Collaborative Protection Profile for Hardcopy Devices Security Problem Definition

(v0.4, 2021-05-09)

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

1. Compliant Targets of Evaluation

The Target of Evaluation in this cPP is an Hardcopy Device (HCD). HCDs support job functions to convert hardcopy documents into digital form (scanning), convert digital documents into hardcopy form (printing), duplicate hardcopy documents (copying), or transmit documents over a Public Switched Telephone Network (PSTN) connection (PSTN faxing). Hardcopy documents typically take the form of paper, but can take other forms (e.g. transparencies).

For the purpose of this cPP, a conforming HCD must support at least one of the job functions printing, scanning, or copying and must support the functions network communications and administration.

Users

A conforming TOE must define at least the following two User roles:

[U.NORMAL]
Normal Users who are identified and authenticated and do not have an administrative role.

[U.ADMIN]
Administrators who are identified and authenticated and have an administrative role.

A conforming TOE may allow additional roles, sub-roles, or groups. In particular, a conforming TOE may allow several administrative roles that have authority to administer different aspects of the TOE.

Note that a User can be a human user or an external IT entity. Also, a Normal User can be a Local User interacting with the TOE using its physical operator console or a Network User interacting with the HCD using programs installed on personal computers or other IT devices external to the HCD which communicate with the HCD through the LAN.

Assets

User Assets:

[D.USER.DOC]

From a User's perspective, the primary Asset to be protected in a TOE is User Document Data.

[D.USER.JOB]

A User's job instructions, User Job Data (information related to a User's Document or Document Processing Job), may also be protected if their compromise impacts the protection of User Document Data. Together, User Document Data and User Job Data are considered to be User Data.

As an illustrative example, data sent by a Network User for printing contains a User's Document [D.USER.DOC] which must not be accessed by anyone else, and job instructions such as the destination to send scanned Documents [D.USER.JOB] which must not be altered by anyone else.

Administrator Assets:

From an Administrator's perspective, the primary Asset to be protected in a TOE is data that is used to configure and monitor the secure operation of the TOE. This kind of data is considered to be TOE Security Functionality (TSF) Data.

There are two broad categories for this kind of data:

1. Protected TSF Data, which may be read by any User but must be protected from unauthorized modification and deletion [D.TSF.PROT]; and,
2. Confidential TSF Data, which may neither be read nor modified or deleted except by authorized Users [D.TSF.CONF].

Examples of TSF Data include, but are not limited to:

- Firmware and/or software in the HCD (against unauthorised modification or deletion)
- Audit records generated by the HCD (against unauthorised modification or deletion)
- User authentication and authorization information

An illustrative example is data that is used by the TOE to identify and authenticate authorized Users. Typically, a username that is used for identification may be read by anyone but must be protected from unauthorized modification and deletion [D.TSF.PROT]. In contrast, a User's password that is used for authentication must be confidential, prohibiting any Unauthorized Access [D.TSF.CONF].

If TSF Data is compromised, it can be used for a variety of malicious purposes that include elevation of privileges, accessing stored Documents, redirecting the destination of processed Documents, masquerading as an authorized User or Administrator, altering the operating software/firmware of the TOE, and attacking External IT Entities.

In a conforming TOE, TSF Data is clearly identified and categorized as either Protected TSF Data or Confidential TSF Data.

From a network security perspective, it is important to ensure the secure operation of the TOE and other IT entities in its Operational Environment. Since the Operational Environment is outside of the TOE, Organizational Security Policies are employed to address protection of the Operational Environment.

2. Security Problem Definition

2.1 Threats

The following are Threats against the TOE that are countered by conforming products.

1. Unauthorized Access to User Data

An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component [T.UNAUTHORIZED_ACCESS]. For example, depending on the design of the TOE, the attacker might access the printed output of a Network User's print job, or modify the instructions for a job that is waiting in a queue, or read User Document Data that is in a User's private or group storage area.

2. Unauthorized Access to TSF Data

An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces or the physical Nonvolatile Storage component [T.TSF_COMPROMISE]. For example, depending on the design of the TOE, the attacker might use Unauthorized Access to TSF Data to elevate their own privileges, alter an Address Book to redirect output to a different destination, or use the TOE's Credentials to gain access to an external server.

An attacker may cause the installation of unauthorized software/firmware on the TOE [T.UNAUTHORIZED_UPDATE]. For example, unauthorized software/firmware could be used to gain access to information that is processed by the TOE, or to attack other systems on the LAN.

3. Network Communication Attacks

An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication [T.NET_COMRPOMISE]. For example, here are several ways that network communications could be compromised: By monitoring clear-text communications on a wired LAN, the attacker might obtain User Document Data, User Credentials, or system Credentials, or hijack an interactive session. The attacker might record and replay a network communication session in order to log into the TOE as an authorized User to access Documents or as an authorized Administrator to change security settings. The attacker might masquerade as a trusted system on the LAN in order to receive outgoing scan jobs, to record the transmission of system Credentials, or to send malicious data to the TOE.

4. Malfunction

A malfunction of the TSF may cause loss of security if the TOE is permitted to operate while in a degraded state [T.TSF_FAILURE]. Hardware or software/firmware malfunctions can produce unpredictable results, with a possibility that security functions will not operate correctly.

5. Weak Cryptography

An unauthorized user or attacker that observes network traffic transmitted to and from the TOE may cryptographically exploit poorly chosen cryptographic algorithms, random bit generators, ciphers or key sizes [T.WEAK_CRYPTO].

2.2 Assumptions

The following assumptions must be upheld so that the objectives and requirements can effectively counter the threats described in this Protection Profile.

1. Physical Security

Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment [A.PHYSICAL]. The TOE is assumed to be located in a physical environment that is controlled or monitored such that a physical attack is prevented or detected.

2. Network Security

The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface [A.NETWORK]. The TOE is not intended to withstand network-based attacks from an unmanaged network environment.

3. Administrator Trust

TOE Administrators are trusted to administer the TOE according to site security policies [A.TRUSTED_ADMIN]. It is the responsibility of the TOE Owner to only authorize administrators who are trusted to configure and operate the TOE according to site policies and to not use their privileges for malicious purposes.

4. User Training

Authorized Users are trained to use the TOE according to site security policies [A.TRAINED_USERS]. It is the responsibility of the TOE Owner to only authorize Users who are trained to use the TOE according to site policies.

2.3 Organizational Security Policies

The following are Organizational Security Policies (OSPs) that are upheld by conforming products.

1. User Authorization

Users must be authorized before performing Document Processing and administrative functions [P.AUTHORIZATION]. Authorization allows the TOE Owner to control who is able to use the resources of the TOE and who is permitted to perform administrative functions.

2. Auditing

Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity [P.AUDIT]. Stored on an External IT Entity and also in the TOE, an audit trail makes it possible for authorized personnel to review and identify suspicious activities and to account for TOE use as may be required by site policy or regulations.

3. Protected Communications

The TOE must be able to identify itself to other devices on the LAN [P.COMMS_PROTECTION]. Assuring identification helps prevent an attacker from masquerading as the TOE in order to receive incoming print jobs, recording the transmission of User Credentials, or sending malicious data to External IT Entities.

4. Storage Encryption

If the TOE stores User Document Data or Confidential TSF Data on Nonvolatile Storage Devices, it will encrypt such data on those devices [P.STORAGE_ENCRYPTION]. Data is assumed to be protected by the TSF when the TOE is operating in its Operational Environment. However, if Nonvolatile Storage Devices are removed from the TOE for Servicing, redeployment to another environment, or decommissioning, an attacker may be able to expose or modify User Document Data or Confidential TSF Data. Encrypting such data prevents the attacker from doing so without access to encryption keys or keying material.

Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on any Nonvolatile Storage Device without protection [P.KEY_MATERIAL]. Unauthorized possession of key material in cleartext may allow an attacker to decrypt User Document Data or Confidential TSF Data.

5. PSTN Fax-Network Separation (conditionally mandatory)

If the TOE includes a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN [P.FAX_FLOW]. The TOE is assumed to be in an Operational Environment that is protected, such as by an external firewall. However, the PSTN fax modem may be connected to a public switched telephone network. Ensuring separation of the PSTN fax and network prevents an attacker from using the PSTN fax modem to attack the TOE or its protected environment.

6. Image Overwrite (optional)

Upon completion or cancellation of a Document Processing job, periodically, or when requested by an authorized administrator, residual image data in the TOE shall be made irretrievable from its Nonvolatile Storage Devices [P.IMAGE_OVERWRITE]. A customer may be concerned that image data that has been dereferenced by the TOE operating software/firmware may remain on Nonvolatile Storage Devices in the TOE after a Document Processing job has been completed or cancelled. Such customers desire that the image data be made unavailable by overwriting it with other data or by destroying its cryptographic key.p

7. Purge Data (optional)

The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices [P.PURGE_DATA]. A customer may be concerned that data which is considered confidential in the

Operational Environment may remain in Nonvolatile Storage Devices in the TOE after the TOE is permanently removed from its Operational Environment to be decommissioned from service or to be redeployed to a different Operational Environment. Such customers desire that all customer-supplied User Data and TSF Data be purged from the TOE so that it cannot be retrieved outside of the Operational Environment.

8. Root of Trust

The vendor provides a Root of Trust (RoT) that is comprised of the TOE firmware, hardware, and pre-installed public keys or required critical security parameters, free of intentionally malicious capabilities [P.ROT_INTEGRITY]. The platform trusts the RoT since it cannot verify the integrity and authenticity of the RoT.

3. Security Objectives

3.1 Security Objectives for the TOE

The following Security Objectives will be fulfilled by the TOE.

3.1.1 User Authorization

The TOE shall perform authorization of Users in accordance with security policies [O.USER_AUTHORIZATION].

This objective supports the policy that Users are authorized to administer the TOE or perform Document Processing functions that consume TOE resources. Users must be authorized to perform any of the Document Processing functions present in the TOE.

The mechanism for authorization is implemented within the TOE, and it may also depend on a trusted External IT Entity. If a conforming TOE supports more than one mechanism, then each should be evaluated as separate modes of operation.

In the case of printing (if that function is present in the TOE), User authorization may take place after the job has been submitted but must take place before printed output is made available to the User.

Users must be authorized to perform PSTN fax sending functions and document storage and retrieval functions, if such functions are provided by the conforming TOE.

Note that the TOE can receive a PSTN fax without any User authorization, but the received Document is subject to access controls.

3.1.2 User Identification and Authentication

The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles [O.USER_I&A].

The mechanism for identification and authentication (I&A) is implemented within the TOE, and it may also depend on a trusted External IT Entity (e.g., LDAP, Kerberos, or Active Directory). If a conforming TOE supports more than one mechanism, then each should be evaluated as separate modes of operation.

3.1.3. Access Control

The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies [O.ACCESS_CONTROL].

The guiding principles for access control security policies in this PP are:

1. User Document Data [D.USER.DOC] can be accessed only by the Document owner or an Administrator.
2. User Job Data [D.USER.JOB] can be read by any User but can be modified only by the Job Owner or an Administrator.
3. Protected TSF Data [D.TSF.PROT] are data that can be read by any User but can be modified only by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.
4. Confidential TSF Data [D.TSF.CONF] are data that can only be accessed by an Administrator or (in certain cases) a Normal User who is the owner of or otherwise associated with that data.

The Security Target of a conforming TOE must clearly specify its access control policies for User Data and TSF Data.

3.1.4. Administrator Roles

The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions [O.ADMIN_ROLES].

This objective addresses the need to have at least one Administrator role that is distinct from Normal Users. A conforming TOE may have specialized Administrator sub-roles, such as for device management, network management, or audit management.

3.1.5. Software/Firmware Update Verification

The TOE shall provide mechanisms to verify the authenticity of software/firmware updates [O.UPDATE_VERIFICATION].

This objective addresses the concern that malicious software/firmware may be introduced into the TOE as a software/firmware update. Verifying authenticity, such as with a digital signature or published hash, is required. Access control by itself does not satisfy this objective.

3.1.6. Self-test

The TOE shall test some subset of its security functionality to help ensure that subset is operating properly [O.TSF_SELF_TEST].

A malfunction of the TOE may compromise its security if the malfunction is not detected and the TOE is allowed to operate. Self-test is intended to detect such malfunctions. It is performed during power-up.

3.1.7. Communications Protection

The TOE shall have the capability to protect LAN communications of User Data and TSF Data from Unauthorized Access, replay, and source/destination spoofing [O.COMMS_PROTECTION]. This objective addresses the common concerns of network communications:

1. Sensitive data or Credentials are obtained by monitoring LAN data outside of the TOE.
2. A successfully authenticated session is captured and replayed on the LAN, permitting the attacker to masquerade as the authenticated User.
3. Sensitive data or Credentials are obtained by redirecting communications from the TOE or from an External IT Entity to a malevolent destination.

3.1.8. Auditing

The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE [O.AUDIT].

The TOE must be able to send audit data to a trusted External IT Entity (e.g., an audit server such as a syslog server). Audit data may also be stored in the TOE with appropriate access controls to ensure confidentiality and integrity. If a conforming TOE supports both mechanisms, then each should be evaluated as separate modes of operation.

3.1.9. Storage Encryption (conditionally mandatory)

If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices. [O.STORAGE_ENCRYPTION].

This objective addresses the concern that User Document Data or Confidential TSF Data on a Field-Replaceable Nonvolatile Storage Device may be exposed if the device is removed from the TOE, such as for Servicing, Redeployment to another environment, or Decommissioning.

3.1.10. Protection of Key Material (conditionally mandatory)

The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material [O.KEY_MATERIAL].

This objective addresses the concern that unauthorized possession of keys or key material may be used to decrypt User Document Data or Confidential TSF Data.

3.1.11. PSTN Fax-Network Separation (conditionally mandatory)

If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function [O.FAX_NET_SEPARATION].

This objective addresses customer concerns about having a telephone line connected to a device that is inside their firewall. Depending on implementation, it may be satisfied in different ways, such as by system architecture (no data path from the PSTN fax interface to the network interface), by system design (fax chipset recognizes only PSTN fax protocols), or by active security function (flow control).

3.1.12. Image Overwrite (optional)

Upon completion or cancellation of a Document Processing job, periodically, or when requested by an authorized administrator, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices [O.IMAGE_OVERWRITE]. This objective addresses customer concerns that image data may remain on Field-Replaceable Nonvolatile Storage Devices in the TOE after a Document Processing job has been completed or cancelled.

3.1.13. Purge Data (optional)

The TOE provides a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices [O.PURGE_DATA]. This objective addresses customer concerns that data that is protected in the Operational Environment may remain in Nonvolatile Storage Devices after the TOE is permanently removed from its Operational Environment to be decommissioned from service or to be redeployed to a different Operational Environment.

3.1.14. Authentication Failures

The TOE resists repeated attempts to guess authorization data [O.AUTH_FAILURES] by responding to consecutive failed attempts in a way that prevents an attacker from exploring a significant amount of the space of possible authorization data values.

Note: This Security Objective needs to be Conditionally Mandatory based on the condition that the TOE has an internal authentication mechanism. Also, the HCD must ensure the HCD does not outlaw 3rd Party external authentication mechanisms.

3.1.15. Firmware Integrity

The TOE ensures its own integrity has remained intact [O.FW_INTEGRITY] and attests its integrity to outside parties on request.

3.1.16. Strong Cryptography

The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards [O.STRONG_CRYPTO], including support for random bit generation based on recognized standards and a source of sufficient entropy. The TOE uses key sizes that are recognized as providing sufficient resistance to current attack capabilities.

3.2. Security Objectives for the Operational Environment

The following Security Objectives must be provided by the Operational Environment. Additional details about objectives for the Operational Environment are in Appendix A.7.

3.2.1. Physical Protection

The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes [OE.PHYSICAL_PROTECTION].

Due to its intended function, this kind of TOE must be physically accessible to authorized Users, but it is not expected to be hardened against physical attacks. Therefore, the environment must provide an appropriate level of physical protection or monitoring to prevent physical attacks.

3.2.2. Network Protection

The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface [OE.NETWORK_PROTECTION].

This kind of TOE is not intended to be directly connected to a hostile network. Therefore, the environment must provide an appropriate level of network isolation.

3.2.3. Trusted Administrators

The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes [OE.ADMIN_TRUST].

Administrators have privileges that can be misused for malicious purposes. It is the responsibility of the TOE Owner to grant administrator privileges only to individuals whom the TOE Owner trusts.

3.2.4. Trained Users

The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them [OE.USER_TRAINING].

Site security depends on a combination of TOE security functions and appropriate use of those functions by Normal Users. Manufacturers may provide guidance to the TOE Owner regarding the TOE security functions that apply to Normal Users.

3.2.5. Trained Administrators

The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly [OE.ADMIN_TRAINING].

This kind of TOE may have many options for enabling and disabling security functions. Administrators must be able to understand and configure the TOE security functions to enforce site security policies.