Advances in Measuring the Security and Architectural Integrity of Mission-Critical Systems

Dr. Bill Curtis
Executive Director

CISQ
Consortium for IT Software Quality
Why Measure IT Applications?

Evaluate Application Quality with CISQ Measures

Six Digit Defects

now affect

Board of Directors
CEO, COO, CFO
Business VPs
Corporate Auditors
CIO

accountable for

Governance
Risk management
Risk measurement
Brand protection
Customer experience

Evaluate Application Quality with CISQ Measures

© 2017. Consortium for IT Software Quality
What is CISQ?

CISQ is chartered to define automatable measures of software size and quality that can be measured in the source code, and promote them to become Approved Specifications of the OMG®.

CISQ Sponsors

- Booz Allen Hamilton
- Cognizant
- Synopsys
- CAST
- Huawei

© 2017. Consortium for IT Software Quality
Reducing Operational Incidents & Costs

Study of structural quality measures and maintenance effort across 20 customers in a large global system integrator

TQI increase of .24 decreased corrective maintenance effort by 50%
Reducing Operational Losses

Large international investment bank
Business critical applications
Too many Insecure Apps

Industry segment

Security

© 2017. Consortium for IT Software Quality
CISQ/OMG Standards Process

CISQ Exec Forum

- Automated Function Points
- Reliability
- Performance Efficiency
- Security
- Maintainability

OMG

- Approved Measure Specifications

ISO Fasttrack

Deployment Workshops
• OMG Supported Specification for Automated Function Points

• Mirrors IFPUG counting guidelines, but automatable

• Specification developed by international team led by David Herron of David Consulting Group
Example architectural and coding violations composing the CISQ measures:

- SQL injection
- Cross-site scripting
- Buffer overflow
- Empty exception block
- Unreleased resources
- Circular dependency
- Expensive loop operation
- Un-indexed data access
- Unreleased memory
- Excessive coupling
- Dead code
- Hard-coded literals

CISQ Structural Quality Measures

<table>
<thead>
<tr>
<th>CISQ Quality Characteristic Measures</th>
<th>Example architectural and coding violations composing the CISQ measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>22 violations (Top 25 CWEs)</td>
</tr>
<tr>
<td>Reliability</td>
<td>29 violations</td>
</tr>
<tr>
<td>Performance Efficiency</td>
<td>15 violations</td>
</tr>
<tr>
<td>Maintainability</td>
<td>20 violations</td>
</tr>
</tbody>
</table>
The 22 CWEs in the Security Measure

- CWE-22  Path Traversal Improper Input Neutralization
- CWE-78  OS Command Injection Improper Input Neutralization
- CWE-79  Cross-site Scripting Improper Input Neutralization
- CWE-89  SQL Injection Improper Input Neutralization
- CWE-120 Buffer Copy without Checking Size of Input
- CWE-129 Array Index Improper Input Neutralization
- CWE-134 Format String Improper Input Neutralization
- CWE-252 Unchecked Return Parameter of Control Element Accessing Resource
- CWE-327 Broken or Risky Cryptographic Algorithm Usage
- CWE-396 Declaration of Catch for Generic Exception
- CWE-397 Declaration of Throws for Generic Exception
- CWE-434 File Upload Improper Input Neutralization
- CWE-456 Storable and Member Data Element Missing Initialization
- CWE-606 Unchecked Input for Loop Condition
- CWE-667 Shared Resource Improper Locking
- CWE-672 Expired or Released Resource Usage
- CWE-681 Numeric Types Incorrect Conversion
- CWE-706 Name or Reference Resolution Improper Input Neutralization
- CWE-772 Missing Release of Resource after Effective Lifetime
- CWE-789 Uncontrolled Memory Allocation
- CWE-798 Hard-Coded Credentials Usage for Remote Authentication
- CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
Modern Apps Are a Technology Stack

1. **Unit Level**
   - Code style & layout
   - Expression complexity
   - Code documentation
   - Class or program design
   - Basic coding standards
   - Developer level

2. **Technology Level**
   - Single language/technology layer
   - Intra-technology architecture
   - Intra-layer dependencies
   - Inter-program invocation
   - Security vulnerabilities
   - Development team level

3. **System Level**
   - Integration quality
   - Architectural compliance
   - Risk propagation
   - Application security
   - Resiliency checks
   - Transaction integrity
   - Function point
   - Effort estimation
   - Data access control
   - SDK versioning
   - Calibration across technologies
   - IT organization level

© 2017. Consortium for IT Software Quality
How Do CISQ Measures Relate to ISO?

- ISO 25000 series replaces ISO/IEC 9126 (Parts 1-4)
- ISO 25010 defines quality characteristics and sub-characteristics
- CISQ conforms to ISO 25010 quality characteristic definitions
- ISO 25023 defines measures, but not at the source code level
- CISQ supplements ISO 25023 with source code level measures

Software Product Quality

- **Functional Suitability**
  - Functional appropriateness
  - Accuracy
  - Compliance
- **Reliability**
  - Maturity
  - Availability
  - Fault tolerance
  - Recoverability
  - Compliance
- **Performance Efficiency**
  - Time behavior
  - Resource utilization
  - Compliance
- **Operability**
  - Appropriateness
  - Recognizability
  - Learnability
  - Ease of use
  - Attractiveness
  - Technical accessibility
  - Compliance
- **Security**
  - Confidentiality
  - Integrity
  - Non-repudiation
  - Accountability
  - Authenticity
  - Compliance
- **Compatibility**
  - Co-existence
  - Interoperability
  - Compliance
- **Maintainability**
  - Modularity
  - Reusability
  - Analyzability
  - Changeability
  - Modification stability
  - Testability
  - Replaceability
  - Compliance
- **Portability**
  - Adaptability
  - Installability
  - Replaceability
  - Compliance

*CISQ automated quality characteristic measures highlighted in blue*
Emerging CISQ Measures

- Must measure functional and non-functional code segments
- Must add future effort to fix bugs into productivity
- Must estimate the corrective costs in future releases

Automated Enhancement Points

Quality-Adjusted Productivity

Automated Technical Debt

Effort & Cost

Productivity

Estimation

Benchmarks

Value & ROI

Etc.
**CISQ in Service Level Agreements**

Evaluate Product Quality against Targets in Quality Level Agreements

<table>
<thead>
<tr>
<th>Outsourcer</th>
<th>Automated Function Points</th>
<th>Reliability</th>
<th>Performance Efficiency</th>
<th>Security</th>
<th>Maintainability</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR 1</td>
<td>245</td>
<td>3.16</td>
<td>2.34</td>
<td>3.01</td>
<td>1.99</td>
</tr>
<tr>
<td>VENDOR 2</td>
<td>628</td>
<td>2.78</td>
<td>2.78</td>
<td>3.12</td>
<td>2.34</td>
</tr>
<tr>
<td>VENDOR 3</td>
<td>931</td>
<td>1.67</td>
<td>3.54</td>
<td>2.98</td>
<td>1.76</td>
</tr>
<tr>
<td>VENDOR 4</td>
<td>659</td>
<td>3.12</td>
<td>3.11</td>
<td>2.79</td>
<td>3.11</td>
</tr>
<tr>
<td>VENDOR 5</td>
<td>86</td>
<td>2.56</td>
<td>2.88</td>
<td>3.03</td>
<td>2.56</td>
</tr>
<tr>
<td>VENDOR 6</td>
<td>1047</td>
<td>3.76</td>
<td>2.89</td>
<td>2.97</td>
<td>2.55</td>
</tr>
</tbody>
</table>

Monitor and Manage Service Provider Performance

**TECHNICAL CODE QUALITY**

<table>
<thead>
<tr>
<th>AVERAGE TQI FEBRUARY 2012-JUNE 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best in Class</td>
</tr>
<tr>
<td>Good</td>
</tr>
<tr>
<td>Average</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**QUALITY**

<table>
<thead>
<tr>
<th>PRE-PRODUCTION FEBRUARY 2012-JUNE 2014</th>
<th>2012.02</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**COST EFFECTIVENESS**

| COST PER FUNCTION POINT / ENHANCEMENT FEBRUARY 2012-JUNE 2014 | 2012.02 |
|                                                              |         |

© 2017. Consortium for IT Software Quality
App Certification Using CISQ

CISQ measures

CISQ-conformance assessment

Technology vendors

CISQ-conformant technology

used in

c CISQ service process

Vendor authorized service providers

CISQ-conformant service process

to provide

CISQ/OMG
- only assess vendor conformance
- do not certify applications
- program initiates in 2017

Service providers
- use CISQ-conformant technology
- in a CISQ-conformant service process
- to provide application certifications

Application Certification

Security $X_\sigma$
Reliability $X_\sigma$
Performance $X_\sigma$
Maintainability $X_\sigma$

© 2017. Consortium for IT Software Quality
CISQ’s Current Work Agenda

Embedded software extensions

- Reliability
- Security
- Performance
- Maintainability

Embedded software

Internet of things

Software supply chain

Deploy CISQ into policy

Dept. of ABC

Acquisition Requirements

All acquired systems shall be evaluated for structural quality using the following automated CISQ measures:

- Security
- Reliability
- Performance
- Maintainability

Contract System XYZ

Acceptance:

Contractor shall sustain the following thresholds on the CISQ measures:

- CISQ Reliability 3.8σ
- CISQ Security 4.0σ
- CISQ Performance 3.5σ
- CISQ Maintainability 3.3σ

© 2017. Consortium for IT Software Quality
Consortium for IT Software Quality

The Consortium for IT Software Quality (CISQ) is an IT industry leadership group comprised of IT executives from the Global 2000, system integrators, outsourced service providers, and software technology vendors committed to introducing a computable metrics standard for measuring software quality & size. CISQ is a neutral, open forum in which customers and suppliers of IT application software can develop an industry-wide agenda of actions for improving IT application quality to reduce cost and risk.

CISQ Sponsors

- SYNNOPSYS
- Booz Allen Hamilton strategy and technology consultants
- CAST
- Cognizant
- HUAWEI

ADVANCING THE MEASUREMENT OF SOFTWARE SIZE, QUALITY, AND RISK

- Become a sponsor to lend thought leadership
- Join CISQ to stay current

© 2017. Consortium for IT Software Quality