# The Evaluated Configuration – Defining a user-friendly Target of Evaluation

Stephan Müller, David Ochel

atsec information security

Common Criteria

@sec
the information security provider

ICCC

# Overview

- Definitions
  - Target of Evaluation (TOE)
  - Evaluated Configuration
- Examples
  - Configuration Restrictions
  - Assumptions
- Enhancing the Business Value
- Example: SUSE Linux on IBM

# Target of Evaluation (TOE)

- the TOE is often a product subset
  - "a product, a part of a product, a set of products, …"
    CEM 2.2 B.6.2

- aspects of the TOE Boundary
  - product architecture
  - code ownership, legal implications
  - security relevance of product components
  - testing efforts

# Evaluated Configuration

- a “specific configuration or set of configurations” of the TOE as defined in the Security Target CEM 2.2 B.6.2

- subject to: analysis, testing, vulnerability analysis, assumptions CEM 2.2 B.6.4

# “a specific configuration”

limit the configuration flexibility offered by the product to

- prevent “insecure” configuration settings
  - e.g. by mandating SSL encryption
- improve mechanism strength
  - e.g. by enforcing a minimum password policy
- reduce testing effort
  - e.g. evaluation on a subset of supported platforms

# Typical Assumptions

Examples for restrictions on the TOE environment:

- Security Function Protection
  - e.g. physical protection of software TOEs
- Security Function Support
  - e.g. CPU states to support privilege enforcement
- Threat mitigation
  - e.g. managed user community in the TOE's network
- "Root" assumption
  - TOE administrators are well-behaved and smart

# Enhancing the Business Value

- evaluated configurations often
  - suit developer and evaluator
  - are not of much use in customer scenarios
- therefore: think out of the “evaluation” box
  - consider customer requirements
  - enable TOE interoperability
  - automate testing of multiple configurations
  - lift initial restrictions in TOE re-evaluations

# Example: SUSE Linux on IBM

- initial assurance level EAL2
  - "proof of concept"
- re-evaluation at EAL3
  - augment TOE Security Functions (TSF)
  - enhance evaluated configuration

# CAPP Compliance & TSF

- Controlled Access Protection Profile
  - requires EAL3 as minimum assurance level
  - compliance demonstrates the fulfillment of customer requirements!
- Additional TOE Security Functions
  - Auditing
  - SSL / TLS
  - Abstract Machine Testing

# Strength of Function and Platforms

- Strength of Function / Attack Resistance
  - SOF increased from basic to medium
  - in line with EAL3, able to withstand higher attack potential
- Underlying Hardware
  - EAL2: IBM xSeries
  - EAL3: IBM xSeries, zSeries, iSeries, pSeries

# Questions?

- david@atsec.com
- stephan@atsec.com