Biometric Product Essential Security Requirements - CMFA

Table of Contents

Status . . . 1
References . . . 2
Glossary . . . 2
Background and Purpose . . . 2
Conventional authentication . . . 2
CMFA . . . 3
CMFA boundary . . . 3
CMFA configuration . . . 5
Use Case(s) . . . 5
Resources to be protected . . . 5
Attacker access . . . 5
Attacker Resources . . . 6
Boundary of Device . . . 6
Essential Security Requirements . . . 6
Assumptions . . . 6
Optional Extensions . . . 7
Outside the Scope of Evaluation . . . 7

Title	Biometric Product Essential Security Requirements - CMFA
Maintained by	Biometrics Security iTC
Version	1.0
Date of Issue	May 4, 2021
Supersedes	N/A

Status

The Biometrics Security iTC has been requested by vendors to develop an Essential Security Requirements (ESR) for Continuous Multifactor Authentication (CMFA) products. The CMFA ESR version 1.0 contains material generated by the members of the BIO-iTC, for a PP-Module to be reviewed by the membership of the BIO-iTC and endorsed in 2021.

References

- [BIOPP-Module] - collaborative PP-Module for Biometric enrolment and verification - for unlocking the device - [BIOPP-Module]
- [PP_MD_V3.2] - Protection Profile for Mobile Device Fundamentals, Version: 3.2.

Glossary

Computer

A self-contained device which is composed of a hardware platform and its system software (operating system and applications). The device is typically some sort of general purpose computing platform, such as a laptop, tablet or smartphone that is designed to be portable (though this is not required).

Confidence rating

The resulting output from the CMFA Engine based on the provided inputs that is used to determine the authentication status of the user.

Input trust (Trusted input)

The level of reliability of the input to the CMFA product. For example, how easy (or difficult) it may be to attack the sensor and send unreliable data to the CMFA product.

- The term "trusted sensors" may be used to mark sensors with a high level of reliability

Background and Purpose

This document describes the high-level fundamental security requirements expected of any computers that implement CMFA. It is intended to provide a minimal, baseline set of requirements which can be built upon by the future PP-Module to provide an overall set of security solutions for CMFA running on a computer.

Conventional authentication

Most computers implement user authentication functionality. This type of authentication is called "conventional authentication" hereafter. Conventional authentication requires the user to successfully pass a verification at a point in time to unlock the computer. In case of a mobile device, the [PP_MD] requires the mobile device to authenticate a user with password or biometric and lock the computer after the fixed time of inactivity.

Conventional authentication suffers from several shortcomings such as the inconvenience of frequent unlocking and several adversarial attacks (e.g., shoulder surfing and smudge attacks for password authentication). Conventional authentication is at a point in time, so once the user has authenticated successfully, there is no way to know if the computer is still under the control of the authenticating user. CMFA extends the conventional authentication and delivers continuous and transparent authentication to reduce such shortcomings.

CMFA

CMFA determines the current level of authentication of a user, the confidence rating, by expanding on conventional authentication using inputs received through sensors or components attached to or part of a computer. This confidence rating achieves the highest value right after the conventional authentication succeeds and begins to decline as time progresses as the value of the conventional authentication event decreases. However, CMFA can increase the confidence rating, for example, if CMFA recognizes user's voice from a microphone, or maintain the confidence rating, for example, if CMFA recognizes that the computer is in a known place (e.g. office) and connected to the defined (trusted) Wi-Fi network. CMFA can also decrease the confidence rating, for example, if CMFA detects rapid changes to location, such as appearing in a new location immediately.

To properly determine a confidence rating, CMFA must be configured with an adequate set of inputs. The set of inputs must, in combination, be able to provide protection against attacks that meet the level of Basic Attack Potential.

The confidence rating is continuously maintained and updated by CMFA and where it can be used by the computer to determine whether to remain in the unlocked state or transit to the locked state based on the rating. The confidence rating may also be provided to external program or service for more granular access control.

CMFA boundary

CMFA, the TOE, is composed of the firmware (where applicable) and software attached to or running on the computer. CMFA determines the confidence rating and provides it to the computer (or external services) and the computer (out of scope of the TOE), based on the confidence rating, is responsible to maintain the unlocked state or transit to the locked state.

An example of a CMFA boundary within the overall context of the inputs used for continuous authentication is shown below.

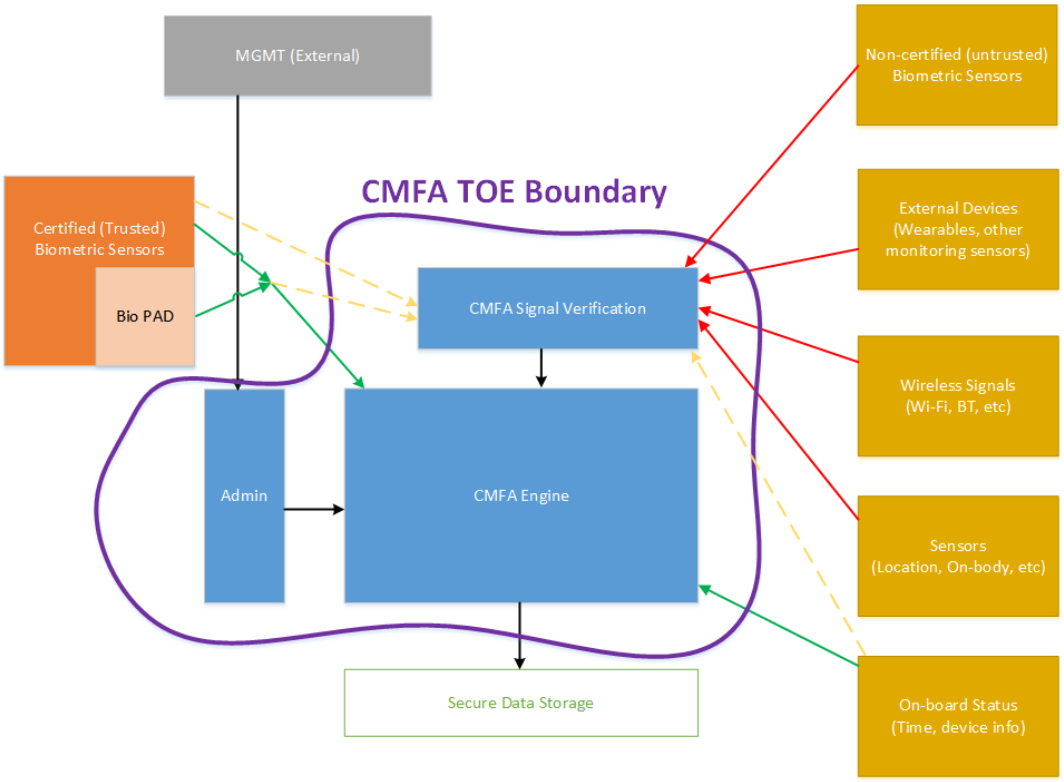

Figure 1. Example CMFA Boundary

- The purple boundary is the CMFA TOE, including the CMFA Engine, the CMFA Signal Verification and the Admin interface
  - CMFA Engine is the core of the system, determining the confidence rating based on inputs and configuration data
  - CMFA Signal Verification is used to establish the trust level of the incoming input data (Yellow boxes)
  - Admin is the component that receives configuration data from the external management service (such as an MDM)
- The orange Biometric Sensors & PAD are for any dedicated biometric sensors (such as face, fingerprint or vein) that are used for the conventional authentication (or has been validated to) the requirements of [BIOPP-Module]. CMFA Engine will set the confidence rating to the highest value when biometric verification using one of these dedicated biometric sensors succeeds. Biometric sensors (e.g. microphone for voice) that are not the dedicated biometric ones may also be used to maintain or increase the confidence rating.
- The yellow sensors/connection input can cover any type of input that may be used. For example, the type of Wi-Fi connection, location data, time or wearable device connectivity. They can also include non-certified biometrics that may also be used for input.
- Black lines show "internal" communications between components as well as management of the CMFA TOE by a management system (such as an MDM).
- The different color lines between sensors and the TOE are used to show an example of paths and the level of trust that is associated with the input.
  - Green lines show highly trusted input (trust established both by the source and the path to the TOE) that can be trusted fully without additional checks (and hence is input directly to the CMFA Engine).

- Red lines show less trusted input that must be checked before being used.
- Yellow, dashed lines show potential alternative paths for sources (generally for sources that may be normally considered highly trusted but which may want to be separately verified anyway).

CMFA configuration

The configuration process for CMFA is likely to encompass multiple steps, covering both administrator and user actions. The administrator may provide configuration information such as acceptable Wi-Fi networks, time settings, location data or specific sensors to be used. The user may provide biometric data for user enrolment if additional biometric sensor is configured, or select external devices to use as sensor input. This combination of information provided by the administrator and user would be used for configuration of CMFA.

Use Case(s)

CMFA is used primarily for continuous authentication of a user for computers such as smartphones, where the confidence rating is used to determine the locked state of the computer.

In addition to being used by the computer for determining the locked state, the confidence rating can also be provided to other systems, such as applications installed on the computer or to external services such as a PC login at the office, building or room entrance control or ATMs. Those external services may communicate CMFA related information to the computer so that the external services can request additional user data, such as specific sensor information, to perform secondary CMFA analysis before granting the access to a user.

The first version of the PP-Module will focus on the use case that the CMFA is used for continuously authentication to determine the state of a computer itself. Additional PP-Modules have to be created for other use cases.

Resources to be protected

- The confidence rating determined by the CMFA that is provided to the computer (or trusted external third party or service).
- Any personal information gathered by CMFA, such as biometric information and behavior patterns of a user.
- Any data used to determine the confidence rating including CMFA configuration data.

(User data stored on the computer shall be protected by the computer itself)

Attacker access

- An attacker can steal the computer in the unlocked state however an attacker needs to take some actions (e.g. take the computer out of office that GPS can detect) before accessing CMFA data, user data or service stored in the computer. If the CMFA uses biometric sensors or learns

behavior patterns of a user, biometric enrolment and learning shall be done by a legitimate user in the protected environment (i.e. an attacker cannot attack the CMFA during biometric enrolment and learning user behavior).

- [If a biometric sensor is used for CMFA, an attacker may present any kind of presentation attack instruments during biometric verification for the sake of impersonation.]
- [If a biometric sensor is used for CMFA, an attacker may try to spoof sensor/connection input during biometric verification for the sake of impersonation.]

Normal text indicates attacker access related to Essential Security Requirements and [Normal text within square parenthesis] indicate ones related to Optional Extensions.

Attacker Resources

Any resources allowed to be used by the basic attack potential to examine and attack CMFA and inputs used by CMFA.

Commercially and/or publicly available software/knowledge/equipment, and, if it is commercially available, samples of the computer running CMFA to test and attack

Boundary of Device

The hardware, firmware, software and security functionalities of the CMFA define the boundary

All of the security functionalities are contained and executed within the boundary of the CMFA (Refer CMFA boundary for more information)

Essential Security Requirements

CMFA shall allow a user or administrator to select or de-select inputs used for continuous authentication.

CMFA shall configure an adequate set of inputs for continuous authentication.

CMFA shall define the trust (reliability) of all inputs.

CMFA shall continuously and accurately determine the current level of confidence in the authentication of a user based on inputs and configuration data.

CMFA shall protect CMFA data, especially sensitive personal information, in cooperation with its operating environment.

Assumptions

A computer conforms to the relevant PP and is assumed to be configured in a secure manner

Admin or user configures the CMFA and its operating environment correctly in a manner to

ensure that the security policies will be enforced

Any user enrolment process is assumed to be done by a legitimate user in the protected environment

A computer that runs CMFA is assumed to be used in a controlled and observable environment

Optional Extensions

Requirements captured in this section may already be realized in some products in this technology class, but this ESR is not mandating these capabilities exist in “baseline” level products.

CMFA shall prevent biometric verification from being successful when presentation attack instruments are used

Outside the Scope of Evaluation

none