BOGO: Buy Spatial Memory Safety, Get Temporal Memory Safety (Almost) Free

Tong Zhang, Dongyoon Lee, Changhee Jung

Department of Computer Science, Virginia Tech

Motivation

Memory safety issue causes ~70% vulnerabilities in CVE

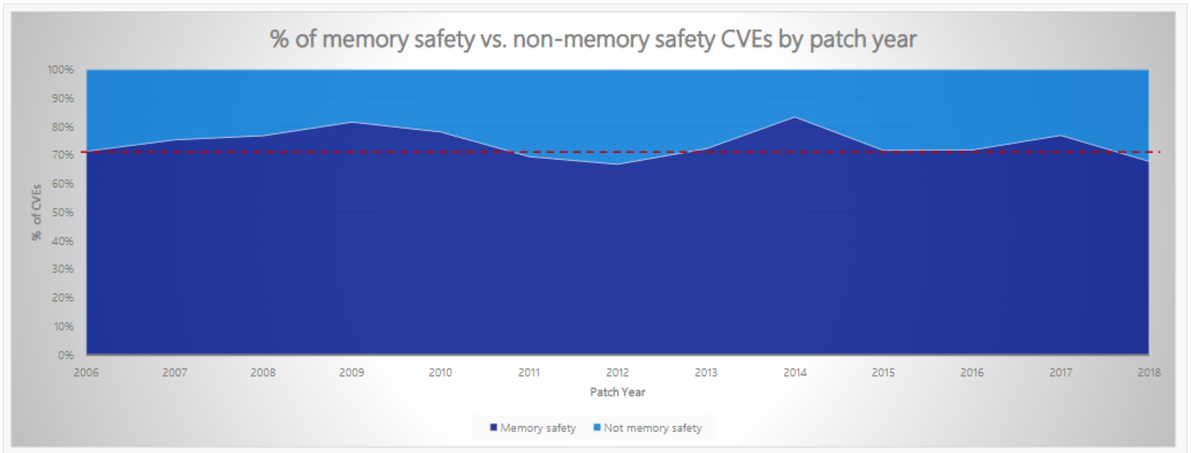


Image: Matt Miler

Common Types of Memory Safety Issue

- Spatial Memory Safety

```
char buf[10];
buf[11] = 'a';
```

Buffer overflow

- Temporal Memory Safety

```
char buf = malloc(10);
free(buf);
buf[0] = 'a';
```

Use-After-Free

Hardware Solution: Intel MPX and toolchain can only support spatial memory safety

How to add temporal memory safety?

Background

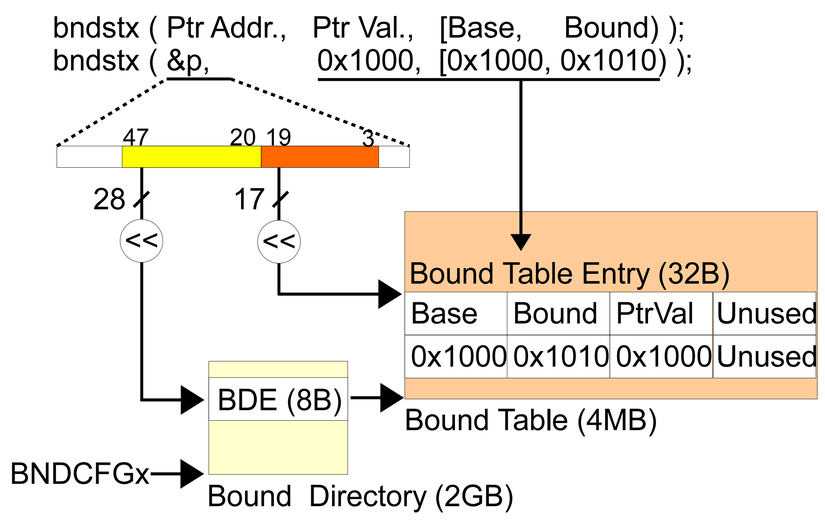
Spatial Memory Safety on Intel MPX

Original Program

```
p=malloc(16);
… // p = p + 4;
*p = 'a';
```

Instrumented Program

```
p=malloc(16);
bnd0 = bndmk(p,16);
bndstx (&p,p,bnd0);
… // p = p + 4;
bnd1 = bndldx(&p,p);
bndcl (&p, bnd1);
bndcu (&p, bnd1);
*p = 'a';
```



Challenges

- Alias Pointer Issue

```
char buf = malloc(10);
char *p = buf;
free(buf);
p[0] = 'a';
```

UAF Undetected

```
char buf = malloc(10);
char *p = buf;
free(buf);
buf = NULL;
p[0] = 'a';
```

UAF Undetected

- Nullify **buf** won't solve the problem
- Hard to find all aliased pointers

- Naïve scan BD(2GB)+BT(4MB per BDE)

```
char buf = malloc(10);
char *p = buf;
free(buf);
p[0] = 'a';
```

Bound of buf	buf, buf+10
Bound of p	buf, buf+10

Nullify bounds by search BD+BT

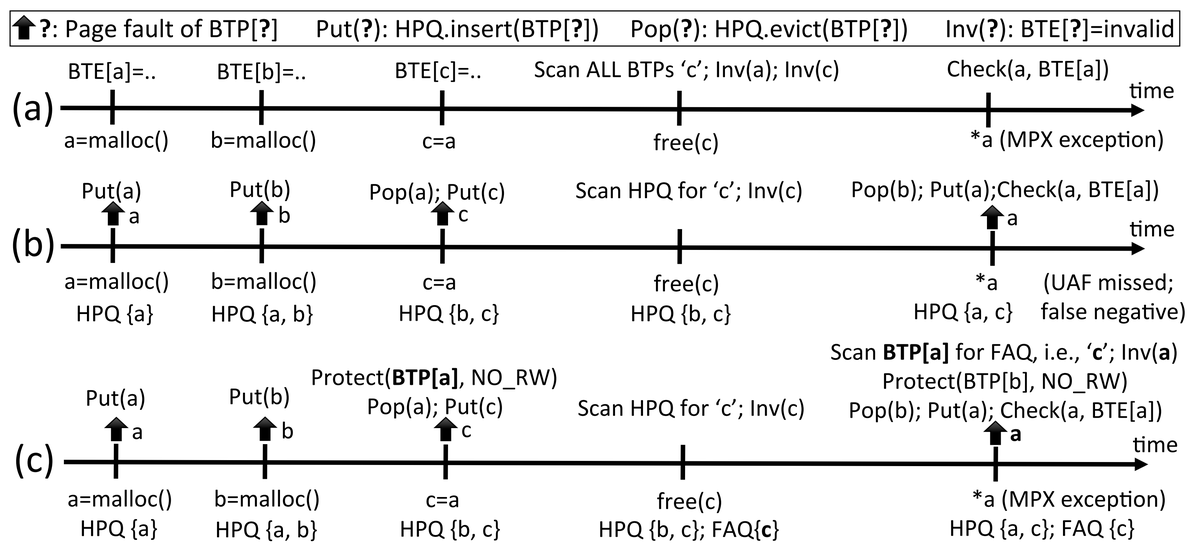
P's bound is nullified, UAF is detected

Bound of buf	NULL
Bound of p	NULL

Our Design

Main idea: Working set tracking and scan hot pages only

a) Full Scan b) Partial Scan c) Partial Scan + PageFault Scan



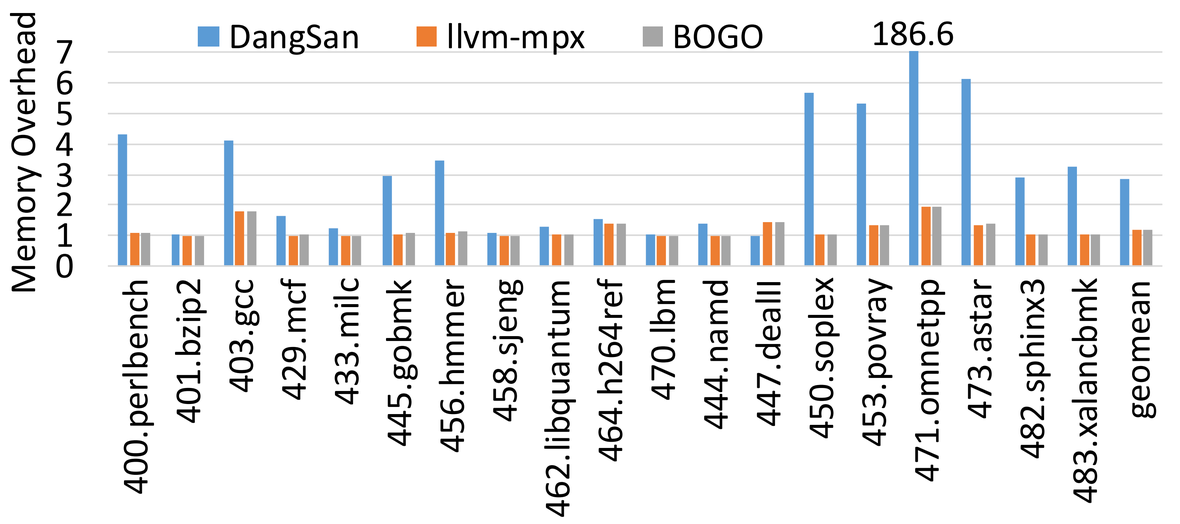
Good Properties

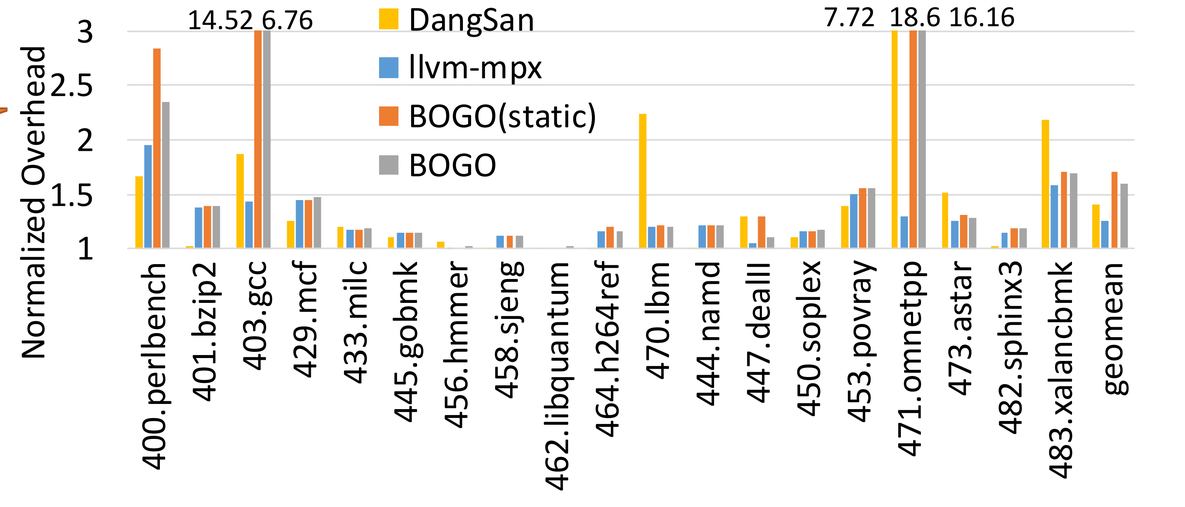
- Partial Scan + PageFaultScan = LowOverhead + No False Negative
- PageFaultScan + RedundancyPredication = Low Overhead + No False Positive

Other Optimizations:

- No PageFaultScan Optimization
- Full PageScan Optimization

Result





Conclusion

BOGO adds temporal memory safety seamlessly to spatial memory safety on Intel MPX. BOGO adds much less memory overhead than other state-of-the-art solutions.