
Contents

Introduction	v
1.0.1 Outline of the thesis	x
1 Preliminaries	1
I A Rule-based Approach to Security Analysis and Certification	9
2 Program Transformation for Software Certification	11
2.1 Narrowing in Rewriting Logic	14
2.2 The Unfolding Operation	16
2.2.1 Analyzing potential incompleteness	18
2.2.2 Methodology optimization	20
2.2.3 Incompleteness and Equational Axioms	21
2.2.4 Completeness of the Transformation	22
2.3 Transforming Rewrite Theories	30
2.3.1 Correctness of the transformation system	33
2.4 Coherence and Consistence	40
2.5 Securing Transfer of Code	41
2.6 Implementation	46
3 Access Control Policy Specification	49
3.1 Policy Specification Language	51
3.1.1 Policy Evaluation Mechanism	53
3.2 Policy operators: Composition, Delegation, and Closure	53
3.3 Checking Domain Properties of Access Control Policies	58
3.4 Implementation	59
II Analysis and Verification of Distributed and Complex Systems	61
4 Web Systems Filtering	63
4.1 The Filtering Language	65
4.2 Filtering is a Tree Embedding Problem	70
4.3 An Approximate Tree Matching Algorithm	71
4.3.1 Data Tree Encoding	72

4.3.2	Expanded Pattern Tree	74
4.3.3	Evaluating an unconditional, positive, ground filtering rule	75
4.3.4	Evaluating a generic filtering rule	76
4.4	A Lazy Implementation: an Experimental Evaluation	77
4.5	Semantic Filtering via DL Reasoning	80
4.6	The Extended Filtering Language	81
4.7	An XML Formalization of the Semantic Filtering Language	85
4.7.1	Using DIG to Model and Query Ontologies	85
4.7.2	The Extended DIG Ask Language	86
4.7.3	An XML Syntax for the Filtering Language	88
4.8	The XPhil Filtering System	91
5	Web Systems Verification	95
5.1	The Web specification language	96
5.2	Expanding rules with meta-symbols	99
5.3	Verification Methodology	102
5.3.1	Detecting correctness errors.	102
5.3.2	Detecting completeness errors.	103
5.4	Web Specification Restrictions	106
6	Biological Systems Modeling and Analysis	115
6.1	Quantitative Pathway Logic	117
6.1.1	Simulation and analysis of QPL models	120
6.2	Representing QPL models via Discrete Functional Petri Nets	122
6.2.1	Discrete Functional Petri Nets	122
6.2.2	Translating QPL models into DFPNs	124
6.2.3	Model equivalence.	126
6.3	Reachability analysis over DFPNs	131
6.4	Implementation	133
	Conclusions	137
A	Some technicalities	141
A.1	XPHILSchema	141
	Bibliography	145