**오용 탐지**

서명 분석(signature analysis)

전문가 시스템(expert systems)

상태 전이 분석(state transition analysis)

페트리 넷(petri-nets)

**비정상행위 탐지**

통계(statistics)

전문가 시스템(expert systems)

신경망(neural networks)

컴퓨터 면역학(computer immunology)

데이터 마이닝(data mining)

HMM(Hidden Markov Models)

**(1) 오용 탐지 방법론**

서명 분석(signature analysis)

지식 기반 접근(knowledge based approach) 방식을 이용하는 침입 탐지 방법론으로서 침입 양상에 대하여 의미적인 단계를 부여하고 이에 대한 광범위한 정보를 축적한다. 감사 증적으로부터 감사 사건을 직접 검색하여 감사 사건의 기록 순서, 기록 패턴 등을 축적된 정보와 비교하여 침입을 탐지한다. 상용 침입탐지시스템 제품에 자주 적용되는 방법론이다. 대표적인 서명 분석 방식의 공개용 네트워크 기반 침입탐지시스템로서 Snort(http://www.snort.org/)가 있다.

전문가 시스템

서명 분석 방법론과 마찬가지로 지식 기반 접근을 이용한 탐지 방법론이다. 그림에서 예시하는 바와 같이 우선 순위 기반으로 수립된 규칙 집합(rule set)과 감사 증적의 사건들을 비교하여 침입을 탐지한다. 감사 데이터에 대한 추상적인 단계를 부여하며 각 공격 유형에 대한 지식들을 규칙 집합으로 표현한다. 추론 엔진(inference engine)은 사실(fact)로 변환된 감사 사건과 규칙 집합을 비교하며 규칙 집합의 관리를 위하여 규칙 기반 언어(rule based language)를 사용한다. 1992년, 벨기에에서 발표된 전문가 시스템 기반의 침입탐지시스템인 ASAX(Advanced Security audit trail Analysis on uniX)는 RUSSEL(RUle baSed Sequence Evaluation Language)이라는 규칙 기반 언어를 사용하며 1.0 버전이 공개용으로 배포되고 있다.

상태 전이 분석(state transition analysis)

그림에서 예시하는 바와 같이 침입을 상태 전이의 집합으로 표현한 상태 전이 다이어그램(state transition diagram)을 통하여 침입 탐지 과정을 분석하는 방법론으로서 UCSB(University of California, Santa Barbara)에서 개발하였다. 제품으로는 1992년도에 발표된 USTAT(A Real-time Intrusion Detection System for Unix), 1997년에 발표된 NSTAT(A Model-based Real-time Network Intrusion Detection System) 등이 있다.

페트리 넷(petri-nets)

퍼듀(Purdue)대학교에서 개발한 지식 기반 침입 탐지 방법론이다. 그림에서 예시하는 바와 같이 Colored Petri-Nets(CPNs)을 사용하여 침입탐지시스템의 행위를 모델링하고 있다. 페트리 넷은 복잡하고 분산된 시스템을 추상화한 모델을 정립하는데 매우 유용하며 페트리 넷을 이용하여 침입탐지시스템을 모델링 할 경우 개념적으로 단순화가 가능하고 도식적인 표현이 가능하므로 복잡한 침입탐지시스템의 행위들의 집단화(gathering), 분류(classification), 상관 관계(correlation) 등을 매우 효과적으로 설명할 수 있다. 퍼듀대학교의 COAST(Computer Operations, Audit, and Security Technology) 프로젝트의 일환으로 개발된 IDIOT(Intrusion Detection In Our Time) 시스템은 페트리 넷 기반의 침입 패턴 매칭 엔진을 탑재하여 효과적인 오용 탐지 기능을 제공한다.

**(2) 비정상행위 탐지 방법론**

통계(statistics)

통계 기반 탐지 방법론은 침입탐지시스템에 가장 많이 적용되는 방법론으로서 통계적인 공식을 사용하여 침입 가능성을 추정한다. 모든 상태 변수의 평균값을 도출하여 침입 판정에 사용하며 대부분의 상용 시스템에서 사용하는 방법론이다. IDES(the Intrusion Detection Expert System)는 통계 기반 탐지 방법론을 사용하는 SRI International's System Design Laboratory의 규칙 기반 침입 탐지 전문가 시스템이다.

IDES는 최근 NIDES(the Next-Generation Intrusion Detection Expert System)로 확장되었으며 EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbances) 기능을 지원할 계획에 있다.

NIDES는 사용자 행위에 대하여 빈도(frequency), 평균(means), 분산(covariance)과 같은 통계치 프로파일을 유지하여 단기 프로파일과 장기 프로파일을 비교하여 침입을 추정한다. 그림은 NIDES의 실시간 처리 흐름도를 예시한다.