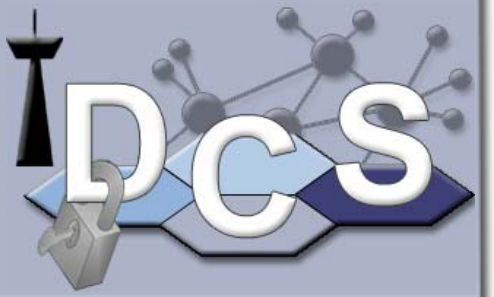
UNIVERSITÄT SIEGEN

Präsentation des Lehrstuhls für Digitale Kommunikationssysteme

Univ.-Prof. Dr. Christoph Ruland

Universität Siegen
Naturwissenschaftlich-Technische Fakultät
Elektrotechnik und Informatik
Lehrstuhl Digitale Kommunikationssysteme
Univ.-Prof. Dr. Christoph Ruland



Arbeits- und Forschungsgebiete

Aktuelle Forschungsausrichtung Anwendungsorientiert

- Automotive Security
  - CAN, FlexRay, LIN, MOST
- Sicherheit von Industrieanwendungen
  - Smart Metering, PLC, MUC, Smart Grids
- Robuste Kommunikation von Embedded Systems
  - Kryptographische Verfahren, inkl. auf Basis Elliptischer Kurven
  - Datenkompressionsverfahren
  - Fehlererkennung und – korrekturverfahren, inkl. Reed Solomon und TurboCodes (ohne/mit SISO Decodierung)
- Embedded WebServer
- Sicherer Softwaredownload
- Einsatz von RFIDs in Sicherheits- und Industrieanwendungen

Aktuelle Forschungsausrichtung Grundlagenforschung

- Joint Channel Coding and Cryptography
  - Einsatz kryptographischer Verfahren über gestörte Kanäle
- Einsatz formaler Methoden beim Design sicherer Protokolle im Messwesen
- RFID-Security Simulationen und Implementierungen
- Codierungsgewinn für passive und aktive RFID Tags
- Document Tracking Services

Aktuelle Forschungsausrichtung

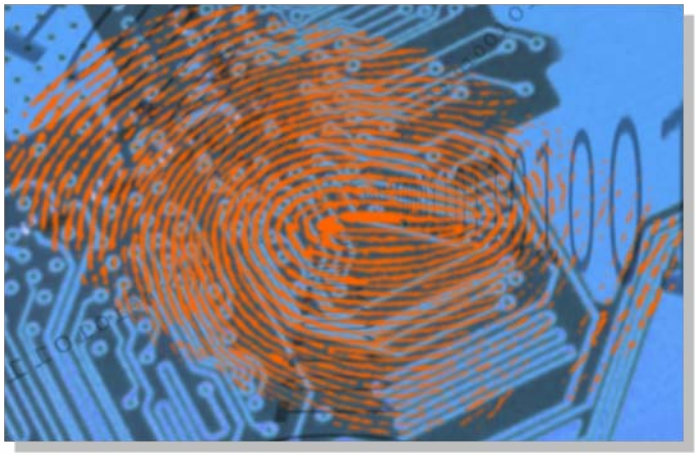
- Automotive Security
  - In Fahrzeugen werden immer mehr Elektronik, Software und Kommunikationssysteme eingebaut, von denen Gefahren ausgehen können
  - Kommunikation erfolgt innerhalb von Fahrzeugen, zwischen Fahrzeugen, und zwischen Fahrzeugen und der Außenwelt

- Sicherheits- und Risikoanalysen für das Fahrzeug und seine Komponenten vom Design bis zur Verschrottung
- Sicherheitskonzepte und –Lösungen für entsprechende Sicherheitssysteme und das erforderliche Schlüsselmanagement
- Co-Chair der eSecurity Working Group des eSafety Forums der EU (Intelligent Car Initiative 2010), deren Aufgabe es ist,
  - Forschungsbedarf, Regulierungsbedarf, Sicherheitsbedarf, etc.

  aufzuzeigen.

Aktuelle Forschungsausrichtung

- Sicherheit für Industrieanwendungen
  - Sicherer Informationsaustausch von Maschinen oder Steuereinheiten, Messgeräten und Überwachungseinheiten ist von besonderer Wichtigkeit
  - alle Kommandos an, bzw. Meldungen von die/den Steuer- und Messgeräte/n werden mit digitalen Signaturen versehen
  - ein Rechtemanagement gewährleistet, dass nur befugte Stellen Kommandos ausführen dürfen



- Digitale Signaturen und Verschlüsselung von Messdaten und Steuerdaten
- Sicherheit für PLC-Kommunikation
- Realisierung sicherer MUCs
- Datenerfassungssysteme werden in die Systeme mit eingeschlossen
- Wesentliche Bedeutung für Smart Grids

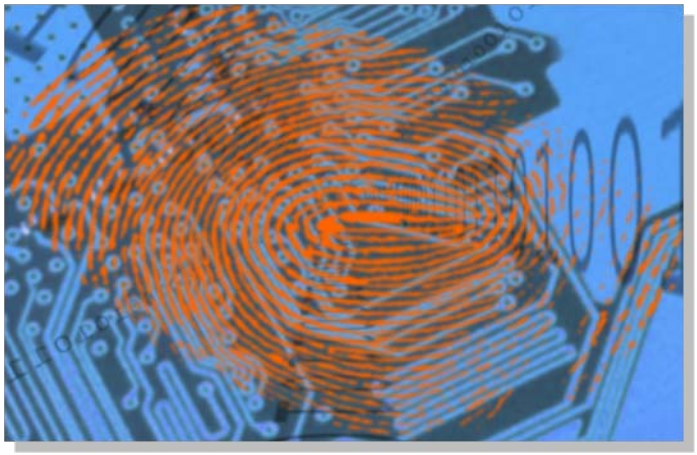
Aktuelle Forschungsausrichtung

- Robuste Kommunikation von Embedded Systemen
  - Industrielle Umgebungen sind einerseits durch starke Störungen gekennzeichnet, andrerseits wird eine große Zuverlässigkeit benötigt.
  - Im Messwesen werden Daten von sehr vielen Messgeräten gesammelt, die eine große Datenmenge zur Folge haben.

- Kanalcodierung sorgt für eine automatische Fehlerkorrektur ohne Wiederholung der Daten
- Kryptographische Verfahren sorgen für die Gewährleistung, dass die Daten nicht manipuliert wurden und von dem Absender stammen, von dem es erwartet wird
- Datenkompressionsverfahren reduzieren (Mess-) Daten bis auf 10%
- Implementierungen für Embedded Systems (Atmel, Renesas, Texas Instruments) sind vorhanden oder werden z. Zt. entwickelt

Aktuelle Forschungsausrichtung

- Embedded Webserver
  - Embedded Systeme in industriellen Anwendungen bieten in zunehmendem Masse zusätzliche WebServer, weil sie bestimmte Dienste erbringen und von außen abgefragt und gesteuert werden müssen.
  - Linux-Kernel müssen spezifisch konfiguriert und kompiliert werden, damit die benötigten Funktionen vorhanden sind
  - Besondere Anforderungen werden an die Kommunikationsfähigkeiten gestellt



- LAN-Anschluss
- GPRS-Anschluss, SMS
- TCP/IP
- SSL/TLS (zertifikatsbasiert)
- SOAP
- XML, XML Signaturen, SML, WSDL
- RFID - Interfaces

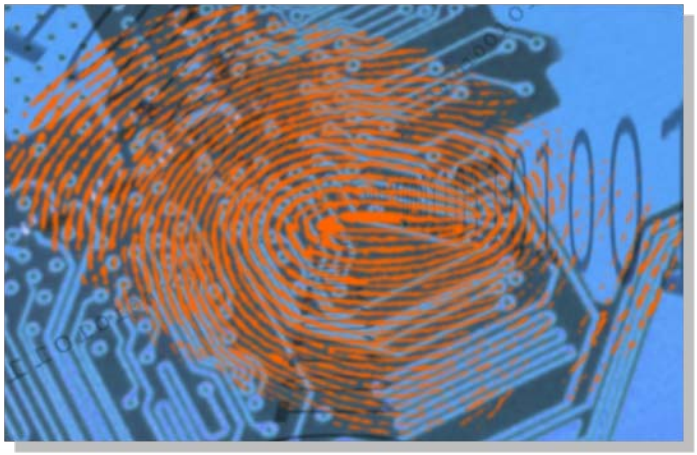
Aktuelle Forschungsausrichtung

- Software-Download (regulierter) Software
  - Viele Geräte verlangen den Einsatz von zertifizierter, zugelassener oder geeichter Software
  - Hoher Kostenaufwand bei Austausch der Software vor Ort oder im Prüflabor

  - Online Nachladen der Software als kostengünstige Lösung
  - Möglichkeiten für Download regulierter Software durch Neuerungen im Eichrecht
  - Konzept umschließt den gesamten Lebensweg der Software von der Entwicklung über die Prüfbehörde und den Betreiber der Geräte bis zu Online-Prüfmöglichkeiten der Zulassungsstellen

Aktuelle Forschungsausrichtung

- RFIDs in Sicherheits- und Industrieanwendungen
  - Wir entwickeln Systeme, in denen RFID eingesetzt werden
    - **Als elektronische Siegel**
    - **Zur Manipulations-/Plagiaterkennung**
    - **Für Logistikanwendungen**
    - **Für die Verlässlichkeit von Sensor-Informationen**
    - **Zur drahtlosen Übertragung zwischen gefährdeten oder sicheren Innenbereichen und der Außenwelt**

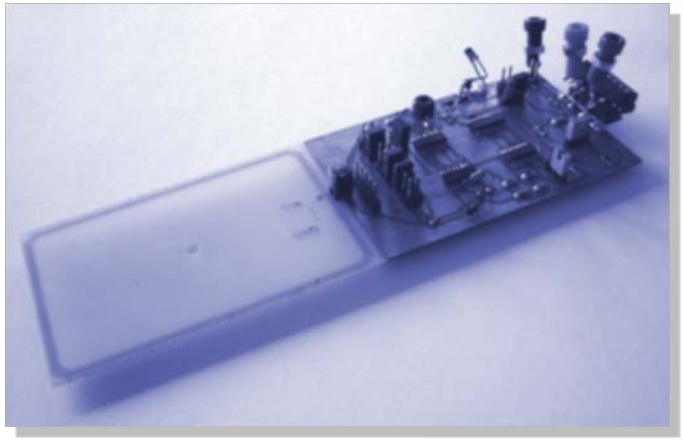


Entwicklung neuer Varianten von RFID-Basisstationen bzgl.

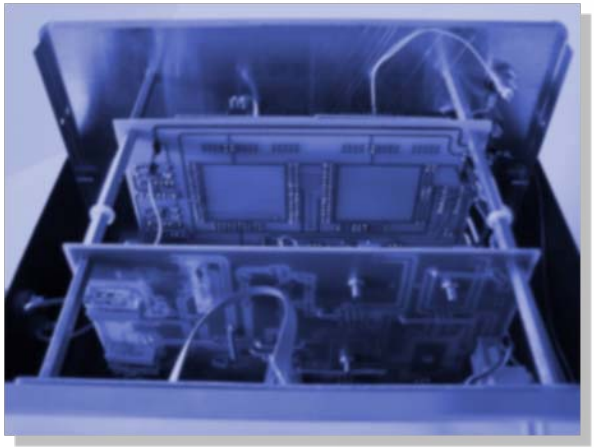
- Demodulation und Decodierung

Aktuelle Forschungsausrichtung

- RFID-Security Simulationen und Implementierungen
  - Grundlegenden elektrotechnische, nachrichtentechnischen und kryptographischen Aspekte
    - **Wie viel Energie kann zu einem RFID-Tag übertragen werden?**
    - **Welche Sicherheitsstufe kann damit erreicht werden?**
    - **Welche Verarbeitungskapazitäten lassen sich realisieren?**
    - **Welche kryptographischen Methoden sind integrierbar?**
    - **Können digitale Signaturen generiert und verifiziert werden?**
  - Verwendung digitaler Signaturen auf Basis elliptischer Kurvenkryptographie
  - Ein besonderer Augenmerk wurde auf die Implementierung digitaler Signaturen „giving message recovery“, gelegt die besonders für kurze Nachrichten geeignet sind
  - RFIDs im UHF-Bereich (bis 1 m)



Aktuelle Forschungsausrichtung



- Joint Channel and Cryptography
  - neues Forschungsgebiet, das kryptographische Verfahren mit neuen Entwicklungen der Kanalcodierung verbindet
  - moderne Kanalcodierungsverfahren mit automatischer Fehlerkorrektur setzen auf Softinput und Softoutput (SISO)
  - Der Decryptor korrigiert iterativ unter Verwendung des Softinputs
  - Feedback von Decryptor zum Decoder führt zur verbesserten Decodierung verschachtelter Blöcke
- Turbo Concatenated Codes
  - Anwendung von Joint Channel and Cryptography auf systematische fehlererkennende Codes als äußeren Code
  - Iterative Decodierung verschachtelter Blöcke mit Feedback zwischen äußeren fehlererkennenden und inneren fehlerkorrigierenden (Faltungs- oder Turbo-) Codes

Aktuelle Externe Forschungsprojekte

- TERESA
  - **T**rusted computing **E**ngineering for **R**esource constrained **E**mbedded **S**ystems **A**pplications
  - Projekt im 7. Rahmenprogramm der EU
  - http://www.teresa-project.org
  - Unser Anteil: Anwendung auf Sicherheitsaspekte im Messwesen
- OVERSEE
  - **O**pen **Ve**hicula**r** **Se**cur**e** Platform
  - Projekt im 7. Rahmenprogramm der EU
  - http://www.oversee-project.org
  - Unser Anteil: Design und Integration von IT-Sicherheit für die interne und externe Kommunikation

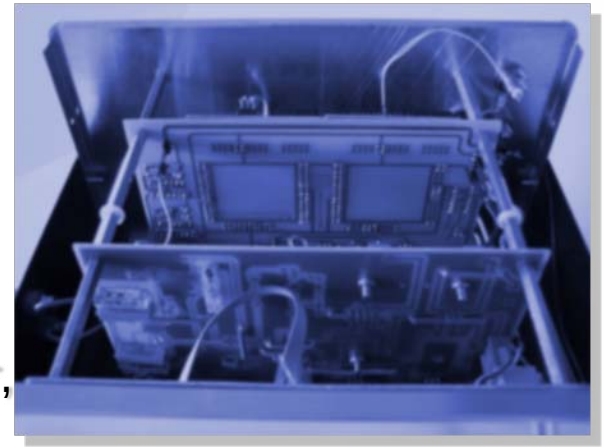
Aktuelle Externe Forschungsprojekte

- DFG-Graduiertenkolleg 1564
  - „Imaging New Modalities“
  - Multimodale Bilderkennung und -analyse im Bereich der zivilen Sicherheit
  - http://www.grk1564.uni-siegen.de
  - Unser Anteil: Rückverfolgbarkeit sensibler privater Daten
    - Sicherheitskonzept für den Schutz privater Daten, z.B. biometrischer Merkmale
    - Erkennung von Datenlecks
    - Nicht-Abstreitbarkeit der Datenweitergabe

Aktuelle Externe Forschungsprojekte

- Stromtankstellen
  - Entwicklung des Gateways mit Kommunikation zu
    - Unterschiedlichen Backend-Infrastrukturen
    - Autorisierung, Accounting und Billingserver
    - Managementzentralen, Energieprovider
    - Stromsteckdosen und ihren Messgeräten
    - Fahrzeugen

    auf Basis von embedded WebServern



- Eichpflichtiges Messwesen
  - Strom-, Gas-, Wasser-, Wärmezähler, Taxameter, Spielautomaten, etc.
  - Entwicklung von Sicherheitskonzepten (entsprechend den Eichvorschriften
  - Entwicklung und Integration der kryptographischen Software und Sicherheitsfunktionalität auf Basis von Embedded Systemen und Kryptoprozessoren

Forschungsprojekte der letzten Jahre

- Sicherheit in Kommunikationssystemen (1)
  - DFG (Deutsche Forschungsgemeinschaft)
    - Neue Betriebsarten von Blockalgorithmen und Verschlüsselung in SDH- und ATM-Netzen
    - Internet Security System für Voice-over-IP unter Berücksichtigung von Quality of Service
  - Forschungsverbund Datensicherheit NRW
    - Authentikation von Bitströmen
    - Sicherheit für MiGrid (Grid-Infrastruktur zur kooperative Wertschöpfung im Mittelstand)

Forschungsprojekte der letzten Jahre

- Drahtlose Kommunikationssysteme
  - DFG (Deutsche Forschungsgemeinschaft)
    - Heterogene Multimedia-Kommunikation auf Basis mobiler Agenten (Schwerpunktprogramm Adaptivität in heterogenen Kommunikationsnetzen mit drahtlosem Zugang)
  - Industrieprojekte
    - Verifikation eines GSM-Simulators basierend auf ML Designer (Siemens)
    - Optimierung eines GPRS/EDGE Offer-Tools (Siemens)
    - Selbstoptimierende Netzwerke (Siemens)

Forschungsprojekte der letzten Jahre

- Sicherheit in Kommunikationssystemen (2)
  - EU-Projekte im 5. Rahmenprogramm
    - **USB_CRYPT**
      Crypto Module with USB-Interface
    - **SETIC**
      Secure Terminal IC
  - EU-Projekte im ISIS-Programm
    - **WEBSIG**
      Digital Signatures for Web-Contents
    - **ELIAS**
      Elliptic Curve Cryptography Standards Reference Implementation
  - EU-Projekte im 6. Rahmenprogramm
    - **eMayor**
      Electronic and Secure Municipal Administration for European Citizens

Forschungsprojekte der letzten Jahre

- Sicherheit in Kommunikationssystemen (3)
  - Projekt im Vernet-Programm (vertrauenswürdige Netze), Bundeswirtschaftsministerium
    - SELMA
      Sicherer Elektronischer Messdaten-Austausch
  - Industrieprojekte
    - Entwicklung von ATM-Verschlüsselungsgeräten mit SDH-Interface (155 Mbit/s) (BSI)
    - Einsatz von FPGA‘s als Kryptobausteine (Bosch Telecom)
    - RFID-Analyse (Siemens CT)
    - Messgeräte-Sicherheitsmanagementsysteme (EDV ITF Fröschl)
    - Zuteilung von Zugangsschlüsseln für die Verteilung von Informationen und Dienstleistungen (Secutanta)
    - Prototyp eines RFID geschützten Messgerätes (Secutanta)

Forschungsprojekte der letzten Jahre

- Sicherheit in mobilen Systemen (1)
  - DFG (Deutsche Forschungsgemeinschaft)
    - Authentikation in künftigen Mobilfunksystemen (Schwerpunktprogramm Mobilkommunikation)
  - Industrieprojekte
    - Security für das Electronic Road Pricing System (Maut Gebühren) in Singapur (Mitsubishi Heavy Industries, Kobe)
    - BLUETOOTH-Security (Nokia)

Forschungsprojekte der letzten Jahre

- Sicherheit in mobilen Systemen (2)
  - EU-Projekte im 4. und 5. Rahmenprogramm
    - **SCARAB**
      Smart Card and Agent Enabled Reliable Access to Telecommunication Services
    - **GNIUS**
      GSM Network for Improved Access and Universal Services
  - EU-Projekte im CRAFTS-Programm
    - **NEWTRON (NEW TRANSPONDER)**
      Sicherheitstechnologie für eine neue Transpondergeneration

Forschungsprojekte der letzten Jahre

- Sicherheit in automobilen Systemen
  - Studie RTTI TMC/TPEG Security (BSI)
    Sicherheitsanalyse von TPEG
  - Bussysteme in Kraftfahrzeugen (BSI)
    Sicherheitsanalyse von CAN, MOST, LIN sowie der Gateways
  - RFID-Siegel (Volkswagen AG)
    - 1. RFID Processing
    - 2. RFID-Antennen und Ausbreitung

Unser Team

10 – 15 wissenschaftliche Mitarbeiter und Gastwissenschaftler
5 nicht-wissenschaftliche Mitarbeiter

Unsere Lehre

Diplom-Grundstudium und Bachelor:

- Grundlagen der Nachrichtentechnik
- Digitale Kommunikationsnetze

Diplom-Hauptstudium und Master:

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

Unsere Absolventen

200 Diplomanden
24 Doktoranden

Univ.-Prof. Dr. rer. nat. Karl Christoph Ruland

Universität Siegen
Fakultät IV Naturwissenschaftlich-Technische Fakultät
Elektrotechnik und Informatik
Lehrstuhl für Digitale Kommunikationssysteme

Hölderlinstrasse 3
D-57076 Siegen
Tel: +49-271/740-2522
Fax:+49-271/740-2536

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