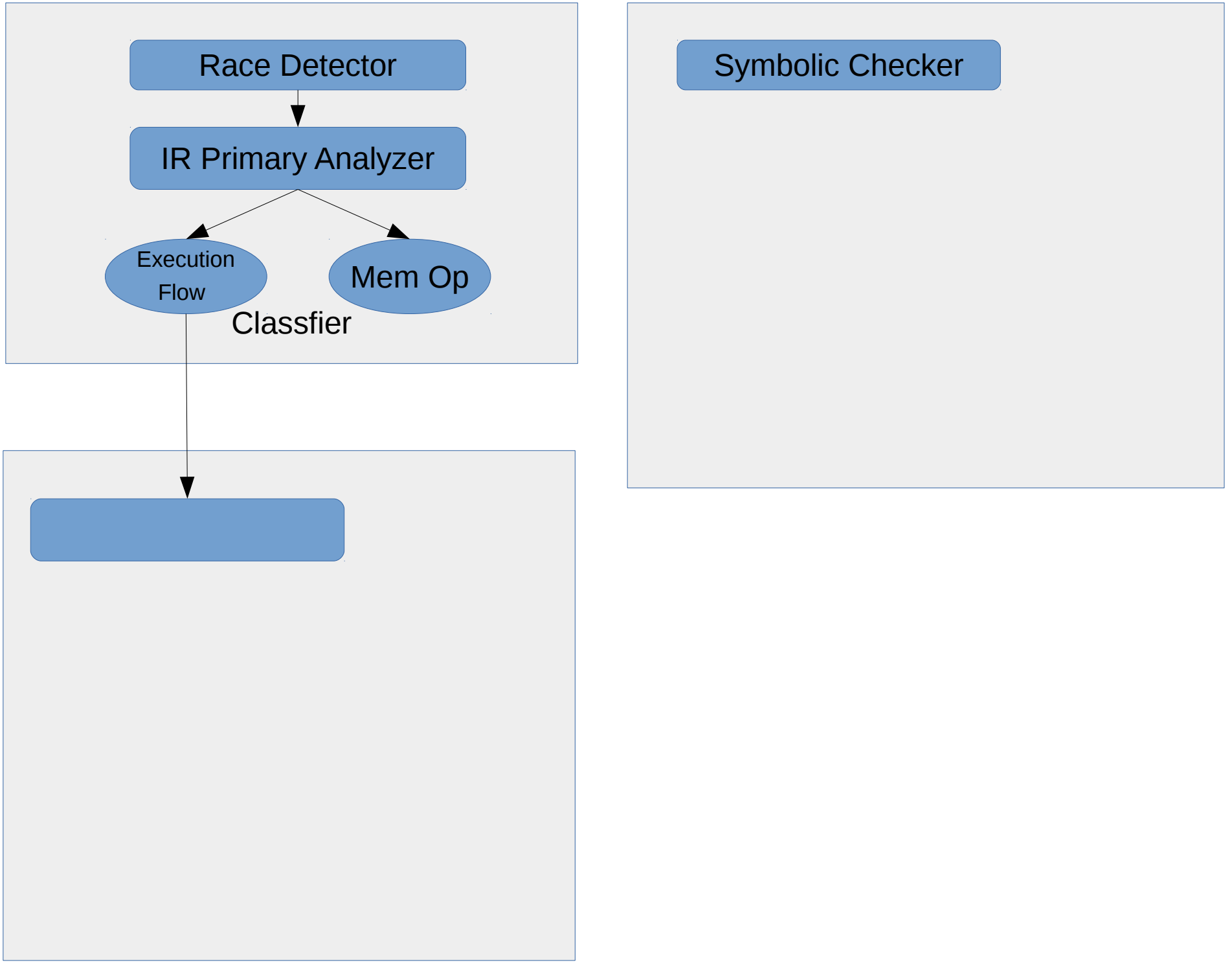
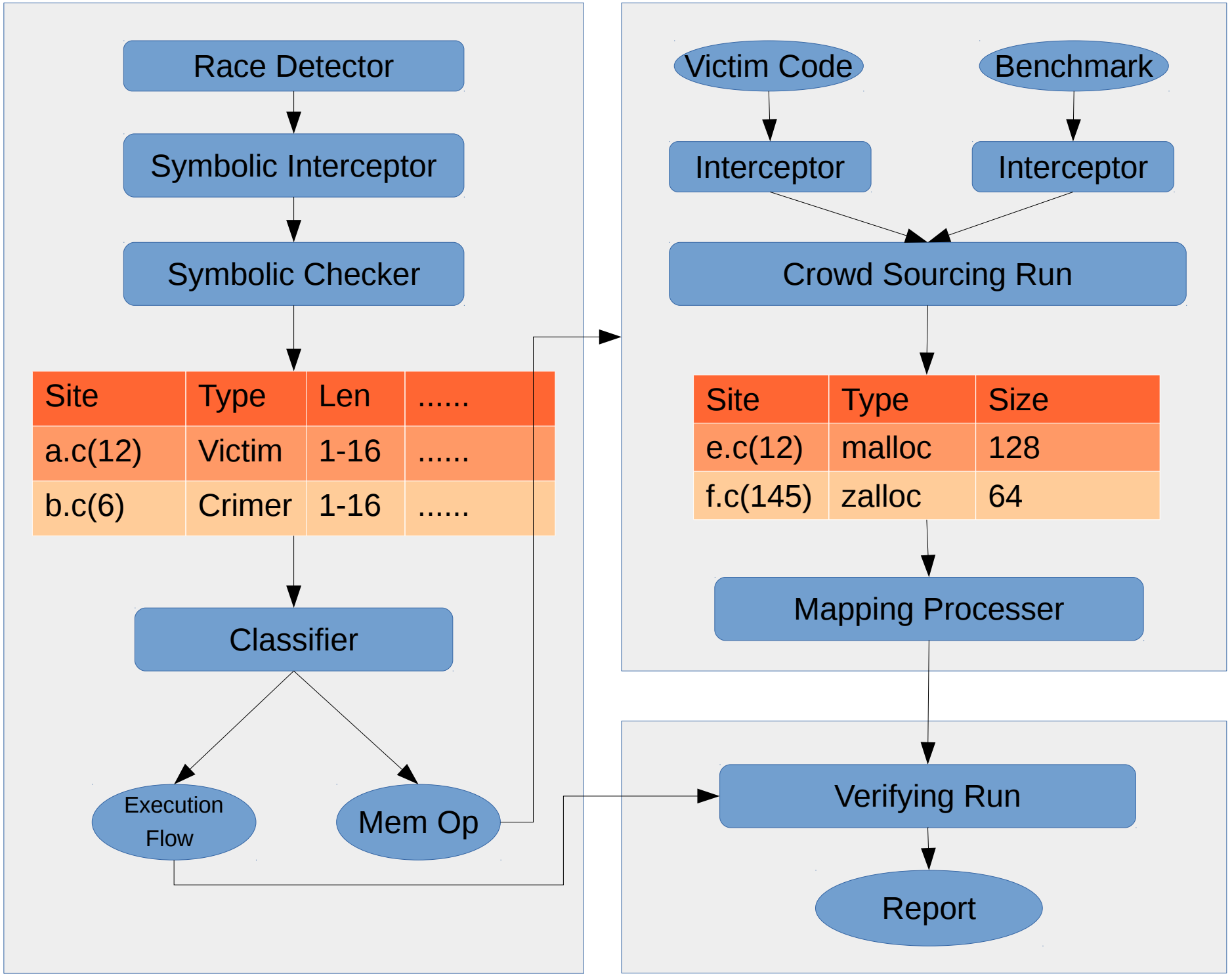
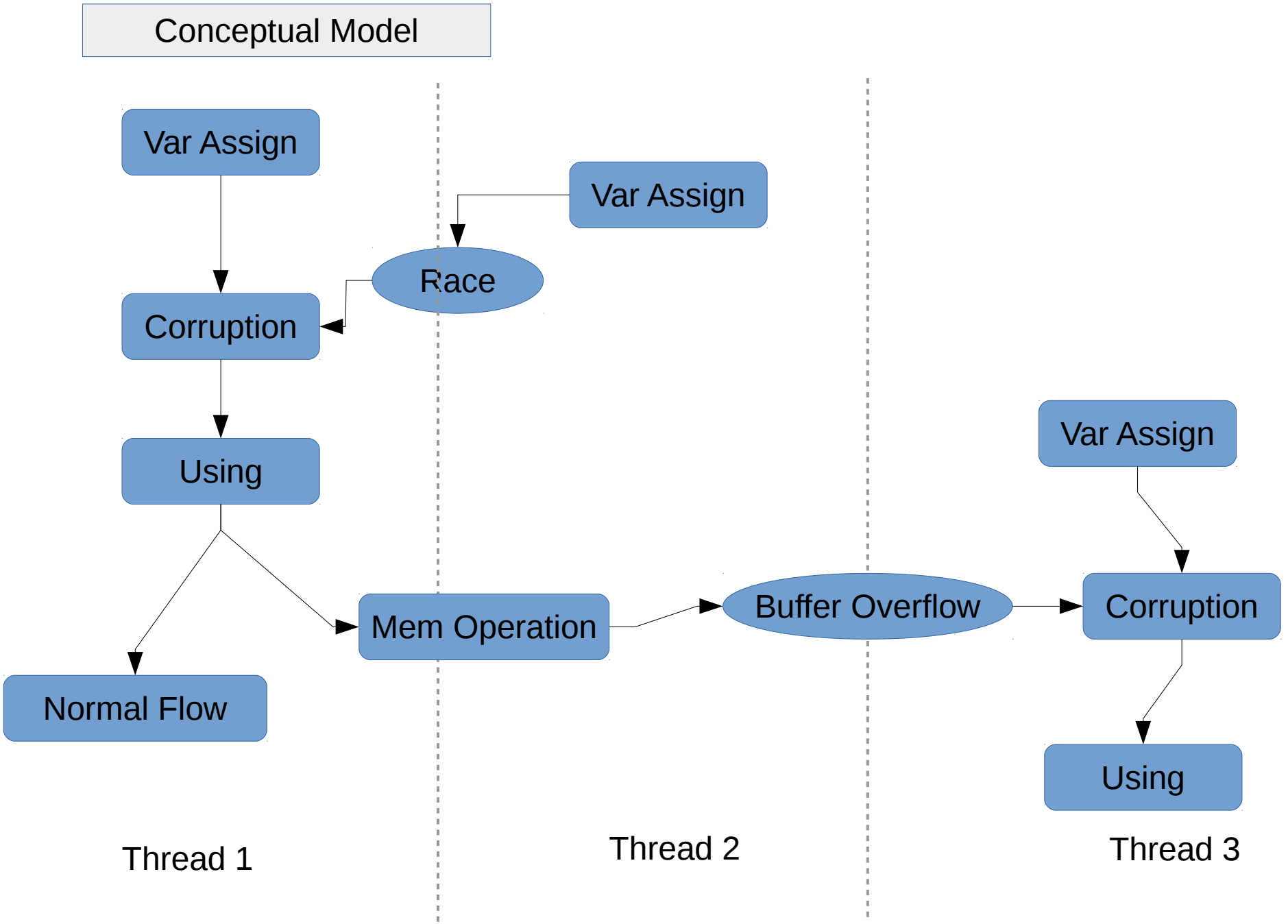
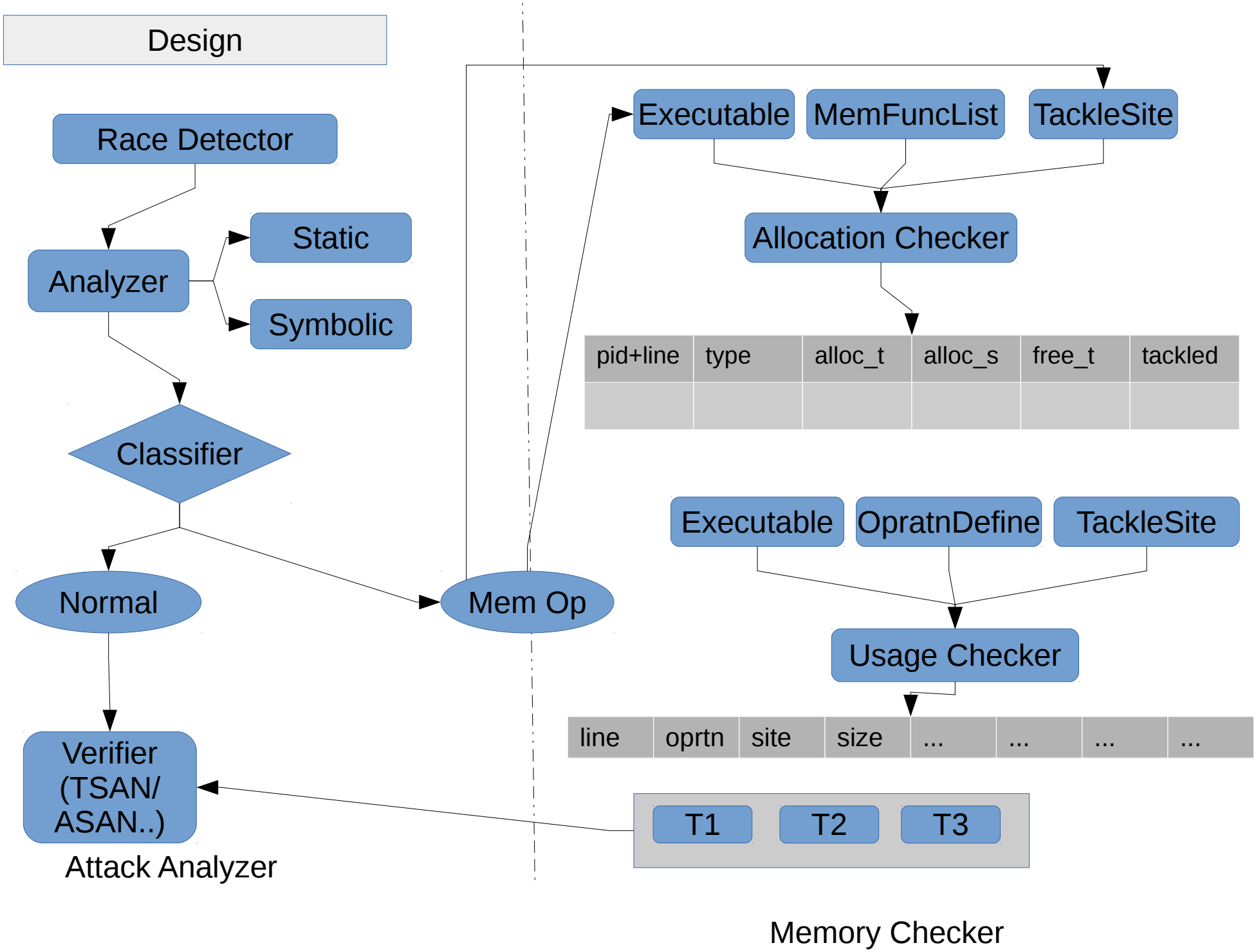
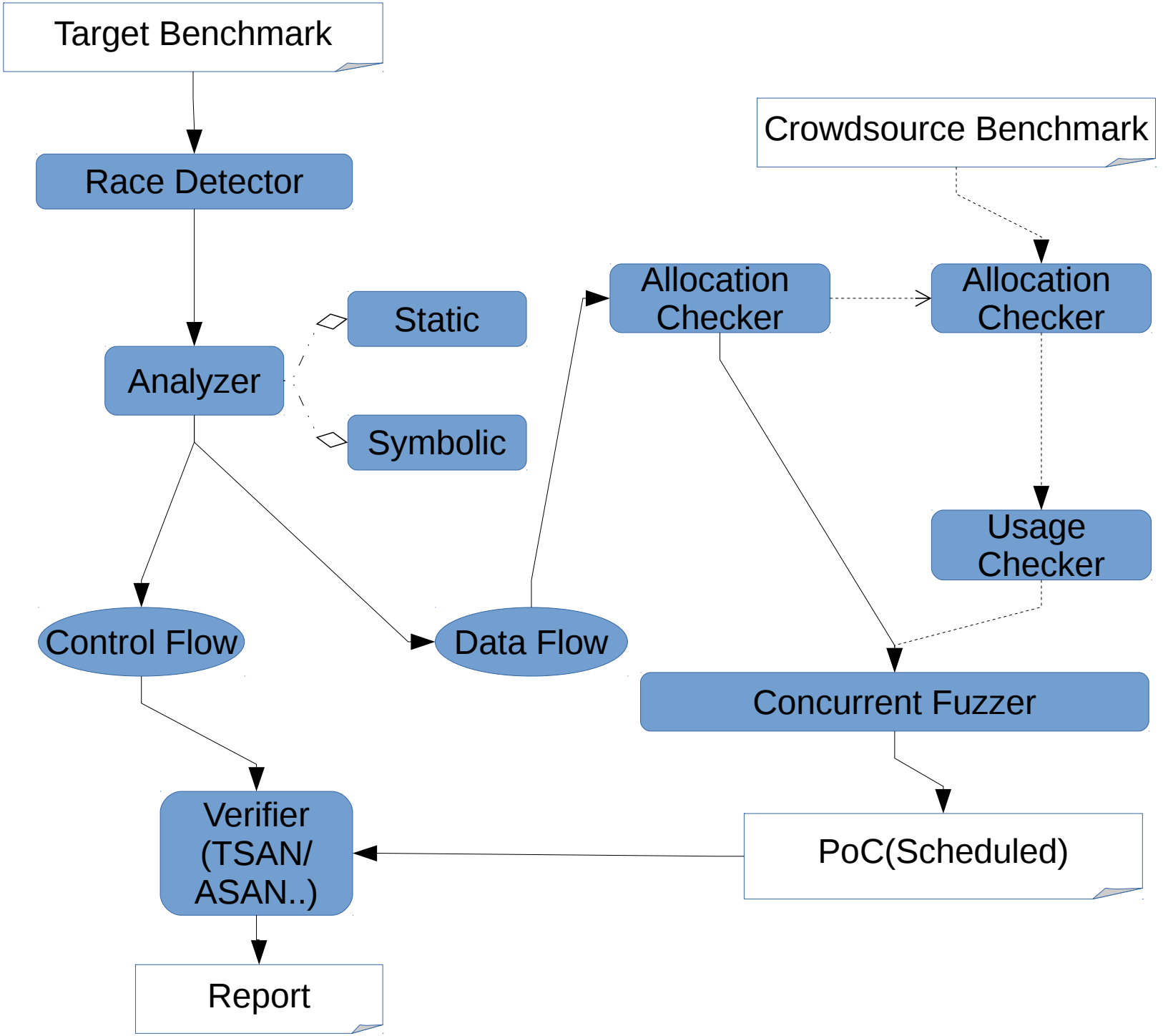

Race Detector
IR Primary Analyzer
Execution Flow
Mem Op
Classfier
Symbolic Checker


Race Detector
Symbolic Interceptor
Symbolic Checker
Site
Type
Len
.....
a.c(12)
Victim
1-16
.....
b.c(6)
Crimer
1-16
.....
Classifier
Execution Flow
Mem Op
Victim Code
Benchmark
Interceptor
Interceptor
Crowd Sourcing Run
Site
Type
Size
e.c(12)
malloc
128
f.c(145)
zalloc
64
Mapping Processer
Verifying Run
Report


Conceptual Model
Var Assign
Var Assign
Race
Corruption
Using
Var Assign
Mem Operation
Buffer Overflow
Corruption
Normal Flow
Using
Thread 1
Thread 2
Thread 3


Design
Race Detector
Analyzer
Static
Symbolic
Classifier
Normal
Verifier
(TSAN/
ASAN..)
Attack Analyzer
Mem Op
Executable
MemFuncList
TackleSite
Allocation Checker
pid+line
type
alloc_t
alloc_s
free_t
tackled
Executable
OpratnDefine
TackleSite
Usage Checker
line
oprtn
site
size
...
...
...
...
T1
T2
T3
Memory Checker


Target Benchmark
Race Detector
Analyzer
Static
Symbolic
Control Flow
Data Flow
Allocation Checker
Crowdsource Benchmark
Allocation Checker
Usage Checker
Concurrent Fuzzer
PoC(Scheduled)
Verifier (TSAN/ ASAN..)
Report