An Empirical Study of an Advanced Kernel Tailoring Framework

Junghwan Kang / ultract@nsr.re.kr
Contents

• Introduction
• Review
  – My Previous Work @ OSSummit NA 2017
• Advanced Features
• Demo
• Evaluation
• Discussion
• Conclusion
Introduction
Introduction

• Motivation of My Work
  – Minimize the Attack Surface of the Linux Kernel
  – Automate the Kernel Configuration
  – Produce a Stable Tailored Linux Kernel

More than 12,000 Options (Has Prompts)
Introduction

• 1st Approach – Undertaker-Tailor
  – Uses Ftrace (Kernel Function Tracer)
  – Formulates Dependency Relationships of Kernel Configuration Options
  – Uses SAT Solver
Introduction

• 1st Approach – Undertaker-Tailor
  – Great! However, tailored kernels often fail to run
    • Failed to Boot Up 😞
    • Found Some Bugs & Fixed them
Introduction

• 2nd Approach – Localmodconfig
  – Command For Configuring the Kernel
  – Very Useful to reduce the # of Kernel Modules
    • Mostly Drivers Removed
    • Still Unnecessary Configuration Options…

```
"make localmodconf" Create a config based on current config and loaded modules (lsmod). Disables any module
option that is not needed for the loaded modules.

To create a localmodconf for another machine, store the lsmod of that machine into a file
and pass it in as a LSMOD parameter.

target$ lsmod > /tmp/mylsmod
target$ scp /tmp/mylsmod host:/tmp
host$ make LSMOD=/tmp/mylsmod localmodconf

The above also works when cross compiling.
```
3rd Approach – Kernel Tailoring Framework

- Uses the Undertaker-Tailor with Some Fixes
- Automates Kernel Tailoring Workflow
- Checks Tailored Kernels if it includes essential configurations, by looking into
  - Boot State
  - System Logs, Kernel Modules
  - Peripherals (Keyboard, Mouse, Network, etc.)

- **Got a Working Tailored Kernel!**
  - But, Not Boot Up Sometimes…
  - *I Needed Next Approaches for an Advanced Kernel Tailoring*…
Introduction

- 4th Approach – **Advanced Kernel Tailoring Framework**
  - Improves a Stability
    - Enables tailoring with fine-grained configuration options (Not Grouping)
    - Includes Various Conditions to Verify Tailored Kernels
      - Shows Relationships between Configuration Options & the Conditions
  - Supports for Other Linux Distributions
    - Debian
    - Ubuntu
    - ...
  - Measures Performance of between a Tailored & Original Kernel
    - Lmbench (Micro-benchmark for Linux/UNIX/POSIX)
    - Phoronix-Test-Suite (Benchmark for Linux & Other Operating Systems)
Review - My Previous Work

※ Details of My Previous Work are in a Presentation File at OSSummit NA 2017 😊
(http://sched.co/BCsG)
Review – My Previous Work

• Design
  – Architecture
Review – My Previous Work

• Design
  – Workflow

- Prerequisite
  - Select Linux Distribution
    - Debian
    - Ubuntu
    - ...
  - Identify Use Cases
    - #1 Default Apps
    - #2 Browsing
    - #3 ETC

- Automatic Kernel Tailoring
  - Trace Kernel Features
  - Select Configuration Options

- Complete !!
  - Undertaker-tailor
  - Build Tailored Kernel
  - Verify Tailored Kernel

Repeat Verification Tests For All Configuration Options

Stable Tailored Kernel
Review – My Previous Work

• Design
  – Kernel Configurer
    • Selects Configuration Options
      – Replenishes a Shortage of the Kernel Configuration by the Undertaker-Tailor
    • Groups Configuration Options For Tests
      – Reduces the number of Tests for Tailored Kernels (Configure & Build & Verify a Tailored Kernel)
Review – My Previous Work

• Design
  – Kernel Configurer

- Candidates of Configuration Options
  - .config by undertaker-tailor
  - .config by localmodconfig

Select & Group the Configuration Options

```plaintext
# Grouping example :)
# Merge & Sort each groups of configuration

CONFDIRKMAP PND, COMPAT_BITS_MIN=0  # ARCH group
CONFDIRKMAP PND, COMPAT_BITS_MAX=16  #
CONFDIRKMAP PND, COMPAT_STATE=y  # NEED group
CONFDIRKMAP PND, COMPAT_LENGTH=y  #
CONFDIRKMAP PND, COMPAT_LEN=y  # GENERIC Group
CONFDIRKMAP PND, DMA=y
CONFDIRKMAP PND, DMA=y
```
Review – My Previous Work

• Design
  – Kernel Configurer

by Kernel Tailoring Framework

.config by undertaker-tailor

ARCH X86 NET ACPI

≥
Review – My Previous Work

• Implementation
Review – My Previous Work

- Implementation
  - Multi-VMs for a Verification
    - # of Maximum VMs: 5
Review – My Previous Work

• Evaluation
  – Elapsed time: About 5 Hours (# of Verification VMs: 5)
  – Kernel Image Size: About $\frac{1}{2}$ ↓
  – # of Kernel Modules: $\frac{110}{3269} \approx 3.4\%$
  – Got a Working Tailored Linux Kernel!!
    • But, I found out that the Kernel doesn’t boot up sometimes 😞
Advanced Features
Advanced Features

• Fine-grained Kernel Tailoring
  – Not Grouping
  • Tailoring Each Kernel Configuration Option
  • Relationship with Conditions for a Verification

Candidates of Configuration Options
(# of Candidates: 650
For Gooroom)
Advanced Features

- Fine-grained Kernel Tailoring
  - Only Selectable Configuration Options
    - Uses a Model File by the undertaker-kconfigdump
      - “HasPrompts”
• Fine-grained Kernel Tailoring
  – Dependency between Configuration Options
    • Counts how other configuration options “Depend on” a particular configuration option (reverse dependency)
    • Tailoring in the order of degree of the dependency from lowest to highest
Advanced Features

- Fine-grained Kernel Tailoring
  - Randomize Configuration Options
  - Minimize Dependency between Candidates of Configuration Options

**Candidates of Configuration Options**

Test VM #1
- Necessary To Boot up
- CONFIG_AAA
- CONFIG_BBB
- CONFIG_CCC

Dependency Relationship

Test VM #2
- CONFIG_AAA
- CONFIG_BBB
- CONFIG_CCC

Test VM #3
- CONFIG_AAA
- CONFIG_BBB
- CONFIG_CCC

**Example**

Test VM #1
- Successful to Boot up 😊

Test VM #2
- Successful to Boot up 😊

Test VM #3
- Fail to Boot up!! 😞
Advanced Features

- Various conditions for a verification
  - Display
    - Resolution and Dimension
  - Network
  - Peripherals
    - Keyboard and Mouse
  - Security
    - Protection Mechanisms for the Linux Kernel
  - File Systems
  - Etc
    - Power State
    - System Logs (Journalctl)
    - Running Applications
Advanced Features

• Various conditions for a verification - Display
  – Resolution & Dimension
  • phoronix-test-suite system-info → Compare the Before and After
  • xdpyinfo or xrandr
    → Compare the Before and After
Advanced Features

- Various Conditions for a Verification
  - Network
    - IPv4
      - `/bin/ip a | grep "192.168."`
    - IPv6
      - `/bin/ip a | grep "inet6 [a-z0-9]+::[a-z0-9:]+"`
      - `dmesg or journalctl | grep "Failed to insert module 'ipv6'"
  - Ping the Gateway
Advanced Features

• Various Conditions for a Verification - Peripherals
  – Keyboard & Mouse Device
    • /dev/input & udevadm(udev management tool) info
      – ID_INPUT_KEYBOARD, ID_INPUT_MOUSE
    • lsmod | grep 'psmouse'
Advanced Features

- Various Conditions for a Verification
  - Security Mechanisms for the Linux Kernel
    - `checksec` → Compare the Before and After
      - Check Kernel Protection mechanisms.
        E.g. Restrict `/dev/mem`, ASLR, GCC stack protector support…
        (https://github.com/slimm609/checksec.sh)
    - `phoronix-test-suite` info → Compare the Before and After
Advanced Features

• Various Conditions for a Verification
  – File Systems
    • mount → Compare the Before and After
    – Filters Plugable(Dynamic) File Systems
      E.g. grep -v "binfmt_misc\|iso9660\|fusectl"
      ※ Verifiable by Other Conditions or Use-cases
Advanced Features

• Various Conditions for a Verification
  – Etc
    • Power State (Suspend & Hibernation)
      – grep "suspend" | /sys/power/disk
      – grep "disk" | /sys/power/state
      ※ https://www.kernel.org/doc/Documentation/power/
    • Journalctl → Compare the Before and After
    • phoronix-test-suite info → Compare the Before and After
    • Running Applications
Advanced Features

• Supports for Other Linux Distributions
  – Gooroom (Our Custom Desktop Linux 😊)
    • Beta 1.0 64bit, Kernel Ver 4.9
    • Xfce Desktop Environment, Lightdm
  – Debian
    • Stretch (9.4) 64bit Desktop, Kernel Ver 4.9
    • Gnome Desktop Environment, Lightdm
  – Ubuntu
    • Bionic Beaver (18.04) 64bit Desktop, Kernel Ver 4.15
    • Gnome Desktop Environment, Lightdm
Demo

※ This Video: https://youtu.be/fHceA4asiXU
Previous Work: https://youtu.be/fnnCn-Bxjnw
Evaluation
Evaluation

• Total Elapsed Time
  – Gooroom Beta 1.0
    • 7 Hours 55 Minutes
      – # of Verification VMs: 8
      – # of Candidates of Configuration Options: 650
  – Debian 9.4
    • 9 Hours 20 Minutes
      – # of Verification VMs: 8
      – # of Candidates of Configuration Options: 628
  – Ubuntu 18.04
    • 14 Hours 45 Minutes
      – # of Verification VMs: 8
      – # of Candidates of Configuration Options: 997
Evaluation

• Kernel Image & Initial Ramdisk & Kernel Modules
  – Gooroom Beta 1.0
    • Kernel Image Size
      – Tailored: 14,399,796 Bytes (≈ 72%)
      – Original: 20,090,752 Bytes, ※ Decompressed by extract-vmlinux
    • Initial Ramdisk Size
      – Tailored: 6,672,465 Bytes (≈ 20%)
      – Original: 34,078,719 Bytes
    • The Size of Kernel Modules
      – Tailored: 6,650,050 Bytes (≈ 0.04%), # of .ko: 91 (≈ 0.03%)
      – Original: 186,697,093 Bytes, # of .ko: 3,387
Evaluation

- Kernel Image & Initial Ramdisk & Kernel Modules
  - Debian 9.4
    - Kernel Image Size
      - Tailored: 12,289,612 Bytes (≈ 61%)
      - Original: 20,161,244 Bytes, ※ Decompressed by extract-vmlinux
    - Initial Ramdisk Size
      - Tailored: 5,910,123 Bytes (≈ 30%)
      - Original: 19,582,713 Bytes
    - The Size of Kernel Modules
      - Tailored: 5,026,255 Bytes (≈ 0.03%), # of .ko: 91 (≈ 0.03%)
      - Original: 189,458,941 Bytes, # of .ko: 3,387
Evaluation

• Kernel Image & Initial Ramdisk & Kernel Modules
  – Ubuntu 18.04
    • Kernel Image Size
      – Tailored : 20,951,272 Bytes (≈ 22%)
      – Original : 94,147,992 Bytes, ※ Decompressed by extract-vmlinux
    • Initial Ramdisk Size
      – Tailored : 12,377,995 Bytes (≈ 22%)
      – Original : 53,935,618 Bytes
    • The Size of Kernel Module
      – Tailored : 5,772,651 Bytes (≈ 0.02%), # of .ko : 64 (≈ 0.01%)
      – Original : 236,401,113 Bytes , # of .ko : 5,161
Evaluation

- **Kernel Configuration File**
  - Gooroom Beta 1.0

<table>
<thead>
<tr>
<th></th>
<th>Original <code>.config</code></th>
<th>1st Tailored <code>.config by Undertaker-Tailor</code></th>
<th>Localmodconfig <code>.config</code></th>
<th>Final Tailored <code>.config</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (=y)</td>
<td>1785</td>
<td>359</td>
<td>1194</td>
<td>565</td>
</tr>
<tr>
<td>Module (=m)</td>
<td>3189</td>
<td>75</td>
<td>101</td>
<td>90</td>
</tr>
<tr>
<td>Disable (not set)</td>
<td>1601</td>
<td>1377</td>
<td>2329</td>
<td>1608</td>
</tr>
<tr>
<td>Etc (String, Number)</td>
<td>139</td>
<td>47</td>
<td>83</td>
<td>65</td>
</tr>
<tr>
<td>Total (Enable + Module + Etc)</td>
<td>5113</td>
<td>481</td>
<td>1378</td>
<td>720</td>
</tr>
</tbody>
</table>

- 1785 → 565 (≈ 32%)
- 3189 → 90 (≈ 3%)
- 5113 → 720 (≈ 14%)
Evaluation

- Kernel Configuration File
  - Gooroom Beta 1.0

<table>
<thead>
<tr>
<th>Sub-Directory of Linux Kernel</th>
<th>Original .config</th>
<th>1st Tailored .config by Undertaker-Tailor</th>
<th>Localmodconfig .config</th>
<th>Final Tailored .config</th>
</tr>
</thead>
<tbody>
<tr>
<td>arch</td>
<td>271</td>
<td>149</td>
<td>256</td>
<td>189</td>
</tr>
<tr>
<td>block</td>
<td>32</td>
<td>8</td>
<td>32</td>
<td>12</td>
</tr>
<tr>
<td>crypto</td>
<td>130</td>
<td>35</td>
<td>54</td>
<td>47</td>
</tr>
<tr>
<td>drivers</td>
<td>3109</td>
<td>85</td>
<td>473</td>
<td>140</td>
</tr>
<tr>
<td>fs</td>
<td>261</td>
<td>22</td>
<td>58</td>
<td>44</td>
</tr>
<tr>
<td>init</td>
<td>126</td>
<td>48</td>
<td>125</td>
<td>85</td>
</tr>
<tr>
<td>kernel</td>
<td>93</td>
<td>47</td>
<td>89</td>
<td>57</td>
</tr>
<tr>
<td>lib</td>
<td>127</td>
<td>40</td>
<td>99</td>
<td>62</td>
</tr>
<tr>
<td>mm</td>
<td>52</td>
<td>18</td>
<td>47</td>
<td>26</td>
</tr>
<tr>
<td>net</td>
<td>640</td>
<td>16</td>
<td>73</td>
<td>29</td>
</tr>
<tr>
<td>security</td>
<td>52</td>
<td>8</td>
<td>52</td>
<td>19</td>
</tr>
<tr>
<td>sound</td>
<td>214</td>
<td>14</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>usr</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>virt</td>
<td>14</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>5128</td>
<td>491</td>
<td>1391</td>
<td>732</td>
</tr>
</tbody>
</table>

3019 → 140 (≈ 5%)
640 → 29 (≈ 5%)
214 → 19 (≈ 9%)
## Evaluation

- **Kernel Configuration File**
  - Debian 9.4

<table>
<thead>
<tr>
<th></th>
<th>Original .config</th>
<th>1st Tailored .config by Undertaker Tailor</th>
<th>Localmodconfig .config</th>
<th>Final_Tailored .config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (=y)</td>
<td>1761</td>
<td>364</td>
<td>1170</td>
<td>565</td>
</tr>
<tr>
<td>Module (=m)</td>
<td>3202</td>
<td>75</td>
<td>103</td>
<td>94</td>
</tr>
<tr>
<td>Disable (not set)</td>
<td>1602</td>
<td>1391</td>
<td>2335</td>
<td>1605</td>
</tr>
<tr>
<td>Etc (String, Number)</td>
<td>139</td>
<td>47</td>
<td>83</td>
<td>65</td>
</tr>
<tr>
<td>Total (Enable + Module + Etc)</td>
<td>5102</td>
<td>486</td>
<td>1356</td>
<td>724</td>
</tr>
</tbody>
</table>

1761 → 565 (≈ 32%)  
3202 → 94 (≈ 3%)  
5102 → 724 (≈ 14%)
## Evaluation

- **Kernel Configuration File**
  - Debian 9.4

<table>
<thead>
<tr>
<th>Sub-Directory of Linux Kernel</th>
<th>Original .config</th>
<th>1st Tailored .config by Undertaker-Tailor</th>
<th>Localmodconfig .config</th>
<th>Final Tailored .config</th>
</tr>
</thead>
<tbody>
<tr>
<td>arch</td>
<td>273</td>
<td>149</td>
<td>258</td>
<td>190</td>
</tr>
<tr>
<td>block</td>
<td>32</td>
<td>8</td>
<td>32</td>
<td>12</td>
</tr>
<tr>
<td>crypto</td>
<td>127</td>
<td>35</td>
<td>49</td>
<td>47</td>
</tr>
<tr>
<td>drivers</td>
<td>3111</td>
<td>92</td>
<td>474</td>
<td>147</td>
</tr>
<tr>
<td>fs</td>
<td>261</td>
<td>21</td>
<td>55</td>
<td>44</td>
</tr>
<tr>
<td>init</td>
<td>126</td>
<td>48</td>
<td>124</td>
<td>84</td>
</tr>
<tr>
<td>kernel</td>
<td>93</td>
<td>47</td>
<td>89</td>
<td>55</td>
</tr>
<tr>
<td>lib</td>
<td>126</td>
<td>40</td>
<td>94</td>
<td>63</td>
</tr>
<tr>
<td>mm</td>
<td>52</td>
<td>18</td>
<td>47</td>
<td>26</td>
</tr>
<tr>
<td>net</td>
<td>639</td>
<td>16</td>
<td>72</td>
<td>28</td>
</tr>
<tr>
<td>security</td>
<td>42</td>
<td>8</td>
<td>42</td>
<td>17</td>
</tr>
<tr>
<td>sound</td>
<td>214</td>
<td>14</td>
<td>25</td>
<td>19</td>
</tr>
<tr>
<td>user</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>virt</td>
<td>14</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5117</strong></td>
<td><strong>497</strong></td>
<td><strong>1369</strong></td>
<td><strong>736</strong></td>
</tr>
</tbody>
</table>

3111 → 147 (≈ 5%)

639 → 28 (≈ 4%)

214 → 19 (≈ 9%)
Evaluation

- Kernel Configuration File
  - Ubuntu 18.04

<table>
<thead>
<tr>
<th></th>
<th>Original <code>.config</code></th>
<th>1st Tailored <code>.config</code> by Undertaker Tailor</th>
<th>Localmodconfig <code>.config</code></th>
<th>Final Tailored <code>.config</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (=y)</td>
<td>2381</td>
<td>338</td>
<td>1596</td>
<td>634</td>
</tr>
<tr>
<td>Module (=m)</td>
<td>4937</td>
<td>45</td>
<td>74</td>
<td>55</td>
</tr>
<tr>
<td>Disable (not set)</td>
<td>749</td>
<td>1423</td>
<td>2630</td>
<td>1620</td>
</tr>
<tr>
<td>Etc (String, Number)</td>
<td>173</td>
<td>45</td>
<td>105</td>
<td>69</td>
</tr>
<tr>
<td>Total (Enable + Module + Etc)</td>
<td>7491</td>
<td>428</td>
<td>1775</td>
<td>758</td>
</tr>
</tbody>
</table>

2381 → 634 (≈ 23%)
4937 → 55 (≈ 1%)
7491 → 758 (≈ 10%)
Evaluation

- Kernel Configuration File
  - Ubuntu 18.04

<table>
<thead>
<tr>
<th>Sub-Directory of Linux Kernel</th>
<th>Original .config</th>
<th>1st Tailored .config by Undertaker Tailor</th>
<th>Localmodconfig .config</th>
<th>Final Tailored .config</th>
</tr>
</thead>
<tbody>
<tr>
<td>arch</td>
<td>315</td>
<td>157</td>
<td>304</td>
<td>211</td>
</tr>
<tr>
<td>block</td>
<td>45</td>
<td>8</td>
<td>40</td>
<td>15</td>
</tr>
<tr>
<td>cmd</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>crypto</td>
<td>151</td>
<td>4</td>
<td>65</td>
<td>53</td>
</tr>
<tr>
<td>drivers</td>
<td>5085</td>
<td>74</td>
<td>681</td>
<td>133</td>
</tr>
<tr>
<td>fs</td>
<td>280</td>
<td>7</td>
<td>75</td>
<td>41</td>
</tr>
<tr>
<td>init</td>
<td>141</td>
<td>39</td>
<td>140</td>
<td>83</td>
</tr>
<tr>
<td>kernel</td>
<td>118</td>
<td>55</td>
<td>111</td>
<td>66</td>
</tr>
<tr>
<td>lib</td>
<td>156</td>
<td>38</td>
<td>116</td>
<td>66</td>
</tr>
<tr>
<td>mm</td>
<td>67</td>
<td>21</td>
<td>64</td>
<td>28</td>
</tr>
<tr>
<td>boot</td>
<td>679</td>
<td>16</td>
<td>64</td>
<td>33</td>
</tr>
<tr>
<td>security</td>
<td>67</td>
<td>7</td>
<td>65</td>
<td>20</td>
</tr>
<tr>
<td>sound</td>
<td>377</td>
<td>12</td>
<td>30</td>
<td>19</td>
</tr>
<tr>
<td>ubuntu</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usr</td>
<td>7</td>
<td>0</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>virt</td>
<td>14</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>7513</td>
<td>441</td>
<td>1793</td>
<td>773</td>
</tr>
</tbody>
</table>

- New Directories

- 5085 → 133 (≈ 3%)
- 679 → 33 (≈ 5%)
- 377 → 19 (≈ 5%)
Evaluation

- Verification Log - Gooroom Beta 1.0

[ Boot Up ]
- BINfmt_script
- DEVTMPFS
- EPOLL
- FILE_LOCKING
- FUTEX
- INOTIFY_USER
- MULTIUSER
- RD_GZIP
- SERIAL_8250
- SHMEM
- SIGNALFD
- SYSFS
- TIMERFD
- TMPFS
- TTY
- UNIX
- UNIX98_PTYS
- VT

[ Phoronix-test-suite ]
- DMI → Motherboard & BIOS Information
- DMIID → Motherboard & BIOS Information
- DRM_LEGACY → Graphics
- IOSCHED_CFQ → Disk Scheduler - CFQ(Before), NOOP(After)
- PACKET → No Internet Connectivity
- PAGE_TABLE_ISOLATION → Security - KPTI
- RETPOLINE → Security - Full generic retpoline Protection

[ Journalctl Log ]
- ECRYPT_FS → Failed to find module 'ecryptfs'
- IPV6 → device (enp2s1): addrconf6: failed to start neighbor discovery ...
- NAMESPACES → Failed to start Hostname Service ...
- PACKET → (Socket Filtering) are enabled in your kernel ...
- PARPORT → Failed to find module 'lp', 'parport_pc', 'ppdev'
- PRINTER → Failed to find module 'lp'
- RETPOLINE → Spectre V2 : kernel not compiled with retpoline;
- TMPFS_POSIX_ACL → Failed to apply ACL on /dev/dri/card0: Operation not supported ...

Evaluation

- Verification Log - Gooroom Beta 1.0


<table>
<thead>
<tr>
<th>[ Checksec ]</th>
<th>[ Network ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT → SELinux Enable</td>
<td>IPv6 → IPv6 Address Not Set</td>
</tr>
<tr>
<td>CC_STACKPROTECTOR_STRONG → GCC stack protector support</td>
<td>NAMESPACES → IPv4 Address Not Set</td>
</tr>
<tr>
<td>RANDOMIZE_BASE → Address space layout randomization</td>
<td>PACKET → IPv4 Address Not Set, Ping to Gateway Failed</td>
</tr>
<tr>
<td>RELOCATABLE → Address space layout randomization</td>
<td>SECURITY → SELinux Enable</td>
</tr>
<tr>
<td>SECURITY → SELinux Enable</td>
<td>SECURITY_SELINUX → SELinux Enable</td>
</tr>
<tr>
<td>STRICT_DEVMEM → Restrict /dev/mem access</td>
<td>STRICT_DEVMEM → Restrict /dev/mem access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[ File Systems ]</th>
<th>[ Power State ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT_SECURITY_SMACK → smackfs</td>
<td>HIBERNATION → /sys/power/disk, /sys/power/state</td>
</tr>
<tr>
<td>NAMESPACES → hugetlbfs</td>
<td>SUSPEND → /sys/power/disk</td>
</tr>
<tr>
<td>SECURITY → smackfs</td>
<td>SWAP → /sys/power/disk, /sys/power/state</td>
</tr>
<tr>
<td>SECURITY_SMACK → smackfs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[ Peripherals ]</th>
<th>[ Kernel Module ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>INPUT_KEYBOARD</td>
<td>MODULE_UNLOAD → Kernel Module Loading Failed</td>
</tr>
<tr>
<td>INPUT_MOUSE</td>
<td></td>
</tr>
<tr>
<td>KEYBOARD_ATKBD</td>
<td></td>
</tr>
<tr>
<td>MOUSE_PS2</td>
<td></td>
</tr>
</tbody>
</table>

| [ Applications ] |
|-----------------
| ADVISE_SYSCALLS → Browser Not Working - Fatal Error |
| NAMESPACES → Pulse Audio Not Working |
**Evaluation**

- **Verification Log - Debian 9.4**
  
  [ Boot Up ]
  - BINFORM_SCRIPT
  - DEVTFMPFS
  - EPOOL
  - EXT4_USE_FOR_EXT2
  - FILE_LOCKING
  - FUTEX
  - INOTIFY_USER
  - MULTIUSER
  - RD_GZIP
  - SHMEM
  - SIGNALFD
  - SYFS
  - TIMERFD
  - TMPFS
  - TTY
  - UNIX
  - UNIX98_PTYS
  - VT

  [ Phoronix-test-suite ]
  - DMI → Motherboard & BIOS Information
  - DMID → Motherboard & BIOS Information
  - IOSCHED_CFQ → Disk Scheduler - CFQ(Before), NOOP(After)
  - NET_VENDOR_REALTEK → No Internet Connectivity
  - PACKET → No Internet Connectivity
  - PAGE_TABLE_ISOLATION → Security - KPTI
  - RD_LZ4 → No Internet Connectivity
  - RETPOLINE → Security - Full generic retpoline Protection

  [ Journalctl Log ]
  - IPV6 → device (enp2s1): addrconf6: failed to start neighbor discovery ...
  - NAMESPACES → Failed to start Hostname Service ...
  - NET_VENDOR_REALTEK → setsockopt(udp, IP_ADD_MEMBERSHIP)(0.0.0.0): No such device
  - PACKET → (Socket Filtering) are enabled in your kernel ...
  - PARPORT → Failed to find module 'lp', 'parport_pc', 'ppdev'
  - PRINTER → Failed to find module 'lp'
  - RD_LZ4 → setsockopt(udp, IP_ADD_MEMBERSHIP)(0.0.0.0): No such device
  - RETPOLINE → Spectre V2 : kernel not compiled with retpoline; no mitigation available!
  - SERIAL_8250 → bad device “/dev/ttyS0” given
  - TMPFS_POSIX_ACL → Failed to apply ACL on /dev/dri/card0: Operation not supported ...
  - VT_CONSOLE → /dev/ttyS0: not a tty

Evaluation

- Verification Log - Debian 9.4

  **[ Checksec ]**
  - AUDIT → SELinux Enable
  - CC_STACKPROTECTOR_STRONG → GCC stack protector support
  - RANDOMIZE_BASE → Address space layout randomization
  - RELOCATABLE → Address space layout randomization
  - SECURITY → SELinux Enable
  - SECURITY_SELINUX → SELinux Enable
  - SLAB_FREELIST_RANDOM → SLAB freelist randomization
  - STRICT_DEVMEM → Restrict /dev/mem access
  - VMAP_STACK → Virtually-mapped kernel stack

  **[ File Systems ]**
  - NAMESPACES → hugetlbfs

  **[ Peripherals ]**
  - INPUT_KEYBOARD
  - INPUT_MOUSE
  - KEYBOARD_ATKBD
  - MOUSE_PS2

  **[ Network ]**
  - IPV6 → IPv6 Address Not Set
  - NAMESPACES → IPv4 Address Not Set
  - PACKET → IPv4 Address Not Set, Ping to Gateway Failed

  **[ Power State ]**
  - HIBERNATION → /sys/power/disk, /sys/power/state
  - SWAP → /sys/power/disk, /sys/power/state

  **[ Kernel Module ]**
  - MODULE_UNLOAD → Kernel Module Loading Failed

  **[ Applications ]**
  - NAMESPACES → Pulse Audio Not Working
Evaluation

- Verification Log - Ubuntu 18.04 ∗ [Phoronix-test-suite]
  DMI → Motherboard & BIOS Information
  DMIID → Motherboard & BIOS Information
  IOSCHED_CFQ → Disk Scheduler - CFQ(Before), NOOP(After)
  PACKETT → No Internet Connectivity
  PAGE_TABLE_ISOLATION → Security - KPTI
  RETPOLINEE → Security - Full generic retpoline Protection
  VIRTIO_BALLOON → No Internet Connectivity

- [Boot Up]
  BINFORMT.Script
  DEVTMPFS
  EPOOL
  EXT4_FS
  FUTEX
  INOTIFY_USER
  MULTIUSER
  RD_GZIP
  SERIAL_8250
  SERIAL_8250_CONSOLE
  SHMEM
  SIGNALFD
  TIMERFD
  TMPFS
  UNIX
  UNIX98_PTYS
  VT

- [Journalctl Log]
  FILE_LOCKING → [autospawn] core-util: lock: Permission denied ...
  FUSE_FS → Failed to find module 'fuse'
  INPUT_EVDEV → cannot open input layer
  IPv6 → device (enp2s1): addrconf6: failed to start neighbor discovery ...
  OSF_PARTITION → Failed to mount Mount unit for core, revision 5145
  PACKET → (Socket Filtering) are enabled in your kernel ...
  PARPORT → Failed to find module 'lp', 'parport_pc', 'ppdev'
  PARPORT_PC Failed to find module 'parport_pc'
  POSIX_TIMERS Failed to call clock_adjtime(): Function not implemented
  PRINTER → Failed to find module 'lp'
  PRINTK → activation of module imklog failed
  RETPOLINE → Spectre V2 : kernel not compiled with retpoline; no mitigation available!
  SQUASHFS_XZ → squashfs: SQUASHFS error: Filesystem uses "xz" compression
  TMPFS_POSIX_ACL → Failed to apply ACL on /dev/dri/card0: Operation not supported ...

• **Verification Log - Ubuntu 18.04**


<table>
<thead>
<tr>
<th>[Checksec]</th>
<th>[Peripherals]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMAP_STACK → Virtually-mapped kernel stack</td>
<td>INPUT_KEYBOARD</td>
</tr>
<tr>
<td>HARDENED_USERCOPY → Hardened Usercopy</td>
<td>INPUT_MOUSE</td>
</tr>
<tr>
<td>SLAB_FREELIST_RANDOM → SLAB freelist randomization</td>
<td>KEYBOARD_ATKBD</td>
</tr>
<tr>
<td>CC_STACKPROTECTOR_STRONG → GCC stack protector support</td>
<td>MOUSE_PS2</td>
</tr>
<tr>
<td>RANDOMIZE_BASE → Address space layout randomization</td>
<td>[Network]</td>
</tr>
<tr>
<td>AUDIT → SELinux Enable</td>
<td>PACKET → IPv4 Address Not Set, Ping to Gateway Failed</td>
</tr>
<tr>
<td>SECURITY_SELINUX → SELinux Enable</td>
<td>IPV6 → IPv6 Address Not Set</td>
</tr>
<tr>
<td>SECURITY → SELinux Enable</td>
<td>[Power State]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[File Systems]</th>
<th>[Kernel Module]</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQUASHFS → squashfs</td>
<td>MODULE_UNLOAD → Kernel Module Loading Failed</td>
</tr>
<tr>
<td>SQUASHFS_XZ → squashfs</td>
<td>[Applications]</td>
</tr>
<tr>
<td>CONFIGFS_FS → configs</td>
<td>FILE_LOCKING → Pulse Audio Not Working</td>
</tr>
<tr>
<td>FUSE_FS → fuse.gvfsd-fuse</td>
<td></td>
</tr>
</tbody>
</table>
Evaluation

• Boot Up Time - Gooroom Beta 1.0
  – Tailored Kernel Image
    • Startup finished in 1.577s (kernel) + 2.930s (userspace) = 4.507s
    • Startup finished in 1.410s (kernel) + 2.928s (userspace) = 4.338s
    • Startup finished in 1.523s (kernel) + 3.241s (userspace) = 4.764s
  – Original Kernel Image
    • Startup finished in 2.695s (kernel) + 3.324s (userspace) = 6.020s
    • Startup finished in 2.839s (kernel) + 3.502s (userspace) = 6.341s
    • Startup finished in 2.836s (kernel) + 3.082s (userspace) = 5.918s
Evaluation

• **Boot Up Time - Debian 9.4**
  
  – **Tailored Kernel Image**
  
  • Startup finished in **1.416s** (kernel) + 6.751s (userspace) = **8.167s**
  • Startup finished in **1.450s** (kernel) + 6.649s (userspace) = **8.100s**
  • Startup finished in **1.442s** (kernel) + 6.598s (userspace) = **8.041s**

  – **Original Kernel Image**
  
  • Startup finished in **1.845s** (kernel) + 7.243s (userspace) = **9.089s**
  • Startup finished in **1.800s** (kernel) + 7.228s (userspace) = **9.029s**
  • Startup finished in **2.053s** (kernel) + 6.992s (userspace) = **9.046s**
• Boot Up Time - Ubuntu 18.04
  – Tailored Kernel Image  ※ system-analyze
    • Startup finished in 1.724s (kernel) + 5.912s (userspace) = 7.636s
    • Startup finished in 1.662s (kernel) + 4.319s (userspace) = 5.982s
    • Startup finished in 1.737s (kernel) + 5.660s (userspace) = 7.397s
  – Original Kernel Image
    • Startup finished in 3.931s (kernel) + 5.752s (userspace) = 9.683s
    • Startup finished in 3.980s (kernel) + 4.162s (userspace) = 8.143s
    • Startup finished in 3.894s (kernel) + 3.793s (userspace) = 7.688s
Evaluation

- Performance – Lmbench on the Gooroom
  - Most of the Test Results are Similar, except Some Test Items

<table>
<thead>
<tr>
<th>Processor, Processes - times in microseconds - smaller is better</th>
<th>Context switching - times in microseconds - smaller is better</th>
</tr>
</thead>
<tbody>
<tr>
<td>fork proc</td>
<td>exec proc</td>
</tr>
<tr>
<td>Tailored</td>
<td>353.29</td>
</tr>
<tr>
<td>Original</td>
<td>393.29</td>
</tr>
<tr>
<td>* Variation</td>
<td>-40.00</td>
</tr>
</tbody>
</table>

*Local* Communication bandwidths in MB/s - bigger is better

<table>
<thead>
<tr>
<th></th>
<th>TCP</th>
<th>File reread</th>
<th>Mmap reread</th>
<th>Bcopy(libc)</th>
<th>Bcopy(hand)</th>
<th>Mem read</th>
<th>Mem write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tailored</td>
<td>2301.14</td>
<td>3944.31</td>
<td>5484.96</td>
<td>4640.73</td>
<td>2479.63</td>
<td>5567.86</td>
<td>3444.14</td>
</tr>
<tr>
<td>Original</td>
<td>2196.57</td>
<td>3427.71</td>
<td>5348.34</td>
<td>4141.60</td>
<td>1784.83</td>
<td>5054.29</td>
<td>2547.57</td>
</tr>
<tr>
<td>* Variation</td>
<td>104.57</td>
<td>516.60</td>
<td>136.61</td>
<td>499.13</td>
<td>694.80</td>
<td>513.57</td>
<td>896.57</td>
</tr>
</tbody>
</table>
Evaluation

• Performance - Phoronix-test-suite on the Gooroom
  – I’ll show you the original results
Discussion
Discussion

- **Fine-grained Kernel Tailoring**
  - Considering the dependency & Randomizing the Configuration Options
    - Reduced a failure rate of the kernel tailoring empirically
      - The tailored Kernel is always working well 😊
    - The Relationship between conditions for a verification and the Configuration Options
      - Useful to make whitelist for the kernel tailoring
Discussion

• Fine-grained Kernel Tailoring
  – Takes longer than the previous method
    • More than 2 hours at the Gooroom
  – Reduces candidates of configuration options by selectable options (“HasPrompts”) thankfully
• The Performance of the Tailored Kernel
  – A little better performance
  – To understand the reason, I need an analysis about the results more…
• The Performance of Tailored Kernel
  – It is difficult to collect configuration options about the performance by undertaker-tailor & tailoring framework
  – The Configuration Options need to be added by hand
    • I refer to the linux performance and tuning guidelines
    • I added what the configuration options are in the original .config already
Discussion

- Conditions for the Verification
  - The conditions are found out heuristically
    - Trial and error
    - Comparing the before and after
  - H/W Spec, Drivers & Modules, Applications, Etc
  - It need to be formalize and organize
  - *The more conditions are added, the more configuration options are gathered…*
Discussion

• Desktop Manager Issues for the Verification
  – Xfce or Lightdm is better than Gnome or Gdm
    • A vm using Gnome is slow to be revert and play
    • Gdm service can’t be restarted properly for the use-cases and the verification
  – xfce4-terminal and gnome-terminal
    • They have different options to execute use-cases and the Verification scripts
I have troubles to make Kconfig model files on the Ubuntu

- undertaker-kconfigdUMP can’t handle “imply” attribute of the kconfig

• “imply”(weak select) → “select”

Discussion

• The limitation of the Localmodconfig
  – It only includes configuration options of inserted modules via the insmod command
• The kernel tailoring is only for a virtual machine yet
  – I need another new approach for the physical machine
    • How to automate to trace kernel features and verify tailored kernels like the virtual machines ??
Conclusion
Conclusion

• We looked into the several approaches for the kernel tailoring
  – Undertaker-tailor
  – Localmodconfig
  – My Kernel tailoring framework
• Advanced features of the kernel tailoring framework
  – Fine-grained kernel tailoring
    • Enhanced Stability of a Tailored Kernel
    • Relation between Configuration Options & Various Verification Conditions
  – Supported for other linux distributions
    • Debian, Ubuntu
  – A little performance benefit
• Future work
  – Formalizing or organizing the Conditions for a Verification
  – Kernel tailoring toward the physical machine 😊
Questions?
(https://github.com/ultract/linux-kernel-tailoring-framework)