Technical Communities: Theory and Practice

ICCC 2012 – Paris
20 September, 2012

Brian Smithson, Senior Security Architect
Global Solutions Engineering,
Ricoh Americas Corporation
Agenda

- Background
- Technical communities today
- In theory…
  - The NIAP approach
  - CCDB Vision versus NIAP approach
- In practice…
  - What do technical community members think?
  - What makes this so difficult?
- Recommendations
- Summary
Successful collaborative CC development in the smartcard industry led to discussion of technical communities for other industries.

- Tony Boswell gave a presentation “Building Successful Communities to Interpret and Apply CC” at the 10th ICCC.
- David Martin gave CCDB progress reports on Technical Communities at the 10th, 11th, and 12th ICCC.
- Chris Salter wrote a paper, “Common Criteria Reforms” in January 2011, in which technical communities are a key element.
Background (2)

- Recognizing industry experience in technical communities, the CCDB asked industry to propose “terms of reference” at the 12th ICCC.
- Industry work groups produced three documents:
  - “Technical Communities and Collaborative Protection Profiles” (an overview of different ways technical communities can be formed)
  - “Terms of Reference for Collaborative Technical Communities” (essential terms of reference, in response to the CCDB request)
  - “Terms of Reference Guidance for Collaborative Technical Communities” (guidance for forming and operating technical communities)
Technical communities today

- There are many technical communities developing protection profiles, some old and some new
- None has been approved by the CCDB as a “Collaborative Technical Community”, but work is progressing on a trial CCDB process for the USB Technical Community (US, UK, and SE)
- NIAP has started several new technical communities based on its own approach, documented in a white paper, on its web site, and in a yet to be published NIAP Technical Communities Guide document
IN THEORY:

NIAP approach¹

- **Purpose**
  - Form TCs around major technology areas
  - Tailor assurance activities to better fit each technology
  - Track evolving technologies and evolving threats
  - Make evaluations objective, measurable, repeatable, effective, efficient

- **Principles**
  - Collaboration and collective ownership of process
  - Leverage industry expertise
  - International perspective
  - Transparency
  - Open to all interested individuals

¹ NIAP Technical Communities web page; Technical Communities: A Collaborative Approach for Protection Profile Development Version 1.0; An Update on the NIAP Evolution (C. Houck, 12th ICCC, from my notes); NIAP Technical Community Guide (unpublished draft v0.3, May 2012)
**IN THEORY:**

**CCDB Vision vs. NIAP approach**

<table>
<thead>
<tr>
<th>CCDB Vision¹</th>
<th>NIAP Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CCDB and CCMC select technology areas, appoint technical communities, and approve final PPs</td>
<td>NIAP selects technology areas based on US government priorities, operates technical communities, and approves final PPs</td>
</tr>
<tr>
<td>Decision-making rules are determined by the technical community</td>
<td>The technical community can set some rules, but NIAP has final say on all decisions</td>
</tr>
<tr>
<td>Work in progress is open for all interested parties and is referenced on the CC portal</td>
<td>Work in progress is only available to technical community members</td>
</tr>
<tr>
<td>CC/CEM compliance and approval of extended assurance components are expressed as requirements</td>
<td>PP development lifecycle and process are specified in detail</td>
</tr>
</tbody>
</table>

¹ Vision statement for Collaborative PP and supporting document development; CCDB Report to 11th ICCC; Building CC Technical Communities - A Progress Report (D. Martin, 12th ICCC, from my notes)
IN PRACTICE:

What do TC members think?

- An unscientific survey of technical community members
  - 24 from vendors
  - 11 from labs
  - 8 from schemes
  - 4 from consultancies

- Very good response rate (36%)
- Very good balance of responding stakeholder groups
- Most responses were about NIAP TCs

- Confidentiality promised for individual answers
- Opt-in acknowledgement of participants

Thank you: Chris Brych, Erin Connor, Matt Keller, NIAP, Nithya Rachamadugu, Wouter Slegers, Alan Sukert, and all anonymous participants
IN PRACTICE:

Key NIAP results from the survey¹

- Open to all interested parties? Maybe only after “kick-off”.
  - Before that, a smaller, select group is engaged to produce a first draft PP
  - Pre-kick-off activity is not part of NIAP’s documented lifecycle and process

- Are all stakeholders fairly represented? Yes, but…
  - When NIAP is the only scheme and represents only US government customers, international perspective is limited
  - Some stakeholders are not represented in pre-kick-off activities
  - NIAP reserves the “final say” on decisions

- Is it working well? Well…
  - Leadership is a little sporadic and often doesn’t “keep things moving”
  - There is a lack of well-defined goals and plans to achieve them
  - It is unclear what is expected from each stakeholder group

¹ Additional detail on these results were presented and discussed last week at the 2nd Joint CCUF/CCDB Workshop.
**IN PRACTICE:**

**What makes this so difficult?**

- Industry and government work on many kinds of standards
  - Conformity and interoperability
  - Design and construction
  - Process and management
  - Codes and certifications

- What makes the CC different?
  1. It is for the evaluation of security
  2. Stakeholder groups have internal conflicts of interest (more than usual)
Accepted practice for evaluating the security of something involves some form of risk assessment.

Risk assessment is best tailored to the end customer – its assets, valuation, environment, threats, risk tolerance, etc. – not tailored to a technology.

Even within one national government, risk assessments are performed by agency, division, department, function…

Further, each nation has its own set of security concerns.

But we are trying to create a standard for all 26 nations.
**IN PRACTICE:**

**Internal conflicts of interest**

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Want</th>
<th>As long as it isn’t costly for us or inconvenient for our customers, and it doesn’t put us at a competitive disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors</td>
<td>Want to cooperate with other vendors to improve security for our industry and for society</td>
<td>As long as it isn’t costly for us or inconvenient for our customers, and it doesn’t put us at a competitive disadvantage</td>
</tr>
<tr>
<td>Schemes</td>
<td>Want to cooperate with all CCRA nations to improve security throughout the world</td>
<td>But our primary objective is our own national security, and do we <strong>really</strong> trust those other nations?</td>
</tr>
<tr>
<td>Labs</td>
<td>Want evaluations to be objective, measurable and repeatable</td>
<td>But not so much that it reduces our ability to differentiate or lowers barriers to entry</td>
</tr>
<tr>
<td>Consultants</td>
<td>Want to make the CC easier for developers and evaluators</td>
<td>But not so easy that they no longer need specialists like us</td>
</tr>
</tbody>
</table>

*Individually, stakeholder groups make suboptimal decisions, but it is time-consuming to reach multi-stakeholder consensus.*

---

1 This is entirely speculation on my part. Any resemblance to a particular stakeholder is purely coincidental.
Vendors, because vendors must keep everyone happy

- Vendors need to keep themselves and each other happy, otherwise the technical community will lose vendor support and collapse
- They need to satisfy the relevant schemes, otherwise their products won’t be accepted for evaluation in those schemes, and their certified products won’t be approved for procurement in those countries
- They need to satisfy the labs, otherwise evaluations will be unreasonably difficult, costly, and time-consuming
- They need to satisfy end customers, otherwise customers won’t value certified products over non-certified products
- No other stakeholder group has those motivations
- Vendors know their industry and their technology

**Vendors should be leveraged to make first-draft decisions**
**RECOMMENDATIONS**

Who should manage TCs?

- **Industry**, because industry has a broader view than individual schemes and it has a low tolerance for long-term uncertainty
  - Industry is compelled to set goals and objectives, make plans, establish schedules
  - Industry is motivated to move quickly to complete PP development projects
  - Industry can quickly mobilize resources and infrastructure
  - So far, industry-led TCs have worked pretty well

*Schemes can set parameters, ensure fairness, and provide oversight*

*Industry should be leveraged to perform day-to-day management*
**RECOMMENDATIONS**

What about that CCDB Vision?

- **Continue!** The CCDB should continue to work toward its vision of collaborative technical communities
  - Learn from the NIAP TC experiences
  - Don’t work in a vacuum, consult industry
  - **Collaborate** on the design of collaborative technical communities

  *Bring the “Common” back into the Common Criteria*
Summary

- Progress toward the CCDB vision of collaborative technical communities has been slow, but is continuing
- NIAP has moved forward with its own approach, sharing many CCDB principles but exhibiting some important differences
- NIAP’s implementation has been somewhat uneven, but industry can help
  - Vendors can streamline the PP development process by making first-draft decisions and trade-offs
  - Industry can streamline the whole TC process by managing the TCs
- Technical communities are good for the CC, and the CCDB should continue its work toward a common model for collaborative PP development
Questions?