Common Criteria Recognition Arrangement
Development Board

CCDB USB cPP WG

Title: USB Portable Storage Device Essential Security Requirements
Maintained by: CCDB Work Group for USB Portable Storage Devices
Version: 2.0
Date of issue: *2013-October-28*
Supersedes: **N/A**

Status

The CCDB Working Group approves this draft of the ESR for distribution to the international Technical Community. The CCDB WG consists of representatives of the following CCRA participants: Australia, Denmark, Finland, Germany, Japan, Netherlands, Singapore, Sweden, Turkey, UK, and USA.

Background and Purpose

The following provides a high level set of security requirements that a USB Portable Storage Device, (hereafter referred to as device) will satisfy when evaluated against the Collaborative PP (cPP) written for such technology. In addition to stating what properties the device will minimally exhibit, the ESR also expresses functionality that could be optionally considered as an extension, but goes beyond the expected baseline. Furthermore, the ESR identifies aspects that are definitely outside the desired scope so as to limit the final set of security functional requirements specified in the cPP, as well as the assurance activities performed during the course of evaluation. The reason behind this scoping of the device's capabilities to be specified in the cPP is to ensure that objective and repeatable assurance activities can be captured in the cPP while still delivering a cPP in a timely manner. Another factor is to ensure the security functionality prescribed is not well beyond the current best practices and is achievable by multiple developer products. Having said that, this ESR allows for the specification of an optional capability – updating the device's system files (e.g., patches). The device does not have to provide a means for updating system files, but if it does, a conforming Security Target (ST) will include the requirements that ensure it will do so in a trusted manner.

The expectation is that the device will employ cryptographic means to provide the necessary protection of user data, the strength of which lies in the quality of the cryptographic algorithms and the entropy of the authorization factor (e.g., password, passphrase). The device will encrypt the user data as it is stored on the device, and decrypt the data as it leaves the device. The host computer plays no role in the encryption/decryption of user data.

In addition to protecting the user data, the device is also responsible for ensuring the residing system files (e.g., software, firmware) cannot be modified by untrusted entities through the logical interface. The intent here is to ensure the device cannot be compromised by malware running on a host computer, which could then use the device as a delivery mechanism to spread the malware. This protection ensures "unauthorized" modifications – modifications or replacement of any arbitrary system files, including configuration files or critical data, such as a digital certificate, cannot be performed through the logical interface. As stated above, it may be possible for a developer to build a device that allows for product updates. If this capability is provided, the updates or modification must be done in a controlled and trusted manner that employs a form of cryptography, such as a digital signature.

The cryptographic mechanisms (e.g., algorithms, key sizes) must not exhibit publicly known vulnerabilities or weaknesses, and are subject to approval by the appropriate cryptographic authorities, which are represented by the national schemes committing to the ESR and the procurement of devices compliant with the resulting cPP.

It is worth noting that while this ESR identifies attacks that may be mounted against the device, that does not mean the device is expected to mitigate all known attack vectors. Since the authorization factor will not

persistently be stored on the device, a physical attack will not result in the disclosure of the encrypted user data without performing a cryptanalysis. However, this ESR does explicitly exclude from evaluation the device's ability to thwart an attack where the device is stolen, physically tampered with, returned to the user, who in turn uses the device unknowing that the device has been compromised, and the attacker re-obtains the device and extracts the authorization factor and gains access to the user data (a.k.a. "The Evil Maid" attack).

Use Case(s)

The device is a portable storage device that provides a USB interface for connecting to a host computer. The device does not provide for the use of removable media (e.g., Compact Disk/DVD, Secure Digital memory cards), this limits that ability of an attacker to obtain encrypted user data without obtaining the device itself. It is intended to be used for the following scenarios:

- Transfer of sensitive data between two host computers.
- Long term storage of sensitive data.

Resources to be protected

- User data stored on the device (from unauthorized disclosure).
- The device's system files (from unauthorized modification).

Attacker access

- Attacker gains physical access to the device and can attempt to retrieve or modify the user data through the logical interface or by physical tampering.
- Attacker modifies the system files through the logical interface (an attacker could modify the system files through a physical attack, but that is outside the scope of this ESR).

Attacker Resources

- Arbitrary amount of time.
- Commercially and/or publicly available equipment/ software/knowledge (including electron microscopes, Focused Ion Beam instruments, etc.). The examples of sophisticated tools are provided to convey the expectation that cryptography will be used to protect the data and system files, and that even if such tools were employed by an attacker, a cryptanalysis would be required to discern any meaning to the user data.

Boundary of Device

- The hardware, firmware and software of the device define the physical boundary.
- All of the security functionality is contained and executed solely within the physical boundary of the device.

Essential Security Requirements

- A user must be authorized by the device before accessing any user data on the device
    - Minimum strength (entropy of authorization factor) for authorizing the user access to the data contained within the device subject of approval by appropriate cryptographic approval authorities of committed nations.
    - The entropy of the authorization factor shall not be weakened by choices of algorithms or any conditioning that is used in the key derivation process.
    - Authorization factor shall not be persistently stored on the device.
- The device implements cryptography as a protection mechanism to prevent unauthorized modification of the system files residing on the device.
- The protection of user data and system files is carried out by employing cryptography on the device (i.e., the host computer plays no role in protecting the user data and system files while they reside on the device).
- Any form of data recovery from the device must be configurable to be disabled.
- The device shall not be bootable.

Assumptions

- The host computer is trusted to not disclose the authorization factor.

Optional Extensions

- Updates to the device's system files are optional.
    - If the device provides an update mechanism to system files, the updates must be made securely (e.g., commensurate with the protection afforded user data - cryptography).

Outside the Scope of Evaluation

- Resistance against physical attacks of the device, where the device is compromised and returned to the user, are not to be considered.
- Anti-malware checks on the user data transferred to and from the device.