Trial use experiences with ASE and APE for the new CC EAL1 concept

Thomas Borsch

Bundesamt für Sicherheit in der Informationstechnik /
Federal Office for Information Security

6th ICCC / 2005-09-28

Presentation Contents

- Motivation for Low Assurance PPs/STs
- Course of events & the BSI Trial Use Project
- The new ASE/APE EAL1 Concept
- PPs defined in the Trial Use Project and PP usage
- Trial Use results

Motivation

- EAL1 evaluations do not need a full-scale ST/PP
  - Too complex to be written by a developer
  - Too expensive to be evaluated at an EAL1 level
  - Too difficult to be understood by an end user
- The evaluation effort ratio between ST/PP and the rest of EAL1 is adverse
  - CEM2.2: 78 ASE work units vs. 36 work units related to other EAL1 SARs

This leads to the following conclusion:

Conclusion

Simplified EAL1 ASE/APE would
reduce work without loosing assurance

CC could enter new markets
as small to medium-sized vendors
would be able to have their products certified

Increased number of certified products would enable
more secure IT infrastructures

Course of Events

- 2003: Rewrite of the ASE/APE Criteria under sponsorship of NLNSCA (lead nation) and BSI
- 01/2004: New ASE/APE Criteria available for trials
- 02/2004: Start of BSI ASE/APE Trial Use Project
- 02/2005: Final results of Trial Use Project
- 05/2005: Incorporation of trial results into CC3.0 ASE/APE

Scope of BSI Trial Use Project

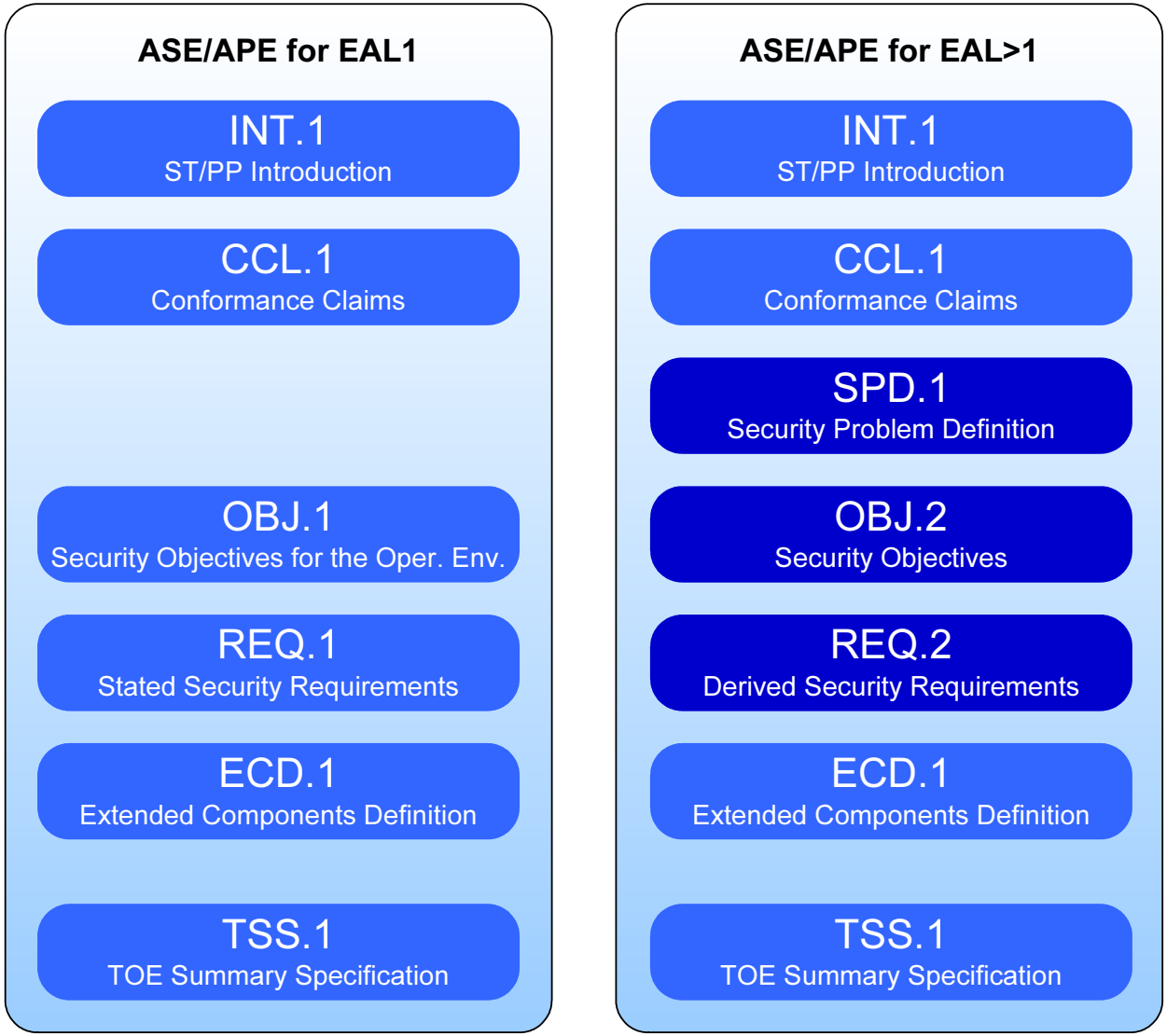
- Validation of CC2.4 Low Assurance (EAL1) Concept:
  - Definition / Evaluation and Certification of four Protection Profiles according to CC 2.4 EAL1
  - Involvement of BSI accredited Evaluation Labs
  - Evaluation of PP conformant products (preferably two)
  - Involvement of Product Vendors
  - Analysis of the CC2.4 ASE/APE Criteria and the CEM
  - Comparison of the efforts (CC2.1 vs. CC2.4/3.0) to be spent for development and evaluation of EAL1 PPs

CC2.2 → CC2.4 → CC3.0

- Common Criteria Version 2.2:
  - Bases entirely on CC2.1
  - Incorporates a number of Interpretations
- Common Criteria Version 2.4:
  - Has a new ASE/APE concept compared to CC2.2
  - Uses Part 2 of the CC2.2
  - Small adaptations in several classes (e.g. ADV, ATE, ...) to harmonize them with the new ASE/APE concept
- Common Criteria Version 3.0
  - Same ASE/APE concept as CC2.4 with minor changes
  - Modified/updated classes ADV/ALC/AGD/AVA/ATE

New ASE/APE Concept

ASE/APE is leveled



New ASE/APE Concept

EAL1 ASE/APE

- No Security Problem Definition
  i.e. no Assumptions, Threats and OSPs
- Only Security Objectives for the Operational Environment
  i.e. no Security Objectives for the TOE
- SFRs only have to be stated
  i.e. no need to consider Dependencies
- No Rationales
  i.e. no need to argue why a Threat is covered by an Objective which is fulfilled if a SFR is implemented by the TOE
- Other assurance components are the same for all EAL

Trial Use LAPPs

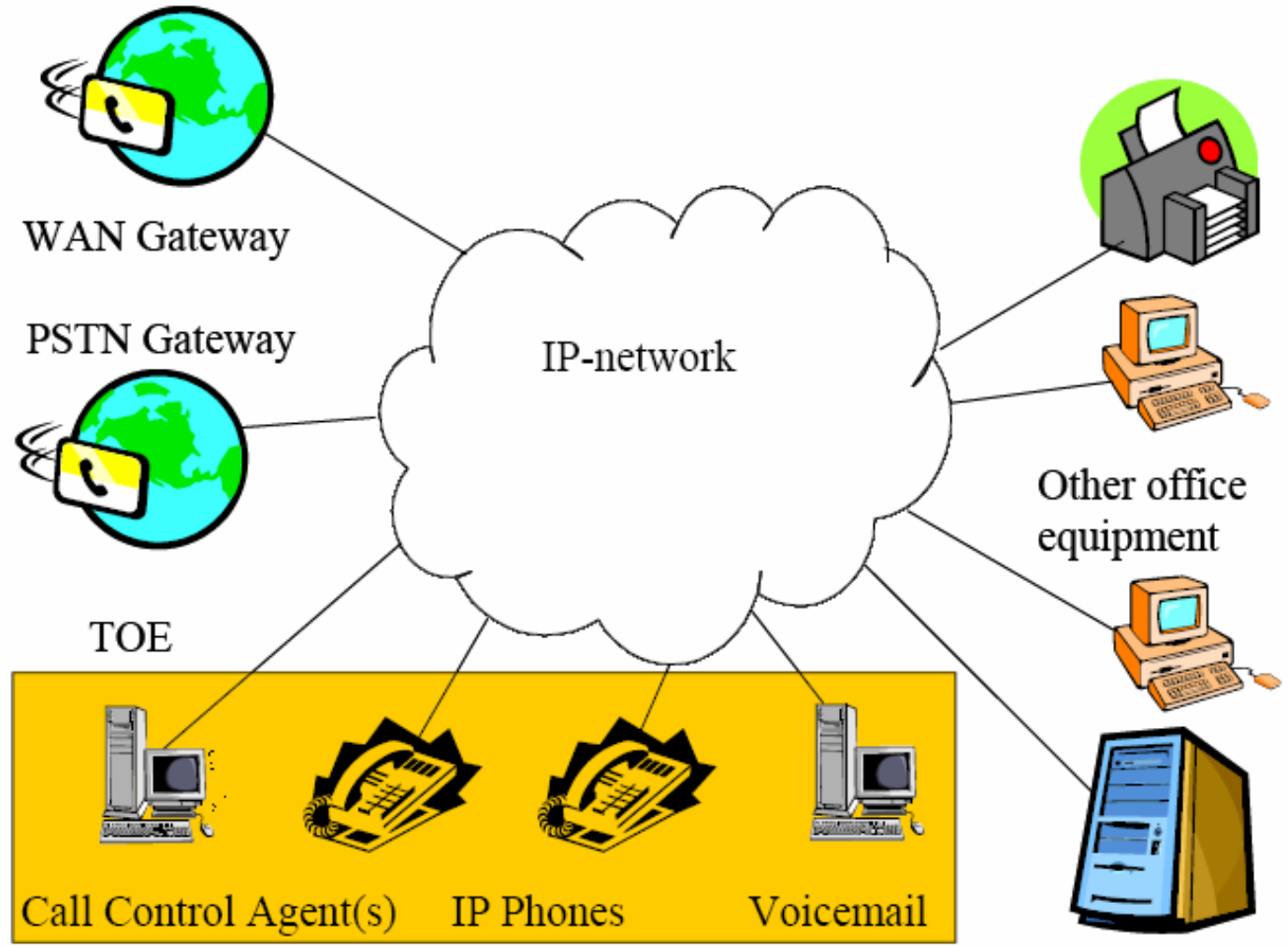
- PPs developed, evaluated and certified as part of the ASE/APE trial project:
  - PP for VoIP Infrastructures
  - PP for VPN Gateways
  - PP for Personal Firewalls
  - PP for Photocopier Devices

The PPs in more detail:

LAPP - VoIP Infrastructure

- Title: LAPP for a VoIP infrastructure, Version 1.1
- Certification ID: BSI-PP-0012-2005
- Conformance Claims:
  - CC2.4, Release 256 + Interpretations, Part 2 and 3 conformant, EAL1
- Functionality:
  - Restricting phone calls to certain numbers (and change of restrictions)
  - Management of Users and Telephones
  - Logging of connection information
  - Storage and secure retrieval of voice mails

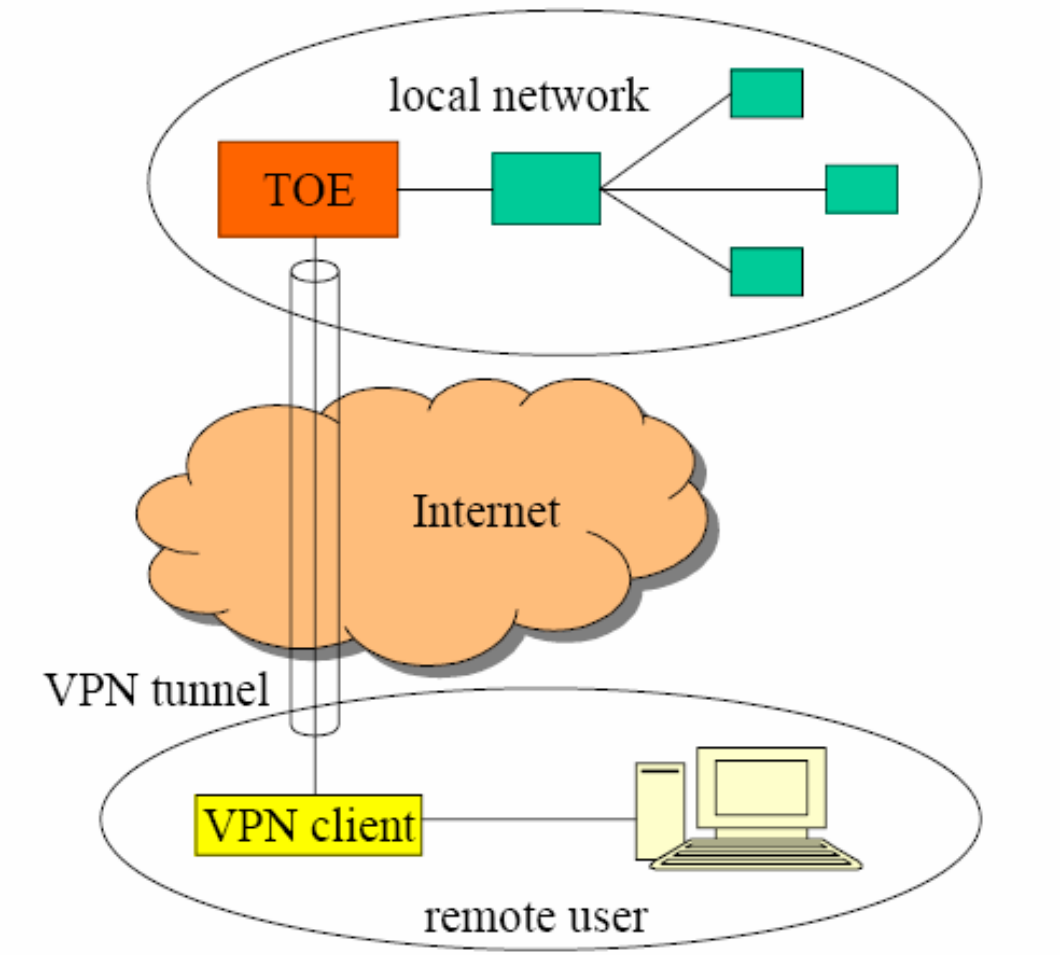
LAPP - VoIP Infrastructure



LAPP - VPN Gateway

- Title: LAPP for a VPN Gateway, Version 1.4
- Certification ID: BSI-PP-0013-2005
- Conformance Claims:
  - CC2.4, Release 256 + Interpretations,
    Part 2 and 3 conformant, EAL1
- Functionality:
  - Identification and authentication of remote user/networks
  - VPN Tunneling
  - Management

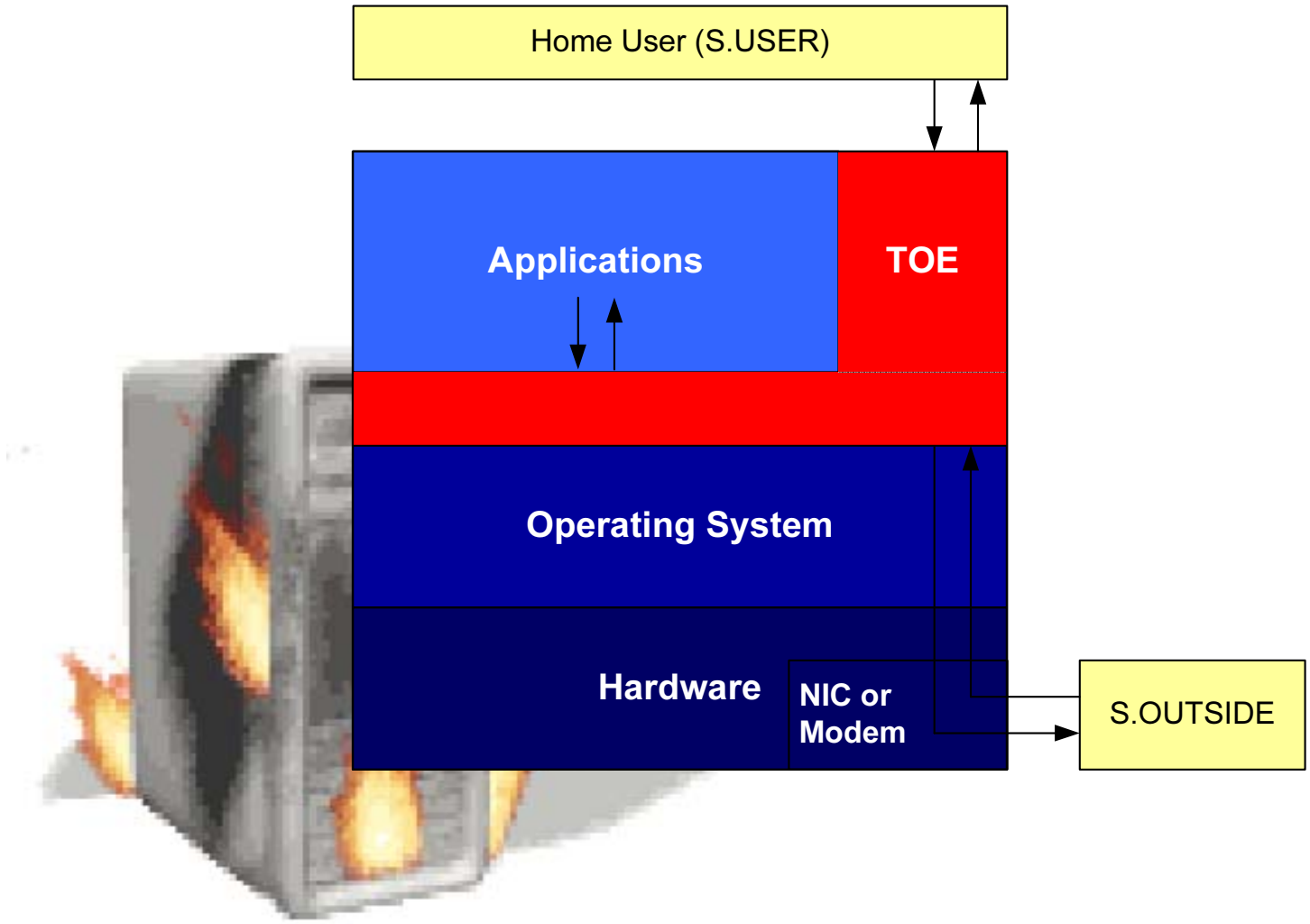
LAPP - VPN Gateway



LAPP - Personal Firewall

- Title: LAPP for a Software Based Personal Firewall for home Internet use, Version 1.2
- Certification ID: BSI-PP-0014-2005
- Conformance Claims:
  - CC2.4, Release 256 + Interpretations, Part 2 and 3 conformant, EAL1
- Functionality:
  - Regulate incoming and outgoing traffic
  - Management of rule set
  - Warning of the user
  - Event Logging

LAPP - Personal Firewall



LAPP - Photocopier Device

- Title: LAPP for a Office Based Photocopier Device, Version 1.3
- Certification ID: BSI-PP-0015-2005
- Conformance Claims:
  - CC2.4, Release 256 + Interpretations, Part 2 and 3 conformant, EAL1
- Functionality:
  - Object re-use (residual information is not retained)
  - No leakage of information (except printing it on paper by request of the user)

Using the PPs

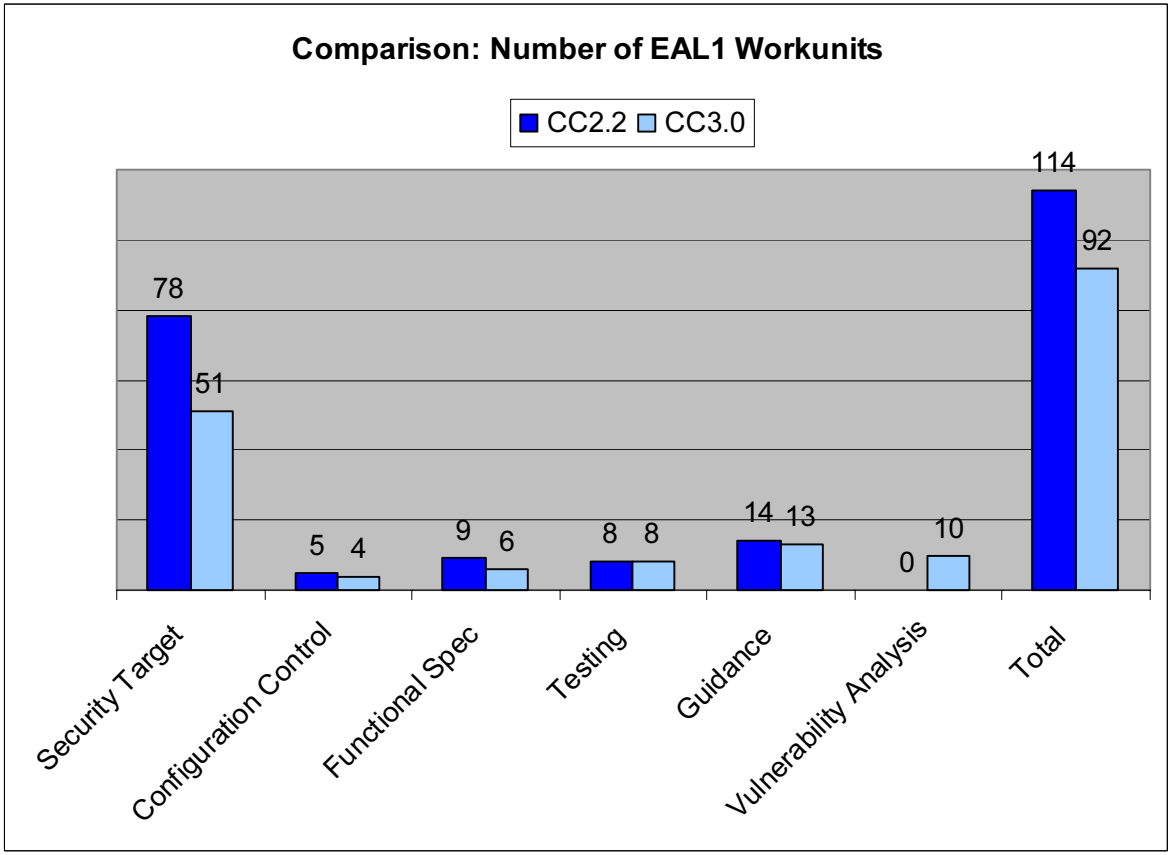
- Two products have been evaluated against the PPs:
  - A VPN gateway of a small vendor
  - A VoIP Infrastructure from Cisco
- Further inquiries for product certification have occurred:
  - VPN PP was of particular interest
  - Inquiries came from small vendors
  - Not applied for certification yet
    (mainly because of the version change from CC2.4 to CC3.0)

Trial Use Results - Positive

- Problems with the ASE/APE criteria encountered during the trials have been fixed in CC3.0
  (17 Interpretations have been raised during the trials)
- Defining and Evaluating PPs and STs according to CC2.4 EAL1 is much more efficient compared to CC2.2
  (2-3 man-days for the PP development and 3-4 man-days for the evaluation)
- Reduced complexity of PPs/STs will open new markets for the CC
  (Increasing interest from small to medium-sized vendors has shown that already)

Trial Use Results - Positive

- Most work intensive examinations have been left out
  (No rationales required for EAL1 ASE / APE)
- Much better ratio between ASE and other EAL1 requirements



Trial Use Results - Negative

- It is more difficult for a vendor to step-up from EAL1 to EAL>1
  (Low Assurance PPs/STs have to be augmented significantly to get a full scale PP/ST)
- Missing “formal” specification of SPD, OBJ and the free placement of requirements can have disadvantages
  (Evaluators and Certification Schemes have to take more care that a sensible TOE is specified)
- Scheme procedures may have to be adopted to be able to keep up with the development and evaluation speed
  (5 man-days for developing and evaluating a PP)

Contact Information

Bundesamt für Sicherheit in der
Informationstechnik (BSI) /
Federal Office for Information Security

Thomas Borsch
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)1888-9582-467
Fax: +49 (0)1888-10-9582-467

thomas.borsch@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de