

Building Successful Communities to Interpret and Apply CC

Tony Boswell
CLEF Technical Manager
SiVenture

10th

International
Common
Criteria
Conference



10 ICC

Overview

- Why do we need Communities in CC?
- What is a Community (and why isn't it a committee)?
- Creating, building and maintaining a successful CC Community



Spoiler

The secret behind nearly all of the following slides is not writing it down, or even the meaning of the words...

...it is following the ideas day-by-day, meeting-by-meeting!

(And especially when being a community member has to compete with your 'real' job)

The main message will turn out to be about the 'soft' things, not the technical things.

September 2009

3

Why do we need Communities?

- We need to interpret and accept CC for different situations...and these may be defined by
 - technology types
 - usage domains(And maybe other things)
- Ultimately we are looking to deal with what happens when CC abstraction meets reality!
- Maybe we should ask “when do we **not** need a community”?
- (And how did we get where we are today...?)

Interpreting for Technology Types

- Technology types define and aim to establish consistency in dealing with:
 - what attacks should be considered, what are the baseline attack techniques, and how should these be rated for attack potential?
 - what are the typical TOE architectures, what problems do they raise, and how do we deal with them?
 - what are the meaningful differences between assurance levels for this technology?

Interpreting for Usage Domains

- Usage domains are more about how a CC certificate gets used:
 - what do we actually rely on in the operational environment?
 - how does CC effectively align with commercial boundaries (e.g. hardware, software, 3rd party components)?
 - how can we make CC cost-effective?

What are we looking for?

- Relevance of interpretation (to the domain of use)
- Consistency of application
 - reducing developer uncertainties
 - reducing variation between labs and CBsbut not slavish consistency
- Supported interpretation



What sort of outputs?

Examples of what communities may produce:

- protection profiles
 - containing interpretations, refined/extended assurance components, etc.
- methodology
 - e.g. applying composition (and maybe ALC requirements) in the situations typical of the technology type or usage domain
- catalogues of attack methods
 - to establish evaluation content and improve consistency between evaluations
- qualification/competence processes
 - initial qualification of a lab for a domain
 - updating for consistency at (or close to) state-of-the-art



Community Characteristics (1)

- Relevant: identifies and solves real problems
 - therefore has to involve all the players, and especially the problem-owners
- Representative: no gaps in the stakeholder web
 - both problems and solutions should benefit from the views of all the stakeholders
- Inclusive: not just the people we may prefer to talk to
 - and of course this means the Community will include competitors
- Engaged: caring about the solutions
 - experience and expertise
 - regular attendance (by the same person); tangible contributions



Community Characteristics (2)

- **Connected:** works with other communities
 - e.g. CBs, evaluators, industry/vendor groups, deployment schemes (e.g. payment schemes)
 - 'sub-communities' enable better consensus within the main Community
- **Output-oriented:** produces specific deliverables
 - obviously related to the problems!
- **Authoritative:** can determine acceptance as well as definition
 - avoid 'solutions in principle' or ideas that face further hurdles to get adopted
 - avoid 'not invented here'
 - channel to formal adoption of outputs



What should it feel like?

- Trusting
- Collaborative
- Expert
- Appreciative
- Real work(!)

And at times:

- frustrating
- exhausting
- over-ambitious



Can we 'engineer' good Communities?

...or do we just have to put the elements together and hope?

I think it comes down to the individual attitudes of the members

If we can reflect on, and remind ourselves about the target characteristics, without talking about them, then that's probably best!

This needs to remain a working group (not a self-help group)...but one that is unusually tolerant of uncertainty and difference of opinion.



Some ideas for how to form...

- Get the relevant people together
 - don't expect perfection at the start: allow, and encourage, the word to spread
- Engage on a tangible (and relevant) task soon
- Make (!) everybody talk and listen together
 - probably needs provocative topics
 - share something uncomfortable...like an area where we are all afraid to admit that we don't really know what we're doing
- Agree that what is said in the room stays amongst the participants
- Expect it to take time
 - but work on an output anyway

...and build

How does a community continue to develop healthily?

- Consider whether the community should build, or whether to disband
- Maintaining outputs is probably necessary, but may not be a sufficient motivation to keep the group engaged
- But improving the interpretation, where feedback is gained from all the members (developers, evaluators, certifiers, and certificate consumers) may present new challenges
- ‘Continuing professional development’!



Challenges – the unknown

- **Scaling**
 - (and preserving all those very personal aspects such as ‘one conversation’ and trust)
- **Continuity of members and loss of ‘collective memory’**
 - how important is the history?
 - how are the ‘norms’ passed on?
- **Rigidity**
 - sticking to previous views and outputs ‘because they are ours’, or because they look too hard to change
- **Complacency**
 - as for rigidity, but also believing that this is right because we are infallible!



Questions?

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

September 2009

16