# A framework for modelling and testing of security policies

DISS. ETH NO. 20513

# A Framework for Modelling and Testing of Security Policies

A dissertation submitted to

ETH ZURICH

for the degree of

Doctor of Sciences

presented by

Lukas Alexander Brügger

Dipl. Informatik Ingenieur ETH

born 14.06.1982

citizen of Plaffeien

accepted on the recommendation of

Prof. Dr. David Basin
Prof. Dr. Peter Müller
Prof. Dr. Burkhart Wolff

2012

# Abstract

In this thesis, we present a uniform framework for modelling security policies and show how this framework is used for model-based conformance testing of systems implementing these policies. The framework can be used to model a wide range of different kinds of security policies. It also provides support for modelling dynamic system behaviour for modelling stateful policies. The framework supports both unit and sequence tests, and includes techniques for automatic test execution.
We show how to model large-scale policies and systems, and present techniques that allow for an efficient and effective testing of these systems. Our contributions include support for formally verified policy transformation procedures, allowing one to tame inherent state-space explosions in test case generation for security policies.
The framework is implemented in a theorem proving environment and has a rigorous formal foundation. We provide powerful techniques to reason about policies and support for a tighter integration of tests and proofs.
We provide evidence of the strength of our framework by instantiating it with two large-scale case studies: one is in the area of firewalls and networks, and the other in the area of access to electronic health care records.

# Zusammenfassung

In dieser Arbeit präsentieren wir ein einheitliches Framework für die Modellierung von Sicherheitsrichtlinien und zeigen, wie dieses zur model-basierten Konformitätsprüfung dieser Systeme benutzt werden kann. Das Framework bietet die Möglichkeit, eine Vielzahl sehr unterschiedlicher Sicherheitsrichtlinien modellieren zu können. Es bietet auch Unterstützung für Modellierung dynamischen Systemverhaltens, was für die Modellierung von zustandsbehafteten Sicherheitsrichtlinien benutzt werden kann. Das unterstützt sowohl Unit wie auch Sequenz-Tests. Ausserdem bietet es auch Techniken für die automatische Testdurchführung an.
Wir zeigen, wie auch sehr grosse Sicherheitsrichtlinien und Systeme modelliert werden können, und präsentieren Techniken für ein effizientes und effektives Testen dieser Systeme. Unsere Beiträge beinhalten das Konzept von formal verifizierten Transformationen von Sicherheitsrichtlinien, die es ermöglichen, die inhärenten Zustandsexplosionen zu vermindern.
Das Framework basiert auf einem Theorembeweiser und hat eine starke formale Grundlage. Wir bieten leistungsstarke Techniken um Sicherheitsrichtlinien zu analysieren, und bieten Unterstützung für eine engere Integration von Tests und Beweisen.
Wir belegen die Stärke unseres Framework durch die Instanziierung mit zwei gross angelegten Fallstudien: Die eine ist im Bereich von Firewalls und Netzwerken, die andere im Bereich der Zugriffskontrolle zu elektronischen Patientenakten.