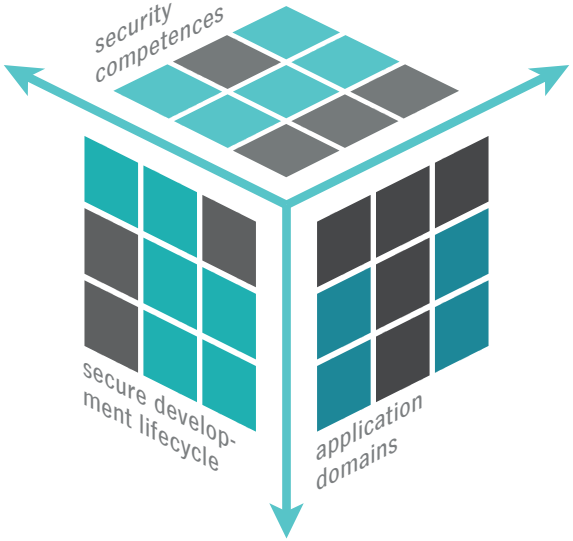
OUR SERVICES

Our work is highly research-oriented. We support enterprises in various aspects of IT security. Selected offerings include:

- Threat analysis
- Best practices and methods for IT security
- Technology assessment
- Research on novel and applicable security solutions
- Identifying legal obstacles
- Implementing legal requirements of innovation technology
- IT security testing
- Awareness and training



ABOUT THE FZI

The FZI Research Center for Information Technology is a non-profit institution for applied research in information technology and technology transfer. Its task is to provide businesses and public institutions with the latest research findings in information technology. It also qualifies young researchers for their career in academics or business as well as self-employment.

ABOUT THE COMPETENCE CENTER FOR IT SECURITY

With the Competence Center for IT Security the FZI has created a central contact point for practical questions for IT security with the support of the State of Baden-Wuerttemberg.

The centre offers solutions for questions of IT security for small and medium-sized enterprises (SMEs) in Baden-Wuerttemberg.

The security solutions that are researched at the Competence Center for IT Security are easy to understand, easy to apply, and easy to communicate.

Teilnehmer der Allianz für Cyber-Sicherheit

SecurITy made in Germany

Baden-Württemberg
MINISTERIUM FÜR FINANZEN UND WIRTSCHAFT

CONTACT

Competence Center for IT Security

Email: kompetenzzentrum-it-sicherheit@fzi.de

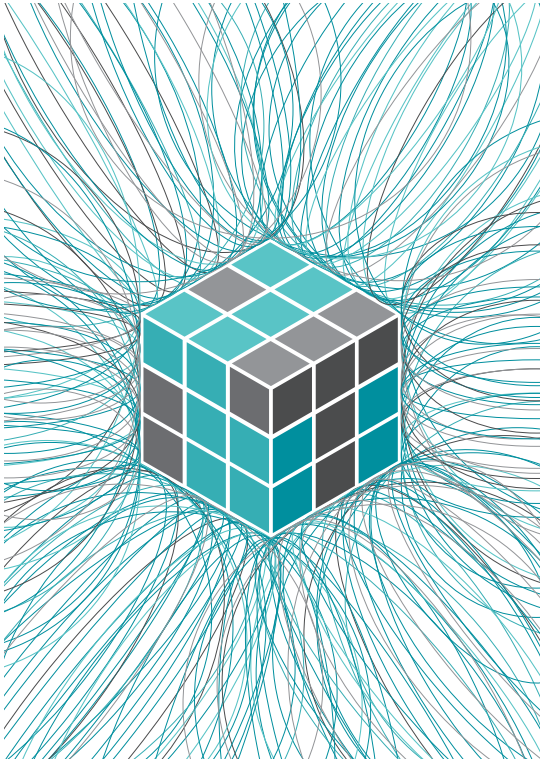
http://www.das-sicherheitszentrum.de

FZI Forschungszentrum Informatik
Haid-und-Neu-Str. 10–14
76131 Karlsruhe, Germany

www.fzi.de/en | fzi@fzi.de

0320181000

RESEARCH ON YOUR BEHALF



FZI RESEARCH CENTER FOR INFORMATION TECHNOLOGY

COMPETENCE CENTER FOR IT SECURITY

Kompetenzzentrum IT-Sicherheit

The increasing complexity and global networking of IT systems raises new security challenges. To address these challenges one not only needs an expertise in methods and mechanisms for IT security. The key to success lies in a holistic approach.

NOVEL CHALLENGES WITH IOT DEVICES

The ever-increasing digitalisation requires IT systems to be networked across all industries. Systems that previously had been operated in total isolation are now connected to the Internet. This trend results in an increased attack surface and may provide attackers with global access. Critical infrastructures such as power plants or hospitals in particular require protection – attacks on such systems can seriously affect the safety of humans and the environment. This paradigm shift raises new challenges for IT security:

- As previously, IT security played no role in many systems, there is little technical or organisational know-how
- There are hardly any certifications
- Staff are lacking the expertise to deal with the new threat situation

A HOLISTIC APPROACH TOWARDS SECURE IT SYSTEMS

The design and implementation of a secure IT system is an interdisciplinary approach. To begin with, comprehensive expertise in methods and mechanisms for IT security is required:

- Hardware security
- Cryptography
- Secure software development
- Network security
- Legal aspects (e.g. data protection, liability, ...)
- Organisational aspects (e.g. IT security management)

However, an IT system is always designed for a specific application and its own specific requirements. One must also be proficient in the system's specific domain:

- Protocols and mechanisms (e.g. OPC-UA, CAN, ETSI C-ITS, ...)
- Requirements (e.g. availability, real-time, ...)
- Common software development processes (e.g. V-Model, SDL, ...)

Researchers at the FZI have a long-standing experience in applied research in a wide range of domains.

However, IT security is not a one-step process. It must be considered in all phases of the product life cycle. It is therefore also important to know which methods and measures of IT security are best suited in which phases.

At the Competence Center, the FZI bundles these competencies with in-depth expertise in IT security methods and mechanisms into a holistic research offer that takes into account the entire life cycle of an IT system.