문제1. 침입탐지시스템의 오용탐지 기법이 사용하는 6가지 방법론을 나열하고 해당 방법론에 대한 설명을 서술하시오.

ID : 8309156297
소속 : 삼원중공업
작성자 : 박용주
작성일 :2021.03.18

1. 침입탐지 방법론

침입탐지에는 두 개의 상보적인 흐름이 있다. 첫째는 공격에 관한 축적된 지식을 사용하여 어떤 공격을 사용하고 있다는 증거를 찾는 방식이며, 두 번째는 감시중인 시스템의 정상행위에 관한 참조모델을 생성한 후 정상행위에서 벗어나는 경우를 찾는 방식이다. 전자를 오용탐지 또는 지식기반 탐지기법이라고 하며 후자를 비정상행위탐지 또는 행위 기반 탐지기법이라고 한다.

2. 오용탐지 기법

1) 전문가시스템(Expert System)

전문가시스템은 공격에 관한 규칙집합을 가지고 있어 감사 이벤트가 전문가시스템 내에서 의미를 가지는 사실로 변환이 되고, 추론엔진은 이 규칙들과 사실을 기반으로 침입을 판단한다. 전문가시스템기법은 감사 자료에 의미를 부여함으로서 감사 자료의 추상화 정도를 증가시킨다.

전문가시스템에서 규칙기반언어(rule-based language)는 공격에 관한 전문가의 지식을 모델링 하기 위한 자연스러운 도구이다. 이 접근방식은 알려진 취약점을 이용하려는 시도들에 관한 증거를 찾기 위해 감사 자료를 체계적으로 탐색할 수 있도록 한다.

또한 보안정책이 적절히 적용되고 있는지 검증하는데 사용될 수도 있다. 하지만 전문가시스템의 전체적 성능은 아직 낮은 정도이며 늦은 처리속도로 인해 프로토타입 에서만 사용되며 상용제품들은 보다 효율적인 접근방식을 취한다. 대표적인 시스템으로는 RUSSEL이라는 규칙기반언어를 사용한 ASAX (Advanced Security audit trail Analysis on unix) 등이 있다.

2) 시그너쳐 분석(Signature Analysis)

시그너쳐 분석은 전문가시스템과 동일한 방식으로 지식을 획득하지만 지식을 사용하는 방식이 다르다. 공격에 대한 의미적 기술은 감사 자료에서 곧바로 검색이 가능한 형태의 정보로 변경된다. 예를 들면, 공격 시나리오는 공격 시 생성되는 감사이벤트 시퀀스로 변경 되거나 시스템에 의해 생성된 감사 자료에서 탐색할 수 있는 데이터 패턴으로 변경된다. 이 기법은 공

격에 관한 기술이 저수준에서 이루어진다.
시그너쳐 분석기법은 아주 효율적인 구현이 가능하므로 상업적인 침입탐지 제품에 응용되고 있다. 이 방식의 주약점은 다른 지식기반 접근방법과 마찬가지로 새로 발견된 취약점에 대해 자주 갱신을 해주어야 한다는 것이다.

3) 페트리넷(Petri-net)
페트리넷은 95년 Purdue의 S. Kumar의 박사학위 논문으로 기존 패턴 매칭 방법을 개선한 것으로 침입에 관한 시그너쳐를 표현하기 위해서 칼라페트리넷(CPN)을 사용하였다. CPN은 일반성, 개념적 단순성, 그래프 표현성 등의 장점을 가지고 있다. 시스템 관리자는 공격의 시그너쳐를 작성하고 IDIOT 시스템에 통합할 수 있다. CPN의 일반성으로 아주 복합한 시그너쳐도 쉽게 작성할 수 있다. 그러나 복잡한 시그너쳐를 감사자료와 비교하는 작업은 상당히 많은 계산비용을 요구한다. 이를 구현한 시스템으로는 '96년 Purdue의 COAST에서 개발한 IDIOT (Intrusion Detection System In Our Time) 시스템이 있다.

4) 상태전이분석(State Transition Analysis)
상태전이분석은 92년 UCSB의 P. A. Porras의 석사학위 논문으로 개념상으로는 모델기반 추론과 동일하다. 이 기법은 공격을 목표와 상태 전이의 집합으로 기술하며 상태전이 다이어그램으로 표현한 것으로 일반적으로 STAT라 부른다.
STAT 기반 침입탐지 방식이 처음 설계되고 도구로 개발된 것이 '92년 개발한 UCSB에서 개발한 USTAT이며 멀티 호스트로 확장한 것이 NSTAT이다. 현재 DARPA 프로젝트로 수행 중인 네트워크 기반 침입탐지시스템이 NetSTAT이다. STAT는 일부 상용 제품에서도 사용되고 있다.

5) 신경망(Neural Network)
신경망은 타당한 방법으로 새로운 입력-출력 쌍을 얻기위해 두 집합의 정보간 관련성을 학습하고 일반화하는데 사용되는 알고리즘 기법이다. 신경망은 이론적으로 지식기반 침입탐지 방식에서 공격을 학습하고 감사 스트림에서 탐색하는데 사용될 수 있다. 입력과 출력간의 관계를 알 수 있는 믿을만한 방법이 없으므로 신경망은 공격을 추론하거나 설명할 수 없어 주로 비정상행위 탐지 기법으로 많이 연구되었으나 최근에는 지식기반 프로파일을 구성하여 오용탐지 기법으로도 사용된다.

6) 유전 알고리즘(genetic algorithm)
유전 알고리즘은 자연 선택의 원리와 자연계의 생물 유전학에 기본 이론을 두며, 모든 생물은 주어진 다양한 환경 속에 적응함으로써 살아남는다는 다원의 적자생존(survival of the fittest)의 이론을 기본 개념으로 한다. GSSATA는 패턴 매칭에서 생기는 문제(backreferencing operator in a string)를 해결하기 위하여 공격시나리오로부터 시간에 대한 개념을 제거하고 여기에 John Helland가 제안한 유전 알고리즘을 사용하였다.