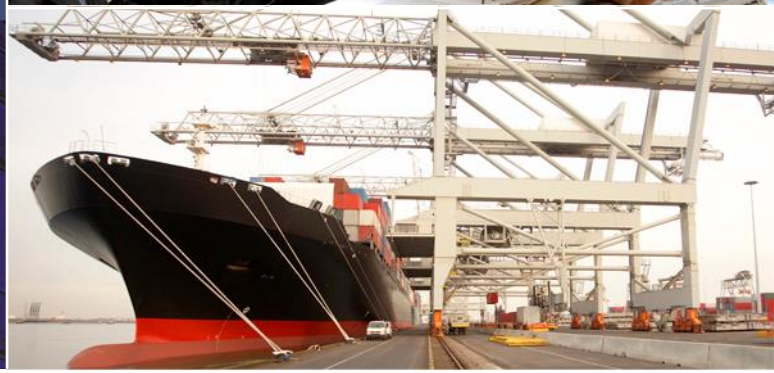

Making A Better Standard Protection Profile

Tony Apted, James Arnold, Tammy Compton

19 September 2012

SAIC
From Science to Solutions

Synopsis

- Background
- Current Examples
- Way Forward
- Software Devices Protection Profile (SDPP) Example
- Conclusions and recommendations

Background – History

In the United States, the Common Criteria Evaluation and Validation Scheme (CCEVS) is moving away from evaluations against defined *Evaluation Assurance Levels (EALs)* in favor of so-called *Standard Protection Profiles, Extended Packages*, and *Tailored Assurances*.

Evaluation Assurance Levels are held to be misleading, ineffective, and to yield generally inconsistent results.

- It is generally held that consumers assume that, for example, EAL 3 is better than EAL 2, regardless of such factors as security functional claims, security functions, or even the applicable technologies, which may not be comparable.
- Despite being evaluated, even at EAL 4 and higher, evaluated products remain vulnerable as evident in bugs reported even after having completed evaluation.
- One or more of the Common Criteria Schemes has admitted an inability to ensure consistency among their own evaluations, and ensuring consistency across Common Criteria Schemes is a greater challenge that has not been met.

Background – History

In contrast, Standard Protection Profiles, Extended Packages, and Tailored Assurances are being promoted to:

- Simplify the problem by minimizing functional requirements to focus on key security functions.
- Eliminate assurance levels in order to define and focus on best and achievable assurance activities.
- Better objectify the problem with more clear and concise guidance to evaluators.
- Bring transparency to the evaluation process/activities to help consumer understanding.

Background – Problem

The approach to developing the Standard Protection Profiles, Extended Packages, and the recent Tailored Assurance Package has involved a number of Technical Communities. However, the Technical Community concept has a number of challenges:

- Technical Communities have been operating in vacuums.
  - Some Technical Communities are essentially closed to the evaluation community at large.
- Technical Communities are not necessarily orthogonal.
  - There are common security features found among varying technologies.
- Technical Communities do not have common management/leadership.
  - Overall direction, guidance, organization, etc. could vary significantly across communities.
- Technical Communities do not have common goals.
  - The goals depend largely on the leadership and majority/most vocal participants.
- Technical Communities have been limited by government.
  - Community outputs (e.g., protection profiles) have been subsequently modified

CCEVS has a web page summarizing the Technical Community concept, purpose and approach, protection profile content, community organization, and guiding principles for the organization. However, it doesn't address the problem of consistency among the products of the communities – Protection Profiles and Extended Packages.

http://www.niap-ccevs.org/evolution/communities/

Background – Consistency Goal

While the change in direction represented by Standard Protection Profiles, Extended Packages, and Tailored Assurance might, in general, serve to help solve some of the purported Common Criteria problems, the distributed Technical Community development model introduces new challenges, particularly in the area of consistency across communities and their products. We see three levels of consistency:

- The Common Criteria and Common Evaluation Methodology apply uniformly (normalized by EAL) across all evaluated products on an international basis (for convenience, we refer to this as C^0).
  - Not acceptable due to inability to bring a level of consistency acceptable to all stakeholders.
- Standard Protection Profiles and Extended Packages apply uniformly across all conforming products (C^1).
  - This approach arguably improves consistency among products evaluated using a given Standard Protection Profile or Extended Package due to the explicit and objective guidance offered therein.
  - This approach doesn't ensure consistency across products evaluated using different Standard Protection Profiles or Extended Packages. Exceptions involve intersections where Standard Protection Profile content is borrowed or referenced and, in effect, reused.
- The idea proposed herein, where rules and guidelines need to be established to bring consistency across Standard Protection Profiles and Extended Packages (C^2).
  - The draft Tailored Assurance Package is a step in that direction.

Current Examples – Network Devices Protection Profile

The “Security Requirements for Network Devices” Protection Profile (commonly referred to as the Network Devices Protection Profile, or NDPP) and other derivative Protection Profiles (PPs) are essentially standard Common Criteria (CC) PPs with the following primary differences:

- The Security Problem Definition (SPD) is presented both in symbolic terms (Annex A) and in informal English prose intended to better serve the broader Security Target (ST) reading audience.
- Explicit assurance activities are defined for Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) to better direct evaluators to remove some subjectivity and also to help the broader ST reading audience understand what was actually done during the evaluation (i.e., provide transparency).
- Mappings are provided to other standards to help justify the choice of SFRs in the PP.
- Optional requirements are identified or defined to offer *some* flexibility where conforming Targets of Evaluation (TOEs) might exceed the basic SFRs in the PP. Note that unlike standard CC PPs, conforming TOEs are not free to add SFR claims outside those defined in the PP.
- In some cases, Scheme-specific requirements are included that go beyond evaluation work performed by a Common Criteria Test Laboratory (e.g., NSA evaluation of entropy design).

Current Examples – Extended Package (EP)

So far, there is only a single Extended Package – the *NDPP Extended Package Stateful Traffic Filter Firewall*.

- It builds on (and depends directly on) the NDPP, without copying its content, and has a similar organization, but has the following notable differences:
  - It assigns assurance activities specifically to Security Target and guidance document content evaluation and testing.
  - It adds auditable events for FAU_GEN.1 and management functions for FMT_SMF.1 both defined in the NDPP.
  - Unlike the NDPP, it offers rationale that explicitly map threats and assumptions to security objectives.
  - There are no Annexes, though NDPP Annex A is similar to the Rationale.

A general idea behind the Extended Package (EP) concept is to minimize the work to develop the EP and to avoid redundancy that could lead to inconsistencies (e.g., when the NDPP independently evolves).

Current Examples – Tailored Assurance Package (TAP)

- Security Assurance Requirements (SARs)
  - Assurance Activities (per component)

The objective of the Tailored Assurance Package (TAP) is to replace the former EAL2 upper assurance bound for CC evaluations conducted under CCEVS. As such, it comprises a selected set of CC assurance requirement components refined with assurance activities defined for each SAR.

The TAP has been developed to accommodate evaluations of products for which there currently is no suitable PP . However, it would seem sensible to ensure that the work of Technical Communities producing PPs and EPs should be consistent with the TAP.

At the time of the review (mid August 2012), the TAP was a work in progress out for limited review. As such, it may have evolved to have additional content.

Way Forward – Previous Recommendations

A presentation from the Norway conference identified a number of problems that were revisited last year in a review of the Network Devices Protection Profile (NDPP), leading to the following recommendations:

- Emphasize key requirements for the core security problem
- Keep PPs simple and to the point
- Publish PPs that are stable and as objective as possible
- Make sure that PP content is CC conformant
- Stray away from the CC only where absolutely necessary
- Use EPs where possible to promote reuse of established content
- Allow flexibility in meeting PPs
- PPs should be evaluated and certified/validated

Such recommendations bear repeating until they are ingrained in the evolving CC paradigm. While this proposal doesn't address all these recommendations, it adopts them to the extent applicable.

Way Forward – CCEVS Guiding Principles

As mentioned earlier, the CCEVS has a web page summarizing, among other things, guiding principles.

http://www.niap-ccevs.org/evolution/communities/

- Consistency
- Transparency
- Scalability
- Improved "time to market"
- Leverages industry expertise
- International perspective

These all seem like reasonable guiding principles and have been adopted when crafting this proposal.

Way Forward – f(C^0,C^1) → C^2

As summarized earlier, C^0 (Common Criteria and Common Evaluation Methodology) has been rejected in favor of C^1 (Standard Protection Profiles, Extended Packages, and Tailor Assurance).

C^2 is essentially a function of C^0 and C^1, where rules and guidelines are used to extend the isolated consistency of C^1 across communities, so that all products would be treated consistently akin to C^0, but better.

C^2 is defined as:

- **A set of rules or requirements** that should be satisfied by the products (Protection Profiles and Extended Packages) of Technical Communities
- **A set of guidelines** that should serve to direct choices or preferences made by Technical Communities.

Note that the following rules are directed at the content of PPs and EPs and the following guidelines assume the published Technical Community model and delve into the working of each such community.

Way Forward – C^2 Rules

1. Each PP shall conform to the Common Criteria APE requirements.
   - This might seem obvious, but given the exceptions in the available examples it is important to reiterate.
2. Each Security Functional Requirement shall be tested.
   - If a requirement cannot be tested (or subject to a suitable alternative), it should not be included. Note that the new approach seems heavily biased toward assurance born of testing.
3. Each assurance activity shall be unambiguously associated with either a requirement element or component.
   - Assurance activities can be defined for both functional and assurance requirements and can be defined at the element and component level. Assurance activities are refinements of, and not replacements for, identified requirements.
4. Each assurance activity shall be associated with only one specific aspect of the evaluation (e.g., Security Target, design, guidance, testing, vulnerability analysis).
   - Appropriate grouping or categorization of assurance activities will facilitate better evaluation organization and planning, leading to more consistency across evaluations. This correspondence should be implicit for security assurance requirements.

Way Forward – C² Rules

5. Each assurance activity shall be objectively stated and identify applicable inputs, actions, and outputs of the activity.
   - The more subject to interpretation, the less chance to achieve consistency. It should always be clear what materials an action is based on and also what should be produced as a result.
6. Each assurance activity shall not require custom (e.g., CC specific) input material beyond references, mappings, and the Security Target.
   - One of the objectives is to minimize the need for the costly development of custom evaluation artifacts to support evaluations.
7. Each assurance activity shall be designed to yield cost effective and meaningful assurance when completed by an evaluator.
   - The point is to avoid activities that are exceptionally onerous and don't clearly yield any security assurance (e.g., review of arbitrary statements about RFC conformance).
8. Each assurance activity shall be designed only to be performed by Common Criteria Testing Laboratories in order to reach evaluation conclusions.
   - It is important from an international perspective, that special conditions or external evaluation work not be included that may be limited to a specific nation, such as an explicit requirement for FIPS certification, for example.

Way Forward – C² Rules

9. Each assurance activity shall not extend any TOE functional requirements.
    - Any intended requirement extensions should be included in the requirements directly (e.g., as refinements). Rather, assurance activities should serve to interpret requirements and impose requirements on the work to be performed by evaluators.
10. Each deviation from these rules shall be justified.
    - If exceptions are made, it needs to be clearly and reasonably explained why they were necessary and why they should be acceptable.

Way Forward – C² Guidelines

1. A PP should be developed only when an EP will not do.
   - The general preference is to continuously build on the existing body of PPs and Eps, extending rather than reproducing or recreating where possible.
2. PPs and EPs should not be created when the potential targets could be accommodated by adding optional claims in an existing PP or EP.
   - Optional components should be used to their best advantage to accommodate technology variations without necessitating additional PPs or EPs where possible.
3. PPs and EPs should be developed with core (i.e., non-optional) requirements that are truly central and necessary to the secure operation of that technology.
   - PPs and EPs should be broadly reusable and applicable and as such it is important to ensure the core requirements are really necessary.
4. PPs and EPs should be developed with optional requirements designed to address as many known technology variations as deemed reasonably possible.
   - Following on the previous guidelines, it should be desirable to account for as many variations as possible to broaden the use of each PP and EP.

Way Forward – C² Guidelines

5. PPs and EPs should reuse material from already approved and accepted PPs, EPs, and potentially other sources (e.g., the Tailored Assurance Package) where possible.
   - While building on PPs and EPs is important, obvious benefits can be gained from using available materials where they may fit.
6. PPs and EPs should use extended requirements only where necessary or some obvious (or reasonably stated) benefit exists.
   - If we're not going to use the CC, then we should agree to abandon it. The CC has history and community knowledge and should not be discarded easily.
7. PPs and EPs should not stifle innovation by restricting conforming STs and TOEs to single, specific mechanisms when alternative mechanisms should prove acceptable.
   - For example, the PP or EP should not restrict the TOE to only a password-based authentication mechanism when digital certificate or token-based mechanisms can provide the same security functionality.

Way Forward – C² Guidelines

8. PPs and EPs should be developed according to a well-defined schedule, defining review periods and revision milestones.
   - It is generally important that the community and potential users of a given PP or EP are informed about its development so good business decisions can be made about when and whether to engage in use of the PP/EP (e.g., to develop a Security Target).
9. PPs and EPs should be evaluated to ensure that all the rules and requirements are actually satisfied.
   - The alternative of leaving this to TOE developers in the context of their evaluations is unappealing and contradicts the goals of PPs and EPs.

Software Devices Protection Profile (SDPP) Example

A draft Software Devices Protection Profile (SDPP) has been developed as a worked example and to further serve as an outline and general model for the C^2 approach.

It can be found at the following URL:

http://somewhere-on-google-docs

Note that it has not been developed by an actual Technical Community and is not approved by any Scheme.

Conclusions and recommendations

It is recommended that the National Information Assurance Partnership (NIAP) Steering Committee for Technical Communities should consider the C^2 rules and guidelines proposed herein and further develop them into a definitive set of instructions and guidance for Technical Communities at large.

Contacts

Tony Apted
James Arnold
Tammy Compton

SAIC Accredited Testing & Evaluation Labs

http://www.saic.com/infosec/testing-accreditation/common-criteria.html