

IEEE P2600 Hardcopy Device and System Security comments

Cl **Global** SC **5.2.1** P **23** L **41** # **2**
 Sukert, Alan Xerox Corp

Comment Type **E** Comment Status **D**

Section 3.1.54 defines the term "multifunction device". However, here the term is denoted as "multi-function device". We probably should be consistent in either including the hyphen or not including the hyphen in the standard when we refer to a multifunction device.

SuggestedRemedy

Global "search and replace" to whichever of the two we agree is the desired spelling for multifunction device.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Use "multifunction device" throughout document.

Cl **Main** SC **3.1.19** P **6** L **12** # **3**
 Sukert, Alan Xerox Corp

Comment Type **E** Comment Status **D**

The 'Contrast: Forward-Channel' needs to be added to the end of the definition of back-Channel to be consistent with the corresponding Contrast associated with the Forward-Channel definition.

SuggestedRemedy

Add the suggested wording.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Cl **Main** SC **4.4.1** P **21** L **11** # **4**
 Sukert, Alan Xerox Corp

Comment Type **E** Comment Status **D**

This section refers to the "SOHO environment". The specific definition of "SOHO environment" was deleted in Clause 3. That's OK since the acronym SOHO is defined in Section 3.2. However, the term "environment" as it is used in the context of this standard is not defined in Section 3.1, so it may not be clear to the reader what we mean when we refer to a "SOHO environment".

SuggestedRemedy

Either add the definition of "environment" in Section 3.1 (my recommendation) or put back in the deleted definition of "SOHO environment".

Proposed Response Response Status **W**

PROPOSED ACCEPT IN PRINCIPLE.

change"...SOHO environment..." to "...in a typical home office..."

Cl **Main** SC **4.4.3.4 & 4.4.4.3** P **22** L **12&3** # **9**
 Sukert, Alan Xerox Corp

Comment Type **E** Comment Status **D**

Since in all of Clause 8 there reference is to "Recommended Mitigation Techniques for HCD Manufacturers", I wonder if these two sub-section titles should be titled "For (or Use by) HCD Manufacturers" for consistency

SuggestedRemedy

Make the titles consistent between the two clauses.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Insert HCD in front of manufacturers

Cl **Main** SC **4.4.4.1** P **22** L **19** # **5**
 Sukert, Alan Xerox Corp

Comment Type **E** Comment Status **D**

Sorry for the nits. This section is titled "Use by information administrators and support personnel" but the text that follows doesn't mention support personnel. I also noted that section 4.4.3.2 is similarly titled but doesn't explicitly mention support personnel. For consistency sake support personnel should be mentioned somewhere in the text or it shouldn't be included in the title.

SuggestedRemedy

See comment above.

Proposed Response Response Status **W**

PROPOSED ACCEPT.

Remove "and support personnel" from 4.4.3.2. and 4.4.4.1 title. Change administrators to professionals. Change information technology to IT.

Cl **Main** SC **5.3.1** P **27** L **12** # **6**
 Sukert, Alan Xerox Corp

Comment Type **E** Comment Status **D**

Think the sentence as stated is not grammatically correct. Should read "Figure 3 shows an example of a network architecture typical of..."

SuggestedRemedy

See above comment

Proposed Response Response Status **W**

PROPOSED REJECT.

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8 P 78 L 4 # 7
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

The word 'manufacturers' is misspelled in the sentence "...a list of recommendations for manufactures..." Note same misspelling on line 8.

SuggestedRemedy

Correct spelling

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl Main SC 8.3.1.3 P 92 L 35 # 8
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

I believe that per our convention we have been using, the reference to '802.1x' here should be to 'IEEE 802.1x'.

SuggestedRemedy

Correct reference

Proposed Response Response Status W

PROPOSED ACCEPT.

Change to IEEE Std. 802.1x

Cl Main SC 8.3.11.2 P 100 L 40-41 # 1
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

The beginning of this sentence just doesn't read correctly to me, and it also has an extra 'by' on line 41.

SuggestedRemedy

Suggest changing to read something like this - "When data, whether it is User Data or not, is no longer needed by the HCD, the memory that is used to store this data is freed up for use by the HCD's operating system..."

Proposed Response Response Status W

PROPOSED ACCEPT.

Change to read "When data, whether User Data or not, it no longer... " Delete extra "by"

Cl Main SC 8.3.11.2 P 101 L 13 # 12
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

When you changed this sentence you accidentally deleted a 'to' that should be in the sentence. The sentence should read "The equipment needed to recover data..."

SuggestedRemedy

See comment

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl Main SC 8.3.13.2 P 103 L 18 # 13
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

Consistent with other sub-sections in Clause 8, 'user data' and 'management data' in this sentence should both be capitalized.

SuggestedRemedy

See comment

Proposed Response Response Status W

PROPOSED ACCEPT.

Should be consistent throughout.

Cl Main SC 8.3.5.2 P 95 L 15 # 10
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

Misspelling - "debub" should be "debug".

SuggestedRemedy

Correct spelling

Proposed Response Response Status W

PROPOSED ACCEPT.

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8.3.5.3 P 95 L 26 # 11
 Sukert, Alan Xerox Corp

Comment Type E Comment Status D
 Misspelling - "access" should be "access". Also, I think this sentence is missing a word - should read ""Restricting access from service and debug ports on the HCD to any portions in the HCD..."

SuggestedRemedy
 Correct spelling and grammar

Proposed Response Response Status W
 PROPOSED ACCEPT.

- Fix spelling of access
- add "of"

Cl Main SC 8.4.2.3 P 106 L 9-10 # 14
 Sukert, Alan Xerox Corp

Comment Type T Comment Status D
 I noticed that the background discussion in 8.4.2.2 for T.TSF.CRED.EM is the same with respect to wireless networking as in 8.3.1.2 for T.UD.SNIFF.NET. However, the associated manufacturer mitigation technique recommendations for the two are somewhat different as follows:
 T.UD.SNIFF.NET - ""Providing support for wire-level authentication mechanisms like 802.1x to control port access on the wired network."
 T.TSF.CRED.EM - ""Where wireless networking is offered, supporting the available encryption mechanism for that networking standard.""

I know these threats are slightly different but from a wireless perspective the threat is the same, except in the first case the affected asset is User Data and in the later case the affected asset is authentication data. I am wondering why the two mitigation techniques shouldn't be the same.

SuggestedRemedy
 Consider whether the two mitigation techniques should be the same

Proposed Response Response Status W
 PROPOSED REJECT.

Cl Main SC 8.4.3.3 P 107 L 12 # 15
 Sukert, Alan Xerox Corp

Comment Type E Comment Status D
 I noticed that this mitigation technique is the same as the one for T.TSF.CRED.EM in 8.4.2.3 (subitem #b) except the wording in 8.4.3.3 is slightly different from the wording in 8.4.2.3 and contains additional explanatory information (namely reference to specific encryption mechanisms). I'm wondering why the two should read the same since they are the same technique.

SuggestedRemedy
 See comment

Proposed Response Response Status W
 PROPOSED ACCEPT.

Use 8.4.2.3 (b) text in 8.4.3.3 (b)

Cl Main SC 8.4.4.4 P 108 L 9 # 16
 Sukert, Alan Xerox Corp

Comment Type T Comment Status D
 T.UD.SALVAGE and T.TSF.SALVAGE are basically the same threat, except the first applies to all user data and the second one applies specifically to authentication data. Given that the mitigation techniques should be identical except for the addition of the overwrite capability for T.UD.SALVAGE.

In comparing the two sets of mitigation strategies I found that the wording in 8.3.11.4, page 102, line 16 was slightly different than the corresponding wording in 8.4.4.4. They probably should be made consistent since they are talking about the exact same technique.

SuggestedRemedy
 Make 8.4.4.4, page 108, line 9 and 8.3.11.4, page 102, line 16 consistent.

Proposed Response Response Status W
 PROPOSED ACCEPT.

Model 8.4.4.4 after 8.3.11.4

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8.4.5.1 P 108 L 17-18 # 17
 Sukert, Alan Xerox Corp

Comment Type T Comment Status D

I sincerely apologize for thinking about this now after all this time.

The definition of T.TSF.CRED.GUESS includes obtaining user credentials by guessing or observation. I think the definition for this threat needs to also encompass the use of social engineering methods, which in my view isn't either guessing or observing, to get user credentials because we know it has been done (I keep thinking of that British Study where about 70% of those asked would have willingly given their passwords to a stranger).

SuggestedRemedy

Suggest changing only the definition of T.TSF.CRED.GUESS in 8.4.5.1, 7.2 (Table 3) and Table 40 (page 61) to read something like "Obtaining user credentials or other authentication data by guessing, observation, or other social engineering methods (see Table 40)". Note that we do define the term "social engineering" in Clause 3 so we can use it here. I am not recommending a change in anything else associated with this threat either in 8.4.5, 7.2 or Table 40.

If agreed the threat definition would have to be changed in the PPs for which this threat applies also.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Insert the following text in 8.4.5.2:

"Other techniques for obtaining user passwords, such as using social engineering, are not included in this threat. Those threats must be addressed by increasing the security awareness of users."

Cl Main SC 8.4.6.3 P 109 L 21 # 18
 Sukert, Alan Xerox Corp

Comment Type E Comment Status D

This mitigation technique is requiring administrator authorization for any change to any device settings that would affect other users. I just keep thinking that "other" is the wrong word here because requiring SA authorization should be for changes to device settings that affect any user, including the SA, and "other" users suggests there are a class of users for which this shouldn't be required.

SuggestedRemedy

Change the sentence to read "Requiring administrator authorization for any change to any device settings that would affect any user."

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Change "other users" to "a user other than the user making the change"

Cl Main SC 8.6.3.2 P 116 L 27-30 # 19
 Sukert, Alan Xerox Corp

Comment Type E Comment Status D

I noticed a couple of grammatical errors in this paragraph that should be corrected

SuggestedRemedy

Paragraph should read as follows (changes are in bold type)

...This is due to the fact that the fax connection provides a connection that is usually not part of the environment's firewall protection from outside networks or the Internet. Many HCD fax connections also have the capability to support a data modem function in addition to the fax modem function either because it's part of the modem chipset that is used or because it is used for remote debug or management.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

Change paragraph as follows:

"In some operational environments, especially Operational Environment A, users may be concerned..."

"This is because fax is from an outside network and is a connection that is usually not part of the environment's firewall protection."

"Many HCD fax interfaces also have the capability to support a data modem function in addition to a fax modem function. This is because it is either an inherent part of the modem chipset or because it is used for remote debug or management."

IEEE P2600 Hardcopy Device and System Security comments

Cl Main SC 8.6.3.4 P 117 L7-11 # 20
Sukert, Alan Xerox Corp

Comment Type T Comment Status D

The threat in this case (T.EA.FAXBRIDGE) deals with using the fax connection to access internal components in the HCD. Given that particular threat, I don't understand how the last two IT Professional mitigation techniques presented - secure passwords and authorized administrators - has to do with mitigating this threat. I can certainly see why the first two apply but not these last two.

It seems to me that an additional mitigation technique for this threat is associated with ensuring that the configuration settings for the fax connection should be set to the appropriate values to minimize this threat.

SuggestedRemedy

Delete the IT professional mitigation techniques listed in lines 9-11.

Add the following new mitigation technique in 8.6.3.4: Ensuring that the HCD settings for the configuration of the fax connection are set by the administrator to the appropriate non-default values.

Proposed Response Response Status W

PROPOSED ACCEPT IN PRINCIPLE.

-delete 8.6.3.4 c) and d)

- add the following as 8.6.3.3 f) :

"Ensuring that configuration of the HCD's fax connection (including both enabling and disabling) requires administrator authorization."

Cl Main SC 9.4.2 P 132 L 1 # 21
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

To be consistent with then other items in the sub-section, Item e) should be written as ""Use of PSTN fax system...""

SuggestedRemedy

See comment

Proposed Response Response Status W

PROPOSED ACCEPT.

Cl PP SC PP Appendix C P L # 22
Sukert, Alan Xerox Corp

Comment Type E Comment Status D

The acronym TSC - TOE Scope of Control needs to be added to the list of acronyms in this appendix.

SuggestedRemedy

Add the acronym TSC

Proposed Response Response Status W

PROPOSED ACCEPT.