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
Code-reuse attacks are hard to defeat.
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

Homescu, Neisius, Larsen, Brunthaler, Franz

Profile-guided Automated Software Diversity

Code-reuse Attacks
Initially:
Attacker writes to memory and diverts flow control.
Initially:
Attacker writes to memory and diverts flow control.

Then:
$W \oplus X$ prevents code injection.
Initially:
Attacker writes to memory and diverts flow control.

Then:
$W \oplus X$ prevents code injection.

Now:
Attacker strings code gadgets together.
What are Gadgets?

- Valid x86 code.
- Any length.
- Ends with a free branch.
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.
Guinea pig harem says 'hello'

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 lots of men will be looking at Sooty with envy. 'We knew that he had gone missing after wiggling through the bars of his cage. We looked for him that
A GUINEA pig called Sooty had himself a night to remember after escaping from his pen and creating a tunnel, bringing 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 Little Friend's Farm, 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."
A GUINEA pig named Sooty had himself a night to remember after escaping from his pen and tunneling into a 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."
"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
Multicompiler
Built on LLVM
NOP Insertion

<table>
<thead>
<tr>
<th>Before Diversification</th>
<th>After NOP Insertion</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOV [ECX], EDX</td>
<td>MOV [ECX], EDX</td>
</tr>
<tr>
<td>ADD EBX, EAX</td>
<td>NOP</td>
</tr>
<tr>
<td>ADC [ECX], EAX</td>
<td>ADD EBX, EAX</td>
</tr>
<tr>
<td>RET</td>
<td>90</td>
</tr>
</tbody>
</table>

**Gadget:** ADC [ECX], EAX RET

**Gadget:** Removed

 NOP insertion is most effective. (Breaks 99.99% of gadgets)

Homescu, Neisius, Larsen, Brunthaler, Franz
NOP Insertion

Before Diversification

Gadget: ADC [ECX], EAX RET
MOV [ECX], EDX | ADD EBX, EAX

After NOP Insertion

Gadget: Removed
MOV [ECX], EDX | NOP | ADD EBX, EAX

NOP insertion is most effective.
(Breaks 99.99% of gadgets)
Highest performance impact.
(Overhead up to 25%)
Profile-guided Diversity
Traditionally used to direct more aggressive optimization on hot code.
Traditionally used to direct more aggressive optimization on hot code.

The majority of run-time is spent in a small portion of the code.
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.
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.
foo();
for ( int i=0 ; i<100 ; i++ ){
    bar();
    for ( int i=0 ; i<100 ; i++ ){
        baz();
    }
}
foo();
for (int i=0; i<100; i++) {
    bar();
    for (int i=0; i<100; i++) {
        baz();
    }
}
\[ p_{NOP}(x) = p_{max} - (p_{max} - p_{min}) \frac{\log(1+x)}{\log(1+x_{max})} \]
Example

Source

\[
\ldots
\]

\[
\text{ADD EAX, EBX}
\]

\[
\text{MOV [ECX], EAX}
\]

\[
\text{JMP @L1}
\]

\[
\ldots
\]

\[
\text{@L2:}
\]

\[
\text{ADD EAX, ECX}
\]

\[
\text{DEC ECX}
\]

\[
\text{J CXZ @L2}
\]

\[
\ldots
\]

\[
\text{MOV [EBX], EAX}
\]

\[
\text{RET}
\]

W/O Profiling

\[
\ldots
\]

\[
\text{ADD EAX, EBX}
\]

\[
\text{NOP}
\]

\[
\text{MOV [ECX], EAX}
\]

\[
\text{NOP}
\]

\[
\text{JMP @L1}
\]

\[
\ldots
\]

\[
\text{@L2:}
\]

\[
\text{NOP}
\]

\[
\text{ADD EAX, ECX}
\]

\[
\text{NOP}
\]

\[
\text{DEC ECX}
\]

\[
\text{J CXZ @L2}
\]

\[
\ldots
\]

\[
\text{MOV [EBX], EAX}
\]

\[
\text{NOP}
\]

\[
\text{RET}
\]

W/ Profiling

\[
\ldots
\]

\[
\text{ADD EAX, EBX}
\]

\[
\text{NOP}
\]

\[
\text{MOV [ECX], EAX}
\]

\[
\text{NOP}
\]

\[
\text{JMP @L1}
\]

\[
\ldots
\]

\[
\text{@L2:}
\]

\[
\text{ADD EAX, ECX}
\]

\[
\text{NOP}
\]

\[
\text{DEC ECX}
\]

\[
\text{J CXZ @L2}
\]

\[
\ldots
\]

\[
\text{MOV [EBX], EAX}
\]

\[
\text{NOP}
\]

\[
\text{RET}
\]

Legend: Hot Code, Cold Code, Inserted NOPs
Performance
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

25–50%  pNOP=10−50%  pNOP=0−30%

Homescu, Neisius, Larsen, Brunthaler, Franz  Profile-guided Automated Software Diversity 21/32
Profile-guided NOP Insertion Performance

$p_{\text{NOP}} = 0$--$50\%$

<table>
<thead>
<tr>
<th>$p_{\text{NOP}}$</th>
<th>Geo. Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>8%</td>
</tr>
<tr>
<td>30%</td>
<td>5%</td>
</tr>
<tr>
<td>25-50%</td>
<td>5%</td>
</tr>
<tr>
<td>10-50%</td>
<td>3%</td>
</tr>
<tr>
<td>0-30%</td>
<td>1%</td>
</tr>
</tbody>
</table>
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 version 5.3.16

$p_{NOP} = 0 - 30\%$

Profiled with Computer Language Benchmarks Game

ROPgadget and microgadgets

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

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

**Extra%** is $\frac{p_{NOP}^{0-30\%}}{p_{NOP}^{50\%}}$
### Surviving Gadgets

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

**Extra% is** \( \frac{p_{NOP}^{0-30\%}}{p_{NOP}^{50\%}} \)
### Gadgets Benchmark

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

**Extra% is** $\frac{p_{NOP}^{0-30\%}}{p_{NOP}^{50\%}}$
# Surviving Gadgets

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

**Extra% is** \( \frac{p_{NOP}^{0–30%}}{p_{NOP}^{50%}} \)
## Gadgets Surviving in a Population of 25 Versions

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>$p_{\text{NOP}}%$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>At least 2 versions</td>
</tr>
<tr>
<td></td>
<td>50 25–50 10–50</td>
</tr>
<tr>
<td>470.lbm</td>
<td>586 608 614</td>
</tr>
<tr>
<td>462.libquantum</td>
<td>871 819 849</td>
</tr>
<tr>
<td>473.astar</td>
<td>1335 1373 1551</td>
</tr>
<tr>
<td>458.sjeng</td>
<td>1502 2110 2008</td>
</tr>
<tr>
<td>444.namd</td>
<td>2189 2449 2524</td>
</tr>
<tr>
<td>464.h264ref</td>
<td>3639 4343 5163</td>
</tr>
<tr>
<td>447.dealII</td>
<td>5764 7647 7723</td>
</tr>
<tr>
<td>400.perlbench</td>
<td>6827 10380 7935</td>
</tr>
<tr>
<td>471.omnetpp</td>
<td>17156 17523 17914</td>
</tr>
<tr>
<td>483.xalancbmk</td>
<td>76765 79688 82053</td>
</tr>
</tbody>
</table>
## Gadgets Surviving in a Population of 25 Versions

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>At least 2 versions</th>
<th></th>
<th></th>
<th></th>
<th>At least 12 versions</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50 25−50 10−50</td>
<td>30</td>
<td>0−30</td>
<td>50 25−50 10−50</td>
<td>30</td>
<td>0−30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>470.lbm</td>
<td>586 608 614</td>
<td>602</td>
<td>723</td>
<td>50</td>
<td>50</td>
<td>46</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>462.libquantum</td>
<td>871 819 849</td>
<td>1082</td>
<td>1229</td>
<td>41</td>
<td>41</td>
<td>41</td>
<td>43</td>
<td>41</td>
</tr>
<tr>
<td>473.astar</td>
<td>1335 1373 1551</td>
<td>1580</td>
<td>2165</td>
<td>45</td>
<td>44</td>
<td>44</td>
<td>41</td>
<td>48</td>
</tr>
<tr>
<td>458.sjeng</td>
<td>1502 2110 2008</td>
<td>2927</td>
<td>3593</td>
<td>41</td>
<td>44</td>
<td>44</td>
<td>42</td>
<td>42</td>
</tr>
<tr>
<td>444.namd</td>
<td>2189 2449 2524</td>
<td>3509</td>
<td>4225</td>
<td>54</td>
<td>64</td>
<td>63</td>
<td>64</td>
<td>67</td>
</tr>
<tr>
<td>464.h264ref</td>
<td>3639 4343 5163</td>
<td>7138</td>
<td>7216</td>
<td>44</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>49</td>
</tr>
<tr>
<td>447.dealII</td>
<td>5764 7647 7723</td>
<td>8759</td>
<td>10550</td>
<td>44</td>
<td>44</td>
<td>44</td>
<td>44</td>
<td>47</td>
</tr>
<tr>
<td>400.perlbench</td>
<td>6827 10380 7935</td>
<td>8361</td>
<td>11117</td>
<td>44</td>
<td>48</td>
<td>44</td>
<td>42</td>
<td>40</td>
</tr>
<tr>
<td>471.omnetpp</td>
<td>17156 17523 17914</td>
<td>60388</td>
<td>29870</td>
<td>48</td>
<td>47</td>
<td>47</td>
<td>44</td>
<td>48</td>
</tr>
<tr>
<td>483.xalancbmk</td>
<td>76765 79688 82053</td>
<td>102370</td>
<td>109543</td>
<td>42</td>
<td>42</td>
<td>16</td>
<td>16</td>
<td>44</td>
</tr>
</tbody>
</table>
### Gadgets Surviving in a Population of 25 Versions

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>At least 2 versions</th>
<th>pNOP%</th>
<th>At least 12 versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50 25 – 50 10 – 50</td>
<td></td>
<td>50 25 – 50 10 – 50</td>
</tr>
<tr>
<td>470.lbm</td>
<td>586 608 614</td>
<td>602 723</td>
<td>50 50 46</td>
</tr>
<tr>
<td>462.libquantum</td>
<td>871 819 849</td>
<td>1082 1229</td>
<td>41 41 41</td>
</tr>
<tr>
<td>473.astar</td>
<td>1335 1373 1551</td>
<td>1580 2165</td>
<td>45 44 44</td>
</tr>
<tr>
<td>458.sjeng</td>
<td>1502 2110 2008</td>
<td>2927 3593</td>
<td>41 44 44</td>
</tr>
<tr>
<td>444.namd</td>
<td>2189 2449 2524</td>
<td>3509 4225</td>
<td>54 64 63</td>
</tr>
<tr>
<td>464.h264ref</td>
<td>3639 4343 5163</td>
<td>7138 7216</td>
<td>44 41 42</td>
</tr>
<tr>
<td>447.dealll</td>
<td>5764 7647 7723</td>
<td>8759 10550</td>
<td>44 44 44</td>
</tr>
<tr>
<td>400.perlbench</td>
<td>6827 10380 7935</td>
<td>8361 11117</td>
<td>44 48 44</td>
</tr>
<tr>
<td>471.omnetpp</td>
<td>17156 17523 17914</td>
<td>60388 29870</td>
<td>48 47 47</td>
</tr>
<tr>
<td>483.xalancbmk</td>
<td>76765 79688 82053</td>
<td>102370 109543</td>
<td>42 42 16</td>
</tr>
</tbody>
</table>

483.xalancbmk has a baseline of 566,342 gadgets.
Preserves the security properties of NOP insertion.
Profile-guided software diversification has a **minimal impact on performance**.

Attacks against a diverse program have a **high chance of failure**.
Questions?

Thank You!