

IEEE P2600 Hardcopy Device and System Security comments

Cl 01 SC 1 P 1 L 1 # 14

Steinhagen, Jennie M

Comment Type ER Comment Status A

Meets all editorial requirements.

SuggestedRemedy

Response Response Status C

ACCEPT.

Thanks!

Cl 05 SC 5.3.2.3 P 8 L 2 # 15

Chen, Nancy

Comment Type T Comment Status R

TOE functions are defined as a type of TOE asset here, but the PP has no threat/objective for the asset. Later in Section 10.4 there are SFRs that enforce the TOE Function Access Control SFP. These SFRs are used for supporting the objectives for protecting user data and TSF data. If TOE functions are assets, shouldn't they be protected? This seems an inconsistency.

Note: This applies to all other PPs.

SuggestedRemedy

Either

- (1) Remove TOE functions from asset category, or
- (2) Add a threat from unauthorized access to TOE functions as TOE assets, and add the corresponding objective, or
- (3) Clarify in the existing objectives for protecting user data and TSF data that access to TOE functions also need to be protected.

The security objective fulfillment table need to be adjusted accordingly.

(1) or (2) seem more appropriate for environment C, because of the possible need for adding objectives if Normal User authorization mechanism is implemented. (see my comment on section 7.3 of PP-C.)

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.

Cl 05 SC 5.4 P 10 L 13 # 7

Smithson, Brian

Individual

Comment Type T Comment Status R

[Thrasher - left over from meeting 40] The ""major security features"" list includes an assertion that all users are identified and authenticated, and are authorized before being granted permission to perform TOE functions. However, if the FAX package is claimed, then it is likely that incoming faxes will need to be received without the sender having been identified and authenticated, and the incoming fax function will therefore need to be performed without such authorization.

SuggestedRemedy

Add an app note to 5.4 ""There may be some cases where identification and authentication of a TOE user may not be possible. In such cases, specific authorization to perform necessary TOE functions must be specified by the ST Author. The allowable cases are identified in the SFR Packages to which they apply.""Add an app note to clause 16.1, fax sfr package introduction, ""In typical fax systems, users who send an incoming fax to the TOE cannot be identified or authenticated, but the TOE must be able to receive incoming faxes without authorization based on identification and authentication. It is allowable for the ST Author to make an exception to O.USER.AUTHORIZED in the TOE Function Access Control SFP of the ST to permit incoming fax functions to be performed without identification and authentication of the sender by giving explicit authorization in FDP_ACF.1.3(b) in clause 10.4.Alternatively, make a note about this in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.

However, an explanation similar to what is in the suggested remedy will be added to the Guide explaining why fax is different.

IEEE P2600 Hardcopy Device and System Security comments

Cl 08 SC 8.1 P 14 L 4 # 8
 Smithson, Brian Individual

Comment Type T Comment Status R

The objective O.AUDIT.LOGGED currently says ""The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration"". However, the PP does not assume by default that the TOE will maintain or protect the log of audit events. Instead, it relies by default on external audit storage and protection (OE.AUDIT_STORAGE.PROTECTED and OE.AUDIT_ACECSS.AUTHORIZED). In app note 5, the ST Author is instructed to add appropriate objectives and SFRs for local storage and protection. Consequently, none of the SFRs that fulfill O.AUDIT.LOGGED (FAU_GEN.1, FAU_GEN.2, and FIA_UID.1) actually deal with storage or protection.

SuggestedRemedy

Change the definition of O.AUDIT.LOGGED from ""The TOE shall create and maintain a log of TOE use and security-relevant events, and prevent its unauthorized disclosure or alteration"" to ""The TOE shall create a log of TOE use and security-relevant events"". In app note 5, change ""an internal capability to provide access"" to ""an internal capability to store and provide access"" (consistent with app note 7). In app note 5, add ""The ST Author should add to the security objectives rationale tables that P.AUDIT.LOGGING is additionally enforced by additionally enforced by O.USER.AUTHORIZED and OE.USER.AUTHORIZED"". Alternatively, make note of this in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.

However, an explanation similar to what is in the suggested remedy will be added to the Guide.

Cl 09 SC 9.1 P 19 L 16 # 3
 Smithson, Brian Individual

Comment Type T Comment Status R

[Smithson - left over from meeting 40] According to the PP objectives, some kinds of data do not require both confidentiality and integrity protection in the NVS package. However, FPT_CIP_EXP requires both in all cases.

SuggestedRemedy

In FPT_CIP_EXP.1.1 ECD, change ""confidentiality and integrity of user and TSF data when either is written"" to ""[selection: integrity, confidentiality and integrity] of [assignment: list of user or TSF data] when written"". In FPT_CIP_EXP.1.2 ECD, change ""alteration of user and TSF data when either is written"" to ""alteration of [assignment: list of user or TSF data] when written"". In clause 18.3, iterate FPT_CIP_EXP.1: in (a) select ""confidentiality and integrity"" and assign ""D.DOC, D.CONF""; in (b) select ""integrity"" and assign ""D.FUNC, D.PROT"". Modify application note 118 to indicate the appropriate set of objectives that are being fulfilled by each iteration. Modify the security requirements rationale tables to correspond to the iterations. Alternatively, make a note about this in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.

However, an explanation similar to what is in the suggested remedy will be added to the Guide.

IEEE P2600 Hardcopy Device and System Security comments

Cl 09 SC 9.1 P 19 L 19 # 10
Farrell, Lee Individual

Comment Type TR Comment Status R

[atsec] PP evaluators asked that we remove the section option "prevents" from FPT_CIP_EXP.1.2.

SuggestedRemedy

Change FPT_CIP_EXP.1.1 as follows:

"FPT_CIP_EXP.1.1: The TSF shall provide a function that ensures the confidentiality of user and TSF data when either is written to [assignment: media used to store the data]."

Also apply this change to the instance of this extended component in subclause 18.2, page 53, line 34.

Rationale:

In previous meetings, the Working Group agreed to the following:

- a) confidentiality shall be ensured.
- b) integrity shall be ensured by either prevention or detection [i.e. selection: prevent, detect], if detection is selected, action shall be specified.

In document 41b, SFR FPT_CIP_EXP. 1.1 requires two things:

- a) confidentiality shall be ensured.
- b) integrity shall be ensured.

SFR FPT_CIP_EXP. 1. 2 says integrity shall be ensured by either prevention or detection [i.e. selection: prevent, detect], if detection is selected, action shall be specified.

The proposed modifications should be acceptable because the modified FPT_CIP_EXP 1.2 already covers the same requirement (b) that is deleted from FPT_CIP_EXP.1.1

FPT_CIP_EXP.1.2 The TSF shall provide a function that [selection: prevents, detects and performs [assignment: list of actions] when it detects] alteration of user and TSF data when either is written to [assignment: media used to store the data].

Response Response Status C

REJECT.

This general problem has been addressed in version 41c as per the atsec suggest remedy. atsec believes that detection is absolutely necessary. See comment #1.

This alternative approach will be documented in the Guide but will require additional work on the part of the ST author during the ST evaluation.

Cl 09 SC 9.1 P 19 L 19 # 1
Smithson, Brian Individual

Comment Type T Comment Status A

[atsec] PP evaluators asked that we remove the section option "prevents" from FPT_CIP_EXP.1.2.

SuggestedRemedy

Change ""[selection: prevents, detects and performs [assignment: list of actions] when it detects]"" to ""detects and performs [assignment: list of actions] when it detects"".Apply also to the instance of this extended component in subclause 18.2, page 53, line 34.

Response Response Status C

ACCEPT.

This has been fixed in version 41c.

Cl 09 SC 9.2 P 21 L 11 # 2
Smithson, Brian Individual

Comment Type E Comment Status A

[Nevo] Sharp asked for an application note clarifying the meaning of ""further processing by the TSF"".

SuggestedRemedy

Add an app note after FPT_FDI_EXP.1.1:The intention of ""further processing by the TSF"" is to ensure that the data being forwarded between interfaces is a normal function of the TOE and does not violate the security policies of the TOE Alternatively, make a note about this in the PP Guide.

Response Response Status C

ACCEPT IN PRINCIPLE.

This will be added to the Guide.

IEEE P2600 Hardcopy Device and System Security comments

Cl 10 SC 10.4 P 23 L 4 # 5
 Smithson, Brian Individual

Comment Type T Comment Status R

[Hirota-san - left over from meeting 40] The Common Access Control SFP rules restrict operations on D.DOC and D.FUNC from being performed by anyone except for the owner of the data. However, FMT_MSA.3.2 allows an authorized role to alter the default attribute values when those objects are created, which implies that someone other than the owner could be granted permission to perform such operations.

SuggestedRemedy

Change the access control rule from ""Denied, except for his/her own documents"" to ""Denied, except (1) for his/her own documents, or (2) if authorized by another role or mechanism if such functions are provided by a conforming TOE"". Add an app note ""The ST Author should specify appropriate roles or mechanisms for authorizing users to delete another user's documents or to modify or delete another user's function data, if such functions are provided by a conforming TOE."" Make a similar change for the D.DOC rule(s), and add an appropriately modified app note, to each of the following clauses: 13.2 (PRT), 14.2 (SCN), and 16.2 (FAX).

Alternatively, make a note about this in the PP Guide.

Response Response Status C
 REJECT.

The committee believes that the process for authorizing another user in the print/scan/copy cases is contrary to the original intention of the security objective for document protection.

Explanatory material will be added to the Guide to explain these concerns.

Cl 13 SC 13.2 P 41 L 14 # 12
 Aubry, Carmen Individual

Comment Type E Comment Status R

Does this rule imply that the TOE must produce the hardcopy output right away, immediately after the user requested it, or is the system allowed to add the user's job to the queue of jobs to process? (which means it can come out hours later).

SuggestedRemedy

I think this rule misses its goal if the "release" can be a "release to the queue of waiting jobs" rather than a "release of the already processed and print-ready job".

Response Response Status C
 REJECT.

Implementations of this scenario will vary from product to product and as such it cannot be specified in a PP. APPNOTE 74 defines "read" as being released to hardcopy output as a minimum but could be extended in a specific ST.

Cl 13 SC 13.2 P 41 L 14 # 11
 Aubry, Carmen Individual

Comment Type E Comment Status R

Concerning the application note 75: "A User will need to authenticate using the Operator Panel on the TOE to perform "Read" operations."

It implies that even if you want to view your job/document on a remote PC you still have to go to the Operator Panel on the TOE to authenticate in order to perform the read operation. And since you're not allowed to authenticate via one interface in order to use another afterwards, this basically implies you're only allowed to perform read operations from the operator panel (view thumbnails, print previews).

The chapter is about hardcopy device print functions, but since the 1st application note explicitly states that "Read" is not only about releasing pending hard copy output but also about viewing for example, it creates the confusion for the 2nd application note.

SuggestedRemedy

Instead of the first line of the 2nd appnote, I would propose the following: "To release pending hardcopy output to a Hardcopy Output Handler, a User will need to authenticate using the Operator Panel on the TOE."

Response Response Status C
 REJECT.

APPNOTE 75 is talking about doing read operations on the TOE and as such read operations done remotely are not covered.

Text will be added to the Guide to explain this.

IEEE P2600 Hardcopy Device and System Security comments

Cl 18 SC 18.2 P 53 L 34 # 13
 Aubry, Carmen Individual

Comment Type G Comment Status R

Concerns FPT_CIP_EXP.1.2: Full Disk Encrypted (CC certified) products like Seagate would not satisfy this requirement because they allow prevention instead of detection, as Helmut says: " Seagate uses active measures to *prevent* unauthorized modifications. Unless one physically modifies the disk controller or analyzes it physically to get access to its protected data, it is not possible to modify the content of the disk using the regular interfaces. Consequently, there is no function to detect direct modifications. There is just a function that validates the credentials passed to the disk controller and if they are correct, the disk allows to perform read and write functions to it. The only functionality that the disk has internally (using its error detection and correction codes) is to validate that the data has not been modified using other methods (e. g. a strong magnetic field)."

This might be a problem for part of our customers which prefer FDE solutions that are FIPS (and CC) certified and that are probably already on a list of approved products.

SuggestedRemedy

Modify the SFR in order to allow FDE products like Seagate's disks to satisfy the requirement.

Response Response Status C

REJECT.

Since the Seagate product as described does detect gross modification (de-gaussing for example) and it exceeds the detection requirement by preventing modification, the ST author can argue that his solution exceeds the requirements of the PP.

Cl 18 SC 18.2 P 54 L 23 # 6
 Smithson, Brian Individual

Comment Type T Comment Status R

[Smithson - left over from meeting 40] Audit and management specifications in the ECDs of FPT_CIP_EXP.1 and FPT_FDI_EXP.1 were not reflected the use of those extended SFRs in the NVS and SMI packages. For NVS audit, we had decided to require none and recommend ""Failure condition..."". For NVS management, we had decided to require none and recommend none. For SMI audit and management, we had decided to require none and recommend none. So the only thing to do is recommend an audit event and audit information for the NVS package.

SuggestedRemedy

Add a new SFR class FAU to the NVS package in which we require no audit events or information, but recommend ""Failure condition that prohibits the function to work properly, detected attempts to bypass this functionality (e.g., detected modification)"" for FPT_CIP_EXP.1, Basic audit level, no additional information required. Add app notes (similar to those in the SMI package) indicating that dependency FPT_STM.1 is resolved in the common PP section, that FAU_GEN.1 fulfills O.AUDIT.LOGGED and is a dependency of FAU_GEN.2, and FAU_GEN.1 performs audit functions that are recommended for FPT_CIP_EXP.1. Add these SFR/objective relationships to the two tables in clause 18.4, security requirements rationale. Alternatively, make a note of this in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.

Some explanatory information will be added to the Guide.

Cl 18 SC 18.3 P 55 L 13 # 4
 Smithson, Brian Individual

Comment Type T Comment Status R

In FPT_CIP_EXP.1, the assignment of ""media used to store the data"" is currently ""a Removable Nonvolatile Storage Device"". However, there may be more than one such devices.

SuggestedRemedy

In both FPT_CIP_EXP.1.1 and FPT_CIP_EXP.1.2, change ""[assignment: a Removable Nonvolatile Storage device]"" to ""[assignment: list of Removable Nonvolatile Storage devices]"". Alternatively, make a note about this in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.

Explanatory information will be added to the Guide.

IEEE P2600 Hardcopy Device and System Security comments

CI 19 SC 19.3 P 56 L 11 # 9
Smithson, Brian Individual

Comment Type T Comment Status R

PP app note 114 refers to defining roles, but the SFR no longer deals directly with roles but instead depends on FMT_SMR.1.

SuggestedRemedy

Remove PP app note 114.
Alternatively, make a note about it in the PP Guide.

Response Response Status C

REJECT.

This comment was WITHDRAWN by the commenter.