네트워크 침해 조기 탐지 기술 현황 및 발전 방향☆

김 현 우* 정 석 봉* 김 세 헌**

◈ 목 차 ◈

1. 서 론

인터넷의 사용이 급증하면서 국가 경제와 산업에 막대한 가치가 새롭게 창출되었으며, 기존 경제활동 또한 인터넷의 도입으로 인하여 활력과 효율성이 제고되었다. 또한 인터넷의 범용적인 사용으로 인해 컴퓨터에 저장되어 있는 대량의 정보와 각종 기관들의 관리 시스템들이 네트워크로 연결되었다.

이처럼 정보화 사회의 도래로 국가 사회가 전반적으로 정보시스템에 대한 의존도가 심화되고 있는 가운데, 해킹·바이러스 유포, 정보시스템에 대한 불법 침입·마비·파괴, 프라이버시 침해 및 개인정보 오·남용, 인터넷을 통한 범죄행위, 암호기술의 부정사용, 전자거래의 안전·신뢰성 저해, 지적재산권 침해, 불건전 정보의 유통 등 정보화의 역기능 또한 심화되고 있다. 인터넷은 개방성 및 확장성이라는 본질에 의하여 해킹 및 바이러스에 취약할 수밖에 없으며 인터넷 관련 기기, 네트워크, 소프트웨어 등은 보안성이 완벽하지 못하여 위협에 직면하고 있는 것이다. 따라서, 현재의 인터넷과 같은 대단위 네트워크에서는 해킹 및 바이러스에 의한 침해사고에 대응할 수 있는 구조가 제시되어야 한다.

☆ 본 연구는 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었습니다.
* 한국과학기술원 산업공학과 박사 과정
** 국가정보원 국가정보보안협의회 산학연 회장

네트워크 보안 솔루션으로 널리 사용되고 있는 침입차단시스템은 침입이 발생하지 않도록 네트워크의 출입구를 제어하는 기능을 수행하므로 인증을 받지 않은 외부의 접근 시도는 차단할 수 있다고 하지만, 이미 인증된 사용자나 이를 가장한 침입자에 대한 공격에는 취약하다. 특히 내부인 혹은 허가된 외부인에 의해 자주 발생하는 시스템 및 네트워크 침입을 다룰 때에는 침입을 즉각적으로 탐지·대처하는 기술이 필요하다. 침입탐지시스템(Intrusion Detection System, IDS)은 이러한 요구에 부응하는 보안도구로서 정보시스템 혹은 네트워크로부터 보안 관련 정보들을 수집·분석하여 침입 또는 오용을 탐지할 뿐 아니라 침입에 대한 적절한 대응기능을 포함하는 시스템이다 [1].

하지만, 기존의 침입탐지시스템은 갈수록 다양해지는 침입에 대해 능동적으로 대처하는 데 있어 많은 어려움이 있으며, 대규모 네트워크 환경에서의 효율적인 탐지에는 적합하지 않은 구조를 지니고 있다. 따라서 대규모 네트워크 환경에서 다양한 형태의 침입을 탐지하기 위해서는 호스트 혹은 네트워크 기반에서의 감시 및 탐지는 물론이며, 침입 여부에 대한 판정과 더불어 각 시스템이 제공하는 침입탐지 정보의 광범위한 분석을 가능하게 하는 침입탐지시스템의 개발이 요구되고 있다.

본 고에서는 대규모 네트워크 환경에서 효과적인 침입탐지를 가능하게 하는 네트워크 침해 조기 탐지 기술 현황을 알아 보고, 대규모 네트워크에 적합한 침

입탐지시스템의 요구 사항을 고찰해 본다.

2. 침입탐지시스템

침입탐지시스템은 보호하고자 하는 대상 시스템 즉, 침입을 판단하기 위한 데이터를 제공하는 소스에 따라서 네크워크 기반 침입탐지시스템(Network-based Intrusion Detection System, NIDS)과 호스트 기반 침입탐지시스템(Host-based Intrusion Detection System, HIDS)으로 분류할 수 있다 [2]. 침입탐지시스템은 분석 대상에서 추출한 정보를 이용해서 침입여부를 판단하는데, 이때 사용하는 침입탐지방식에 따라서 오용탐지(misuse detection) 방식과 비정상행위탐지(anomaly detection) 방식으로도 나눌 수 있다.

2.1 데이터 소스에 따른 분류

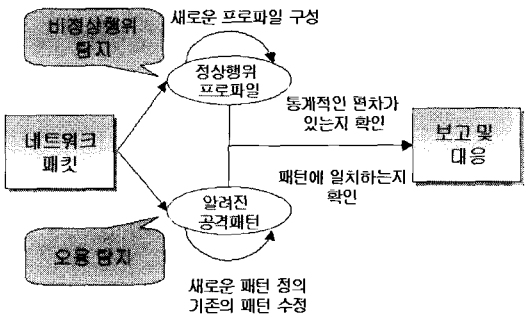
NIDS는 네트워크의 특정 지점에서 여러 호스트를 대상으로 침입을 탐지하기 때문에, 호스트의 운영체제가 하드웨어에 관계없이 동일하게 분석할 수 있는 네트워크 패킷을 분석대상으로 삼는다. 기본적으로 NIDS는 네트워크를 지나가는 모든 패킷을 받아들여서 분석할 수 있는 스니핑(Sniffing)이라는 기술을 사용하기 때문에, NIDS가 설치된 호스트와 관계가 없는 패킷에 대해서도 분석을 하고 침입을 탐지할 수 있다. 이와는 달리, HIDS는 특정 호스트 내부에 설치되는 침입탐지 시스템이다. HIDS는 자신이 설치된 운영체제 내부 시스템의 여러 가지 상태를 모니터링 하다가 특정한 패턴의 행위가 일어나거나 비정상적인 상황이 발생하면 경고를 발생시킨다. 보통 NIDS는 패킷을 검사해서 침입을 탐지하고, HIDS는 시스템 내부 자료를 검사해서 침입을 탐지한다고 생각하면 된다. 위의 두 가지 침입탐지시스템은 설치 위치와 탐지방식이 다르기 때문에 각각의 장단점이 존재한다. NIDS의 경우 하나의 시스템으로 여러 개의 호스트를 보호할 수 있다는 점과 호스트 내부로 공격자가 침투하기 전에 탐지해서 대응할 수 있다는 장점이 있다. 그러나, 네트워크 호스트들이 다양한 운영체제를 사용하는 경우에는 설치하지 못하는 호스트가 생길 수도 있으며, 여러 가지 관리상의 문제가 생길 소지가 HIDS에 비해서 높다는 단점이 있다. HIDS의 경우에는 침입탐지에 사용할 수 있는 분석 대상이 다양하고 특정 운영체제 하나에서만 동작하기 때문에 NIDS에 비해서 상대적으로 정확한 탐지가 가능하며, 즉각적인 대응이 가능하다는 장점을 가지고 있다. 그러나, 시스템 내부에 설치되므로 시스템의 성능을 저하시킬 수 있다는 단점이 있다. NIDS와 HIDS의 특징을 요약하여 비교하면 표 1과 같다.

(표 1) NIDS와 HIDS

항 목	네트워크 기반 IDS	호스트 기반 IDS
탐지 대상	네트워크를 통과하는 패킷	시스템 내부 사용자들의 활동
특 징	기존 시스템 자원에 영향 주지 않음	각 서버의 플랫폼 별로 agent 필요
기반 기술	패킷 캡춰링	프로세스 모니터링
	프로토콜별 패킷 분석	실시간 로그분석
	패킷 조각 모음	TTY 모니터링

2.2 탐지방식에 따른 분류

오용탐지 방식은 알려져 있는 공격행위로부터 특정 시그니처(signature)를 추출해내고 분석 대상에 그런 시그니처가 존재하는지를 확인하여 존재할 경우 침입임을 판단하는 방식이다. 그러므로, 시그니처 목록을 얼마나 최신 버전으로 유지하느냐가 탐지율을 결정하게 된다. 비정상행위 탐지방식은 기존의 네트워크 사용상황을 기반으로 정상적인 행위의 범위를 정해두고 이를 넘어서는 행위를 비정상 행위로 규정하고 탐지하는 방식이다. 통계적인 방법에 기반하는 경우가 가장 많고 다른 방법들도 학계에서 연구가 진행되고 있다. 비정상행위탐지는 오용탐지에 비해서 False Negative 비율이 낮은 반면 False Positive 비율이 너무 높아서 실제 환경에 사용하기가 힘들기 때문에 오용탐지방식의 한계를 극복하기 위해 부분적으로 채용되고 있다. 이렇게 두 가지의 방식을 같이 사용하는 것을 하이브리드 침입탐지시스템이라고 하며 연구와 개발이 진행되고 있다. 그림 1은 비정상행위탐지와 오용탐지가 같이 적용되는 NIDS의 동작을 보여 주고 있다.



(그림 1) NIDS 동작개요

3. 네트워크 침입 탐지 기법

네트워크 침해 조기 탐지를 위해서는 네트워크의 트래픽을 분석하는 일이 선행되어야 한다. 네트워크의 트래픽 분석은 현 인터넷 망의 트래픽 중에서 네트워크 보안 측면에서 이상 상태를 결정짓는 트래픽 또는 트래픽 파라미터를 결정하는 일인데, 트래픽 특성은 인터넷 공격 특성을 분석함으로써 얻을 수 있다. 인터넷 공격들이 야기하는 트래픽 특성을 분석하여 이들을 규명 지을 수 있는 트래픽 파라미터를 정의하고, 정의된 트래픽 파라미터의 정상 상태 프로파일 모형을 구축함으로써 네트워크 침해 조기 탐지를 위한 이상행위 판정 모듈의 알고리즘을 구축할 수 있다.

3.1 네트워크 이상 트래픽 분석

네트워크의 트래픽 분석은 감시 대상인 광역 네트워크에서의 해킹 및 바이러스를 예방하기 위하여 선행되어야 하는 기술이며, 이를 통하여 네트워크 접속점 및 구성 요소에서의 보안 제어 기능이 강화되어야 한다.

일반적으로 네트워크의 공격은 트래픽 기반 공격과 비트래픽 기반 공격으로 구분 지을 수 있다. 트래픽 기반 공격은 네트워크의 안정적 운영에 큰 영향을 미치는 공격으로, 네트워크의 트래픽 양을 폭주하게 만드는 특징을 가지고 있다. 서비스 거부 공격은 트래픽 기반 공격의 대표적인 형태로서 대규모 네트워크 기반의 침입탐지시스템은 이러한 트래픽 기반의 공격으로부터 네트워크를 보호하는 것을 목표로 해야 한다. 반면에, 비트래픽 기반 공격은 특정 호스트의 해킹이나 정보 유출, 시스템 파괴를 목적으로 하며 이러한 공격들은 네트워크 트래픽 양에 영향을 거의 미치지 않는 특징이 있다. 현재의 침입탐지시스템은 주로 비트래픽 기반의 공격 탐지를 수행하고 있다.

대규모 네트워크에서는 기존의 호스트 및 네트워크 기반의 침입탐지시스템보다 사용할 수 있는 정보에 한계가 있다. 기존의 침입탐지시스템에서는 시스템의 로그 파일 및 각 사용자의 행위를 판단하여 이상탐지에 사용한다. 그러나, 광대역 네트워크에서는 각 접속점에서의 패킷 및 플로우의 수, 패킷 헤더 정보, MIB (Management Information Base) 정보 등 사용 가능한 정보의 양이 극히 제한되어 있다. 대규모 네트워크의 침입탐지시스템에서는 이러한 제한된 트래픽 정보로부터 침입행위를 규정 지을 수 있는 트래픽 파라미터를 선정하는 일이 중요하다.

3.2 네트워크의 정상 상태 특성 도출을 위한 기존 연구 방법

이상탐지 시스템의 오탐률을 줄이고 효율적인 이상탐지시스템을 개발하기 위해서는 보다 정확한 네트워크의 정상적인 행위에 대한 프로파일을 구축해야 한다. 기존의 침입탐지시스템에서는 정상상태의 프로파일을 정의하기 위하여 다음과 같은 비정상행위 탐지 기술들이 연구되었다.

□ 통계적 접근(statistical approach)

이 방법은 비정상적인 침입의 탐지를 주로 통계적으로 처리하는 것으로 과거의 통계 자료를 바탕으로 네트워크 트래픽 파라미터를 관찰하여 각 행위에 대한 프로파일을 작성하고, 작성된 프로파일을 통해 비정상 정도를 측정하여 침입 행위를 탐지한다. 통계적으로 잘 연구된 방법들을 사용하여 과거의 경험적인 자료를 토대로 처리하기 때문에 비교적 정확한 탐지가 가능하다고 알려져 있다.

□ 예측 가능한 패턴 생성(predictive pattern

generation)

이 방법은 특정 행위를 이루는 이벤트의 순서가 인식할 수 있는 패턴이라는 가설에 근거하여, 해당 순간까지 발생한 이벤트들을 바탕으로 다음 이벤트를 예측하여 침입을 탐지한다. 시간에 따른 룰을 이용하여 각 이벤트에 시간을 부여할 수 있으며, 룰에 따라 어떤 이벤트들이 순차적으로 발생했다고 가정하면 그 후에 발생할 수 있는 이벤트의 특징과 발생 확률을 예측하여 정상과 비정상 상태를 구분할 수 있다.

□ 신경망 (neural networks)

이 방법은 현재까지 주어진 사용자의 행동이나 명령을 신경망으로 학습시켜서 다음 행동이나 명령을 신경망이 예측하도록 하는 것이다. 신경망은 공격을 추론하거나 설명할 수 없어서 비정상행위 탐지기법으로 많이 연구되고 있는데, 연구 자료의 특성에 의존할 필요가 없으며, 노이즈가 많은 데이터를 잘 탐지할 수 있는 장점을 가진다.

이러한 기존의 연구들은 호스트 및 네트워크 기반의 침입탐지시스템에 특화된 것으로, 아직 전역적인 네트워크 상에서는 그 성능이 검증되지 못하였다. 따라서 네트워크의 각 지점에서 방대한 양의 트래픽을 대상으로 하는 효율적인 이상 탐지 알고리즘이 필요한 실정이다. 대규모 네트워크에서의 침입탐지 기술은 방대한 분량의 데이터를 처리해야 하므로 빠른 처리 속도가 요구되며, 새로운 침입에 대한 능동적 대응이 필요하다.

4. 대규모 네트워크의 IDS 현황

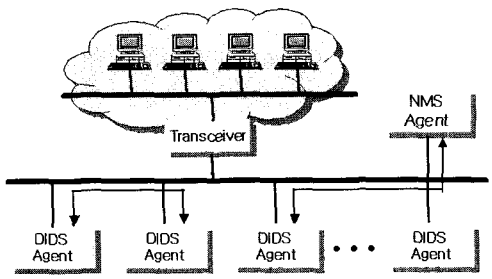
네트워크가 점차 커지고 복잡해지면서 네트워크 기반 침입탐지시스템과 다중 호스트 기반 침입탐지시스템의 관리 및 구현이 어려워지게 되면서 단일 호스트 기반의 침입차단시스템을 통합·관리 할 수 있는 분산 침입탐지시스템(Distributed IDS)이 필요하게 되었다. 분산 침입탐지시스템은 데이터의 빠른 처리속도를 위하여 NMS(Network Management System)와 연동한다 [3].

분산 침입탐지시스템은 방대한 분량의 트래픽 데이터를 효과적으로 처리하기 위해서 트래픽 데이터의 양을 분산적으로 분석하는 방법이다. 그러므로, 한 곳에 트래픽 데이터를 모아서 분석하는 네트워크 기반 침입탐지시스템이나 다중 호스트 기반 침입탐지시스템이 네트워크가 커짐에 따라서 복잡도 또한 크게 증가하는것과 달리 분산 침입탐지시스템은 분산 조정자에 의해 트래픽 데이터를 적절하게 분할하여 분석하기 때문에 네트워크 크기에 상관없이 성능을 일정하게 유지할 수 있는 특징을 가진다.

분산 침입탐지시스템에서의 중요한 기능은 데이터를 효율적으로 분할하고 분석하여 침입행위를 지능적으로 판단하는 능력으로, 뛰어난 침입 판단 능력을 가지기 위해서는 시스템들 간의 협동 능력, 새로운 침입기법에 대한 학습 능력, 뛰어난 확장성 등의 특징을 포함하고 있어야 한다. 이동 에이전트 기술과 멀티 에이전트 기술을 분산 침입탐지시스템에 적용시키면 이러한 조건들을 만족시킬 수 있다. 그러나, 이동 에이전트 기술은 보안상의 문제가 해결되지 않아서 아직까지는 멀티 에이전트 기반의 분산 침입탐지시스템이 더 적절하며, 이동 에이전트의 보안 문제가 해결된다면 이동 에이전트 기반의 분산 침입탐지시스템이 더욱 효과적으로 적용되리라 기대된다 [4].

멀티 에이전트 기반 분산 침입탐지시스템에서의 분산된 호스트 사이에서 각 에이전트들의 협력관계는 그림 2와 같이 나타난다. 네트워크의 전반적인 상황을 체크하고 문제점을 알려주는 기능을 제공하는 NMS는 NMS 에이전트를 통하여 침입 탐지를 위해 오용탐지 방식을 사용한다.

멀티 에이전트 기반의 분산 침입탐지시스템은 쉽게 구성하고 설계할 수 있지만, 새로운 구성 요소를 시스



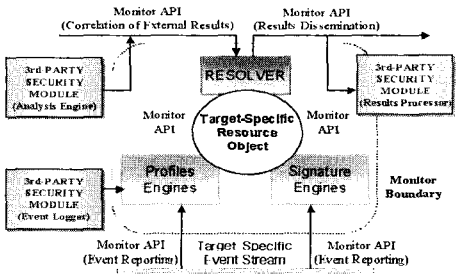
(그림 2) 멀티 에이전트 기반 분산 침입탐지시스템

템의 중지나 재시작 없이 시스템에 적용할 수 있기 때문에 가능한 기술인 동적 재구성 능력의 차이에 따라 그 성능이 크게 달라지는 특징이 있다. 그러므로, 침입탐지 후 빠른 대응을 위해서는 자율적인 판단 능력을 보유하는 것이 가장 중요한 문제로 이 분야에 대한 많은 연구가 진행 중이다.

한편, 미국은 침입을 고의적이면서도 불법적인 시도의 잠재 가능성으로 정의하고 일찍부터 시스템 또는 네트워크 침입탐지 연구에 노력을 기울여 왔다. 특히, DARPA 프로젝트의 일부로서 NIDES의 후속 시스템으로 개발된 EMERALD (Event Monitoring Enabling Responses to Anomalous Live Disturbance)는 네트워크 기반의 침입 분석과 상호 연동성을 증가시키고 분산 컴퓨팅 환경에 맞는 침입탐지시스템 개발을 목적으로 하고 있다. 그림 3은 EMERALD의 시스템 구성도를 나타내고 있다 [5].

EMERALD는 네트워크에 독립적으로 분산되어 있어 있는 모니터를 사용하여 대규모 네트워에서의 비정상 활동을 감지한다. EMERALD는 분산환경에서 실용적인 시스템 구현을 위해 기존의 침입 탐지시스템에서보다 작고 분산적이며 상호 협력적인 구성요소를 채택하는데, 이들 요소들은 계층적인 구조를 이루며 광범위한 네트워크를 감시한다.

EMERALD에서는 이종환경의 특징 기반과 통계 기반 분석을 사용하였는데, 자원 객체에 따른 독립적인 코드 분석과 resolver에서 이루어지는 종합 분석이 계층적으로 구현되었다. EMERALD는 시스템과 네트워크 오용을 분석하고 해석하는 능력을 가지며, 다른 응용 도메인으로 크게 확장할 수 있는 분석 기술을 지원하여 무한한 확장성을 제공한다.



(그림 3) EMERALD 시스템 구성도

(표 2) 계층적 구조의 대규모 네트워크 IDS 특성

시스템	특 성
AAFID	분산 에이전트기반탐지
EMERALD	오용·비정상 통합 탐지 및 계층화
NETSTAT	호스트와 네트워크 IDS 배치 및 공격 시나리오 표현
GrIDS	각 호스트의 행위 관계 그래프 생성

계층적 구조의 침입탐지시스템은 대규모 네트워크 상에서 분산 구조를 통해 얻어지는 방대한 양의 감사 정보를 효과적으로 분석할 수 있는 장점을 가진다. 계층적 구조를 가지는 침입탐지시스템 연구들의 기능적 특성을 요약하면 표 2와 같다.

또, 한편으로는 대규모 네트워크 시스템에 분산되어 있는 멀티 센서 및 다양한 소스들 사이에서 발생한 정보를 결합시키는 기술에 관한 연구도 진행되고 있다 [6]. 데이터 퓨전 기술로 불리는 이 연구는 분산되어 있는 센서들 사이에서 다양한 패킷 스니퍼, 시스템 로그 파일, SNMP 정보, 사용자 프로파일 같은 데이터를 입력 받아서 침입자 및 침입 행위의 확인, 침입 행위의 진단 및 평가 등 을 추정하는 기술이다. 데이터 퓨전 기술은 주로 베이지안 추정등의 방법을 사용하여 각 개별적인 센서들의 분석 결과를 효과적으로 종합 할 수 있으며, 효율적인 전체 네트워크 상황의 분석·진단 뿐 아니라 높은 오탐율을 극복하는 중요한 기술로 각광 받고 있다.

5. 대규모 네트워크에 적합한 IDS 요구사항

5.1 현재 침입탐지시스템의 한계

현재의 침입 탐지 시스템은 대규모 네트워크에 적용되기에는 다음과 같은 한계를 가진다.

□ 단일 시스템에서의 침입탐지 기능만 제공하므로 보안의 대상이 제한됨
□ 시스템 자체에 대한 유연성에 한계가 있으므로 다

양한 형태의 침입에 대해 능동적으로 대처하기 어려움

□ 초고속 네트워크에서 실시간으로 패킷 분석을 수행하는데 한계를 가짐

□ 오용침입에 대한 탐지 기법이 주를 이루고 있어 알려진 공격에 대해서만 탐지가 가능하고 업데이트에 따른 유지 및 관리 비용이 요구됨

5.2 대규모 네트워크를 위한 IDS 요구 사항

현재의 네트워크 보안의 개념은 각 지역망을 개별적으로 보호하는데 초점이 맞추어져 있어 사고를 미연에 방지하기 어렵다. 또한, 분산 서비스 거부 공격과 같은 특정 유형의 공격들은 특정 호스트를 목표로 하기 보다는 네트워크 인프라스트럭처 자체에 대한 공격을 시도하여 네트워크의 안정적 운영을 위협하고 있다. 따라서 이러한 위협들을 조기에 탐지하고 대응하는 네트워크 수준의 이상 탐지 기술이 요구된다. 대규모 네트워크에서의 효과적인 침입탐지를 위해서는 다음과 같은 연구들이 선행되어야 한다.

□ 네트워크 트래픽 특성 연구

방대한 양의 네트워크 데이터를 처리하기 위하여 트래픽 파라미터를 결정하고 수집하는 기술은 향후 대규모 네트워크를 위한 침입 탐지 시스템의 핵심 요구사항 중 하나이다. 이를 위해 다음의 기술들이 연구되어야 할 것이다.

- 네트워크 침해 트래픽 분석에 관한 연구
- 네트워크 패킷 수집 및 분석 기술에 관한 연구

□ 대규모 네트워크를 위한 침입 탐지 및 공격 방지 기술

실시간 침입 탐지 기술 및 네트워크 침해 행위의 자동적 방어 기술이 요구된다. 이를 위해 다음의 연구들이 수행되어야 한다.

- 계층적이고 분산된 시스템 설계를 위한 멀티 에이전트의 작업 환경에 관한 연구
- 멀티 에이전트들의 침입 탐지 협력 기술에 관한 연구
- 광대역 네트워크를 위한 고속 이상 탐지 알고리즘 개발에 관한 연구
- 침입 행위 경보 전달 기술에 관한 연구
- 다량의 경보들의 alert correlation에 관한 연구
- 다양한 침입 패턴 인지 기술에 관한 연구
- 침입 행위에 대한 자동적 방지 기술에 관한 연구

□ 빠른 대응 및 능동적 방어 기술

네트워크에 대한 침해가 발생하였을 때 피해를 최소화하고 침해 행위에 대한 능동적 방어를 수행하기 위한 연구가 요구된다. 이를 위해서 다음의 연구들이 수행되어야 한다.

- 자동 경계 및 경보 발생 기술에 관한 연구
- 네트워크 자동 보호 기술에 관한 연구
- 침해 유형 분석 기술에 관한 연구
- 네트워크 침해 정도를 파악하고 진단할 수 있는 기술에 관한 연구
- 침해 시스템 격리 매커니즘에 관한 연구
- 실시간 대응 및 시스템 복구 기술에 관한 연구
- 공격 근원지 역추적 기술에 관한 연구
- 대량의 트래픽 발생시 버퍼 제어 기술에 관한 연구

이 밖에도 네트워크 공격으로부터 시그너처를 획득 및 분석하는 기술, 사후 처리를 위한 공격 행위의 증거 획득 기술 등도 요구된다.

6. 결 론

빠른 속도로 발전하고 있는 통신 환경에 적응하기 위해서 고성능의 처리능력을 가지는 침입탐지시스템이 요구되고 있다. 특히, 최근의 특정 유형의 공격들은 네트워크 인프라스트럭처 자체에 대한 공격을 시도하여 네트워크의 안정적 운영을 위협하고 있으며, 단일 시스템에 대한 공격에 비해 천문학적인 피해 규모를 발생시킨다. 따라서 본 고에서는 여러 침해 대응 기술 중에서 침입탐지시스템에 대해서 알아 보고, 현재 대규모 네트워크에서의 침입탐지시스템 현황에 대해서 살펴 보았다. 또한 향후 대규모 네트워크를 위한 침입탐지시스템 요구 사항을 제시하였다.

참고문헌

[1] Dorothy E. Denning, "An intrusion-detection model", IEEE Transactions on Software Engineering, v.13 n.2, p.222-232, Feb. 1987.

[2] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems", Computer Networks, 31, pp. 805-822, 1999.

[3] X. Qin, W. Lee, L. Lewis, and J. B. D. Cabrera, "Integrating intrusion detection and network management", Network Operations and Management Symposium, pp. 329-344, April 2002.

[4] M. C. Bernardes, and E. S. Moreira, "Implementation of an Intrusion Detection System based on Mobile Agents", Proceedings of International Symposium on Software Engineering for Parallel and Distributed Systems, pp. 158-164, 2000.

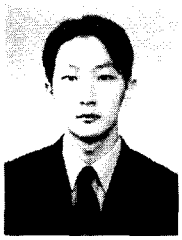
[5] P. A. Porras, and P. G. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", Proceedings of the 20thNational Information Systems Security Conference, October 1997.

[6] T. Bass, "Intrusion Detection systems and Multi-sensor Data Fusion", Communication of the ACM, vol. 43, No. 4, pp. 99-105, April 2000.

◐ 저 자 소 개 ◑

김 현 우

1999년 한국과학기술원 산업경영학과 학사
2001년 한국과학기술원 산업공학과 석사
2001년~현재 한국과학기술언 산업공학과 박사과정



정 석 봉

1999년 한국과학기술원 산업경영학과 학사
2001년 한국과학기술원 산업공학과 석사
2001년~현재 한국과학기술원 산업공학과 박사과정

김 세 현

1972년 서울대학교 물리학과 학사
1977년 스탠포드대학교 물리학과 석사
1981년 스탠포드대학교 OR 박사
1982년~현재 한국과학기술원 산업공학과 교수
2003년 한국정보보호학회 회장
2003년~현재 한국PKI포럼 이사
2004년~현재 국가정보원 국가정보보안협의회 산학연 회장