Consolidating Advice on Trustworthy Software

Briefing to BCS
Southampton UK, 29 January 2013

Ian Bryant
TSI Technical Director

© Copyright 2003-2012
Consolidating Advice on Trustworthy Software

• Challenges
• Advice
• Promulgation
• Questions?
Today’s Audiences

• BCS Quality SG
• BCS e-Learning SG
• BCS Hampshire Branch
• Southampton Solent University (Hosts)
Today’s Speaker

Ian Bryant

- **Technical Director**, *Trustworthy Software Initiative (TSI)*
- **Visiting Lecturer**, *Cyber Security Centre (CSC), De Montfort University (DMU)*
- **Deputy Chair**, *BSI IT Security Techniques Committee - Security Controls and Services Panel*
  - IST/033/-/4 – Lead UK Expert for ISO/IEC JTC1 SC27 WG4
  - Liaison to IST/005 (SC22 shadow – Programming Languages)
  - Liaison to IST/015 (SC7 shadow – Systems and Software Engineering)
- **Subject Matter Expert**, *ETSI Methods for Testing and Specification (MTS) SIG*
- **Co-Chair**, *UK National Information Assurance Forum (NIAF)*
- {On academic sabbatical from **Principal Professional Engineer** (ICT / Security / Resilience), *HM Government*}
Consolidating Advice on Trustworthy Software

- Challenges
  - Advice
  - Promulgation
  - Questions?
Appropriate Conduct?

- *Babylonian Code* of Hammurabi (~1780 BCE) is earliest known example of code of conduct for craftsmen, engineers and builders.
- Hippocrates - ancient Greek philosopher and “father of medicine” lays out the *Oath* - a moral framework for the conduct of doctors and other healthcare professionals in late 5th Century BCE.
- 1907 collapse of 1st *Quebec Railway Bridge* was traced to lack of due diligence in design, implementation and compliance.
  - Emergence of Codes of Ethics in Professional Engineering bodies, which typically includes *Risk* and *Trustworthiness*.
  - UK’s Royal Academy of Engineering and Engineering Council now maintain core *Statement of Ethical Principles*. 
Engineering Principles

• UK’s Royal Academy of Engineering and Engineering Council publish consolidated *Statement of Ethical Principles*

• This includes:
  – Acting in a reliable and **trustworthy** manner
  – Giving due weight to all relevant facts and published guidance, and the wider public interest
  – Identifying, evaluating, and quantifying **risks**
  – Being alert to ways in which work might affect others, holding health and safety paramount
ICT “Cultural (D-)Evolution”
Implicit Requirements (1)

• Typical Customers only really understand and/or care about Explicit (Functional) Requirements

• For instance, a Local Authority may want a Bridge

• The expressed Functional Requirement may only be:
  • Vector (end points ➔ direction, length)
  • Capacity (number of lanes)
Implicit Requirements (2)

• In most industries, in addition to meeting Functional Requirements, Supplier **gives due weight to all relevant guidance** {c.f. Ethical Principles}, including Non-Functional Requirements (NFR)

• For the Bridge, this will include:
  • Strength (of components and overall)
  • Clearance required over river
  • Known Failures modes - - - - - - - - - - - - >

• The software industry **does not have a good track record of addressing the NFR for Trustworthiness**
Typical Implicit (Non-Functional) Requirements: “NFR”

**PAGICCC**
- Performance
- ARM (Availability (incl. Resilience), Reliability (incl. Robustness) & Maintainability (incl. Documentation))
- Governance (Legal (incl. IPR), Regulatory, Policy)
- ILS (Integrated Logistic Support incl. Escrow)
- Compatibility (Operating Environment, Interfaces, Platforms and Dependencies)
- Cultural Fit (including Reputation, Brand)

**QUESTESS**
- Quality (e.g. Faults Delivered, Fault Removal Efficacy)
- Usability / human factors and Accessibility
- Evolution (incl. Extensibility / Scalability, PDS (Post Design Services))
- Standards
- TEA (Training, Education and Awareness)
- Environmental Impact
- Security (incl. IA, Audit/control and DPA)
- Safety
Trustworthy Software Requirement

- Requirements for Trustworthy Software can arise from
  - Explicit (Functional) Requirement for Trustworthiness
  - Implicit (Non Functional) Requirement (NFR) for Trustworthiness
    - Direct NFR for software under consideration
    - As Collateral NFR from other software in environment
  - Requirements cover whole ICT domain (including ICS) and activities (Specification, Realisation and Use)
  - Assurance requirements range from Due Diligence (all software) to Comprehensive
NFR Example: Possible Security Features

- Information labelling and handling
- Equipment siting and protection
- Supporting utilities
- Cabling security
- Maintenance
- Secure disposal or re-use
- Separation of development, test and operational facilities
- Controls against malicious code
- Controls against mobile code
- Information back-up
- Network controls
- Security of network services
- Electronic messaging
- On-line transactions
- Publicly available information
- Audit logging
- Auditing system use
- Protection of log information
- Clock synchronisation
- Privilege management
- Equipment identification in networks
- Remote diagnostic and configuration port protection
- Segregation in networks
- Network connection control
- Network routing control
- Secure log-on procedures
- User identification and authentication
- Password management system
- Use of system utilities
- Session time-out
- Limitation of connection time
- Information access restriction
- Sensitive system isolation
- Input data Verification
- Control of internal processing, including Least Privilege
- Message integrity
- Output data Verification
- Cryptographic controls
- Key management
- Technical vulnerability management (patches and updates)
- Collection of evidence

A Checklist of areas to consider, abstracted from ISO/IEC 27001 / 27002 Control Sets
Risk Management Summary

- **Terminate**
  - A decision is made not to undertake the activity that is likely to trigger the risk, where the risks outweigh the possible benefits,

- **Treat**
  - **The most common approach is to introduce preventative actions to reduce the probability or impact if the risk occurs and maximise the potential for success**

- **Transfer**
  - Share the exposure, either totally or in part, with a partner or contractor, or through insurance. Any partnership will need to be carefully monitored as it may not be possible to transfer all risks and certain aspects may remain, such as loss of reputation

- **Tolerate**
  - The ability of an effective action against some risks may be limited or the cost of taking such action may be disproportionate to the potential benefits gained

Residual Risk = \( \Sigma f \) (Asset) \cdot (Adversity, Vector, Exposure) - \( \Sigma f \) (Countermeasure(s))
ICT Adversity Context

Source: UK TSI / US SwA (2012)
Challenge – Divergent Adversity Views

• Few practitioners treat Adversity holistically
• Information Security community address Threat
  – Deterministic model with problems handling Known, Unknown and Unknowable (KuU) factors
  – Often ignores Hazards
• System Reliability / Safety community address Hazards
  – Typically Stochastic model
  – Approach usually ignores Threat
Facets of Trustworthiness

- Explicit (Functional) Requirements for Trustworthiness
- Implicit (Non Functional) Requirements (NFR) for Trustworthiness
  - Direct NFR for software under consideration
  - As Collateral NFR from other software in environment
Software related problems and disruption are high cost to economy:
- US Government (NIST) estimates ~$60 billion / year to US alone
- Software bugs “source of 90% of ICT Incidents” (GovCERT-UK, 2012-099)
Consolidating Advice on Trustworthy Software

• Challenges

➢ Advice

• Promulgation

• Questions?
UK Trustworthy Software Initiative (TSI)

- Minister for the Cabinet Office Francis Maude, stated in respect of the Future Plans for UK’s Cyber Security Strategy in December 2012:
  
  “We support and fund the Trustworthy Software Initiative, which aims to improve cyber security by making software more secure, dependable and reliable, and to educate on why trustworthy software is important”

- TSI President, Sir Edmund Burton, describes the goal as being to provide a “significant, strategic foundation for the UK Cyber Security Strategy”

- TSI Executive Chair, Stephen Newman, characterises the role as being to provide a “public-private partnership for cultural transformation”
TSI Mission

- UK initiative to coalesce previous *ad hoc* activities
- Renamed from “SSDRI” in September 2012
- Planned Outcomes:
  - Body Of Knowledge (BOK) as appropriate to varying audiences
  - Adoption (ADO), including Training, Education and Awareness (TEA) options to help improve the skills base
  - Independent Verification (VER) options to allow the supply-side to demonstrate capability and the demand-side to discriminate during acquisition
  - Coherence (COH) with international and standardisation efforts
TSI Proposition

• Undesirable consequences of current - untrustworthy - software has major impacts on organisations, and countries, from political, economic, financial and security perspectives

• Users, developers and procurers of software, who engage with TSI have the opportunity to define, trial and refine a consensus body of knowledge and associated services

• Applying TSI’s emergent tools and techniques to new / existing projects could reduce the development / reworking costs / timescales associated with software, systems and projects
TSI Philosophy

• Many of concepts and practices needed for Trustworthy Software have existed for many years
• “Due Diligence” implies software should be reasonably trustworthy, although implementations vary with Audiences and Assurance Requirements
• TSI focuses on Pareto ("80:20") approaches to Making Software Better, iteratively using existing learnings and interpreting them for Common Good
  – e.g. Switching on an acting on Compiler Warning Flags obviates many common “repeat offender” weaknesses
Holistic Control View – Bow Tie Model

TSI approach predicated on whole-life view (ISO/IEC 12207 & 15288), covering Specification, Realisation and Use
Example of Bow Tie LifeCycle

Proactive Treatment Needed \( - and \) Reactive Measures Required
\( / \) or -

Weakness

Platform

Implementation Susceptibility

Vulnerability

Class

Event

Supporting

Composed Incident Evidence

Investigation
Trustworthy Software Framework (TSF) - Structure

Existence  
Concepts  
Principles  
Techniques  
Repository

Level 0  
Level 1  
Level 2  
Level 3  
Level 4

Title
7 Areas
31 Groups
135 Controls
Unlimited

Citations  
Methods  
Data Sharing

[TSI/2012/324] © Copyright 2003-2012
Trustworthy Software Framework (TSF) - Use

- Level 0 Title: Trustworthy Software Framework (TSF)
- Level 1 Areas: e.g. TE – Technical
- Level 2 Groups: e.g. TE.02 – Appropriate Tool Choice
- Level 3 Control Consensus: e.g. TE.02.10 – Programming Language(s)
- Level 4 Repository: e.g. ISO/IEC 24772
  “Guidance on language selection”

TSI: UK’s public-private partnership for Making Software Better
Information Sharing - Boundary Objects

- A mutually recognized means of Information Sharing across domain and/or linguistic boundaries
- Used to encapsulate one or more discrete facts or observations
### Trustworthy Software Framework
#### Level 1/2 Summary – Areas and Groups

<table>
<thead>
<tr>
<th>Governance (9)</th>
<th>Risk (12)</th>
<th>Personnel Controls (8)</th>
<th>Physical Controls (5)</th>
<th>Procedural Controls (21)</th>
<th>Technical Controls (66)</th>
<th>Compliance (10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Environment (3)</td>
<td>Trustworthiness Risks (4)</td>
<td>Producer Organisation Competence (2)</td>
<td>Provide Artefact Protection (4)</td>
<td>Supplier Management (1)</td>
<td>Appropriate tool choices (3)</td>
<td>Situational Awareness (4)</td>
</tr>
<tr>
<td>Management regime (2)</td>
<td>Plan for Assurance (2)</td>
<td>Management Organisation Competence (2)</td>
<td>Management Requirements (5)</td>
<td>Structured Design (3)</td>
<td>Ongoing Review (4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Configuration Management (6)</td>
<td>Structured Implementation (5)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trusted Software Asset Management (3)</td>
<td>Trustworthy Realisation (19)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fault Management (2)</td>
<td>Minimise risk exposure (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hygienic Coding (10)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Methodological Implementation (7)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Internal Pre-release Review (4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Internal Verification (5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dependable Deployment (2)</td>
<td></td>
</tr>
</tbody>
</table>

© Copyright 2003-2012

TSI: UK’s public-private partnership for Making Software Better
Trustworthy Software Levels (TSL)

- Risk-based analysis to select appropriate effort, from:
  - *Supremum* (Greatest Upper Bound) Nature (from 5 Facets of Safety, Reliability, Availability, Resilience, Security)
  - Potential Impact of compromise on *Supremum* Facet
- Effort defined in 5 Trustworthy Software Levels (TSL):
  - (TSL0 = No Requirement)
  - TSL1 = Due Diligence
  - TSL2 = Baseline Trustworthy Practices
  - TSL3 = Enhanced Trustworthy Practices
  - TSL4 = Specialist Trustworthy Practices
TSL Risk Analysis

- **Supremum** (Greatest Upper Bound) Nature
- From 5 Facets of Safety, Reliability, Availability, Resilience, Security
- Potential Impact of compromise on *Supremum* Facet
Why Standardisation?

“If you think of standardization as the best that you know today, but which is to be improved tomorrow; you get somewhere.”

Henry Ford 1863-1947
(American industrialist and pioneer of the assembly-line production method)
General Benefits of Standardisation

- To Demand-side
  - A *de facto* or *de jure* expression of specification, providing risk reduction
  - A target for compliance

- To Supply-side
  - A level playing field, with improved business opportunities
  - Avoidance of nugatory effort, and reduced cost of doing business

- To Corpus-production side
  - *De facto* or *de jure* repository of knowledge
Types of Standard Development Organisation (SDO)

- **De Jure**
  - Major internationally constituted International SDOs (e.g., ISO, ITU-T, ETSI) have formal processes
  - Procedures and processes take time, although work ongoing to streamline approvals
- **De Facto**
  - Loosely constituted international SDOs (e.g. IETF) have processes that are less formal
  - Diverse participants and transparency of the processes sometimes slow the work
- **Ad Hoc**
  - Other groups and consortia typically focus on specific technologies and applications (e.g. MISRA)
  - Such focus allows work products to be produced rapidly, although limited in scope
Mapping Current Trustworthiness Standards Activity

<table>
<thead>
<tr>
<th>Trustworthiness Component</th>
<th>ISO</th>
<th>ISO/IEC JTC1</th>
<th>IEC</th>
<th>ITU-T</th>
<th>ETSI</th>
<th>IETF</th>
<th>W3C</th>
<th>CC</th>
<th>OMG</th>
<th>TOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td></td>
<td>SC7 + SC38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reliability</td>
<td></td>
<td>SC7 + SC22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SC7 + SC22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td>SC27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resilience</td>
<td></td>
<td>TC233</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DRAFT 2012-04

TSI: UK’s public-private partnership for Making Software Better

[TSI/2012/324] © Copyright 2003-2012
Consolidating Advice on Trustworthy Software

- Challenges
- Advice
- Promulgation
- Questions?
TSI Audiences

Corpus
- Research
- Educate
- Professions
- Respond
- Specify
- Operate
- Use

Supply
- Produce - Disbursed
- Produce - Collateral
- Produce - Mainstream
- Produce - Niche
- Assure
- Configure

Demand

TSI: UK’s public-private partnership for Making Software Better

[TSI/2012/324]
© Copyright 2003-2012
Global Context for Software

Internet Users

Source: UK National IA Forum (2010)
Training, Education and Awareness (TEA)

• Training
  – Aimed at the current workforce across the whole ICT domain

• Education
  – Aimed at the future workforce across the whole ICT domain

• Awareness
  – For everyone involved in, or using, any ICT who would not be covered by Training and/or Education

• Working with the Professional Bodies
  – British Computer Society (BCS) and Institute of Engineering and Technology (IET)
  – Accreditation of Degrees, issue of Chartered Status, Continuing Professional Development (CPD)

• Led by Coordination Group (CG) including Academics
Training

• T.1 - General overview
• T.2 - Specialism customised guidance
• T.3 - Verification of Skills
• T.4 - Chartered Status
• T.5 - Continuing Professional Development (CPD)
• T.6 - Executive Course
Education

• E.1 - Primary Education
• E.2.A - Secondary Education
  – A: IT GCSE
  – B: E.Bac
• E.3 - Further Education
• E.4 - Higher Education (Bachelor)
  – A: Technical – Existence
  – B: Technical - Examinable
  – C: Non-technical - Existence
• E.5 - Higher Education (Taught Masters)
• E.6 - Higher Education (Post-graduate Research)
Awareness

• A.0 - Existence of TSI
  – Website
  – Green Papers
  – White Papers
• A.1 - Audience specific overviews
• A.2 - Audience customised guidance
Training, Education & Awareness

Current Priorities

• 1st tranche of activity is the longest lead time items:
  – Input into new IT GCSE /E.Bac in Information Technology (E.2)
  – High-level overview of Trustworthy Software for undergraduates (E.4.A):
    • Not just those in specialisms such as Security and Dependability
    • Rather all “technical” - Computer Science & Electronic Engineering
    • TSI will provide Courseware for those not able to produce their own
    • BCS and IET looking into Degree Accreditation as incentive

• 2nd tranche of activity:
  – More detailed Trustworthy Software education for “technical” undergraduates (E.4.B)
  – Other undergraduate areas (E.4.C) that influence future organisational contexts (e.g. Business Studies, Law, Accountancy)
  – Training of current workforce (T.1)
Assuring Uptake

- Independent Organisational Verification needed for:
  - Producer (PRD) Organisations
  - In-service Management (MGT) Organisations

- TSI Pareto (“80:20”) approach is to always seek re-use of existing learnings where they exist

- Emergent *TickITPlus Scheme* has been identified as potentially providing an extensible route for Independent Verification of Organisational Trustworthy Software practices
Adoption Challenge

• Assertion
  • “Most of the principles and techniques needed to make software trustworthy have existed for many years”

• Challenge:
  • Only the cognoscenti now typically engage with initiatives to improve software trustworthiness
Supply-side:

- **Mainstream = “The Industry”** (e.g. Microsoft, Oracle, ...)
- **Niche = Specialist Industries** (e.g. Aviation, “Security”)
- **Disbursed = Small scale developers** (e.g. SmartPhone Apps)
- **Collateral = Developers don’t consider themselves as such** (e.g. Embedded components, website CMS users, spreadsheets, ...)
## Software Marketplace (2)

<table>
<thead>
<tr>
<th>TSL</th>
<th>Mainstream</th>
<th>Niche</th>
<th>Disbursed</th>
<th>Collateral</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Requirement</td>
<td>Not Sure</td>
<td>None</td>
<td>Not Sure</td>
</tr>
<tr>
<td>1</td>
<td>Due Diligence</td>
<td>Medium ratio; Large overall</td>
<td>None</td>
<td>Large ratio; Huge overall</td>
</tr>
<tr>
<td>2</td>
<td>Baseline Trustworthy Practices</td>
<td>Medium ratio; Large overall</td>
<td>Small ratio; Tiny overall</td>
<td>Medium ratio; Large overall</td>
</tr>
<tr>
<td>3</td>
<td>Enhanced Trustworthy Practices</td>
<td>Small ratio; Small overall</td>
<td>Medium ratio; Tiny overall</td>
<td>Small ratio; Tiny overall</td>
</tr>
<tr>
<td>4</td>
<td>Specialist Trustworthy Practices</td>
<td>None</td>
<td>Medium ratio; Tiny overall</td>
<td>None</td>
</tr>
</tbody>
</table>
Terms from Economics

- Rivalrous (or Subtractable) - those goods which can be consumed by only one person at the same time
- Excludable - those goods which can reasonably prevent those who have not paid from consumption

<table>
<thead>
<tr>
<th></th>
<th>Excludable</th>
<th>Non-Excludable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rivalrous</td>
<td>Private Goods</td>
<td>Common Goods</td>
</tr>
<tr>
<td>Non-Rivalrous</td>
<td>Club Goods (&quot;Natural Monopoly&quot;)</td>
<td>Public Goods</td>
</tr>
</tbody>
</table>
Markets

• Trustworthy ICT Market groupings are disjointed, although arguably individually Rational in Economic terms
  – Knowledge Market(s)
    • Non-Rivalrous (minimum “Club Good”) and \( \textit{in idealised world at least} \) Non-Excludable (probably “Public Good”)
    • Breaks into Market “Stovepipes” of Safety / Reliability / Availability / Resilience / Security, with poor cross-fertilisation of Adversity models
  – Products and Services Market(s)
    • Rivalrous and Excludable (“Private Goods”)
    • Either 4 Organisational groupings of Mainstream / Niche / Distributed / Collateral
    • Or 3 Requirements groupings of Explicit Specialist / Explicit Mass Market / Implicit Mass Market
  – The delineations are orthogonal
Consolidating Advice on Trustworthy Software

• Challenges
• Advice
• Promulgation

➢ Questions?
Contact

Ian Bryant
Technical Director TSI

TSI Office
Gateway House pp4.30
De Montfort University - Cyber Security Centre
The Gateway, Leicester, LE1 9BH, England

ian.bryant@uk-tsi.org
+44 79 7312 1924
www.uk-tsi.org
(Twitter: @uktsi)