Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

***HiWi Job** or **IDP** in collaboration with Fraunhofer Research Institute AISEC*

Implementation of fTPM features on the TrustZone-M

Date: *30. Januar 2019*

Motivation

Recently launched ARMv8 Cortex-M microcontrollers support the TrustZone-M security feature. While the TrustZone has found its adoption years ago on Cortex-A controllers and became widely used in both industry and academia, the more resource-constrained Cortex-M controllers now catch up with the TrustZone-M technology and offer new perspectives for increasing the security of IoT applications.

Task Description

The first part of this work is to become acquainted with the TrustZone-M on one of the ARMv8 microcontrollers and to compare its functionalities with the TrustZone on Cortex-A controllers. Another widely adopted piece of security hardware is the Trusted Platform Module (TPM)[1]. On the most resource-constrained devices, integrating a TPM chip and a full software stack making use of the TPM's security features might be too resource-consuming and expensive. While a firmware TPM (fTPM)[2], a software-TPM in other words, was already implemented for the TrustZone on Cortex-A, the next step of this work is to evaluate which of the fTPM functionalities can be realized with the TrustZone-M. Based on that, selected functionalities of the fTPM implementation should be implemented on the TrustZone-M.

Requirements

- Most important: motivation to work in the field of microcontrollers
- Good C programming skills and basic experiences with microcontroller programming
- Optional: Experience with the TrustZone on Cortex-M/Cortex-A controllers

Contact

Michael Weiss (michael.weiss@aisec.fraunhofer.de)
Manuel Huber (manuel.huber@aisec.fraunhofer.de) or
Fraunhofer Research Institute AISEC
Parkring 4, 85748 Garching (bei München)
Phone: 089/3229986165

[1] `https://trustedcomputinggroup.org/wp-content/uploads/TPM-2.0-A-Brief-Introduction.pdf`

[2] `https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/raj`