Trusted embedded computing scheme

Subject: Embedded systems and Cryptography
Thesis advisor: Prof. Dr. Lorenz Müller
Expert: Felix Kunz

Smart devices are often distributed in critical infrastructure and used for operational transactions, machinery steering or storage of critical data. Such devices are computers with own Operating Systems connected to different networks. They are at high risk to be corrupted by hackers. The goal of this master thesis is to develop a scheme, how smart devices can be secured in order to assure trusted executions of requested tasks assigned from an external control server.

Specific problem and solution approach

Taking a realistic situation we can assume that an attacker has no direct physical access to the smart device or to the control station. But he can install a malware into the storage annex of the device and disrupt or abuse the device during operation. To ban such kind of attacks one has to enable mutual authentication between the controller and the smart device and to assure that only authentic and integer applications can run critical operations. These requests can be fulfilled if a non-accessible and hardware based root secret can be retrieved inside the smart device. Such a root secret has to be based on unique physical features of the device hardware that cannot be detected by a malware, means the root secret comes from a so called Physical Unclonable Function (PUF).

During the commissioning of the smart device such a PUF function has been embodied and tested in the device hardware. Then the implemented PUF secret is shared with the controlling server. A security protocol based on the derived root secret has been developed that fulfills the mentioned security request for a save operation of the smart device in the field.

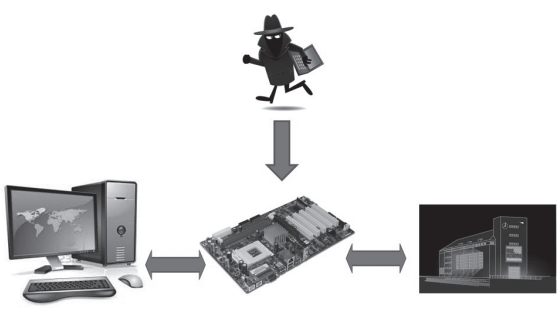
The most important steps of the secure operation protocol are:

- The server sends a random challenge R and a time stamp T to the device over a previously established channel.
- The device generates the PUF root secret and returns the MAC of R and T using it as key. The server checks the authenticity of the sender using his stored root secret of the device.
- If approved the server encrypts the application that shall be executed with a secret key based on the root secret and sends it to the device. The device decrypts the program using again his root secret and executes it directly. With this step the device authenticates the server and checks the integrity of the application simultaneously.

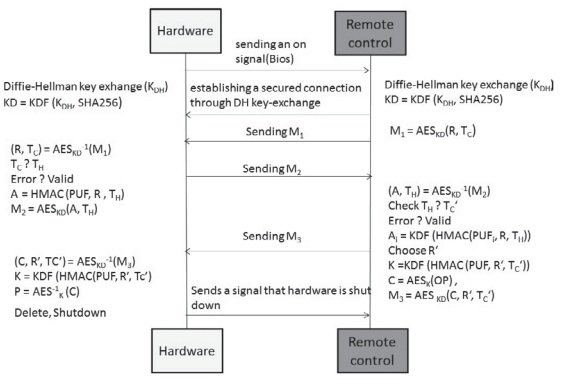
A program not encrypted correctly would not run and any malware in the local storage of the device cannot interfere in the protocol processing as the full protocol processing is implemented in hardware never leaving the control.

Result and conclusion

In this work a scheme for the secure operation of critical applications on smart devices in the field has been developed and tested in a demonstrator setup. The usability of an electronic PUF function as root secret for such a protocol has been tested with success.



The Attacker model



The protocol overview

Aryan Soroush Sanaz

sanaz_aryan_soroush@yahoo.com