Term Project

2019 정보보호

1. 대상 프로그램

- **binutils-2.28 프로젝트의 objdump**

binutils 는 GNU 에서 제공하는 바이너리를 처리하는 유틸리티를 제공하는 오픈소스 프로젝트이다. objdump 는 다양한 실행 파일에 대한 정보를 보여주는 유틸리티이다. (리눅스: ELF 파일, 윈도우 PE 파일)

- binutils 다운로드: http://ftp.gnu.org/gnu/binutils/binutils-2.28.tar.gz

- binutils 빌드 (ASAN 사용):

```
$ export AFL_USE_ASAN=1

$ CC=afl-gcc CXX=afl-g++ ./configure --prefix=/home/seclab/practice/
term/binutils-asan/ --disable-shared --disable-gdb --disable-gprof --disable-gold --
disable-gas

$ make && make install
```

- Fuzzing:

```
$ python fuzzer.py ./objdump "-x @@" ./seed/ ./output/
```

2. 보고서 작성

1) 시드 파일 수집 및 생성
   - 퍼징에 사용할 1 개 이상의 시드 파일을 수집하거나 생성하는 방법 작성

2) 변이 전략 수행
   - AFL 을 참고하여 bit flipping, byte flipping, arithmetic inc/dec, interesting value (0, 0xffffffff, 0x7fffffff), block insertion, block deletion 등의 다양한 변이 전략 구현
   - 구현한 변이 전략에 대한 설명 및 퍼징 수행 결과 작성
   - *퍼징은 5 시간 이상 수행함

3) 크래시 중복 제거
   - ASAN 메시지를 활용한 크래시 중복 제거 방법 및 결과 작성

4) 코드 커버리지 측정
   - 퍼징 결과 생성된 입력 파일들을 사용하여 대상 프로그램의 코드 커버리지 측정

5) AFL 과의 비교 수행
   - 구현한 fuzzer 와 AFL 을 사용하여 같은 시간동안 fuzzing 을 수행한 뒤, 각 fuzzer 에 대한 4)의 코드 커버리지 결과 비교

6) 최신버전 대상 새로운 버그 제보
   - binutils 2.32 버전을 대상으로 퍼징 수행 및 새로운 버그 제보
   - https://sourceware.org/bugzilla/

3. 제출

- 6 월 21 일 23:59 까지 yscec 에 제출
- 보고서, 소스코드, 퍼징 결과 디렉터리