Profile-guided Automated Software Diversity

Andrei Homescu Steven Neisius Per Larsen
Stefan Brunthaler Michael Franz

University of California, Irvine

International Symposium on
Code Generation and Optimization
2013

Overview

Synopsis

- Code-reuse attacks are hard to defeat.

Synopsis

- Code-reuse attacks are hard to defeat.
- Diversity makes code-reuse nearly impossible.

Synopsis

- Code-reuse attacks are hard to defeat.
- Diversity makes code-reuse nearly impossible.
- Unfortunately, there is considerable overhead.

Motivation

Code-reuse Attacks

History of Code Reuse Attacks

Initially:
Attacker writes to memory and diverts flow control.

History of Code Reuse Attacks

Initially:
Attacker writes to memory and diverts flow control.

Then:
W⊕X prevents code injection.

History of Code Reuse Attacks

Initially:
Attacker writes to memory and diverts flow control.

Then:
W⊕X prevents code injection.

Now:
Attacker strings code gadgets together.

What are Gadgets?

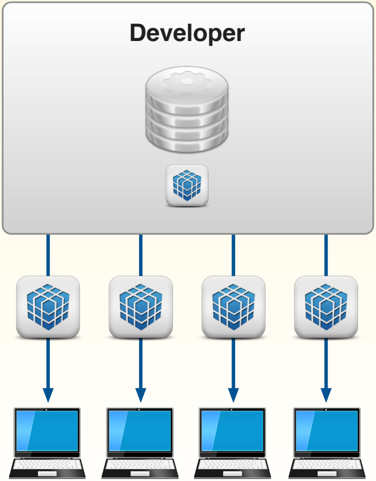
- Valid x86 code.
- Any length.
- Ends with a free branch.

Primary Source of Code-reuse Attacks

Attacker has the program code.

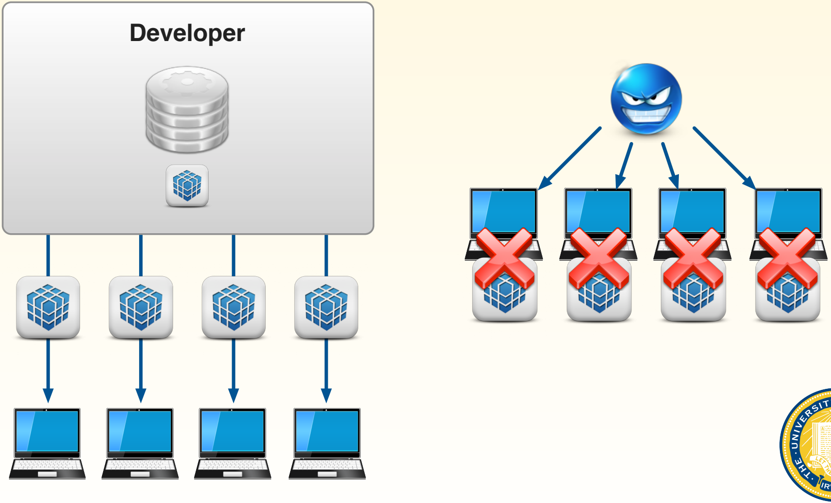
Primary Source of Code-reuse Attacks

Attacker has the program code.

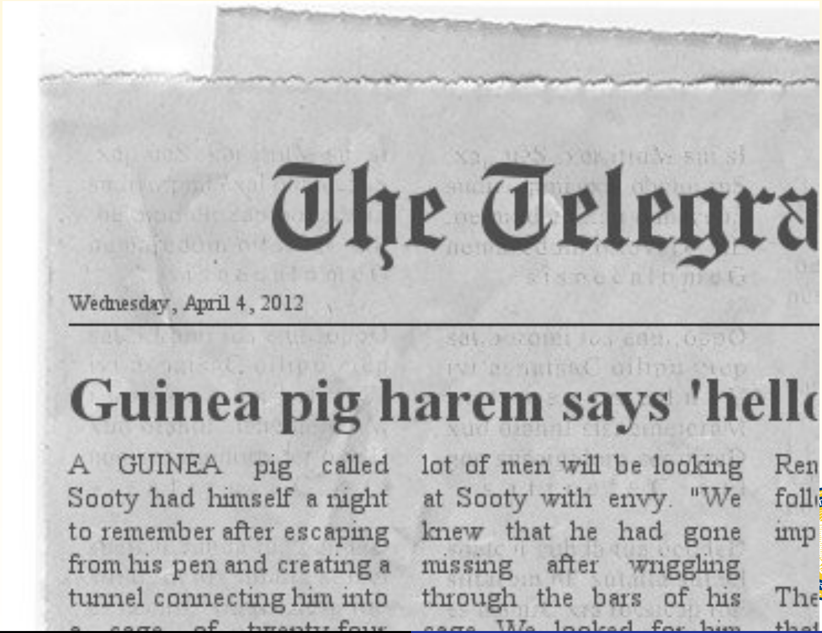


Primary Source of Code-reuse Attacks

Attacker has the program code.



Code-reuse Attack Example



The Telegra

Wednesday, April 4, 2012

Guinea pig harem says 'hell

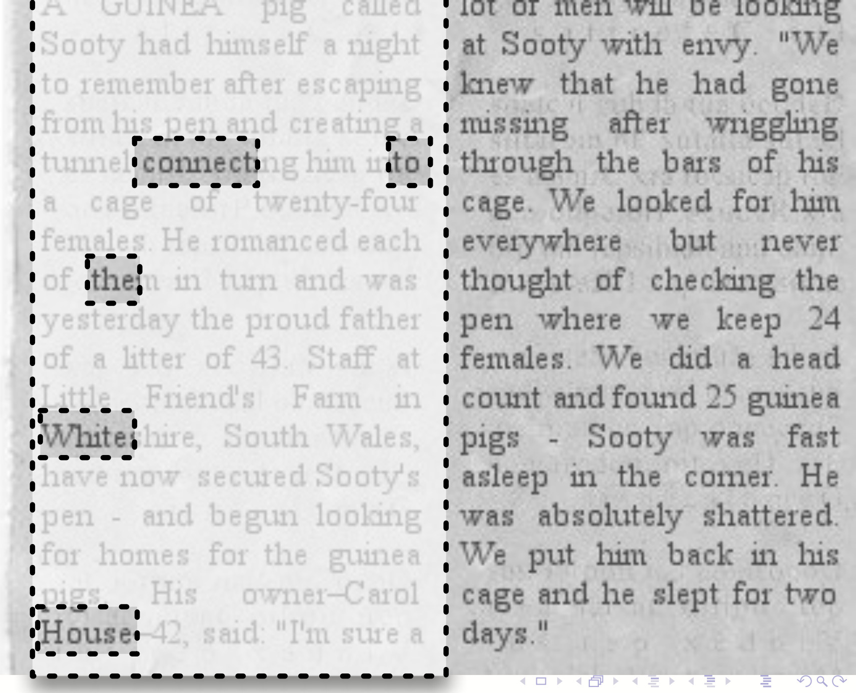
A GUINEA pig called Sooty had himself a night to remember after escaping from his pen and creating a tunnel connecting him into a cage of twenty four

lot of men will be looking at Sooty with envy. "We knew that he had gone missing after wriggling through the bars of his cage. We looked for him

Ren
foll
imp

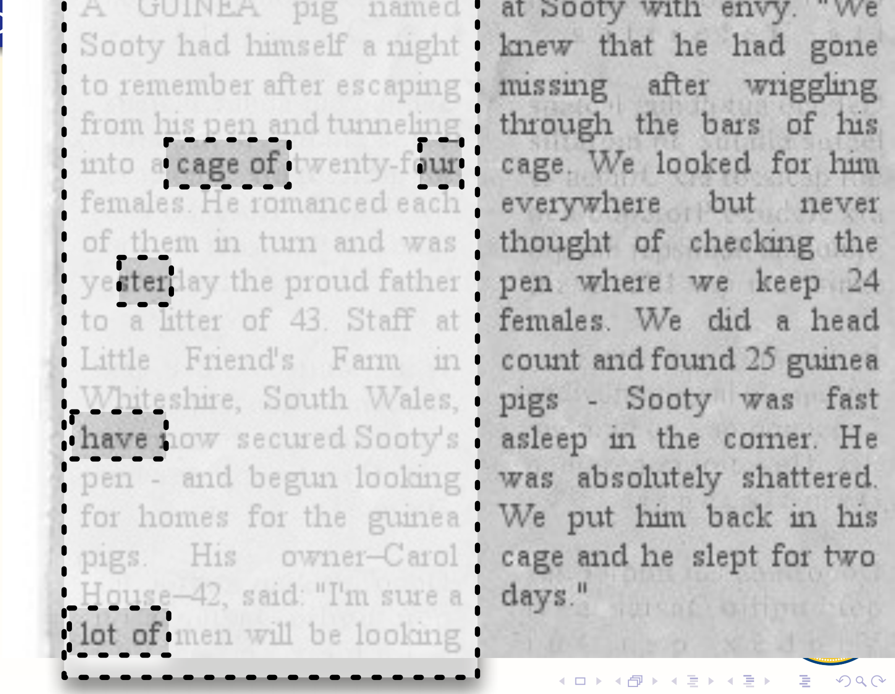
The
that

Co



A GUINEA pig called Sooty had himself a night to remember after escaping from his pen and creating a tunnel connecting him into a cage of twenty-four females. He romanced each of them in turn and was yesterday the proud father of a litter of 43. Staff at Little Friend's Farm in Whiteshire, South Wales, have now secured Sooty's pen - and begun looking for homes for the guinea pigs. His owner–Carol House, 42, said: "I'm sure a lot of men will be looking at Sooty with envy. "We knew that he had gone missing after wriggling through the bars of his cage. We looked for him everywhere but never thought of checking the pen where we keep 24 females. We did a head count and found 25 guinea pigs - Sooty was fast asleep in the comer. He was absolutely shattered. We put him back in his cage and he slept for two days."

Co



A GUINEA pig named Sooty had himself a night to remember after escaping from his pen and tunneling into a cage of twenty-four females. He romanced each of them in turn and was yesterday the proud father to a litter of 43. Staff at Little Friend's Farm in Whiteshire, South Wales, have now secured Sooty's pen - and begun looking for homes for the guinea pigs. His owner—Carol House—42, said: "I'm sure a lot of men will be looking at Sooty with envy. "We knew that he had gone missing after wriggling through the bars of his cage. We looked for him everywhere but never thought of checking the pen where we keep 24 females. We did a head count and found 25 guinea pigs - Sooty was fast asleep in the corner. He was absolutely shattered. We put him back in his cage and he slept for two days."

Ultimate Defense

"The ultimate defense is to drive the complexity of the ultimate attack up so high that the cost of attack is too high to be worth performing."

Operating system protection through program evolution.
F. Cohen, 1993.

Motivation

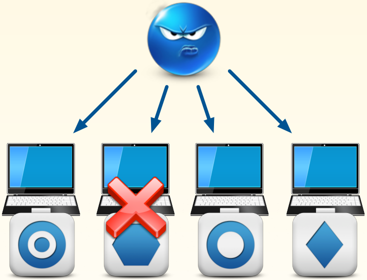
Software Diversity

Types of Diversity

- Watermarking
- Obfuscation
- Tamperproofing
- Exploit Defense

Types of Diversity

- Watermarking
- Obfuscation
- Tamperproofing
- Exploit Defense

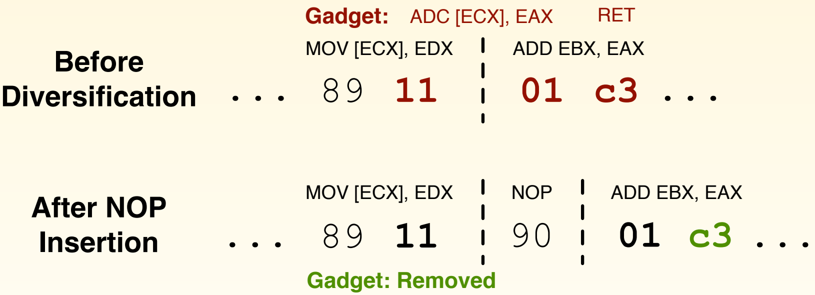


How We Diversify

Multicompiler

Built on LLVM

NOP Insertion



Gadget: ADC [ECX], EAX RET

Before Diversification

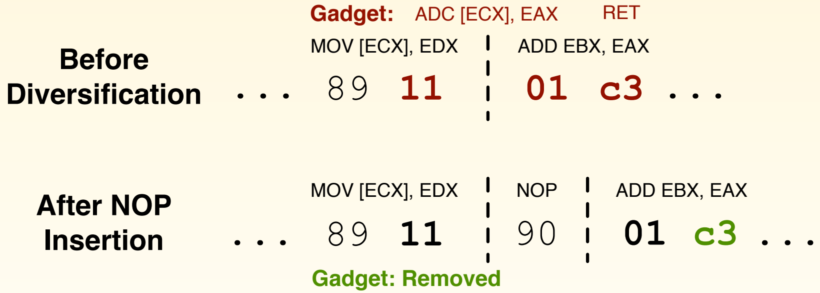
... MOV [ECX], EDX: 89 11 | ADD EBX, EAX: 01 c3 ...

After NOP Insertion

... MOV [ECX], EDX: 89 11 | NOP: 90 | ADD EBX, EAX: 01 c3 ...

Gadget: Removed

NOP Insertion



Before Diversification

Gadget: ADC [ECX], EAX RET

MOV [ECX], EDX | ADD EBX, EAX

. . . 89 **11** | **01 c3** . . .

After NOP Insertion

MOV [ECX], EDX | NOP | ADD EBX, EAX

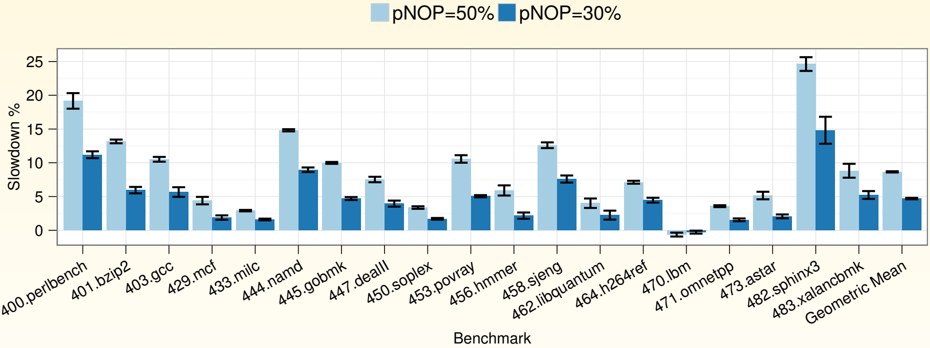
. . . 89 **11** | 90 | **01 c3** . . .

Gadget: Removed

NOP insertion is most effective.

(Breaks 99.99% of gadgets)

NOP Insertion



Highest performance impact.

(Overhead up to 25%)

Contribution

Profile-guided Diversity

Profile-guided Optimization

- Traditionally used to direct more aggressive optimization on hot code.

Profile-guided Optimization

- Traditionally used to direct more aggressive optimization on hot code.
- The majority of run-time is spent in a small portion of the code.

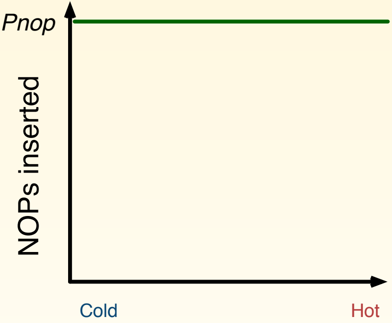
Profile-guided Optimization

- Traditionally used to direct more aggressive optimization on hot code.
- The majority of run-time is spent in a small portion of the code.
- The majority of the diversity overhead is from a small portion of the code.

Profile-guided Optimization

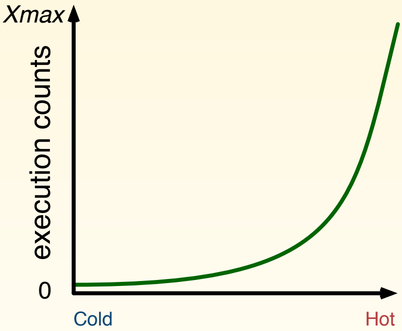
- Traditionally used to direct more aggressive optimization on hot code.
- The majority of run-time is spent in a small portion of the code.
- The majority of the diversity overhead is from a small portion of the code.
- No, this will not make exploits run faster.

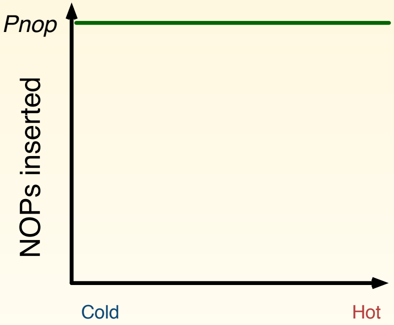
Insertion Probability



```
foo();
for ( int i=0 ; i<100 ; i++ ){
    bar();
    for ( int i=0 ; i<100 ; i++ ){
        baz(); } }
```

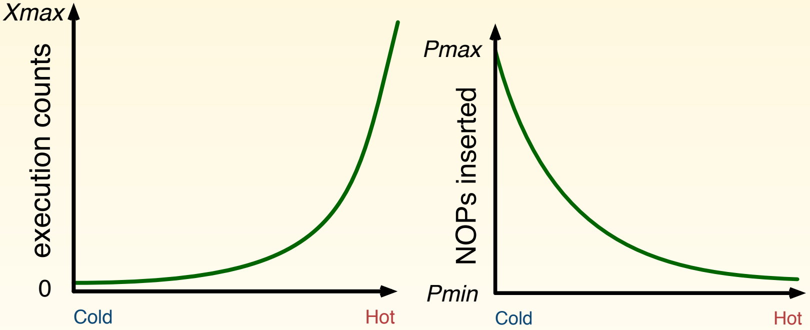
Insertion Probability





```
foo();
for ( int i=0 ; i<100 ; i++ ){
    bar();
    for ( int i=0 ; i<100 ; i++ ){
        baz(); } }
```

Insertion Probability



$$p_{NOP}(x) = p_{max} - (p_{max} - p_{min})\frac{\log(1+x)}{\log(1+x_{max})}$$

Example

Source

```
...
ADD EAX, EBX
MOV [ECX], EAX
JMP @L1

...

@L2:
ADD EAX, ECX
DEC ECX
JCXZ @L2

...


MOV [EBX], EAX
RET
```

W/O Profiling

```
...
ADD EAX, EBX
NOP
MOV [ECX], EAX
NOP
JMP @L1
...
@L2:
NOP
ADD EAX, ECX
NOP
DEC ECX
NOP
JCXZ @L2
...
MOV [EBX], EAX
NOP
RET
```

W/ Profiling

```
...
ADD EAX, EBX
NOP
MOV [ECX], EAX
NOP
JMP @L1
...
@L2:
ADD EAX, ECX
NOP
DEC ECX
JCXZ @L2

...

MOV [EBX], EAX
NOP
RET
```

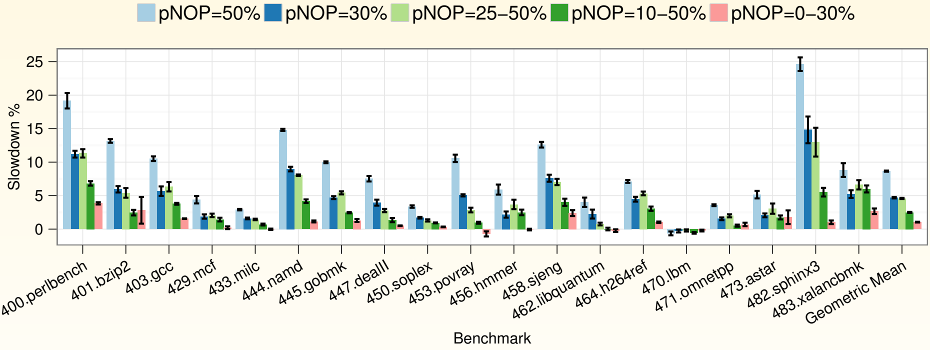
Legend: Hot Code, Cold Code, Inserted NOPs

Performance

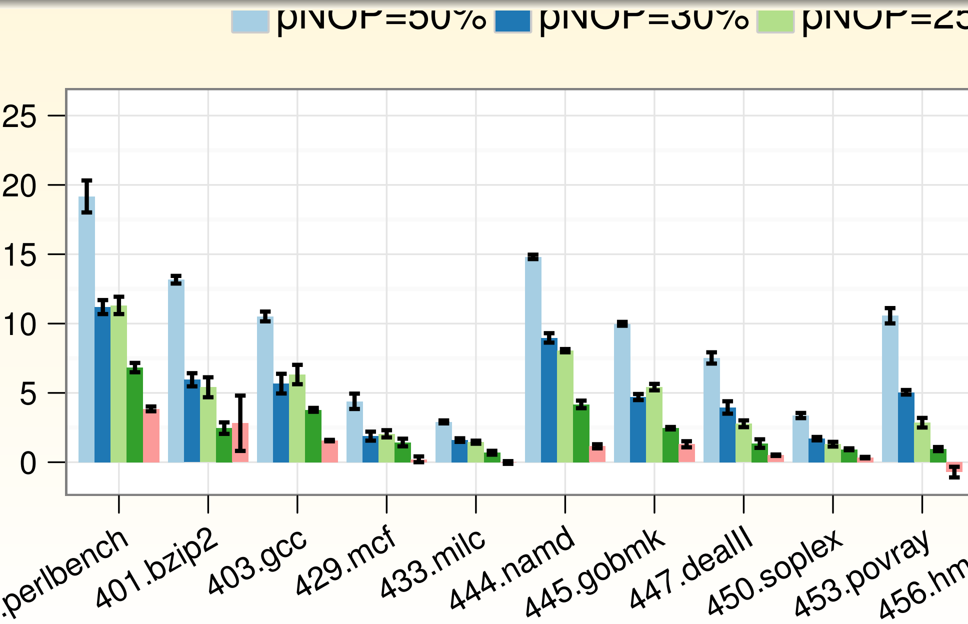
Experimental Setup

- SPEC CPU 2006 benchmarks.
- Profiled with `train` input set.
- `-O2` optimization level.
- 5 diverse versions of each benchmark.
- 3 timed runs per version.

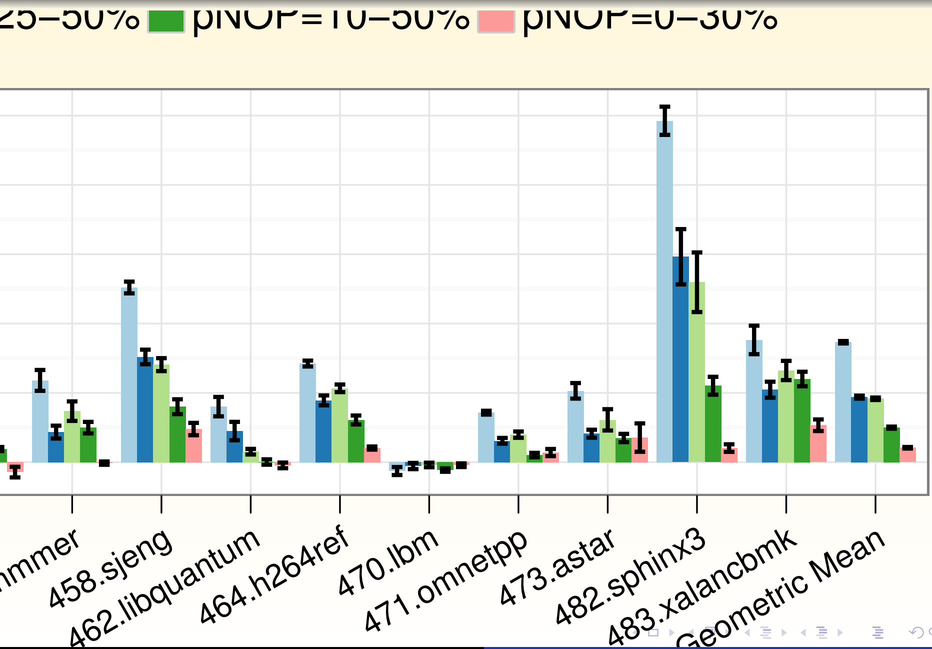
Profile-guided NOP Insertion Performance



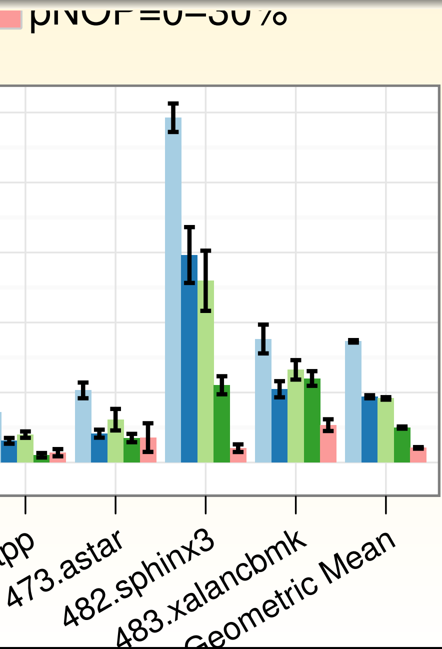
Profile-guided NOP Insertion Performance



Profile-guided NOP Insertion Performance



Profile-guided NOP Insertion Performance



p_{NOP} %	Geo. Mean
50%	8%
30%	5%
25-50%	5%
10-50%	3%
0-30%	1%

Performance Results

- Overhead with profiling becomes negligible.

Performance Results

- Overhead with profiling becomes negligible.
- Allows stronger diversifying transformations without sacrificing performance.

Contribution

Security

Security Criteria

- Concrete Evaluation
  - `ROPgadget` and `microgadgets`
  - Launch attack on real program.
  - Analyze gadgets common to all.
- Statistical Evaluation
  - `Survivor`
  - Pairwise gadget survival.
  - Population analysis.

What is Survivor?

- Compares attack surface of two binaries.
- Gadgets at same offset.
- Ignores NOPs.

PHP Attack

- PHP version 5.3.16
- $p_{\text{NOP}} = 0 - 30\%$
- Profiled with Computer Language Benchmarks Game
- `ROPgadget` and `microgadgets`
- 25 diversified versions

PHP Attack

- PHP version 5.3.16
- $p_{\text{NOP}} = 0 - 30\%$
- Profiled with Computer Language Benchmarks Game
- `ROPgadget` and `microgadgets`
- 25 diversified versions
- No attack succeeded between versions

PHP Attack

- PHP version 5.3.16
- $p_{\text{NOP}} = 0 - 30\%$
- Profiled with Computer Language Benchmarks Game
- `ROPgadget` and `microgadgets`
- 25 diversified versions
- No attack succeeded between versions
- No attack possible with surviving gadgets

Surviving Gadgets

	Gadgets			p_{NOP}			**Gadgets**	
Benchmark	**Baseline**	50%	$25-50\%$	$10-50\%$	30%	$0-30\%$	**Extra%**	**Surviving%**
470.lbm	344	61.60	61.92	61.80	62.88	62.92	**2%**	**18.29%**
462.libquantum	709	52.32	52.28	52.28	52.28	52.92	**1%**	**7.46%**
473.astar	1362	16.64	18.56	22.24	46.20	59.04	**254%**	**4.33%**
458.sjeng	3317	15.08	16.00	16.04	17.24	17.44	**15%**	**0.53%**
444.namd	5322	38.48	39.12	39.60	42.72	43.24	**12%**	**0.81%**
464.h264ref	16233	16.32	16.44	15.68	16.76	18.76	**14%**	**0.12%**
447.dealII	24654	21.20	22.52	22.80	24.92	26.28	**23%**	**0.11%**
400.perlbench	43065	24.68	25.32	24.20	24.08	25.68	**4%**	**0.06%**
471.omnetpp	75246	45.28	47.20	48.08	49.56	59.16	**30%**	**0.08%**
483.xalancbmk	566342	246.80	254.36	253.68	271.24	274.16	**11%**	**0.05%**

Surviving Gadgets

	Gadgets	p_{NOP}					Gadgets	
Benchmark	**Baseline**	50%	$25-50\%$	$10-50\%$	30%	$0-30\%$	**Extra%**	**Surviving%**
470.lbm	344	61.60	61.92	61.80	62.88	62.92	**2%**	**18.29%**
462.libquantum	709	52.32	52.28	52.28	52.28	52.92	**1%**	**7.46%**
473.astar	1362	16.64	18.56	22.24	46.20	59.04	**254%**	**4.33%**
458.sjeng	3317	15.08	16.00	16.04	17.24	17.44	**15%**	**0.53%**
444.namd	5322	38.48	39.12	39.60	42.72	43.24	**12%**	**0.81%**
464.h264ref	16233	16.32	16.44	15.68	16.76	18.76	**14%**	**0.12%**
447.dealII	24654	21.20	22.52	22.80	24.92	26.28	**23%**	**0.11%**
400.perlbench	43065	24.68	25.32	24.20	24.08	25.68	**4%**	**0.06%**
471.omnetpp	75246	45.28	47.20	48.08	49.56	59.16	**30%**	**0.08%**
483.xalancbmk	566342	246.80	254.36	253.68	271.24	274.16	**11%**	**0.05%**

Extra% is $\dfrac{p_{\text{NOP}}0-30\%}{p_{\text{NOP}}50\%}$

Surviving Gadgets

	Gadgets	p_{NOP}					Gadgets	
Benchmark	**Baseline**	50%	$25-50\%$	$10-50\%$	30%	$0-30\%$	**Extra%**	**Surviving%**
470.lbm	344	61.60	61.92	61.80	62.88	62.92	**2%**	**18.29%**
462.libquantum	709	52.32	52.28	52.28	52.28	52.92	**1%**	**7.46%**
473.astar	1362	16.64	18.56	22.24	46.20	59.04	**254%**	**4.33%**
458.sjeng	3317	15.08	16.00	16.04	17.24	17.44	**15%**	**0.53%**
444.namd	5322	38.48	39.12	39.60	42.72	43.24	**12%**	**0.81%**
464.h264ref	16233	16.32	16.44	15.68	16.76	18.76	**14%**	**0.12%**
447.dealII	24654	21.20	22.52	22.80	24.92	26.28	**23%**	**0.11%**
400.perlbench	43065	24.68	25.32	24.20	24.08	25.68	**4%**	**0.06%**
471.omnetpp	75246	45.28	47.20	48.08	49.56	59.16	**30%**	**0.08%**
483.xalancbmk	566342	246.80	254.36	253.68	271.24	274.16	**11%**	**0.05%**

Extra% is $\frac{p_{\text{NOP}}0-30\%}{p_{\text{NOP}}50\%}$

Surviving Gadgets

	Gadgets	p_{NOP}					Gadgets	
Benchmark	**Baseline**	50%	$25-50\%$	$10-50\%$	30%	$0-30\%$	**Extra%**	**Surviving%**
470.lbm	344	61.60	61.92	61.80	62.88	62.92	**2%**	**18.29%**
462.libquantum	709	52.32	52.28	52.28	52.28	52.92	**1%**	**7.46%**
473.astar	1362	16.64	18.56	22.24	46.20	59.04	**254%**	**4.33%**
458.sjeng	3317	15.08	16.00	16.04	17.24	17.44	**15%**	**0.53%**
444.namd	5322	38.48	39.12	39.60	42.72	43.24	**12%**	**0.81%**
464.h264ref	16233	16.32	16.44	15.68	16.76	18.76	**14%**	**0.12%**
447.dealII	24654	21.20	22.52	22.80	24.92	26.28	**23%**	**0.11%**
400.perlbench	43065	24.68	25.32	24.20	24.08	25.68	**4%**	**0.06%**
471.omnetpp	75246	45.28	47.20	48.08	49.56	59.16	**30%**	**0.08%**
483.xalancbmk	566342	246.80	254.36	253.68	271.24	274.16	**11%**	**0.05%**

Extra% is $\frac{p_{\text{NOP}}0-30\%}{p_{\text{NOP}}50\%}$

Surviving Gadgets

	Gadgets	p_{NOP}					Gadgets	
Benchmark	**Baseline**	50%	$25-50\%$	$10-50\%$	30%	$0-30\%$	**Extra%**	**Surviving%**
470.lbm	344	61.60	61.92	61.80	62.88	62.92	**2%**	**18.29%**
462.libquantum	709	52.32	52.28	52.28	52.28	52.92	**1%**	**7.46%**
473.astar	1362	16.64	18.56	22.24	46.20	59.04	**254%**	**4.33%**
458.sjeng	3317	15.08	16.00	16.04	17.24	17.44	**15%**	**0.53%**
444.namd	5322	38.48	39.12	39.60	42.72	43.24	**12%**	**0.81%**
464.h264ref	16233	16.32	16.44	15.68	16.76	18.76	**14%**	**0.12%**
447.dealII	24654	21.20	22.52	22.80	24.92	26.28	**23%**	**0.11%**
400.perlbench	43065	24.68	25.32	24.20	24.08	25.68	**4%**	**0.06%**
471.omnetpp	75246	45.28	47.20	48.08	49.56	59.16	**30%**	**0.08%**
483.xalancbmk	566342	246.80	254.36	253.68	271.24	274.16	**11%**	**0.05%**

Extra% is $\frac{p_{\text{NOP}}0-30\%}{p_{\text{NOP}}50\%}$

Gadgets Surviving in a Population of 25 Versions

	$p_{\text{NOP}}\%$									
	At least 2 versions					**At least 12 versions**				
Benchmark	50	$25-50$	$10-50$	30	$0-30$	50	$25-50$	$10-50$	30	$0-30$
470.lbm	586	608	614	602	723	50	50	46	50	50
462.libquantum	871	819	849	1082	1229	41	41	41	43	41
473.astar	1335	1373	1551	1580	2165	45	44	44	41	48
458.sjeng	1502	2110	2008	2927	3593	41	44	44	42	42
444.namd	2189	2449	2524	3509	4225	54	64	63	64	67
464.h264ref	3639	4343	5163	7138	7216	44	41	42	43	49
447.dealII	5764	7647	7723	8759	10550	44	44	44	44	47
400.perlbench	6827	10380	7935	8361	11117	44	48	44	42	40
471.omnetpp	17156	17523	17914	60388	29870	48	47	47	44	48
483.xalancbmk	76765	79688	82053	102370	109543	42	42	16	16	44

Gadgets Surviving in a Population of 25 Versions

	$p_{\text{NOP}}\%$									
	At least 2 versions					At least 12 versions				
Benchmark	50	$25-50$	$10-50$	30	$0-30$	50	$25-50$	$10-50$	30	$0-30$
470.lbm	586	608	614	602	723	50	50	46	50	50
462.libquantum	871	819	849	1082	1229	41	41	41	43	41
473.astar	1335	1373	1551	1580	2165	45	44	44	41	48
458.sjeng	1502	2110	2008	2927	3593	41	44	44	42	42
444.namd	2189	2449	2524	3509	4225	54	64	63	64	67
464.h264ref	3639	4343	5163	7138	7216	44	41	42	43	49
447.dealII	5764	7647	7723	8759	10550	44	44	44	44	47
400.perlbench	6827	10380	7935	8361	11117	44	48	44	42	40
471.omnetpp	17156	17523	17914	60388	29870	48	47	47	44	48
483.xalancbmk	76765	79688	82053	102370	109543	42	42	16	16	44

Gadgets Surviving in a Population of 25 Versions

	p_{NOP}%									
	At least 2 versions					**At least 12 versions**				
Benchmark	50	$25-50$	$10-50$	30	$0-30$	50	$25-50$	$10-50$	30	$0-30$
470.lbm	586	608	614	602	723	50	50	46	50	50
462.libquantum	871	819	849	1082	1229	41	41	41	43	41
473.astar	1335	1373	1551	1580	2165	45	44	44	41	48
458.sjeng	1502	2110	2008	2927	3593	41	44	44	42	42
444.namd	2189	2449	2524	3509	4225	54	64	63	64	67
464.h264ref	3639	4343	5163	7138	7216	44	41	42	43	49
447.dealII	5764	7647	7723	8759	10550	44	44	44	44	47
400.perlbench	6827	10380	7935	8361	11117	44	48	44	42	40
471.omnetpp	17156	17523	17914	60388	29870	48	47	47	44	48
483.xalancbmk	76765	79688	82053	102370	109543	42	42	16	16	44

483.xalancbmk has a baseline of 566,342 gadgets.

Security Results

Preserves the security properties of NOP insertion.

Conclusion

Profile-guided software diversification has a minimal impact on performance.

Attacks against a diverse program have a high chance of failure.

Questions?

Thank You!