



## Improving the Flexibility and Applicability of Protection Profiles

Helmut Kurth, atsec information security corp.

[Helmut.kurth@atsec.com](mailto:Helmut.kurth@atsec.com)

# Outline

## *What to expect*

- The idea of “Protection Profiles”
- Current CC requirements for PPs
- Some examples why they are counterproductive
- Some examples, where new ideas have been tested/used
- Extending the idea of Protection Profiles
  - Extended functional packages
  - Architecture-dependent requirements
  - SFR options
  - Refinements for assurance requirements
- Conclusion

# The idea of "Protection Profiles"

## *How did it come up*

- Orange Book:
  - Classes combining functional and assurance aspects
  - Aimed at Operating Systems, does not work elsewhere
- German Criteria ("Green Book")
  - Separated functionality and assurance
  - Introduced "Functionality Classes"
  - Approach taken one-to-one into the ITSEC
- U.S. Federal Criteria
  - Extended the concept of functionality classes, introduced "Protection Profiles"
  - Approach taken one-to-one into the Common Criteria

# Current CC Requirements for PPs

## *How Protection Profiles are defined*

- Definition:
  - “implementation-independent statement of security needs for a TOE type”
  - PP “describes the general requirements for a TOE type, and is therefore typically written by”:
    - A user community
    - A developer of a TOE or a group of developers
    - A government or large corporation
  - Security Targets can then claim conformance
    - Strict or (if the PP allows) demonstrable

# PP Concept

## *What Protection Profiles are for*

- Expressing common security requirements for a “type” of product
    - When developed by vendors
    - Showing what all products of this type should provide
  - Expressing minimal security requirements for a “type” of product
    - When developed by users/government
    - Showing what all products of this type are required to have
- ➔ Protection Profiles always express a **minimal** set of requirements for a type of product!

## Some common misconceptions

### *What PPs are not for*

- They are no “wishlist” for “nice-to-have” requirements
  - Customers tend to misuse them for this
- They are no instrument to exclude competitors
  - Vendors tend to misuse them for this
- They are no playground for research
  - Researchers tend to misuse them for this
- They are method for security requirement analysis
  - “I don’t know what I wanted until I wrote a Protection Profile”

# Consequences

## *Minimum set of requirements*

- Most products will have more security functions than the CC requires
  - Addressing additional threats, security objectives, and/or policies
  - Reducing requirements on the IT environment
  - Being suitable for different (**potentially** less restrictive) operational environments

# CC requirements for PP compliance

## *The CC view of strict compliance*

- An ST is equivalent or more restrictive than a PP if:
  - all TOEs that meet the ST also meet the PP, and
  - all operational environments that meet the PP also meet the ST
- First one is fine, but what about the second one?
  - What if a product has more security functionality that requires restrictions to aspects of the operational environment not necessary for the security functions defined in the PP?

## Example 1

### ***Firewall PP***

- Defines minimum security requirements for packet filtering, management, user authentication etc.
- Does not include requirements related to availability
- Has the usual assumptions on the trustworthiness of administrators, physical security, etc.

# Example 1

## *Firewall Product*

- Satisfies all the minimum security requirements for packet filtering, management, user authentication etc.
- Includes additional requirements related to availability
- Has the usual assumptions on the trustworthiness of administrators, physical security, etc.
- Has a distributed architecture with load balancing, heartbeat functionality, failover functionality
- Requires a dedicated network for those functions between the distributed parts of the TOE
- **Needs an additional assumption on the security of this communication link**

## Example 2

### *Operating System PP*

- Defines minimum security requirements for user authentication, file access control, auditing, basic network security functions, management, etc.
- Is fairly generic leaving some freedom how those functions are implemented
- Does not require multiple access control policies, multiple authentication mechanisms, directory support, etc.
- Has the usual assumptions on the trustworthiness of administrators, physical security, etc.

## Example 2

### *Operating System Product*

- Implements multiple user authentication functions, different file access control policies, extensive auditing, wide range of network security functions, support for distributed TSF (clustering), remote management capabilities, etc.
- Implements all the PP requirements, but those are only a small subset of the overall security functionality provided
- Requires a number of specific assumptions and has dependencies on the IT environment the PP authors could not imagine

# Compliance with multiple PPs

## *What does this imply for a modern OS*

- Compliance to:
  - an OS PP, a directory PP, an authentication server PP, a firewall PP, a system management PP, ....
- Experience with existing PPs:
  - If they are not designed for being composed with other PPs, composition will not work
  - Security Problem Definition will not be compatible
  - Claiming strict compliance with multiple PPs implies that you can only specify assumptions common to all PPs!
    - This is usually the empty set!

## Possible solution

### ***Build a PP with optional “extended packages”***

- Has been done with the multi-function printer devices and the BSI operating system Protection Profile
- The BSI operating system Protection Profile has elaborated a methodology how to define and use those
- Addresses quite a number, but not all of the problems with the CC
- Issues still open:
  - Architecture dependent security functional requirements
  - SFR options for strict compliance
  - Product type specific assurance requirements/refinements

# Architecture dependent SFRs

## *What is this? An Example*

- Assume a product is implemented using a distributed TSF
- In this case one may want to ensure:
  - That TSF data is held consistent in the different parts of the TSF
  - That the communication between the different parts of the TSF is protected
  - That the parts of the TSF implement a mechanism allowing them to detect when one part is no longer responding
- This could be expressed in “conditional SFRs”:
  - If the TSF is distributed, then ...

# SFR Options

*There may be many ways ....*

- PPs should not prescribe an implementation
- They should also not be too generic
- If the PP author accepts three ways to satisfy the same objective, it should be possible to state this in a PP
  - If the product uses option A, then the following set of SFRs need to be taken, if option B, then another set of SFRs are required
  - Example: User authentication either by Kerberos or by use of a directory service
  - Both may fit, but requirements are different

# Assurance Requirements

## ***Product type specific assurance assessment***

- The CC allow for more specific assurance requirements
  - Extended requirements
  - Refinements
- Both options are rarely used
  - May breaks mutual recognition
- Smart card sector works with “supporting documents”
  - One possible solution, but sometimes “binding” to PPs is weak
- Specific functional requirements may require specific evaluation activities
  - E. g. specific protocols may require specific testing methods

# Recommendation

## *How to modify the CC*

- More extended Protection Profile framework
  - Support for
    - Extended packages
    - Architectural dependencies
    - SFR options
    - Refinements of assurance requirements
  - Refined PP evaluation methodology
  - Extended guidance for PP development

## Conclusion (1)

### *Future PP development*

- Protection Profiles have been a good idea
  - Not used to the extend possible
- Framework for PPs in the CC is too restrictive
  - PPs often too generic
  - If more specific, too many products were excluded
- New ideas have been tested recently
  - Brought more flexibility
  - Need to be extended and integrated into the CC

## Conclusion (2)

### ***Industry involvement***

- Vendor involvement in PP development necessary
  - Otherwise requirements may not be realistic
- PP framework must allow to specify common requirements as detailed as possible
  - Using optional packages, SFR options and more
- PP framework must allow to refine assurance requirements
  - But should not harm mutual recognition
  - Requires extended PP evaluation methodology and definition of acceptance procedure under the CCRA

# Questions & Answers



Thank you

