[5B-42]

DesignCPN을 이용한 네트워크 비정상행위 탐지 기법

김현정, 엄남경, 이상희, 이상호
충북대학교 전자계산학과
triumph@netsec.cbnu.ac.kr

Approach for Anomaly Detection on Network using DesignCPN

Hyun Jung Kim, Nam Kyung Um, Sang Hee Lee, Sang Ho Lee
Computer Science Dept, Chung-Buk Univ.

요 약

IDS(Intrusion Detection System : 이하 IDS 라 함)를 위한 비정상행위 탐지 기법이란 정상 행위의 프로파일을 정의한 후, 이에 반하여 발생되는 비정상행위를 탐지해내는 IDS 탐지분석 기법 중의 하나로써, 통계적 기법, 신경망, 면역학 등을 기반으로 정상 행위를 학습시킨다. 그러나 정상 행위에 대한 학습 시간이 지나치게 길어지는 문제점으로 인해, 이를 보완하기 위한 명세 기반의 방법론을 비정상행위 탐지에 활용하는 방안이 대두되고 있다. 이 논문에서는 기존의 명세 기반 방법론인 상태-전이 모델과 EFSA(Expended Finite State Automata)등이 갖는 동시상태제어 불가, 전이 조건의 획일성 등을 보완할 수 있도록 CPN(Coloured Petri Net)을 이용한 비정상 행위 탐지용 시험열을 생성하고자 한다. 이 시험열을 통해 정상 상태가 아닌 침입으로 간주되는 유형을 빠른 속도로 탐지할 수 있다.

I. 서론

인터넷의 발전함에 따라, 네트워크를 통해 침입을 시도하는 공격자들로 인한 피해 또한 기하급수적으로 증가하고 있다. 따라서 네트워크 상의 침입을 예방하고 탐지하는 시스템이 개발되고 있는 실정이다. 현재 침입탐지시스템은 침입에 대한 분석 기법에 따라 오용 탐지(Misuse Detection), 비정상행위 탐지(Anomaly Detection), 복합 탐지(Hybrid Detection)으로 나누어지고 있다. 오용 탐지는 네트워크 상의 침입에 해당되는 흔적을 이용해 프로파일을 형성하여 침입 탐지에 이용하는 방식으로 새롭게 생성되는 공격유형을 빠르게 프로파일로 형성해야 한다는 단점을 가진다. 비정상행위 탐지는 정상 행위에 대한 프로파일을 생성하고 이에 반하는 행위를 침입으로 규정짓기 위한 기법으로 오용 탐지 기법의 단점을 보완할 수 있으나, 정상 행위에 대한 학습 시간이 지나치게 길어질 수 있다는 문제점을 가질 수 있다. 복합 탐지를 탐지 방식을 혼합하는 방식이나, 타 방식에 비해 구현 면에서 매우 복잡하다는 단점을 가진다. 이 논문에서는 비정상 행위 탐지 기법이 정상 행위의 학습 시간이 길어지며, 학습에 대한 고비용이 들게 됨을 보완하기 위해 CPN 을 지원하는 DesignCPN 툴을 이용하여 상태 기반의 정상 행위를 형성하는 기법을 제안한다. 이 방식은 명세 기반 방법론인 상태-전이 모델과 EFSA 등이 갖는 동시상태 제어 불가, 전이 조건의 획일성 등을 보완할 수 있어 저비용의 빠른 비정상 행위 탐지를 할 수 있게 된다[1][2].

이 논문의 구성은 다음과 같다. 2 장에서는 관련 연구에 대해 다루고, 3 장에서는 이 논문에서 제안하는 CPN 을 이용한 비정상행위 탐지 기법에 대해 기술한다. 4 장에서는 DesignCPN 툴을 이용한 시험열 탐지 기법에 대해 다룬 후, 5 장과 6 장에서는 각각 실험 및 평가와 결론 및 향후 연구 방향을 제시하고자 한다.

II. 관련 연구

2.1 침입 탐지 기법 분류

침입 모델에 따라 오용 탐지 기법, 비정상행위 탐지기법, 복합 탐지 기법으로 나누어지고 있으며, 침입탐지에 필요한 기록(Audit Data)을 어디에서 획득하느냐에 따라 호스트기반 침입탐지 시스템(Host-based IDS), 복합호스트 기반 침입탐지 시스템(Multi-Host Based IDS), 네트워크 기반 침입탐지 시스템(Network based IDS)로 분류하고 있다[3].

오용 탐지 기법에 속하는 연구로는 전문가 시스템(Expert System)에서 RUSSEL 이라는 규칙 기반 언어를 이용한 ASSX (Advanced Security audit trail Analysis on uniX), 흔적 분석(Signature Analysis), 페트리 네트(Petri Net), 상태 전이 분석(State Transition Analysis) 등을 이용한 방법론이 있다. 또한 비정상행위 탐지 기법에 속하는 연구로는 통계적 기법을 이용한 미국의 DARPA 에서 추진하는 프로젝트의 일환인 NIDES, EMERALD 등이 있고, 전문가 시스템, 신경망(Neural Network), 컴퓨터 면역학(Computer Immunity)에 의한 방식 등이 정상 행위 모델링에 사용되고 있다. 또한 데이터 마이닝을 이용한 방식의 JAM(Java Agent for