Criticising the Common Criteria Argument

Patrick Graydon

The University of York
A Contribution to the Development of the Common Criteria

Criticising the Common Criteria Argument

Patrick Graydon

The University of York
A long time ago . . .

• Assurance Based Development of a shadow implementation of Tokeneer
  – Tokeneer developed for Common Criteria evaluation at EAL 5
  – Work raised some criticisms of the standard
  – No point in criticising 2.1 when 3.1 is current
Evaluating Standards

• Question: Can you evaluate a standard by extracting and criticising its argument?
  – Requirements form evidence
  – Explanation of requirements explains evidence

• Case study target: The Common Criteria For Information Technology Security Evaluation
  – A major international security standard
Criticising the Standard’s Argument

The Standard

- Explanations (Objectives)
- Requirements (Elements)

Is the security evidence sufficient?
Is the evidence adequately explained?
The Common Criteria Standard

- The standard comprises three parts:
  - Part 1: Introduction and general model
  - Part 2: Security functional components
  - Part 3: Security assurance components
- This trilogy has a Part 4 (sort of):
  *The Common Methodology for Information Technology Security Evaluation*
Security Targets and Evaluation

Security Problem (Assets, threats, etc.)

Template Functional Requirements

Part 2

Template Assurance Requirements

Part 3

Security Target

Target of Evaluation

ST Evaluation

TOE Evaluation

07/02/2012

Criticising the Common Criteria Argument
Capturing the Elements

**Developer Action Element:**
**ALC_DVS.2.1D** The developer shall produce and provide development security documentation.

**Content and presentation elements:**
**ALC_DVS.2.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

...
Capturing the Elements

Evaluator action elements:

**ALC_DVS.2.1E** The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

**ALC_DVS.2.2E** The evaluator *shall confirm* that the security measures are being applied.

Not explicitly modelled in the argument (corresponds to confirming that the argument reflects the real world)

The development security procedures are being applied (ALC_DVS.1.2E)

The evaluators’ report on site visit(s)

Reflects application notes

07/02/2012

Criticising the Common Criteria Argument
Capturing the Objectives

Objectives
Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE and its parts. It includes the physical security of the development location and any procedures used to select development staff.

Application notes
This family deals with measures to remove or reduce threats existing at the developer's site. . . . The evaluator should visit the site(s) in order to assess evidence for development security. . . . Any decision not to visit shall be agreed with the evaluation authority. . . . It is recognised that confidentiality may not always be an issue for the protection of the TOE in its development environment. The use of the word “necessary” allows for the selection of appropriate safeguards.
Evaluation Assurance Levels

• Standard defines 7 EALs
  – Standard levels of assurance
  – Each a package of SARs
  – Each builds on the one below

• We modelled all 7 EALs
  – Modelled only families that appear in an EAL
    (did not model ALC_FLR [“flaw remediation”])
The Captured Argument

• Not a security argument
  – No system-specific detail
  – Argues over (not through) threats and SFRs

• Not a full rationale
  – No evidence of technique adequacy
  – No mention of trade-offs made
Reviewing the Argument

• Phased process\(^1\), i.e. one family’s worth at a time
• Looked for:
  – Vagueness or potential misinterpretation
  – Unreasonable assumptions (implicit or explicit)
  – Logical fallacies (from taxonomy\(^2\))
  – Omission of expected practice
  – Insufficient evidence

1. P. Graydon, J. Knight, and M. Green, “Certification and safety cases”, *Proc. of the 28\(^{th}\) International Systems Safety Conference (ISSC)*, 2010
The security requirements are sufficient

- Each SFR is traced back to the security objectives for the TOE
- The SFRs meet all security objectives for the TOE
- The reason why the SARs were chosen has been explained

- Shows reliance, not sufficiency
- ‘Adequately’ meet?
- Does the explanation show adequacy?

ST’s security requirements rationale

07/02/2012
Criticising the Common Criteria Argument
Sentencing the Issues

• First, check the standard: did we introduce the issue in the process of argument capture?
Further Classification

<table>
<thead>
<tr>
<th>Impact</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing or inadequate evidence</td>
<td>21</td>
<td>34</td>
<td>5</td>
<td>60</td>
</tr>
<tr>
<td>Misleading or inadequate explanation</td>
<td>18</td>
<td>7</td>
<td>3</td>
<td>28</td>
</tr>
<tr>
<td>Other (mostly vagueness)</td>
<td>22</td>
<td>7</td>
<td>4</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>61</td>
<td>48</td>
<td>12</td>
<td>121</td>
</tr>
</tbody>
</table>
Missing or Inadequate Evidence

• Either:
  – The standard’s argument omits a premise
  – Evidence that could practicably increase confidence not demanded

• We use the As Confident As Reasonably Practicable (ACARP) principle
System Level Testing Against SFRs

- Security Problem
- Security Objectives
- Functional Requirements
- Functional Specification
- Design Description
- Implementation Representation
- Implementation

E.g. source code

ADV_FSP requires a tracing (not proof of refinement)

An analysis of test coverage demonstrates the correspondence between the tests . . . and the TSFIs

An analysis of test depth shows all subsystems have been tested

07/02/2012

Criticising the Common Criteria Argument
Adequacy of Structural Coverage

An analysis of test coverage demonstrates the correspondence between the tests . . . and the TSFIs

An analysis of test depth shows all subsystems have been tested (and, at EAL 7, that “the TSF operates in accordance with its implementation representation”)

Evidence of structural (code) coverage?

07/02/2012
Criticising the Common Criteria Argument
Adequacy of Proof Process

“The proof of correspondence between the formal specifications of the TSF subsystems [given in the design documentation] and of [sic] the functional specification shall demonstrate that all behaviour described in the TOE design is a correct and complete refinement of the TSFI that invoked it.” (EAL 7)

- Proof process determines resulting confidence
  - Machine checked?
  - Translated? By hand?
  - Quality of tools?

The CC does not specify
Criticalising the Common Criteria Argument

Correctness Of Security Policy Model

Security Objectives

Functional Requirements

Functional Specification

Design Description

Evidence that model’s definition of “secure” is appropriate? Dashed line shown in Fig. 10 of Part 3, but . . .

(Formal) Security Policy Model

Formal proof of correspondence between the model and any formal functional specification

“Throughout the design, implementation, and review processes, the modelled security requirements may be used as precise design and implementation guidance . . .”
Sufficiency of SARs

We modelled the EALs' SARs, but . . .

Template Assurance Requirements

Part 3

Security Target

ST Evaluation

Must “explain why the SARs were chosen”

CEM: “Any explanation is correct so long as it is coherent and neither the SARs nor the explanation have obvious inconsistencies with the remainder of the ST”

Security Assurance Requirements

Security Requirements Rationale

No evidence that SARs are sufficient

07/02/2012
Criticising the Common Criteria Argument
Clarity of the Security Problem

ADV_SPD Objective:
“Evaluation of the security problem definition is required to demonstrate that the security problem intended to be addressed by the TOE and its operational environment, [sic] is *clearly* defined.”

ADV_SPD Elements:
“The security problem definition shall describe the assumptions about the operational environment of the TOE.”

No evidence that the description is clear

ST Evaluation
**Appropriateness of Architecture**

**ADV_ARC objective:**
“The security architecture descriptions supports the implicit claim that security analysis of the TOE can be achieved by examining the TSF; without a sound architecture, the entire TOE functionality would have to be examined.”

**ADV_ARC Elements:**
Evaluator must confirm that architecture description “demonstrates” that the TSF:
- “protects itself from tampering”
- “prevents bypass of the SFR-enforcing functionality”

---

**Security Architecture**

**TOE Evaluation**

- **How good is good enough?**
- **How does the evaluator decide?**
- **Must we follow “best practice”?**

**Better evidence could be provided**
ToE Generated From Given Source

E.g. source code

Implementation Representation

Test Executable(s)

Functional Testing

CM plan

CM system

At EALs 4–7, must “support the production of the ToE by automated means”

At EALs 3–7, must “describe how the CM system is used for the development of the system”

At EALs 4–7, must “define the TSF to a level of detail such that the TSF can be generated without further design decisions”

At EALs 6–7, evaluator must “determine that the application of the production support procedures results in a TOE as provided by the developer for testing activities”

Good enough?

07/02/2012

Criticising the Common Criteria Argument
Details of Code Obfuscation

At EALs 4–7, must “be in the form used by the development personnel”

ADV_IMP application notes:
“The components [of ADV_IMP] require details on the shrouding tools/algorithms . . . to gain confidence that the shrouding process does not compromise any security functionality.”

No element of ADV_IMP explicitly requires this detail
Implementation Standards

At EALs 5–7:
- Developer must “describe and provide the implementation standards that are being applied”
- Evaluator must “confirm that the implementation standards have been applied”

**ALC_TAT application notes:**
“Implementation guidelines may be accepted as an implementation standard if they have been approved by some group of experts (e.g. academic experts, standards bodies). Implementation standards are normally public, well accepted and common practise in a specific industry, but developer-specific implementation guidelines may also be accepted as a standard; the emphasis is on expertise.”

**No element of ALC_TAT requires evidence of adequacy**
Tool Correctness

At EALs 4–7, tools must be “well-defined”

“These are tools that are clearly and completely described. For example, programming languages and computer aided design (CAD) system that are based on a standard published by standards bodies are considered to be well-defined.

Impact of tool failure varies:
- Might miss a defect or vulnerability
- Might introduce a defect or vulnerability
In some cases, tool failure might have sever consequences.

No element of ALC_TAT requires evidence of correctness
Misleading or Inadequate Explanation

• Either:
  – The objectives are too narrow
    (i.e. don’t support the higher levels of argument)
  – The objectives are too wide
    (i.e. aren’t supported by evidence)

• Explanation is important
  – Defines the “spirit” of the requirements
  – Basis for making judgments of degree
Objective of Exhaustive Testing

ATE_COV Objective at EALs 6 & 7:
“In this component, the objective is to confirm that the developer performed exhaustive tests on all interfaces in the functional specification. The objective of this component is to confirm that all parameters of all of the TSFIs have been tested.”

ATE_COV Application Notes:
“The developer is required to demonstrate that the tests exercise all of the parameters of all TSFIs. This additional requirement includes bounds testing . . . and negative testing . . . . This kind of testing is not, strictly speaking, exhaustive, because not every possible value of the parameters is expected to be checked.”

ATE_COV Elements at EALs 6 & 7:
The TSFIs must be “completely tested”.

Objective of exhaustive testing deliberately not satisfied (and completely is undefined)
Other

• Issues that did not fit either of the other two categories
• Nearly all were issues of vagueness
“Focused” and “Methodical”

• At EALs 2 and 3: “The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.”

• At EAL 4, this analysis must be “independent”

• At EAL 5, it must also be “focused”

• At EALs 6 and 7, it must instead be “methodical”

• Neither “focused” nor “methodical” is defined
Findings

• We applied our evaluation method to the CC
  – It was feasible
    • Took one analyst several weeks to capture and criticize
  – It found issues of interest
Threats to Validity of Findings

• Overlooking expected practice
  – Inexperienced analyst might not find all issues

• Might fail to find remote definitions
  – We searched the CC and normative references
  – Should be cross-referenced anyway

• Might not know common security parlance
  – Definitions vary; should be captured anyway
Threats to Validity of Findings

• Estimates of cost or feasibility might be wrong
  – Would lead to false report of missing evidence
  – We considered only forms of evidence with established techniques and tool support
  – Suggest writing standards to keep with ACARP
Threats to Generalisability

• Some standards might lack a complete arg.
  – Writers might consider it ‘complete’ without explanation at all levels
    • E.g., DO-178B lacks top-level argument
  – Might lead to false-positive ‘insufficient evidence’
    • Analyst must assume the highest importance
  – There really ought to be an argument
    • Might be presented separately
    • How else would we know the standard is sufficient?
Is now a good time to ask questions?