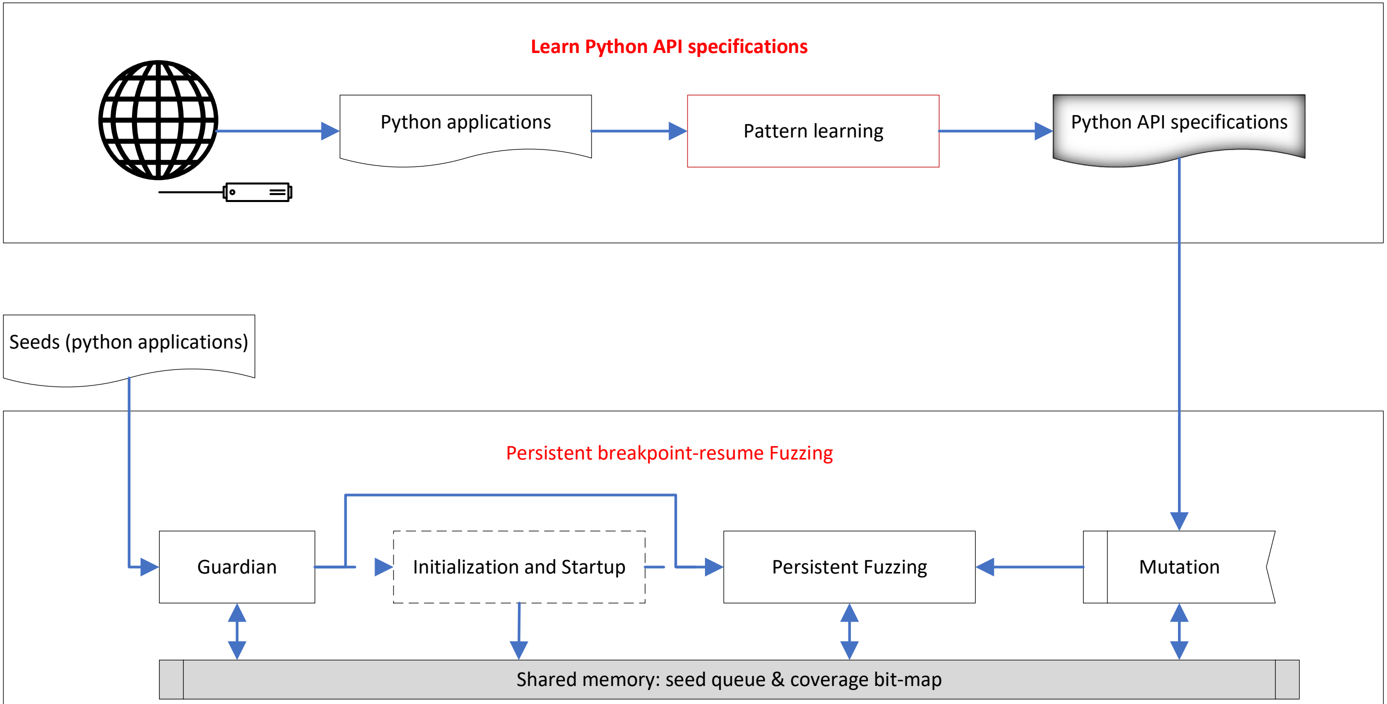

Learn Python API specifications

Python applications

Pattern learning

Python API specifications

Seeds (python applications)

Persistent breakpoint-resume Fuzzing

Guardian

Initialization and Startup

Persistent Fuzzing

Mutation

Shared memory: seed queue & coverage bit-map

Challenge 1: How to generate python applications with correct syntax and meaningful semantic?

-> pattern learning for python API specifications

Challenge 2: Efficiency

2.1 Why not AFL++

-> TOO low efficiency with large coverage bit-map (over 1500 K)

-> Only support non-persistent mode for Python, which means it will cost much time during startup phase (import libraries)

2.2 Why not Atheris

-> No global status for recovery after exiting triggered by error happens

-> Persistent mode for python applications, not support for python interpreter

-> Not support path coverage

-> Persistent fuzzing with breakpoint resume & path coverage & optimization of bit-map summary algorithm