

오용탐지

1. 전문가 시스템 (Expert System)

공격에 관한 규칙 집합을 가지고있어 감사이벤트가 전문가 시스템내에서 의미를 가지는 사실로 변환이 되고 추론엔진은 이 규칙들과 사실을 기반으로 침입을 판단합니다

전문가 시스템 기법은 감사자료에 의미를 부여함으로서 감사자료에 추상화 정도를 증가시킵니다. 이 접근 방식은 알려진 취약점을 이용하려는 시도들에 관한 증거를 찾기 위해 감사자료를 체계적으로 탐색할수 있게 합니다.

또한 보안정책이 적절히 적용되고 있는지 검증하는데 사용할수도 있습니다. 하지만, 전문가 시스템의 전체적 성능은 아직 낮은 정도이며 늦은 처리 속도로 인해 프로토타입에서만 사용되며

대표적인 시스템으로는 러셀이라는 규칙기반언어를 사용

2. 시그니처 분석 (Signature Analysis)

전문가 시스템과 동일한 방식으로 지식을 획득하지만 지식을 사용하는 방식이 다릅니다.  
공격에 대한 의미적 기술은 감사자료에서 곧 바로 검색이 가능한 형태의 정보로 변경됩니다.

공격 시나리오는 공격 시 생성되는 감사이벤트 시퀀스로 변경되거나 시스템에 의해 생성된 감사자료에서 탐색할수 있는 데이터 패턴으로 변경되는 것입니다. 이 기법은 공격에 관한 기술이 저수준인 경우 시행됩니다.

시그니처 분석기법은 아주효율적 구현이 가능함으로 상업적인 침입탐지 제품에 응용되고 있습니다. 이방식의 주요 약점은 다른지식 기반 접근방법과 마찬가지로 새로발견된 취약점에 대해 자주 갱신해야합니다

3. 패트리넷 (Petei-net)

95년 쿠마의 기존패턴 매칭방법을 개선한것으로 침입에 관한 시그니처를 표현하기 위해 칼라패트리넷 cpn을 사용하였습니다. cpn은 일반성 개념적단순성 그래프표현성등의 장점

시스템 관리자는 공격의 시그니처를 작성하고 idiot시스템에 통합할수 있습니다. cpn 일반성으로 아주복잡한 시그니처도 쉽게 작성할수 있지만 복잡한 시그니처를 감사자료와 비교하는 작업은 상당히 많은 계산비용을 요구합니다

4. 상태전이분석 (State Transition Analysis)

공격을 목표와 상태전이의 집합으로 기술하며 상태전이 다이어그램으로 표현한것으로 일반적으로 stat라 불립니다.

stat기반 침입탐지 방식이 처음 설계되고 도구로 개발된것이 92년 개발한 ucsb에서 개발한 ustat이며 멀티호스트로 확장한것이 nstat입니다

현재 달파의 프로젝트로 수행중인 넷트워크 기반 침입탐지 시스템이 넷 stat입니다 신경망은 타당한 방법으로 새로운 입력 출력사항을 얻기 위해 두집합의 정보간 관련성을 학습하고 일반화 하는데 사용되는 알고리즘 기법입니다

5. 신경망 (Neural Network)

타당한 방법으로 새로운 입력 출력사항을 얻기위해 두 집합의 정보간 관련성을 학습하고 일반화 하는데 사용되는 알고리즘 기법입니다

신경망은 이론적으로 지식기반 침입탐지 방식에서 공격을 학습하고 감사스트림에서 탐색하는데 사용될수 있습니다 입력과 출력간의 관계를 알수있는 믿을만한 방법이 없음으로 신경망은 공격을 추론하거나 설명할수 없어 주로 비정상행위 탐지기법으로 많이 연구되었으나 최근에는 지식기반 프로파일을 구성하여 오용탐지 기법으로도 사용됩니다

6. 유전알고리즘 (genetic algorithm)

자연선택의 원리와 자연계의 생물유전학에 기본이론을 두며 모든 생물은 주어진 다양한 환경속에 적응함으로써 살아남는다는 다윈의 적자생존의 이론을 기본개념으로 합니다

gssata는 패턴매칭에서 생기는 문제를 해결하기 위하여 공격시나리오부터 시간에 대한 개념을 제거하고 여기에 존헬런드가 제안한 유전알고리즘을 사용하였습니다

이상입니다.