제 22주년 한국정보보호학회 충청지부 학술대회 및 정기 총회

2018년 2월 9일(금)
공주대학교 간호보건대학

주관 : 공주대학교 의료정보학과
주최 : 한국정보보호학회 충청지부

후원 : 위너다임, 네이버시스템, 오픈링크시스템
아이티센, 대신정보통신, 숭실대학교 사이버보안연구센터
충남대학교 핀테크보안연구센터, 에스제이정보통신

목 차

KIISC Korea Institute of Information Security and Cryptology Chungnam

바이너리 파일 시각화 기반 소프트웨어 보안약점 탐지를 위한 파일 섹션단위 시각화 기법에 대한 성능 검증

박 건 호* 최 대 선** 박 기 웅***

요 약

최근 소프트웨어 수가 많아지면서 취약점에 대한 탐지의 필요성이 증가한다. 전통적인 퍼징 테스팅 기법에서 딥러닝을 결합한 소프트웨어 취약점 탐지 방법까지 소프트웨어 취약점 탐지에 대해 다양한 방법으로 연구가 진행되고 있다. 본 논문에서는 Convolutional Neural Network(CNN)를 소프트웨어 보안약점 탐지에 사용하기 위해, 바이너리 파일 시각화 과정에서 활용할 수 있는 파일 섹션단위 시각화 기법을 제안하고 이에 대한 성능을 검증한다. 파일 섹션단위 시각화 기법을 적용한 이미지를 사용하여 CNN 학습 및 평가를 한 결과 97.05%의 정확도를 보이는 것으로 나타났다.

I. 서 론

현재 우리는 소프트웨어 속에서 살아가고 있다. 4차 산업 혁명이 생활과 밀접하게 다가오면서, 모바일 디바이스, IoT 디바이스 등 컴퓨팅 시스템을 일상생활 곳곳에서 만날 수 있고 그에는 많은 소프트웨어들이 탑재된다. 소프트웨어의 수가 많아지면서 소프트웨어 취약점 역시 많아졌다. 이런 현상을 반영하기 위해 알려진 취약점에 대한 리스트를 제공하는 Common Vulnerabilities and Exposures(CVE)는 소프트웨어 취약점에 부여하는 일련번호를 4자리에서 5자리로 확대하였다. 소프트웨어 취약점이 많아짐에 따라 소프트웨어 취약점 탐지에 관한 필요성이 증가한다. 전통적인 퍼징 테스팅 기법에서 딥러닝을 결합한 소프트웨어 취약점 탐지 방법까지 소프트웨어 취약점 탐지 방법에 대한 다양한 연구가 진행되고 있다. 그 중 한 연구 [3]는 바이너리 파일의 시각화를 통해 생성된 이미지를 CNN 알고리즘을 통해 학습 및 평가하여 소프트웨어 보안약점 탐지에 대한 유용성을 검증하였다. 해당 논문에서 활용한 딥러닝 알고리즘 중 하나인 CNN은 서로 다른 종류의 이미지의 특징을 분석하여 이미지 종류를 분류하는 것에 탁월한 성능을 보인다. CNN은 입력되는 데이터가 이미지라는 전제조건이 존재하기 때문에 파일의 바이너리 값과 같은 비이미지 데이터를 CNN에서 사용하기 위해서는 비이미지 데이터를 이미지로 변환하는 시각화 작업이 필요하다. 이 과정에서 비이미지 데이터를 시각화할 때 적용되는 시각화 기법에 따라 CNN의 성능이 달라질 수 있다.

본 논문에서는 바이너리 파일 시각화 기반 소프트웨어 보안약점 탐지를 위해 파일 섹션단위 시각화 기법을 제안하고 이에 대한 성능을 검증하고자 한다. 파일 섹션단위 시각화 기법이란 바이너리 파일을 섹션별로 분할한 뒤, 분할한 하나의 섹션단위가 이미지의 한 구역을 형성하도록 시각화하는 것을 의미한다. 앞서 소개한 기초 연구를 바탕으로 바이너리 파일 섹션단위 시각화 기법을 적용하여 성능을 검증한다. 기초 연구에서 사용한

본 연구는 한국연구재단 연구과제(NRF-2017R1C1B2003957, NRF-2016R1A4A1011761) 지원으로 수행되었습니다.
* 세종대학교 정보보호학과 시스템보안연구실 (imguno0629@naver.com)
** 공동교신저자: 공주대학교 의료정보학과 교수 (sunchoi@kongju.ac.kr)
*** 공동교신저자: 세종대학교 정보보호학과 교수 (woongbak@sejong.ac.kr)

PE 파일 셋에 본 연구에서 제안한 파일 섹션단위 시각화 기법을 적용하고 CNN의 학습 및 평가를 거쳐 정확도를 측정하여 성능을 검증한다.

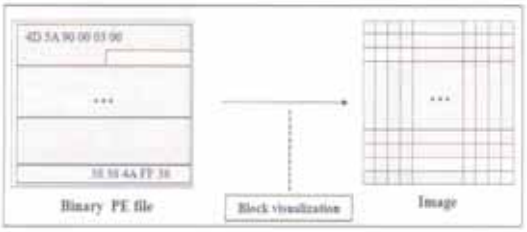
본 논문의 구성은 2장에서 관련 연구를 소개하고, 3장에서는 파일 섹션단위 시각화 기법에 대해 서술한다. 4장에서는 실험과 실험 결과에 대해 기술하며, 5장에서 결론과 향후 연구 방향에 대해 제시한다.

II. 관련 연구

CNN은 이미지를 입력으로 받는 알고리즘이기 때문에 시각화 작업이 선행적으로 요구된다. Cortesi [2] 는 파일의 Byteclass, Entropy를 시각화하여 이미지를 생성하는 방법에 대해 웹에서 공개하고 있다. 시각화한 바이너리 파일을 CNN에서 활용한 연구가 진행되었다. 석선회 [1] 는 악성코드의 패밀리를 분류하기 위해 Microsoft 데이터 셋과 VXHeavens 데이터 셋을 시각화한 이미지를 생성하여 CNN을 통해 악성코드의 패밀리를 분류하였다. 또한 본 논문의 기초 연구가 되는 박건호 [3] 는 소프트웨어 보안약점에 대한 코드인 Juliet Test Suite 중 CWE 190 Integer Overread을 시각화하여 소프트웨어 보안약점 발견에 대한 유용성 검증 연구를 진행하였다. 소프트웨어 보안약점의 존재유무에 따라 생성한 PE 파일의 바이너리 Offset 순서대로 픽셀을 그리는 Line 시각화 기법을 적용하여 이미지를 생성하고, CNN을 통해 학습 및 평가를 거쳐 정확도를 검증하였다.

III. 파일 섹션단위 시각화 기법

소프트웨어 보안약점 탐지를 위한 바이너리 파일 시각화를 위해 제안하는 파일 섹션단위 시각화 기법은 [그림 1]과 같다. CNN은 이미지의 지역성을 활용하여 이미지의 특징을 분석한다. CNN은 이미지의 지역성을 기반으로 인접한 픽셀 간 관계에 대한 정보를 수집하여 이미지 상의 한 객체에 대한 특징을 분석한다. 파일 섹션단위 시각화 기법은 소프트웨어 보안약점 탐지를 위한 바이너리 파일의 시각화 과정에서 파일 내 한 섹션 단위가 이미지 상에서 지역성을 가질 수 있도록 파일을 섹션단위로 분할하여 시각화한다. 해당 기법을 사용한 이미지는 파일의 한 섹션단위 별로 한 구역을 형성하여 이미지에 표현되어 이미지 상에서 파일의 구조가 나타나게 된다. 파일 섹션단위 시각화 기법과 비교할 수 있는 Line 시각화 기법은 파일의 바이너리 Offset 순서대로 이미지의 픽셀을 그려 시각화를 한다. 해당 기법은 파일의 바이너리 순서가 이미지 상에서 그대로 나타나게 된다.

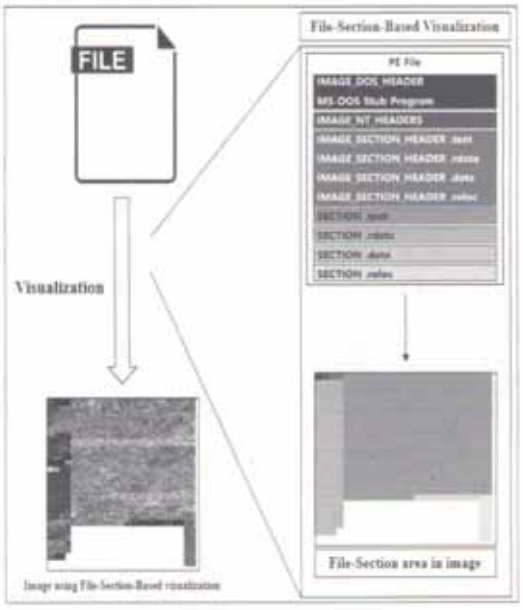


[그림 1] File-Section-Based Visualization Encoding Schema

IV. 실 험

본 장에서는 파일 섹션단위 시각화 기법을 적용한 바이너리 파일의 시각화 이미지를 생성하여 CNN을 사용한 학습 및 평가로 정확도를 측정한다. 실험에는 기초연구와 동일하게 National Institute of Standards and Technology(NIST)에서 제공하는 Juliet test suite의 CWE 190 Integer Overread를 활용하여 실험을 한다. CWE 190 Integer Overread를 소프트웨어 보안약점의 존재유무에 따라 보안약점이 존재하는 버전과 존재하지 않는 버전으로 나누어 각각 PE 파일로 컴파일 한다. 컴파일한 PE 파일을 [그림 2]와 같이 파일 섹션단위 시각화 기법을 적용하여 이미지를 생성한다. 파일 섹션단위 시각화 기법을 적용하기 위해 PE 파일 내 섹션을 구분하는 작업이 선행된다. 본 실험에서는 PE 파일의 PE 헤더를 나누어 논리적 섹션 별로 단위를 설정하여 시각화를 진행한다. 각 섹션 내 데이터를 3bytes씩 읽어 하나의 RGB 픽셀로 매핑시켜 이미지를 생성한다. 파일 섹션단위 시각화 기법을 이용하여 생성한 이미지 2,342개를 사용하여 CNN을 통한 학습 및 평가로

성능을 검증한다. 실험 결과 CNN은 97.05%의 정확도로 소프트웨어 보안약점의 존재유무에 따라 시각화된 이미지를 분류하는 것으로 나타났다.



〔그림 2〕 파일 섹션단위 시각화 기법을 적용한 PE 파일 시각화 과정

V. 결 론

현재 CNN이 많은 관심을 받고 있고, 정보보안 분야에서도 이를 적용한 다양한 연구 주제들이 등장하고 있다. 각 분야에서 사용되는 데이터의 형태가 다르기 때문에 CNN을 사용하기 위해 각 분야의 데이터 형식에 맞는 시각화 기법이 적용되어야 최상의 결과를 얻을 수 있다. 본 논문에서는 바이너리 파일 시각화 기반 소프트웨어 보안약점 발견을 위해 파일 섹션단위 시각화 기법을 제안하고 CNN의 학습 및 평가로써 정확도를 검증하였다. 그 결과, 97.05%의 정확도를 보이며 기초연구의 Line 시각화 기법보다 2% 낮은 정확도가 나타났다. 파일 섹션단위 시각화 기법은 이전 연구인 라인단위 시각화 기법보다 이미지 상에서 파일의 구조를 인간의 눈으로 구분하기 용이하다는 장점이 있지만, CNN이 이미지에서 소프트웨어 보안약점에 대한 정보를 학습 및 평가하는 성능은 라인단위 시각화 기법보다 떨어진다는 단점이 있다. 차후, CNN을 활용한 소프트웨어 보안약점 탐지의 정확도 향상을 위해 CNN이 바이너리 파일을 시각화한 이미지를 분석하기에 용이하도록 바이너리 파일을 CNN과 친숙한 형태로 시각화하는 인코딩하는 기법을 제안하는 연구를 진행할 계획이다. 더 나아가 시각화 대상을 바이너리 파일에서 메모리 정보, 프로세스 정보 등으로 확대하여 시스템의 보안을 위협하는 요소들에 대한 탐지에 CNN을 활용할 수 있도록 연구를 진행할 예정이다.

참 고 문 헌

〔1〕 석선화, and 김호원. "Convolutional Neural Network 기반의 악성코드 이미지화를 통한 패밀리 분류." 정보보호학회논문지 26.1 197-208, 2016

〔2〕 Aldo Cortesi. "binvis.io"

〔3〕 K-H. Park, S. Choi, C. Kim, and Ki-Woong Park. "Usability of Software Weakness Discovery based on the Binary File Visualization." The 3rd International Conference on Next Generation Computing (ICON) 2017b, Dec. 21 - 24. 2017