침입탐지 기술의 현황과 전망

성균관대학교 김병구 · 정태명

1. 서 론

인터넷의 발전은 데이터 전송 속도의 고속화, 대용량의 데이터 전송 등을 가져와 업무 효율을 향상시키고 생활의 질을 높여주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 거두고 있는 반면, 인터넷 확장으로 인한 외부인의 시스템 불법 침입, 중요 정보의 유출 및 변경 · 훼손 · 불법적인 사용, 컴퓨터 바이러스 및 서비스 거부 등 역기능들이 날로 증대되어 피해 규모가 심각한 수준에 이르고 있다. 특히, 컴퓨터 시스템의 침해 사고가 국내 · 외에서 빈번히 일어나고 있는 지금, 이에 대한 대응책이 어느 때보다 절실히 요구되고 있다[1]. 이러한 대응책의 중심은 암호화 및 복호화 기술과 시스템 보안 기술의 개발이며, 정보보호를 위한 시스템 보안 관련 기술은 크게 그림 1에 나타난 바와 같이 분류할 수 있다. 특히, 이러한 기술 중의 하나인 침입탐지 기술은 침입차단 기술과 함께 안전한 정보화 환경 구축을 위해 주목받는 기술 중의 하나가 되고 있다.

본 논문에서는 초기의 단일 호스트 혹은 단일 환경 하에서의 침입탐지에 대한 기존 연구를 소개하고 현재 진행되고 있는 침입탐지 기술의 연구 현황과 개발 방향들을 살펴보고자 한다. 또한 침입탐지 시스템의 다양한 기능과 이의 활용법을 제시하고, 타 보안 기법과의 연동을 통한 응용 기법들을 제시한다. 마지막으로 외부인의 시스템 불법 침입, 중요 정보의 유출 및 변경, 컴퓨터 바이러스 및 서비스 거부공격 등의 정보 침해 행위에 대응하고, 보다 안전한 정보 보호를 도모하기 위한 수단으로써의 침입탐지 기술 응용 분야들을 예시하고, 이러한 침입탐지 기술의 전망에 대해서 언급한다.

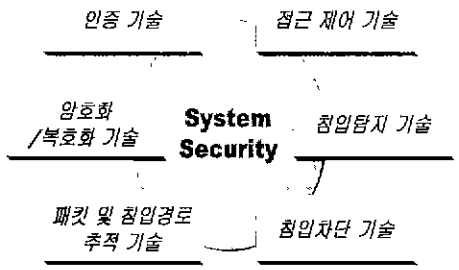

그림 1 시스템 보안 관련 기술

본 논문의 구성은 다음과 같다. 2장에서 침입탐지 기술의 기본적인 분류와 기능들을 살펴보고, 일반적인 침입탐지 구조와 현재의 침입탐지 기술 연구 현황을 보인다. 3장에서 침입 탐지 기술의 확장 기법과 침입탐지 시스템의 응용 분야를 예시하고 4장에서는 결론 및 향후 침입탐지 시스템의 전망을 제시한다.

2. 침입탐지 기술의 현황

침입은 정보 접근, 정보 조작, 시스템 무력화 등 대상 시스템에 대한 고의적이면서도 불법적인 행위로 정의할 수 있으며, 침입탐지 시스템은 이러한 침입을 목적으로 특정 시스템에 불법적으로 접속하여 시스템을 사용, 오용, 남용하는 것을 감지하고 문제점을 처리하는 시스템이라 정의하고 있다[1,6]. 즉, 침입탐지 시스템이란 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨

어를 말한다. 본 장에서는 이와 같은 침입탐지 시스템의 기본적인 침입탐지 기법과 기능을 분류하고, 일반적인 침입탐지 시스템의 구조를 설명한 후, 이를 바탕으로 현재의 침입탐지 시스템 연구 현황을 기술한다.

2.1 기존 침입탐지 기법의 분류

기존의 침입탐지 기법에 대한 분류는 탐지 방법을 중심으로 이루어지는 침입탐지 모델 기반으로 분류하는 방법과, 탐지 영역을 중심으로 분류하는 데이터 소스(data source) 기반의 분류 방법으로 크게 나눌 수 있다[1,2].

표 1 침입탐지 모델 기반의 분류

	침입 탐지 기법 종류
비정상적인 침입 탐지 기법	통계적인 방법 (Statistical Approach)
	특징 추출 (Feature Selection)
	예측 가능한 패턴생성 (Predictive Pattern Generation)
	행위 측정 방식들의 결합 (Anomaly Measures)
	신경망 (Neural Network)
오용 침입 탐지 기법	조건부 확률 (Conditional Probability)
	전문가 시스템 (Expert System)
	상태 전이 분석 (State Transition Analysis)
	키-스트로크 관찰 (Keystroke Monitoring)
	모델에 근거한 탐지 (Model-based Detection)
	패턴 매칭 (Pattern Match)

침입탐지 모델 기반의 분류는 침입탐지 방법에 따라 비정상적인 침입탐지 기법과 오용 침입탐지 기법으로 나뉠 수 있으며, 표 1은 이의 세부 분류를 보인다[1,2,8]. 침입탐지 모델은 침입 탐지 시스템 개발에 있어 요구되는 침입 패턴 분석과 유형별 분류 및 탐지 방법 등을 연구함에 있어 많은 기초 정보들을 제공한다[4].

데이터 소스 기반의 분류는 데이터 소스의 종류에 따라 호스트 기반과 네트워크 기반의 침입탐지 시스템으로 분류될 수 있으며, 각기 다른 종류의 침입유형을 탐지하게 된다. 그림 2는 데이터 소스에 따른 분석 정보들을 간략히 보여주고 있다. 호스트 기반의 침입탐지는 시스템 로그 정보와 특정 행위에 대한 감사 자료 분석 등 시스템 내부에서 생성되는 정보에 대한 분석을 통하여 침입을 탐지하며, 네트워크 기반의 침입탐지는 네트워크 상의 패킷 헤더 및 데이터를 분석하거나 패킷 트래픽 량을 분석하여 침입 유무를 판단한다.

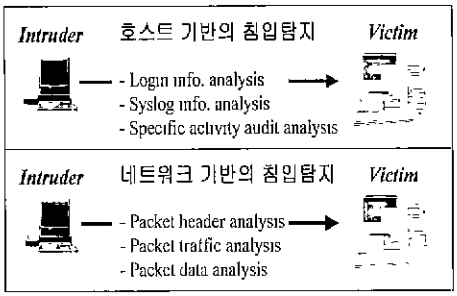

그림 2 데이터 소스 기반의 분석 방법

2.2 침입탐지 기능의 분류

일반적인 침입탐지 기능은 크게 실시간 침입탐지 및 대응 기능, 새로운 침입 패턴 생성 기능, 침입탐지 정보에 대한 통계적인 분석 기능으로 분류할 수 있으며, 이러한 기능들을 활용함으로써 보다 향상된 시스템 및 네트워크 보호를 도모할 수 있다.

2.2.1 실시간 침입탐지 및 대응 기능

침입탐지 시스템은 네트워크를 통한 서비스 거부 공격, 웹 관련 CGI 버그를 이용한 공격과 시스템 내의 버퍼 오버플로우, 중요 시스템 파일 변경, race condition 유발 등의 오용 또는 비정상적인 행위에 대한 침입탐지를 수행하며, 이에 대한 실시간 탐지와 대응이 중요시된다. 침입탐지 시스템은 데이터 소스와 탐지 모델에 따른 분석을 수행하며, 이에 대한 결과를 보고하게 된다. 침입탐지 결과는 일차적으로 사람에게 직접 보고하고 대응하는 것이 정확하나, 이는 자동화된 대응 방식에 비해 느리고, 침입이 일어난 당시에 즉각적인 대응을 하기에 힘든 단점이 있다. 따라서 침입탐지 결과에 대한 효율적이고 자동적인

대응 방식이 요구되며, 메일이나 시스템 콘솔 또는 웹 인터페이스 등과 같은 다양한 방식으로 수행될 수 있다[5].

2.2.2 새로운 침입 패턴 생성 기능

침입탐지 시스템은 시스템이나 네트워크로부터의 데이터 수집과 분석을 통하여 새로운 침입 패턴의 생성을 가능케 하며, 비정상적인 행위들에 대한 패턴을 분석함으로써, 자동적인 침입 패턴을 생성할 수 있다. 이는 기존에 알려지지 않은 침입이나 새로운 침입 패턴에 능동적으로 대처할 수 있도록 하여, 보다 안전한 시스템 보안을 제공하게 된다[6].

2.2.3 침입탐지 정보에 대한 통계적인 분석 기능

침입탐지 시스템은 수집된 감사 데이터로부터 다양한 통계 생성 및 침입 시도 정보, 침입 행위 종류 등에 대한 일별, 주별, 월별 등의 통계 정보 제공을 통하여, 침입탐지 시스템의 정보를 보다 명료하게 사용자에게 전달하는 기능을 수행한다. 가령, 특정 호스트나 특정 서비스 등에 대한 침입탐지 정보를 통계적으로 분석 제공하여 외부나 내부의 침입으로부터 취약한 부분들을 점검할 수 있다. 즉, 침입탐지 정보에 대한 직관적인 통계 정보는 안전한 시스템 관리 정책 설정에 활용될 수 있다.

2.3 일반적인 침입탐지 시스템의 구조

침입탐지 시스템은 수집 정보에 대한 분석을 통해서 침입 유무를 판단하며, 그림 3은 이의 수행을 위한 침입탐지 시스템의 일반적인 구조를 나타내고 있다. 정보 수집기(Event Collector)는 호스트나 네트워크로부터 데이터를 수집하며, 수집된 데이터는 특정 침입탐지 모델을 적용하여 분석된다. 분석 결과는 웹이나, 시스템 콘솔, 메일 등 다양한 방법에 의해 관리자에게 보고되고, 이에 따라 적절한 대응이 이루어지게 된다.

침입탐지 모델을 적용한 수집 정보의 분석은 시스템 설정(Configuration)과 패턴 생성기(Pattern Generator)에 의해서 생성된 패턴 데이터베이스(Pattern DB) 설정에 따라 정보 분석기(Event Analyzer)에서 수행된다. 분석된 결과는 로그 저장소(Log Storage)에 저장되며, 이벤트 보고기(Event Reporter)를 통해 해당 관리자에게 보고된다. 이와 같은 침입탐지 시스템의 구조는 데이터 소스 기반에 따라 다시 세부적으로 구분될 수 있다.

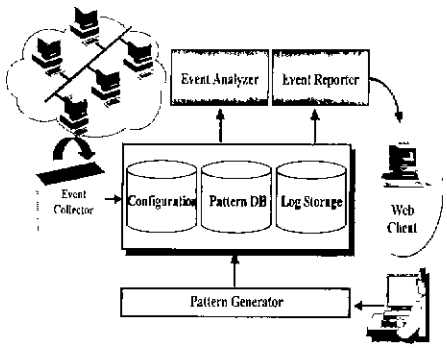

그림 3 일반적인 침입탐지 구조

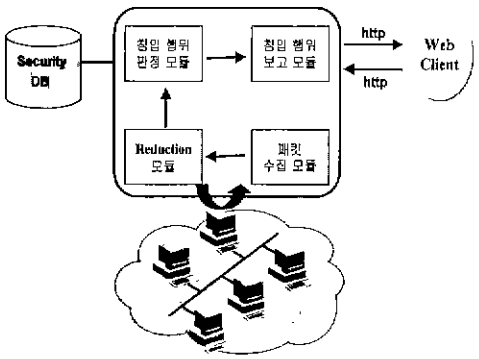

그림 4 네트워크 기반의 침입탐지

그림 4는 네트워크 기반의 침입탐지 구조를 보이며, 이는 크게 패킷 수집과 Reduction 모듈, 침입행위 판정 모듈, 침입 행위 보고 모듈로 나뉜다[1]. 패킷 수집과 Reduction 모듈은 네트워크 상의 패킷을 수집하고 축약함으로써, 침입행위 판정 모듈의 부하를 줄여주며, 분석 결과는 침입행위 보고 모듈에 의해 해당 관리자에게 보고된다.

그림 5는 호스트 기반의 침입탐지 구조이며, SunOS에서 제공하는 BSM(Basic Security Module)을 예로 보인다[2]. BSM은 호스트에서 발생하는 각종 이벤트에 대한 감사 기록을 생성하고 관리하며, Audit Class, Audit Control,

Audit User에 의해서 설정된 감사 레코드를 생성한다. 생성된 감사레코드에 대한 필요 정보 추출 과정을 통해서 해당 이벤트에 대한 침입 유무를 판정하게 된다.

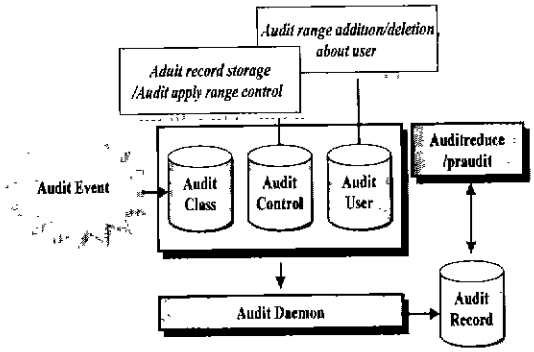

그림 5 호스트 기반의 침입탐지(BSM)

2.4. 침입 탐지 기술의 연구 동향

표 2에서 보는 바와 같이 1980년경부터 지금까지 국내외적으로 여러 종류의 침입 탐지 시스템들이 개발되었거나 개발되고 있다. 이러한 침입 탐지 시스템의 구체적인 예로 그림 6에서 보이는 NIDES(Next-generation Intrusion -Detection System)는 연구 개발과정에서 산출된 단일 환경 하에서의 대표적인 침입탐지 시스템의 예라 할 수 있다[10]. NIDES는 1980년대에 SRI International의 Computer Science Laboratory에서 개발된 IDES(Intrusion Detection Expert System)의 확장형이며, 통계 알고리즘을 이용한 비정상적 행위탐지 기법과 알려진 침입 형태에 대한 전문가 시스템을 적용하는 오용 침입탐지 기법 모두를 이용하고 있다. SRI는 네 개의 NIDES 소프트웨어 프로토타입을 개발하고, 이의 기능성과 성능을 지속적으로 향상시켜왔다. 현재 NIDES 프로토타입 시스템은 구성요소의 재사용과 구성을 용이하게 하는 형태를 지닌 시스템으로 평가받고 있으며, 이러한 기술은 시스템 보안 향상에 계속적으로 공헌하고 있다.

그러나, 기존의 침입 탐지 시스템이나 프로토타입들은 일반적으로 단일 시스템 환경에 적합하게 설계되고 적용되었으므로 대규모 네트워크로의 확장에 어려움을 가지게 되었다. 이는 각각의 시스템들이 지닌 독자적인 메시지 처리 방식에

표 2 기존의 침입탐지 시스템

침입탐지 시스템	시스템의 개발자	특징 및 기능
NIDES	SRI International	IDES를 기반의 전문가 시스템
EMERALD	SRI International	진산망에서의 오용 탐지
STAT	Porras	상태 전이를 이용한 시스템
MIDAS	NCSA	오용 침입탐지 시스템
IDIOT	Purdue Univ	전문가 시스템
GrIDS	UC Davis	활동 그래프를 이용한 시스템
NADIR	Los Alamos National Lab.	전문가 시스템
Real-Secure	ISS	네트워크 기반의 시스템
Omniguard /ITA	AXENT	에이전트 기반의 시스템
AAFIDS	Purdue Univ	에이전트 기반의 시스템
NeoWatcher	(주)인젠	네트워크 패킷 모니터링 및 분석
RT-IDS	성균관대학교	네트워크 기반의 실시간 시스템
MH-IDS	진남대학교	호스트 기반의 시스템

기인하며, 이러한 문제를 극복하기 위해서 제각기 다른 기존 시스템들을 재 사용할 수 있는 침입 탐지 시스템 프레임워크의 개발이 요구되고 있다. 따라서 전체적으로 통합된 침입탐지 전략을 세우기 위해서는 침입탐지 기법의 확장 및 서로 다른 방식으로 얻어지는 정보들에 대한 통합과 정제가 필요하며, 이에 따른 침입탐지 응용간 통신 프로토콜에 대한 정의가 필요하다. 이는 현재의 네트워크 관리 시스템들을 기반으로 하여 확장되어질 수도 있으며, 침입탐지 시스템에 적합한 공통 메시지를 정의함으로써 이루어질 수 있다. 이 밖에도 장애 허용과 극복(fault tolerant and recovery) 등에 대한 연구를 통해 대규모 네트워크에 적합한 침입탐지 시스템으로의 확장

이 고려되어야 한다.

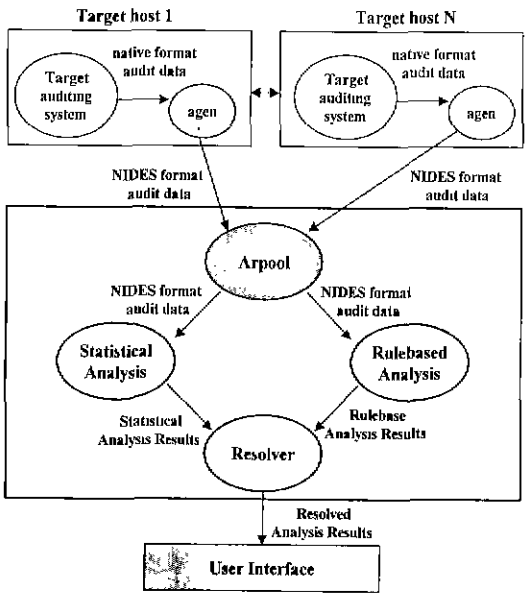

그림 6 NIDES의 침입탐지 수행도

현재 SRI, UC Davis 등에서 연구 중인 CIDF(Common Intrusion Detection Framework)는 복잡한 구조를 지닌 대규모의 네트워크 환경에서 적용될 수 있는 침입탐지 시스템 설계와 구현을 위한 다양한 접근 방법을 시도하고 있다[16,20] 이는 DARPA(Defence Advanced Research Projects Agency)의 지원 하에서 개발 중이며, 침입탐지와 관련하여 DARPA에 의해 지원된 연구들과 시스템들이 서로 상호 동작하도록 하는데 기본적인 목적을 두고, 침입탐지 시스템을 구성하는 요소들이 지닐 수 있는 가능한 모든 역할들을 정의하고 있다.

CIDF는 상호 협력하는 침입탐지 및 대응 시스템들에 대한 프레임워크를 디자인하기 위해 요구되는 사항들을 제시하며, 대규모 네트워크 환경에서의 침입에 적절히 대처하기 위해 침입탐지 시스템들이 서로 협력하는 방식을 보여준다. 상호 협력하는 침입탐지 및 대응 시스템이란 두 개 이상의 침입탐지 및 대응 시스템들이 자동으로 서로의 데이터를 교환하고, 이를 통해서 단일 시스템에서 도달하기 어려운 결과를 도출할 수 있는 시스템을 의미한다. 시스템간의 상호 협력은 구성과 정보 표현 및 시스템간의 상호 포용력 여부 등의 다양한 측면이 고려된다. 침입탐지 및 대응 시스템이 상호 협력하기 위해서 정의되어지는 언어는 침입과 관련된 내용을 포용력 있게 표현할 수 있어야 하며, 기술된 언어의 의미를 정확하고 단순하게 기술할 수 있어야 한다. CIDF는 이러한 공통 언어의 사용 요구에 대해서 "S-Expression"을 제안하고 있다[17].

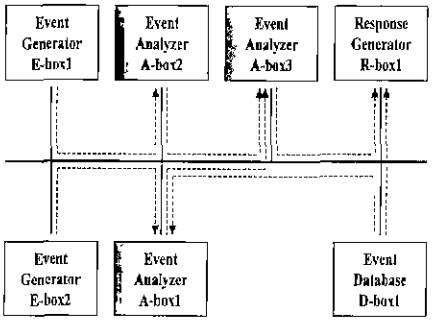

그림 7 대규모 네트워크에 적합한 침입탐지 시스템 연구의 예(CIDF)

CIDF는 현재 지속적으로 연구되고 있으며, 연구 결과를 이후 표준으로 제정하기 위해서 Internet Engineering Task Force(IETF)와의 공동 수행을 진행 중이다. 이러한 CIDF에 대한 연구가 가지는 가장 중요한 의미는 기존의 침입탐지 시스템들이 지닌 구성요소들을 재 사용하고, 그림 7에서처럼 서로 다른 종류의 구성요소들이 서로 통신할 수 있는 인터페이스를 정의한다는 것이다. 현재, 침입탐지에 대한 많은 연구 결과와 시스템들이 개발된 것은 사실이나, 서로 다른 환경을 기반에서 다양한 탐지 기술들로 구성된 개개의 침입탐지 구성요소들을 어느 곳에서나 쉽게 적용한다는 것은 어렵다. 따라서 CIDF의 연구는 더욱 값진 연구로써 평가받는다.

이처럼, 기존의 단일 시스템 혹은 단일 환경에서의 침입탐지 시스템들이 지닌 한계를 극복하고, 대규모 네트워크에 적용 가능한 침입탐지 및 대응 시스템의 상호 수행과 관련된 연구는 서로 다른 침입탐지 기법들과 침입정보를 표현하기 위한 공통적 표기 및 공통 언어에 기반을 둔 수행에 관심을 갖는다. 침입탐지에 대한 공통적인 표기법에 대한 연구는 여러 연구기관에서 지속적으로

진행되고 있으며[18,19], 이러한 공통 표기를 기반으로 한 상호 협력적인 보안 모니터링에 대한 연구로는 NIDES[10], EMERALD[11], GrIDS[12], AAFID[13,14] 등의 시스템 개발 그룹에서 진행되고 있다.

그러나, 이와 같은 침입탐지 시스템 연구들은 대규모의 하부구조를 지닌 네트워크에서의 정보 수집과 분석이 각각의 전담 시스템에서 수행되는 경우가 많고, 이에 따른 부하 집중이 문제시된다. 설령, 대등적인 위치에서 정보를 교환한다고 하더라도 개개 침입탐지 시스템에 대한 접근 통제가 용이하지 않고 제공되어야 하는 정보의 정의가 미흡하다는 단점을 갖는다. 따라서 기본적인 침입탐지는 개별적으로 수행하되, 대규모 네트워크 상에서의 분산적이고 협력적인 침입 형태를 탐지하기 위한 침입탐지 시스템들 간의 효율적인 정보 교환 구조에 대한 고려가 필요하다.

3. 침입탐지 기술의 확장 및 응용

본 장에서는 안전한 정보 보호를 도모하기 위해서 다양한 보안 메커니즘을 접목하는 침입탐지 기술의 확장 기법들을 제시하고, 침입탐지 기술이 효율적으로 이용될 수 있는 응용 분야들을 살펴본다.

그림 8에서와 같이 침입탐지 기술은 네트워크 보안, 혹은 시스템 보안을 목적으로 활용될 수 있다. 전자는 네트워크 트래픽의 모니터링과 감시를 통한 패킷 분석은 해당 네트워크의 보안 기능을 강화시켜주며, 후자는 특정 시스템의 이벤트 모니터링과 감시를 통하여 시스템 내의 불법 사용과 유해 행위를 점검할 수 있도록 한다. 이는 침입탐지 시스템을 이용해서 제공될 수 있는 보안 기능을 보여주며, 이러한 침입탐지 기능들은 다양한 보안 메커니즘과 접목됨으로써 보다 강력한 정보 보안 수준을 제공할 수 있게 된다.

3.1. 침입탐지 기술의 확장

네트워크를 통한 시스템 침투 기법은 정당한 사용자의 권한을 훔쳐 접근하는 패킷 스니퍼링, CRACK과 같은 개인 도용, 운영체제나 응용 프로그램의 오류를 이용하여 침입하는 sendmail 공격이나 NFS 공격과 같은 취약성공격, 정당한 호스트로 위장하여 인증 없이 불법 접근하는 파

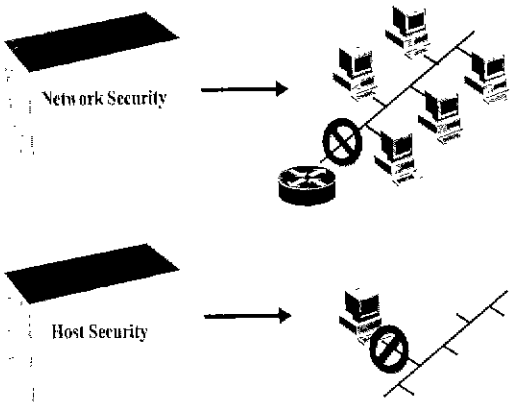

그림 8 침입탐지 시스템의 기능 및 활용

일변조를 통한 공격 외에도 시스템이나 프로토콜의 구조적 결함을 공격하는 IP Spoofing과 같은 수법, 시스템의 정상적 서비스를 방해하는 우편폭탄(mail bombing)등 그 공격법이 매우 다양하다. 이와 더불어 초기의 단순한 침투 기법은 정보 통신의 발전과 더불어 시스템 침투 기법도 고도화되고 전문적으로 발전해 가고 있으므로 이에 대응하는 침입 탐지 기법들도 그 복잡성을 더해가고 있다. 이처럼 다양한 침입 행위에 대해서 침입탐지 기술은 침입한 당시에 침입 사실을 정확하게 파악할 수 있어야 하며, 해당 관리자가 올바른 조치를 내릴 수 있도록 실시간으로 보고할 수 있는 기능을 갖추고 있어야 한다. 동시에 침입에 대한 효과적인 탐지와 차단은 타 기법들이 추구하는 침입 예방 기술을 접목함으로써 보다 전체적인 보안 강화를 제공할 수 있게 된다. 이를 위해 제안되는 침입탐지 기술의 확장 방법으로 침입차단 시스템과의 연동과 TCP wrapper와의 연동을 통한 서비스 접근 제어를 들 수 있다.

3.1.1 침입차단 시스템과의 연동을 통한 접근 제어

흔히 방화벽으로 불리는 네트워크 침입 차단 시스템은 해당 네트워크의 보안 정책에 따라 인가된 인터넷 서비스와 호스트에 대한 접근은 허용하되, 인가되지 않은 서비스와 호스트에 따르는 트래픽을 철저하게 막음으로써 효율적인 보안 서비스를 제공한다. 물론 방화벽 시스템을 구현하는 것이 해당 네트워크의 보안을 완전하게 보장하지는 않지만, 네트워크 단위의 보안 유지를 위해 가장 효과적이고 비용이 비교적 적게 드는

방법이기 때문에, 많이 도입되고 있다. 침입 차단 시스템을 통한 접근 제어는 네트워크의 보안 사고나 위협이 더 이상 확대되지 않도록 막고 격리하는 기술이며, 특히 내부 네트워크를 보호하기 위해서는 외부에서의 불법적인 트래픽이 들어오는 것을 막고, 허가하거나 인증된 트래픽만 허용하는 적극적인 방어 대책이라고 할 수 있다. 따라서, 침입 차단 시스템을 통하여 네트워크 사용자에게 가능한 한 투명성을 보장하면서 위험 지대를 줄이고자 하는 적극적인 보안 대책을 제공할 수 있다.

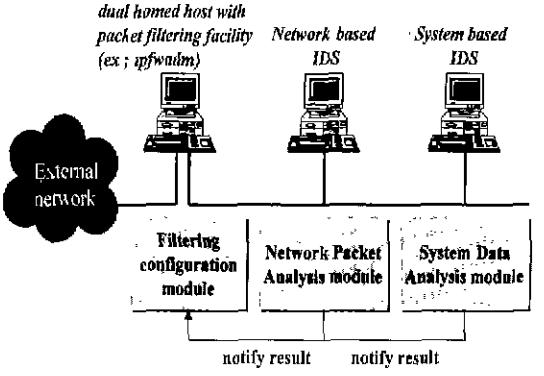

그림 9 방화벽과의 연동을 통한 접근제어

인터넷에서의 다양한 침입 형태에 대한 탐지 및 차단은 일관된 정책 구현과 침입 탐지 기술의 확장을 통해 보다 구체화 될 수 있다. 이러한 보안 체계의 현실화를 위해서는 정보 보호 시스템, 즉 네트워크를 통한 침입의 탐지와 차단 기능이 상호 적절히 도움을 줄 필요가 있다. 현재 침입 탐지 시스템들의 침입탐지 결과에 대한 일관적이지 못한 대응 방법들에 의해 네트워크 침입에 대한 일관적이지 못한 정책을 유발하기 쉽다. 따라서 침입 탐지와 이의 대응에 대한 일관성 있는 보안 정책의 적용을 위해 방화벽 등에서 제공하고 있는 침입 차단 기능을 응용할 수 있다. 이를 통해 방화벽 시스템을 이용한 침입탐지 기술의 확장은 새로운 유형의 침입에 대해 유연성 있는 대응을 제공하며, 네트워크상의 정보 보호를 위한 합리적인 보안 정책 설정과 적용을 도모할 수 있다. 즉, 현재의 침입 탐지 시스템과 침입 차단 시스템이 지닌 기능을 서로 접목시킴으로써, 보다 안전하고 유연성 있는 보안 유지 기능의 제공이 가능하다.

그림 9는 침입탐지 시스템과 방화벽 사이의 연동을 통한 접근제어 기법의 예를 보이고 있으며, 이는 침입탐지 시스템에서의 침입탐지 결과를 방화벽의 패킷 필터링과 프락시 정책에 반영함으로써, 외부의 침입에 대해 보다 능동적으로 대처할 수 있는 구조를 갖도록 한다.

3.1.2 TCP-wrapper와의 연동을 통한 접근 제어

TCP-wrapper는 시스템 서비스 접근을 제어하고 모니터링하기 위한 단순하면서도 효율적인 도구이다. 이는 내부로의 시스템 트래픽을 제어하고 모니터링 하는 도구로써, 외부의 침입으로부터 시스템을 보호하는데 성공적으로 이용될 수 있다. 무엇보다도 TCP-wrapper는 어떠한 소스 코드의 변경 없이 유닉스 시스템에 설치될 수 있다는 장점을 가지며, 방화벽과는 달리 특정 시스템에 대한 접근제어 기능을 제공한다.

그림 10은 침입탐지 시스템과 TCP- wrapper 간의 연동을 통한 침입탐지 기술의 확장을 보이며, 침입탐지 시스템에서의 침입탐지 정보를 TCP wrapper의 접근 제어 정책에 적용시킴으로써, 외부의 침입에 대한 능동적이고 간단한 대응을 제공하게 된다.

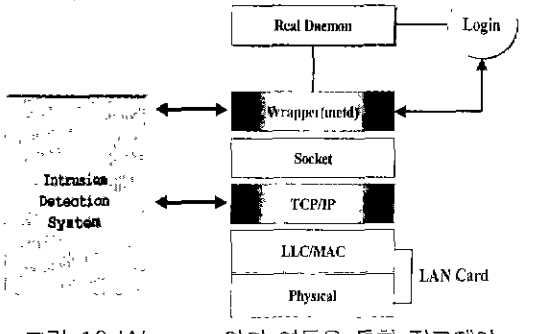

그림 10 Wrapper와의 연동을 통한 접근제어

3.2. 침입탐지 기술의 응용 분야

침입탐지 기술은 개인 정보 등이 외부의 침입에 의해 유출되거나 파괴되는 것을 보호하기 위한 수단으로써, 안전한 정보 보호를 위해 여러 분야에서 응용될 수 있다. 그림 11은 정부기관, 금융기관, 교육기관, 민간기업 등과 같이 정보 보호가 요구되는 단체들뿐만 아니라 전자상거래의 활성화에도 침입탐지 기술이 사용되어질 수 있음

을 도식적으로 나타내고 있다.

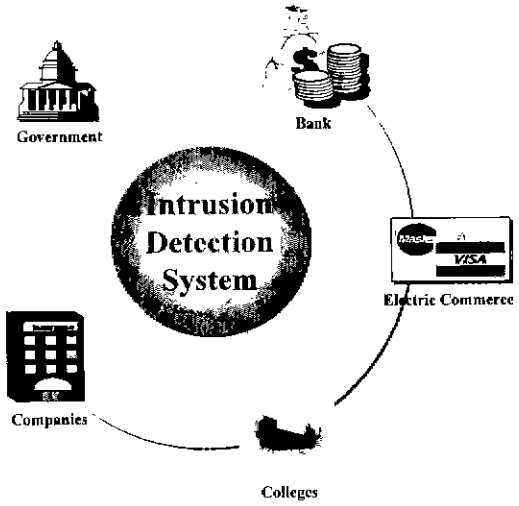

그림 11 침입탐지 시스템의 응용 분야

3.2.1. 전자상거래에서의 응용

침입탐지 기술은 인터넷 모범 상점 인프라의 중요 부분에 적용되어 인터넷의 패킷 정보 뿐 아니라, 사용자의 행위, 통계적인 시스템의 변화 등을 고려하여 침입 여부를 판단하게 되고, 이미 설정된 대응 정책에 따라 적절한 대응 행위를 취하게 된다.

그림 12는 전자 상거래를 형성하는 상점과 고객의 재정을 담당하는 금융기관에 설치된 침입탐지 시스템을 보여주고 있다. 일반적으로 침입의 형태는 인터넷 상점의 전산자원을 고갈시키는 서비스 거부 행위(Denial of Service), 정보를 탈취하거나 파괴, 변조하는 행위 등으로 나타나게 되는데, 대부분의 경우 이러한 침입의 행위가 복합적으로 이루어진다. 가령, 인터넷 상점 내부 시스템에 침입하여 개인 정보를 습득하여 네트워크를 통해 자신의 시스템으로 옮겨 놓고 자신의 침입 사실을 은닉하기 위해서 시스템 파일을 변조하거나 삭제하는 경우가 그 예이다.

침입탐지 시스템은 침입 상황에 대한 실시간 경보, 침입 통계 작성 및 탐지된 침입에 대응하는 기능을 가지며, 이를 통해서 안전한 전자상거래를 도모할 수 있다. 인터넷은 정보의 변조, 도용, 탈취 등의 침입에 항상 노출되어 있으므로 사실상 전자상거래는 범죄의 위험 속에서 실현되는 행위로 볼 수 있기 때문에 보안의 중요성은 더욱 강조되고 이를 간과하고는 결코 전자상거래의 활성화를 기대할 수 없다.

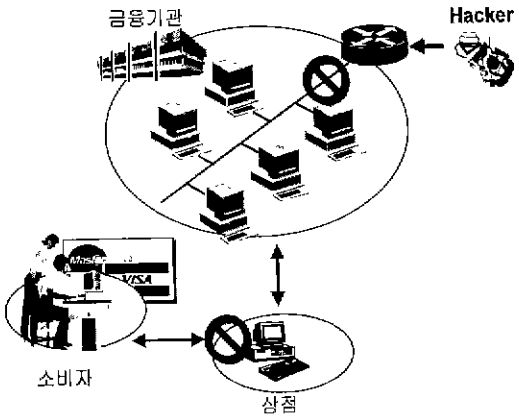

그림 12 전자상거래에서의 응용 예

3.2.2 기타 분야에서의 응용

인터넷으로 전세계가 하나의 가상공간이 되어가고 경쟁은 갈수록 치열해지며, 모든 분야에서 최고만이 살아남는 현실을 생각해 볼 때 정보보호에 대한 중요성은 더 이상 간과되어서는 안될 중요 사안이다. 정보보호 산업은 그 규모가 기하급수적으로 늘어나고 있고, 국가기관 및 사회 기반 구조가 모두 정보화 되어 앞으로는 더욱더 정보보호에 대한 수요가 증가할 것으로 예상된다.

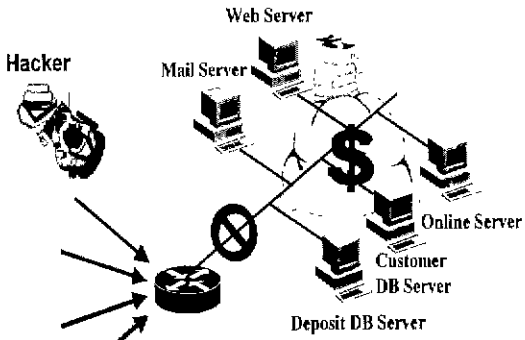

그림 13 금융기관에서의 응용 예

그림 13에 나타난 것처럼, 금융기관의 중요 데이터 서버들을 보호하기 위해 설치된 침입탐지 시스템은 예금 관련 데이터베이스의 감시와 고객 정보의 유출 방지, 웹서버 등 사내 전산자원의 불법사용 여부를 판단하게 되고, 설정된 대응 정

체에 따라 적절한 대응을 취하게 된다.

그림 14는 대학 및 기타 교육기관의 전산자원을 보호하기 위해 설치된 침입탐지 시스템을 보여주고 있으며, 학적 데이터베이스의 감시, 연구자료들에 대한 불법적인 유출 방지, 학내 시스템에 대한 유해 행위 등을 탐지하고, 탐지 결과에 대한 적절한 대응을 취하게 된다.

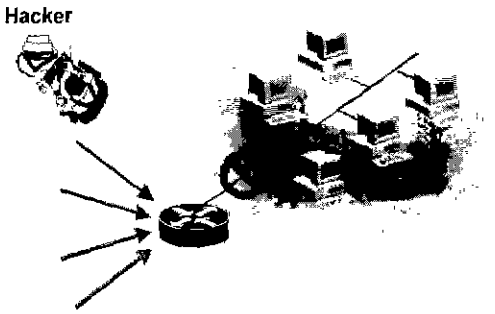

그림 14 교육기관에서의 응용 예

이외에도 침입탐지 기술은 서비스 거부공격, 금융사기, 바이러스 등의 수많은 정보 침해 유형에 적절히 대응하기 위해서 기타 여러 분야에서 응용될 수 있으며, 인터넷으로 대변되는 정보화 사회를 보다 안전한 공간으로 만들고, 활성화시킬 것으로 전망된다.

3.2.3 대규모 인프라 넷에서의 응용

인터넷의 특징 중 하나는 분산 환경에서의 네트워크를 이용한 원거리 응용 서비스가 다양하게 제공된다는 것이며, 이러한 분산 환경의 확대는 자연스럽게 정보 시스템들에 대한 보안 관리 문제를 제기하였다. 즉, 모든 데이터가 한곳으로 집중되는 예전의 메인 프레임 환경에서와 달리 대규모의 데이터와 시스템이 분산되어 있으므로, 관리 대상의 시스템과 정보가 대량화, 다양화되었다. 따라서, 대규모의 전산망에 있어서 단일 시스템이 전체적인 보안 관리를 수행한다는 것은 불가능하며, 부분적인 보안 관리나 일률적인 관리 방식으로는 더 이상의 보안 유지가 어렵게 되었다. 따라서, 대규모 전산망을 부분적으로 관리하고 있는 시스템들이 서로 협력할 필요성이 제기되었으며, 그림 15는 이러한 대규모 인프라 넷에 분산되어 설치된 침입탐지 시스템들을 보여주고 있다.

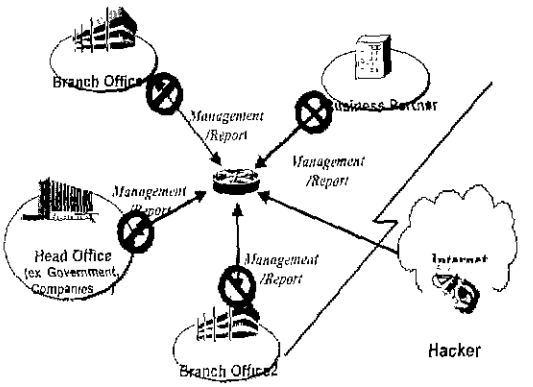

그림 15 대규모 인프라 넷에서의 응용 예

시스템 및 네트워크의 정보를 보호하기 위해서 많은 회사들이 여러 가지 방법들을 동원하고 있으며, 지사나 협력회사와의 정보 교환은 보다 많은 보안을 요구한다. 가령 산업스파이에 의한 회사 기밀의 유출은 심각한 정보 침해의 유형으로써 자사에 큰 타격을 입힐 수도 있다. 따라서 정보 침해 행위를 탐지하고 대응할 수 있는 침입탐지 기술이 응용된다면, 어떠한 사업이라도 보다 안전하게 시도될 수 있을 것이다.

4. 결론 및 향후 전망

본 논문에서는 초기의 단일 호스트 혹은 단일 환경 하에서의 침입탐지에 대한 연구를 바탕으로 현재의 침입탐지 기술 연구 현황과 개발 방향들을 살펴보았다. 또한 다양한 침입탐지 기능과 타 보안 기법과의 연동을 통한 확장 기법들을 살펴보고, 침입탐지 기술이 적용될 수 있는 여러 응용분야들을 제시하였다.

초기의 네트워크 환경에서는 네트워크 및 시스템에 대한 호기심과 영웅심으로 시스템에 침입하였으나, 현재는 정보의 불법 유출에서부터 사이버테러의 목적에까지 다양한 공격 형태를 이루고 있다. 더구나 갈수록 늘어나는 인터넷, 연동되는 인터넷 링크의 증가와 함께 네트워크가 고속화함에 따라 침입 경로가 다양해지고, 지능화되고 있어서 공격 수법의 분석과 추적 등이 어려워지고 있다. 이처럼 네트워크 상에서의 침입 시도는 해가 갈수록 증가되고 다변화되고 있으며, 악의적인 사용자들에 의한 독창적이고 새로운 침입 방

식의 개발은 침입 탐지에 대한 어려움을 증가시키고 있다. 따라서, 최근의 침입탐지 시스템의 동향 및 경향은 글로벌 네트워크에서의 상호 협력을 추구하고 있으며, 이를 통해서 탐지할 수 있는 침입 유형 및 이로써 얻어지는 장점 등이 주논의 대상이 되고 있다.

인터넷 같은 다양한 정보통신의 발달로 정보통신 시스템 사용자들은 많은 혜택을 받아 업무를 쉽게 처리할 수 있는 반면, 시스템 구현상의 오류나 사용자의 실수, 사용에 대한 무지 등으로 인한 중요 정보의 누출, 파괴, 위조, 변조로 금전적 피해와 정신적 피해를 입는 경우가 종종 발생하고 있다. 정보화 사회에서 정보는 곧 자신의 재산이며, 이는 보안이라는 도구를 사용하여 위험부담을 줄임으로써 상대적으로 가치를 높일 수 있는 것이다. 따라서 침입탐지 기술은 현대 정보화 사회에서 필수적인 요소이며, 침입차단 기술이나 기타 정보 보호 기법들과 더불어 정보 보호의 중요한 수단이다.

현재의 침입탐지 기술은 인터넷의 팽창에 따라 대규모 네트워크 환경에 적합한 기법들이 요구되고 있으며, 이에 따른 고려사항들이 지속적으로 논의되고 있다. 즉, 이후의 침입탐지 기술은 무엇보다도 급변하는 인터넷 환경에 적용할 수 있어야 하며, 보다 간편한 보안 관리 기능을 제공할 수 있어야 한다. 또한, 시스템과 네트워크에 부하를 줄이면서 모든 이벤트를 모니터링 해야만 하며, 스위칭 환경으로의 기반 기술 변화를 수용할 수 있어야 한다. 이러한 고려 사항들은 향후 침입탐지 기술 연구에 커다란 영향을 미칠 전망이다.

참고문헌

[1] 한국정보보호센터, 실시간 네트워크 침입탐지 시스템 개발에 대한 연구, Dec., 1998.

[2] 한국정보보호센터, 멀티호스트 기반 침입탐지 시스템 개발에 대한 연구, Dec., 1998.

[3] 정보통신부, 정보시스템 침해사고 방지기술 개발에 관한 연구, Jan., 1999.

[4] 한국정보보호센터, 침입 탐지 모델 분석 및 설계, Sep., 1996.

[5] 한국정보보호센터, 대규모 전산망에서의 침입탐지를 위한 기본 시스템 개발에 대한 연구, Dec., 1997.

[6] D. E. Denning, "An Intrusion-Detection Model," In Proceedings of the IEEE Symposium on Security and Privacy, pp. 118-131, 1986.

[7] Atkins, Buis, Hare, Nachenberg, Kelley, Nelson, Phillips, Ritchey and Steen, Internet Security, New Riders Publishing, 1996.

[8] S. Kumar and E. Spafford, "A pattern matching model for misuse intrusion detection," In Proceedings of the 17th National Computer Security Conference, pp. 11-21, Oct., 1994.

[9] H. Javitz and A. Valdes, "The SRI IDES statistical anomaly detector," In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp. 316-326, May, 1991.

[10] D. Anderson, T. Frivold and A. Valdes, "Next-generation intrusion detection expert system(NIDES)," Technical Report SRI-CLS-95-07, May, 1995.

[11] P. A. Porras and P. G. Neumann, "EMERALD: Event monitoring enabling responses to anomalous live disturbances," In National Information Systems Security Conference, pp. 353-365, Baltimore, MD, Oct., 1997.

[12] 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 intrustion detection system for large networks," In Proceedings of the 19th National Information Systems Security Conference, 1996.

[13] J. S. Balasubramaniyan, J. O. Garcia Fernandez, D. Isacoff, E. Spafford and D. Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents," COAST Technical Report 98/05, Jun., 1998.

[14] M. Crosbie and G. Spafford, "Active Defense of a Computer System using Autonomous Agents," COAST Technical Report No 95-008, Feb., 1995.
[15] Crosbie, M. Dole, B. Ellis, T. Krsul, and I. Spafford, "IDIOT - Users Guide," Technical Report TR-96-050, Purdue University. COAST Laboratory, Sep., 1996.
[16] C. Kahn, P. A. Porras, S. Staniford-Chen and B. Tung, "A Common Intrusion Detection Framework-data formats." Internet draft-ietf-cidf-data-formats-00.txt, Mar., 1998.
[17] R. Rivest, "S-expression," Internet draft-rivest-sexp-00.txt, 1997.
[18] P. R. Gallagher, Jr., "A Guide to Understanding Audit in Trusted Systems." NCSC-TG-001 VERSION-2 Library No. S-228, 470, Jul,, 1987.
[19] M. Bishop, "A Standard Audit Trail Format," In Proceedings of the 18th National Information Systems Security Conference, Baltimore, pp. 136-145, 1995.
[20] H. Debar, M. Dacier and A. Wespi, "Research Report Towards a Taxonomy of Intrusion Detection Systems," Technical Report RZ 3030, IBM Research Division, Zurich Research Laboratory, Jun., 1998.

김 병 구

1999 성균관대학교 정보공학과 학사
현재 성균관대학교 전기전자 및 컴퓨터 공학부 석사과정
관심분야 네트워크 보안, 침입 탐지, 보안 관리
E-mail: bkkim@rtlab.skku.ac.kr

정 태 명

1995 미국퍼듀대학교 공학박사
미국 BBN 연구소 연구원
현재 성균관대학교 전기전자및컴퓨터공학부 교수
한국정보처리학회 총무이사, IEEE Senior member, 침입탐지 및 차단 연구회 위원장, 인터넷 모빌싱점 인증 위원장
관심분야: 실시간 시스템, 네트워크 관리, 보안 관리
E-mail: tmchung@ece.skku.ac.kr