|  |
| --- |
| **Open Source Project** |

조선대학교 IT 융합대학 컴퓨터공학과

3학년 20124855 박사홍

3학년 20124826 최용선

3학년 20134844 박효빈

Open Source Software

강문수 교수님

목차

오픈소스 소프트웨어 선택 및 개요

소개

설치방법

기여 방법

핵심 개념

추후 추가 함.

1. **오픈소스 소프트웨어 선택 및 개요**

* **angr가 무엇이며, 어떻게 사용하는가?**

angr는 Mayhem, KLEE 등 Dynamic symbolic execution와 Static analyses를 수행할 수 있는 Multi-architecture binary 분석 툴입니다.

바이너리 분석이 복잡하기 때문에 angr도 복잡하게 만들어졌지만

문서를 통해서 쉽게 사용할 수 있도록 했습니다.

바이너리를 프로그래밍적으로 분석하기 위해서 몇 가지 문제를 해결해야 합니다.

- 분석 프로그램에 바이너리를 로드 하기.

- 바이너리를 중간 표현(Intermediate Representation (IR))로 변환하기.

- 실제 분석 수행

- 종속성 분석, 프로그램 분할과 같은 부분 또는 전체 프로그램 정적 분석.

- Overflow가 일어날 수 있을 때까지 실행할 수 있는 것처럼 프로그램의 상태공간 분석.

- 위 두 예시의 결합. (Overflow를 찾을 때까지 프로그램 실행)

angr는 이러한 문제를 해결하기 위한 요소가 있으며, 이 문서는 어떻게 작동하는지 사용자가 원하는 목표를 이룰 수 있도록 설명합니다.

### **인용**

angr는 학업에 사용하는 경우 논문을 인용해 주세요.

@article{shoshitaishvili2016state,

title={SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis},

author={Shoshitaishvili, Yan and Wang, Ruoyu and Salls, Christopher and Stephens, Nick and Polino, Mario and Dutcher, Audrey and Grosen, John and Feng, Siji and Hauser, Christophe and Kruegel, Christopher and Vigna, Giovanni},

booktitle={IEEE Symposium on Security and Privacy},

year={2016}

}

@article{stephens2016driller,

title={Driller: Augmenting Fuzzing Through Selective Symbolic Execution},

author={Stephens, Nick and Grosen, John and Salls, Christopher and Dutcher, Audrey and Wang, Ruoyu and Corbetta, Jacopo and Shoshitaishvili, Yan and Kruegel, Christopher and Vigna, Giovanni},

booktitle={NDSS},

year={2016}

}

@article{shoshitaishvili2015firmalice,

title={Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware},

author={Shoshitaishvili, Yan and Wang, Ruoyu and Hauser, Christophe and Kruegel, Christopher and Vigna, Giovanni},

booktitle={NDSS},

year={2015}

}

1. **소개**

## angr 설치하기

angr는 Python libary로 사용하려면 Python 환경에서 설치해야 합니다. Python2를 기반으로 만들어졌으며 Python3는 추후 지원됩니다.

angr를 사용하고 실행하려면 [Python 가상환경](https://virtualenvwrapper.readthedocs.org/en/latest/)을 사용하는 것을 추천합니다.

angr에 의존하는 z3, pyvex 는 원시코드를 요구합니다. 하지만 libz3나 libVEX가 이미 설치된 경우 덮어쓰지 않습니다.

### 종속성

Python 모듈을 사용하기 위해서는 pip나 setup.py 스크립트를 사용합니다. Python 라이브러리인 cffi를 설치해야 합니다.

우분투에서 sudo apt-get install python-dev libffi-dev build-essential virtualenvwrapper 명령어를 통해 설치합니다. angr-management를 사용하려면 sudo apt-get install libqt4-dev graphviz-dev 를 설치해야 합니다.

### 대부분의 운영체제(\*nix 시스템)

angr는 python package index에 게시되어 있기 때문에 일반적으로 mkvirtualenv angr && pip install angr 명령을 통해 설치할 수 있습니다.

Fish(shell) 사용자는 [virtualfish](https://github.com/adambrenecki/virtualfish) 또는 [virtualenv](https://pypi.python.org/pypi/virtualenv) 패키지를 사용할 수 있습니다. vf new angr && vf activate angr && pip install angr

### Mac OS X

pip install angr 명령으로 설치할 수 있지만 몇가지 주의사항이 있습니다.

만약 Clang 으로 설치가 되지 않는다면 GCC를 이용해야 합니다.

brew install gcc

env CC=/usr/local/bin/gcc-6 pip install angr

angr를 설치한 뒤에 몇가지 공유 라이브러리 경로를 수정해야 합니다.

BASEDIR=/usr/local/lib/python2.7/site-packages

# If you don't know where your site-packages folder is, use this to find them:

python2 -c "import site; print(site.getsitepackages())"

install\_name\_tool -change libunicorn.1.dylib "$BASEDIR"/unicorn/lib/libunicorn.dylib "$BASEDIR"/angr/lib/angr\_native.dylib

install\_name\_tool -change libpyvex.dylib "$BASEDIR"/pyvex/lib/libpyvex.dylib "$BASEDIR"/angr/lib/angr\_native.dylib

### Windows

angr는 Windows에서 pip를 이용해 설치할 수 있습니다. (Visutal studio 빌드 툴을 이용해서)

Windows에서 Capstone을 설치하기 어렵습니다.

requirements.txt 파일 안에서 capstone을 지우는 것이 좋습니다.

### 개발자를 위한 설치

angr 개발자를 위해서 repo와 스크립트를 만들었습니다.

아래 명령을 통해서 쉽게 설치할 수 있습니다.

git clone git@github.com:angr/angr-dev.git

cd angr-dev

mkvirtualen angr

/setup.sh

### Docker 설치

편의성을 위해서 docker 이미지를 제공합니다.

# install docker

curl -sSL https://get.docker.com/ | sudo sh

# pull the docker image

sudo docker pull angr/angr

# run it

sudo docker run -it angr/angr

### angr container 수정

apt를 통해서 추가적인 패키지를 설치해야 하는 경우 권한 상승이 필요합니다. 아래 명령어를 통해서 권한을 설정해야 합니다.

# assuming the docker container is running

# with the name "angr" and the instance is

# running in the background.

docker exec -ti -u root angr bash

### **문제 해결**

#### libgomp.so.1: version GOMP\_4.0 not found, or other z3 issues

angr-only-z3-custom 과 미리 설치된 버전 간 호환되지 않은 문제 입니다. z3의 재컴파일이 필요합니다. pip install -I --no-use-wheel z3-solver

#### capstone 때문에 angr를 import 할 수 없는 경우

종종 capstone 때문에 angr가 제대로 설치되지 않은 경우가 있습니다. capstone을 재빌드해야 합니다. pip install -I --pre --no-use-wheel capstone

만약 해결되지 않는다면 몇가지 버그 때문일 수 있습니다. virtualenv/virtualenvwrapper 환경에서 pip를 이용한 capstone\_3.0.4 설치에서 버그가 있습니다.

가상 환경에서 /home/<username>/.virtualenvs/<virtualenv>/lib/python2.7/site-packages/capstone/\*.py(c) capstone python을 설치하면,

capstone라이브러리는 /home/<username>/.virtualenvs/<virtualenv>/lib/python2.7/site-packages/home/<username>/.virtualenvs/<virtualenv>/lib/python2.7/site-packages/capstone/libcapstone.so에서 찾을 수 있습니다.

native 환경에서 /usr/local/lib/python2.7/dist-packages/capstone/\*.py(c) capstone python을 설치하면, capstone 라이브러리는 /usr/local/lib/python2.7/dist-packages/usr/lib/python2.7/dist-packages/capstone/libcapstone.so에서 찾을 수 있습니다.

libcapstone.so파일을 파이썬 파일과 같은 디렉토리로 이동하면 문제가 해결됩니다.

#### No such file or directory: 'pyvex\_c'

Ubuntu 12.04를 사용하고 있다면 업데이트를 하는 것이 좋습니다. pip install -U pip를 업그레이드 해서 해결할 수 있습니다.

#### AttributeError: 'FFI' object has no attribute 'unpack'

오래된 cffi 버전의 모듈을 사용하고 있을 수 있습니다. angr는 최소 1.7 이상의 cffi가 필요합니다. pip install --upgrade cffi 명령을 실행해보고 문제가 계속 발생한다면 cffi가 설치되어있는지 확인해보세요.

pypy와 같은 인터프리터를 사용한다면 cffi가 오래된 버전일 수 있습니다. 최신 버전의 pypy를 설치하세요.

### **지원**

angr를 사용하는데 도움을 받으려면 아래를 참고해 주세요.

* Mail: [angr@lists.cs.ucsb.edu](mailto:angr@lists.cs.ucsb.edu)
* Slack channel: [angr.slack.com](https://angr.slack.com/)
* IRC channel: #angr on [freenode](https://freenode.net/)

1. **핵심 개념**