Toward Credible IT Testing and Certification

Rick Kuhn
National Institute of Standards and Technology
kuhn@nist.gov
301-975-3337
Outline

• Need for software certification
• Measurement in physical science and information technology
• Laboratory accreditation and certification processes
• Current trends and implications
Software is Rarely Certified

• One of the stronger software warranties:

THIS SOFTWARE IS NOT DESIGNED, MANUFACTURED OR
INTENDED FOR USE OR RESALE FOR ON-LINE CONTROL
EQUIPMENT IN HAZARDOUS ENVIRONMENTS
REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE
OPERATION OF NUCLEAR FACILITIES, AIR TRAFFIC
CONTROL, AIRCRAFT NAVIGATION OR AIRCRAFT
COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES,
OR WEAPONS SYSTEMS, IN WHICH FAILURE OF THE
SOFTWARE COULD LEAD DIRECTLY TO DEATH,
PERSONAL INJURY, OR SEVERE PHYSICAL OR
ENVIRONMENT DAMAGE.
Examples

• U.S.S. Yorktown dead in the water because Windows NT failed to detect divide by zero error

• $500 Million Ariane 5 rocket explodes because guidance software failed to detect invalid parameter setting
Measurement in Physical Science

• Measurement requires:
  • Traceability to a *reference* - e.g., platinum-iridium meter bar (in years past)
  • Measurement *method* -
  • *Statement of uncertainty* - e.g., using statistical variances
Measurement in Information Technology

-- Examples --

• Traceability to a *reference* - e.g., IEEE standard for POSIX kernel, P1003.1

• Measurement *method* - standard test suite

• *Statement of uncertainty* - specific configuration and platform tested
Reference Data Example - Speech Database
Activity 1: Developer self declaration of conformity.
Activity 2: Conformance demonstrated by 3rd party evaluation only.
Activity 3: Conformance demonstrated by 3rd party evaluation and private sector validation.
Activity 4: Conformance demonstrated by 3rd party evaluation and U.S. Government validation.
NIST ITL Test Competency Centers

R&D / Technical Organizations
- CRADAs
- MOUs
- Consortia
- Workshops

Certificate Issuing Organizations
- Standards Development Organizations
- Trade/Industry Associations
- Government Organizations

Tests for:
- Pre-competitive Advanced IT
- Selected Standards (ANSI, IEEE, ISO, ITU)
- FIPS
- NSA/MISSI
- CC-based Evaluations
- Math & Stat Algorithms
- Special Purpose / Affinity Groups

ITL Test Competency Center

<table>
<thead>
<tr>
<th>Research Function</th>
<th>Operational Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>- test methods research</td>
<td></td>
</tr>
<tr>
<td>- test development/validation</td>
<td></td>
</tr>
<tr>
<td>- test tools development/validation</td>
<td></td>
</tr>
<tr>
<td>- specialized testing (e.g., telecom switches)</td>
<td></td>
</tr>
<tr>
<td>- assist sponsor w/ NVLAP use</td>
<td></td>
</tr>
<tr>
<td>- technical liaison between NVLAP &amp; sponsor</td>
<td></td>
</tr>
<tr>
<td>- technical qualifications of lab and lab personnel</td>
<td></td>
</tr>
<tr>
<td>- test interpretation/review</td>
<td></td>
</tr>
<tr>
<td>- liaison to int’l bodies (e.g., Test Control Board)</td>
<td></td>
</tr>
</tbody>
</table>

Test Center’s Role

Legend:
- CC: Common Criteria for security evaluation
- CRADA: Cooperative R&D Agreement
- FIPS: Federal Information Processing Standard
- IT: Information Technology
- MOU: Memorandum of Understanding
- NSA: National Security Agency
- NVLAP: National Voluntary Lab Accreditation Program

Accreditation Bodies (e.g., NVLAP)

Test Reports
# NIST ITL Test Information

## Conformance Tests and Reference Data

<table>
<thead>
<tr>
<th>Feature</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAVA Conformity Assessment and Diagnostics</td>
<td><a href="http://www.nist.gov/java_ca.htm">http://www.nist.gov/java_ca.htm</a></td>
</tr>
</tbody>
</table>

## Usability Tests

<table>
<thead>
<tr>
<th>Feature</th>
<th>URL</th>
</tr>
</thead>
</table>
# NIST ITL Test Information

## Performance Tests and Reference Data

<table>
<thead>
<tr>
<th>Test Category</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>REC Test Collections on CD-ROM</td>
<td><a href="http://trec.nist.gov/data/docs_eng.html">http://trec.nist.gov/data/docs_eng.html</a></td>
</tr>
<tr>
<td>Speech Processing Evaluations and Benchmark Tests</td>
<td><a href="http://www.nist.gov/speech/online.htm">http://www.nist.gov/speech/online.htm</a></td>
</tr>
<tr>
<td>Optical Character Recognition (OCR)</td>
<td><a href="http://www.nist.gov/itl/div894/894.03/ocr/ocr.html">http://www.nist.gov/itl/div894/894.03/ocr/ocr.html</a></td>
</tr>
<tr>
<td>Fingprint Classification / Matching</td>
<td><a href="http://www.nist.gov/itl/div894/894.03/fing/fing.html">http://www.nist.gov/itl/div894/894.03/fing/fing.html</a></td>
</tr>
<tr>
<td>Fingprint Test Data on CD-ROM</td>
<td><a href="http://www.nist.gov/itl/div894/894.03/databases/def/vip_dbases.html#finglist">http://www.nist.gov/itl/div894/894.03/databases/def/vip_dbases.html#finglist</a></td>
</tr>
<tr>
<td>Face Recognition</td>
<td><a href="http://www.nist.gov/itl/div894/894.03/face/face.html">http://www.nist.gov/itl/div894/894.03/face/face.html</a></td>
</tr>
<tr>
<td>Mugshot/Face Test Data on CD-ROM</td>
<td><a href="http://www.nist.gov/itl/div894/894.03/databases/def/vip_dbases.html#facelist">http://www.nist.gov/itl/div894/894.03/databases/def/vip_dbases.html#facelist</a></td>
</tr>
</tbody>
</table>
Laboratory Accreditation

Goal: Promote development of competitive market to:

• Increase availability of testing services
  – through third-party laboratories
  – market for testing encourages development of software testing industry

• Reduce cost
  – by increasing supply of testing services
National Voluntary Laboratory Accreditation Program

• Accredits third-party testing services, public and private labs

• Works with other national metrology institutes to establish criteria for mutual recognition of test results

• Accreditation in: instrument calibration, computers and electronics, dosimetry, environmental standards, fasteners and metals, product testing
National Voluntary Laboratory Accreditation Program

• Accredits third-party testing services, public and private labs

• NVLAP Computer/Electronics Group
  – Cryptographic Modules Testing
  – FCC Test Methods
  – GOSIP
  – MIL-STD-462 Test Methods
  – POSIX
NVLAP Computer/Electronics Group

- Cryptographic Modules - hardware and software
- FCC Test Methods
- GOSIP - OSI communications
- MIL-STD-462 Test Methods - electromagnetic emanations (TEMPEST)
- POSIX - IEEE operating system standard
Conformance Testing

• Reference: specification or standard
  – normally no access to source code
• Measurement method: test cases + test configuration + platform
• Uncertainty statement: accounts for limitation to tested platform, options, and test suite
Trends

• More standard component-based software
  – integrating components without source code
• Increased concern about liability
  – Y2K is just the beginning
• Increased demand for testing
  – need for consensus on prudent testing practices
  – need for precise definition of standards
Implications of Trends

• More standard component-based software
  – means usually no access to source code
• Increased concern about liability
  – means stronger assurance needed
• Increased demand for testing
  – means more efficient test methods needed
Bottom Line Implications

• Needs for rigorous assurance of standardized software
  – precise specifications of components
  – specification-based testing using
    • formal specifications
    • realistic fault models
    • statistical methods