BEACON: 감탄고토 Fuzzing

Tae Eun Kim

2021.11.04

Abstract

지향성 퍼징은 대상 프로그램의 특정 위치에 도달하는 입력을 생성하는 것을 목적으로 한다. 기존의 지향성 퍼징 도구들은 어떻게 더 의미있는 입력을 생산할지에 관심을 가져왔다. BEACON[1]은 이와 달리 어떻게 목표 지점에 도달 할 수 없는 입력의 실행을 조기에 종료할 지에 관심을 가진다. 기존의 지향성 퍼징과 BEACON은 함께 사용될 시, 서로를 보완하며 더 뛰어난 성능을 보여줄 것으로 기대된다.

지향성 퍼징의 목적은 사용자가 원하는 지점까지 도달하는 입력을 빠르게 생성하는 것이다. 기존의 지향성 퍼징 도구들, 특히 Greybox 퍼징 도구들은 목표 지점과의 거리 등을 고려하여 점진적으로 목표 지점에 더 가까이 도달하는 입력을 만드려고 노력하였다. 따라서 퍼징 과정에서 목표 지점과 더 가까운 입력을 찾는다면 그 입력을 새로운 Seed로 삼는 접근을 취해왔다.

BEACON은 기존의 퍼징 도구들과는 조금 다른 방식으로 목표 지점에 도달하는 입력을 찾는다. BEACON은 직접적으로 목표 지점으로 향하는 입력을 찾기보다, 목표지점으로 향하지 않는 입력을 조기에 종료한다. 무의미한 실행을 조기에 종료함으로써, 주어진 시간안에 목표지점에 도달하는 입력을 찾을 가능성을 높이는 것이다.

구체적으로 BEACON은 두가지 기준을 가지고 입력의 목표지점 도달 가능성을 판단한다. 이 기준들은 입력이 지나는 프로그램의 각 위치에서 검사가 이루어진다. 첫번째 기준은 Control Flow Graph상에서 현재 지점과 목표지점 사이의 길이 존재하는 지의 여부이다. 두번째 기준은 현재 위치에서 가지고 있는 변수의 값들이, 목표지점에 도달하기 위한 조건을 만족하는지의 여부이다. BEACON은 이 두 기준을 각 프로그램 지점에 assert문의 형태로 삽입하여 특정 입력이 목표지점에 닿을 수 없는 것이 확인되면 해당 입력의 실행을 즉시 종료한다.

기존 지향성 퍼징이 목표지점에 더 가까이 도달할 입력을 "생성"하는 것에 더 관심을 두었다면, BEACON은 이미 생성된 입력이 목표지점에 도달하지 못할 경우, 조기에 "종료 "하는 것에 관심을 둔다. 따라서 두 접근은 서로 독립적인 접근이며 서로를 보완할 수 있을 것이다.

[1]Huang et al., BEACON : Directed Grey-Box Fuzzing with Provable Path Pruning