Assurance Activities – Ensuring Triumph, Avoiding Tragedy

Tony Boswell
CLEF Technical Manager
SiVenture
Overview

What are Assurance Activities?

How do they relate to earlier CC work?

What are we looking for in Assurance Activities?

How can we keep CCRA intact?
What are “Assurance Activities”? (1)

Assurance Activities are normative descriptions of activities that must take place in order for the evaluation to be complete …

Assurance Activities are in fact a tailored evaluation methodology, presented in-line [with other PP requirements] for readability, comprehension, and convenience

– Protection Profile for USB Flash Drives, v1.0
What are “Assurance Activities”? (2)

Examples – AAs in both the Network Devices PP and the USB Flash Drives PP

- require specific tests defined for cryptographic implementations used in supporting secure connections and protocols
- specify how logon and authentication mechanisms should be tested
- resolve scope questions (e.g. ‘each audit record format type must be covered’)
- make use of references to external standards
- attach to SARs as well as SFRs
What are “Assurance Activities”? (3)

Examples from USB Flash Drives PP continued…

The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked. …[T]he evaluator shall determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(1)).

[Password c]onditioning can be performed using one of the identified hash functions or the process described in NIST SP 800-132; the method used is selected by the ST Author. If 800-132 conditioning is specified, then the ST author will fill in the number of iterations (C) that are performed; this value must be at least 10000. 800-132 also requires the use of a pseudo-random function (PRF) consisting of HMAC with an approved hash function. The ST author selects the hash function used, also includes the appropriate requirements for HMAC and the hash function from Appendix C.
What are “Assurance Activities”? (4)

Examples (not verbatim) from USB Flash Drives PP

The evaluators shall first examine the TSS section to ensure that the authorization factors specified in the ST are described. For password-based factors the examination of the TSS section is performed as part of FCS_CKM.1(3) assurance activities. For the [optional] host split and pin authorization factors, <do something>.

– If other authorization factors are specified, then <do something>.
– If there is only one authorization factor, <no activity required>.
– Test 1: If there is more than one authorization factor, ensure that failure to supply a required authorization factor does not result in access to the TOE.
Are they separable from ‘the new PPs’?

Can we separate Assurance Activities from the context of their use in new–generation PPs?

They are generally used with:

- a low baseline assurance level (EAL1)
- an ‘enhanced’ TOE Summary Specification in the Security Target, which includes a significant level of design information
- optional additions or enhancements

But (I suggest) AAs can be separated from these and other aspects of ‘new PPs’
The importance of detail (1)

Abstraction is often good, but sometimes detail makes a difference…
The importance of detail (2)

- When we have abstract requirements (as in CEM) then we suffer from ‘pixellation’ in mapping them to the real world…

We are missing *detail* in our description and therefore in our requirements. The more detail that we fill in at evaluation-time, the more chance of inconsistency.
Is this new?

- Adding detail to reflect the TOE type is not a fundamentally new concept…
- …Assurance Activities are ways that we can add specific detail to the abstract structure of a CC evaluation

- But what about existing CC constructs such as SFR/SAR refinements, or assurance packages?
Previous approaches (1)

- We have had the ‘detail’ problem before…
  - the lack of detailed methodology for smart card ICs made composite evaluations ‘difficult’ because there was no ‘reference test manual’ or attack potential ratings on which to base consistency

- So we added detail in a combination of interpretation and refinement in PPs, and separate supporting guidance documents
  - especially in the Attack Methods document that deals with applying open-ended test types (like physical probing or power analysis)
Previous approaches (2)

➢ For POI (payment terminals) we combine these with the additional step of a bespoke assurance level (in the form of an assurance package) to represent assurance priorities (see the definition of EAL POI and AVA_POI.1-4)
So: why write Assurance Activities? (1)

- Why not refinements or packages?
  - Because AAs are not about the claim (SFR); they are about its verification, and about detail not broad strokes

- To make it clearer what we expect developers to provide and evaluators to do in evaluation
  - Improved understanding of requirements
  - Improved capture of best practice
  - Improved consistency of evaluation
  - …therefore improved basis for mutual recognition
So: why write Assurance Activities? (2)

- To be able to build specific depth of assurance in the areas we want
  - Remember the long-standing issue of assurance profiles and priorities (i.e. some requirements are more important than others)

  - This links Assurance Activities to the use of a low baseline assurance level, so that we only apply depth (e.g. source code) where we want it
So: why write Assurance Activities? (3)

- To better deploy the collaboration we expect from Technical Communities
  - Rely less on interpretations of generic CC language made by each lab and CB, and more on precise specification for each TOE type
  - Get better risk owner/manager input

- Therefore to *improve* the basis for mutual recognition (CCRA)
Why put Assurance Activities in *PPs*?

🔹 Because they can sit alongside functional requirements that they are testing – we make the Assurance Activities add more to the understanding of an SFR by describing how the SFR is to be evaluated

🔹 Because it will be good to maintain the underlying PP requirements at the same time as the interpretation material
Rules for AAs?

At first it seems good to set down firm rules…but what would these look like?

- Syntax rules?
  - Takes us back to abstraction and pixellation…

- Content rules?
  - The point here is to add detail, but what can we say without knowing the detail?

- Scope rules?
  - Maybe some basics about what should be said (and not said)? E.g. can they be uncompleted in a PP (like SFRs)?
Guidelines for Assurance Activities (1)

Maybe…

❖ Every SFR should have an AA
  - Defining what aspects of functionality are to be tested, and at what level of thoroughness (e.g. every type of firewall rule?)
  - Mapping abstract CC terms to expectations for the TOE type
  - Identifying relationships and dependencies between SFRs
  - Clarify how to treat conditional/optional cases

❖ Every SAR should have an AA
  - It should explain more specifically how the deliverables are expected to be used in support of evaluating the SFRs
  - It may specify additional deliverables above the baseline assurance level in particular areas (e.g. for particular SFRs)
Guidelines for Assurance Activities (2)

- ETR reporting requirements identified, especially where this is important to demonstrating rigour (e.g. as we currently do in ATE_IND.2-9) or consistency

- AAs should, as far as possible, be:
  - Specific
  - Measurable
  - Achievable
  - Realistic (with respect to the assurance level)
  - Time-bounded (within a likely evaluation timescale)

- Identify where alternative assurance evidence is allowed or required
  - FIPS140, ISO27000, ETSI, NIST SPs, etc.
Another thought

Maybe Assurance Activities could help us with the ‘problem of innovation’

This is a topic of other presentations and work, but in brief it concerns the following problem: how do we evaluate in a sufficiently transparent way (so that everybody understands the actual assurance achieved) a TOE whose ST includes claims specific to only that TOE?

Perhaps it would help if we specified both the claim and corresponding Assurance Activities

- With assessment by the CB at the time of acceptance into evaluation
What might be bad about AAs? (1)

- They have no formal recognition or definition in CEM!
  - Except that “activity” is defined as “application of an assurance class of the CC Part 3”
  - We can fix this just by adding them

- Do they undermine the notion of assurance generation in CC part 3 and CEM?
  - Maybe by defining individual AAs we miss something out from the generic CC requirements?
    - Responsibility of PP review to prevent this
    - Already have this risk in every evaluation ever done!
What might be bad about AAs? (2)

Do they undermine CCRA?

- The answer here seems to be similar to the previous question…but let’s look at a bit of CCRA itself…
CCRA Context (1)

From CCRA, ‘Spirit of the Agreement’:

*The complexity of information systems is such that even the most carefully written security evaluation criteria and evaluation methodology cannot cover every eventuality. In many cases the application of the criteria will call for expert professional judgement, as will the oversight of their application. In exercising such judgement, the Participants will endeavour to use the level of assurance in the IT product under evaluation as their metric. The Participants in the Arrangement therefore plan to develop and maintain mutual understanding and trust in each other’s technical judgement and competence, and to maintain general consistency through open discussion and debate.*
CCRA context (2)

Assurance Activities can be a way to crystallise the “expert professional judgement” by making ourselves adopt the discipline of writing down the detail of what we mean, exposing it to review within expert groups, and maintaining it regularly.

We don’t need to make them mandatory…just well-defined.
In Conclusion...

- Assurance Activities capture many of the good things about current changes in CC: adding detail that makes assurance more meaningful and consistent, and basing this on expert community input and review.

- Although they are ‘new’ they do not need to undermine any of the concepts we have worked with, and they do not have to replace or exclude other successful approaches.

- We should adopt them formally rather than leave them ‘undocumented’.
Questions?

Tony Boswell
tony.boswell@siventure.com
tel: +44 1628 651 361