Security for Mixed Critical Systems

In Mixed Criticality Systems, different applications with various criticality levels are executed on the same platform. These different criticality levels of the applications are due to the varying needs for system attributes such as fault-tolerance, real-time operations, safety and security.
Recently, multi-processor systems have become more important for Mixed Criticality Systems. Combined with the increasing usage of networked multi-core chips, security is gaining a considerable attention in these systems. Whereas security has many dimensions such as confidentiality, integrity and authenticity, the applications running on a Mixed Criticality Systems have varying requirements for a given dimension. These requirements need to be addressed at the different levels in the Mixed Criticality System. This includes security for the chip itself, for the communication amongst chips in the cluster and for the software running on the Mixed Criticality System.

☎ Dipl.-Inform. Thomas Koller +49 271 740-2947
✉ thomas.koller@uni-siegen.de

Joint Source and Channel Coding and Cryptography

This new area of research combines cryptographic methods with source and channel coding. Modern channel coding and decoding methods, providing error detection and correction, are increasingly using soft input and soft output (SISO) methods for increased performance, i.e., they deal with real numbers instead of binary „0“s and „1“s. Soft output is the probability of what a received value should have been before transmission, i.e., how probably it was a bit „0“ or a bit „1“. If the cryptographic methods (symmetric and asymmetric) work with soft output values of the decoder, the decoding error rate is significantly reduced and the verification rate of the cryptographic redundancy is significantly increased. If, however, “soft” verification methods are used instead of the classic „hard“ verification methods, the verification rate is further increased, since the verification criteria are not so strict. Thus, not only the error-free messages and their cryptographic redundancy are accepted, but also the messages whose cryptographic redundancy is slightly different than the transmitted value. This result in those messages being accepted as authentic, which would otherwise have been discarded through hard verification. The reduction of the security level can be compensated.

☎ PD Dr.-Ing. habil. Nataša Živić +49 271 740-2332
✉ natasa.zivic@uni-siegen.de

Security in Real-time and Industrial Communications

We work mainly on authentication of data and non-repudiation services for communication in high speed networks, for realtime applications and the distribution of information in broadcast- and multicast networks. Multimedia distribution and industrial applications are examples. The provision and verification of the trustworthiness of data have to be performed „on the fly“ during transmission of data, so they can be forwarded and processed without essential delay. We focus on the analysis of the impact of security mechanisms on quality of service of data communication, for example on delay, throughput, error propagation, relation to error recovery and (self-) synchronization. Therefore, modes of operation of cryptographic mechanisms are one of our main subjects. Project examples are the integration of security in automotive bus systems and the distribution of information via traffic information systems.

Industrial Applications and Smart Factory

Reliability and authentication of information, which are exchanged between machines (M2M), are very important, because lost or manipulated data can cause huge damages. One of our application oriented activities is the integration of digital signatures in industrial applications. The implementation use embedded systems and other components with limited resources, for example the integration in PLC components. Preferably we use elliptic curve cryptography and lightweight cryptographic modules. We combine them with forward error correction codes like Reed-Solomon or Convolutional Codes to increase the reliability in industrial and electrically noisy environments. We integrated cryptography in metering systems (gas and electricity) and developed gateways for eMobility networks. Key management is included as well.

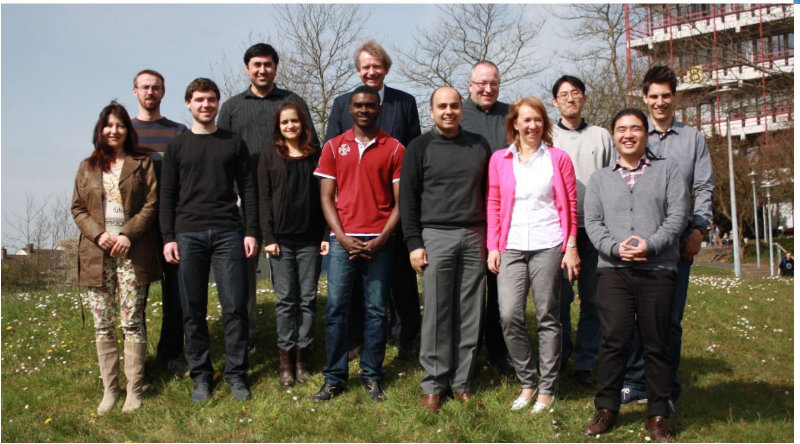
We develop security concepts, which are subject to official security evaluations. Our approved solutions can be easily applied to other transaction oriented systems like cashier terminals, taximeters, betting machines, wages, pumps and other metrological units.
Automation 4.0 will request for such security services and mechanisms. The usage of TSL/SSL is not enough, end-to-end security is needed for verification, for storage of messages inclduing the signature and liability reasons. Therefore our results and experiences should be of great interest for Automation 4.0.

☎ Univ.-Prof. Dr. Christoph Ruland +49 271 740-2522
✉ christoph.ruland@uni-siegen.de

Cooperation sought and offered

We look for cooperation with partners from industry, private and public organizations to

- share our knowledge by consultancy
- develop technical concepts and specifications
- implement new technologies in prototypes (hardware and software)
- accept the security challenges of Factory 4.0, smart grids and broadcast communication
- share our activities in security standardization and resulting benefits by having early access to



Chair for Data Communications Systems
Univ.-Prof. Dr. rer. nat. Karl Christoph Ruland

Hoelderlinstraße 3
57068 Siegen Germany

☎ +49 271 740-2522
📠 +49 271 740-2536
✉ christoph.ruland@uni-siegen.de
🌐 http://www.dcs.uni-siegen.de

Office:

☎ Birgit Wichmann +49 271 740-2521
✉ birgit.wichmann@uni-siegen.de

September 2014

UNIVERSITÄT SIEGEN
Naturwissenschaftlich Technische Fakultät

Faculty of Science and Technology

Department Electrical Engineering and Computer Science

Chair for Digital Communications Systems

DCS

Univ.-Prof. Dr. Karl Christoph Ruland

The Chair for Digital Communications Systems

Our Team

12-18 scientific and non-scientific team members

International Standardization

We participate in national and international standardization (DIN and ISO) of cryptographic security

Our Research Activities

- 13 EU-Projects
- Part of DFG Graduate School 1564 "Imaging New Modalities"
- DFG project "Modes of Operation for Compressive Sensing based Encryption"
- DAADA-Projects and cooperation with
  Shanghai University
  Duksung University, Seoul
  University of Arizona, Tucson
  University of Belgrade
  Technical University of Chisinau, Moldova

Our Graduates

more than 140 supervised graduate thesis
26 dissertations (doctoral thesis)
6 doctorate students became professor

Our courses

Fundamentals of Data Communication
Data Communication Technology I and II
Cryptography and its Applications I and II
Data Networks (interfaces, Protocols, Services)
Mobile Communication

Our Research and Work Areas

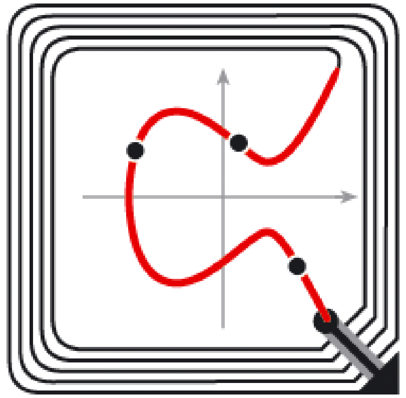
Integration of Cryptography and Robustness into all Layers of Communications and Distributed Systems

- Embedded System Security and Cryptography for real-time and industrial applications
- Hardware and physical layer cryptography
- Cryptography over noisy channels
- Compression, Error Correction Coding and Cryptography
- Reliability, Robustness, Safety and Security
- RFID Security, Robustness and Efficiency
- Content based Image and Audio Authentication
- Smart Grid Security and E-Mobility

These research areas are presented on the following pages.

Error Control in RFID Systems

Radio Frequency Identification (RFID) Systems have become a part of everyday life over the course of the past decades. Among those systems, the group of long-range systems is mainly used for item management in logistics and the supply chain. In these domains, long reading distances, quick and a reliable identification of a large number of objects are the keys to success. Extended distances, difficult propagation environments and mobile objects do however lead to varying channel conditions, hindering the successful identification. The protocols currently standardized and used, fall short of dealing with these challenges. In the course of the research at our chair, we analyze and evaluate the use of established and novel error-control methods, to extend the protocols used in long-range RFID systems, making them more robust and improving their performance. This covers the use of state of the art channel codes and their corresponding decoders as well as modern hybrid ARQ protocols. The limitations of the resources of the tags and a desire for compatibility with legacy systems remain always in focus of our efforts, which are based on the widespread, international standards EPCglobal (UHF) and ISO-18000-63.



Under security aspects we focus on the implementation of „digital signatures giving message recovery". Short messages are contained in the signature, which is not appended to the message. This results in much shorter signed messages. Data to be sent from RFID tags are mostly short, they contain stored information, identities or sensor data, for examples passport information, bank notes identities, tickets or temperatures. All of them can be included in the signatures of type „giving message recovery".

☎ Dipl.-Ing. Andreas Schantin +49 271 740-3988
✉ andreas.schantin@uni-siegen.de

Grid Security – Secure Wireless Date/Time Distribution

Long Wave Radio systems are widely used to distribute the actual date and time information, because wireless transmission guarantees timeliness. DCF is an example of such a timestamp distribution system. The provision of timeliness and reliability of time information is very important for many devices, which are controlled by time stamped telematic telegrams or time triggered events, and play an essential role for public and private safety. The correct behavior of the devices of any system is only possible, if a synchronized and correct system time is available in all devices.

The distribution of time telegrams is used to synchronize the system clocks of the receivers and their real time clocks. These received time messages, cannot be securely verified by the Long Wave Radio Receiver, because there is no backchannel. Time telegrams can be manipulated or generated by „man-in-the-middle" attacks.. By manipulating the receiver´s system clock the control behavior of the device can be completely changed. Even the application of digital signatures and encryption to time telegrams doesn´t protect against man-in-the-middle attacks. With our approach we are able to verify time telegrams in Longwave-broadcast transmission systems without return channel.

This research area is embedded in our wider scope of security in Smart Grids, because all information exchange in smart grids has to be timeliness, unique, authentic and confidential.

☎ Dipl.-Ing. Matthias Schneider +49 271 740-3166
✉ matthias.schneider@uni-siegen.de

Cryptography for Compressive Sensing

Compressive Sensing is a very hot topic in data communication, because sampling and compression of input signals is done in one step and the compression rate is much higher than known before and expected. Compressive Sensing is used for image giving sensors, which work in different ranges of the spectrum. Again, security and authenticity of the sensor information is important for the further processing. Therefore we work on research projects, partially funded by DFG, to integrate different modes of operation of encryption and authentication in the process of compress sensing. This integration shows many advantages against adding security after compression.

☎ M. Sc. Robin Fay +49 271 740-3322
✉ robin.fay@uni-siegen.de

Content based Image and Audio Authentication

The rapid development of wireless mobile communication technology and the advent of various new multimedia services have accelerated the growth of multimedia traffic, in such a way that multimedia content is currently playing an important role in the success of multimedia services. In this regard, content security in multimedia communication has emerged as the biggest concern regarding the authenticity and integrity of multimedia content. However, those emerging security demands are difficult to be met by the standardized cryptographic methods, since they are basically designed to authenticate the binary representation rather than the perceptual content of the image or audio data.

authentic or not authentic?

Therefore, our research in this area aims at investigating a new security concept based on the semantic meaning of multimedia content including the image and audio for providing the secure multimedia communication. In addition, we will develop a novel method which can tolerate a certain level of distortion preserving the perceptual content (e.g., noise generated by transmission errors over a wireless channel or by image compression) while having the capability to detect and localize the malicious tampering.

☎ M. Eng. Jinsuh Shin +49 271 740-3325
✉ jinsuh.shin@uni-siegen.de