MFP Technical Community
Waltham face-to-face meeting

November 5, 2014
Held as part of the PWG-IDS F2F meeting

Agenda

- Recent drafts
- Current situation
- Direction
- Activities
- What do we need to do?
- Questions for NIAP (while we have them on the call)
- FDE AA cPP
- Other issues to be resolved

Recent drafts

- Draft 0.8.3: implemented a number of resolutions that were decided during the F2F in New Delhi. Meanwhile, we continued to discuss how to handle full drive encryption.

- Draft 0.8.4: P.STORAGE_ENCRYPTION and its objective and requirements were made entirely *optional* and moved to Appendix C.2. There were three selections available to fulfill the requirements:
  - Conform to NIAP's published SWFDE PP
  - Conform to the to-be-published FDE cPP
  - Conform to the SFRs that were in draft 0.8.3 which supported the objective (which are based on NIAP's SWFDE PP)

- Draft 0.8.5: Corrected an error due to misunderstanding: P.STORAGE_ENCRYPTION is *mandatory*, so it was moved back into the main Security Problem Definition and the selectable requirements were moved to Appendix D.1.

Current situation (1)

- It is likely that many MFPs can not conform to NIAP's SWFDE PP, nor to the FDE cPP, maybe not to the current SFRs in Appendix D.1.
  - All are based on a "lost laptop" model, in which (1) a user interacts with the TOE to unlock encryption before use, and (2) the unlock key can't reside in the powered-down TOE.
  - Several implementations to consider for MFPs are not supported by SWFDE PP, FDE cPP., and/or current SFRs:
    - Vendor- or third-party hardware encryption
    - Use of self-encrypting drive
    - Use of a TPM for storage and crypto functions

- In other words, draft 0.8.5 may have a *mandatory* objective with three ways to satisfy it, *none of which is possible to achieve.*

Current situation (2)

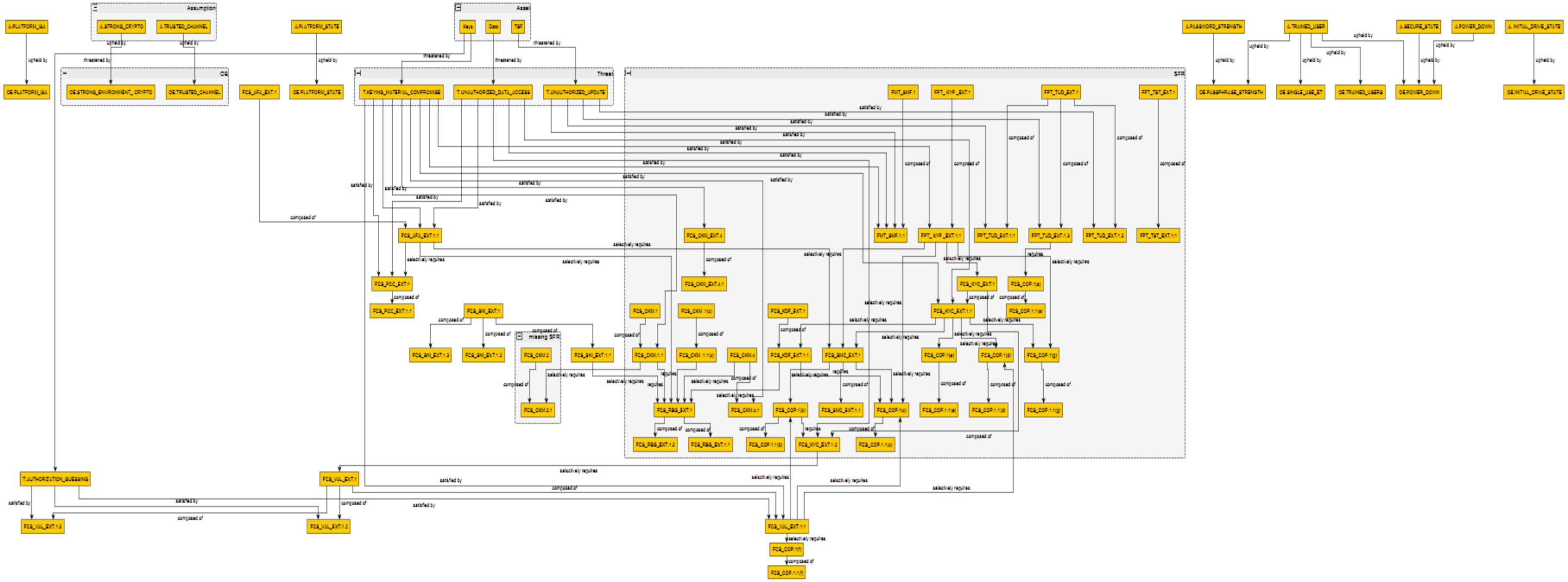
- Choices that have been considered:
  1. Modify the SWFDE PP-based SFRs in the MFP PP so they can be used in a variety of MFP implementations; or,
  2. Work with the FDE iTC to modify the two-part cPP so that:
     - The Authorization Acquisition (AA) part can accommodate the use case of an MFP; or; explicitly include the FDE AA SFRs in the MFP PP, modified for MFPs
     - The Encryption Engine (EE) part can be used by an MFP vendor, independently by an SED vendor to CC certify an SED so an MFP vendor can re-use that certification to fulfill MFP PP requirements; or, explicitly include the FDE EE SFRs in the MFP PP, modified for MFPs

Direction

- The FDE cPP is more recent, has received broader input, is more adaptable to different implementations, and it will eventually displace the SWFDE PP.Therefore, NIAP and IPA have agreed to consider using the FDE cPP requirements as a base instead of the SWFDE PP requirements.
- The FDE iTC is not in a position to make major revisions to the AA part, so it is reasonable certain that we would need to include and modify AA-based requirements in the MFP PP.
- The EE part is not so clear, but any requirement for major revision would likely mean that we would need to include and modify EE-based requirements as well.
- Maybe in a few years a new version of the FDE cPP could be used like a component in an MFP cPP ☺.

Activities

- Some dependency analysis and modification work has been done on the AA part of the FDE cPP:
  (it looks like this, MFP-applicable parts are indicated by the shading)



- Similar work has only just started on the FDE cPP's EE part (and on the Supporting Documents for both parts).

What do we need to do?

- As questions of NIAP (while we have Lonnie on the phone)
- ***All*** vendors need to look at the FDE cPP drafts to what would need to be removed, modified, or added, to support their drive encryption implementation. The draft FDE AA and EE cPPs and their Supporting Document can be found here: https://ccusersforum.onlyoffice.com/products/projects/tmdocs.aspx?prjID=239468#1675079
- It is up to us to respond to what NIAP and IPA have put in the draft PP, especially in the areas of encryption and protocols. Otherwise, whatever is there will become the new standard.
- There are about 20 open issues that need to be resolved.

Questions for NIAP (1)

- The following are from currently-posted issues, not related to the SWFDE SFRs, that might be answered by NIAP.
  If I've missed some, please speak up during the meeting.

0.8.1 ¶433	Undelete FAU_SAR.1 / FAU_SAR.2 / FAU_STG.1 / FAU_STG.4	There is configuration to send the audit log from TOE to the external Entity by the request from the external Entity like server. In this case, these components are involved. These must be undeleted. The description is written based on the Push transmission to server from TOE. However, when the TOE transmits the data by Pull from server (or PC), it is necessary to perform access control from external as well as saving the data in the TOE.
0.8.2 ¶598-631	The differences between NDPP Errata and MFP-PP	There are some differences between the NDPP Errata#2 and the MFP-PP v0.8.2. I found them in at least the following SFRs. FCS_TLS_EXT.1, FCS_SSH_EXT.1.1, FCS_SSH_EXT.1.5, FCS_SSH_EXT.1.6, FCS_SSH_EXT.1.7. They should be revised to match the NDPP Errata#2.
0.8.4, ¶610	FCS_TLS_EXT.1 mismatch between MFP and NDPP (errata#2)	Cipher list in MFP-PP (FCS_TLS_EXT.1.1) matches older NDPPv1.1 list (section FCS_TLS_EXT.1) not the updated list in NDPPv1.1 Errata #2.

Questions for NIAP (2)

0.8.4 ¶166	Identity certificate used by IKE for peer auth and FCS_CKM.1.1(3)	…Regarding FCS_CKM.1.1(3) and the Identity certificate used by IKE for peer authentication. An MFP can provide the following options to install the Identity certificate: The MFP provides the admin the ability create a certificate signing request. The admin submits the certificate signing request to the CA. The CA generates an Identity certificate from the signing request and signs it. The admin installs the Identity certificate on the MFP. (With this option, the MFP generates a public/private key pair.) The MFP provides the admin the ability to import the Identity certificate and associated private key. The admin obtains an Identity certificate and private key from the CA. The admin imports the Identity certificate and associated private key into the MFP's certificate store. (With this option, the operational environment generates a public/private key pair.)
0.8.4 ¶241	Administrative passwords and FIA_PMG_EXT.1	The ND PP has the following Application Note with FIA_PMG_EXT.1: "'Administrative passwords" refers to passwords used by administrators at the local console or over protocols that support passwords, such as SSH and HTTPS. The MFP PP does not have an Application Note with FIA_PMG_EXT.1. This raises the question on what the MFP PP considers to be administrative passwords. Are all passwords used by the administrator considered to be administrative passwords? Or, are only passwords used by the administrator that provide access to management functions considered to be administrative passwords? For example, would the SNMPv1/v2 Get community name be considered an administrative password if it doesn't provide read access to any confidential User or TSF Data?

Questions for NIAP (3)

0.8.5 ¶364	FTA_SSL.3.1 precludes stateless web interface?	This is a question and not an an issue. Does FTA_SSL.3.1 preclude a TOE with a web-based interface that doesn't maintain stateful user sessions from conforming to the MFP-PP?
any	CAVS certificate required?	To have a product listed on the NIAP PCL, NIAP has verbally communicated to atsec that crypto algorithms must have CAVS certificates issued. This has been verbally communicated for evaluations conforming to ND PP. Will there be a similar requirement for evaluations conforming to the MFP PP?

FDE AA cPP AA: Threats

- In this and the next few sections, we will look at what parts of the FDE AA cPP might not apply to MFPs

T.AUTHORIZATION_GUESSING	Threat agents may exercise host software to repeated guess authorization factors, such as passwords and pins.	Remove	No user interaction
T.KEYING_MATERIAL_COMPROMISE	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption	OK	
T.UNAUTHORIZED_DATA_ACCESS	unauthorized disclosure of protected data stored on a storage device	OK	
T.UNAUTHORIZED_UPDATE	Threat agents may attempt to perform an update of the product which compromises the security features of the TOE	OK	

FDE AA cPP: Assumptions

A. INITIAL_DRIVE_STATE	Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption	Not sure	It may be performed by the factory but it may also be performed at the customer site when an Admin activates drive encryption
A.PASSWORD_STRENGTH	Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected	Remove	Passwords are not used
A.PLATFORM_I&A	The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the Operating system's login interface, but it will not change or degrade the functionality of the actual interface.	Remove	No user interaction
A.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product	Remove	Already covered by trusted update (the TOE is the platform)
A.POWER_DOWN	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible	Remove	MFPs routinely go into power-save modes
A.SECURE_STATE	Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization	Not sure	This is a strange assumption about the OE. Is the OE in this case the part of the TOE that conforms to EE? The existing OE doesn't seem to uphold this assumption anyway.
A.STRONG_CRYPTO	All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG	Not sure	We need to look at what is meant (for MFPs) by "all cryptography implemented in the OE and used by the product"
A.TRAINED_USER	Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform	Remove	No user interaction
A.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure	OK	

FDE AA cPP: OEs

OE.INITIAL_DRIVE_STATE	The OE provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption	Not sure	It may be performed by the factory but it may also be performed at the customer site when an Admin activates drive encryption
OE.PASSPHRASE_STRENGTH	An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE	Remove	Passwords are not used
OE.PLATFORM_I&A	The Operational Environment will provide individual user identification and authentication mechanisms that operate independently of the authorization factors used by the TOE	Remove	No user interaction
OE.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product	Remove	Already covered by trusted update (the TOE is the platform)
OE.POWER_DOWN	Volatile memory is cleared after power-off so memory remnant attacks are infeasible	Remove	Volatile memory is not in the hands of the attacker
OE.SINGLE_USE_ET	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor	Remove	External tokens are not used
OE.STRONG_ENVIRONMENT_ CRYPTO	The Operating Environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE and Appendix A	Not sure	We need to look at what is meant (for MFPs) by "all cryptography implemented in the OE and used by the product"
OE.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors	Remove	No user interaction
OE.TRUSTED_CHANNEL	Communication among and between product components (e.g.i.e., AA and EE) is sufficiently protected to prevent information disclosure	OK	

FDE AA cPP: SFRs (1)

FCS_AFA_EXT.1	Authorization Factor Acquisition	Remove	No user interaction
FCS_AFA_EXT.1.1	Authorization Factor Acquisition	Remove	No user interaction
FCS_CKM .1(c)	Cryptographic key generation (Symmetric Keys)	Not sure	Do we need to generate symmetric keys? (it isn't attached to anything in the FDE AA cPP) It may be related to how the product is going to be managed at customer site (for instance are there changes in UEFI or BIOS configuration; do the product need to be put in recovery mode? If yes, when it exits this mode, a new key would be required)
FCS_CKM .1.1(c)	Cryptographic key generation (Symmetric Keys)	Not sure	Do we need to generate symmetric keys? (it isn't attached to anything in the FDE AA cPP)
FCS_CKM.1	Cryptographic Key Generation (Asymmetric Keys)	Not sure	Do we need to generate asymmetric keys?
FCS_CKM.1.1	Cryptographic Key Generation (Asymmetric Keys)	Not sure	Do we need to generate asymmetric keys?
FCS_CKM.4	Cryptographic Key and Key Material Destruction	Modify or remove	Do we ever need to destroy keys? (except in the Purge option)
FCS_CKM.4.1	Cryptographic Key and Key Material Destruction	Modify if not removed	At least remove the requirement for volatile memory clearing

FDE AA cPP: SFRs (2)

FCS_CKM_EXT.4	Cryptographic Key and Key Material Destruction	Not sure	
FCS_CKM_EXT.4.1	Cryptographic Key and Key Material Destruction	Not sure	
FCS_COP.1(a)	Cryptographic Operation (Signature Verification)	OK	it is part of FPT_TUD
FCS_COP.1(b)	Cryptographic operation (Hash Algorithm)	see FCS_SMC_EXT	it is part of FCS_SMC_EXT (hash selected)
FCS_COP.1(c)	Cryptographic operation (Keyed Hash Algorithm)	see FCS_SMC_EXT	it is part of FCS_SMC_EXT (keyed hash selected)
FCS_COP.1(d)	Cryptographic operation (Key Wrapping)	see FCS_KYC_EXT	needed only if key wrapping is selected in FCS_KYC_EXT
FCS_COP.1(e)	Cryptographic operation (Key Transport)	see FCS_KYC_EXT	needed only if key transport is selected in FCS_KYC_EXT
FCS_COP.1(f)	Cryptographic operation (AES Data Encryption/Decryption)	Remove	
FCS_COP.1(g)	Cryptographic operation (Key Encryption)	see FCS_KYC_EXT	needed only if key protection is selected in FCS_KYC_EXT

FDE AA cPP: SFRs (3)

FCS_KDF_EXT.1	Cryptographic Key Derivation	Not sure	Need to figure out if/when/why this is used
FCS_KYC_EXT.1	Key Chaining	Modify	
FCS_KYC_EXT.1.1	Key Chaining	Modify?	Is a keychain of length 1 the same as a DEK? Are other options relevant? Are they sufficient?
FCS_KYC_EXT.1.2	Key Chaining	Modify	Remove selection (no option for validation)
FCS_PCC_EXT.1	Cryptographic Password Construct and Conditioning	Remove	
FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)	OK	Is it OK for TPMs?
FCS_RBG_EXT.1.1	Extended: Cryptographic Operation (Random Bit Generation)	OK	
FCS_RBG_EXT.1.2	Extended: Cryptographic Operation (Random Bit Generation)	OK	
FCS_SMC_EXT.1	Submask Combining	Not sure	
FCS_SNI_EXT.1	Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	Not sure	Need to figure out if/when/why this is used
FCS_VAL_EXT.1	Validation	Remove	

FDE AA cPP: SFRs (4)

FMT_SMF.1	Specification of Management Functions	Modify	
FMT_SMF.1.1	Specification of Management Functions	Modify	change to suit MFPs
FPT_ KYP _EXT.1	Extended: Protection of Key and Key Material	Modify	
FPT_ KYP _EXT.1.1	Extended: Protection of Key and Key Material	Modify	change to suit MFPs
FPT_TST_EXT.1	Extended: TSF Testing	OK	
FPT_TST_EXT.1.1	Extended: TSF Testing	OK	
FPT_TUD_EXT.1	Trusted Update	OK	
FPT_TUD_EXT.1.1	Trusted Update	OK	
FPT_TUD_EXT.1.2	Trusted Update	OK	
FPT_TUD_EXT.1.3	Trusted Update	OK	
FCS_CKM.2	Referenced but missing SFR	Not sure	I am not sure if it is a mistake in the FDE cPP or an omission
FCS_CKM.2.1	Referenced by missing SFR	Not sure	I am not sure if it is a mistake in the FDE cPP or an omission

Open discussion