패턴 추출 에이전트를 이용한 분산 침입 탐지 시스템

정종근, 이해군, 허경, 신숙경
한국학술진흥재단

Attributed Intrusion Detection System using Pattern Extracting Agent

Jong-Geun Jeong, Hae-Gun Lee, Kyung-Her, Suk-Kyung Shin
Korea Research Foundation E-mail : jkjeong@krf.or.kr

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(Intrusion Detection System)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 분산 침입 탐지에 필요한 감사 파일을 자동적으로 추출하기 위해서 패턴 추출 에이전트를 이용하였다.

ABSTRACT

As network security is coming up with significant problem after the major Internet sites were hacked nowadays, IDS(Intrusion Detection System) is considered as a next generation security solution for more trusted network and system security. We propose the new IDS model which can detect intrusion in the expanded distribute environment in host level, drawback of existing IDS, and implement prototype. We used pattern extraction agent so that we extract automatically audit file needed in intrusion detection even in other platforms.

Ⅰ. 서론

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.

Ⅱ. 실시간 침입 탐지 시스템의 분석

지금까지 연구되어온 대부분의 침입 탐지 시스템은 침입 탐지 모델 기반과 데이터 소스 기반에 따라 분류하고 규칙 기반의 탐지 방법을 이용하고 있다. 이와 같은 침입 탐지 시스템들은 한 개의 침입 탐지 프로세스에 의해 침입 탐지를 수행하므로 시스템의 부하는 물론 한 프로세스의 결함이 전체 시스템의 성능을 떨어뜨리는 문제점을 가지고 있다. 이에 대한 해결책은 다중 에이전트를 이용하여 분산 시스템 전체에서 시스템에 대한 감시와 자료 수집, 탐지 등의 작업을 수행토록 하는 것이다[2][4][5].
또한, 이들 침입 탐지 시스템들은 자체적인 학습 기능이 없으므로 시스템의 환경 변화나 새로운 공격 유형이 나타날 때 유연하게 대처할 수 없다.

2.1 실시간 침입 탐지 시스템 구조

실시간 침입 탐지 시스템은크게 감사 레코드 수집기(Audit Record Collector : ARC), 작업 할당기, 침입 분석기 등의 3부분으로 나눌 수 있다.

2.1.1 감사레코드 수집기

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.

2.1.2 작업 할당기

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

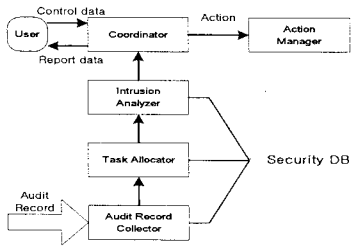

그림1. 실시간 침입 탐지 시스템 구조

2.1.3 침입 분석기

침입 분석기는 (그림2)와 같이 침입을 판정하기 위한 단순 분석기(Simple Analyzer), 고난도 분석기(Complex Analyzer), 지능형 분석기(Intelligent Analyzer)로 나누어서 동작한다.

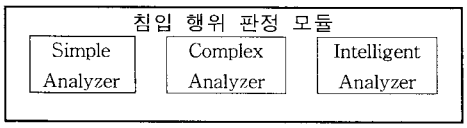

그림2. 침입 분석기

시스템의 기능 확장과 성능의 효율성을 고려하여 3단계로 구분하는데 그 특징은 (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

Ⅲ. 실시간 패턴 추출 에이전트를 이용한 자동침입 탐지 시스템 설계

3.1 제안된 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. (그림3)은 자동 패턴 추출 에이전트(A design of Automatic Intrusion Detection System using real-time Pattern Extracting Agent ; AIDSPEA)의 구조를 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.

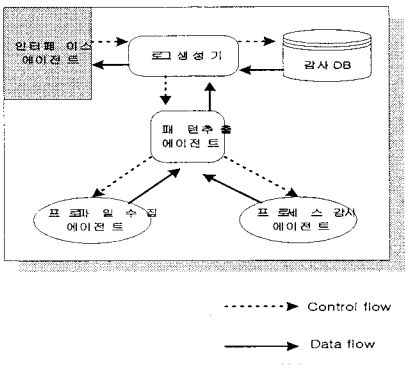

그림3. 자동 패턴 추출 에이전트 구조

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 침입 탐지 서비에게 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

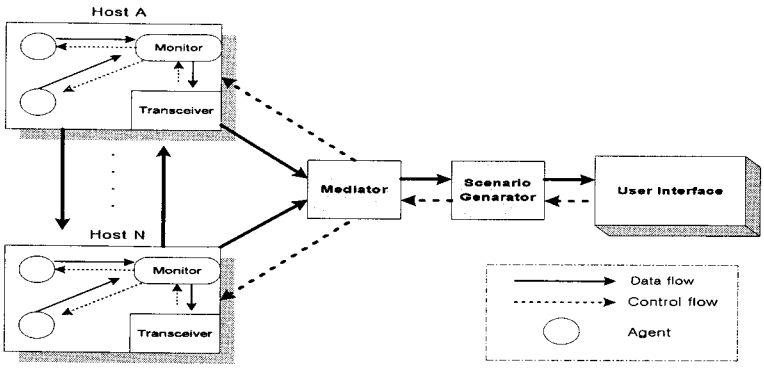

그림4. 제안된 패턴 추출 에이전트 침입 탐지 시스템 모델

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. 다음은 패턴 추출 에이전트의 클래스 구조에 대한 알고리즘이다.

```
class Patt_extractor_agen {
 rcv_scenario();
  //시나리오로부터 추출 패턴 수신
 request_profile();
  //프로파일 수집 에이전트에게 시나리오에
    해당하는 자료만 요청
 rcvprofile(); //프로파일 수신
 request_process();
  //프로세스 감시 에이전트에게 시나리오에
    해당하는 자료만 요청
 rcvprocess(); //process 자료 수신
 sendprofile(); //수집된 프로파일 전송
 sendprocess(); //수집된 프로세스 전송
 }
 clsaa store_pattern_DB {
 request_pattern(); //추출된 감사 자료 요청
 stroe_DB();
  // 감사 자료로 사용할 자료 저장
 }
 class InterF_agen {
 request_pattern();
  //패턴추출 에이전트에게 감사 자료 요청
 rcv_pattern(); //감사자료 수신
 sendpattern(); }//추출된 감사자료 송신
```

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

3.2 로그 감사 데이터 표준화

이전까지 연구되어온 침입 탐지 시스템의 감사 데이터 기법은 시스템 의존적인 특성을 지니고 있어 이종의 환경을 지원하기에 적합하지 않았다. 따라서 본 연구에서는 로그 데이터 분석기에서 각각의 시나리오에서 수집되어 분석된 로그 자료는 로그필터(log filter)를 이용해서 감사 자료를 표준화하여 일관된 로그 감사 자료 구조를 유지하게 하였으며, 생성 구조는 (그림5)와 같다.

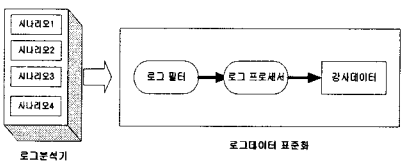

그림5. 로그필터를 이용한 감사 자료의 표준 형식 생성 구조

각 운영체제의 로그 분석기에서 필요한 로그 정보를 수집한 다음, 로그 필터를 통해 로그 프로세서에서 필요로 하는 로그 필드만을 추출 한 다음 로그프로세서에 의해 표준 형식으로 변환된다. 이때 로그프로세서는 침입 탐지 시스템에서 필요로 하는 감사 자료를 표준화된 구조대로 생성하는 역할을 한다. 본 논문에서 제안한 감사 자료 표준화를 위해 각기 다른 OS인 SUN 기종과 AIX 기종의 OS에서 생성되는 로그파일을 표준화하였다.

3.3 침입 판단 엔진

침입 판단 엔진에서는 침입 탐지 시스템의 핵심 부분으로서 침입을 판단하고 이에 대응하는 보고를 하는 역할을 한다. (그림10)의 구조와 같이 침입에 대한 보고는 관리자의 모니터에 즉시 경고 메시지를 보낸다.

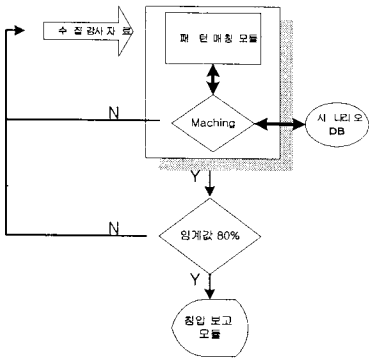

그림6. 침입 판단 구조도

대상 호스트에 분산되어 있는 에이전트로부터 로그 자료를 수집하여 표준화된 감사 자료로 변환 다음 탐지 규칙에 의해 침입 여부를 결정한다. 본 논문에서 적용한 침입 결정 방법은 시나리오에서 적용한 패턴과 에이전트에서 추출된 패턴의 비교율의 임계값이 80%에 해당되면 침입으로 결정한다.

Ⅳ. 제안된 시스템의 성능평가

본 논문에서는 실험을 위해 시나리오 생성기에서 생성된 4개의 시나리오와 연관된 명령어들을 실험 자료로 이용하였다. 이 자료들은 UNIX에서 사용하는 명령어나 파일, 디렉토리에 해당하며, 침입 판단을 위해 임계값을 주었다. 이때 임계값을 너무 높게 주게되면 침입 판정의 정확도는 높게 되지만 전체적인 탐지율은 낮아지고 침입을 정상적인 사용으로 인정해버리는 치명적인 에러가 생길 수 있고, 임계값을 낮게 주면 탐지의 정확도는 낮아지지만 탐지율은 높아진다. 따라서, 본 논문에서의 임계값의 조정은 침입 판단 엔진에서 할 수 있게 하였다.
(그림7)은 침입 판정을 위해 임계값을 조정했을 때의 탐지율을 그래프로 보이고 있다.

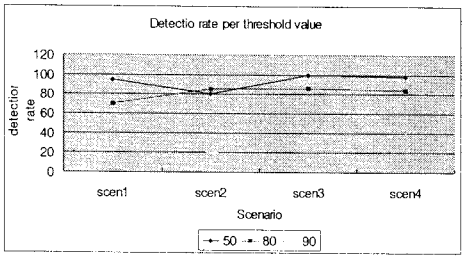

그림7. 임계값 별 침입 탐지율 변화

(그림7)에서 알 수 있듯이 임계값을 낮게 줄수록 침입 탐지율은 높아지고 소요시간은 짧아지며, 임계값을 높일수록 탐지율이 낮아지는 반면에 정확도는 올라가고, 탐지 시간이 길어지는것을 볼 수 있다. 본 시스템의 특징은 에이전트 단계에서 침입 탐지에 필요한 감사자료를 추출하여 표준화된 포맷으로 변형시킴으로써 침입 탐지 호스트에서의 작업 부하를 최소화 시켰고, 탐지에 적합한 임계값을 조정하게 할 수 있게 함으로써 시스템의 상황에 적절히 대처할 수 있게 하였다.

참 고 문 헌

[1] S.Kumar and E.Spafford, "A pattern matching model for misuse intrusion detection." Seventeenth National Computer Security Conference, Baltimore, MD, October 1994, 11-21.

[2] S.Stolfo, A.Prodromidis, S. Tselepis, W. Lee, "Java Agents for Meta learning over Distributed Databases", in AAAI97 workshop on AI Methods in Fraud and Risk Management 1996.

[3] Neil Crowe and Sandra Schiavo, "An Intelligent Tutor for Intrusion Detection on Computer System", code Cs/rp, Department of Computer Science, Naval postgraduate school monterey, 1997

[4] Sandeep Kumar, gene Spafford. "A Pattern Matching Model for Misuse Intrusion Detection", Proceedings of the 17th National Computer Security Conference, October 1994.