침입탐지시스템 개선을 위한 탐지기술의 분석 및 조사

김학주*, 김태경*, 정태명**
*성균관대학교 컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:hjookim@rtlab.skku.ac.kr

An Analysis of Intrusion Detection Techniques for the improvement of IDS

Hak-Joo Kim*, Tae-Kyung Kim*,
Tae-Myung Chung**
*Dept of Computer Enginnering, SungKyunKwan University
** School of Information & Communication Engineering,
SungKyunKwan University

요 약

현재 구현중인 침입탐지 시스템인 Secure Fortress에 대해 그 특성과 구조에 대해서 살펴보고 시스템의 개선을 위해 새로운 침입탐지 기술인 유전알고리즘, 신경망, 면역시스템을 조사 및 분석하여 연구 동향이나 발전 가능성 등의 요소에 비추어 개선 방향을 정한다. 유전 알고리즘은 다윈의 자연선택설을 바탕으로 선택, 재생 및 교배, 돌연변이의 과정을 통해 솔루션을 도출하는 방식이며 면역시스템은 생물학적인 면역 체계에서처럼 시스템이 스스로를 보호한다는 개념에서 출발하여 유닉스의 시스템 콜을 이용하여 시스템 프로세스 중심의 지식베이스를 구성하고 침입행위를 규정한다. 또한 신경망은 감시 대상이 되는 요소에 따라 통계정보를 등급화하는 일련의 과정을 통해 비정상적인 행위를 초기 학습 후 시스템에 순응하는 기술을 사용하여 고정적인 규칙에서 탈피한 여러 가지 장점을 갖는다. 차후에는 이 알고리즘의 도입을 위한 서비스별 침입대상 요소 선정등의 준비 작업이 필요하다.

1. 서론

인터넷 및 인트라넷의 보급으로 인하여 정보화가 급속도로 진전되고 정보통신망에 대한 의존도가 확대됨에 따라 기업 및 조직들의 많은 업무들이 오프라인에서 온라인으로 옮겨지게 되었다. 이에 따라 정보시스템의 역기능적 현상 또한 빈번히 발생되고 있는데, 오프라인에서 이루어지던 정보의 유출, 변조, 파괴 등의 불법적인 행위들도 온라인으로 옮겨지게 되어 정보보호의 중요성이 부각되었고 이와 관련된 정보보호 제품에 대한 수요도 점차적으로 증가하고 있는 추세이다. 특히 네트워크의 보안이 중요한 문제로 대두되면서 기업 및 조직의 네트워크 시스템 보안 관리자들은 방화벽(Firewall)과 더불어 침입탐지시스템(IDS : Intrusion Detection System)등의 네트워크 보안 솔루션을 도입하고 있다.

본 논문에서는 연구적 차원에서 자체 개발중인 침입탐지 시스템에 대해 고찰을 한 후 문제점을 해결하고 보완하여 악의적인 목표를 가진 공격자에 대해 효율적이고 정확한 탐지를 수행하기 위하여 새로운 침입탐지 기술에 대해 분석 및 조사한다.

본 논문은 총 5장으로 구성된다. 2장에서는 침입탐지 시스템의 개요와 구성을 살펴본 후 현재 구현중인 침입탐지 시스템의 특성 및 개선의 필요성을 분석하고 3장에서는 새롭게 대두된 침입탐지 방법에 대한 조사와 그 개념에 대해 살펴보며 4장에서는 이러한 새로운 침입탐지 시스템에 대해 비교 및 분석을 통해 특성을 도출해낸다. 5장에서는 현재 개발중인 침입탐지 시스템을 어떤 방식으로 개선할 것인지에 대해 결론을 내리고 이로 인해 얻을 수 있는 기대효과와 앞으로의 연구의 진행방향을 제시할 것이다.

2. 관련연구

2.1 침입탐지 시스템의 개요

침입탐지 시스템(Intrusion Detection System)은 네트워크나 컴퓨터 시스템 내에서 일어나는 이벤트를 모니터링하고 보안 관점에서 분석하는 작업을 수행하는 시스템으로써 허가 받지 않은 접근이나 해킹 시도를 감지하여 시스템 또는 네트워크 관리자에게 통보해 주고, 필요한 대응을 취하도록 하는 시스템을 말한다.[1]

[그림 1]는 침입탐지 시스템의 일반적인 동작과정이다. 호스트나 네트워크로부터 탐지를 위한 데이터를 수집하여 분석에 알맞은 형태로 가공하거나 분석에 필요한 데이터만을 갖도록 축약하고, 설정해놓은 정책(policy)이나 규칙(rule)에 비추어 침입인지를 결정하여 관리자에게 보고하고 대응을 기다리거나 미리 설정해놓은 대응방법에 의해 조치를 취한다.

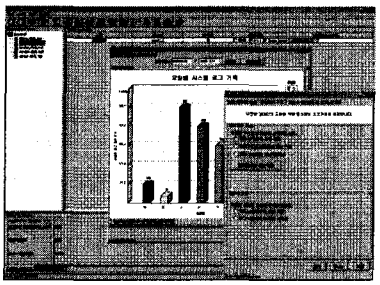
[그림 1] 침입탐지 시스템의 동작

침입탐지 시스템에서는 어떤 방식의 침입탐지 방법을 사용하느냐에 따라 그 구성방식이나 특성에 큰 차이를 보인다. 이러한 침입탐지 방법 중 가장 일반적인 분류가 오용탐지(misuse detection)와 비정상행위탐지(anomaly detection)인데 오용 탐지 방식은 지식기반(knowledge based)의 탐지 방법으로써 기존에 알려진 침입행위에 대한 정보를 가지고 분석한 데이터가 거기에 일치하는 지를 판단해 침입 여부를 판단하는 방식이고, 비정상행위 탐지 방식은 행위기반(behavior based)의 탐지 방법으로써 미리 시스템이나 네트워크에 대한 정상적인 입력패턴을 규정해 두고 분석한 데이터가 그 패턴에서 벗어나게 되면 침입행위로 판단하는 방식이다. 이 두 가지 방식은 나름대로 장단점을 갖고 있는데 비정상행위 탐지 기법은 새로운 침입행위에 대해서도 대응할 수 있으나 침입행위에 대한 오보율이 높고 오용 탐지 기법은 그 반대의 특성을 갖는다. 이러한 특성 때문에 침입탐지 시스템 시장에서는 오용탐지 방식과 혼합방식(hybrid detection)의 시스템이 대부분을 차지한다.

침입탐지 시스템은 단순히 접근 제어 기능만을 수행하는 수동적인 시스템에서 점차 침입 패턴을 데이터베이스화하고 전문가 시스템(Expert System)을 접목시켜 네트워크나 시스템 사용을 실시간적으로 모니터링이 가능한 시스템으로 발전해왔으며 최근에는 네트워크 보안 개념의 변화에 따라 점점 자동화, 지능화, 능동화되어 가고 있다.

2.2 구현중인 침입탐지 시스템에 대한 고찰

현재 연구실에서 구현중인 침입차단 시스템인 Secure Fortress의 특성을 살펴보면 시스템의 유연성 및 확장성을 고려하여 에이전트 및 메니저 구조를 취하고 있고 각 기능이 모듈화되어 있으며 호스트와 네트워크 기반(host based & network based)의 침입행위에 대하여 오용 탐지 방식을 적용한다.

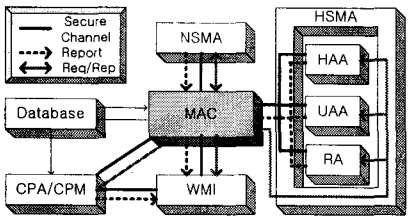


[그림 2] Secure Fortress

상세 구조는 아래의 [그림 3]에서 보는 바와 같이 하나의 에이전트 관리기능 모듈(MAC : Multi-Agents Coordinator)과 5개의 에이전트로 이루어져 있다. 각 에이전트들은 크게 네트워크 관련 보안 모니터링 에이전트 (NSMA : Network Security Monitoring Agent)와 호스트 관련 보안 모니터링 에이전트 (HSMA : Host Security Monitoring Agent), 콘텐츠 관련 보안 에이전트인 CPA(Contents Probing Agent) / CPM(Contents Probing Manager)등으로 이루어진다.

NSMA는 감시대상 네트워크에서 발생하는 패킷 정보를 수집하고, 침입에 대해 분석하는 기능을 수행하며 침입 판정된 보안위반 사건에 대해서 MAC으로 통보하는 기능을 한다. HSMA는 호스트 기반의 분석정보를 토대로 동작하는 에이전트인데 호스트가 생성하는 로그 정보로부터 보안관련 감사정보를 수집하고 이를 분석하여 사용자의 오용을 탐지하여 트랩 메시지를 통해 MAC에 보고한다. CPA는 CPM과 연동하여 Email을 통해 이루어지는 각종 스팸메일, 정크 메일, 바이러스 등 다양한 컨텐츠를 대상으로 유해한 행위에 대한 탐지와 대응행위를 하는 에이전트이다. 이 모든 에이전트들은 MAC에 의해 중앙 관리되며 대부분의 보안 위반 이벤트들이

WMI(Web Monitoring Interface)를 통해 설정된 규칙과 정책에 따라 웹 기반으로 사용자에게 제공된다.



[그림 3] Secure Fortress의 구성도

Secure Fortress는 다양한 상황에 적용가능하며 에이전트를 이용한 모듈화를 통해 여러 가지 장점도 지니고 있지만 최근 더욱 가속화되고 있는 네트워크 상황에 적응하고 고도화 및 복합화 되어가고 있는 새로운 공격에 대한 능동적인 대처와 효율성 증대 및 오보율 감소 등을 위하여 새로운 침입탐지 기법의 도입이 필수적이다.

3. 새로운 침입탐지 기술에 대한 조사

신경망, 면역시스템, 유전알고리즘 등 개념적인 부분에 국한되어 있지만 다른 분야의 학문과 연계를 통한 새로운 침입탐지 기술에 대한 연구는 이미 오래 전부터 시작되었으며 아직 상용화까지는 이루어지고 있지 않지만 테스트 베드를 통한 실험적인 구현이 이루어지고 있다.

3.1 신경망(Neural Networks)

신경망은 거의 사람 뇌의 동작에 가깝게 만든 프로그램이나 데이터구조 시스템을 말한다. 다수의 데이터의 관계들에 관한 많은 양의 데이터나 규칙이 공급되며 초기에 학습을 통해 기본적인 규칙을 획득한다.

침입탐지 시스템에 있어서의 신경망의 적용은 비정상적인(anomalous) 행위를 학습하여 일정한 규칙을 부여함으로써 시스템에 자동적으로 순응하는 기술을 사용한다. 현재 테스트되고 있는 실험적인 모델들은 호스트 기반과 네트워크 기반의 형태들이 모두 존재하고 탐지에 사용되는 통계에 필요한 요소(factor)가 다르긴 하지만 각 요소 별로 만들어진 통계 정보를 등급화하여 특정한 수식 및 연산을 적용함으로써 침입을 탐지한다. 예를 들면 텍사스 대학의 Jake Ryan등이 진행하고 있는 NNID(Neural Network Intrusion Detector) 프로젝트에서는 사용자마다 시스템의 사용목적이 다르기 때문에 사용하는 명령어의 순서가 다르다는 점에 착안하여 사용된 명령어를 기록한 후 이에 대한 명령어 분산 벡터(command distributed vector)를 생성하여 사용자를 구별하고 침입 행위를 규정한다.

따라서 통계적인 방식과 유사해 보이나 통계수치를 바탕으로 고정된 규칙에 의한 탐지에서 벗어나 새롭고 다양한 침입행위에 대한 규칙 설정이 가능하고 그로 인해 탐지가 가능하다는 장점이 있다. 그러나 탐지성능이 통계의 대상이 되는 요소의 선택과 내부적인 알고리즘에 의해 크게 좌우되며 제시되고 있는 테스트의 결과가 실제 네트워크 환경에서의 다양한 공격에도 그 실효성을 인정받을 수 있을 지에 대해서는 아직 미지수이다.[3][4]

3.2 면역 시스템(Immune System Approaches)

면역시스템은 컴퓨터 시스템이 스스로 자신을 보호하는데 목적을 두고 나온 개념이다. 생물학적인 면역 체계와 시스템의 보호 체계 사이의 유사점에 주목하여 마치 유기체의 면역 체계가 해로운 병원체나 다른 위험 요소와 해롭지 않은 요소를 결정하는 것처럼 시스템이 침입행위를 스스로 결정토록 하는 방식인데 일련의 UNIX 시스템 콜이 이러한 요구사항을 만족시킬 수 있을 것이라는 가설에서 시작한다.

면역 시스템은 시스템 콜에 전달되는 인자들을 모두 무시한 채 일시적인 명령에 대한 시스템 프로세스 중심으로 일반적인 행위에 대한 지식베이스를 도출해낸다. 따라서 비정상행위 탐지와 오용 탐지 두 가지 방식이 모두 적용 가능하고 일시적인 명령에 대한 시스템 콜을 탐지 대상으로 삼기 때문에 성능면에서도 뛰어나다는 장점이 있다.[5][6][7]

3.2 유전 알고리즘(Genetic Algorithms)

유전 알고리즘은 다윈의 자연 선택설을 포함하는 진화론 알고리즘의 한 부분으로써 '염색체(chromosomes)'로 알려진 암호화된 형태의 객체와 새로운 개체를 형성하기 위한 방법으로 염색체의 결합과 돌연변이를 사용한다.

이에 착안하여 유전 알고리즘을 이용한 침입탐지 시스템 개발 프로젝트로는 프랑스의 Suplec이 추진중인 G^ASSATA(Genetic Algorithm as an Alternative Tool for Security Audit Trails Analysis)가 있는데 이 시스템에서는 시스템 이벤트들의 수와 공격의 횟수를 기준으로 200(공격 수)×24(로그이벤트 수)크기의 벡터를 사용하여 분류하고 그 벡터를 바탕으로 개체 선택, 재생 및 교배, 돌연

변이의 3가지 과정으로 이루어진 군집에서의 자연선택과정을 Fitness Function으로 구현한다.

$$F(I_i) = \alpha + (\sum_{i=1}^{N_e} R_i . I_i - \beta . T_e^2)$$

4. 새로운 침입탐지 기술의 분석

위에서 소개한 침입탐지 기술들은 나름대로 장단점이 있으며 개발에 관련된 논문에서는 그 오보율이 모두 10%미만으로 침입에 대한 정확한 판단이 가능하다고 발표되고 있다. 따라서 새로운 공격에 대한 탐지율로는 전반적으로 높은 정확성을 갖는다고 할 수 있다.

[표1] 각 탐지기술의 결과치 비교

탐지기술	project	탐지율	오보율
신경망	NNID	96%	7%
	NN	100%	?
면역시스템	-	87.5%	1%
유전알고리즘	GASSTA	99.6%	0.04%

위에서 비교한 세 가지 탐지기술들은 낮은 오보율을 가지면서도 새로운 침입행위에 대한 탐지가 가능하다는 공통적인 장점이 있으나 알고리즘 자체의 한계도 분명 존재한다. 신경망은 accountability면에서의 제약 때문에 다수의 사용자가 있는 시스템에서는 오보율이 높아질 가능성이 크다는 단점이 있고 면역시스템은 정상행위 규정 대상이 일시적인 시스템 프로세스로 한정되며 전달되는 인자들 역시 무시되어 보다 광범위하고 복잡한 침입행위에 대해서는 한계가 있다. 게다가 시스템 콜을 이용하기 때문에 호스트에 독립적이지 못하다. 유전 알고리즘은 이진코드(binary code)에 대해서 탐지가 불가능하며 하나의 이벤트 그룹에 대해서 동시에 공격이 일어날 경우 벡터에 반영이 되지 않아 이런 경우 역시 탐지가 불가능하다. 또한 정의된 군집에 대한 개체를 평가할 함수를 도출하는 문제도 여전히 계속 논의중인 상태이다.

5. 결론

지금까지 살펴본 침입탐지 기술에서 애초의 요구(자동화, 지능화)를 만족시키며 현재의 상황에 가장 알맞는 기술은 신경망이라 하겠다. 그 이유는 위에서 분석한 내용처럼 신경망에서의 침입탐지 시스템은 네트워크와 호스트 베이스의 침입탐지에 모두 적용이 가능하며 이에 따라 에이전트 별로 독립된 기능의 수행이 가능해 Secure Fortress의 범용적인 사용요구에 일치한다. 또한 차후에 확장성이 보장되고 시스템의 내부적인 오류로 인한 동작정지 시에도 독립적인 에이전트가 MAC과 연계하여 동작하기 때문에 시스템 내성(system tolerance)을 보장할 수 있다. 게다가 네트워크나 시스템 기반으로 제공되는 많은 서비스 혹은 서비스를 구성하는 요소들을 침입판단 요소로 적용한다면 침입의 판단 뿐 아니라 그에 대한 대응까지도 가능할 것으로 보인다. 이미 지적되었던 사용자의 증가에 따른 오보율의 증가 가능성문제는 여전히 남아있겠지만 이는 탐지 대상이 되는 요소들을 보다 세분화하고 이를 정확한 공격 유형에 대해 그룹화하는 작업을 통해 극복이 가능할 것이다.

앞으로 신경망 기반의 탐지기술의 도입을 위해서는 현재 시스템에서 제공되는 서비스에는 무엇이 있는지 파악하고 이 서비스의 구성요소와 침입가능여부를 판별하는 단계를 거쳐 탐지대상이 될 요소들을 정립하고 이를 바탕으로 정책과 규칙을 생성해내는데 필요한 내부 알고리즘 및 시스템 분석에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] Roger S. Pressman "Software Engineering A Practltiners' Approach" 3rd Ed. McGraw Hill

[2] Ludovic Me Supelec "GASSATA, a Genetic Algorithm as an Alaternative Tool for Security Audit Trails Analysis"

[3] Susan C. Lee and David V. Heinbuch "Training a Neural-Network Based Intrusion Detector to Recognize Novel Attacks" Workshop on Information Assurance and Security 2000

[4] Jake Ryan, Meng-Jang Lin and Risto Miikkulainen "Intrusion Detection with Neural Networks" 1998

[5] Steven A. Hofmeyr and S. Forrest, "Architecture for an Artificial Immune System" 2000

[6] Dipankar Dasgupta and Fabio Gonzalez "An Immunity-Based Technique to Characterize Intrusions in Computer Networks" 2002

[7] Towards an Artificial Immune System for Network Intrusion Detection : An Investigation of Dynamic Clonal Selection" 2002