

Operating System Protection Profile

Modularity and Flexibility using the Common Criteria

Matthias Intemann

Presenter:

Gereon Killian, Head of Certification

Federal Office for Information Security (BSI), Germany

11th ICC

Antalya, September 22nd, 2010

Agenda

- ❑ Operating System Protection Profile (OSPP)
 - ❑ Goals
 - ❑ Results
- ❑ Results regarding the Common Criteria
 - ❑ Solutions
 - ❑ Related Issues
- ❑ Outlook
 - ❑ Operating System Protection Profile
 - ❑ Community
- ❑ Conclusion

OSPP Goals

- ❑ Scope
 - ❑ Servers and workstations in a professional, well-managed environment
 - ❑ Main focus on software components
- ❑ Forming **common base** of security functions
- ❑ Adding **optional packages** of security functions
- ❑ Taking networking and **distributed security** into account
- ❑ Comparable security, independent from platforms
- ❑ Addressing needs of users, developers and ITSEF
- ❑ Independence from other certification standards but avoid blocking (e.g. by enforcing certain cryptographic algorithms)
- ❑ Full recognition under CCRA (**no extended SARs**)

OSPP Approach

- ❑ Building and involving **OSPP forum**, which consists of
 - ❑ OS vendors (all relevant architectures represented)
 - ❑ BSI (project lead)
 - ❑ NIAP
 - ❑ OS experienced evaluation facility
 - ❑ and others.
- ❑ Addressing use-cases using **optional** Extended Packages (e.g. Labeled Security)
- ❑ Extended Packages **dependent** on Base Package,
- ❑ ... allowing **dependencies between** packages and
- ❑ ... all being **certified as part of the OSPP**

Security Functionality OSPP Base Package

- ❑ Identification and authentication (I&A)
 - ❑ Users (human or other systems) may be anonymous
 - ❑ I&A can be remote (I&A client functionality)
 - ❑ Password mechanism is mandatory, others optional
- ❑ User Data Protection (storage and basic packet filter)
- ❑ Auditing
- ❑ Cryptographic Services (TLS, SSHv2, IPSec with IKE)
- ❑ Trusted Paths / Channels
- ❑ Security Management
 - ❑ Selected users may use administrative functions
 - ❑ Delegation of authority
 - ❑ Localised and centralised management

Security Functionality OSPP Extended Packages (I)

- ❑ Labeled Security (LS)
 - ❑ Multi-Level Security (Bell-La Padula model)
- ❑ Advanced Audit (AUD)
 - ❑ Audit server functionality
- ❑ Extended I&A (EIA)
 - ❑ I&A server functionality
- ❑ General Purpose Cryptography (CRYPTO)
 - ❑ Providing cryptography to user
(Candidate for future Base Package)

Security Functionality

OSPP Extended Packages (II)

- ❑ Virtualization (VIRT)
 - ❑ Separation and management of compartments
 - ❑ Hardware virtualization mechanisms *and* OS functionality virtualization mechanisms are supported
- ❑ Advanced Management (AM)
 - ❑ Advanced delegation and approving of tasks (four-eyes principle)
- ❑ Integrity Verification (IV)
 - ❑ Verifying Integrity of TSF code, TSF data, and user data
- ❑ Trusted Boot (TB)
 - ❑ Verifying Integrity of IV-module before invocation using trust anchor (read-only TSF code and data)

OSPP from a formal perspective

- ❑ OSPP Base Package is **obligatory**
- ❑ OSPP Extended Packages are **optional**
- ❑ OSPP Extended Packages contain **SFRs and SPDs**
(no SARs allowed in **functional packages** according to CC)
- ❑ Conformance Claim (shortened example):

Operating System Protection Profile with
OSPP Extended Package – Labeled Security and
OSPP Extended Package – Extended Identification and Authentication

- ❑ **Dependencies** between Extended Packages
(TB depends on IV)
- ❑ Extended Packages are evaluated with Base Package
 - ❑ Options are taken into account
 - ❑ **No existing Work Units** → rational for possible combinations in ETR and Certification Report of PP

Common Criteria Solutions (Functional Packages)

Definition from CC V3.1R3 Part1:

A package is a named set of security requirements. A package is either

- a functional package, containing **only** SFRs, or
- an assurance package, containing **only** SARs.

- ❑ Interpretation with CP for clarification:
 - ❑ “only” is meant to **exclude SARs** from functional packages
 - ❑ Functional packages can consist of **SFRs and a (partial) SPD**
- ❑ Also solved: PP with optional packages, as conformance to packages is claimed separately

Common Criteria Solutions (Evaluation of Packages)

Evaluation of functional packages

- ❑ Packages have been evaluated as **part of the PP**
- ❑ Dependencies and possible combinations are **additionally analysed** during evaluation and documented in ETR and Certification Report
- ❑ → If packages are frequently used, we probably have to change the CEM regarding evaluation of packages in APE

Common Criteria Solutions (Conformance to Packages)

Confirmation of functional package conformance

- ❑ At the moment, ASE_CCL and APE_CCL are interpreted to include all parts of packages, even though not explicitly listed
- ❑ Provided CP ...
- ❑ ... includes changes to CEM for clarification regarding refinement of functional packages
- ❑ ... takes packages obsoleting assumptions into account
- ❑ ... removes hierarchical functional packages from CEM
- ❑ ... removes augmentation on functional packages, as those always are augmented

Common Criteria Solutions (Scheme Specifics)

- ❑ Dealing with scheme specific requisitions without blocking other schemes
- ❑ The extended component FCS_RNG.1 is defined and evaluated with OSPP but not used in Security Requirements

Excerpt from OSPP, V. 2.0:

ST Author Note:

If the key generation is based on a random number generator or random bit generator, national schemes may require additional extended SFRs to be claimed. For example, in the German scheme, the ST author shall claim FCS_RNG.1 from the version of AIS20/AIS31 current at the time of ST release published by the German scheme.

ST Author Note:

If the national scheme does not define any specific evaluation requirements for random number generators, the extended component FCS_RNG.1 defined with this PP has to be added to the ST by the ST author.

Common Criteria Related Issues

- ❑ Evaluation and certification of packages is only possible as part of an ST or PP but limited to the elements used, without taking package relations into account
- ❑ Conditional relations of SFR to the product is not yet addressed (if TOE implements I&A by username / password, include FIA_UAU.7)
- ❑ Composition of TOEs on top, re-using security functionality (e.g. crypto-lib from the OS), is not well addressed (ACO does not take re-usage into account!)
- ❑ Supporting Documents to strengthen faith in OS evaluation at EAL 4 are needed. Is this a job for the OSPP Forum?

Outlook

OSPP and Community

- ❑ Maintenance of OSPP Base and OSPP Extended Packages
- ❑ Additional Extended Packages
- ❑ Improvement of PP-Acceptance by OS customers
- ❑ Improving CC regarding packages as mechanism for optional elements and as structure elements
- ❑ Using SFs through non-TOE Applications (e.g. DB on top of OS)
 - Comparable to Smart Card Evaluations (Composition)?
 - Main issue is to use Security Functionality originating in the platform as part of the application security (e.g. I&A)
- ❑ Supporting Documents for Assurance regarding complex software products
- ❑ Analysing experiences from using OSPP in the community
(one certificate issued, more to foresee)

Conclusion

- ❑ OSPP offers
 - ❑ Comparability
 - ❑ Flexibility
 - ❑ State-of-the-Art security functionality
 - ❑ International recognition (CCRA)
 - ❑ Takes other PPs and certification standards into account
 - ❑ Meeting of vendor *and* market requirements
 - ❑ Optimisation of evaluation and certification work
 - ❑ Community for maintaining OSPP
- ❑ OSPP does not offer
 - ❑ Composite evaluation of applications on top of operating systems
 - ❑ Supporting Documents

Contact

Bundesamt für Sicherheit in der
Informationstechnik (BSI)



Matthias Intemann
Godesberger Allee 185-189
53175 Bonn
GERMANY

Protection Profiles:
<https://www.bsi.bund.de/Schutzprofile>

zertifizierung@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de