24

딥러닝을 이용한 악성파일 탐지 기술

기술개요

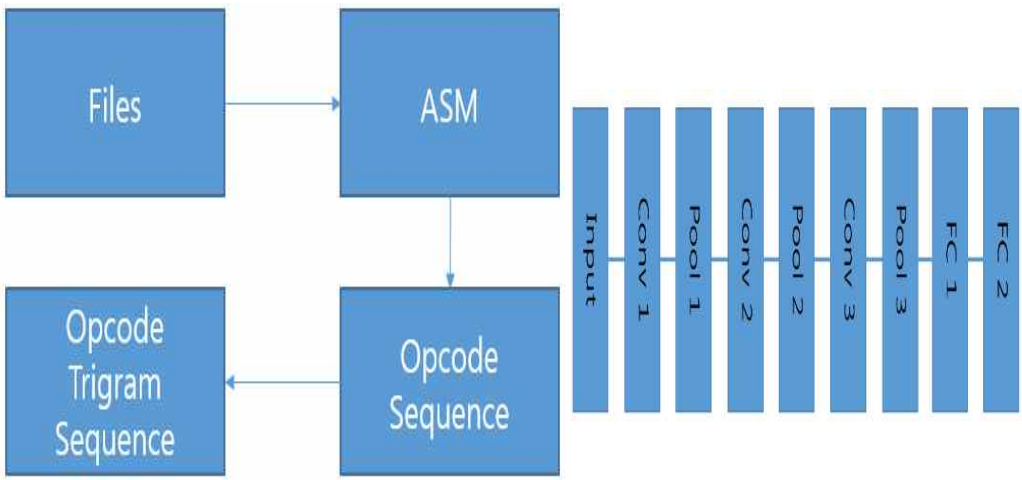
▪ 딥러닝을 이용한 악성파일 탐지 프로그램

- 정상파일 및 악성파일로부터 악성파일 탐지를 위한 딥러닝 모델을 학습하고 라벨링이 되어있지 않은 정상파일 및 악성파일이 주어졌을 때 악성 여부를 탐지하는 기술

기술의 특장점

▪ 악성파일을 탐지하기 위하여 PE파일의 opcode를 전처리 데이터로 사용

- opcode를 전처리 데이터로 사용하기 때문에 api 시스템콜을 전처리 데이터로 사용하는 기존 방식보다 훨씬 빠르게 학습 및 테스트 데이터를 수집할 수 있음
- 딥러닝 방식을 사용하여 머신러닝 방식에 비해 전처리가 수월하고 높은 탐지율을 보임
- 딥러닝 모델 사용으로 대용량의 데이터에 대한 학습이 용이함



< 딥러닝을 위한 전처리 과정 >

< 악성파일 탐지를 위한 딥러닝 모델 >

적용분야

▪ 악성파일 탐지 및 대응 시스템

- 기존의 안티바이러스 업체에서 자신의 안티바이러스 엔진 보완
- 국방 및 기관에서 네트워크로 유입되는 악성여부 판단
- 패턴이 알려지지 않은 제로데이성 악성파일에 대응

기술완성도 (TRL)

▪ TRL 4단계; 실험실 규모의 소재/부품/시스템핵심성능 평가 단계

기술이전 내용 및 범위

▪ 기술이전 내용

- 정상파일 및 악성파일 전처리 기술
- 악성파일탐지를 위한 딥러닝 모델 트레이닝 기술
- 악성파일탐지를 위한 딥러닝 모델 테스트 기술

▪ 기술이전 범위

- 소스코드: ASM 추출 모듈, opcode 추출 모듈, 트라이그램 추출 모듈, 딥러닝 트레이닝 모듈, 딥러닝 테스트 모듈
- 문서: 시스템 설계서, 개발문서, 기술문서

관련 지재권 현황

No.	출원번호	특허 명	상태
1	2017-0130810	파일 이미지를 이용한 악성코드 탐지 방법 및 이를 위한 장치	출원
2	2017-0001184	클라우드 기반으로 악성코드를 탐지하는 장치 및 이를 이용한 방법	출원
3	2017-0010978	네트워크 보안기능 가상화 기반의 클라우드 보안분석장치, 보안 정책 관리 장치 및 보안 정책 관리 방법	출원

기술이전 문의

▪ 연구성과확산실 (02-597-1260 / curl@etri.re.kr)