Secure updates using PUFs

Firmware update is essential to prevent bugs and vulnerabilities discovered during the lifetime of the device. In practice, the device firmware update procedure is not secure. Most of the attacks use this un-secure update method to update a modified version of firmware to take control of the device.

Secure update procedure is widely used in high-end devices. Firmware updates are signed by the administrator. The devices usually have a public key stored in a one time write memory in i.e. a fuse, or it is stored in a dedicated security hardware like TPM chip. When the device performs update it checks the signature of the firmware update with the public key installed in the device. The device only updates the firmware if it has a valid signature.

As the above mention solutions are not present in low-end IoT devices. We propose a solution to add the secure update process in these devices using SRAM based PUFs. As we can generate a unique Pub/Pri key pair from the PUF. We can extract the private key from the device during the initialization process. We can then use this private key to sign the firmware. During secure update process device will check the validity of the signature by using the public key from the SRAM PUF, and it will only allow firmware updates if the signature is valid.

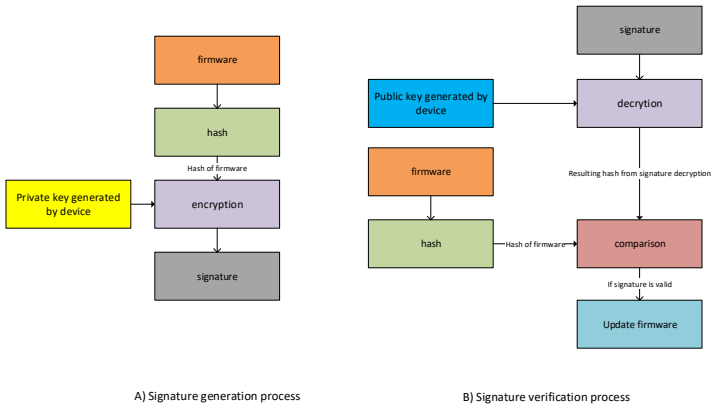

Figure 1: Secure update process