Time based authentication for embedded devices

In a typical authentication setup, a verifier server sends the authentication request to the low powered embedded devices. These devices then calculate the hash of the program/firmware running on the device and send it to the verifier. The problem with this approach is that an attacker can execute a DoS attack on these embedded devices, by repeatedly requesting the authentication.

Our idea is to fix this DoS issue by using time-based authentication. In this method, an embedded device will generate the verification data after a certain time and sends it to the verifier for verification. This will remove the need authentication requests from verifier part.

A PUF response will be used to generate a seed. This seed will be used in a deterministic random number generator to generate a random number. This random number will be used as a key to HMAC function along with firmware code data as input. The device will wait for the timeout and after the timeout, it sends the keyed-hash from HMAC function to the verifier. Verifier will calculate the same random number using the seed value, which will be pre-installed in the verifier. It then calculates HMAC using original firmware code data as input. It will verify the authenticity by comparing calculated keyed-hash with received keyed-hash value.

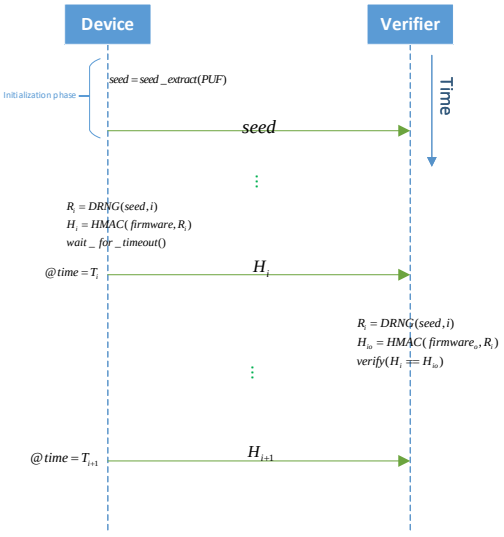

Figure 1: verification protocol

Figure 1 shows the working of the protocol. In initialization phase, the device will send the seed which it generated using PUF to the verifier. After that, it will generate random number R_i from deterministic random number generator using the seed. The device then calculates the HMAC H_i using R_i as the key and the firmware code as the data input. It will wait for timeout T_i, and then it will send the H_i to the verifier. The verifier will then calculate H_{io} using original firmware $firmware_o$ as the input data and R_i as the key to the HMAC function. It will verify the device by comparing the result of HMAC function H_{io} with the received H_i.

basic idea for this protocol is taken from [1].

References

[1] Ahmad Ibrahim, Ahmad-Reza Sadeghi, and Shaza Zeitouni. Seed: Secure non-interactive attestation for embedded devices. In *10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2017)*, July 2017.