Trustworthy Selection and Use of Commodity Products and Services

Prof. Ian Bryant

[WMG/CSC/UCR/073332 | v1.0 | 20211204]
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?
Trustworthy Selection and Use of Commodity Products and Services

➢ What Are Commodities?
  • What Has Gone Before?
  • What Is Needed Now?
  • What Is CUPA?
  • How Is CUPA Used?
  • Questions?
What Are Commodities?

- Commodity items are predominantly “Off The Shelf” (OTS), largely mainstream Commercial (COTS), but also specialised, Government / Military versions (GOTS / MOTS)
- This can include some Modified items that are based upon OTS, and made available under call-off arrangements
- These items include
  - Products
  - Services
- There are Trustworthiness considerations for both
  - Commodities explicitly providing Protective features
  - Commodities with No explicit Protective features
- Unlike Bespoke (a.k.a. Tailored) delivery, individual Customers (Relying Parties) have minimal influence over either the nature of the item, or the associated delivery Terms & Conditions (T&C)
Commodity Usage

- Commodity Products and Services may be used:
  
  • Individually
  • As part of a Solution Assemblage, including
    - Infrastructures
    - Bespoke Solutions

- The End User may:
  
  • Be the Customer, with a direct relationship with the Supplier
  • Have an indirect relationship with the Supplier
    - Through an in-house function, who are the Customer
    - Though an outsourced function (e.g. delivery partner), who are the Customer
    - Through a delivery partner, who are themselves only in an indirect relationship

- Diverse and Disjointed market means the interests multiple Customers (“Relying Parties” - RP) are seldom clear to the Supplying Parties (SP)
Typical Solution Composition

- Commodity %
- Bespoke %

Risk
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?
Assurance Approaches

– Formal Schemes
  • Based on Consensus, but not always a Single Consensus
  • Typically well documented, but can presented a constantly moving target, confusing both Supplying Parties and Relying Parties
  • Requires niche skills, leading to Group Think, and presenting communication barriers to the consumers
  • Often expensive, and time-consuming

– Informal Methods
  • Not based on any Consensus
  • Neither method – nor Commodities! – often well documented
  • Typically performed without SQEP (Suitably Qualified and Experienced Personnel)
  • Limited opportunities for Reuse
Domains of Security Activity

- **PER** (Personnel)
- **INF** (Information)
- **D** (Supply Chain)
- **SYS** (Info-Cyber Systems)
- **EM** (Emanations)
- **PHY** (Physical)

**CSC/UCR/073332**
© Copyright 2014-21

Cyber Security Centre
Learning from Lessons Identified

– From Assurance
  • Churn and Costs of Formal Schemes
  • Poor Robustness and Reuse of Informal Methods

– From Market
  • Lack of Consensus from Relying Parties as to Gaps
  • Lack of Standards to which Supplying Parties can Conform

– From Implementation
  • Poor Consensus between Security Domains, for instance a Physical Device relying on Digital Controls
  • Assurance tasks typically too rigidly documentation-centric
  • Wedded to single delivery model, for instance “Cyber” strongly aligned to Software, with poor understanding of Hardware
  • Poor responsiveness to Novelty and Innovation
  • Business Models marginalise low margin items, for instance Free and/or Open Source Software (FOSS)
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
  ➢ What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?
Understanding Assurance

- Trustworthiness can be characterised as a Spectrum, with widely accepted limits:
  - **Optimal** – Reviewed and endorsed by Trusted Party
  - **Intolerable** – Substantive rationale against from Trusted Party
- There are also middle areas:
  - **Known**:
    - Has been used by Trusted Parties, but not formally reviewed
    - Have encountered no substantive reasons to desist
  - **Unproven**:
    - Not known to be used by Trusted Parties, nor formally reviewed
    - No Open Source substantive reasons to desist
- Assurance Artefacts need to provide sufficient information to allow Relying Parties (RP) to place Commodities on the spectrum
Community Based Approach

- Relying Party Implementers (RP-I)
- Relying Party Governance (RP-G)
- Central Administration (CA)
  - CA-S (Secretariat)
  - CA-T (Technical)
- Assuring Party (AP)
- Supplying Party (SP)
- Scheme Administration (SA)
- Scheme Laboratories (SL)

Core Community & Platform

Extended Community
Function of Central Administration

- Support a Community-based and Owned approach to Trust and Confidence in Off The Shelf (OTS) Products and Services
- Provide interaction route(s) for
  - Understanding Stakeholder Demand
  - Documenting Use Cases
  - Establishing, maintaining, and expressing list of Gaps
- Standardise a spectrum of Assurance approaches
  - Establish and maintain way of Normalising, and levelling-up, multiple Schemes’ outputs
  - Provide Configure-Operate-Maintain (COM) Consensus
  - Provide scalable and reusable input to multiple System / Platform / Infrastructure Approval
  - Establish and maintain Usage and Issue Monitoring
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
- How Is CUPA Used?
- Questions?
Elements of OTS Assurance

B.1. Contextual Screening

B.2.A. Entity Appraisal

B.2.B. Offering Appraisal

B.3. Independent Review

B.4. Technical Testing

B.5. Usage Validation

B.6. Ongoing Monitoring
## Spectrum of Assurance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Appraisal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Homologation</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Legacy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
</tr>
<tr>
<td>Baseline (Bronze)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Structured (Silver)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Granular (Gold)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Proven (Platinum)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Trustworthy Selection and Use of Commodity Products and Services

- What Are Commodities?
- What Has Gone Before?
- What Is Needed Now?
- What Is CUPA?
  - How Is CUPA Used?
- Questions?
Relying Parties and CUPA

- Central Governance (RP-G) responsible for:
  - Recognition of CUPA as Competent Body on behalf of own Organisation
  - Publication of Implementer’s Guidance (e.g. Specific Risk Metrics for OTS selection, ...) for own Organisation
  - Tracking of use of OTS across own Organisation
  - Contributing to CUPA Stakeholder Group on behalf of own Organisation

- Implementers (RP-I) responsible for:
  - Validating A-R-E Commodities as providing a Pragmatic, Appropriate, and Cost Effective (PACE), fit to their own use case(s), both for Suitability, and for Robustness
  - Reviewing A-R-E Cautions, SP Configure / Operate / Maintain documents, and SSA + Open Sources for new Susceptibilities
  - Providing Regular and Triggered updates (SSU) into CS3
Relying Party Management Process

1. Business Requirement(s)
   - Initiates process
   - Evidence for Approvals

2. Commodity Usage Risk Appraisal (CURA)
   - Commodity Risk Appraisal Questionnaire (CRAQ)

3. Commodity Usage Solution Identification (CUSI)
   - Solution Induced Risk
   - Check for Match
   - Candidate(s)

4. Commodity Usage Continual Monitoring (CUCM)
   - Known In Use
   - New In Use
   - 1. Submit Updates (SSU)
   - 2. Receive Alerts (SSA)

5. Commodity Solution Appraisal Questionnaire (CSAQ)

6. RP A-R-E Repository (RPAR)
   - RP Coordination Process (RPCP)

7. Relying Party Implementation (RP-I)
   - Mandate
   - RP Implementation Guides (RPIG)

8. CUPA Administration
   - Register & Escrow
   - Relying Party Governance (RP-G)
**Risk-based Selection of Commodities (1)**

- A “one size fits all” Solution is not always appropriate
- For instance, when choosing a Rental Vehicle we can postulate a set of “Assets” and “Adversities”:

| Assets | Zhong
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2 people + shopping</td>
<td>VS-1  VS-2  VS-3  VS-4</td>
</tr>
<tr>
<td>3/4 people + luggage</td>
<td>VS-5  VS-6  VS-7/8 VS-9/10</td>
</tr>
<tr>
<td>5/6 people</td>
<td>VS-11 VS-12 VS-13 VS-11/13</td>
</tr>
</tbody>
</table>

- Where VS = Vehicle Stratum

<table>
<thead>
<tr>
<th>VS</th>
<th>Adversity</th>
<th>Vehicle Stratum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
<td>(No Vehicle)</td>
</tr>
<tr>
<td>1</td>
<td>Sunshine</td>
<td>City Car</td>
</tr>
<tr>
<td>2</td>
<td>Snow</td>
<td>2 seater soft-top</td>
</tr>
<tr>
<td>3</td>
<td>Distance</td>
<td>AWD sportcar</td>
</tr>
<tr>
<td>4</td>
<td>None</td>
<td>Grand Tourer</td>
</tr>
<tr>
<td>5</td>
<td>Sunshine</td>
<td>Compact</td>
</tr>
<tr>
<td>6</td>
<td>Snow</td>
<td>4 seater convertible</td>
</tr>
<tr>
<td>7</td>
<td>Distance</td>
<td>VS-7 SUV</td>
</tr>
<tr>
<td>8</td>
<td>None</td>
<td>VS-8 AWD Saloon</td>
</tr>
<tr>
<td>9</td>
<td>Sunshine</td>
<td>VS-9 Saloon</td>
</tr>
<tr>
<td>10</td>
<td>Snow</td>
<td>VS-10 Estate</td>
</tr>
<tr>
<td>11</td>
<td>Distance</td>
<td>VS-11 MPV</td>
</tr>
<tr>
<td>12</td>
<td>Sunshine</td>
<td>VS-12 AirCon'd MPV</td>
</tr>
<tr>
<td>13</td>
<td>Snow</td>
<td>VS-13 Large SUV</td>
</tr>
</tbody>
</table>

- *(Implied VS only loosely match to the Rental Industry ACRISS / SIPP Codes)*
- Each RP will need to map its own Risk Approach to CUPA Levels
Risk-based Selection of Commodities (2)

- “PEILAT-S”: suggested Criteria for Relying Parties to consider
- Initial Requirement – Solution Agnostic
  - Perimeters
  - Entities
  - Interconnections
  - Locales
  - Archetypes
  - Temporal
- Refined Requirement – adjust for Solution-induced Risks (SIR)
  - Solution
- Derive a Hierarchical Protection Requirement
  - Protection Goals (e.g. Threat Actors x Exposures)
  - Effort Expected (e.g. Due Care – Reasonable Effort – Best Effort)
- Map to the Assurance Levels produced by CUPA
Any Questions?

Paper Download: https://is.gd/wmgcsc073331

“Septem Circumstantiae”
from “Ethica Nicomachea”
Aristotle
(4th Century BCE)
Contact

Prof. Ian Bryant
Principal Investigator (UCR)

Room 253 International Manufacturing Centre
University of Warwick
University Road, Westwood Heath, CV4 7AL, England

i.bryant@warwick.ac.uk

+44 24-769-51924

https://is.gd/wmgcsc