An Illustration of AFL

M. Raveendra Kumar, TCS Research

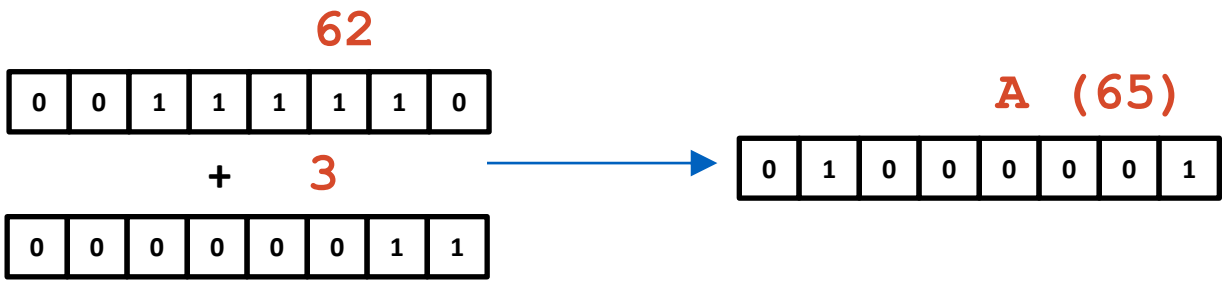
Mutation operations -- examples

Walking bit flip operations

Single bit

Two bits

Arithmetic



Deterministic: flip the bits in a fixed order starting from left most bit position.

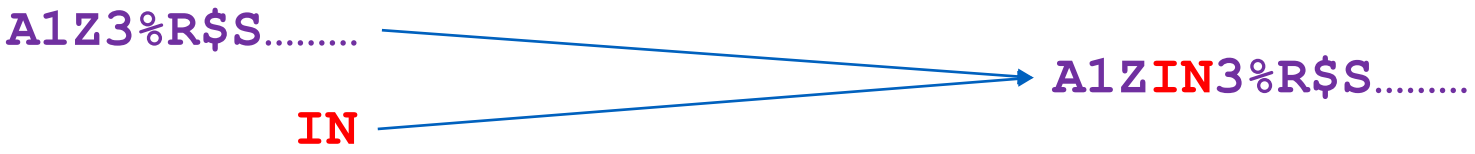
Non-deterministic: flip bits at a random location

Random Mutation operations

S.No	Class of mutation operation	Randomness
1	Walking bits	1. Selecting a byte, 2. Selecting a flip position
2	Setting interesting value	1. Selection of interesting value, 2. Selection location in the input.
3	Subtraction / addition of a value	1. Selection of value to subtract/add. 2. Selection of Location in the input
4	Adding/Deleting the content	1. Location to add/subtract 2. Length of data to add/subtract. 3. Value of byte to add
5	Clone bytes	1. From location 2. To location 3. Clone size
6	Set to random value	1. From location 2. To location 3. Size and Value
7	Override data	1. From location 2. To location 3. Size and value

Mutation operations Example

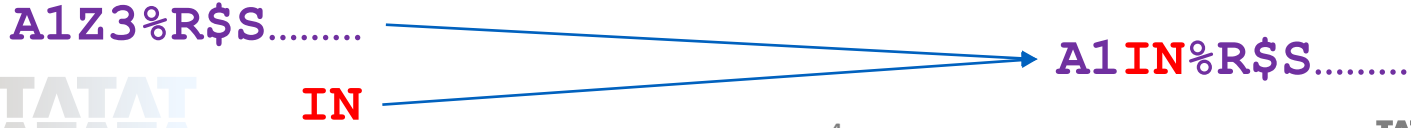
Adding and deleting the content



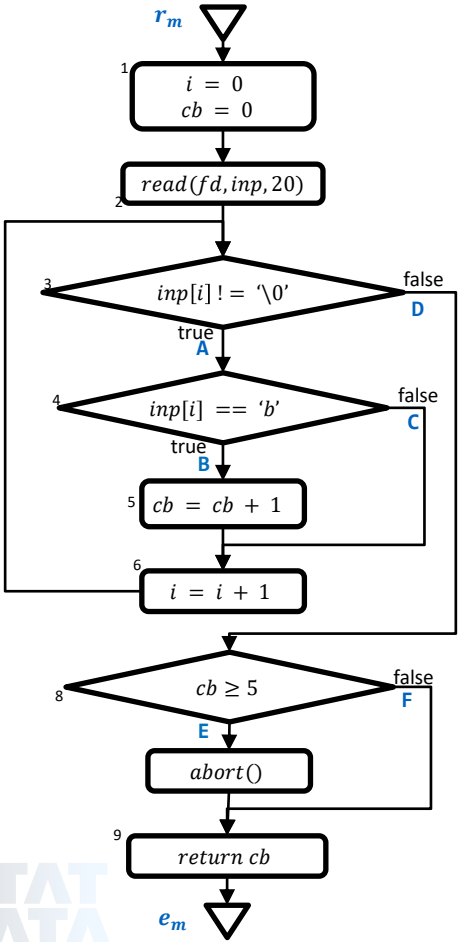
Clone the content

Set random value at a random location

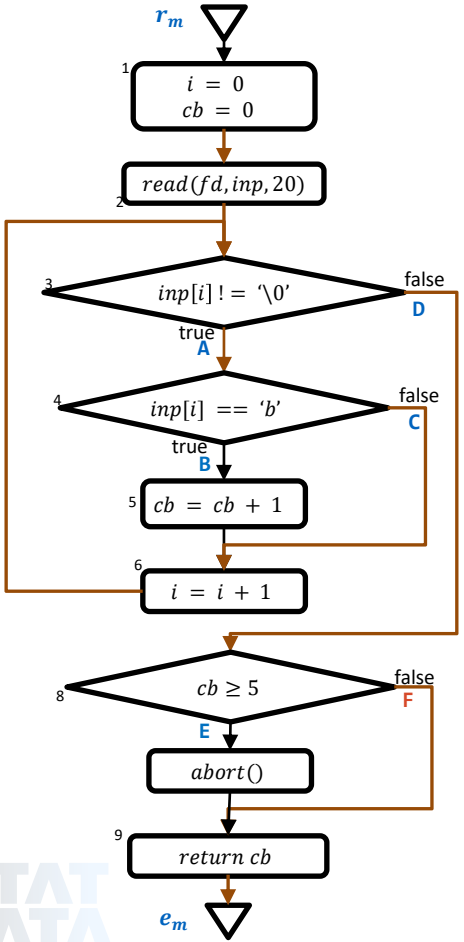
Override data a random location



Coverage Guided Fuzzing – Working example



Coverage Guided Fuzzing – Working example

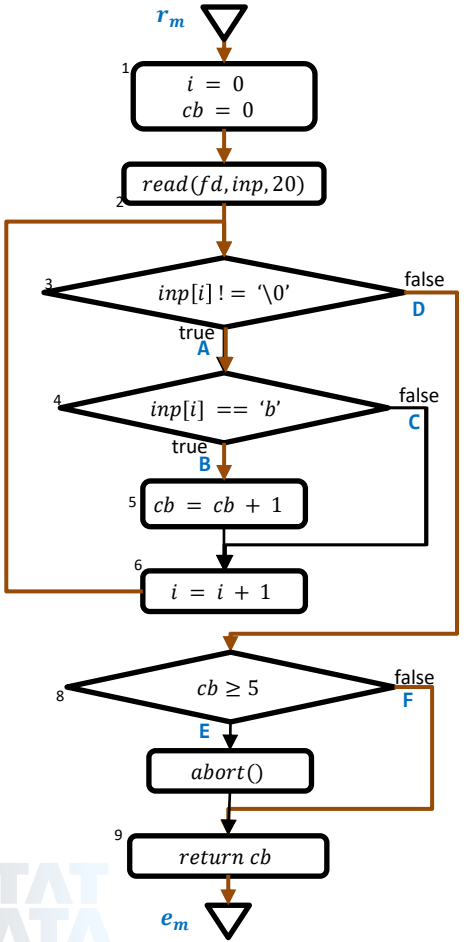


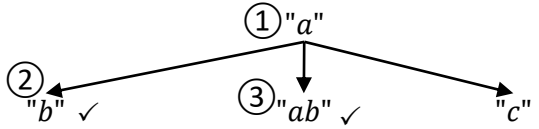
Initial input ①"a"

Evaluation

Id	input	AB	AC	BA	CA	BD	CD	DE	DF
1	"a"		1				1		1

Coverage Guided Fuzzing – Working example

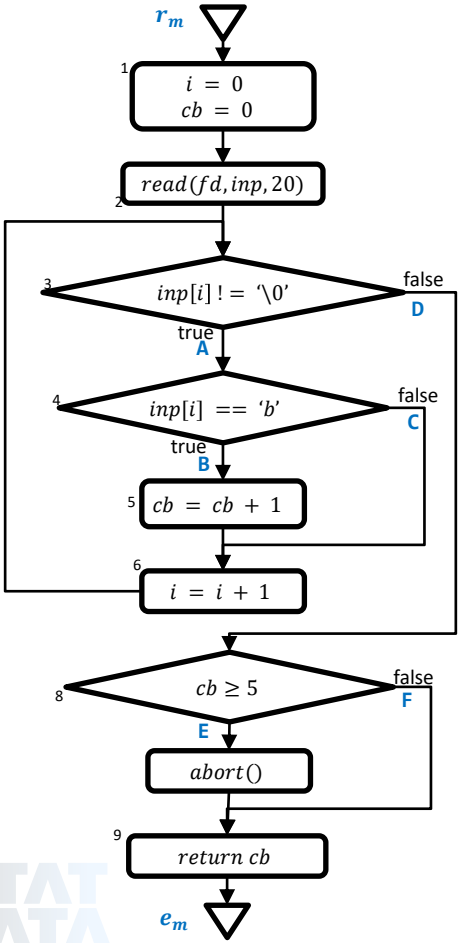


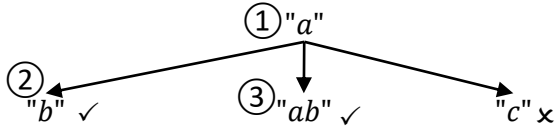


Fitness check

Id	input	AB	AC	BA	CA	BD	CD	DE	DF
1	"a"		1				1		1
2	"b"	1				1			1
3	"ab"	1	1		1	1			1
	"c"		1				1		1

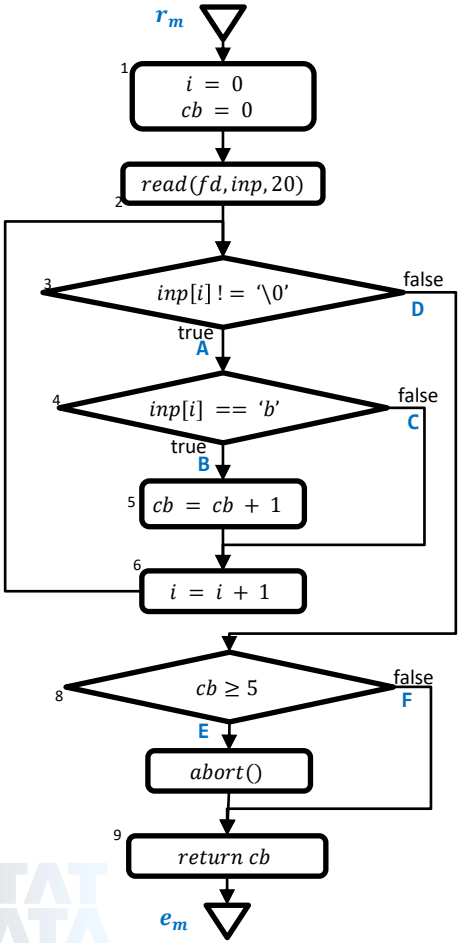
Coverage Guided Fuzzing – Working example

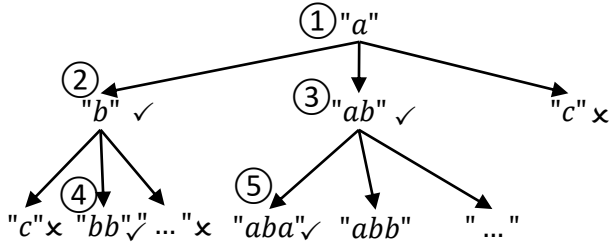




Id	input	AB	AC	BA	CA	BD	CD	DE	DF
1	"a"		1				1		1
2	"b"	1				1			1
3	"ab"	1	1		1	1			1
✗	"c"		1				1		1

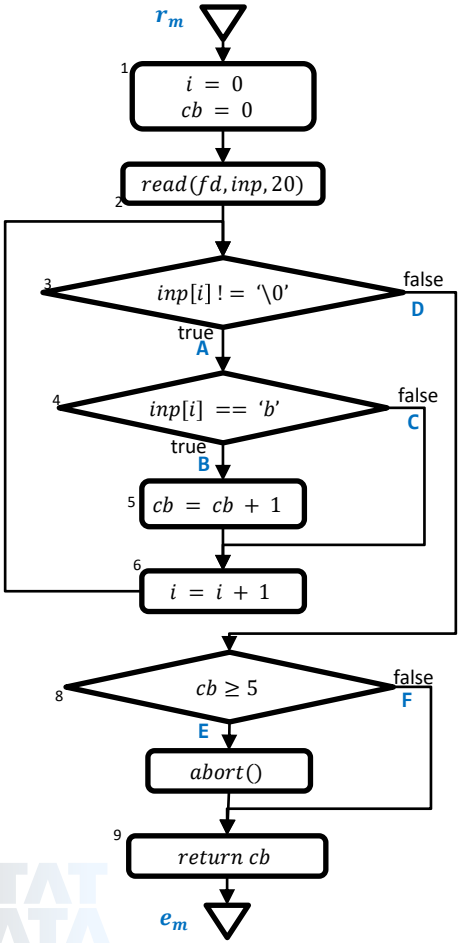
Coverage Guided Fuzzing – Working example

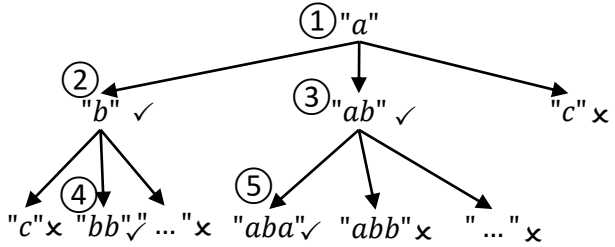




Id	input	AB	AC	BA	CA	BD	CD	DE	DF
1	"a"		1				1		1
2	"b"	1				1			1
3	"ab"	1	1		1	1			1
4	"bb"	2		1		1			1
5	"aba"	1	2	1	1		1		1
	"abb"	2	1	1	1	1			1

Coverage Guided Fuzzing – Working example





Id	input	AB	AC	BA	CA	BD	CD	DE	DF
1	"a"		1				1		1
2	"b"	1				1			1
3	"ab"	1	1		1	1			1
4	"bb"	2		1		1			1
5	"aba"	1	2	1	1		1		1
	"abb"	2	1	1	1	1			1