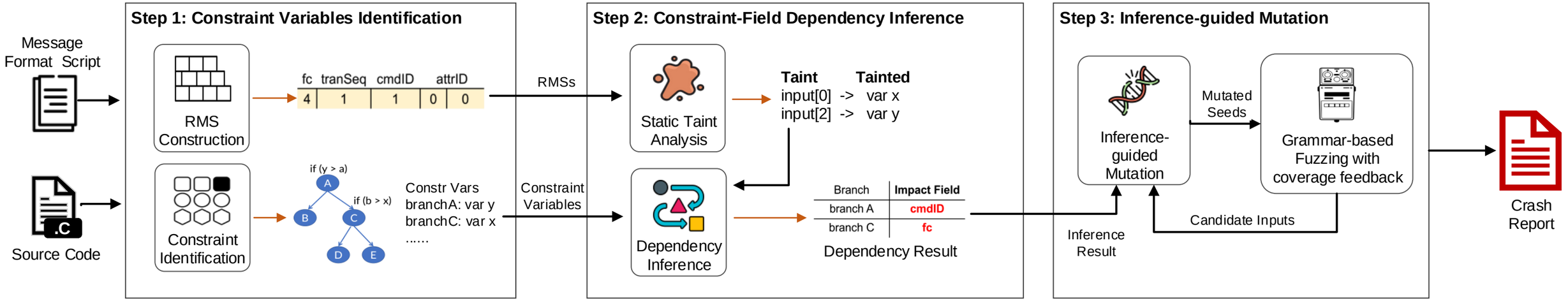
Message Format Script
Source Code
.C
Step 1: Constraint Variables Identification
RMS Construction
fc tranSeq cmdID attrID
4 1 1 0 0
Constraint Identification
if (y > a)
if (b > x)
A
B
C
D
E
Constr Vars
branchA: var y
branchC: var x
.....
RMSs
Constraint Variables
Step 2: Constraint-Field Dependency Inference
Static Taint Analysis
Taint Tainted
input[0] -> var x
input[2] -> var y
Dependency Inference
Branch Impact Field
branch A cmdID
branch C fc
Dependency Result
Step 3: Inference-guided Mutation
Inference-guided Mutation
Mutated Seeds
Grammar-based Fuzzing with coverage feedback
Inference Result
Candidate Inputs
Crash Report