**PC LOGIN SECURITY KEY**

**OVERVIEW:**

The proposed device is to be used as a physical key to login into the PC. The device serves as an alternate method for logging in (for regular users this is the only method for logging in). This could be an alternative for the keys available in the market like Yubikey, Google key, etc.

**DEVICE DETAILS:**

**Hardware Features:**

ESP8266 (ESP-12E) is the brain of the device, all the authentication, communication with the PC and other processing is done by this. The ESP-12E is coupled with a tactile switch to initiate the login. It is a Wi-Fi module which can either work as an access point or a user.

**Firmware Capabilities:**

The current firmware is provided with limited capabilities taking in consideration of the security for the device. The firmware operates in two modes:

**Key Mode:** Serves as the physical key

**Command Mode:** To make setup or make changes to the device (secret key, UID, etc.)

**WORKING:**

* The device will have a UID used to identification and authentication.
* The device needs to be plugged into the PC. Once the on board button is pressed (short press) the device UID is sent to the PC.
* On receiving the UID the PC will compared it with the paired UID and sends and acknowledgement to the device if it gets matched.
* The device then sends the preconfigured secret key to the PC.
* The secret key is authenticated by the PC and allows the user to get logged into the device.
* The device COM port will be registered in PC and if the device is disconnected from it the PC gets logged out of the account. *(feature yet to be added)*

**INSTALLATION AND INITIALISATION:**

* Every device comes with a pre-configured UID. The device has to be connected to the Admin PC and using a provided software Admin enters into the command mode to view the UID.
* The UID is captured and a random secret key is generated by the software. These both are then saved into a settings file.
* Once the secret key, UID and the COM port of the device are captured the files are dumped into the OS files and are made only accessible to the Admin.
* Registry changes in the OS are made to enable the new login method.
* A user account is created with a password know only to the Admin and this user account is mapped with the device along with a master key.

**ADVANTAGES:**

* Smaller form factor.
* Wi-Fi capability enables making updates to the firmware of the device over the air (OTA).
* Serial data cannot be sniffed by any device as it requires authentication by the paired PC.

**DISADVANTAGES:**

* The settings file saved in the PC is in plain text. Though it is very hard for a regular user to get his hand on the file, it is not impossible.
* Doesn’t have a dedicated encryption chip for encrypting the data.

**FUTURE SCOPE:**

* The settings file can be encrypted in the PC to provide added security.
* OTA updated can be enabled to provide easy updates (if needed) to the device without actually having physical access to the device.