

# Appropriate Assurance: fitting like a Glove, not a Tent

Tony Boswell  
CLEF Technical Manager  
SiVenture

10th

International  
Common  
Criteria  
Conference

10 ICC



## Overview

- Looking beyond the basic assurance levels
- Alternative approaches: what might make assurance more appropriate?
- Potential Obstacles
- Conclusions

September 2009

2

## Do TOEs fit single assurance levels?

Sometimes we deal with TOEs that have single assurance levels...and we have certainly managed to use CC (and other schemes) for many years using only a single assurance level in an ST

But it seems that we very often have discussions about security priorities in a TOE, and these lead to the idea of an assurance profile: the idea that different aspects of a TOE would ideally be evaluated to different assurance levels

## Examples of different priorities

- Different levels in a key hierarchy: session keys, device-specific keys, scheme-wide keys, etc.
- Types of asset: long-term scheme key, PIN value, single transaction details
- Layered protection mechanisms: layering to provide defence in depth does not require all mechanisms to be equally strong
- Environmental protection: some interfaces and functionality may not be protected by the environment; others may only be available in physically protected areas
- Composite TOEs: different component roles

## Impacts of imposing a single level

With only a single target level where we have different assurance requirements, we may find the following:

- ST uses the highest assurance level for all aspects
  - may cause evaluation to be rejected on cost or time grounds
- ST uses the highest assurance level and leaves out the lower level functionality
  - this may not lead us to the sort of TOE scope that we want to encourage
- ST uses a lower assurance level in order to get the 'right' scope

September 2009

- this may not fit the target environment; may leave<sup>5</sup> no

## What might we do instead?

- One ST for each assurance level
  - requires us to ignore TOE-scoping principles; may leave gaps
  - too much unnecessary work for everybody (users, lab, CB)
- Multiple assurance levels within a single ST
  - the 'obvious' next step, but can we do better?
- New assurance components (or refinements and extensions to existing components)
  - these are probably a desirable part of any solution, e.g. in order to help make scope clear
- Defining new assurance levels
  - using existing part 3 components, plus extensions relevant to technology or TOE type, and refining and linking them in new ways

## EALs: new vs. old (1)

We could just define groups of functions (SFRs) and map each to an existing EAL

e.g. external secure channels protected to EAL4;  
authentication of administrators at a local console to EAL3

But ‘appropriate assurance’ could mean something more than this, such as

- matching the assurance demands of a component to what is appropriate in the risk environment
- matching tools and techniques to the TOE technology and the types of Security Functions
- identifying key properties and roles of certain deliverables

## EALs: new vs. old (2)

Defining appropriate assurance could sometimes involve using existing part 3 components

In other cases it could involve taking inspiration from these components and identifying core elements

E.g. to what extent does AVA\_VAN depend on the activities in ADV\_TDS or ADV\_IMP, as opposed to the ADV inputs?

Consider:

design analysis vs.

design information vs.

design-informed testing vs.

design-informed

## EALs: new vs. old (3)

Some other thoughts (in the ATE area)...

- When might it be appropriate to focus on assurance generated from a particular tool?
  - perhaps when a security property maps clearly to what a tool finds or demonstrates: not just a general property such as coverage
- Why would we think it a good thing that a developer does CC-specific tests?
  - CC is not something you add to a product, it is meant to be a measuring tool that you use on a product

**So...**

We could be talking about 2 aspects to appropriate assurance:

- Making assurance-generation better fit the type of TOE and the type of security properties
- Applying different levels of assurance to different parts of the TOE



## Why might assurance profiles be difficult? (1)

- How will the evaluators know which level to apply to which functions?
  - (by proper definition and careful tracing)
- How will we deal with dependencies between functionality at different assurance levels?
  - (by including dependencies in a justification of an assurance profile...don't we already have similar issues with SFR-enforcing and SFR-supporting?)
- How do we pick the right profile? There is a risk that the ST profile does not match the user's required profile
  - (true, but with a profile we have a better ability to respond to feedback – how do we pick the 'right' assurance level now?)

## Why might assurance profiles be difficult? (2)

- Can we harmonise internationally and support mutual recognition (CCRA)?
  - (maybe requires ASE to be updated, but this should be possible)
- What does it say on the certificate? Will an ST reader understand a profile? How can we compare TOEs?
  - (maybe “EALx-y-z”, or maybe the name of an assurance level/package defined in a well-known place such as a PP)
  - (no more complicated than the current situation: a real understanding, or comparison of TOEs, requires reading the ST, not just the assurance level)
  - (comparison may become easier if bespoke assurance levels/packages better reflect the requirements of a specific user domain)

September 2009

f2a

## Possible constraints

We probably have to constrain the way we apply bespoke assurance...

Anybody can design a bespoke assurance profile, but they are probably of maximum value when they are shared between different products

There is also potential for abuse...such as picking what is “convenient” and developer/product-specific

So definitions of bespoke assurance profiles should probably be created by communities and embodied in certified PPs (with coherence and quality assessed when the PP is evaluated)

## Conclusions - making an ST fit like a 'glove'

- Requires a coherent model in the ST, so that it is clear what aspects are assured to what level
- Requires matching the assurance techniques to the TOE technology, development techniques, and the security properties being evaluated
- Should be based on a community-wide view
  - even those who own the requirements or risks may not be in a position to define an appropriate bespoke assurance profile



**Questions?**

**Tony Boswell**  
**[tony.boswell@siventure.com](mailto:tony.boswell@siventure.com)**  
**tel: +44 1628 651 361**

September 2009

15