

The Modelling and Analysis of Security Protocols: the CSP Approach

P.Y.A. Ryan and S.A. Schneider
with
M.H. Goldsmith, G. Lowe, and A.W. Roscoe

Table of Contents

Contents

	Preface	xi
Chapter 0	Introduction	1
0.1	Security protocols	1
0.2	Security properties	6
0.3	Cryptography	14
0.4	Public-key certificates and infrastructures	21
0.5	Encryption modes	23
0.6	Cryptographic hash functions	23
0.7	Digital signatures	24
0.8	Security protocol vulnerabilities	28
0.9	The CSP approach	34
0.10	Casper, the user-friendly interface of FDR	37
0.11	Limits of formal analysis	38
0.12	Summary	38
Chapter 1	An introduction to CSP	41
1.1	Basic building blocks	42
1.2	Parallel operators	49
1.3	Hiding and renaming	55
1.4	Further operators	60
1.5	Process behaviour	62
1.6	Discrete time	74
Chapter 2	Modelling security protocols in CSP	77
2.1	Trustworthy processes	77
2.2	Data types for protocol models	82
2.3	Modelling an intruder	84
2.4	Putting the network together	87
Chapter 3	Expressing protocol goals	93
3.1	The Yahalom protocol	95
3.2	Secrecy	97
3.3	Authentication	101
3.4	Non-repudiation	110

3.5	Anonymity	116
3.6	Summary	122
Chapter 4	Overview of FDR	125
4.1	Comparing processes	126
4.2	Labelled transition systems	129
4.3	Exploiting compositional structure	135
4.4	Counterexamples	139
Chapter 5	Casper	141
5.1	An example input file	141
5.2	The %-notation	149
5.3	Case study: the Wide-Mouthed-Frog protocol	151
5.4	Protocol specifications	157
5.5	Hash functions and Vernam encryption	159
5.6	Summary	160
Chapter 6	Encoding protocols and intruders for FDR	161
6.1	CSP from Casper	161
6.2	Modelling the intruder: the perfect spy	163
6.3	Wiring the network together	167
6.4	Example deduction system	169
6.5	Algebraic equivalences	171
6.6	Specifying desired properties	172
Chapter 7	Theorem proving	175
7.1	Rank functions	177
7.2	Secrecy of the shared key: a rank function	181
7.3	Secrecy on n_B	187
7.4	Authentication	191
7.5	Machine assistance	197
7.6	Summary	199
Chapter 8	Simplifying transformations	201
8.1	Simplifying transformations for protocols	201
8.2	Transformations on protocols	205
8.3	Examples of safe simplifying transformations	208
8.4	Structural transformations	211
8.5	Case study: The CyberCash Main Sequence Protocol	213
8.6	Summary	219
Chapter 9	Other approaches	221
9.1	Introduction	222
9.2	The Dolev-Yao model	222
9.3	BAN logic and derivatives	222
9.4	FDM and InaJo	227

9.5	NRL Analyser	227
9.6	The B-method approach	228
9.7	The non-interference approach	229
9.8	Strand spaces	229
9.9	The inductive approach	232
9.10	Spi calculus	234
9.11	Provable security	235
Chapter 10	Prospects and wider issues	237
10.1	Introduction	237
10.2	Abstraction of cryptographic primitives	237
10.3	The refinement problem	238
10.4	Combining formal and cryptographic styles of analysis	238
10.5	Dependence on infrastructure assumptions	240
10.6	Conference and group keying	240
10.7	Quantum cryptography	241
10.8	Data independence	242
Chapter A	Background cryptography	245
A.1	The RSA algorithm	247
A.2	The ElGamal public key system	248
A.3	Complexity theory	250
Chapter B	The Yahalom protocol in Casper	253
B.1	the Casper input file	253
B.2	Casper output	254
Chapter C	CyberCash rank function analysis	269
C.1	Secrecy	269
C.2	Authentication	273
	Notation	293