

# Contents

- 1 Introduction . . . . . 1**
  - 1.1 Historical Context . . . . . 1
  - 1.2 Black-Box Security Protocol Analysis . . . . . 3
  - 1.3 Purpose and Approach . . . . . 6
  - 1.4 Overview . . . . . 6
    - 1.4.1 The Protocol Analysis Model . . . . . 6
    - 1.4.2 Applications of the Model . . . . . 7
- 2 Preliminaries . . . . . 9**
  - 2.1 Sets and Relations . . . . . 9
  - 2.2 BNF Grammars . . . . . 10
  - 2.3 Labelled Transition Systems . . . . . 11
- 3 Operational Semantics . . . . . 13**
  - 3.1 Analysis of the Problem Domain . . . . . 13
  - 3.2 Security Protocol Specification . . . . . 17
    - 3.2.1 Role Terms . . . . . 18
    - 3.2.2 Protocol Specification . . . . . 21
    - 3.2.3 Event Order . . . . . 23
  - 3.3 Describing Protocol Execution . . . . . 24
    - 3.3.1 Runs . . . . . 25
    - 3.3.2 Matching . . . . . 27
    - 3.3.3 Run Events . . . . . 29
    - 3.3.4 Threat Model . . . . . 30
  - 3.4 Operational Semantics . . . . . 31
  - 3.5 Example Protocol Specification . . . . . 33
  - 3.6 Problems . . . . . 34
- 4 Security Properties . . . . . 37**
  - 4.1 Security Properties as Claim Events . . . . . 37
  - 4.2 Secrecy . . . . . 39
  - 4.3 Authentication . . . . . 41

4.3.1	Aliveness . . . . .	41
4.3.2	Synchronisation . . . . .	45
4.3.3	Non-injective Synchronisation . . . . .	46
4.3.4	Injective Synchronisation . . . . .	48
4.3.5	Message Agreement . . . . .	50
4.4	Authentication Hierarchy . . . . .	51
4.5	Breaking and Fixing the Needham-Schroeder Protocol . . . . .	55
4.6	Summary . . . . .	62
4.7	Problems . . . . .	63
<b>5</b>	<b>Verification . . . . .</b>	<b>67</b>
5.1	Patterns . . . . .	67
5.2	Verification Algorithm . . . . .	74
5.2.1	Well-Typed Patterns . . . . .	75
5.2.2	Realisable Patterns . . . . .	75
5.2.3	Empty Patterns and Redundant Patterns . . . . .	77
5.2.4	Algorithm Overview . . . . .	78
5.2.5	Pattern Refinement . . . . .	79
5.3	Example of Search Space Traversal . . . . .	82
5.4	Verifying Security Properties Using Pattern Refinement . . . . .	89
5.5	Heuristics and Parameter Choices . . . . .	90
5.5.1	Heuristics . . . . .	90
5.5.2	Choosing a Bound on the Number of Runs . . . . .	92
5.5.3	Performance . . . . .	94
5.6	Verifying Injectivity . . . . .	96
5.6.1	Injective Synchronisation . . . . .	96
5.6.2	The LOOP Property . . . . .	99
5.6.3	Model Assumptions . . . . .	103
5.7	Further Features of the Scyther Tool . . . . .	103
5.8	Problems . . . . .	105
<b>6</b>	<b>Multi-protocol Attacks . . . . .</b>	<b>107</b>
6.1	Multi-protocol Attacks . . . . .	108
6.2	Experiments . . . . .	109
6.3	Results . . . . .	110
6.3.1	Strict Type Matching: No Type Flaws . . . . .	112
6.3.2	Simple Type Matching: Basic Type Flaws Only . . . . .	113
6.3.3	Untyped Matching: All Type Flaws . . . . .	113
6.3.4	Attack Example . . . . .	113
6.4	Attack Scenarios . . . . .	115
6.4.1	Protocol Updates . . . . .	116
6.4.2	Ambiguous Authentication . . . . .	118
6.5	Preventing Multi-protocol Attacks . . . . .	120
6.6	Summary . . . . .	122
6.7	Problems . . . . .	122

<b>7</b>	<b>Generalising NSL for Multi-party Authentication</b>	123
7.1	A Multi-party Authentication Protocol	124
7.2	Analysis	127
7.2.1	Initial Observations	127
7.2.2	Proof of Correctness	127
7.2.3	Secrecy of Nonces Created in Role $r_0^P$	132
7.2.4	Non-injective Synchronisation of Role $r_0$	133
7.2.5	Secrecy of Nonces Created in Role $r_x^P$ for $x > 0$	134
7.2.6	Non-injective Synchronisation of Role $r_x^P$ for $x > 0$	134
7.2.7	Injective Synchronisation of All Roles	135
7.2.8	Type-Flaw Attacks	135
7.2.9	Message Minimality	136
7.3	Variations on the Pattern	136
7.4	Weaker Multi-party Authentication Protocols	139
7.5	Problems	140
<b>8</b>	<b>Historical Background and Further Reading</b>	143
8.1	Historical Background	143
8.1.1	Models	143
8.1.2	Initial Tools	143
8.1.3	Logics	144
8.1.4	Tool Proliferation	145
8.1.5	Multi-protocol Attacks	146
8.1.6	Complexity Results	147
8.1.7	Divergence Between Symbolic and Computational Models	147
8.1.8	Bridging the Gap Between Symbolic Analysis and Code	148
8.2	Alternative Approaches	149
8.2.1	Modelling Frameworks	149
8.2.2	Security Properties	150
8.2.3	Tools	153
	<b>References</b>	157
	<b>Index</b>	167

Operational Semantics and Verification of Security  
Protocols

Cremers, C.; Mauw, S.

2012, XIV, 174 p., Hardcover

ISBN: 978-3-540-78635-1