Common Criteria Recognition Arrangement
Development Board

CCDB HCD WG

Title: Hardcopy Device Essential Security Requirements
Maintained by: CCDB Hardcopy Devices (HCD) Working Group
Version: 0.7
Date of issue: *2020-May-08*
Supersedes:

Status

The CCDB Working Group for Hardcopy Devices (HCD) has been approved by the CCDB to support the establishment of the international Technical Community for the Hardcopy Devices (HCD). The CCDB WG consists of representatives of the following CCRA participants: Republic of Korea and Japan.
This draft of the ESR is the updated version to incorporate JP scheme and CCRA expert (NIAP) comments on the earlier draft by KR scheme.

Background and Purpose

This document describes a high-level set of security requirements that a Hardcopy Device (hereafter 'HCD') will satisfy when evaluated against the collaborative Protection Profile (cPP) written for such technology.

In general, a Hardcopy Device[1] is a device that provides various functions such as printing, scanning, copying, or faxing via input/output interfaces, and usually has additional security features to enhance its functions. HCDs can be implemented and configured in many different ways depending on the purpose of usage. This document considers HCDs with at least one of functions printing, scanning, or copying. Network communication and administration capabilities are also required. However, this does not mean that the document excludes those HCDs with other capabilities such as sending and receiving documents over PSTN using standard facsimile protocols, or storing and retrieving electronic documents in the HCD. Also, HCDs may not support network communications nor administration capabilities, but, this document addresses HCDs with those capabilities. Finally, HCDs can have audit logs so that security-relevant events and HCD use can be monitored by authorized personnel.

Physically, a Hardcopy Device is a product consisting of hardware, firmware, and/or software. HCDs may or may not embed a nonvolatile storage device, or use removable/Field-Replaceable nonvolatile storage device to store data to be protected. This document expects that HCDs provide proper protection on the stored data to be protected on a nonvolatile storage device[2]. Also, HCDs provide a mean for updating firmware or software to verify them.

The expectation is that HCDs will employ cryptographic means to provide the necessary protection of transmitted/stored data to be protected by explicitly specifying international standards for cryptographic primitives/protocols defined by appropriate international standards bodies.[3]

[1] Note that the CCRA portal refers to 'Hardcopy Devices' as 'Multi-Function Devices'.
[2] Note that a nonvolatile storage device is either non-Field-Replaceable or Field-Replaceable. In this document, the same security requirements are levied on both types of the nonvolatile storage device.
[3] This document expects that the resulting cPP shall not contain requirements that have a dependency on national conformity assessment schemes for cryptography. Instead, it is expected that the iTC will provide Supporting Documents (SDs), developed according to the WTO 6 principles, to be approved by the CCDB then used by each CCRA schemes. Refer to the CCRA Annex K for more details.

Additionally, it is expected that HCDs will provide security capabilities such as identification and authentication of the user of the HCD including administrator role, secure setting/configuration of the HCD, access control to data stored on the HCD, audit record generation for security relevant events, and self-testing.

Use Case(s)

The HCD is a product consisting of hardware, firmware, and/or software used for the support of following primary functions:

- Printing function: The user sends a document to the HCD over a LAN to print it (converting an electronic document to hardcopy form),
- Scanning function: The user scans a document on the HCD and the HCD sends the digital image to outside of the HCD (converting a hardcopy document to electronic form),
- Copying function: The user copies a document on the HCD (i.e. scans a document on the HCD and the HCD prints the document). (duplicating a hardcopy document), and
- Faxing function[4]: The user sends and receives documents on the HCD over the public switched telephone network (PSTN) using standard facsimile protocols.

Hardcopy documents typically take the form of paper, but can take other forms. And the electronic document can be stored on the volatile or (non-Field-Replaceable or Field-Replaceable) nonvolatile storage devices. Thus the HCD is also used for the support of following functions:

- Storing and retrieving function: The user stores or retrieves an electronic document in the HCD, and
- Use of integrated nonvolatile storage device: Data to be protected is stored on the integrated nonvolatile storage devices (e.g. Hard Disk Drive (HDD)), and the authorized personnel removes the HCD and the nonvolatile storage device itself from service in its operational environment to perform preventative maintenance, repairs, or other servicing-related operations.

The HCD is connected to the network to send or receive data including documents and administrative data over a Local Area Network (LAN).

The iTC shall consider all use cases above to specify security requirements of the cPP for HCD, and the HCD claims conformance to the resulting cPP shall address at least one of the functions printing, scanning, or copying. If the HCD presents PSTN faxing function, then the HCD claims conformance to the resulting cPP shall address faxing function too (i.e. it is conditionally mandated depending on the implementation). Similarly, if the HCD presents storing and retrieving function or uses nonvolatile storage device to store data to be protected, then the HCD claims conformance to the resulting cPP shall address these too (i.e. it is conditionally mandated depending on the implementation).

The HCD shall be used considering following functions to enhance use cases above:

- Setting/Configuration function: The authorized role through identification and authentication is provided to configures the security settings of the HCD,
- Auditing function: The HCD generates audit records for the security related events and stores them inside and outside of the HCD,
- Firmware/software updating function: HCDs provide a mean for updating firmware and/or software to verify them, and
- Self-testing function: The HCD checks its correct operation when it is powered on.

[4] Note that the PSTN faxing function is only considered in the Use Cases.

The HCD may be used considering following case:

- Redeploying or Decommissioning the HCD: The authorized personnel remove the HCD from service in its operational environment to move it to a different operational environment, to permanently remove it from operation, or otherwise change its ownership. The HCD may have the capability to make all customer data that may be present in the HCD unavailable for recovery if it is removed from the operational environment.

Resources to be protected

- User document data processed in the HCD (against unauthorised disclosure, modification or deletion).
- User job data[5] related to documents in the HCD (against unauthorised modification or deletion).
- Transmitted communication data on the network (against unauthorised disclosure or modification).
- The HCD critical data[6] (for integrity protection) such as the user’s ID related to security configuration and monitoring of the HCD (against unauthorised modification or deletion).
- The HCD critical data (for confidentiality protection) such as the user’s password related to security configuration or administration of the HCD (against unauthorised disclosure, modification or deletion).
- Firmware and/or software in the HCD (against unauthorised modification or deletion).
- Audit records generated by the HCD (against unauthorised modification or deletion).

Attacker access

- An attacker may access (read, modify, or delete) user document data or change (modify or delete) user job data in the HCD through one of the HCD’s interfaces.
- An attacker may gain unauthorized access to the HCD critical data in the HCD through one of the HCD’s interfaces.
- An attacker may cause the installation of unauthorized firmware and/or software on the HCD.
- An attacker may access data in transit or otherwise compromise the security of the HCD by monitoring or manipulating network communication.
- A malfunction of the security functionality of the HCD may cause loss of security if the HCD is permitted to operate while in a degraded state.

Attacker Resources

- The attacker may take sufficient times for finding vulnerabilities or developing attack methods. It is assumed that the knowledge level of expected attacker may be possible as a layman through an expert.
- There is numerous PC software providing HCD users with a variety of applications delivered by each HCD vendor. Such software could be a target of reverse engineering and a source of information available for the attackers.

[5] User function data.
[6] TSF data.

- It is expected that the attacker will find it difficult to attempt attacks frequently in the expected operational environment. But if the attacker is a malicious user, the attacker may attempt to attack frequently by means of multiple kinds of remote access tools via LAN.
- The attacker may use commercially and/or publicly available software/tools/equipment to test and attack the HCD.
- There are many customer engineers who had already retired from the vendors, and the confidential information may exist on the Internet. It is possible for the attackers to use this confidential information which has not been managed in a secure manner.

Boundary of Device

The HCD is a product physically consisting of hardware, firmware, and/or software, and all of the security functionality is contained and executed within the physical boundary of the HCD. Those parts that are not security relevant do not need to be considered. If it is possible for users to connect personal storage devices (such as portable flash memory devices) to the HCD, those devices and data contained within them are out of scope.

Essential Security Requirements

- The HCD shall perform authorization of users in accordance with security policies
- The HCD shall perform identification and authentication of users for operations that require access control, user authorization, or administrator roles
- The HCD shall enforce access controls to protect user data and the HCD critical data in accordance with security policies.
    - User document data can be accessed only by the document owner or an administrator.
    - Shared user document data can be accessed by the authorized users if the HCD has such a capability.
    - User job data can be read by any user but can be modified only by the job owner or an administrator.
    - The HCD critical data (for integrity protection) 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.
    - The HCD critical data (for confidentiality protection) 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 HCD shall ensure that only authorized administrators are permitted to perform administrator functions.
- The HCD shall provide mechanisms to verify the authenticity of firmware and/or software updates.
- The HCD shall test some subset of its security functionality to ensure that the security functionality is not compromised by the detectable malfunction.
- The HCD shall have the capability to protect LAN communications of transmitted user data and the HCD critical data from unauthorized access, replay and source/destination spoofing.
- The HCD shall generate audit data, and be capable of sending it to a trusted external IT entity and store it in the HCD.

- The HCD shall ensure logical separation of the PSTN and the LAN if it provides a PSTN faxing function.
- The HCD shall encrypt user document data and/or the HCD critical data (for confidentiality protection) stored on the nonvolatile storage device if it uses nonvolatile storage device for the purpose of storing those data. To support encryption, the HCD shall maintain key chains in such a way that keys and key materials are protected. Note that the initial data of the key chain stored on the nonvolatile storage device without protection do not meet the requirement.
- The HCD shall verify the hardware-anchored integrity of firmware/software, including initial boot, operating system, and applications.

Assumptions

- Physical security, commensurate with the value of the HCD and the data it stores or processes, is assumed to be provided by the environment.
- The operational environment is assumed to protect the HCD from direct, public access to its LAN interface.
- Administrators of the HCD are trusted to administrate the HCD according to site security policies.
- Authorised users are trained to use the HCD according to site security policies.

Optional Extensions

- The HCD may provide a capability that user document data and/or the HCD critical data (for confidentiality protection) stored on the nonvolatile storage device is made unavailable upon completion or cancellation of a document processing job or periodically by permanently irretrievable means.
- The HCD may provide a capability that authorized administrators can make all customer-supplied user data and the HCD critical data permanently irretrievable from the non-volatile storage device.

Outside the Scope of Evaluation

- Resistance against physical attacks of the HCD directly from outside are not to be considered.
- Anti-malware checks on user data transferred to and from the HCD are not to be considered. Note that vulnerability analysis on the exploits to the HCD using crafted user data is in the scope of evaluation.