

Explanation of new P2600 PP structure

Brian Smithson, Ricoh Americas Corporation, June 5, 2008

References	1
Overview	1
1.-3. Front matter	2
4. Protection profile introduction	2
5. HCD overview	2
6. TOE overview	2
7. Conformance	2
8.-11. The common Protection Profile	3
12.-18. SFR Packages	3
19. Assurance requirements	4

References

This document refers to P2600.1-36c-prot.pdf, available in on the P2600 web site in this directory:
<http://grouper.ieee.org/groups/2600/drafts/ProtectionProfiles/>

Overview

The goal of the new PP structure is to reduce the complexity of the previous “family of PPs” and reduce the number of redundant SFRs. This should make it easier to understand and evaluate the PP, easier to write every conforming ST, and easier to evaluate every conforming product. This was accomplished by simplifying the asset/threat model.

Simplifying the model made it possible to create a single security problem definition (SPD) and set of objectives (OBJ) that can be used for all of the hardcopy device (HCD) configurations that were covered by the previous PP. The new PP does not contain any optional assets, threats, objectives, or requirements, and it does not require any specific HCD functions or features. The new PP can be used for a large variety of HCD configurations because it uses SFR packages for each configuration component (PRT, SCN, FAX, CPY, DSR, NVS, and SMI).

I believe that this PP structure is entirely consistent with Common Criteria version 3.1.

In this document, I will introduce the new PP structure and explain how it works.

1.-3. Front matter

Clauses 1-3 are IEEE and Common Criteria front matter.

4. Protection profile introduction

The introduction provides an informal description of how the P2600.1 standard for HCD protection profiles can be used to create a security target (or another protection profile) for a variety of HCD configurations:

- There is a common PP for HCDs. All STs must conform to this PP.
- There are some SFR packages. An ST must conform to an SFR package if the target of evaluation of the ST performs functions that are described in the SFR package.

Along with the normal PP references (name, version, date, etc.), there are references for each SFR package. An ST author would use these references when claiming conformance for a particular product.

5. HCD overview

This clause introduces HCDs and the environments that were defined in IEEE Std. 2600. It is largely unchanged from the previous PP structure.

6. TOE overview

The TOE overview introduces the model that had previously been defined for HCDs by the P2600 working group. However, in the new PP structure:

- Assets are now described in very general terms: User Documents, User Function Data, TSF Protected Data, and TSF Confidential Data.
- The functions that had previously been described in separate PPs within a family of PPs are now described as named HCD functions that may or may not be present in a conforming ST.
- A single operational model is described that specifies only “document processing operations” and gives printing, scanning, etc., as examples.

7. Conformance

There are three conformance requirements: (1) conformance to the common PP, (2) conformance to any SFR packages as needed by the conforming product, and (3) conformance to at least one of the basic hardcopy function packages. Since the PP and SFR packages have distinct names (defined in the PP and SFR Package reference sections in clause 4), a conforming product can unambiguously state its conformance claim.

8.-11. The common Protection Profile

Clauses 8-11 comprise the common PP for HCDs. They follow the conventional and required format for CC protection profiles (8. Security Problem Definition, 9: Security Objectives, 10. Extended Components, and 11. Security Functional Requirements).

The security problem definition describes:

- Generic threats to data (unauthorized disclosure and unauthorized alteration);
- Generic policies for user authorization, software verification, audit logging, and management of data input/output; and,
- Assumptions about restricted/monitored access to the TOE, training, and trust.

The security objectives mitigate threats in the TOE or in the operational environment, and uphold assumptions in the operational environment.

There are no extended components.

The security functional requirements address all of the TOE objectives. Since the threats to data and policies have been described in a generic manner, the SFRs are also relatively generic.

The overall result is that this PP can be used for any hardcopy device configuration, from a simple parallel-port printer, USB scanner, standalone copier, or fax machine, to a complex multifunctional product with hard disk storage and network interfaces. The threats, objectives, and requirements apply to any such configuration. To make a complete security target, some additional requirements (based on the same threats and objectives) are added by the SFR packages.

12.-18. SFR Packages

Clauses 12-18 are SFR packages for print, scan, copy, fax, document storage/retrieval, nonvolatile storage, and shared-medium (i.e. network) interface functions. Each package contains only SFRs; they do not define any new assets, threats, assumptions, policies, or objectives. Each SFR package is independent of the other SFR packages, and depends only on the PP. The contents of each package are:

- A brief introduction
- SFRs
- Rationale tables for completeness and sufficiency

Here are a few examples:

The PRT SFR package (clause 12) adds three new SFRs to add some new access control rules that are specific to the printing function. The new access control rules are (1) access control for executing the printing function, which supports the PP objective for user authorization, and (2) access control for retrieving printed documents, which supports the PP objective for preventing unauthorized disclosure of user documents. Any simple printer should be able to use this SFR package in conjunction with the common PP as the basis for a security target. Some advanced printers may have the ability to preview or

even modify a print job before actually printing it, but those features are not expressed as requirements in the PRT SFR package. Instead, they are mentioned in a PP application note which instructs the ST author to add additional access control rules if needed for their particular product.

The SCN, CPY, FAX, and DSR SFR packages are similar to the PRT SFR package.

The NVS SFR package (clause 17) is intended to address the threat that an unauthorized person might take a hard disk drive from the HCD and recover documents or TSF data. The threat is not fundamentally different from the generic threat of unauthorized disclosure that is described in the common PP, but the presence of a removable storage device in a particular TOE makes it necessary to add some new SFRs.

The SMI SFR package (clause 18) is intended to address the threats of network sniffing and of misuse of the TOE to attack other devices on a customer's network. These are already generically described in the common PP (the threat of unauthorized disclosure, and the policy of managing input-output channels), but the presence of a network interface in a particular TOE makes it necessary to add some new SFRs.

19. Assurance requirements

Clause 19 states the assurance requirements. They apply to the common PP and to all of the SFR packages.