파일의 준비를 위한 오버헤드를 방지하기 위하여 데이터가 활발하게 교환되고 있지 않는 동안에도 IDXP 채널을 유지하는 역할을 한다. TLS 암호화 모듈은 IDXP 채널을 통하여 통신하는 침입탐지 구성요소의 기밀성을 제공하기 위하여 메시지의 암호화를 수행한다. IDMEF 메시지 파싱 모듈은 분석기로부터 전송된 IDMEF XML 형식의 메시지를 각각의 원소와 속성으로 분리하는 역할을 수행한다. DB 관리 모듈은 변환된 일반적인 형식의 침입탐지 정보들을 DB에 저장하고, 저장된 DB를 관리하기 위한 모듈이다. 관리기 관리 모듈은 관리기의 상태 정보를 주기적으로 다른 관리기에게 전송하는 역할을 한다. 상호 연관성 분석 모듈은 경보 메시지의 연관성 분석 기법을 적용하기 위한 모듈로써, 관리기가 위치한 지역의 정책이나 관리기의 환경에서 동작시키기에 적합하도록 데이터 마이닝, 확률적 상관 관계 분석, 룰 기반 상관 관계 분석 기법 등의 상호 연관성 분석 기법을 적용할 수 있다[19, 20].

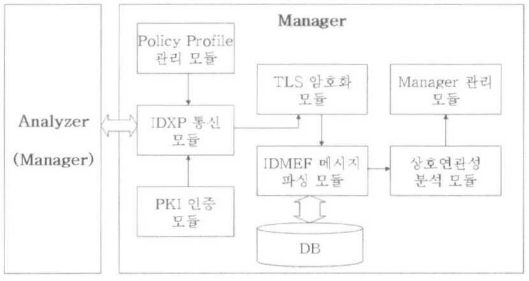


그림 5. 관리기의 세부 모듈

한편, 분석기는 그림 6과 같이 7개의 모듈로 구성되어 있다. Snort 통신 모듈은 Snort가 수집한 로그 정보를 읽어 오기 위한 모듈이다. 정책 프로파일 관리 모듈은 관리기로부터 수신한 정책 프로파일을 기반으로 각각의 관리기에 대한 정책 프로파일 테이블을 생성하고 관리한다. 경보 관리 모듈은 BEEP 세션 내의 분리된 채널을 통하여 경보들을 효과적으로 분리하고, 이러한 경보들을 정책 프로파일 테이블을 참조하여 각각의 관리기들에게 전송한다.

IDMEF 메시지 생성 모듈은 일반적인 형식의 Snort 로그 정보를 IDMEF XML 형식의 메시지로 변환한다. TLS 암호화 모듈은 관리기에서의 TLS 암호화 모듈과 마찬가지로 침입탐지 구성 요소 간의 기밀성을 위하여 메시지를 암호화하는 역할을 수행한다. IDXP 통신 모듈 또한, 관리기에서의 IDXP 통신 모듈과 마찬가지로 침입탐지 구성 요소 간에 IDXP 프로토콜을 사용하여 통신하기 위한 모듈이다. 분석기 관리 모듈은 분석기의 상태 정보를 주기적으로 관리기에게 전송하는 역할을 한다.

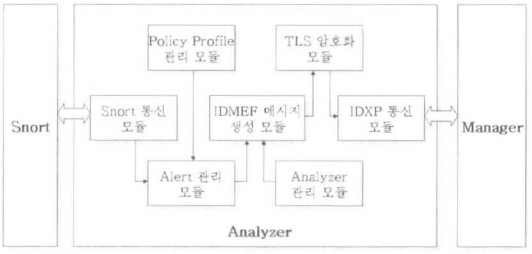


그림 6. 분석기의 세부 모듈

4. 동작 절차

본 논문에서 제안하고 있는 분산 침입탐지 시스템의 전체적인 동작 절차는 그림 7과 같다. 우선 대규모 네트워크 환경의 분산 침입탐지 시스템과 정보 공유를 원하는 침입탐지 구성 요소는 인접한 관리기에게 승인을 요청한다. 이를 받은 관리기는 공개키 기반구조(PKI)를 이용하여 침입탐지 구성 요소의 신원을 확인한 후에 BEEP 세션을 개설하고, 요구되는 보안 사항을 제공하는 보안 프로파일을 협상한다.

그림 7. 통합 침입탐지 시스템의 동작 절차

이러한 과정을 통하여 인증된 침입탐지 구성요소에게 IDXP 프로파일을 교환하여 채널을 생성하고 분산 침입탐지 시스템 전체 관리기에 대한 정책 프로파일을 전송한다. 정책 프로파일을 전송받은 침입탐지 구성 요소는 정책 프로파일 관리 테이블을 생성하고 자신의 지역 정책에 따라 작성된 정책 프로

파일을 다른 관리기들에게 전송함으로써 대규모 네트워크 환경에서 침입탐지 정보를 교환한다.

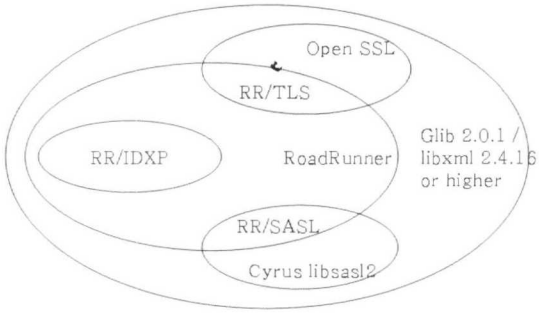


그림 8. RoadRunner 구조

Ⅳ. 프로토타입 구현 및 성능 분석

1. 프로토타입 구현

본 절에서는 3절에서 제안한 통합 침입탐지 시스템의 구현에 대한 내용을 기술한다. 우선, IETF IDWG의 표준 통신 프로토콜인 IDXP의 구현을 위하여 RoadRunner를 사용한다. RoadRunner는 BEEP를 수행하는 어플리케이션 라이브러리로써, C를 기반으로 작성되었다[13, 14].

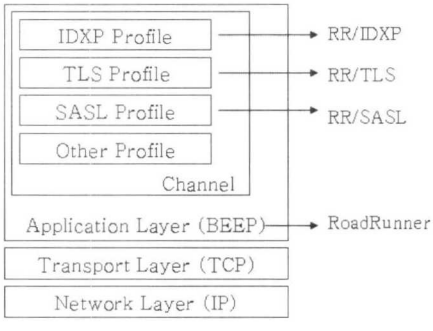


그림 9. RoadRunner 프로파일의 사용

RoadRunner는 강력하고 유연성 있는 BEEP 프레임워크를 제공할 뿐만 아니라, BEEP 프로토콜을 사용하는 네트워크 어플리케이션을 개발하기 위한 유용한 프로파일들을 포함하고 있다. RR/IDXP와 RR/TLS는 RoadRunner를 통하여 생성된 BEEP 채널 상에서 프로파일을 주고 받을 수 있도록 지원하는 오픈 소스 라이브러리이다[15]. 또한, RoadRunner는 RR/TLS, RR/SASL, RR/syslog, RR/IDXP, RR/XMLRPC 등의 라이브러리를 통하여 각종 프로파일을 주고받을 수 있다. 다음 그림 9과 같이 BEEP 채널 생성시에 프로파일들을 상호 교환함으로써 이들 프로파일의 사용을 지원한다.

한편 IETF IDWG의 표준 메시지 형식인 IDMEF를 위해서는 Libidmef를 사용한다. Libidmef는 침입탐지 시스템이 수집한 raw data로부터 IDMEF XML 메시지를 생성하거나 생성된 IDMEF XML 메시지를 파싱하기 위하여, Libxml을 사용하여 C를 기반으로 작성된 라이브러리이다[16].

이러한 라이브러리들을 이용하여 3장에서 설계한 통합 침입탐지 시스템의 프로토타입으로 분석기와 관리기에서의 IDXP 통신 모듈과 TLS 암호화 모듈, IDMEF 메시지 생성·파싱 모듈을 구현하였다. 우선 Snort로부터 수집된 원시 데이터를 분석기의 IDMEF 메시지 생성 모듈에서 IDMEF XML 메시지로 변환하고 이 메시지를 TLS 암호화 모듈과 IDXP 통신 모듈을 통하여 암호화하여 BEEP 세션상의 IDXP 채널로 전송한다[17]. 그리고 관리기의 IDXP 통신 모듈과 TLS 암호화 모듈 통하여 수신된 IDMEF XML 메시지는 IDMEF 메시지 파싱모듈에서 일반적인 형태의 메시지로 변환되어 데이터베이스에 저장된다. 또한 전체 침입탐지 시스템은 각각의 모듈이 유기적인 관계를 가지고 동작하도록 설계되어 있어, 분석기와 관리기의 상호 연관성 분석 모듈은 각 침입탐지 시스템에 최적인 상호 연관성 분석 기법을 적용하여 사용할 수 있다[19, 20]. 본 논문에서 설계한 통합 침입탐지 시스템의 프로토타입을 구현한 분석기와 관리기의 실행 화면은 그림 10과 같다.

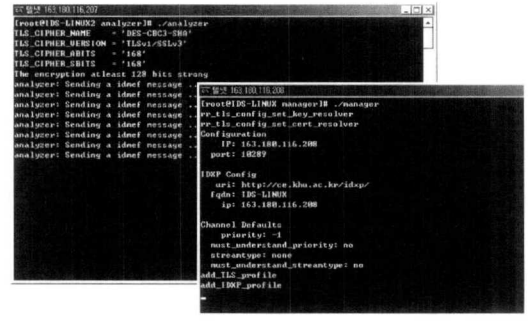


그림 10. 실행 화면

2. 성능 분석

본 논문에서 제안한 통합 침입탐지 시스템의 설계·구현을 통하여 실제 대규모 네트워크 환경에서 얻을 수 있는 기대효과를 알아보기 위하여 다음과 같은 실험을 통한 성능 평가를 수행하였다. 본 논문에

서 제안한 통합 침입탐지 시스템은 3절에서 설계한 바와 같이 상호 연관성 분석 모듈을 통하여 다양한 상호 연관성 분석 기법을 유연성 있게 적용할 수 있고, 각 기법의 장단점으로 인하여 전체 시스템의 탐지율과 경보 메시지의 정확도는 큰 영향을 받게 된다. 따라서 본 논문에서는 정책 프로파일의 도입으로 인한 네트워크 부하 감소에 대한 성능 분석을 실험하였고, 이를 위하여 제안하고 있는 시스템과의 성능 비교를 위한 기준이 되는 시스템으로 분석기가 수집한 정보의 모든 내용을 이웃한 관리기들에게 주기적으로 전송하는 일반적인 분산 침입탐지 시스템을 고려하였다.

본 논문에서 구현한 통합 침입탐지 시스템의 성능 분석을 위하여 Linux Kernel 2.4.18의 운영체제와 100Mbps Ethernet으로 네트워크가 구성된 환경에서 3대의 분석기가 관리기에게 주기적인 경보 메시지를 전송하도록 실험을 수행하였다. 그리고 실제 전송되는 경보 데이터로는 공개 소프트웨어인 Snort 침입탐지 시스템으로부터 생성된 로그 정보를 이용하여 일반적인 분산 침입탐지 시스템에서 송수신될 수 있는 경보 데이터를 생성하였다. 하지만 일반적인 분산 침입탐지 시스템에서는 경보 데이터의 모든 내용을 주기적으로 전송하고, 본 논문에서 제안한 시스템에서는 미리 정의된 정책 프로파일을 통하여 필터링된 정보만을 전송하도록 하였다. 정책 프로파일이 적용된 경보 데이터는 전역 네트워크 수준의 침입탐지 판정을 위하여 중복되거나 무의미한 경보 데이터를 제거함으로써, 평균적으로 일반적인 경보 데이터에 비해 20~30% 정도의 데이터 축약 효과를 보인다. 그리고 두 시스템의 분석기는 모두 IDMEF 형식의 메시지로 변환된 경보 데이터를 무작위로 선택하고 TLS를 이용하여 암호화된 메시지를 IDXP 프로토콜을 통해 전송한다. 전송된 IDMEF XML 형식의 메시지는 다시 일반적인 경보 데이터 형식을 갖는 정보로 변환되어 통합 판정을 위하여 저장된다.

첫 번째 실험에서는 분석기가 앞서 생성된 메시지를 무작위로 추출하여 관리기에게 주기적으로 전송하며 발생할 수 있는 네트워크 트래픽을 측정하였다. 그림 11은 일반적인 분산 침입탐지 시스템에서 발생하는 메시지와 정책 프로파일을 통하여 축약된 메시지를 전송하는 경우의 메시지 크기를 보이고 있다. 본 논문에서 제안하는 정책 프로파일을 통하여 필터링 된 경보 데이터를 전송하는 경우 메시지의 크기가 감소함으로써 네트워크 트래픽이 감소하는 것을 확인할 수 있다.

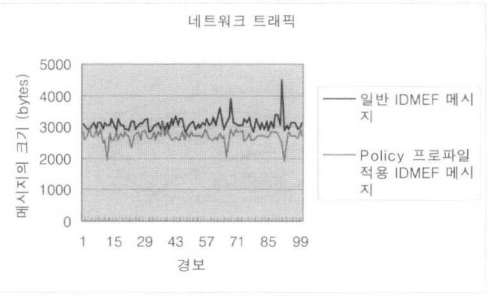


그림 11. 네트워크 트래픽

두 번째 실험에서는 분석기가 관리기에게 일반적으로 발생할 수 있는 IDMEF 메시지와 정책 프로파일 적용으로 축약된 메시지를 전송하는 경우에 나타나는 네트워크 지연시간을 측정하였다. 그림 12는 일반적인 IDMEF 메시지와 정책 프로파일을 적용한 IDMEF 메시지를 전송하는 경우에 나타나는 네트워크 지연시간을 보여 준다. 이처럼 정책 프로파일을 통하여 축약된 메시지를 전송함으로써 메시지 크기의 감소로 인한 IDMEF 메시지의 유효성 검사와 파싱에 필요한 시간 또한 감소하게 되므로, 정책 프로파일을 적용하여 메시지를 송수신하는 경우 네트워크 트래픽과 함께 네트워크 지연시간 또한 감소하는 것을 확인할 수 있다.

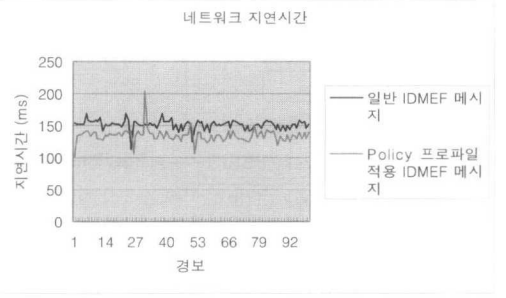


그림 12. 네트워크 지연시간

세 번째 실험에서는 분석기의 수가 늘어남에 따라 발생하는 네트워크 지연시간을 측정하고 평균을 구하여 비교하였다. 그림 13은 3대의 분석기에서 수집된 경보 데이터를 관리기에게 전송하는 환경에서 네트워크 지연시간을 측정한 결과로 분석기의 수가 증가할수록 처리해야 하는 메시지의 수가 증가하므로 평균 네트워크 지연시간 또한 증가한다. 하지만 정책 프로파일 적용을 통하여 분석기의 증가에 따른 네트

워크 지연시간의 증가폭을 줄일 수 있다.

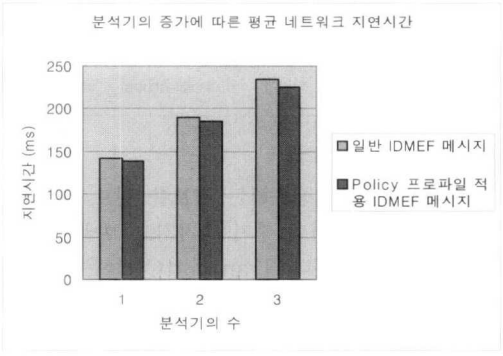


그림 13. 분석기의 증가에 따른 평균 네트워크 지연시간

V. 결론 및 향후 연구 방향

본 논문은 대규모 네트워크 환경에서 침입탐지 정보를 교환할 수 있는 통합 침입탐지 시스템을 설계하고 이를 위한 프로토타입을 구현하였다. 본 논문의 시스템은 분리된 침입탐지 구성 요소가 메시지를 교환하여 침입탐지를 수행하는 IDWG의 침입탐지 시스템 모델을 기반으로 설계함으로써 대규모 네트워크 환경으로의 확장성을 제공한다. 또한 표준화된 IDMEF 형식의 메시지를 IDXP 프로토콜을 사용하여 교환하므로, 이기종 침입탐지 구성 요소 간에 표준화된 침입탐지 정보를 안전하게 교환할 수 있다.

본 시스템에서는 상호 교환되는 침입탐지 정보의 중복이나 무의미한 메시지가 전송되는 것을 미연에 방지하기 위하여 정책 프로파일을 정의하였다. 정책 프로파일을 통하여 침입탐지 구성 요소 간에 전송되는 메시지를 제어함으로써, 침입탐지의 통합 판정에 필요한 의미 있는 정보만을 상호 교환한다. 그리고 공개키 기반구조(PKI)를 이용한 상호 인증을 통하여 대규모 네트워크 환경으로 확장하는 경우에 발생할 수 있는 위장 침입을 방지하였다. 또한 상호 연관성 분석 모듈을 통하여 대규모 네트워크 환경에서 수집한 경보 메시지의 연관성을 분석함으로써 경보 메시지들의 오탐율을 줄이고 정확한 경보를 산출할 수 있다.

그리고, 공개 라이브러리인 RoadRunner를 이용하여 본 논문에서 설계한 통합 침입탐지 시스템을 위한 프로토타입을 구현하였다. 분석기에 의해 수집된 데이터는 표준화된 IDMEF XML 형식으로 변환되고, BEEP에 기반한 IDXP 채널을 통해 상호 교환된다. 이때 IDMEF 형식의 메시지는 TLS를 이용하여 암호화되어 전송되며, 전송된 메시지는 일반적인 데이터 형식으로 변환되어 파일에 저장 된다. 이러한 프로토타입을 이용한 실험 결과, 본 시스템에서는 분석기가 수집한 정보를 정책 프로파일을 통하여 통합 판정에 필요한 의미 있는 정보만을 전송함으로써 네트워크 트래픽과 전송시 발생하는 지연시간이 감소되는 것을 확인하였다.

향후, 본 논문에서 제안한 통합 침입탐지 시스템과 공개 소프트웨어인 Snort를 연동하여 실제 대규모 네트워크 환경에서 침입을 탐지하고, 이러한 침입탐지 정보를 교환하여 관리기에 의해 통합된 정보에 대한 상호 연관성 분석을 통해서 탐지율을 높일 수 있는 방안에 대하여 연구할 계획이다.

부록 A. 정책 프로파일 정의

A.1 정책 프로파일 버전

정책 프로파일의 버전을 정의하고 소유한 정책 프로파일의 버전과 전송 받은 정책 프로파일의 비교를 통하여 최신의 정보를 유지한다. Policy는 Analyzer, Manaer, Source, Target, Classification, Assessment, TransportCycle, ManagerState를 하위 집합으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT policy (
            Analyzer*, Manager*, Source*,
            Target*, Classification*,
            Assessment*, TransportCycle,
            ManagerState
)>
<!ATTLIST policy
            version  CDATA  #FIXED  '1.0'
>
```

A.2 분석기 정보

경보 메시지를 생성하는 분석기가 네트워크 기반인지 호스트 기반인지 에 대한 정보와 같이, 분석기가 분석을 수행하는 방법에 따른 정보를 포함하여 경보를 전송하는 분석기를 제한한다. Analyzer는 Node, Process를 하위 집합으로 갖고 analyerid, model, version, class, ostype, osversion을 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT Analyzer (
            Node?, Process?
)>
<!ATTLIST Analyzer
            analyzerid   CDATA   '0'
            model        CDATA   #IMPLIED
            version      CDATA   #IMPLIED
            class        CDATA   #IMPLIED
            ostype       CDATA   #IMPLIED
            osversion    CDATA   #IMPLIED
>
```

A.3 관리기 정보

침입탐지 시스템 내에 존재하는 관리기들의 유일한 ID를 포함하여 침입탐지 구성 요소들 사이에서 관리기를 구분한다. Manager는 Node, Process를 하위 집합으로 갖고 managerid, model, version, class, ostype, osversion을 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT Manager (
        Node?, Process?
)>
<!ATTLIST Manager
        managerid   CDATA   #IMPLIED
        model       CDATA   #IMPLIED
        version     CDATA   #IMPLIED
        class       CDATA   #IMPLIED
        ostype      CDATA   #IMPLIED
        osversion   CDATA   #IMPLIED
>
```

A.4 이벤트 출발지 정보

분석기가 만들어 내는 경보의 출발지에 관한 정보를 포함하여 자신이 원하는 범위에 있는 경보만을 수신한다. Source는 Node, User, Process, Service를 하위 집합으로 갖고 ident, interface를 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT Source (
        Node?, User?, Process?, Service?
)>
<!ATTLIST Source
        ident       CDATA   '0'
        interface   CDATA   #IMPLIED
>
```

A.5 이벤트 목적지 정보

분석기가 만들어 내는 경보의 목적지에 관한 정보를 포함하여 자신이 원하는 범위의 경보를 제한한다. Target은 Node, User, Process, Service, FileList를 하위 집합으로 갖고 ident, interface를 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT Target (
        Node?, User?, Process?, Service?,
        FileList?
)>
<!ATTLIST Target
        ident       CDATA   '0'
        interface   CDATA   #IMPLIED
>
```

A.6 이벤트 분류 정보

경보의 이름이나 관리기가 그 경보에 대하여 판단할 수 있는 추가적인 정보를 포함한다. Classification은 name, url을 하위 집합으로 갖고 origin을 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ENTITY %attvals.origin
        (unknown | bugtraqid | cve |
        vendor-specific )
<!ELEMENT Classification (
        name, url
)>
<!ATTLIST Classification
        origin   %attvals.origin   'unknown'
>
```

A.7 경보 전송 주기

각 관리기 사이에 전송하는 경보를 경보 발생 즉시 보낼 것인지, 얼마의 주기를 가지고 보낼 것인지에 대한 정보를 포함한다. TransportCycle은 time을 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT TransportCycle
        (#PCDATA)
>
<!ATTLIST TransportCycle
        time   DATETIME   #REQUIRED
>
```

A.8 이벤트 평가 정보

분석기가 보내온 경보에 대하여 지역 관리기가 판단한 이벤트의 영향이나 신뢰 정도를 포함하여 경보의 수신 여부를 판정한다. Assessment는 Impact, Action, Confidence를 하위 집합으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT Assessment
        Impact?, Action*, Confidence?
)>
```

A.9 관리기 상태 정보

분산 침입탐지 시스템에서 정보를 공유하는 모든 관리기들에 대한 정보를 포함한다. ManagerState는 Manager, CreateTime을 하위 집합으로 갖고 ident를 속성으로 갖는다. 이에 대한 XML DTD는 다음과 같다.

```
<!ELEMENT ManagerState (
        Manager, CreateTime
)>
<!ATTLIST ManagerState
        ident       CDATA       '0'
>
```

참 고 문 헌

[1] Dorothy E. Denning, "An Intrusion Detection Model", *IEEE Trans. S.E.*, 1987. 2.

[2] Phillip A. Porras and Peter G. Neumann, "EMERALD : Event Monitoring Enabling Responses to Anomalous Live Disturbances",

Proc. 20th NIST-NCSC National Information Systems Security Conference, 1997.

[3] Eugene Spafford, Diego Zamboni, "New Directions for the AAFID architecture", *RAID 1998*, 1998.

[4] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle, "GrIDS-a graph based intrusion detection system for large networks", *In Proceedings of the 19th National Information Systems Security Conference*, September 1996.

[5] Giovanni Vigna and Richard A. Kemmerer, "NetSTAT : A Network-based Intrusion Detection System", *Journal of Computer Security*, 1999.

[6] Staniford-Chen, S., Tung, B., and Schnackenberg, D., The Common Intrusion Detection Framework (CIDF). *Information Survivability Workshop*, Orlando FL, 1998. 10.

[7] IETF, IDWG, Intrusion Detection Message Exchange Requirements, draft-ietf-idwg-requirements-10.txt, 2002. 10.

[8] IETF, IDWG, Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition, draft-ietf-idwg-xml-09.txt, 2002. 11.

[9] IETF, IDWG, The Intrusion Detection Exchange Protocol (IDXP), draft-ietf-idwg-beep-idxp-07, 2002. 10.

[10] IETF, RFC 3080, The Blocks Extensible Exchange Protocol Core, 2001. 3.

[11] Rajeev Gopalakrishna, Eugene H. Spafford, "A Framework for Distributed Intrusion Detection using Interest Driven Cooperating Agents", *RAID 2001*, 2001. 5.

[12] S. Snapp, J. Brentano and G. Dias et al., "DIDS (Distributed Intrusion Detection System) - motivation, architecture, and an early prototype", *In Proceedings of the 14th National Computer Security Conference*, October 1991.

[13] beepcore.org, http://www.beepcore.org/beepcore/home.jsp

[14] RoadRunner, http://rr.codefactory.se/

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

[16] Libidmef, http://www.silicondefense.com/idwg/libidmef/

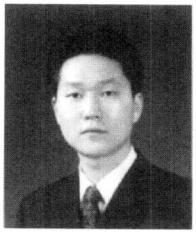
[17] Snort.org, http://www.snort.org/

[18] Clifford kahn, Don Bolinger, Dan Schnackenberg, "Communication in the Common Intrusion Detection Framework v0.7", *CIDF Working Group Draft Specification*, 1998. 6

[19] 이은영, 이상훈, 김도환, 박응기, "침입탐지 경보 메시지 상호 연관성 분석에 대한 연구" 2003년도 추계학술발표회, *한국통신학회*, 2003. 11.

[20] 김도환, 이상훈, 이은영, 박응기, "침입 경보 연관성 분석을 통한 효율적인 관제 에이전트의 설계" 2003년도 추계학술발표회, *한국통신학회*, 2003. 11.

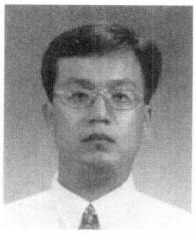
안 정 모(Jeong-Mo Ahn) 정회원



2002년 2월 : 경희대학교 컴퓨터공학과 졸업
2004년 2월 : 경희대학교 컴퓨터공학과 석사
2004년 3월~현재 : (주)엔텔스 기술연구소 연구원

<관심분야> 정보보호, 보안시스템, 데이터베이스

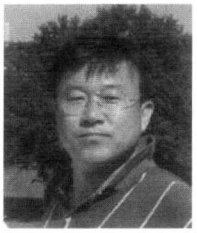
조 진 성(Jinsung Cho) 종신회원



1992년 2월 : 서울대학교 컴퓨터공학과 졸업
1994년 2월 : 서울대학교 컴퓨터공학과 석사
2000년 2월 : 서울대학교 컴퓨터공학과 박사
1997년 4월~8월 : IBM T.J. Watson Research Center Visiting Researcher
1999년 9월~2003년 2월 : 삼성전자 책임연구원
2003년 3월~현재 : 경희대학교 컴퓨터공학과 전임강사

<관심분야> Mobile Computing & Network, Embedded System, Ubiquitous Computing

정 병 수(Byeong-Soo Jeong) 정회원



1983년 2월 : 서울대학교 컴퓨터공학과 졸업
1985년 2월 : KAIST 컴퓨터공학과 석사
1985년~1989년 : DACOM 선임연구원
1995년 2월 : 조지아공대 컴퓨터공학과 박사
1995년~1996년 : Research Scientist, College of Computing, Georgia Institute of Technology
1996년~현재 : 경희대학교 컴퓨터공학과 부교수
<관심분야> Parallel Database, Real-Time Database, Mobile Database