
Fuzz Testing을 통한 위성 SW 분석

종합설계1 Week3

202002473 김승혁

201902733 이정윤

202002699 조민기



오픈소스 위성 소프트웨어 분석

Fuzzer 선정 및 비교

연구 환경 구축

연구 방식 정의



오픈소스 위성 소프트웨어 분석

- NASA cFS
- NASA fprime
- ESA NanoSat MO



nasa/cFS

The Core Flight System (cFS)



39

Contributors

49

Used by

181

Discussions

890

Stars

246

Forks



nasa/fprime-gds

F´ Python Ground Data System (GDS).



34

Contributors

56

Used by

22

Stars

42

Forks



esa/nanosat-mo-framework



A software framework for small satellites based on CCSDS MO services

18

Contributors

10

Used by

102

Stars

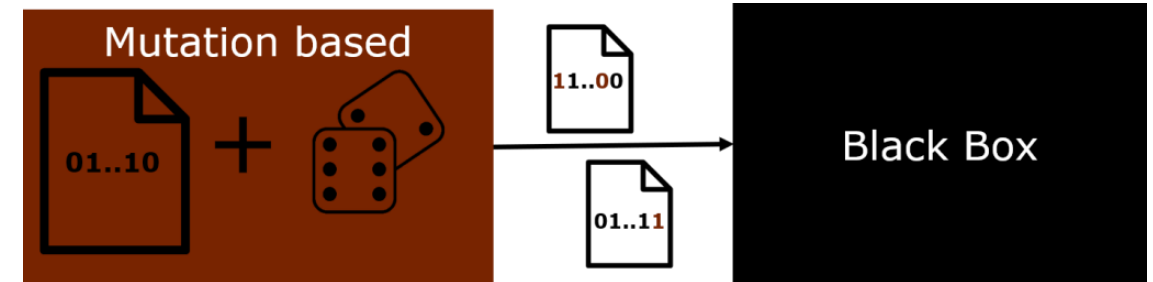
32

Forks

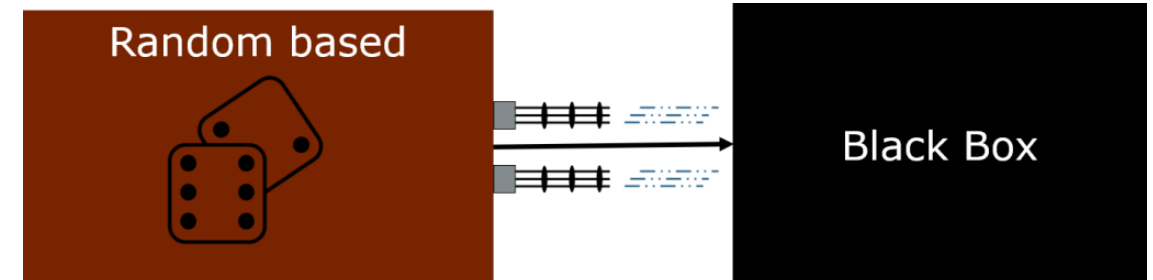


Fuzzer 선정 및 비교

- Mutation or Generation ?
- Mutation: AFL, Honggfuzz, libFuzzer ...
- Generation: Sulley, Peach ...



Mutation



Generation

연구 환경 구축

- 프로그래밍 언어

: C, C++, Python, Java

- OS

: Ubuntu, Arch Linux

- 웹 서버

: AWS, GCP, Naver Cloud

연구 방식 정의

1. 위성 SW 결함 탐지
2. Fuzzer의 실행 접근성과 속도 분석
3. Mutation 방식과 Generation 방식 비교

Thank You