Collaborative Protection Profile for Hardcopy Devices Security Problem Definition

(v0.3, 2021-04-06)

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

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

[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.

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].

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 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 on the TOE [T.UNAUTHORIZED_UPDATE]. For example, unauthorized software 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 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.

5. 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 [A.ROT_INTEGRITY]. The platform trusts the RoT since it cannot verify the integrity and authenticity of the RoT.

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 (or, optionally, 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 that 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 bypass the firewall or other external protection to access the protected environment.

6. 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 Nonvolatile Storage Devices [P.IMAGE_OVERWRITE]. A customer may be concerned that image data that has been dereferenced by the TOE operating software 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.

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.

3. Security Objectives

1. O.AUTH_FAILURES

The TOE resists repeated attempts to guess authorization data 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.

2. O.FW_INTEGRITY

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

3. O.STRONG_CRYPTO

The TOE implements strong cryptographic mechanisms and algorithms according to recognized standards, 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.