FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

CYBER-PHYSICAL SYSTEMS
WE MAKE OBJECTS SMART AND SECURE
HARDWARE-BASED SECURITY

MOTIVATION

The term »cyber-physical systems« comprises diverse mobile and embedded devices such as RFIDs, sensors and smartphones that combine computer technical and physical aspects. These systems have become an integral part of our daily life and often assume important control tasks. Embedded computer platforms such as smartphones (and even sensors) are constantly becoming more efficient, they have high processing power and considerable storage resources, and a multitude of communication interfaces as well.

Cyber-physical systems have an enormous potential for many application areas, they are the drivers in many product innovations, and enablers for many future-oriented technologies. The growing popularity and dissemination of cyber-physical systems and their being used more and more to process and store security critical and privacy sensitive data turns these systems into attractive targets for all kinds of software and hardware attacks.

CHALLENGES

The practical use of cyber-physical systems, particularly in security-critical application areas, requires the careful consideration of security and data protection aspects already during the design phase of these systems. In so doing, companies are taking the security of platforms and networks into account, as well as the security at the application, the architectural and the technological level. Using hardware based solutions often is required in the platform security area, as they can guarantee for the flawless state of an embedded system or that components are original ones, for example.

Cyber-physical systems are often found in areas that until recently did not have much to do with the IT world or only very little. Often they exist specifically for certain requirements, for example with regard to system prerequisites, installation, operation and maintenance. Existing protection measures and common IT security concepts thus have turned out to be insufficient in practice. Also, cyber-physical systems are usually characterized by relatively small computing capacity and high requirements regarding energy efficiency, which must be taken into account in the design of the respective solutions.
Our Offerings

Fraunhofer SIT addresses the security and data protection aspects of cyber-physical systems and their communication channels. The institute specifically offers:

- Technical consultation to secure processes, equipment, documents and products
- Development of cryptographical procedures and security technology
- Hardware testlab for embedded systems
- Analysis and enhancement of existing security architectures for cyber-physical systems, and development of innovative security solutions, particularly for smartphones and RFID systems
- Hardware fingerprint development for the distinct device identification, in particular Physically Unclonable Functions (PUFs)
- Design and development of hardware-based attestation processes for reviewing device integrity (trusted computing)
- Development of unique identity and facility management solutions based on cyber-physical systems that unite physical and logical security concepts.

Customer Benefit

- Cyber-physical system users benefit from the security mechanisms for cyber-physical systems developed by Fraunhofer SIT, because they offer a markedly improved protection against software and hardware attacks. In this the institute’s focus is on smartphones, sensors and RFID systems that store or process sensitive data.
- Cyber-physical system manufacturers benefit from our expertise. Fraunhofer SIT analyzes, develops and tests security mechanisms for cyber-physical systems, smartphones, sensors and RFID systems.
The Fraunhofer Institute for Secure Information Technology SIT is one of the oldest and most respected research institutes for IT security in the world. More than 160 employees support companies and government bodies in securing data, services, infrastructures, and end products.

In Darmstadt more than 400 scientists are carrying out research in the IT security and data protection areas. The institute is an active member of the Center for Advanced Security Research Darmstadt (CASED), which is supported by the state of Hesse, and the Center for Research in Security and Privacy (CRISP), which is supported jointly by federal and Hessian state government bodies.

REFERENCES

Fraunhofer SIT has a long experience in the development and secure design of cyber-physical systems and is also engaged in the security aspects within the car-2-X context. The projects include among others:

- **Key2Share**: An application for NFC capable Android smartphones for the temporary and spatial allocation of access rights for enterprises, cars and hotel rooms. [www.key2share.de](http://www.key2share.de)
- **SeDaFa**: Development of solutions and technologies for own data protection in the connected vehicle. [www.sedafa-projekt.de](http://www.sedafa-projekt.de)
- **DElTA**: Development of a protective profile for the secure charging and invoicing in electric mobility
- **iKoPA**: Securing infrastructure components such as traffic lights or charging stations
- **SIM-TD**: Design and implementation of an encryption solution for car-2-X communication
- **EVITA**: Development of a secure automotive on-board network architecture to protect against the tampering of sensitive data and components
- **BizzTrust for Android**: Enterprise solution for the secure use of smartphones – isolation of applications and data on system level. [www.bizztrust.de](http://www.bizztrust.de)
- **ANSSI**: IT security integration into industrial information systems, threat analysis, risk assessment and anomaly identification

THE INSTITUTE

Prof. Dr. Christoph Krauß
Phone: +49 6151 869-116
Fax: +49 6151 869-224
christoph.krauss@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology SIT
Rheinstrasse 75
64295 Darmstadt
[www.sit.fraunhofer.de](http://www.sit.fraunhofer.de)

CONTACT