ESPRESSO

skalierbarE hardware-geSicherte authentifizierung und PeRsonalisiErung intelligenter SenSorknOten

Programm / Ausschreibung	Bundesländerkooperationen TP, Silicon Alps, Silicon Alps 2017	**Status**	abgeschlossen
Projektstart	01.05.2018	**Projektende**	31.10.2020
Zeitraum	2018 - 2020	**Projektlaufzeit**	30 Monate
Keywords	Internet of Things; IT Security; Side-Channel Attacks; Cryptography		

Projektbeschreibung

Intelligente Sensoren (smart sensors), welche neben der eigentlichen Messdaten-aufzeichnung auch die Verarbeitung der aufgezeichneten Daten übernehmen, werden bereits in vielen verschiedenen Anwendungsszenarien – z.B. in industriellen Produktions-prozessen, in Smart-Home-Umgebungen oder auch in kritischen Infrastrukturen – eingesetzt. Sowohl in industriellen Anwendungsbereichen als auch in privaten Umgebungen müssen die verarbeiteten Daten vor unbefugten Zugriffen und Veränderungen geschützt werden, um die Manipulation von Daten und Steuersignalen zu verhindern. Es muss die Authentizität, Integrität und Vertraulichkeit der Messdaten und der Steuerungsdaten mit geeigneten kryptografischen Methoden geschützt werden, um den Schutz von personenbezogenen Daten zu garantieren, um geistiges Eigentum in Form von Informationen und Konfigurationsparametern zu schützen und um Schäden und Gefahren jeglicher Art aufgrund unautorisierter Manipulationen zu verhindern.

Das Ziel von ESPRESSO ist die Erforschung von Sicherheitstechnologien zur Integration von intelligenten Sensoren in das Internet der Dinge (Internet of Things – IoT). Hierbei ist der Fokus der Forschung auf drei Kernthemen:

(1) Das erste Themenfeld sind Technologien zur sicheren Speicherung und Verwaltung von Schlüsselmaterial. Hier werden neue Ansätze im Vergleich zu bestehenden Hardware-Sicherheitsmodulen untersucht um die Anforderungen des IoT an Backend-Systeme insbesondere im Bereich Skalierbarkeit effizient abzubilden. Die neuen Ansätze werden basierend auf Smartcard-Technologie in einem Prototyp implementiert und evaluiert.

(2) Intelligente Sensoren haben eine lange Lebensdauer und arbeiten in ungesicherten Umgebungen, die Seitenkanalangriffe wie Power-Analyse und Fault-Attacken zulassen. Um Sicherheit unter diesen Bedingungen zu ermöglichen forschen wir an effizienten Implementierungen von Post-Quanten-Kryptographie mit Seitenkanalresistenz für IoT Anwendungen. Auch diese werden prototypisch in Hardware bzw. Software realisiert um insbesondere die Seitenkanalresistenz zu analysieren.

(3) Im Rahmen des Themenkomplex Plattformsicherheit wird die Sicherheit von IoT Systemen über Gerätegrenzen hinweg analysiert. Hierbei werden auch Software-Seitenkanalangriffe berücksichtigt, welche gerade auf Steuerungsgeräten wie

Smartphones von hoher Relevanz sind. Es geht hierbei darum das Problem-bewusstsein zu stärken und entsprechende Schutzmaßnahmen zu entwickeln.

Abstract

Smart sensors, which besides measuring sensor data also process the measured information, are already used in various application scenarios, e.g., in industrial production processes, in smart-home systems, and also in critical infrastructures. Both, industrial applications as well as private applications require that processed data and control signals are protected against unauthorized access and manipulation. It is important to protect the authenticity, integrity, and confidentiality of the measured sensor data as well as the data used to control actuators by means of cryptographic mechanisms, in order to protect sensitive personal information, to protect intellectual property such as configuration parameters, and to prevent damage and harm due to unauthorized manipulations and configurations.
The objective of ESPRESSO is to research security technologies for a secure integration of smart sensors into the Internet of Things (IoT). Thereby the focus is on three core areas of research:

(1) The first area of research are technologies for securely storing and managing key material. In this context, we use novel approaches with respect to existing hardware security modules in order to address the need of IoT applications for high scalability with respect to backend-systems. The novel approaches are going to be implemented and evaluated based on a prototype using smartcard technology.

(2) Smart sensors have a long duration of life and work in non-secured environments, which allow conducting side-channel attacks such as power analysis and fault attacks. In order to achieve security in such settings, we are researching efficient implementations of post-quantum cryptography for IoT applications including side-channel resistance. These technologies are going to be implemented as prototypes in hardware and software in order to analyze in particular the side-channel resistance.

(3) In the context of the research on platform security, we analyze the security of IoT systems across bounds of devices. Thereby, we in particular also consider software side-channel attacks that are highly relevant for control devices, like smart phones. The goal is to create awareness about the attacks and to research corresponding countermeasures.

Projektkoordinator

- Technische Universität Graz

Projektpartner

- PrimeSign GmbH
- Yagoba GmbH
- IoT40 Systems GmbH