Mutation Testing of Memory-Related Operators

Jay Nanavati, **Fan Wu**, Mark Harman,
Yue Jia, Jens Krinke
UCL, UK

Motivation

Bug #68942 **Use after free**
Submitted: 2015-01-29 07:20 UTC
Reference: https://bugs.php.net/bug.php?id=68942

```
if (zend_hash_find(...) == SUCCESS) {
    if (zend_hash_find(...) == SUCCESS) {
        convert_to_long(*z_timezone_type);
        if (SUCCESS == timezone_initialize(...)) {
            return SUCCESS;
        }
```

Motivation

Bug #68942 **Use after free**
Submitted: 2015-01-29 07:20 UTC
Reference: https://bugs.php.net/bug.php?id=68942

```
if (zend_hash_find(...) == SUCCESS) {
    if (zend_hash_find(...) == SUCCESS) {
        convert_to_long(*z_timezone_type);
        if (SUCCESS == timezone_initialize(...)) {
            return SUCCESS;
        }
```

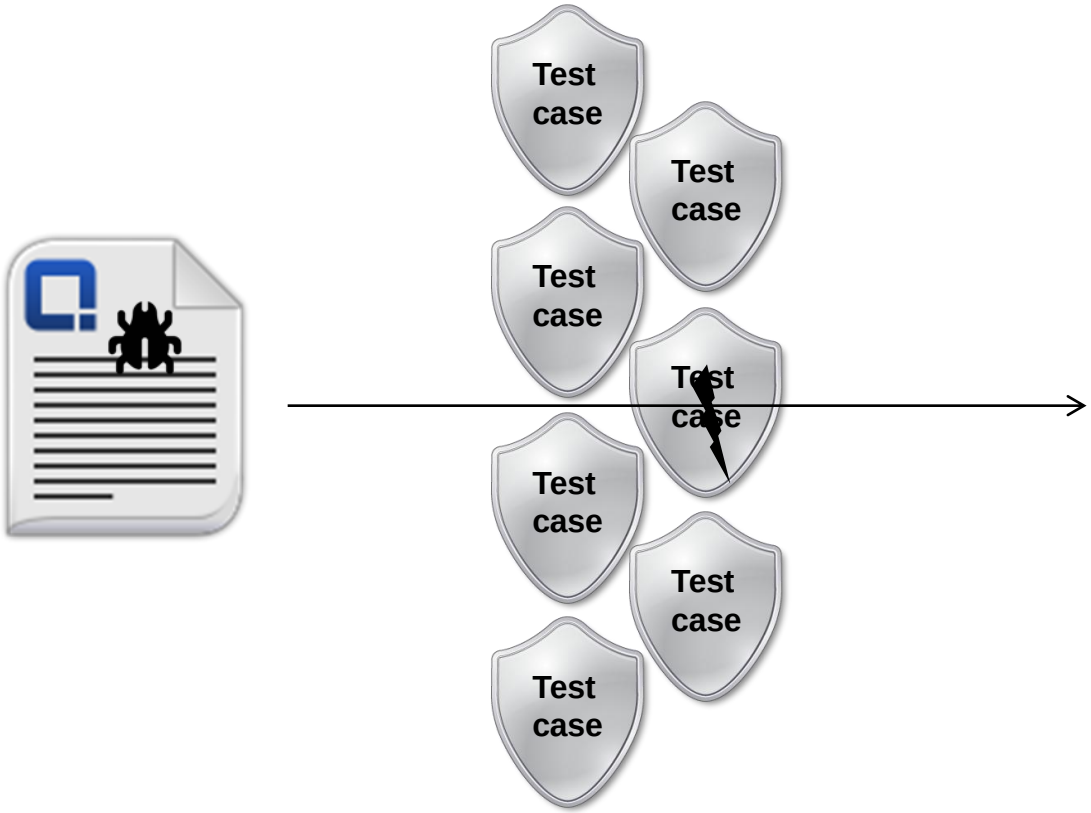
Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Motivation

```
-       if (zend_hash_find(...) == SUCCESS) {

+       if (zend_hash_find(...) == SUCCESS
            && Z_TYPE_PP(z_timezone_type) == IS_LONG) {

            if (zend_hash_find(...) == SUCCESS) {

-                   convert_to_long(*z_timezone_type);

                    if (SUCCESS == timezone_initialize(...)) {

                        return SUCCESS;

                    }
```

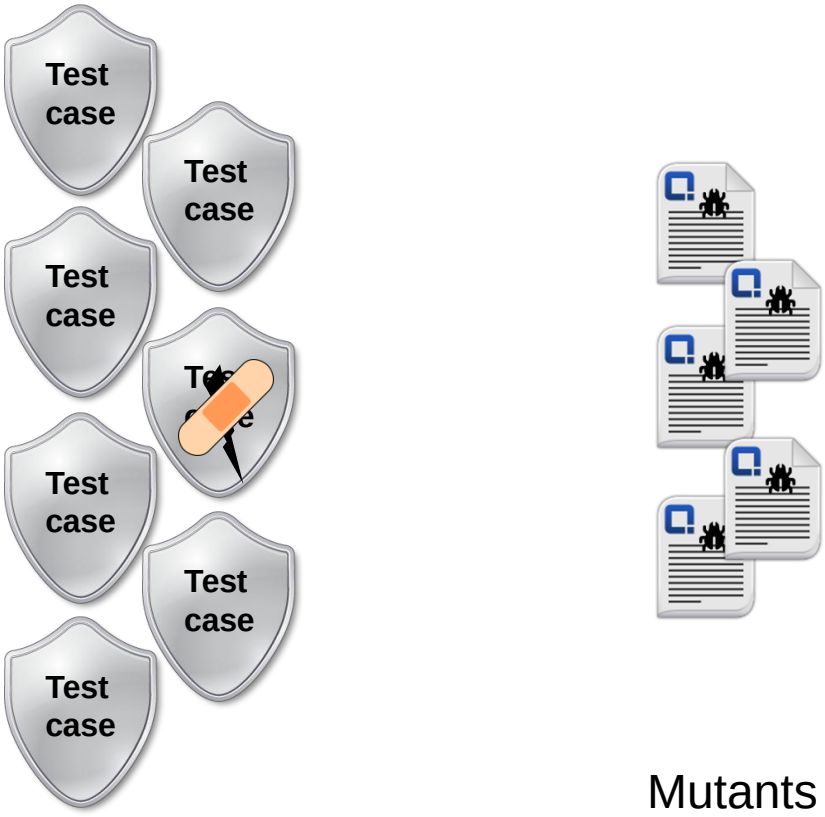
Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Motivation



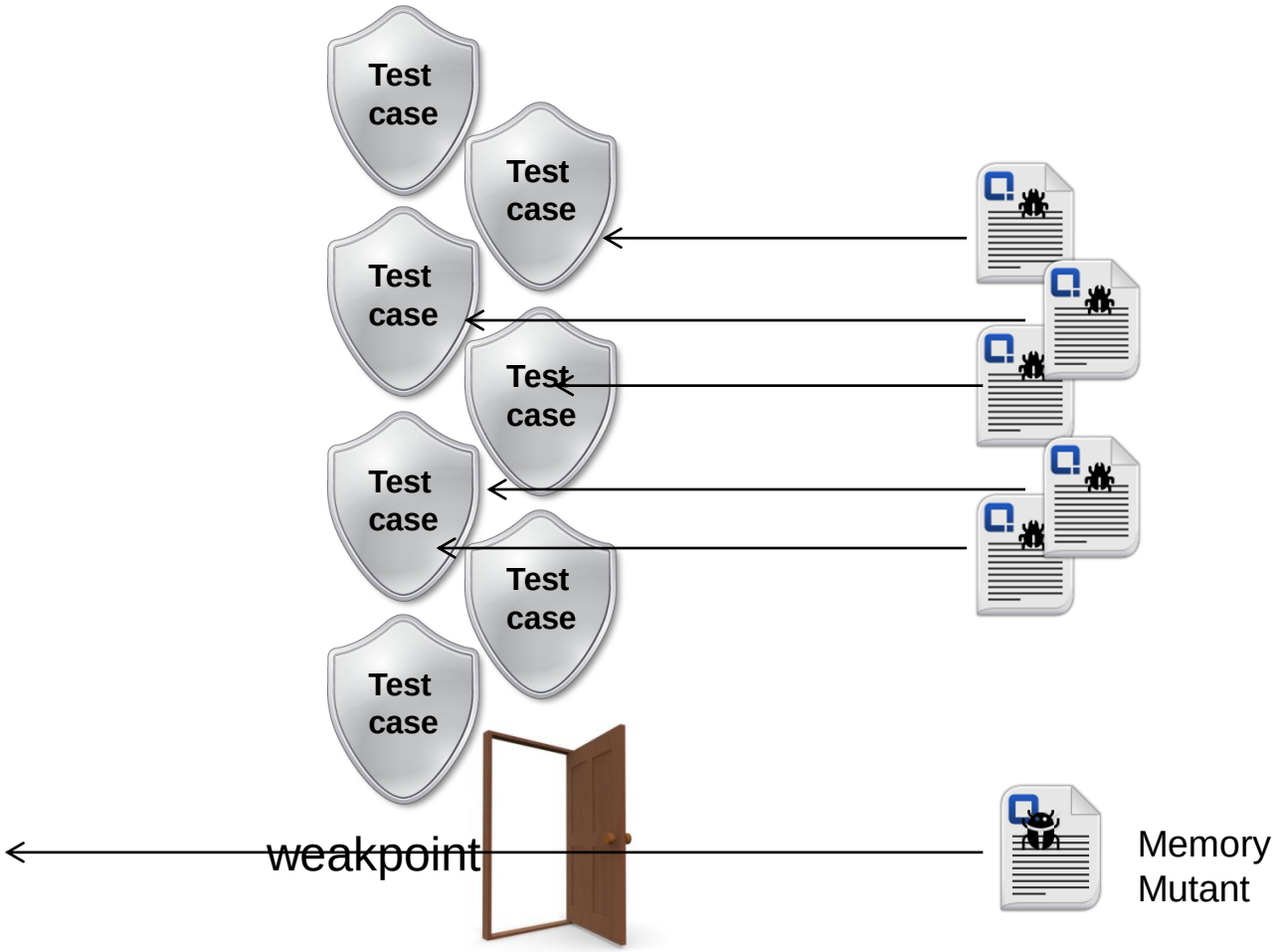
Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Motivation



Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Motivation



Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Memory Mutation Operators

Uninitialized Memory Access

Faulty Memory Allocation

Faulty Heap Management

Memory Mutation Operators

Uninitialized Memory Access

REC2M	calloc(k, sizeof(T))	*Uninitialized memory* malloc(k*sizeof(T))
RMNA	str = NULL	*Use-after-free* str

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Memory Mutation Operators

Faulty Memory Allocation

		Use-before-allocation
REDAWN	malloc(k*sizeof(T))	NULL
		Buffer overflow
REDAWZ	malloc(k*sizeof(T))	malloc(0)
RESOTPE	malloc(k*sizeof(T))	malloc(k*sizeof(T*))
REMSOTP	malloc(k*sizeof(T*))	malloc(k*sizeof(T))

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Memory Mutation Operators

Faulty Heap Management

		Memory leaks
RMFS	free(str)	
REM2A	malloc(k*sizeof(T))	alloc(k*sizeof(T))
REC2A	calloc(k, sizeof(T))	alloc(k*sizeof(T))

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Weakly Killing Criteria

Memory Fault Detection

Control Flow Deviation

Weakly Killing Criteria

Memory Fault Detection (MFD)

$$\mathrm{MFD}: \mathrm{Programs} \times \mathrm{Tests} \mapsto \mathrm{N}$$ (Number of Memory Faults)

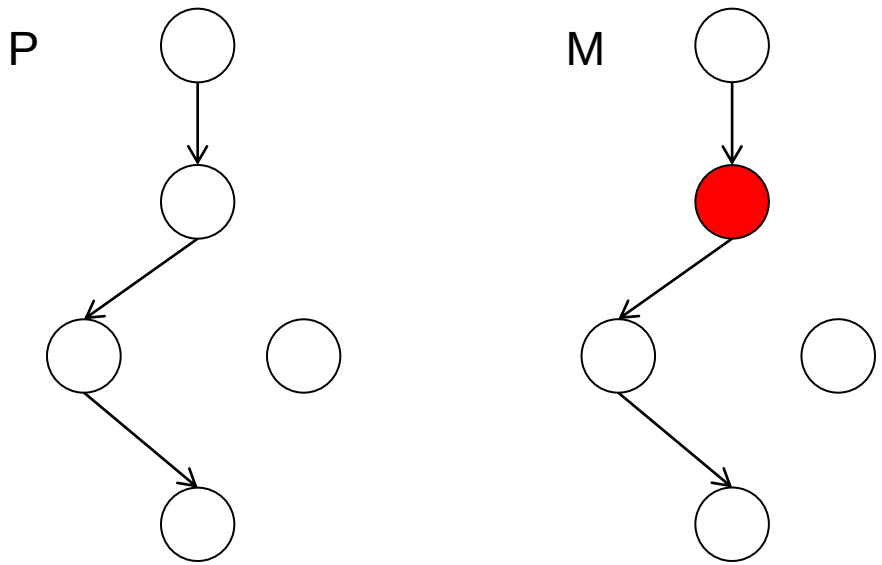
$$\exists t, \mathrm{MFD}(M,t) > \mathrm{MFD}(P,t)$$

Valgrind

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Weakly Killing Criteria

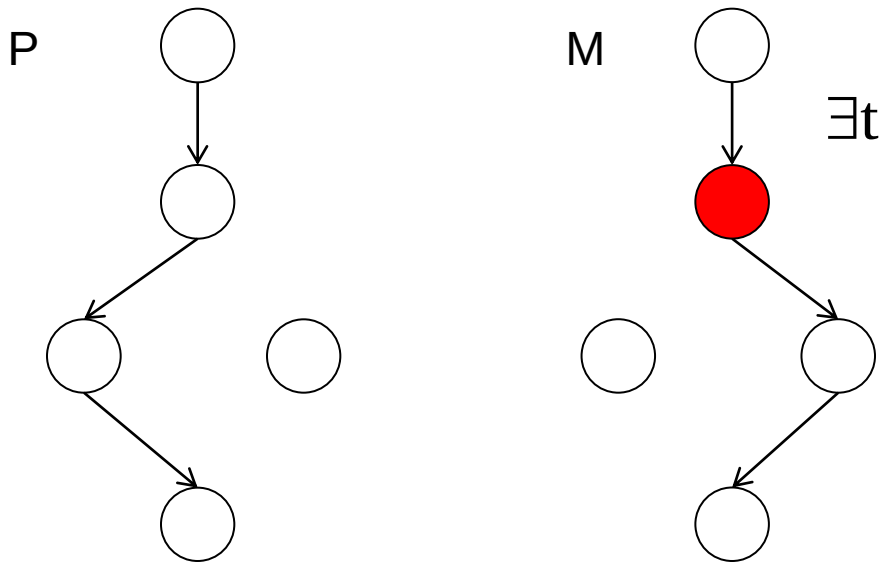
Control Flow Deviation (CFD)



Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Weakly Killing Criteria

Control Flow Deviation (CFD)



$$\exists t, CFD(M,t) \neq CFD(P,t)$$

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Research Questions

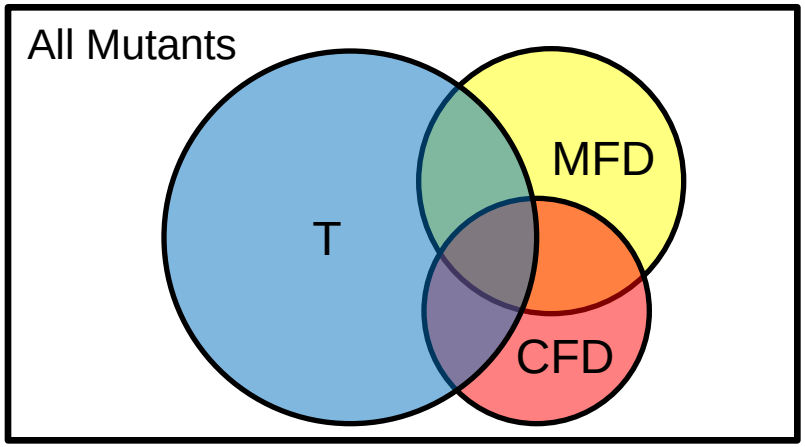
RQ1 What are the characteristics of the proposed Memory Mutation Operators?

- **RQ1a** What is the prevalence of Memory Mutants?
- **RQ1b** How effective is each Memory Mutation Operator in inserting memory faults?
- **RQ1c** What is the Mutation Score for the Traditional criterion applied against the Memory Mutants?

Research Questions

RQ2 What is the reduction rate of survived mutants after introducing Memory Fault Detection and Control Flow Deviation criteria?

RQ3 What is the relation between MFD and CFD criteria?



Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

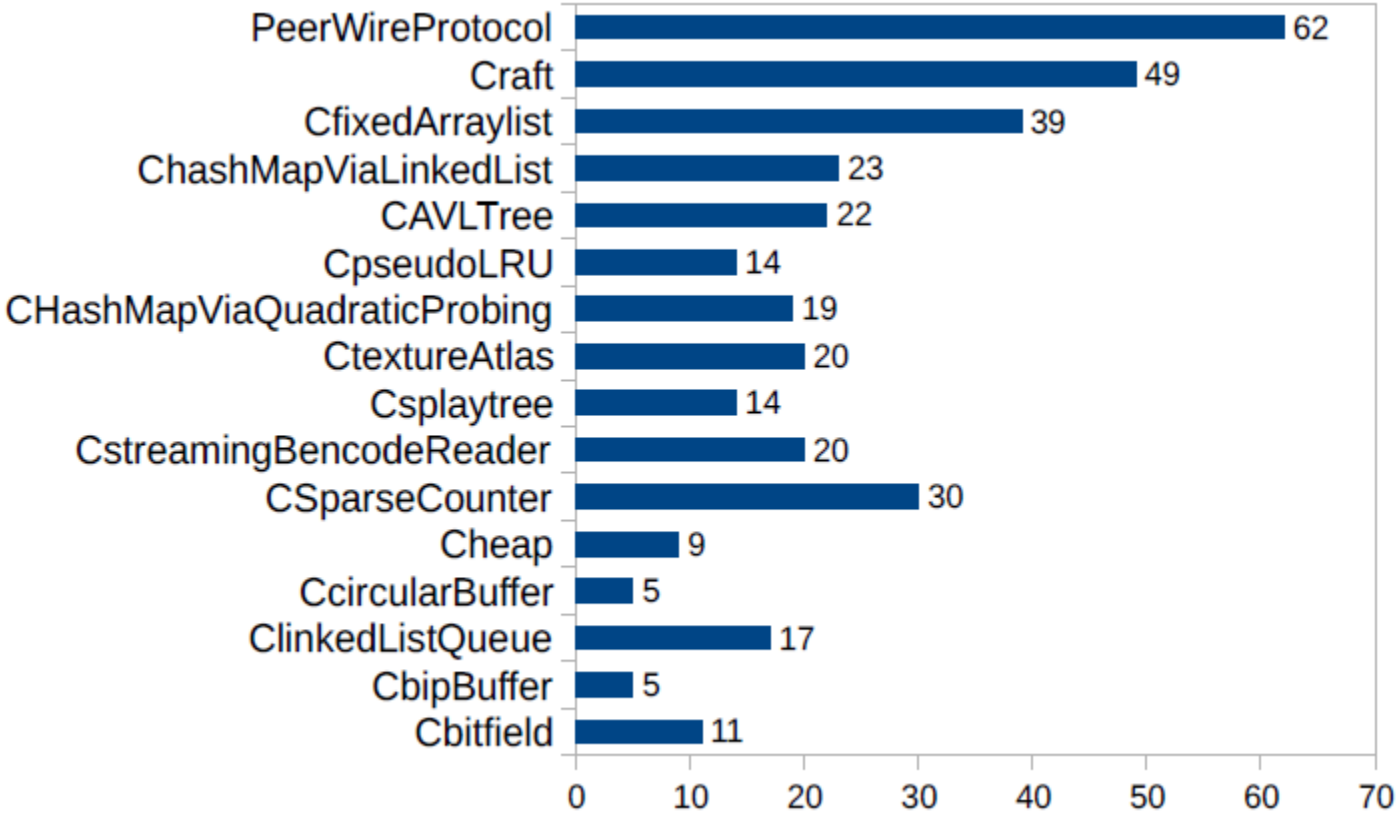
Experiments

No.	Program	LoC
1	PeerWireProtocol	1547
2	Craft	731
3	CfixedArraylist	497
4	ChashMapViaLinkedList	488
5	CAVLTree	405
6	CpseudoLRU	384
7	CHashMapViaQuadraticProbing	1097
8	CtextureAtlas	745
9	Csplaytree	834
10	CstreamingBencodeReader	371
11	CSparseCounter	328
12	Cheap	207
13	CcircularBuffer	118
14	ClinkedListQueue	200
15	CbipBuffer	118
16	Cbitfield	87

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Results (RQ1)

RQ1a What is the prevalence of Memory Mutants?



Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Results (RQ1)

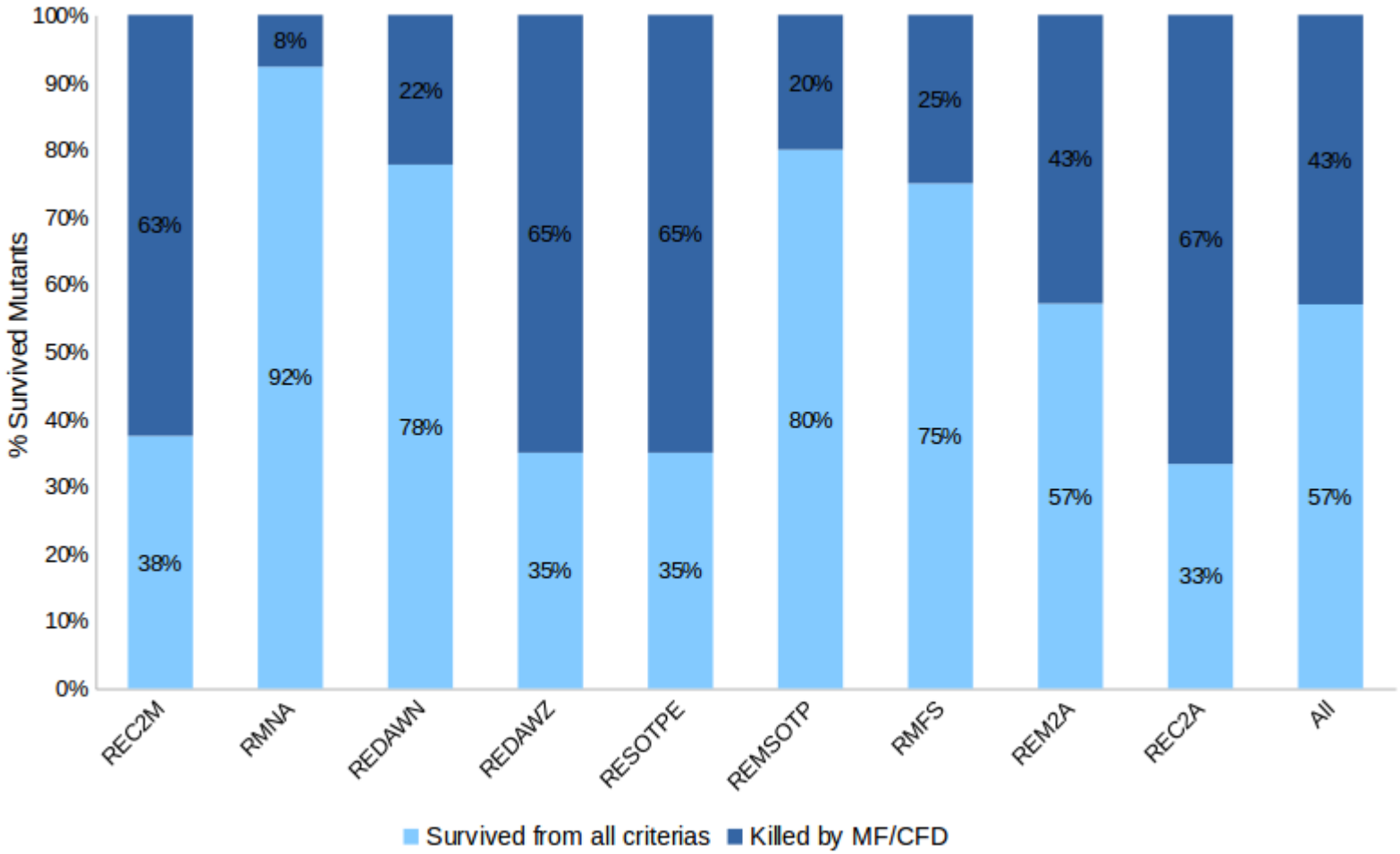
RQ1b How effective is each Memory Mutation Operator in inserting memory faults?

RQ1c What is the Mutation Score for the Traditional criterion applied against the Memory Mutants?

Category	Mutation Operator	Generated Mutants	Survived Mutants	Mutation Score
Uninitialized Memory Access	REC2M	30	25	0.167
	RMNA	39	21	0.462
Faulty Memory Allocation	REDAWN	65	12	0.815
	REDAWZ	63	35	0.444
	RESOTPE	48	28	0.417
	REMSOTP	5	5	0.000
Faulty Heap Management	RMFS	53	53	0.000
	REM2A	27	16	0.407
	REC2A	29	6	0.793
All		359	201	0.440

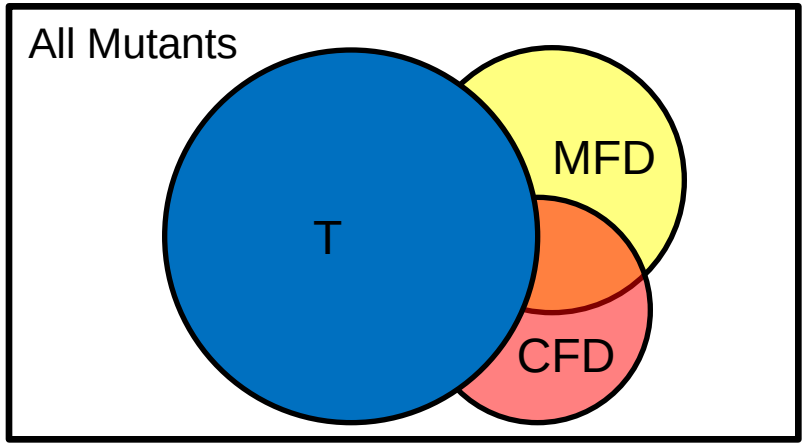
Results (RQ2)

RQ2 What is the reduction rate of survived mutants after introducing Memory Fault Detection and Control Flow Deviation criteria?



Results (RQ3)

RQ3 What is the relation between MFD and CFD criteria?



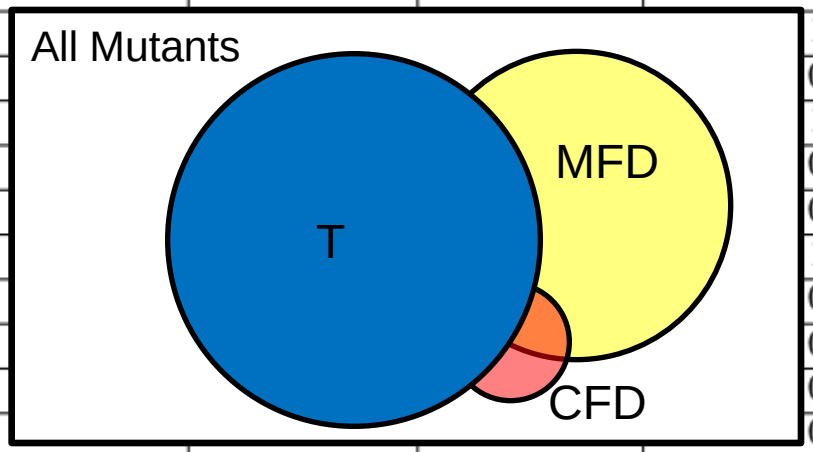
$$c_{\mathrm{MFD}} = \frac{MFD - T - CFD}{MFD \bigcup CFD - T} \qquad c_{\mathrm{CFD}} = \frac{CFD - T - MFD}{MFD \bigcup CFD - T}$$

Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

Results (RQ3)

RQ3 What is the relation between MFD and CFD criteria?

PUT NO.	Number of mutants				c_{MFD}	c_{CFD}
	survived	killed by MFD/CFD	killed by MFD only	killed by CFD only		
1	37	9	4	2	0.444	0.222
2	29	29	25	0	0.862	0
3	37	6	6	0	1	0
4				1	0.5	0.5
5				0	1	0
6				1	0	1
7				0	0	0
8				0	1	0
9				1	0	1
10				0	1	0
11				0	1	0
12				0	0	0
13				0	1	0
14	12	6	4	2	0.667	0.333
15	3	2	2	0	1	0
16	9	3	2	1	0.667	0.333
All	201	91	76	8	0.835	0.088



Jay Nanavati, **Fan Wu**, Mark Harman, Yue Jia, Jens Krinke UCL

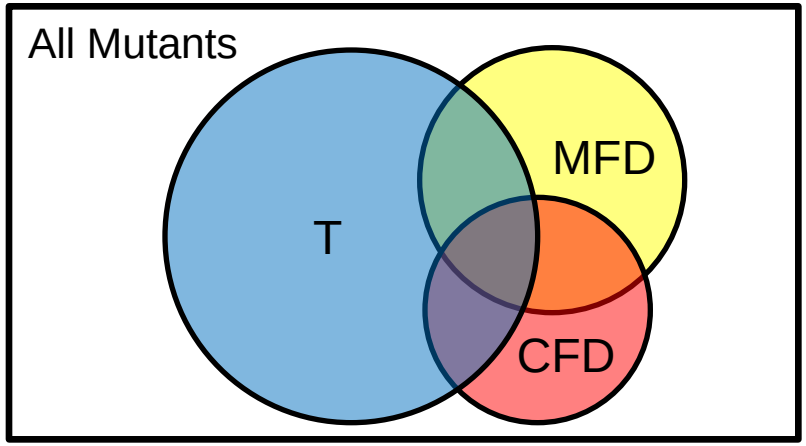
Conclusion & Future Work

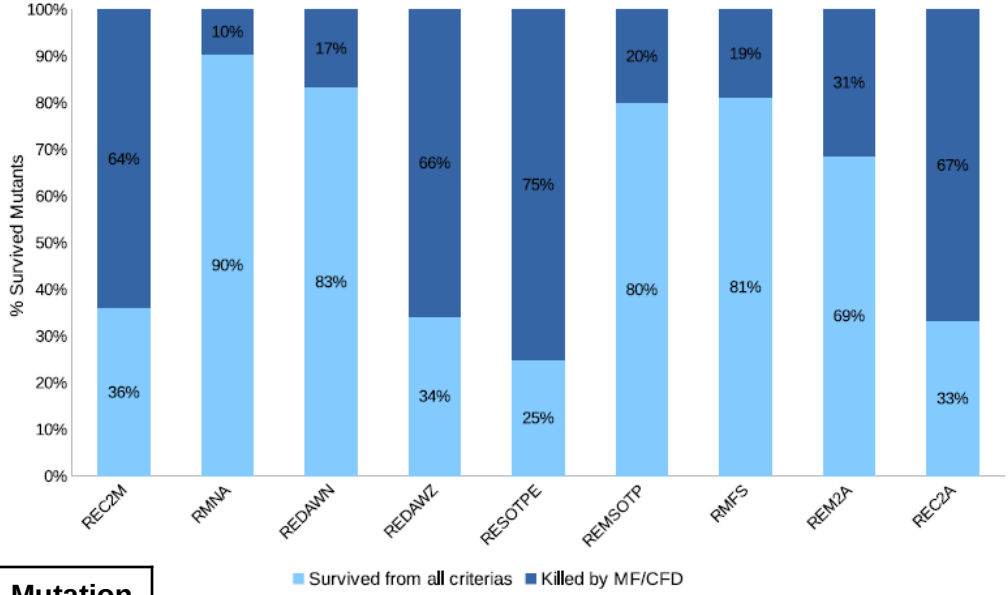
Proposed Memory Mutation Operators

Introduced MFD & CFD, reduced survived mutants

Compare with traditional operators

Extend the comparison between traditional strong killing criterion and MFD/CFD





Category	Mutation Operator	Generated Mutants	Survived Mutants	Mutation Score
Uninitialized Memory Access	REC2M	30	25	0.167
	RMNA	39	21	0.462
Faulty Memory Allocation	REDAWN	65	12	0.815
	REDAWZ	63	35	0.444
	RESOTPE	48	28	0.417
	REMSOTP	5	5	0.000
Faulty Heap Management	RMFS	53	53	0.000
	REM2A	27	16	0.407
	REC2A	29	6	0.793
All		359	201	0.440

		Number of mutants			c_{MFD}	c_{CFD}
		killed by MFD/CFD	killed by MFD only	killed by CFD only		
		9	4	2	0.444	0.222
		29	25	0	0.862	0
		6	6	0	1	0
		2	1	1	0.5	0.5
		5	5	0	1	0
		1	0	1	0	1
		0	0	0	0	0
		8	8	0	1	0
		1	0	1	0	1
		4	4	0	1	0
		13	13	0	1	0
		0	0	0	0	0
		2	2	0	1	0
		6	4	2	0.667	0.333
15	3	2	2	0	1	0
16	9	3	2	1	0.667	0.333
All	201	91	76	8	0.835	0.088