Experience with OSPP Evaluations

Gerald Krummeck, atsec information security

ICCC 2012, Paris

2012-09-19

Experience with OSPP Evaluations

Agenda

- A short OSPP history
- Evaluations using OSPP
- Experience and Pitfalls
- Lessons Learned for OSPP‘s future

How It Started

A short history of OSPP

Development suggested at the ICCC in Rome (2007)

- CAPP and LSPP functionality no longer address core functions of modern operating systems
- Suggestion was to develop a “base PP” and “extended packages”
  - Extended packages contain not only SFRs but also a “security problem definition” part defining what threats and objectives are addressed by the package
- Suggested to develop a framework how extended packages can be combined with the base PP

Scope

A short history of OSPP

- PP for general-purpose operating systems
- Modern operating systems, realistic environments
- Servers and well-managed workstations
- Baseline: agreed functionality set among developers
- Provide more than a baseline
  -> extended packages for additional functionality

The BSI OSPP

Sponsored by our friendly neighborhood CB

- Development started August 2008
- Input/Feedback from OS experts
  - „Technical community“ was not invented yet…
- Evaluated /certified in 2010 with extended packages:
  - Advanced Management
  - Advanced Audit
  - General Purpose Cryptography
  - Extended Identification and Authentication
  - Integrity Verification
  - Labeled Security
  - Trusted Boot
  - Virtualization

Evaluations with OSPP

	BASE	Advanced Audit	Advanced Management	Cryptography	Extended I&A	Integrity Verification	Labeled Security	Trusted Boot	Virtualization
AIX V7.1	🟥		🟥	🟥		🟥	🟥		🟥
RHEL v6.1	🟥	🟥				🟥	🟥		
SLES 11	🟥								🟥
z/OS V1R11 - 13	🟥				🟥		🟥		
z/VM V5.1	🟥						🟥		🟥

Lessons Learned (1)

It’s the little differences …

- Operating systems are **very** different , as are vendors, markets and customers
  - Vendors address different markets and want to distinguish themselves (extended packages, additional SFRs)
  - need for flexibility without settling for the least common denominator only
  - government requirements don‘t fit everybody (in fact, they don‘t fit most customers)
- Assurance
  - EAL4 accepted and established in the market

Pits to Fall Into

Cryptography, an enigma of its own…

- Hardware support (IBM zSeries, Intel, …)
  - Crypto functions performed outside of the TOE
  - OS Developers do no control HW implementation
  - No EAL4-level analysis possible
- Fallback to SW implementation not acceptable to customers
- Need to accept crypto outside of TOE
- Solution: Require communication protocols (IPSec, TLS, SSH) without specific SFRs on crypto (FTP_ITC, no FCS)
- Composition needs to be addressed for SW products
- RNGs: already worded for scheme-specific solutions

More Pitfalls

Your management is my access control

- Right to manage a certain function implemented by access rights to configuration file
- One security function implemented by another
- Management detached from security function (same for audit)
- Possible solution:
  - SFRs for security functions describe their management, too
  - FMT SFRs for global management aspects only

Dealing with Complexity

Having a meaningful TSS

- Squeezing all functional detail into SFRs does not help
  - Comparing SFRs will be impossible
  - Sometimes hard to clearly describe within prescribed SFR wording
- Possible Solutions
  - Use extended SFRs (issue: consistency between PPs)
  - Describe implementation more detailed in TSS
  - Example z/OS: Unique tag for testable statements
    - Anchor for mapping for testing, design doc, guidance, etc.

My Lessons Learned for OSPP Harmonization Effort

Disclaimer: My Lessons only ☺

- Base and extended packages are useful concepts
- Discussion in Technical Community will be critical success factor
- Be careful not to specify implementation details in PPs
  - Even if you know Windows and Linux, that‘s not the whole story yet
- What‘s easy in a specific case may be hard to generalize
  - „I know it when I see it“ (Justice Potter Stewart, 1964)
- Document evaluation work and rationale for verdicts in enough detail to allow judgment by third party
- More guidance on specific evaluation tasks would be helpful
  - Don‘t expect enough detail to program your evaluation robot
- Even if you don‘t like it: Nothing beats experience