Dynamic Binary Translator
&
Randomized Instruction-Set Emulation
Introduction

- Dynamic Binary Translation (Software Dynamic Translation) is the alteration of a running program to achieve a specific objective.
  - Shade [Cmelik and Keppel 1994]
  - Embra [Witchel and Rosenblum 1996]
  - Dynamo [Bala et al. 2000]
  - Strata [Kevin Scott and Jack Davidson 2002]

- virtualize aspects of the host execution environment by interposing a layer of software between program and CPU.
STRATA

SoC Optimizations and Restructuring
SoC Optimizations and Restructuring
Performance of Strata

Figure 2. Performance of Strata-based system call monitor.
In 2004, the Department of Homeland Security reported 323 buffer overflow vulnerabilities.

The most common attack: code-injection attack.
RISE

- Randomized Instruction-Set Emulation (RISE)
- A theoretically strong approach to defending against any type of code-injection attack
- Create and use a process-specific instruction set created by a randomization algorithm
- Code injected by attacker will be invalid
RISE using STRATA

Original Executable → Randomizer → Randomized Code

Secret Key

Derandomizer → Original Code → Processor Core

Runtime
RISE Defuses Injected Code

Diagram:

- Original Executable
- Randomizer
- Randomized Code
- Malicious Code
- Secret Key
- Derandomizer
- Original Code
- Random Bits
- Processor Core
- Runtime
Performance of RISE using STRATA
Overhead of RISE using STRATA

Table 2: Disk image overhead (Kilobytes).

<table>
<thead>
<tr>
<th></th>
<th>BIND</th>
<th>Apache</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Native</td>
<td>SDT-only</td>
</tr>
<tr>
<td>Disk image</td>
<td>1811</td>
<td>1872</td>
</tr>
<tr>
<td>text</td>
<td>1786</td>
<td>1838</td>
</tr>
<tr>
<td>data</td>
<td>23</td>
<td>28</td>
</tr>
<tr>
<td>bss</td>
<td>13</td>
<td>32</td>
</tr>
</tbody>
</table>

SoC Optimizations and Restructuring
Future work

- Dynamic Binary Translation on mobile devices
- Secure execution on mobile devices
- Minimize disk overhead of RISE on mobile devices
- Maximize performance of RISE on mobile devices