Device Manufacturer Initial Firmware Flashing

When the manufacturer flashes the firmware in the IOT device ROM chip, we added a step to add a unique firmware signature to any firmware copy. So even the attacker gets the firmware sample, the firmware flashing program or an unused IOT device (such as an old sensor which was not used anymore), he cannot use them to make a fake IOT device and connect to our sensor.

The firmware flashing program contains 2 parts of program (client and server):

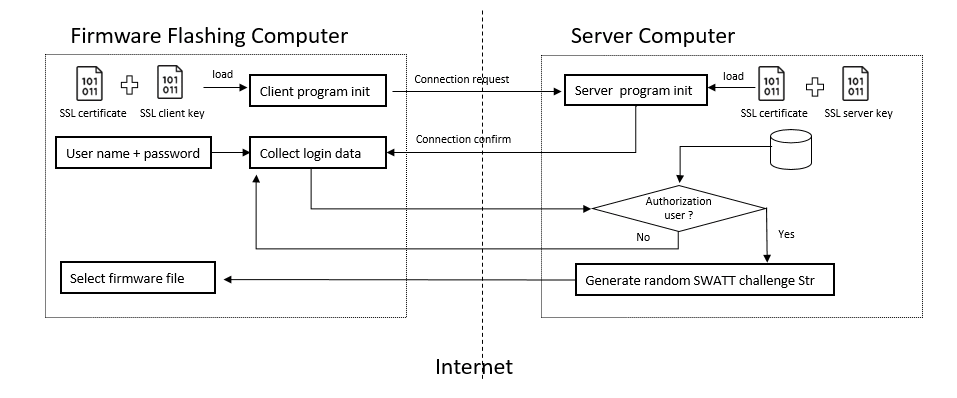
1. Firmware flashing client: This client is used to login server, generate the IOT device signature, flash firmware and signature to IOT device ROM chip.
2. Firmware verification server: Record the IOT flash information to the database. Verify the IOT device registration.

The sensor and client communication is using SSL.

There is 3 Steps to finish the firmware Flashing initialization

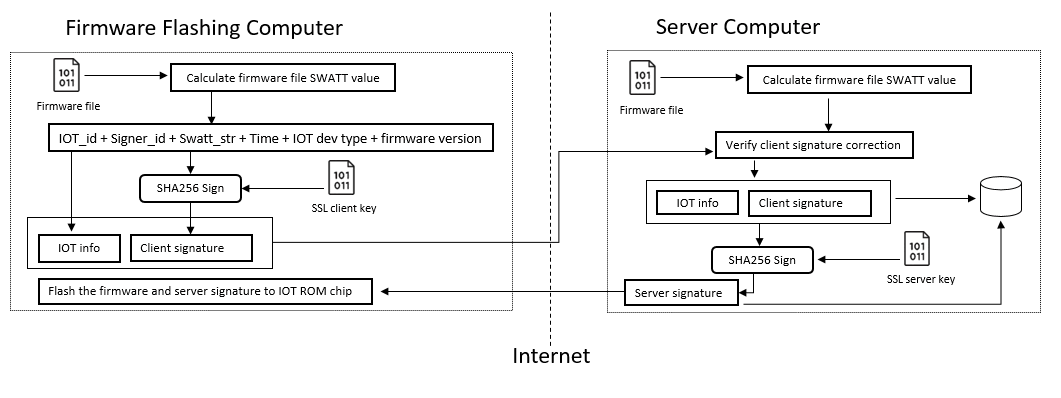
Step 1: Client login

The user need a valid user name and password to start to use the firmware flashing program. After the user name and password has been verified, the server will send a random SWATT challenge string to client and the client firmware selection function will be enabled.



Step 2: Client Signature generate and sensor signature deploy

After the manufacture has selected the firmware file, the client program will calculate the file’s SWATT value based on the SWATT challenge string. The server will also do the same calculation. Then the client will page the IOT device information (IOT\_id + Signer\_id + Swatt\_str + Time + IOT dev type + firmware version) and use client’s SSL key to sign it to get the client signature. The IOT device information and client signature will be send to the server part. After the server has verified the client’s SWATT value and the signature, the server will user its SSL key to sign the whole message (IOT\_id + Signer\_id + Swatt\_str + Time + IOT dev type + firmware version+ client signature) to get the server signature. The server signature will send back to the firmware flashing program and flashed with the firmware to the IOT device’s ROM chip. At the server part the IOT device information, client signature and the server signature will be saved in the data base.



Step3: IOT device verification.

When the IOT device try to connect to the server, it loads the server signature from the ROM and send it with the IOT device information to the server. If all these data can match the record in the server’s data base. Then the IOT device’s data will be accepted by the server.