통계

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.

전문가 시스템

규칙 기반 비정상행위 탐지 방법론으로서 사용 패턴을 표현하는 규칙 집합을 사용하여 침입을 탐지한다. Los Alamos National Laboratory에서 개발한 Wisdom & Sense는 사용자 행위를 주기적으로 기록하여 통계적인 사용자 프로파일을 구축한다. 공격자가 해당 사용자의 권한으로 해당 사용자의 일상적인 행위를 벗어나는 행위를 하는 경우 해당 사용자 프로파일에 근거하여 이를 탐지한다. ComputerWatch data reduction 도구는 AT&T Bell 연구소의 SSD(Secure Systems Department)에서 AT&T System V/MLS 시스템의 다단계 보안 기능의 제공을 위하여 개발되었다. ComputerWatch는 시스템의 행위가 기록된 감사 증적 데이터로부터 통계적인 기법을 사용하여 비정상적인 행위를 탐지해 낼 수 있다.

신경망

일반적으로 신경망은 컴퓨터가 인간 두뇌의 학습 기능을 갖게 하기 위하여 고안되었다. 신경망은 생물학적 신경단위인 뉴런을 모델링한 유닛(unit)들과 유닛 사이의 가중치 연결 (weighted-connection)들로 구성된다. 신경망은 불완전하고 다양한 입력의 해석, 패턴 인식(pattern recognition), 학습, 분류, 일반화, 추상화 등이 필요한 분야에 유용하게 활용되고 있다. 특히, 논리적이고 분석적인 기법을 활용해서도 시뮬레이션하기 어려운 인간의 문제 해결에도 효과적으로 활용되고 있다. 신경망을 이용한 침입탐지시스템은 다양한 행위 예들로부터 침입을 탐지할 수 있고 자동 학습 기능이 있어서 변화하는 공격 패턴에 대하여 능동적으로 대처할 수 있지만 구현이 어려워서 널리 사용되지는 않고 있다.

컴퓨터 면역학

New Mexico 대학교의 Stephanie Forrest가 제안한 방식으로서 컴퓨터 면역학을 침입탐지시스템에 적용하여 유닉스 네트워크 서비스의 정상적인 행위를 모델링 했으며 시스템 호출(system call)의 순서 패턴을 모니터링하여 비정상행위를 탐지한다.

데이터 마이닝

데이터 마이닝이란 대량의 데이터로부터 패턴을 찾고 규칙을 추론함으로서 의사결정을 지원하는 과정을 의미한다. 대표적인 데이터 마이닝 기법으로는 사건들의 연관성(associations) 탐사, 연속성(sequences) 탐사, 분류(classifications) 규칙 탐사, 군집 구분(clustering) 등이 있다.

HMM

최근까지 음성 인식 분야에서 많이 사용되었던 HMM은 관찰 가능한 데이터로부터 은닉된 정보를 찾아내는 과정을 모델링 한 데이터 분석 및 예측 기술이다. HMM 기반 침입탐지시스템은 정상 행위 기반으로 구성된 사용자 프로파일의 임계값보다 낮은 임계값을 요구하는 시스템 호출을 검사함으로서 침입을 탐지하고 있다.