

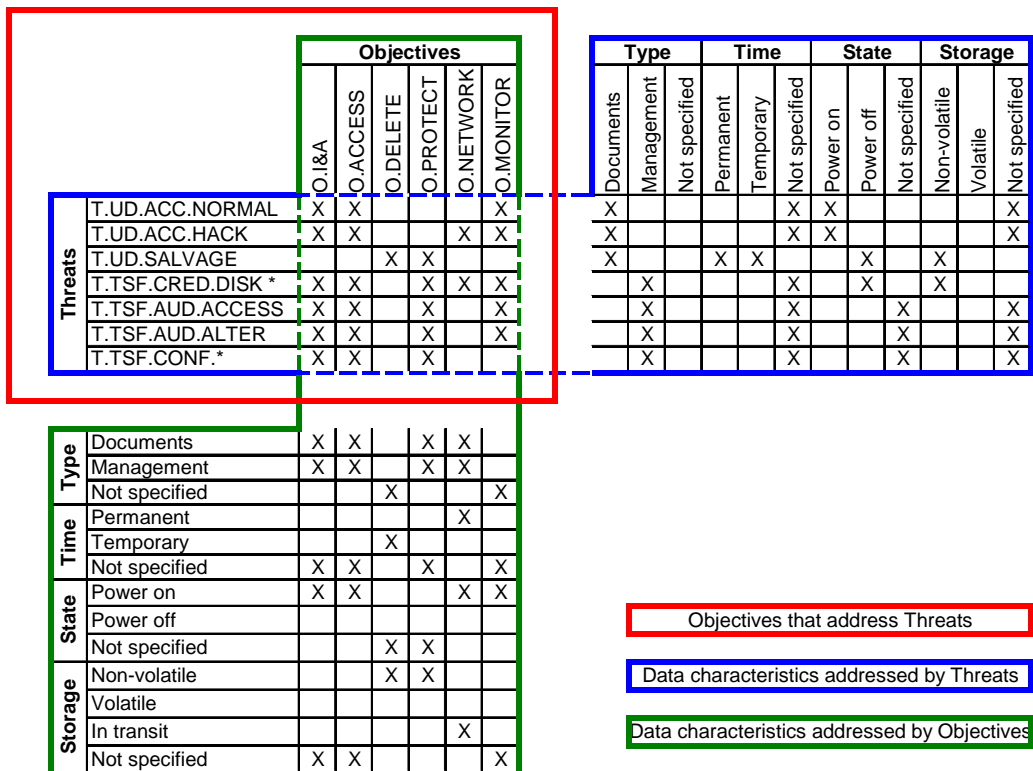
**Proposal to P2600 meeting #20, Camas WA  
 Brian Smithson, Ricoh Corporation, 6/16/06**

**Introduction**

This proposal deals with differences between PP-A and PP-B and also deals with some inconsistencies among threats and objectives related to protecting data that is stored on the HCD.

The chart, below, contains threats and objectives related to protecting data stored on the HCD. There are three outlined areas:

- The red area is a subset of P2600 threats and the objectives that are employed to address those threats.
- The blue area shows the characteristics of the data addressed by each threat, according to how those threats are currently specified.
- The green area shows the characteristics of the data addressed by each objective, according to how those objectives are currently specified.



Objectives are for T.TSF.CRED.DISK|NET|EM|GUESS|MGMT

From this chart, you can see what kinds of data are addressed by each threat and by each objective. It may be useful in the discussion of some issues.

## Issues

### **1. O.DELETE is implementation-specific (and redundant?)**

O.DELETE is an objective that partially mitigates T.UD.SALVAGE by requiring that temporary or residual data is deleted from non-volatile storage so that it cannot be recovered by removing the storage device.

Deleting data is only one way to prevent such recovery. Another way would be to encrypt temporary data. A more exotic way would be to use TCG or some other trust-based technology that only permits data access to the storage device when it is installed in the original HCD. I suppose there are other ways one might imagine.

Also, O.DELETE appears in conjunction with O.PROTECT, which says that all data will be protected from unauthorized disclosure that results from “retrieving them from nonvolatile storage”. Isn’t O.DELETE redundant?

### **2. T.TSF.CRED.DISK is a very different threat from the other T.TSF.CREDs (and it does not cover User Function Data)**

T.TSF.CRED.DISK is the Management Data equivalent of T.UD.SALVAGE.

T.TSF.CRED.DISK specifically refers to “residual or intentionally stored data”, and yet it doesn’t use O.DELETE for residual data.

T.TSF.CRED.DISK does not cover User Function 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.

### **3. Salvaging data in power-off state is a very different threat from obtaining data in a power-on state**

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.

### **4. What does O.PROTECT really mean?**

Assume for the moment that we have an objective that protects data from being retrieved from nonvolatile storage in the powered-off state. What then does O.PROTECT mean? It means that we somehow protect nonvolatile data from being disclosed during normal operation. But we already have O.I&A and O.ACCESS which should prevent such disclosure.

If access controls don’t prevent disclosure, then that means you are able to bypass access controls and read (and write?) data to nonvolatile storage. I think we need to have a little more faith in our access controls than that.

## **5. We still have a problem distinguishing PP-A from PP-B**

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.

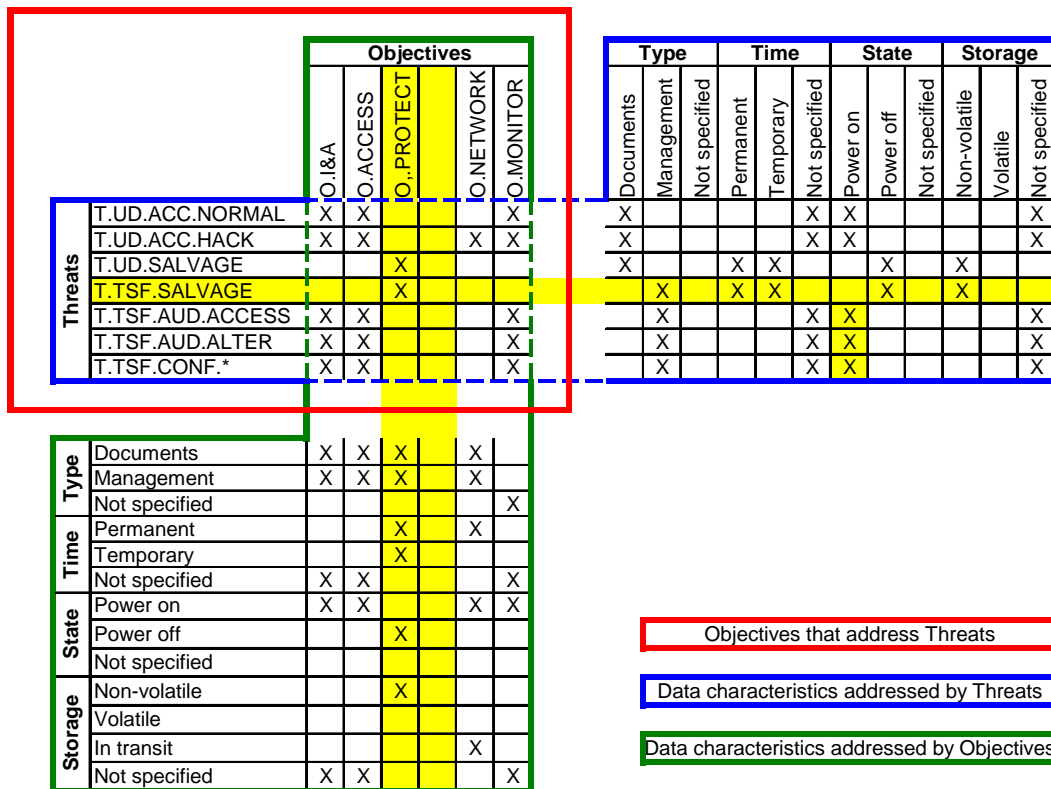
T.UD.SNIFF.EM and T.TSF.CRED.EM are best mitigated by encrypting network traffic, but one could argue that encryption is just as necessary to mitigate T.UD.IMP, T.UD.SNIFF.NET, and T.TSF.CRED.NET, so what is the difference between PP-A and PP-B when it comes to security objectives? You may still need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

# Proposals

## 1. Separate the power-on and power-off threats and objectives

- Replace T.TSF.CRED.DISK with T.TSF.SALVAGE and expand its scope to include both Management Data and User Function Data.
- Change the objective of O.PROTECT to prevent unauthorized access to data on non-volatile storage devices when disconnected from the TOE.
- Remove O.DELETE. It is adequately covered by O.PROTECT.
- Remove O.PROTECT from the list of objectives for all threats except T.UD.SALVAGE and T.TSF.SALVAGE.
- Rely on O.I&A and O.ACCESS to mitigate T.UD.ACC.\* , T.TSF.AUD.\* , and T.TSF.CONF.\*.

Here is a new chart representing these changes, marked in yellow:



## 2. Remove T.UD.SALVAGE from PP-B

I'm not exactly sure why T.UD.SALVAGE is included in PP-B. Its overall importance score was 2.1, which was the same score that T.UD.SALVAGE received for PP-C. Both were considered "moderate" risk by the numbers, but when we finalized the risk ratings, we included this threat in PP-B but not in PP-C.

By the way, T.TSF.SALVAGE would remain in PP-B. It's score (at least, T.TSF.CRED.DISK's score) was 2.4 in PP-B, which is the same score as in PP-A.

### **3. Remove T.TSF.AUD.ACCESS from PP-B**

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.

If 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 does this buy us? 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.

### **4. Remove T.UD.SNIFF.NET from PP-B**

T.UD.SNIFF.NET had an importance score of 2.4 for PP-B, which is in the "should be considered range", but on the high end. T.UD.SNIFF.NET had the same score of 2.4 for PP-C. The score was 2.9 for PP-A.

If we remove T.UD.SNIFF.NET, we would still have T.TSF.CRED.NET in PP-B. The score for T.TSF.CRED.NET was 2.9.

## **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 you won't really have any need to do disk encryption in any environment. You'll simply depend on the access controls of the operating system to protect data during operation, and use some other method ("this disk will self-destruct in five seconds...") to protect data when the TOE is powered off.

However, if you must use encryption for O.PROTECT to protect permanent data, 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.

### ***Removing T.UD.SALVAGE from PP-B***

If you must store User Document data on disk, and you implement O.PROTECT using encryption, then by removing T.UD.SALVAGE from PP-B you would only need to encrypt Documents in PP-A, not in PP-B. You would still need to encrypt TSF data in both environments.

### ***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