OSS Fuzz: 구글의 지구방위 프로젝트

Tae Eun Kim

2022.04.22

Abstract

소프트웨어의 결함은 현실의 큰 문제에까지 영향을 미친다. 소프트웨어의 오류가 재산 피해, 인명 피해와 직결 될 수 있기 때문이다. 따라서 구글은 이러한 프로그램 결함들을 잡아내기 위한 OSS Fuzz 프로젝트를 운영중에 있다. OSS Fuzz의 운영은 성공적이었으며 많은 연구의 귀중한 밑거름이 되었다. 이 때, 프로그램 분석 도구까지 OSS Fuzz에 통합한다면 더 효과적으로 결함을 찾아낼 수 있을 것이다.

우리는 소프트웨어 결함이 큰 위협이 되는 세상에 살고 있다. 소프트웨어에 문제가 생긴다면 하늘의 새는 아니더라도 하늘의 로켓이 떨어지고, 자동차가 급가속하며, 데이터화된 우리의 재산이 증발할 수도 있다. 오픈소스로 관리되는 프로젝트들은 이러한 결함의 위협으로부터 특히 더 위험할 수 있다. 왜냐하면 각 개발자들의 전체 코드에 대한 이해가 떨어지기 쉽기 때문이다. 또한 오픈소스는 그 특성상 수정과 배포가 빈번하게 일어난다. 따라서 한번 결함이 유입되면 그 파급력이 더욱 크다.

이러한 상황에 구글이 발벗고 나섰다. 때는 바야흐로 2016년, OSS Fuzz 프로젝트를 발표한 것이다. 제안은 간단했다. 구글이 막대한 서버 인프라로 컴퓨팅 파워를 지원할테니, 오픈소스 프로젝트는 검사를 위해, 퍼징 도구들은 성능 평가를 위해 등록하라는 것이었다. 그 이후로 6년이 지난 현재, OSS Fuzz 프로젝트에는 500여개의 오픈소스 프로젝트가 등록되어있고, 다양한 퍼저들을 통해 35000여건의 결함을 발견할 수 있었다. 구글이 우리 세상의 안전을 지키고 있는 것이다.

OSS Fuzz의 가장 큰 기여는 퍼징 대상과 퍼징 도구를 한데 모으는 플랫폼을 제공했다는 것에 있다. 오픈 소스 프로젝트 관리자들과 퍼징 도구 개발자들의 필요가 만나는 지점이 형성된 것이다. 또한 OSS Fuzz를 통해 계속해서 발견되는 결함은 벤치마크화 되어 이후 연구들의 초석이 되고 있다.

만약 OSS FUZZ에 정적 분석 도구들도 가세한다면 더 효율적으로 소프트웨어 안전을 도모할 수 있을 것이다. 막대한 컴퓨팅 파워는 공짜로 주어지지 않는다. 많은 전기가 소모되며, 많은 열이 발생한다. 따라서 이러한 자원을 전략적으로 사용할 필요가 있다. 이 때, 프로그램을 안전(Sound)하게 분석한 후,

결함이 발생할 것으로 예상되는 지점들에 집중한다면 결함을 놓치지 않는 동시에 더 효과적인 퍼징이 될 수 있을 것이다.