# 멀티 모달 침입 탐지 시스템에 관한 연구

하회리*, 안선우*, 조명현*, 안성관* 백윤흥*
*서울대학교 전기,정보공학부, 반도체공동연구소
wrha@sor.snu.ac.kr, swahn@sor.snu.ac.kr, mhcho@sor.snu.ac.kr, sgahn@sor.snu.ac.kr, ypaek@snu.ac.kr

# A Study on Multimodal Neural Network for Intrusion Detection System

Whoi Ree, Ha*, Sunwoo, Ahn*, Myunghyun, Cho*, Seonggwan, Ahn*, Yunheung, Paek*
*Dept. of Electrical and Computer Engineering and Inter-University Semiconductor Research Center (ISRC),
Seoul National University

**요 약**

최근 침입 탐지 시스템은 기존 시그니처 기반이 아닌 AI 기반 연구로 많이 진행되고 있다. 이는 시그니처 기반의 한계인 이전에 보지 못한 악성 행위의 탐지가 가능하기 때문이다. 또한 로그 정보는 시스템의 중요 이벤트를 기록하여 시스템의 상태를 반영하고 있기 때문에 로그 정보를 사용한 침입 탐지 시스템에 대한 연구가 활발히 이루어지고 있다. 하지만 로그 정보는 시스템 상태의 일부분만 반영하고 있기 때문에, 회피하기 쉬우며, 이를 보완하기 위해 system call 정보를 사용한 멀티 모달 기반 침입 시스템을 제안한다.

## 서론

침입 탐지 시스템 (intrusion detection system)은 시스템의 비정상적 행위를 탐지하기 위한 보안 프로그램이다. 일반적 행위에 나타나지 않는 조작은 악의적인 행위에 의한 것이라고 생각할 수 있기 때문에, 침입 탐지 시스템은 오래전부터 현재까지 꾸준히 연구되고 있다. 기존에는 말웨어 또는 악성 행위들을 분석하여 특징을 찾는 시그니처 기반 침입 탐지 시스템이 대다수를 이루었지만, 최근에는 AI 기반 연구들도 많이 증가하였다.

AI 를 침입 탐지 시스템에 사용하는 가장 큰 이유는 분석되지 않은 악성 행위를 탐지 할 수 있기 때문이다. 시그니처 기반 침입 탐지 시스템은 악성 행위의 특징을 저장하고 현재 행위와 비교하여 악성 행위를 탐지하기 때문에, 특징이 저장되지 않은 악성 행위나, 향후에 제작된 악성 행위들에 대해서는 취약하다. 하지만 AI 기반 침입 탐지 시스템은 시스템의 정상 행위를 학습하여 비정상 행위를 탐지하기 때문에 처음 보는 악성 행위도 탐지 할 수 있다.

## 로그 기반 비정상 행위 탐지

시스템에 있는 다양한 데이터들이 비정상 행위를 탐지하는 데에 사용될 수 있지만, 최근 각광받고 있는 분야는 시스템 로그를 사용한 비정상 행위 탐지이다. 시스템 로그는 시스템의 중요 이벤트를 기록하기 때문에, 해당 시스템의 상태를 반영하고 있다. 또한 실행되고 있는 상황에서 로그가 발생하여 비정상 행위를 실시간으로 탐지할 수 있다.[1] 실제로 DeepLog (CCS '17)를 필두로 로그를 NLP 기법을 활용하여 정상 패턴을 학습하고, 비정상 행위를 탐지하는 연구들이 발표되고 있다.[2]

하지만 로그 정보는 현재 시스템 상태의 일부분 만

을 반영하고 있다. 어떤 로깅 프로그램을 사용하는지에 따라 다르겠지만, 로깅 프로그램에서 지정한 "중요" 이벤트를 기록하기 때문에 시스템의 세부적인 상황은 나타나지 않는다. 따라서 로그에 반영되지 않는 공격들은 탐지되지 않고, 이 특성을 이용하면 쉽게 로그 기반 비정상 행위 탐지를 회피할 수 있다.

실제로 DeepLog 에서 제안된 로그 기반 비정상 행위 탐지 모델을 구현하여 실험하였을 때, <그림 1>과 같이 논문과 비슷한 F1 점수를 가지는 모델에 대해서 모방 공격을 진행하면, <그림 2> 에서 볼 수 있듯이 취약하다는 것을 알 수 있다.

<그림 1> DeepLog 재현 실험

| | Total | Detection by key | Detection by parameter | TRUE | FALSE | Precision | Recall | F1-score |
|---|---|---|---|---|---|---|---|---|
| Normal Data | 10,000 | 28 | 55 | 9,917 | 83 | 99.47 | 93.25 | 96.26 |
| Anomlay | 16,838 | 15,610 | 91 | 15,701 | 1,137 | | | |

<그림 2> DeepLog 에 대한 모방 공격 실험

| | Total | Detection by key | Detection by parameter | percentage |
|---|---|---|---|---|
| Mimicry Attack | 4,739 | 0 | 0 | 0.00% |

### 멀티 모달 학습

딥러닝에서는 한가지 변수 차원에서 오는 한계를 극복하기 위해 여러 변수 차원을 학습함으로써 정확도를 높이는 연구들이 있다. 예를 들면, 음성 인식 분야에서는 소리 데이터와 입 모양 데이터를 결합하여, 소리 데이터만 사용하는 모델보다 정확도를 높였다.[3] 이 연구에 영감을 받아 본 연구는 로그 데이터의 한계를 극복하기 위한 멀티 모달 인공 신경망을 제안한다.

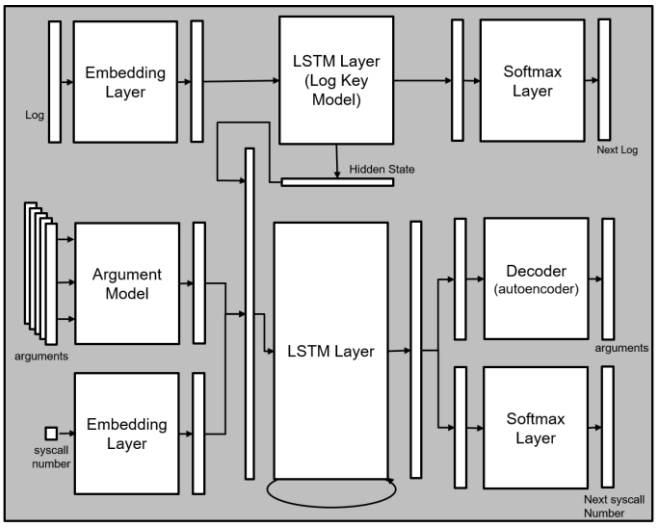
멀티 모달 학습의 이점을 극대화하기 위해서는 학습되는 데이터 타입의 특성이 서로를 상호보완 할 수 있어야 한다. 로그는 중요 이벤트의 결과를 기록하는 대신 다른 runtime 정보에 비해 간간히 발행하는 특성이 있다. 따라서 로그와 상호보완적인 데이터는 로그에서 기록하지 않는 세부 runtime 정보를 기록하여 악성 행위의 과정을 기록하여야 한다.

System call 은 user space 에서 kernel space 로 요청하는 서비스들로, 침입 탐지 시스템에 사용될 수 있는 데이터 타입 중 하나이다. 하지만 system call 은 일초에 수십 번씩 발생하여, 데이터의 양이 너무 방대하고 process 별로도 발생하기[4] 때문에 관리가 용이하지 않아, 최근 연구에는 잘 사용되지 않는다. 하지만 세부 runtime 정보를 반영하고, 현재 행위의 과정을 기록하고 있기 때문에 로그와 상호보완적인 데이터 타입이라고 할 수 있다. 또한 시스템 로그와 같이 사용하게 된다면, 각 process 를 모니터링 하지 않고 kernel 만 모니터링 하면 되기 때문에, kernel 에서 발생한 system call 로 한정되어 기존 단점들을 상쇄할 수 있다.

### 멀티 모달 기반 침입 탐지 시스템

이 연구에서는 로그와 system call 을 모두 학습할 수 있는 새로운 멀티 모달 기반 비정상 행위 탐지 모델을 제시한다. <그림 3>에서 볼 수 있듯, 두 정보 모두 sequential 데이터 처리에 좋은 성능을 보이는 LSTM 레이어를 사용하였고, 두 정보를 상관시켜 학습 하려고 한다.

<그림 3> 멀티 모달 인공 신경망




System call 은 설명한 바와 같이 일초에 수십 번씩 일어난다. 따라서 여러 단계에 거쳐 공격이 진행될 경우, 단계 사이사이에 너무 많은 system call 정보가 생겨 연관성이 흐려질 수 있다. 이를 보완하려 간간

히 발생하는 로그 정보를 사용하고자 한다. 로그 정보를 처리하는 로그 모델의 hidden state 를 system call 과 연관시켜 준다면, 전달 받은 hidden state 를 통해 시스템의 전체적인 상황을 알 수 있고, 이를 system call 과 연관 지어 학습 가능하다.

모방 공격에 대해서도 기존 DeepLog 에서 보여준 방식보다 더 robust 할 것으로 예상된다. 단순히 로그를 모방하거나, 로그를 발생시키지 않는 악성 행위들은 system call 정보를 통해서 탐지 될 것이기 때문이다. 또한, 반대로 system call 에 많은 no-op 을 넣어 모방 공격을 하는 경우에는 로그 정보를 통해 더 정확한 탐지가 가능할 것으로 생각된다.

## 결론

비정상 행위를 탐지하는 방식은 크게 두가지로 나뉜다. 기존 악성 행위를 분석하여 특징을 저장해 탐지하는 시그니처 기반과, 인공지능을 사용한 AI 기반 비정상 행위 탐지이다. 하지만 기존 악성 행위만 잡을 수 있는 한계점 때문에, AI 기반 비정상 행위 탐지 분야가 활발히 연구되고 있으며, 특히 시스템 로그를 사용한 연구들이 최근에 출판되고 있다. 하지만 시스템 로그 정보는 불완전한 시스템 상황을 나타내기 때문에, 상호보완적 관계에 있는 system call 정보를 사용한 멀티 모달 학습 방식을 통해 더 나은 침입 탐지 시스템을 설계 하였다.

**Acknowledgement**

본 연구는 2021 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2020R1A2B5B03095204). 2021 년도 BK21 FOUR 정보기술 미래인재 교육연구단에 의하여 지원을 받아 수행된 연구임. 2020 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2018-0-00230, (IoT 총괄/1 세부) IoT 디바이스 자율 신뢰보장 기술 및 글로벌 표준 기반 IoT 통합보안 오픈 플랫폼 기술개발 [TrusThingz 프로젝트])

## 참고문헌

[1] Min Du, Feifei Li, Guineng Zheng, and Vivek Srikumar. 2017. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '17*). Association for Computing Machinery, New York, NY, USA, 1285–1298. DOI:https://doi.org/10.1145/3133956.3134015

[2] Yun Shen, Enrico Mariconti, Pierre Antoine Vervier, and Gianluca Stringhini. 2018. Tiresias: Predicting Security Events Through Deep Learning. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (*CCS '18*). Association for Computing Machinery, New York, NY, USA, 592–605. DOI:https://doi.org/10.1145/3243734.3243811

[3] T. Afouras, J. S. Chung, A. Senior, O. Vinyals and A. Zisserman, "Deep Audio-visual Speech Recognition," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, doi: 10.1109/TPAMI.2018.2889052.

[4] Gyuwan Kim, Hayoon Yi, Jangho Lee, Yunheung Paek, Sungroh Yoon (2016) *LSTM-Based System-Call Language Modeling and Robust Ensemble Method for Designing Host-Based Intrusion Detection Systems*, arXiv: .