Operational Models for Security and Dependability in Electronic Health Systems

Roland Rieke *

Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany
roland.rieke@sit.fraunhofer.de

Security and privacy are critical aspects for the acceptance of emerging new complex technologies in the public sector, particularly the protection of personal health data is of utmost importance.

In this talk four scenarios are presented where operational models for security and dependability with relevance for application in electronic health systems have been developed and analysed.

These scenarios comprise,

1. a workflow and organisation based access control model for the management of medical records in hospitals,
2. an architecture with protocols for provisioning and enforcement of security policies,
3. model based test case generation for the German electronic Health Card (eHC), Health Professional Card (HPC) and Security Module Card (SMC) and their interplay,
4. a security analysis of the German Health Card infrastructure and services in particular the management services for the insurance master data.

Key priority in (1) is the inherent ambivalence between *Privacy* and *Need to Know* requirements for the processing of medical records. A compact visualisation of aspects of such a system's behaviour and examples of properties that can be verified are given.

Scenario (2) is concerned with policy provisioning and enforcement. In a typical policy controlled system, a set of policy rules, posing restrictions on the system's behaviour, is used to enforce the required security objectives. Integration of policy validation into a policy based architecture was the main goal here.

Main topic in (3) is the compliance of an implementation with the specification. The implementation on the smartcards is measured for compliance to the specification via a suite of test case sequences that are generated from the model.

In (4) the specification of the security requirements and the specification of the security mechanisms was analysed. The use case oriented specification was transfered to an asynchronous model (using APA). In order to prove that the model correctly represents the specification in such complex systems it is very

* Part of the work presented here was developed within the project ProOnline-VSDD being funded by the German Federal Ministry of Health and in the project SicAri, a project funded by the German Federal Ministry of Education and Research.

useful to derive compact representations of component behaviour from global behaviour by computation of adequate property preserving abstractions.

In the finite state model of scenario (4) the modelling of timers, counters and logging mechanisms was critical for the scalability of the model and the properties that can be verified. Modelling problems approached during the course of action and open problems will be presented.

The operational finite state models of the scenarios above are based on *Asynchronous Product Automata (APA)*, a flexible operational specification concept for cooperating systems. An APA consists of a family of so called *elementary automata* communicating by common components of their state (shared memory). A short coverage of the applied modelling and verification concepts and tools and of (technical) challenges is also provided.

Roland Rieke has worked since 1982 as a senior researcher at Fraunhofer SIT. Currently his research interests are focussed on the development of methods and tools for formal security models and application of these techniques. Recent work includes context oriented security policies, attack graph computations and ubiquitous computing. He is member of the ERCIM working group on "Security and Trust Management". Recent publications [1–5].

References

1. Peters, J., Rieke, R., Rochaeli, T., Steinemann, B., Wolf, R.: A Holistic Approach to Security Policies – Policy Distribution with XACML over COPS. In: Proc. of the Second International Workshop on Views On Designing Complex Architectures (VODCA 2006). Volume 168., Elsevier (2007) 143–157
2. Ochsenschläger, P., Rieke, R.: Abstraction Based Verification of a Parameterised Policy Controlled System. In: International Conference "Mathematical Methods, Models and Architectures for Computer Networks Security" (MMM-ACNS-7). Volume 1 of CCIS., Springer (2007) © Springer.
3. Ochsenschläger, P., Rieke, R., Velikova, Z.: Die elektronische Krankenakte - Eine Sicherheitsstrategie. In: DACH Security 2008 - Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven. (2008) 90–100
4. Rieke, R.: Abstraction-based analysis of known and unknown vulnerabilities of critical information infrastructures. International Journal of System of Systems Engineering (IJSSE) **1** (2008) 59–77 Copyright: ©2008, InderScience.
5. Apel, C., Repp, J., Rieke, R., Steingruber, J.: Modellbasiertes Testen der deutschen Gesundheitskarten. In: DACH Security 2007 - Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven. (2007) 338–346