Operating System Protection Profile and Community
–
One Face of the new Approach to PPs

Matthias Intemann

14th ICCC Orlando
September 11th, 2013

Basics

- ❐ OSPP 3.9 Draft
  - ❐ “Classical” PP without EAL claim, but individual SARs
  - ❐ Additional supporting guide with
    - ❐ Fundamental clarifications
    - ❐ Activities
- ❐ Contributors
  - ❐ BSI / NIAP
  - ❐ atsec / SAIC
  - ❐ IBM / Microsoft

- ❐ Time line:
  - ❐ 2010
    - ❐ OSPP 2.0 (BSI-CC-PP-0067-2010) with extended packages
    - ❐ GPOSPP 1.0
  - ❐ 2011
  - ❐ 2012
    - ❐ OSPP 3.9 draft with additional guide, containing activities
  - ❐ 2013
    - ❐ Forming community

What was wrong with the old ones?

- OSPP 2.0 characteristics
  - “works for me”
  - As good as every other average certified BSI PP
  - Introduced Extended Packages for modularity
  - Compromise between one PP fits all OS and containing SARs/SFRs actually needed by users

- Implications
  - Does not work for the whole CCRA
  - ☺
  - Will still be available in the future
  - Have we left someone important behind?

So you started Harmonization?

- When OSPP 3.9 development started, there was no:
  - cPP
  - CCMC Vision Statement
  - Technical Community definition
- We had:
  - Two competing PPs, splitting vendors and labs
  - Many certified Operating Systems following a (GP)OSPP
  - A shared understanding, what functionalities an OS should offer
- “Works for me” is not a sufficient basis for a PP covering key technologies, so we needed harmonization and a “Works for the important customers”

Is a PP like a product?

- ❒ For big amounts: yes.
- ❒ Product Management
(personal lessons learned for small products)
  - ❒ Know your Customers
  - ❒ Don't change more than you can manage
  - ❒ Make the customers understand the changes and help them through the update phase
  - ❒ Always improve the product from every key customer's perspective
  - ❒ Know your competing Partners
- ❒ PPs are being developed and should be maintained. They have customers and are being abandoned if badly crafted.

What went wrong?

- Who says anything did?
  - The outcome is a draft, meant for first gathering of experiences in trials. It is not “fit for production”.
  - Parts are just meant for simply trying things out.
  - Community to do the polishing of making it final was always intended.
  - It was an important project for exchange of positions.
- OSPP as a product . . .
  - We did introduce too many new aspects at once. We have too little experience with too many paradigms.
  - Politics dictated part of the approach, rather than customer needs. But – who are the customers again?
  - Does the vendor support the changes?
  - Which PP should the vendor use?

What are the issues?

- ❐ Guide, especially the Activity-Section, is not complete and has errors (Activities mapped to wrong SFR and SAR, ...)
- ❐ Vulnerability List is missing
- ❐ PP is not evaluated (makes ST evaluation harder, missing mappings, etc.)
- ❐ Approaches are chosen partly to show if approach works or does not (mostly whenever a discussion has lead to a compromise rather than agreement)
- ❐ Community (pilot group in this case) is more consuming than constructive
- ❐ TSS and Guidance are meant to replace ADV evidence
- ❐ Assurance discussion not satisfied (only least common denominator agreed upon)

What will you do about it?

- The Community Cloud within the Cyberspace will take care of all those issues. It just takes time.
- If you have trouble using the draft, you have to join the community.
- There is no “you” but a “we”.

Q&A

Thank you for listening!

Contact

Federal Office for Information Security (BSI)

Matthias Intemann
Godesberger Allee 185-189
53175 Bonn
Germany

matthias.intemann@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de