☞ 침입탐지시스템의 오용탐지 기법이 사용하는 6가지 방법론과 더불어 추가적으로 비정상행위 탐지 방법론에 대한 내용까지 포괄적으로 나열하고 각각의 해당 방법론에 대한 간략한 핵심내용 설명을 서술하였습니다. (과제제출자 나태호)

(주요내용)

침입 탐지 방법론은 탐지를 분석하는 방법에 따라 크게 오용 탐지와 비정상행위 탐지로 분류된다. 오용 탐지와 비정상행위 탐지의 적용 기술에 따른 세부 분류는 다음과 같다.

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.

● 전문가 시스템(expert systems)  
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(neural networks)  
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(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)  
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.

미 국방성의 DARPA(Defense Advanced Research Projects Agency) 프로젝트 “Fraud and Intrusion Detection for Financial Information Systems using Meta-Learning Agents”의 일환으로 추진된 Columbia 대학교의 JAM(Java Agents for Meta learning) 프로젝트에서는 분산 환경에서 이식성과 확장성을 제공하는 에이전트 기반 침입탐지시스템이 개발되었다. 데이터 마이닝 기술이 적용된 이 시스템은 비정상행위의 탐지를 위해 meta-learning 기술을 사용하고 있다.

● HMM(Hidden Markov Models)  
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.