통계(statistics)

가장 많이 적용되는 방법론으로서 통계적인 공식을 사용하여 침입 가능성을 추정한다.

모든 상태 변수의 평균값을 도출하여 침입 판정에 사용하며 대부분의 상용 시스템에서 사용하는 방법론이다.

전문가 시스템(expert systems)

규칙 기반 탐지 방법론으로서 사용 패턴을 표현하는 규칙 집합을 사용하여 침입을 탐지한다.

공격자가 해당 사용자의 권한으로 해당 사용자의 일상적인 행위를 벗어나는 행위를 하는 경우

해당 사용자 프로파일에 근거하여 이를 탐지한다.

신경망(neural networks)

일반적으로 컴퓨터가 인간 두뇌의 학습 기능을 갖게 하기 위하여 고안되었다.

신경망은 생물학적 신경 단위인 뉴런을 모델링한 유닛들과 유닛 사이의 가중치 연결들로 구성된다.

컴퓨터 면역학(computer immunology)

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(data mining)

대량의 데이터로부터 패턴을 찾고 규칙을 추론함으로서 의사결정을 지원하는 과정을 의미한다.

HMM(Hidden Markov Models)

최근까지 많이 사용되었던 HMM은 관찰 가능한 데이터로부터 은닉된 정보를 찾아내는 과정을

모델링 한 데이터 분석 및 예측 기술이다.

출처: https://sugerent.tistory.com/461 [MISTERY]