# Project Asset List

Secure Face ID v1.0a

**Team : 5verFlow**

**Date : 7 Jun 2021**

Assets for this project are shown in the table below. The total number of assets is 16, and gray-colored 2 assets are excluded because Tema 5 does not have control over them. One of the excluded assets is AS-004, which, as a result of the discussion, Team 5 decided to exclude routers without focusing on additional options. And the other is AS-011, an artifact of facial recognition that has been excluded by assuming FaceNet is reliable.

Table 1. Project Asset List

| ID | Type | Assets | Description |
|---|---|---|---|
| AS-001 | External Entity | User | A person who uses the Jetson Nano system through a client app. |
| AS-002 | Hardware | NVIDIA Jetson Nano | Face recognition system using TensorRT. |
| AS-003 | Hardware | Raspberry Pi v2 camera | Input source device of Jetson Nano. |
| AS-004 | Hardware | TP-Link AC-1750 Mesh Wi-Fi Router | Router for communication between Jetson Nano and laptop.<br>** This asset is only for practice purposes and it's not included in DFD.* |
| AS-005 | Hardware | Laptop | Laptop device to develop and run the client application. |
| AS-006 | Application | The Client Application | An application that communicates with the Jetson Nano, The server application,  and sends a request to the Jetson Nano when the user enters a command, such as a communication mode(Secure Mode, Non Secure Mode) or mode of operation (Learning Mode, Run Mode, Test Run Mode). Display image frames and any accompanying amplifying analysis information received from the camera and image analysis application in the format specified. |
| AS-007 | Application | The Server Application | An application that communicates with the Laptop, the client application and sends a response of the client app's requests. |
| AS-008 | Data | Communication Protocol | Secure Mode :<br>Non Secure Mode : |
| AS-009 | Data | Certificates | The certificates to establish secure, authenticated communication with cameras and image analysis applications and user interfaces. |
| AS-010 | Data | Image file | Image file of people in the imgs folder and made by user specified filename. |
| AS-011 | Data | Artifact of Face | Artifacts learned and built with AS-010. |

| | | | |
|---|---|---|---|
| | | recognition | ** This asset is only for practice purposes and it’s not included in DFD.* |
| AS-012 | Data | Video file | Video file when using face recognition system instead of camera input source. |
| AS-013 | Data | Error/Fault Log | Log of system fault or error. |
| AS-014 | Interface | Camera <-> The Server Application | Includes both hardware and software interfaces. |
| AS-015 | Networking Interface | The Server Application <-> The Client Application | Network interface between the server application and the client application. The connection protocol can be changed by a user selection. |
| AS-016 | Interface | The Client Application <-> The User | User interface with the client application. An user can select the UI button and input string. |

Table 2. Asset Analysis

| ID | Type | Assets | Damage Scenario | Security Characteristics |
|---|---|---|---|---|
| AS-001 | External Entity | User | 1. An attacker assumes a user's password and uses i t maliciously.<br>2. An attacker spoofs a user's password and then threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.<br>3. An attacker can input invalid strings maliciously.<br>4. An attacker can resolve the name of attendees by using an image database. | Confidentiality<br>Integrity<br>Availability<br>Authentication<br>Authorization<br>Non-repudiation<br>Information-Disclosure |
| AS-002 | Hardware | NVIDIA Jetson Nano | 1. An attacker can break or steal the device. | Availability |
| AS-003 | Hardware | Raspberry Pi v2 camera | 1. An attacker can break or steal the device. | Availability |
| AS-004 | Hardware | TP-Link AC-1750 Mesh Wi-Fi Router | 1. An attacker can break or steal the device.<br>2. An attacker can decrease | Availability |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | availability by using DoS attacks.<br>** This asset is only for practice purposes and it's not included in DFD.* |  |
| AS-005 | Hardware | Laptop | 1. An attacker can rob the authenticated laptop and connect to server with it. |  |
| AS-006 | Application | The Client Application | 1. An attacker can tamper with the attendee name by intercepting the registering request when learning mode.<br>2. An attacker can insert malicious code into the name buffer by intercepting the registering request when learning mode or test run mode.<br>3. An attacker can play injurious video files and then break the system. | Confidentiality<br>Integrity<br>Availability<br>Authentication |
| AS-007 | Application | The Server Application | 1.An attacker can tamper with the camera video stream so as to spoof the user's learning data. | Integrity |
| AS-008 | Data | Communication Protocol | 1. If the system uses an old version of protocol, an attacker knows the protocol vulnerabilities and exploit easily. |  |
| AS-009 | Data | Certificates | 1.If the certificates are stored in insecure storage, an attacker can access that and then delete, modify or expose them. | Confidentiality<br>Authentication<br>Non-Repudiation |
| AS-010 | Data | Image file | 1. An attacker can know the user's name and face id if the filename is set to plain text and then can maliciously use personal privacy. | Confidentiality<br>Integrity |

| | | | | |
|---|---|---|---|---|
| AS-011 | Data | Artifact of Face recognition | ** This asset is only for practice purposes and it’s not included in DFD.* | Integrity<br>Availability<br>Authorization |
| AS-012 | Data | Video file | 1. If an attacker tampered with a video file, it can cause crack of the system or the client application. | Integrity<br>Availability<br>Authorization |
| AS-013 | Data | Error/Fault Log | 1.An attacker can know the system vulnerabilities and exploit the vulnerability easily. | Confidentiality |
| AS-014 | Interface | Camera <-> The Server Application | | Integrity |
| AS-015 | Networking Interface | The Server Application <-> The Client Application | | Confidentiality<br>Integrity<br>Authentication<br>Non-Repudiation |
| AS-016 | Interface | The Client Application <-> The User | | Integrity<br>Authentication<br>Authorization |