Combinatorial Testing, Cybersecurity, Cloud Computing

Raghu Kacker
Applied & Computational Mathematics Division
NIST Information Technology Lab
Testing for Assurance of Security

- Secure only until break in
- Assurance requires effective testing, different kinds, innovative
- Security Testing: static analysis, dynamic analysis
- Dynamic: Exercise for various possibilities: inputs, configuration
- Combinatorial t-way Testing (CT) can be used in innovative ways
CT with Support of Constraints

- Tests expressed in terms of parameters, discrete test values
- Mixed test values
- Support of constraints
- Variable strength taking relations into account
- Specific inclusions, exclusions
- Efficient generation of small test suite
- Requires knowledge of expected behaviour for each test
Applications explored

- Basic: testing input space and possible configurations
- Security vulnerability testing
- Testing concurrent systems
- Navigation of dynamic web structures
- Analysing system state-space coverage
- Detecting deadlocks for varying network configurations
- Testing Access Control Systems
Detecting Buffer Overflow vulnerabilities


- Buffer overflow vulnerabilities exploited by many security attacks to compromise critical data/control structures
- Statement L copies a string variable S into buffer B without space checking
- To detect this vulnerability
  1: L must be executed during a test execution
  2: When L is executed, B must be overrun. This typically happens when L is unexpectedly long or B is unexpectedly small, or both.
## Experiment: Number of tests

<table>
<thead>
<tr>
<th>Subject</th>
<th>Total</th>
<th>Min</th>
<th>Max</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ghttpd</td>
<td>191</td>
<td>3</td>
<td>36</td>
<td>27.3</td>
</tr>
<tr>
<td>Gzip</td>
<td>32</td>
<td>10</td>
<td>12</td>
<td>10.7</td>
</tr>
<tr>
<td>Hypermail</td>
<td>200</td>
<td>10</td>
<td>10</td>
<td>10.0</td>
</tr>
<tr>
<td>Nullhttpd</td>
<td>191</td>
<td>3</td>
<td>36</td>
<td>27.3</td>
</tr>
<tr>
<td>Pine (read)</td>
<td>89</td>
<td>3</td>
<td>8</td>
<td>6.4</td>
</tr>
<tr>
<td>Pine (write)</td>
<td>49</td>
<td>3</td>
<td>8</td>
<td>5.4</td>
</tr>
</tbody>
</table>

Total number of test cases, Min, Max, Avg number of tests per extreme value
**Experiment: Vulnerability Detection**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Detected</th>
<th>Reported</th>
<th>Missed</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ghttpd</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gzip</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Hypermail</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Nullhttpd</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Pine</td>
<td>7</td>
<td>7</td>
<td>LOI</td>
<td>LOI</td>
</tr>
</tbody>
</table>

LOI: Lack of information
Cloud Computing

- Main concerns: security, privacy, data integrity, availability
- Testing essential to overcome concerns
- Services: Software (SaaS), Platform (PaaS), Infrastructure (IaaS)
- How to test dynamically composed SaaS?
- How to test highly configurable PaaS?
- How to test highly configurable IaaS?
- How to utilize the cloud infrastructure to perform general software testing?
Contact Information

For further information contact:

Rick Kuhn, Computer Security
kuhn@nist.gov 301-975-3337

Raghu Kacker, Applied & Computational Mathematics
raghu.kacker@nist.gov 301-975-2109