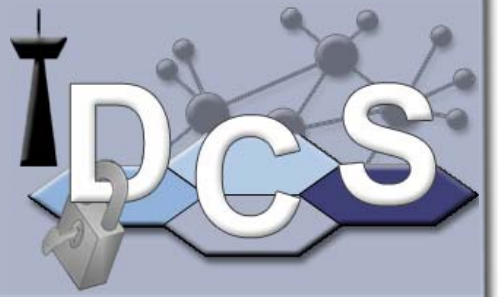
UNIVERSITÄT SIEGEN

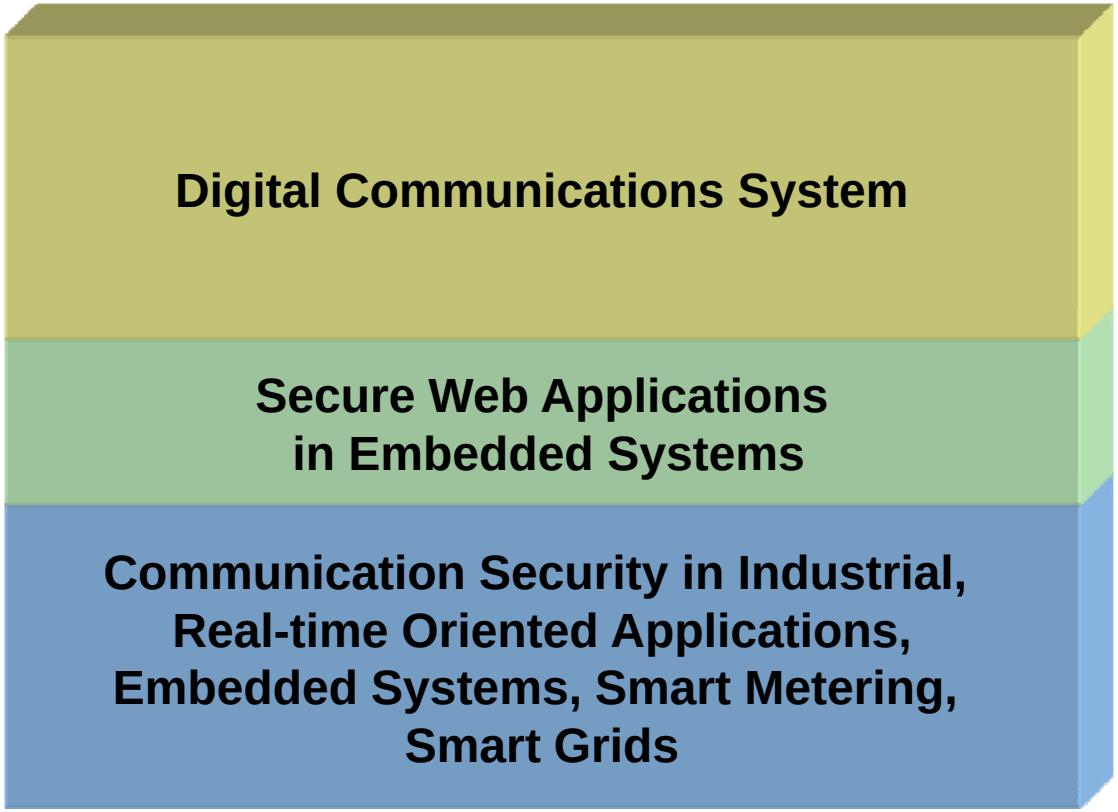
Presentation of the Chair for Data Communications Systems

Univ.-Prof. Dr. Christoph Ruland

University of Siegen
Faculty IV: Science and Technology
Chair for Data Communications Systems
Univ.-Prof. Dr. Christoph Ruland



Scientific Work and Research



Applied Research

- Automotive Security
  - CAN, FlexRay, LIN, MOST
- Security of industrial Applications
  - Smart Metering, PLC, MUC, Smart Grids
- Reliable communication of Embedded Systems
  - Cryptographic Mechanisms, incl. Elliptic Curves
  - Data Compression
  - Error Detection and Correction, incl. Reed Solomon Codes
- Embedded WebServer
- Secure Software Download
- RFIDs in security- and industrial Applications

Fundamental Research

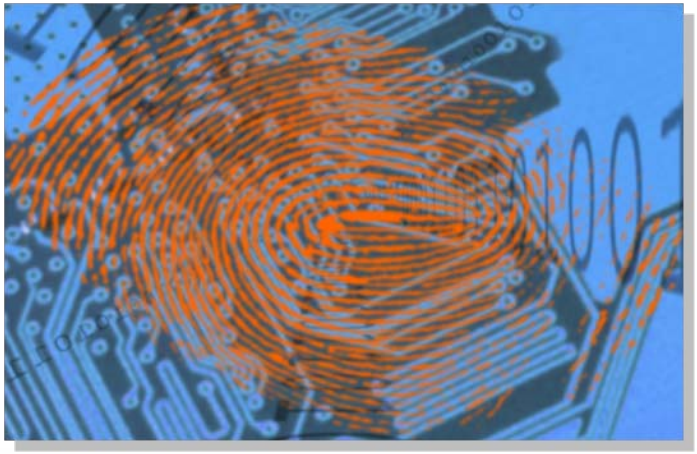
- Joint Channel Coding and Cryptography
  - Application of cryptographic methods over noisy channels
- Application of formal methods in the design of security protocols for metering
- RFID-Security simulations and implementation
- Coding gains for passive and active RFID-tags
- Document Tracking Services

- Automotive Security
  - More and more electronics, software and communications systems, which can cause threats, are attached to vehicles
  - Communication takes place inside of vehicles, among vehicles and between vehicles and the environment/infrastructure

- Security- and risk analysis for the vehicle and its components from design till scrapping
- Security concepts and –solutions for appropriate security systems and the necessary key management
- Co-Chair of the eSecurity Working Group of the eSafety Forum of the European Union (Intelligent Car Initiative 2010). Working on the requirements for research, regulation, security, etc.

Current Research

- Security for industrial applications
  - Secure exchange of information between machines, electronic control units, measuring instruments and monitoring devices is essential
  - Application of digital signatures to commands and messages transmitted and received by control and measuring devices
  - Digital rights management are ensuring that only authorized participants are allowed to execute instructions



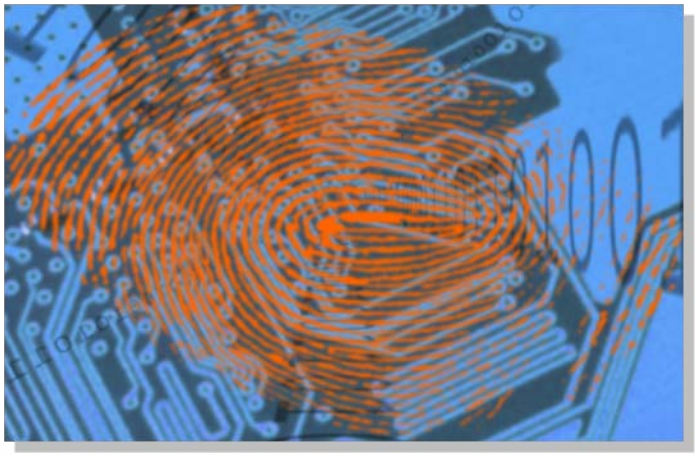
- Digital signatures and encryption of measuring data and control information
- Security for PLC-Communication
- Realization of secure MUCs
- Integration of data collection systems
- Essential for Smart Grids

Current Research

- Reliable communication of Embedded Systems
  - Industrial environments are characterized by strong interferences and high reliability
  - Metering data are collected from a lot of metering devices which cause a high amount of data

- Channel coding provides automatic error correction without retransmission
- Cryptographic methods are used to verify data integrity and authentication of the sender
- Data compression methods reduce (Metering-) data down to 10%
- Implementation for Embedded Systems (Atmel, Renesas, Texas Instruments) are available or under development

- Embedded Webserver
  - More and more Embedded Systems are equipped to act as a Webserver, to provide dedicated services and be able to be controlled and prompted from the environment
  - Linux-Kernels must be configured and compiled to offer the required functionalities
  - Special requirements of communication capabilities



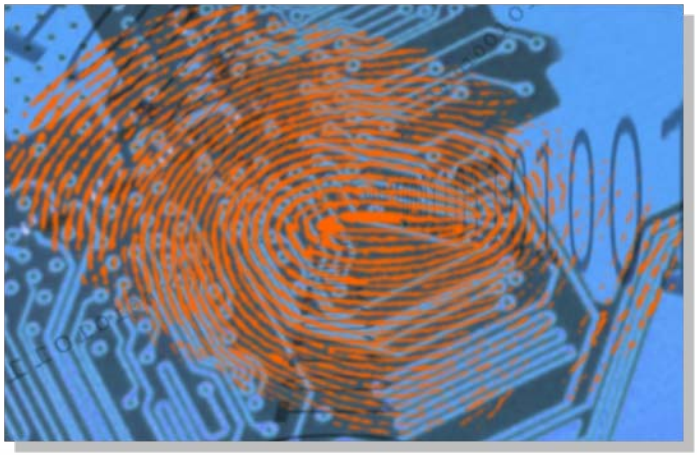
- LAN-Interface
- GPRS-Interface, including SMS
- TCP/IP
- SSL/TLS (based on certificates)
- SOAP
- XML, XML signatures, SML, WSDL
- RFID - Interfaces

Current Research

- Software-Download (regulated) Software
  - Many devices require the usage of certified, approved software (often based on lawful requirements)
  - Costly exchange of software in the field or in testing laboratories

  - Online software updates as a less costly solution
  - New options for download of regulated software due to novel parts in measuring regulations
  - Concept covers the whole life cycle of the application from the development, to the audit by the public authority and the operator of the device till the capability of online audits by public authorities

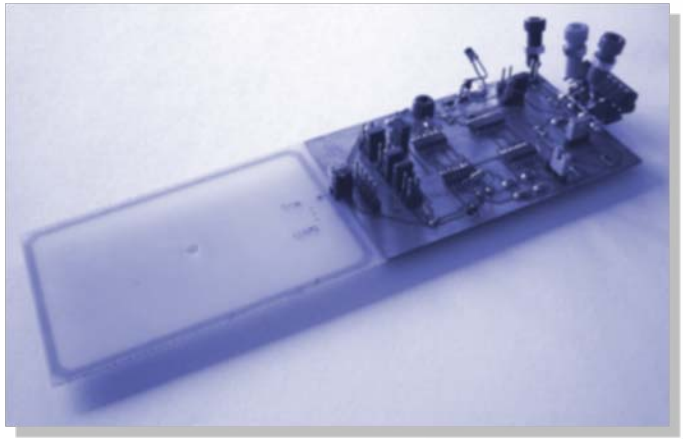
- RFIDs in security- and industrial applications
  - We develop systems, which use RFID
    - **as electronic seal**
    - **for detection of manipulation and counterfeiting**
    - **for logistics applications**
    - **for the reliability of sensor-information**
    - **for wireless transmission between jeopardized or secure inner zones and the environment**



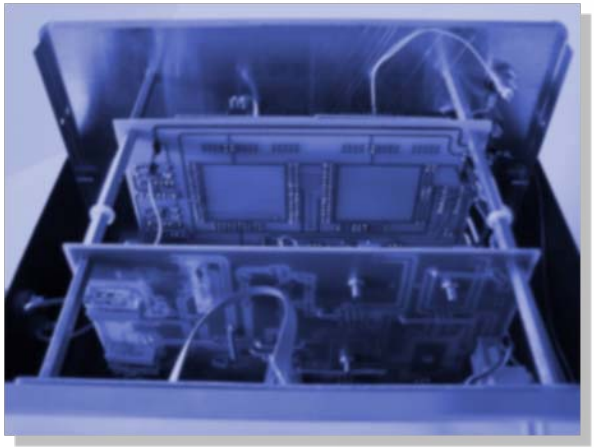
Development of new RFID-Base stations regarding

- **Demodulation and Decoding**

- RFID-Security Simulation and Implementation
  - Fundamental electronic, communication and cryptographic aspects
    - **How much energy can be transferred to a RFID-Tag?**
    - **Which security level can be achieved with it?**
    - **Which processing capacity can be realized?**
    - **Which cryptographic methods are feasible?**
    - **Are generation and verification of digital signatures feasible?**
  - Application of digital signatures based on elliptic curve cryptography
  - Special focus on digital signatures „giving message recovery“, which are appropriate especially for short messages
  - RFIDs in UHF-range (up to 1m)



- Joint Channel and Cryptography
  - New field of research, combining cryptographic methods with new developments of channel coding
  - Novel channel decoding methods with automatic error correction using soft input and soft output (SISO)



  - The cryptographic verification process corrects iterative exploiting the soft outputs
  - Feedback from the cryptographic verification process to the channel decoder leads to improved decoding of interleaved blocks
- Turbo Concatenated Codes
  - Application of Joint Channel and Cryptography as systematic error detecting code as outer code
  - Iterative decoding of interleaved blocks with feedback between outer and inner error-checking and error correcting code (Convolution or Turbocode)

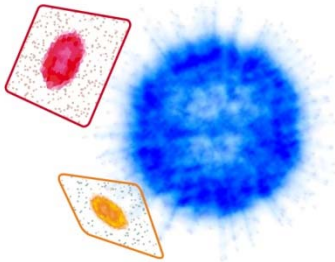
External Research Projects

- TERESA
  - **T**rusted computing **E**ngineering for **R**esource constrained **E**mbedded **S**ystems **A**pplications
  - Project of the 7. framework program of EU
  - http://www.teresa-project.org
  - Our contribution: Application for Security aspects in measurements

- OVERSEE
  - **O**pen **Ve**hicula**r** **Se**cur**e** Platform
  - Project in the 7. framework program of EU
  - http://www.oversee-project.com
  - Our contribution: Design and Integration of IT-Security for internal and external communication

External Research Projects

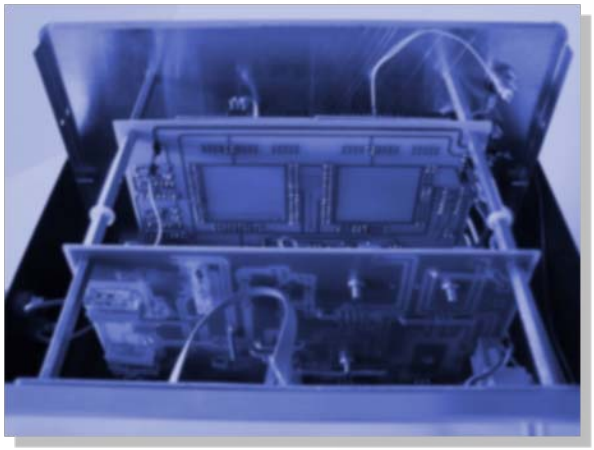
- DFG Research Training Group 1564
  - „Imaging New Modalities“
  - Multimodal image recognition and analyze for public security
  - http://www.grk1564.uni-siegen.de
  - Our contribution:
    - Traceability of sensitive private data
    - Security concept for protection of sensitive information e.g., biometric characteristics
    - Data Leakage Detection
    - Non-Repudiation of Data Forwarding



GRK-1564
Imaging
New Modalities

External Research Projects

- Electricity Charging Stations
  - Development of the gateway with communication to
    - Different backend infrastructures
    - Authorization, accounting and billing server
    - Management center, energy provider
    - Electric power sockets and its metering instruments
    - Vehicles
  - based on embedded WebServers



- Lawful Metering
  - Energy-, gas-, water-, heat-, taximeters and slot machines etc.
  - Design of security concepts according to legal requirements
  - Development and integration of the cryptographic software and security services, based on Embedded Systems and crypto processors

Expired Research Projects (Last Years)

- Security in communications systems (1)
  - DFG (Deutsche Forschungsgemeinschaft)
    - New modes of operation of block algorithms and encryption in SDH- and ATM-Networks
    - Internet Security System for Voice-over-IP with regard to Quality of Service
  - Forschungsverbund Datensicherheit NRW
    - Authentication of bit streams
    - Security for MiGrid (Grid-Infrastructure for cooperative added value in small and medium enterprises)

Expired Research Projects (Last Years)

- Wireless communication systems
  - DFG (Deutsche Forschungsgemeinschaft)
    - Heterogeneous Multimedia-Communication based on mobile agents (Priority program adaptively in heterogeneous communication networks with wireless access)
  - Industry projects
    - Verification of a GSM-Simulator based on ML Designer
    - Optimization of GPRS/EDGE Offer-Tools
    - Self-optimization networks

Expired Research Projects (Last Years)

- Security in communications systems (2)
  - EU-Projects in the 5. framework program
    - **USB_CRYPT**
      Crypto Module with USB-Interface
    - **SETIC**
      Secure Terminal IC
  - EU-Projects in ISIS-program
    - **WEBSIG**
      Digital Signatures for Web-Contents
    - **ELIAS**
      Elliptic Curve Cryptography Standards Reference Implementation
  - EU-Projects in the 6. framework program
    - **eMayor**
      Electronic and Secure Municipal Administration for European Citizens

Expired Research Projects (Last Years)

- Security in communications systems (3)
  - Project in vernet-Program
    (trustworthy networks), Federal Ministry of Economy
    - SELMA
      Secure electronic measurements exchange
  - Industry projects
    - Development of ATM-Encryption device with SDH-Interface (155 Mbit/s)
    - Application of FPGA‘s as crypto-modules
    - RFID-Analysis
    - Security management systems for metering devices
    - Assignment of authorization keys for distribution of information and services
    - Prototype of a RFID secured metering device

Expired Research Projects (Last Years)

- Security in mobile Systems (1)
  - DFG (Deutsche Forschungsgemeinschaft)
    - Authentication in future mobile communication systems (Priority program mobile communications)
  - Industry projects
    - Security for Electronic Road Pricing System (toll) in Singapore
    - BLUETOOTH-Security

Expired Research Projects (Last Years)

- Security in mobile Systems (2)
  - EU-Projects in 4. and 5. framework program
    - **SCARAB**
      Smart Card and Agent Enabled Reliable Access to Telecommunication Services
    - **GNIUS**
      GSM Network for Improved Access and Universal Services
  - EU-Project in CRAFTS-program
    - **NEWTRON (NEW TRANSPONDER)**
      Security technologies for a new Transponder generation

Expired Research Projects (Last Years)

- Security in automotive systems
  - Studies of RTTI TMC/TPEG Security

    Security analysis of TPEG
  - Bus networks in motor vehicles

    Security analysis of CAN, MOST, LIN as well as the gateways
  - RFID-seal
    - 1. RFID Processing
    - 2. RFID-Antennas and Distribution

Our Team

10 – 15 research assistants and visiting assistants
5 technical and administrative staff

Lectures and courses

Diplom (undergraduate) and Bachelor:

- Grundlagen der Nachrichtentechnik
- Digitale Kommunikationsnetze

Diplom (graduate) and Master:

- Digitale Kommunikationstechnologie I und II (mit Praktikum)
- Kryptographische Verfahren und Anwendungen I und II (mit Praktikum)
- Digitale Mobilfunksysteme

Completed Graduations

200 diplomas, masters and bachelors
24 Dr.-degrees

Univ.-Prof. Dr. Karl Christoph Ruland

University of Siegen
Faculty IV: Science and Technology
Department for Electrical Engineering and Computer Science
Chair for Data Communications Systems

Hoelderlinstrasse 3
D-57076 Siegen/Germany
Phone +49-271/740-2522
Fax +49-271/740-2536

E-Mail: christoph.ruland@uni-siegen.de
URL: http://www.dcs.uni-siegen.de