

**Proposal to P2600 meeting #21, Rochester NY
 Brian Smithson, Ricoh Corporation, 7/27/06**

Introduction

This proposal is a refinement of the proposals regarding protection of data stored on disk that I made at the Camas meeting in June.

1. Power-on versus Power-off threats and objectives

There are two types of data: user documents, and TSF data. Unauthorized access could happen in two states: when the TOE is powered on, and when the TOE is powered off. I don't think we have addressed these types and states in an optimal, symmetric manner:

State:	Power on		Power off	
Type:	Threat(s)	Objective(s)	Threat(s)	Objective(s)
User document	T.UD.ACC	O.ACCESS, O.I&A, O.MONITOR, O.NETWORK	T.UD.SALVAGE	O.PROTECT, O.DELETE
TSF data	T.TSF.CRED, T.TSF.AUD, T.TSF.CONF	O.ACCESS, O.I&A, O.MONITOR, O.PROTECT	T.TSF.CRED, T.TSF.AUD, T.TSF.CONF	O.ACCESS, O.I&A, O.MONITOR, O.PROTECT

There are a few problems here:

1. We don't really distinguish the power-on and power-off states for TSF data. The threat vector for power-off vulnerabilities includes physical access and the ability to power down and remove hardware. Such vulnerabilities are not prevented by O.I&A or O.ACCESS, and aside from a log entry when the HCD is powered up, they would not be detected by O.MONITOR.
2. T.TSF.CRED.DISK specifically refers to "residual or intentionally stored data", and yet it doesn't use O.DELETE for residual data.
3. T.TSF.CRED.DISK does not cover User Function Data or non-credential Management Data, which means that one could remove a nonvolatile storage device to obtain address book data, or conceivably, to alter security settings and then replace the storage device.
4. We shouldn't be requiring O.PROTECT for in the power-on state. Access controls like O.ACCESS and O.I&A should handle that.

I propose that we separate the power-on and power-off threats and objectives as follows:

- a. Rename T.TSF.CRED.DISK as T.TSF.SALVAGE and expand its scope to include both Management Data and User Function Data. The new name takes it out of the T.TSF.CRED family and helps make it clearer that we mitigate this threat using the same approaches that we use for T.UD.SALVAGE. The expanded scope gives coverage to User Function Data and the rest of the Management Data types.
- b. Change the objective of O.PROTECT to prevent unauthorized access to data on non-volatile storage devices when disconnected from the TOE.
- c. Remove O.PROTECT from the list of objectives for all threats except T.UD.SALVAGE and T.TSF.SALVAGE.
- d. Apply O.DELETE to T.UD.SALVAGE and T.TSF.SALVAGE.
- e. Rely on O.I&A and O.ACCESS to mitigate T.UD.ACC.*, T.TSF.AUD.*, and T.TSF.CONF.*.

The new chart would look like this:

State:		Power on		Power off	
Type:	Threat(s)	Objective(s)	Threat(s)	Objective(s)	
User document	T.UD.ACC	O.ACCESS, O.I&A, O.MONITOR, O.NETWORK	T.UD.SALVAGE	O.PROTECT, O.DELETE	
TSF data	T.TSF.CRED, T.TSF.AUD, T.TSF.CONF	O.ACCESS, O.I&A, O.MONITOR, O.PROTECT	T.TSF.SALVAGE	O.PROTECT, O.DELETE	

2. Salvaging persistent and residual data on hard disks

We have been requiring O.DELETE and O.PROTECT for Environments A and B. O.DELETE applies only to residual data. O.PROTECT can apply to either persistent or residual data, but I think it is intended to apply only to persistent data. Both objectives apply to “nonvolatile storage”, which would include hard disks as well as other forms of nonvolatile storage. Both objectives apply to all kinds of data: User Document Data, User Function Data, and Management Data.

I think we may want to distinguish hard disks and other field-serviceable storage devices from NVRAM or other nonvolatile storage that is not field-serviceable (e.g. soldered to a controller board). Perhaps “field-serviceable” isn’t the correct term, but if we can agree on the concept, I propose the following objectives:

Data		Environment	
Persistence	Accessibility	A	B
Persistent	Serviceable	Not permitted	O.PROTECT
Residual	Serviceable	O.DELETE	O.DELETE
Persistent	Fixed	O.PROTECT	O.PROTECT
Residual	Fixed	O.DELETE	O.DELETE

The major change here is that storage persistent data on field-serviceable devices would not be permitted. I think this is a necessary limitation based on some feedback from DAPS, and from other government customers per Peter Cybuck.

We will need to be careful how we define “Persistent” versus “Residual”. Some cases are clear, such as document repositories. Other cases may be less clear, such as locked print or proof print.

It’s worth noting that if you don’t store User Document Data in a persistent form in Environment B, then you won’t need to apply O.PROTECT to User Document Data. You would still need O.PROTECT for TSF data. If you assume that O.PROTECT is fulfilled by encryption, then this means that you won’t need to encrypt User Document Data in Environment B unless you intend to provide a persistent document storage function.

3. Encryption of document data on the network

The only threat differences between PP-A and PP-B are T.UD.SNIFF.EM, T.UD.IMP.PRINT|SCAN, and T.TSF.CRED.EM.

T.UD.SNIFF.EM and T.TSF.CRED.EM are best mitigated by encrypting network traffic, but one could argue that encryption is just as necessary to mitigate T.UD.IMP, T.UD.SNIFF.NET, and T.TSF.CRED.NET, so what is the difference between PP-A and PP-B when it comes to security objectives? You may still need to encrypt both documents (SNIFF.NET) and credentials (CRED.NET) in both environments.

T.UD.SNIFF.NET had an importance score of 2.4 for PP-B, which is in the “should be considered range”, but it is on the high end of that range.

T.UD.SNIFF.NET had the same score of 2.4 for PP-C, and T.UD.SNIFF.NET was not required for PP-C. The score for T.UD.SNIFF.NET for PP-A was 2.9.

I propose that we remove T.UD.SNIFF.NET from Environment B. That would mean that you don’t need to encrypt User Document Data over the network in that environment. You would still have T.TSF.CRED.NET in Environment B. The score for T.TSF.CRED.NET for PP-B was 2.9.

4. Audit protection

The main conceptual distinction between PP-A and PP-B is that PP-A is an environment of highly valued or regulated assets, all events including successful security events need to be logged, and controlled access to audit logs is much more important in PP-A than PP-B.

I looked at our original threat analysis spreadsheets and found that we had given T.TSF.AUD.ACCESS and T.TSF.AUD.ALTER a “1” for “elevation of privileges”. I can see how elevation of privileges could be a by-product of altering audit logs, but I don’t now see how it could be a by-product of simply accessing audit logs.

I propose that we change the “1” to a “0” for T.TSF.AUD.ACCESS. Then, its overall importance in PP-B drops from 2.7 to 2.2, but it remains 2.7 for PP-A because of other factors. It would then be reasonable to drop T.TSF.AUD.ACCESS from PP-B’s list of threats.

What difference does this make? On paper, it only makes the list of threats a little shorter for PP-B. In implementation, it may mean more, I don’t know. There can be a big difference between ensuring that some data hasn’t been altered and ensuring that it can’t be seen at all.

What does all of this mean for encryption?

I maintain that we can't require encryption in the PP, but as a practical matter it will likely be a requirement for successful implementation in some of the PP environments. Here's what I think these changes will mean:

Limiting O.PROTECT to power-off protection

If you can implement O.PROTECT without using encryption, then *theoretically* you would not need to do any disk encryption in any environment. You could simply depend on the access controls of the operating system to protect data during power-on operation, and use some other method ("this disk will self-destruct in five seconds...") to protect data when the TOE is powered off.

However, in the more likely (and practical) case that you use encryption for O.PROTECT to protect disk data during power-on, you could reduce the need for encryption by deleting residual data and by not storing User Document data. Then you would only need to encrypt TSF data, and you would only need to do that if you store it on disk. It would not be required for TSF data stored in NVRAM, because it is sufficiently more difficult to remove NVRAM for salvaging than it is to remove a hard disk for that purpose.

Removing T.UD.SALVAGE from PP-B

Removing T.UD.SNIFF.NET from PP-B

Assuming that network encryption is used to mitigate sniffing attacks, then by removing T.UD.SNIFF.NET from PP-B you would only need to encrypt documents in PP-A, not in PP-B. You would still need to encrypt credentials in both environments.

Does this really differentiate PP-A and PP-B?

Proposed changes are shown in the third set of columns in cells outlined in yellow. You can also see that the number of threats in each environment decreases more evenly, for whatever that's worth.

Threat analysis proposed for meeting #20

Threat ID	BEST PRACTICES RISK RATINGS				PROTECTION PROFILE IN HIERARCHY				PROPOSED NEW PROTECTION PROFILE			
	PP-A	PP-B	PP-C	PP-D	PP-A	PP-B	PP-C	PP-D	PP-A	PP-B	PP-C	PP-D
T.DOS.NET.CONNECT	Low	Moderate	Moderate	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.DOS.NET.CRAFT	Low	Moderate	Moderate	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.DOS.NET.FLOOD	Low	Moderate	High	Moderate	Y	Y	N	N	Y	Y	N	N
T.DOS.PRT.CRASH	Low	Moderate	High	Moderate	Y	Y	N	N	Y	Y	N	N
T.DOS.PRT.DELETE	Low	Moderate	High	Moderate	N	N	N	N	N	N	N	N
T.DOS.PRT.CHANNEL	Low	Moderate	High	Moderate	Y	Y	N	N	Y	Y	N	N
T.DOS.PRT.PRIORITY	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.DOS.FAX.HOOK	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.DOS.FAX.LOOP	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.DOS.FAX.TRAIN	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.DOS.FAX.VOLUME	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.DOS.PHY.ALTER	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.DOS.PHY.INTERFERE	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.RESOURCE.COPY	Moderate	Moderate	High	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.RESOURCE.PEER	Moderate	Moderate	High	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.RESOURCE.SUPPLIES	Low	Moderate	High	Moderate	N	N	N	N	N	N	N	N
T.RESOURCE.EXHAUST	Low	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.UD.SNIFF.NET	High	Moderate	Moderate	Moderate	Y	Y	N	N	Y	N	N	N
T.UD.SNIFF.EM	High	Moderate	Moderate	Moderate	Y	N	N	N	Y	N	N	N
T.UD.SNIFF.PHONE	High	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.UD.ACC.NORMAL	High	Moderate	Low	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.UD.ACC.HACK	Moderate	Moderate	Low	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.UD.PHY.OUTPUT	Moderate	Moderate	Moderate	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.UD.PHY.INPUT	Moderate	Moderate	Low	Moderate	N	N	N	N	N	N	N	N
T.UD.PHY.CAMERA	High	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.UD.PHY.EM	Moderate	Moderate	Low	Moderate	N	N	N	N	N	N	N	N
T.UD.ANALYZE	Moderate	Moderate	Low	Moderate	N	N	N	N	N	N	N	N
T.UD.SALVAGE	High	Moderate	Low	Moderate	Y	Y	N	N	Y	N	N	N
T.UD.IMP.FAX	Moderate	Moderate	Moderate	Moderate	N	N	N	N	N	N	N	N
T.UD.IMP.PRINT	High	Moderate	Moderate	Moderate	Y	N	N	N	Y	N	N	N
T.UD.IMP.SCAN	High	Moderate	Moderate	Moderate	Y	N	N	N	Y	N	N	N
T.TSF.CRED.NET	High	High	Moderate	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.TSF.CRED.EM	Moderate	Moderate	Moderate	Low	Y	N	N	N	Y	N	N	N
T.TSF.CRED.MGMT	High	High	Moderate	Moderate	Y	Y	N	N	Y	Y	N	N
T.TSF.CRED.DISK	High	Moderate	Moderate	Low	Y	Y	N	N	Y	Y	N	N
T.TSF.CRED.GUESS	High	High	High	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.TSF.CONF.DEV	Low	Moderate	Moderate	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.TSF.CONF.SEC	High	High	Moderate	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.TSF.CONF.DATE	High	Moderate	High	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.TSF.CONF.AB	High	Moderate	High	Moderate	Y	Y	Y	Y	Y	Y	Y	Y
T.TSF.SW.APPLET	High	High	High	Moderate	Y	Y	N	N	Y	Y	N	N
T.TSF.SW.UPDATE	Moderate	Moderate	Moderate	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.TSF.AUD.ACCESS	High	High	Moderate	Moderate	Y	Y	N	N	Y	N	N	N
T.TSF.AUD.ALTER	High	High	Moderate	Low	Y	Y	Y	N	Y	Y	Y	N
T.EA.PROXY	Moderate	Moderate	Moderate	Moderate	Y	Y	Y	N	Y	Y	Y	N
T.EA.DOS	Low	Moderate	High	Moderate	Y	Y	N	N	Y	Y	N	N
# threats:	30	26	16	8	30	23	16	8	30	23	16	8
delta:		-4	-10	-8		-7	-7	-8		-7	-7	-8