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

***Master's Thesis** or **HiWi Job** in collaboration with Fraunhofer Research Institute AISEC*

Securing the Kernel Crypto API with the TrustZone

Date: *6. Februar 2019*

Motivation

Today, more and more applications on smartphones make use of the ARM TrustZone for securely storing cryptographic key material and for executing cipher operations shielded from the rest of the system. The Android framework, for instance, provides developers with an API that eases the use of cryptographic services a trusted execution environment running in the TrustZone offers. On the other hand, the Linux kernel provides a flexible cryptographic API for use by other kernel components or user space applications, releasing developers from implementing their own crypto algorithms. So far, the kernel crypto API does not make use of the TrustZone. As a result, components using the crypto API do not benefit from the additional protection the TrustZone provides against memory attacks and kernel exploits.

Task Description

The goal of this work is to add TrustZone support for the kernel crypto API. This requires the extension of various components of existing Linux systems, for instance, the crypto API or the driver enabling the interaction with the TrustZone. The first step is to gain a thorough understanding of the involved components and to develop a decent concept. For a proof of concept, a chosen component should make use of the TrustZone-backed crypto API, such as the kernel's disk encryption infrastructure. In the last step, the work should evaluate the developed prototype regarding potential performance impacts.

Requirements

- Most important: motivation to work in the field of kernel programming and embedded devices
- Good C programming skills and preferably experiences with the Linux kernel
- Optional: Experience with the TrustZone on Cortex-A controllers

Contact

Julian Horsch (julian.horsch@aisec.fraunhofer.de) or
Manuel Huber (manuel.huber@aisec.fraunhofer.de)
Fraunhofer Research Institute AISEC
Parkring 4, 85748 Garching (bei München)
Phone: 089/3229986165