KASTEL – An Application-Driven Center of Excellence for IT Security

KASTEL – Kompetenzzentrum für angewandte Sicherheitstechnologie

Jörn Müller-Quade, Karlsruhe Institute of Technology

Summary Smart infrastructures, cloud computing, and public security challenge the IT security of the future. In addition to the classical term of security one also has to deal with data that must be kept in clear text, mutually distrustful parties, and threats from insiders. It is not sufficient anymore to only consider the security of single components within a complex system. Furthermore, security can only be achieved in an interdisciplinary effort. The Center of Excellence for Applied Security Technology KASTEL (Kompetenzzentrum für Angewandte Sicherheits-TEchnoLogie) is a research center for security that combines several areas of IT security, users, and legal experts. ►►► **Zusammenfassung** Intelligente Infrastrukturen, Cloud Computing und öffentliche Sicherheit stellen große Herausforderungen an die IT-Sicherheit der Zukunft. Zusätzlich zum klassischen Schutz der Peripherie muss mit neuartigen Herausforderungen umgegangen werden: Damit die Nutzungsdaten zur intelligenten Steuerung verwendet werden können, dürfen diese von Energieverbrauchern nicht verschlüsselt werden. Ebenso können Daten in der Cloud nicht einfach verschlüsselt werden, wenn Services auf diesen Daten erbracht werden sollen. Darüberhinaus sind große IT-Systeme heute nicht nur durch Bedrohungen von außen, sondern auch durch sogenannte Insider-Angriffe gefährdet. Insgesamt genügt es nicht mehr, die Sicherheit von Teilsystemen zu betrachten. Eine ganzheitliche Sicherheitsbetrachtung benötigt disziplinenübergreifende Methoden. Jedoch hat jede Disziplin ihre eigenen Abstraktionen, eigene Begrifflichkeiten und Konzepte. Die Ergebnisse der einzelnen Disziplinen stehen bisher isoliert und es kann keine ganzheitliche Garantie für das Gesamtsystem gegeben werden. Klare Schnittstellen zwischen den Disziplinen sollen es erlauben, Ergebnisse über Fachgrenzen zu transportieren und somit einen durchgängigen Entwurf ganzheitlich sicherer Systeme zu ermöglichen. Um solche Schnittstellen zu erarbeiten und etablieren, bündelt das Kompetenzzentrum für Angewandte Sicherheits-TEchnoLogie (KASTEL) die Kompetenzen verschiedener Teildisziplinen der IT-Sicherheit, Anwender und Rechtsexperten.

Keywords D.4.6 [Software: Operating Systems: Security and Protection]; K.6.5 [Computing Milieux: Management of Computing and Information Systems: Security and Protection] ►►► **Schlagwörter** IT-Sicherheit, ganzheitliche Sicherheitsbetrachtung

1 The Situation

Our society is depending more and more on information technology. At the same time, attacks on our information infrastructure are growing and becoming more professional and severe. In particular, Stuxnet demonstrated the advancing skill and insight of the attackers. With the advent of intelligent infrastructures information security will become essential for the safety of our society. While a large arsenal of advanced techniques to defend against cyber attacks exists, things still go wrong. Why is this? Large, adaptive, networked IT systems are among the most complex systems ever developed by humans. They are difficult to understand and difficult to defend. The traditional methods for dealing with complex systems are inadequate as security is a very fragile property often conflicting with a simple and modular approach. For example, a secure component can become insecure when used in a different context. Furthermore, for a long time companies had little incentive to invest in security.

There is an additional problem. The separate disciplines of informatics dealing with security, like cryptography, network security, program analysis, verification, or component based software design are highly developed. However, the security guarantees derived from these different disciplines stand isolated. There is no consistent view, not even common notions. Therefore, there is no overall guarantee for the complete system and no integrated development process for secure systems.

The following three simple examples illustrate the difficulty of secure system development:

- In a consulting project the KIT developed a security concept for unforgeable products. This involved the cryptographic generation of product codes, a product code verification procedure, and secure backups ensuring the availability of the system even in case of a partial breakdown.
  Based on presentations given at meetings the industry partner implemented part of the system and presented it at a trade fair. There was no security assessment of the final system and no security expert made the decision which part of the system was realized. No actual security guarantees can be given.
- Security assumptions, like the accessibility of certain hardware components, are often implicit. Thus, these necessary assumptions sometimes get lost in the development process or over time. The CAN bus in cars was designed without security mechanisms as an attacker would have to break into the car to access the bus located inside. This design decision, however, was forgotten later and the first attempts to add wireless communication to the CAN bus violated the assumption introducing many vulnerabilities. A precise documentation of security assumptions is necessary, especially for systems which are under continuous development.
- Modern EC cards have chips employing provably secure cryptographic mechanisms. Most of them, however, still possess an additional magnetic stripe as a fallback solution that can be applied whenever the chip does not work or cannot be used. An attacker who got hold of a PIN and a magnetic stripe by a skimming attack, however, can mount an attack by deliberately disabling his own chip. The fallback mechanism neutralized the security mechanism. This shows that security is a very fragile property.

2 Competence Centers for IT Security

In November 2010, as a reaction to the dissatisfactory situation of IT security, the Bundesministerium für Bildung und Forschung (BMBF, Federal Ministry of Education and Research) announced a competition for building competence centers for IT security research. This step was explicitly taken to strengthen fundamental research in IT security and privacy. Universities and non-university research centers were invited to participate. The main requirements focused on the future challenges

Figure 1 The logo of the competence center KASTEL depicts the Castel del Monte in Apulia. (© KIT).

Figure 2 The Castel del Monte in Apulia serves as an inspiration for KASTEL. Its architecture resists attacks from the outside and from within. In addition to protective walls, the interior structure was chosen so that access to the emperor was possible through a guarded courtyard only. (Source: Public Domain/Wikipedia).

of IT security and their applications. As the result of the competition in February 2011 three research centers for cyber security were announced. These centers are:

- *European Center for Security and Privacy by Design* (EC-SPRIDE) at TU Darmstadt
- *Kompetenzzentrum für angewandte Sicherheitstechnologie* (KASTEL) at Karlsruhe Institute of Technology (KIT)
- *Kompetenzzentrum für die IT-Sicherheitsforschung Sicherheit, Vertraulichkeit, und Schutz der Privatsphäre in der digitalen Gesellschaft* (CISPA) at Saarland University

The funding of these competence centers is divided into two phases. The initial funding period will last four years. Depending on a successful evaluation after three years, the funding can be extended for another four years. However, the competence centers will be established as permanent institutions. After the funding has ended the centers must have established a financing concept, e. g., relying on third party funding, cooperation with the industry, and support by the hosting university.

This article will focus on the aims and the approach of the Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) in Karlsruhe.

3 KASTEL

The competence center KASTEL encompasses eleven research groups from theoretical cryptography to software engineering and law. The members of KASTEL aim at establishing interfaces between their different disciplines. This is necessary to obtain overall security guarantees for complete systems, which is not state of the art, yet. As an example, cryptographers typically neglect programming errors. There exist highly developed techniques for finding programming errors that lead to an information flow from secret values to publicly accessible variables. It is not known if cryptographic guarantees and information

KASTEL Members

Prof. Dr. Bernhard Beckert is with the Institute of Theoretical Informatics (ITI). His main interests lie in the fields of formal logic and logic-based techniques. These techniques are used in the specification, design, development, and verification of software and hardware systems and aim to increase the reliability and security of computer systems.

Prof. Dr. Jürgen Beyerer is the head of the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) and the chair for Vision and Fusion Laboratory (IES) at the KIT. New systems allowing automated visual inspection, pattern recognition, as well as the instrumentation for monitoring and controlling industrial processes, are developed at the IES.

Jun.-Prof. Dr. Dennis Hofheinz is with the Institute of Cryptography and Security (IKS). He is interested in theoretic cryptography and its connections to related areas. Particularly a strong focus lies on the construction and analysis of provable secure cryptosystems and cryptographic protocols.

Prof. Dr. Jörn Müller-Quade is a member of the board of directors at Research Center for Information Technology (FZI) and head of the IKS. He is the initiator of the competence center KASTEL. His main research interests are secure cloud computing, secure multiparty computation, secure key exchange methods, security definitions and models, and general security questions.

Prof. Dr. Alexander Pretschner is the head of the research group Certifiable Trustworthy IT Systems (ZVI) at the Institute for Program Structures and Data Organization (IPD). His work is concerned with the interfaces between software techniques and information and functional security.

Prof. Dr. Ralf Reussner is a member of the board of directors and executive board at the FZI. At the KIT, he is head of the research group Softare Design and Quality (SDQ). His research at the SDQ focuses on component-based architectures, specially the implication of the architecture on the security of software systems.

Prof. Dr. Hartmut Schmeck is a member of the board of directors at the FZI, head of the research group Efficient Algorithms at the Institute of Applied Informatics and Formal Description Methods (AIFB), and scientific spokesperson of the KIT focus COMMputation. His research group is interested in self-organized, adaptive, and secure systems and methods for use in modern computer infrastructures, as well as on information processing and business processes.

Prof. Dr. Gregor Snelting is head of the Programming Paradigms Group. This research group focuses on the compilation, analysis, and application of the different program paradigms. The program analysis of object-oriented languages and applications to the software security and verification is in the center of its research.

Prof. Dr. Indra Spiecker genannt Döhmann, LL.M., is head of the Information and Data Privacy Law group and chair of the Institute of Information and Business Law (IIWR). Public Information, telecommunications law and data privacy law, as well as the comparison with US and European law, are a few of her research topics.

Prof. Dr. Stefan Tai is a member of the board of directors at the FZI, head of the research group Economics and Technology of eOrganizations at the AIFB and spokesperson for the topic Service and Web Engineering in the KIT focus COMMputation. His main research areas are service computing and cloud computing, particularly Middleware/Platforms and reliable e-Business Applications.

Prof. Dr. Martina Zitterbart is the head of the Institute of Telematics at the KIT. Her interests span from multimedia communication systems to mobile and ubiquitous communication, ambient technologies, wireless sensor networks, and network security.

flow guarantees together rule out any information flow to an attacker on the code level. Another example is code verification. With verification all programming errors are provably ruled out. Only specific properties are verified, however, and it is not clear if the verified properties really imply the desired security properties. This is particularly difficult if the security properties are defined by a functional equivalence to an ideal system.

KASTEL is application driven, i. e., the gaps and hence the necessary interfaces between the disciplines will be identified while working on the development of concrete systems. Three prototypes, based on existing systems, will be implemented from specification to a final security analysis. All difficulties encountered in this process will be documented and will be among the first results of KASTEL. Starting from the concrete difficulties and gaps, interfaces and joint security notions will be developed to obtain precise security statements bridging multiple disciplines.

The prototypes to be realized in KASTEL are a smart home for intelligent energy management, a joint collaboration platform built on cloud computing, and privacy preserving surveillance of public places. For each of the three prototypes we investigate four basic research questions.

How is security defined for the prototype? KASTEL aims at a consistent view incorporating technical definitions as well as the legal and economic side.

How to develop secure systems? Security properties should be clearly specified at every level of development. Security must become an integral part of the development process.

How to analyze and prove security? Security does not compose and a simple modular approach is not possible. One has to view the complete system.

How to archive and transfer competence? Semantic properties are used to manage knowledge and competence transfer within KASTEL as well as in education.

The goal of KASTEL is to assess the overall security of systems instead of just working with isolated system components. New threat models and appropriate methods are needed as well as a collaboration of cryptographers, IT security specialists, software engineers, jurists, and network experts. Protecting systems at their periphery with encrypted channels and firewalls is not sufficient anymore.

4 Three Prototypes

In KASTEL, fundamental research questions will be tackled by working on three prototypes. The security of these prototypes will always be considered from two points of view: What is possible in principle? And how can this problem be solved from a practical point of view right now? The practical systems will make the different views of the different disciplines concrete enough to find the gaps which so far prevent an integrated approach to the security of complete systems. On the other hand, we can incorporate new theoretical results in the design and development of practical examples. The three prototypes are *Smart Homes*, *Secure Collaboration*, and *Privacy-aware Surveillance* and will be presented in the remainder of this section.

Figure 3 KASTEL seeks to develop a smart home prototype that provides strong and precise security and privacy guarantees and at same preserves the capabilities that enable an intelligent demand-side management. (© SWR (Björn Lilienthal)).

4.1 Smart Energy and Smart Homes

As part of efforts to improve energy efficiency, power supply grids will be reorganized from their current centralized structure to a decentralized, intelligent structure. To deal with variable grid power levels, arising from unreliable power sources such as wind and solar energy, an intelligent demand-side management in so-called smart homes is required. This necessitates the processing of sensitive high resolution power consumption data. Moreover, electric household appliances need to be enhanced with intelligent, interconnected controllers, to harmonize their power consumption with grid power availability. This, however, introduces several problems concerning security and privacy. There is the question of how fine-grained power-consumption information can be gathered in a way complying with consumer privacy, while still being useful for the grid provider. More dramatically, unprecedented vulnerabilities against cyber-attacks arise from the use of intelligent components. This KASTEL project seeks to develop a smart home prototype that provides strong and precise security and privacy guarantees and at same preserves the capabilities that enable an intelligent demand-side management.

4.2 Cloud Computing and Secure Collaboration

Efficient collaboration platforms are crucial for modern enterprises. Small and medium enterprises can group together to form virtual companies, large enough to win a specific tendering. In order to support such virtual organizations, Collaboration Services (e. g., concurrent document editing) can be realized efficiently by using

Figure 4 In KASTEL, we aim to develop a technology that minimizes the volume of data obtained by surveillance systems. This data must also be protected against abuse. To achieve this goal, raw sensor data is processed and an abstract representation is compiled. Cryptographic methods then secure this abstraction. (Source: jurec/pixelio.de).

high-availability cloud-based collaboration services. Privacy, however, is threatened by uploading sensitive data to untrusted parties. Furthermore a virtual organization can comprise of competing enterprises which are to a certain extend mutually mistrustful.

In KASTEL, we develop a secure collaboration platform in two phases. First, a storage back-end is implemented. It supports fully-automatic data distribution to different clouds and encryption, minimizing data leakage into the cloud. The second phase implements collaboration services and a front-end on top of the secure architecture. The goal is to process the encrypted data efficiently in the cloud, using the whole cloud potential while mitigating privacy issues by a secure design.

4.3 Privacy-aware Surveillance

The automatic surveillance of public space is an important means for preventing threats and solving crimes. On the other hand, it is an intrusion into the privacy of citizens. This is why it is perceived negatively by the public. New technologies make it possible to protect the privacy of citizens better than in conventional systems.

We aim to develop a technology that minimizes the volume of data obtained by surveillance systems. This data must also be protected against abuse. To achieve this goal, raw sensor data is processed and an abstract representation is compiled. Cryptographic methods then secure this abstraction.

5 Four Fundamental Questions

One of the goals of KASTEL is to find satisfying answers to four fundamental questions. Finding universal answers to these questions is hard because different disciplines use different terminology. Also, many concepts are understood differently in different fields. We hope to improve our overall understanding of how to develop secure systems by struggling to find answers to these questions.

5.1 What Is Security?

Different disciplines have different views on what security is. For example:

- In Cryptography, security is a formally defined and provable property. Cryptographic definitions describe abstract protocols and provide exact mathematical definitions. Due to this abstraction, cryptography does not capture the complexity and variety of real systems.
- In Security Engineering, security means that the system is resistant against known attacks. Security Engineering considers overall system security. It is hard, however, to find the borders of a system.
- In Software Engineering, security means the compliance to contracts between components.
- In Law, questions about data privacy and liability are of interest.

The different definitions of security suit the specific methods of the disciplines, however, to achieve holistic security guarantees for complete systems one needs compatible notions. One goal of KASTEL is to provide a framework that allows for the identification of specific security requirements through precise mathematical definitions. This allows for combining requirements of different fields to a big picture. In order to capture formal guarantees as well as being judicially resilient, the security notions found this way have to be applicable on different levels.

5.2 How Can Secure Software Be Developed?

In the development of large software systems, security concerns often play a minor role. One reason is the complexity of the overall system. There are methods that help to identify and to avoid certain flaws. There is, however, no practical method to guarantee the overall security of the system to be built. Furthermore it is not enough to consider known attacks. Analogous to other disciplines of IT security all attacks within a realistic model should be avoided.

KASTEL will incorporate the specification of security properties into the component based software development process. The approach taken aims at extending the Design-by-Contract paradigm. The contracts between the components will have to include security assertions and the security properties of the overall system should be deduced from the contracts. Then it suffices to prove that the different components fulfill their respective contracts. The idea is to pretend at the level of abstraction of a software engineer that security properties compose. The composability problems as well as the concrete realization of security mechanism will later be dealt with by cryptographers.

With this approach it would be possible to break down the security of the overall system in a stepwise refinement process. It mimics a modular approach on an abstract level from which very precise security requirements for the components can be obtained.

5.3 How Can Security Be Proved?

Proving security properties of systems, even of relatively small ones, is often a complicated task. Additionally, in most cases, these proofs of security do not compose: If we construct a complex system from provably secure components it is not sufficient to prove that the way of combining the components is secure. Instead, we have to conduct a proof of the whole system with all of its components. This is one of the main reasons why techniques to rigorously prove the security of a system are not feasible for many practical applications.

Since we strongly believe that the existence of practical tools to analyze and prove the security of systems is one of the major steps towards developing critical infrastructures that we all can rely on, we made this topic one of the fundamental questions of KASTEL. We investigate new methods to make proofs of security more modular and hence feasible in practice.

5.4 How Can Security Expertise Be Transferred?

Many researchers, practitioners, and students will work together to find answers to some fundamental questions about information security in KASTEL. There is the huge challenge of bringing together the knowledge and expertise of different disciplines. Furthermore, KASTEL is a long-term project. Researchers will leave the projects and others will join. The knowledge of those who have left may not be lost.

We will set up a software platform that will help us transfer and archive knowledge. It will be based on a semantic wiki. The basic idea is to enhance the simple but powerful concept of wiki software with concepts from the Semantic Web. By annotating human-readable content with machine-readable attributes, information is enriched with machine-readable meaning (semantics). By storing and processing information intelligently, we hope to provide an added value for all project partners.

The knowledge platform will form the basis for the KASTEL helpdesk. The helpdesk provides a contact point for project partners as well as companies seeking IT security expertise and so helps establishing contacts more efficiently. Also, the helpdesk will serve as a job board. In the long term, the helpdesk will contribute to the financial independence of KASTEL through subscriptions and fees.

6 Qualification Concept

Education is an integral part of the competence center KASTEL. Training more security experts will improve security in the mid term and will help to transfer the academic results of KASTEL to the industry. Instead of offering a new degree, KASTEL provides guidelines for students to select lectures, seminars, and lab training related to security within the broad academic education at KIT. A student following these guidelines and writing a master thesis related to security receives an official certificate issued by the KIT approving the specialization in security. Doctoral researchers working on research projects in KASTEL will be able to also obtain this certificate in addition to their degree.

To help IT professionals to keep up with the rapidly changing challenges in security KASTEL together with the consulting company Secorvo will offer continuing education. This will be a combination of professional courses offered by Secorvo and series of security related talks that will be established with the start of KASTEL.

KASTEL plans to attract pupils and a general audience to security related topics. Under the name "Kryptologikum" hands-on exhibits and talks will popularize the fascinating solutions of cryptographic protocols and IT security which by now go beyond mere enciphering of data.

With the qualification concept addressing a wide audience KASTEL demonstrates the maxim on which the project is built: Secure applications and systems cannot be developed or even evaluated by a few isolated experts but require the input of many disciplines and the users. At the same time it raises the awareness of security problems and ensures that they receive the attention they deserve.

7 Conclusion

Intelligent power supply, cloud computing, and networked surveillance pose big challenges for security and privacy. These complex problems can only be solved in an interdisciplinary effort. However, the different disciplines dealing with IT security currently have no consistent view or common vocabulary. KASTEL will bridge different disciplines by establishing precise interfaces allowing overall security guarantees and an integrated development of secure systems. KASTEL will establish these interfaces guided by the development of three concrete prototypes.

Received: July 27, 2011

Prof. Dr. Jörn Müller-Quade is a member of the board of directors at Research Center for Information Technology (FZI) and head of the IKS. He is the initiator of the competence center KASTEL. His main research interests are secure cloud computing, secure multiparty computation, secure key exchange methods, security definitions and models, and general security questions.

Address: Karlsruhe Institute of Technology, Am Fasanengarten 5, D-76131 Karlsruhe, Germany
Tel.: +49 721 60844205, e-mail: info@iks.kit.edu