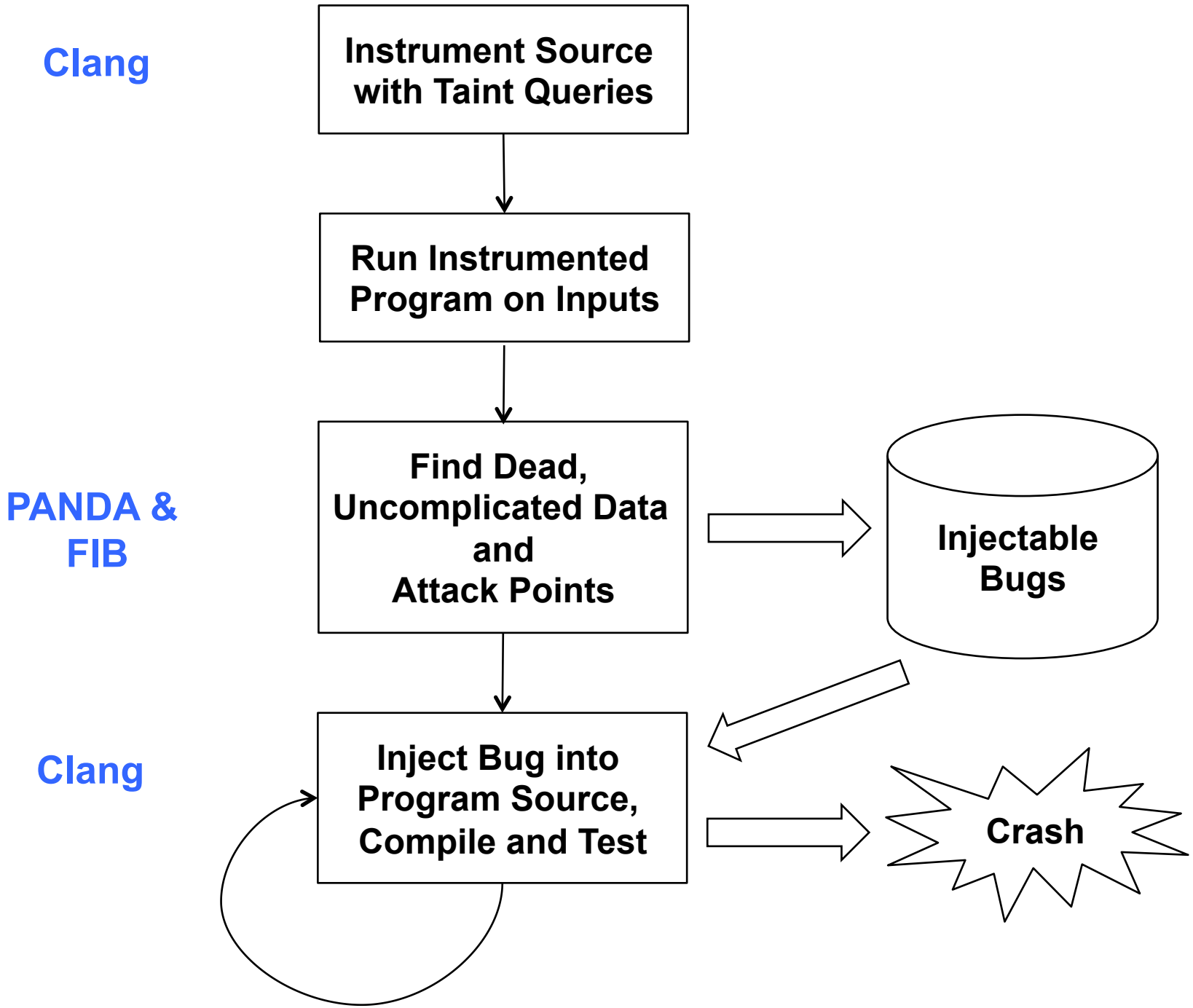
Clang
Instrument Source with Taint Queries
Run Instrumented Program on Inputs
PANDA & FIB
Find Dead, Uncomplicated Data and Attack Points
Injectable Bugs
Clang
Inject Bug into Program Source, Compile and Test
Crash