2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

분산 에이전트를 이용한 침입 탐지 시스템 모델

정종근† , 김용호, 이윤배
조선대학교 전자계산학과
jkjeong@infoman.chosun.ac.kr

Design of Intrusion Detection Syatem Model using Attributed Agent

Jong-Keun Jeong† , Young-Ho Kim , Yun-Bae Lee
Dept. of Computer Science, Chosun University

요 약

최근 세계적으로 유수한 인터넷 사이트들의 해킹으로 인해 네트워크 보안의 중요성이 강조되고 있다. 네트워크 보안을 위해 방화벽보다는 좀 더 신뢰성이 높은 네트워크 및 시스템에 대한 보안 솔루션으로 침입 탐지 시스템(IDS)이 차세대 보안 솔루션으로 부각되고 있다. 본 논문에서는 기존의 IDS의 단점이었던 호스트 레벨에서 확장된 분산환경에서의 실시간 침입 탐지는 물론 이기종간의 시스템에서도 탐지가 가능한 새로운 IDS 모델을 제안·설계하였다. 그리고, 프로토타입을 구현하여 그 타당성을 검증하였다. 이를 위해 서로 다른 이기종에서 침입 탐지에 필요한 감사 파일을 자동적으로 추출하기 위해서 분산 에이전트를 이용한다.

1. 서론

인터넷 전자 상거래의 급증과 인터넷으로 연결된 네트워크의 수가 급속히 증가하면서 시스템에 대한 외부 침입과 내부자의 시스템 파괴나 기밀 유출 등이 사회적으로 큰 문제로 대두 되고 있다. 최근 Yahoo, Amazon, CNN 등의 유명 사이트들이 해커의 침입을 받아 서비스를 중단하는 사건이 발생하기도 하였다. 따라서, 인터넷을 통한 전자 거래에 있어서 내부 정보의 보호는 필수적이며, 새로운 시스템 보호 메카니즘이 필요하다. 현재까지는 방화벽만으로도 외부에서의 공격을 어느 정도 차단 할 수 있으나 내부적인 불법행위는 방어할 수 없다. 따라서 외부에서 침입하는 행위는 물론 내부 사용자의 불법적인 행위까지 실시간적으로 감시할 수 있는 침입 탐지 시스템에 대한 연구가 활발히 진행되고 있다. 대부분의 인터넷 사이트들이나 내부 네트워크들은 단일 호스트가 아닌 분산 환경으로 되어 있기 때문에 단일 호스트에 대한 침입 탐지 방법은 효과를 거두기 어렵다.

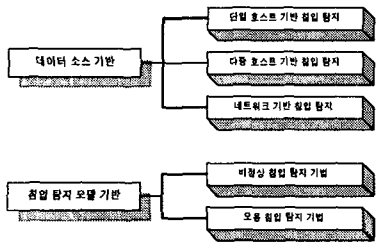
따라서, 본 논문에서는 시스템 내에서 불법적인 행위를 하는 침입자들의 패턴을 추출하여 분석하는 에이전트를 이용하여 분산 환경에서의 다중 호스트 기반의 실시간 침입 탐지 시스템 모델을 제안한다.

2.침입 탐지 시스템의 기술적 분류

2.1 침입 탐지 시스템의 분류

침입 탐지 시스템은 외부의 침입자 뿐만 아니라 내부 사용자의 불법적인 오남용, 오용 행위등을 탐지하는데 목적이 있으며, 미국 COAST(Computer Operations Audit and Security Technology)의 분류에 따라 데이터 소스(source)를 기반으로 하는 분류 방법과 침입 모델을 기반으로 하는 분류 방법으로 나눌 수 있다. 데이터 소스를 기반으로 분류하는 방법은 단일 호스트로부터 생성되어 수집된 감사 데이터(Audit Data)를 침입 탐지에 이용하는 단일 호스트 기반(Single0Host Based)과 여러 호스트들로부터 생성되고 수집된 감사데이터를 침입 탐지에 이용하는 다중 호스트 기반(Multi-Host Based), 그리고 네트워크 상에서 수집된 패킷 데이터들을 모아 침입 탐지에 사용하는 네트워크 기반(Network Based)로 나눌 수 있다. 침입 모델을 기반으로 하는 분류 방법은 정상적인 시스템 내에서의 사용자가 정상 행위에서 벗어나 행위들을 탐지해 내는 비정상 탐지(Anomaly Detection)와 시스템의 알려진 취약점이나 버그 등을 통해 침입하는 행위를 탐지하는 오용탐지(Misuse

Detection)로 구분할 수 있다.



(그림 1) 침입 탐지 시스템의 분류

또 다른 분류 방법으로는 IBM Zurich Research Lab.의 분류가 있는데 여기서는 침입 탐지 시스템의 기능적 특성과 비 기능적 특성으로 분류하고 있다. 기능적 특성은 침입 탐지 방법, 침입 탐지 시 대응, 감사 데이터의 수집 위치 등에 따라 분류하고, 비 기능적 특성은 모니터링 수행 빈도에 따라 분류한다.

2.2 침입 탐지 시스템 기술 분석

침입 탐지 시스템을 구현하는 방법은 다음과 같이 크게 세 가지로 분류할 수 있다.

- 실시간 침입 감시 및 분석 기술
- 실시간 패킷 수집 및 분석 기술
- 사후 감사 분석에 의한 분석 기술

실시간 침입 감시 기술은 허가 받지 않은 파일에 대한 임의적 접근이나 변경, 로그인(login) 프로그램의 변경 등을 탐지해 낸다. 실시간 침입 탐지를 위한 효과적인 방법은 네트워크를 구성하는 여러 가지 시스템과 장치에서 발생하는 불법적인 행위들을 실시간적으로 모니터링하고 조치를 취해야 한다. 대부분의 행위 모니터링은 운영체제(OS)에서 제공해 주는 감사 자료(audit data)를 활용한다. 반면에 다각도에서 탐지해 내기 위해서는 Webserver, Router, Firewall, TCP/UDP port의 활성화 등에 의한 감사 자료들을 이용해야 한다.

실시간 침입 감시는 침입자가 대부분 관리자 권한을 획득하려고 하기 때문에, 이러한 행위가 감지되면 즉각적인 조치를 취하게 함으로써 시스템의 피해를 줄일 수 있다.

실시간 침입 탐지 기술은 단일 호스트 침입 탐지와 다중 호스트 침입 탐지로 나눌 수 있는데, 단일 호스트 침입 탐지는 오직 한 시스템에서만 작동하므로 오늘날과 같은 멀티 플랫폼 환경에는 적합하지 않다.

그리고, 다중 호스트 침입 탐지 방법은 전체 네트워크와 시스템을 에이전트로 인식하여, 분산된 환경에서 감사 자료를 수집, 분석하여 침입을 탐지한다. 이때 에이전트의 역할은 네트워크로 연결되어 있는 다중 호스트에 설치되어 감사 자료의 수집, 추출 등의 일을 담당하게 된다.

3 실시간 침입 탐지 시스템 구조

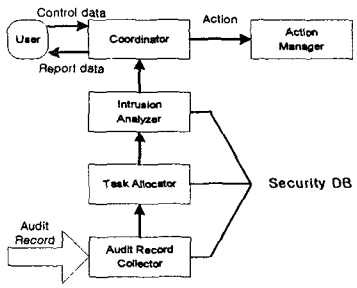
실시간 침입 탐지 시스템은 (그림5)에서와 같이 크게 감사 레코드 수집기(ARC), 작업 할당기, 침입 분석기 등의 3부분으로 나눌 수 있다.

3.3.1 Audit Record Collector(ARC)

ARC는 시스템에서 발생되는 각종 감사 데이터나 패킷 등을 수집하는 역할을 담당한다. ARC는 시스템 내에서 침입 관련 자료들을 수집하기 위해 관리자의 권한을 가지며, 시스템의 모든 상태를 감시하고 필요한 감사 데이터를 추출할 수 있는 기능을 가지고 있어야 한다.

3.3.2 작업 할당기(Task Allocator)

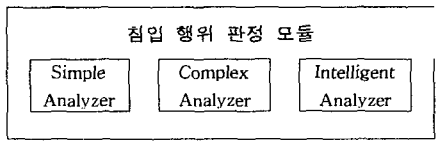
침입 분석기(Intrusion Analyzer)에서 동작하는 몇 개의 침입 여부 판정 세부 기능 모듈에 각 침입 탐지 유형에 따라 적절한 작업이 이루어지도록 한다. Audit Record Collector로부터 제공된 감사 자료들을 침입 분석기가 요구하는 데이터 형식으로 가공하여 분석기에서 침입 판정에 따른 성능을 향상시킨다.



(그림2) 실시간 침입 탐지 시스템 구조

3.3.3 침입 분석기(Intrusion Analyzer)

침입 분석기는 (그림3)과 같이 침입을 판정하기 위한 단순 분석기(Simple Analyzer), 고난도 분석기(Complex Analyzer), 지능형 분석기(Intelligent Analyzer)로 나누어서 동작한다.



(그림3) 침입 행위 분석기

시스템의 기능 확장과 성능에 있어 효율성을 고려하여 3단계로 구분하였고 그 특징은 다음(표1)과 같다.

(표1) 분석기 특징 분류

분석기 분류	기능
Simple Analyzer	· 최소의 정보를 이용한 침입 판정 · 단순 비교에 의해 침입 판정
Complex Anlyzer	· 침입 관련 정보를 조합해 침입 판정 · 침입 판정을 위해 저장 침입 패턴 필요
Intelligent Analyzer	· 침입 판정을 위해 많은 정보 요구 · 침입 판정시 지능적 처리 요구

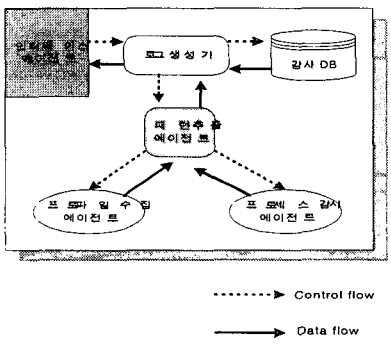
4. 실시간 분산 에이전트를 이용한 자동침입 탐지 시스템 설계

(A design of Automatic Intrusion Detection System using real-time Attributed Agent ; AIDSAA)

4.1 시스템의 구조

에이전트는 분산 환경하에서 네트워크나 시스템의 상태를 감시하기에 가장 적합한 시스템이다. 특히, 실시간 침입 탐지 시스템에서는 침입 정보에 대한 학습이 자동으로 이루어져야 하기 때문에 에어전트를 이용한 침입 탐지 시스템이 가장 이상적이다. 다음 (그림5)에서는 AIDAA의 구조도를 보여주고 있다.

본 논문에서는 과거의 침입 유형에 대한 학습뿐만 아니라 새로운 침입 패턴을 감지하고 학습하기 위한 자동 패턴 추출 에이전트를 제안한다. 에이전트 구조는 (그림4)에서와 같이 크게 4부분 즉, 인터페이스 에이전트, 패턴 추출 에이전트, 프로파일 수집 에이전트와 프로세스 감사 에이전트 등으로 나눌 수 있다.



(그림4) 자동 패턴 추출 에이전트 구조

인터페이스 에이전트는 침입 탐지 서버에서 만들어진 탐지 시나리오등을 전송하거나, 각 대상 호스트에 맞는 환경 설정등을 할 수 있는 곳이다.

패턴 추출 에이전트는 프로파일 수집 에이전트에서 수집된 감사 자료로부터 침입 탐지서버의 시나리오에서 필요로 하는 감사 자료만을 추출하는 역할을 담당한다. 이때 수집된 감사자료는 다시 전송하게 되며, 새로운 패턴을 수집 했을 경우 패턴 데이터베이스에 저장한다.

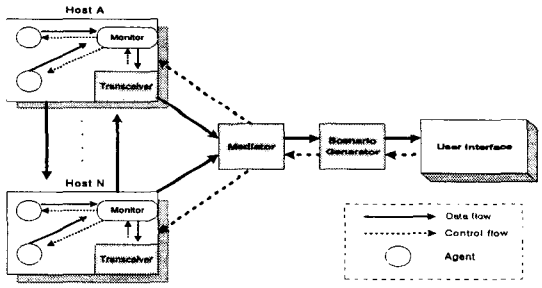
프로파일 수집 에이전트와 프로세스 감사 에이전트는 실제 대상 호스트에서 발생하는 이벤트, 즉, CPU 사용시간, 로그인 실패 ID, 특정 포트 접근 시도 등의 감사 데이터를 커널로부터 수집하는 역할을 한다.

특히, 인터페이스 에이전트는 침입 탐지 시스템의 시나리오를 수신 받아 패턴 추출 에이전트에게 사용자에 현재 프로파일과 프로세스에 대한 정보를 수집하라는 명령을 내린다.

이때 대상 시스템이 이종간일 경우에 감사 파일의 포맷(format)에 문제가 생긴다. 본 논문에서는 이러한 문제를 해결하기 위해 추출된 감사 파일의 표준화방식을 채택하였다. 패턴 추출 에이전트로 이동한 감사 파일들은 로그생성기(Log Generator)에서 표준화된 포맷으로 재 생성된다.

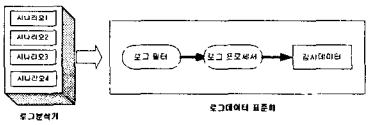
4.2 로그 감사 데이터 표준화(로그생성기)

이전까지 연구되어온 침입탐지 시스템의 감사 데이터 기법은 시스템 의존적인 특성을 지니고 있어 이종의 환경을 지



(그림5) 제안된 패턴 추출 에이전트 침입 탐지 시스템 모델

원하기에 적합하지 않았다. 따라서 본 연구에서는 로그 데이터 분석기에서 각각의 시나리오에서 수집되어 분석된 로그 데이터는 로그필터(log filter)를 이용해서 감사 데이터를 표준화하여 일관된 로그 감사 데이터 구조를 유지하게 하였으며, 생성 구조는 (그림6)과 같다.



(그림6) 로그필터를 이용한 감사 데이터의 표준 형식 생성 구조

각 운영체제의 로그 분석기에서 필요한 로그 정보를 수집한 다음, 로그 필터를 통해 로그 프로세서에서 필요로하는 로그 필드만을 추출한

이때 로그프로세서는 침입 탐지 시스템에서 필요로하는 감사 데이터를 표준화된 구조대로 생성하는 역할을 하게된다.

4.3 시나리오 생성기

실시간으로 시나리오 생성기를 설계하기 위해 본 연구에

서는 4가지 시나리오에서 발생하는 각종 로그 데이터를 수집하여 분석하게된다. 시나리오의 구조는 다음과 같다.

- 시나리오 1 : 자신의 홈 디렉토리가 아닌 사용자의 홈 디렉토리에 불필요하게 드나드는 행위
- 시나리오 2 : 작업 내용을 은폐할 목적으로 일부 로그 파일을 삭제하는 행위
- 시나리오 3 : 처음으로 로그인 된 호스트로부터의 사용자가 중요한 파일을 파괴하는행위
- 시나리오 4 : 잦은 로그인 실패한 사용자가 중요 파일을 파괴하는 행위

5. 결론 및 향후 연구 방향

본 논문에서 제안한 분산 에이전트 침입 탐지 시스템은 실시간적으로 분산된 호스트에 대해 에이전트에서 침입 탐지에 필요한 데이터를 수집하며, 특히 감사 파일의 표준화 단계를 거침으로서 이 기종간의 침입 탐지의 효율성을 극대화하였다. 에이전트에서 침입 탐지에 필요한 데이터를 수집하도록 하기 위해 시나리오생성기에서 침입 시나리오를 작성하여 에이전트에게 전송함으로써 에이전트는 즉각적으로 반응하고 필요한 자료만을 수집하게 된다. 감사파일 표준화 단계에서는 표준 감사 파일 포맷을 만들어 이 기종에서 수집되는 감사 데이터를 하나의 포맷으로 작성함으로 침입 판정에 있어서의 시스템 부하를 최소화하였다. STAT 시스템과 비교 하면, 다중 호스트 기반과 네트워크 기반에서의 침입 탐지 기능을 보강하였다. 해커들의 비정상적인 침입을 탐지하는 비정상행위 탐지에서는 침입 수법이 날로 변하기 때문에 자동화된 시나리오의 업데이트와 침입 기법에 대한 연구가 필요하다.

참고문헌

[1] Wenke Lee and Salvatore J.Stolfo, Data Mining Approaches for Intrusion detection, in Proceeding1998 7th USENIX security Symposium, January, 1998

[2] Neil C.rowe and Sandra Schiavo, An intelligent tutor for Intrusion Detection on Computer System, code Cs/rp, Department of Computer Science, Naval postgraduate school monterey, 1997

[3] 김판구 외 4인, "데이터 마이닝 기법을 적용한 최적침입 탐지 모듈 설계", 1999 춘계 정보과학회 논문집