Introduction

- Some code protection technologies are implemented on major compilers, and they are widespread.
- But it is unknown whether they are applied and worked correctly.

We surveyed:
- the application situations of 4 code protection technologies on GCC (RELRO, SSP, PIE, Automatic Fortification)
- how the situations have been changed by analyzing binaries on each 3 versions of 3 major linux distributions

Our Analysis

Target distributions

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Version</th>
<th>5.0</th>
<th>6.0</th>
<th>7.3</th>
<th>12.1</th>
<th>13.2</th>
<th>13.3</th>
<th>14.04</th>
<th>14.04</th>
</tr>
</thead>
<tbody>
<tr>
<td>CentOS 5.0</td>
<td>5.0</td>
<td>258</td>
<td>123</td>
<td>58</td>
<td>124</td>
<td>125</td>
<td>123</td>
<td>124</td>
<td>124</td>
</tr>
<tr>
<td>CentOS 6.0</td>
<td>6.0</td>
<td>237</td>
<td>117</td>
<td>179</td>
<td>124</td>
<td>125</td>
<td>123</td>
<td>124</td>
<td>124</td>
</tr>
<tr>
<td>CentOS 7.3</td>
<td>7.3</td>
<td>162</td>
<td>117</td>
<td>58</td>
<td>124</td>
<td>125</td>
<td>123</td>
<td>124</td>
<td>124</td>
</tr>
<tr>
<td>openSUSE</td>
<td>12.1</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>openSUSE</td>
<td>13.2</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>openSUSE</td>
<td>14.04</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>12.04</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>13.04</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>13.1</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>14.04</td>
<td>28</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>24</td>
</tr>
</tbody>
</table>

Result1: application situations of 4 code protection technologies

RELRO

- Full RELRO was applied to 25% of binaries in CentOS 7.3, and this is the highest proportion.

SSP

- the mechanism which sets a canary value on the saved ebp in the stack frame
- it detects buffer overflow if the canary value was overwritten

PIE

- the mechanism which generates position-independent executables
- If PIE and ASLR are applied to a binary, the base address of text area in the binary can be also randomized.

Automatic Fortification

the mechanism which replaces library functions that can cause buffer overflow to safe ones

Result2: transitions of applications

We surveyed how the applications have been changed as each distribution's version upgrade

Conclusion

- The application situations are different on each distribution.
- There are cases code protection technologies were disabled on later version though they had been enabled on previous version.
- The code protection technologies are not always applied while the binaries were built with their compile option.

Future Works

We will:
- analyze the binaries in 64bit Linux distributions
- clarify the difference of these code protection technologies' situations between 32bit and 64bit