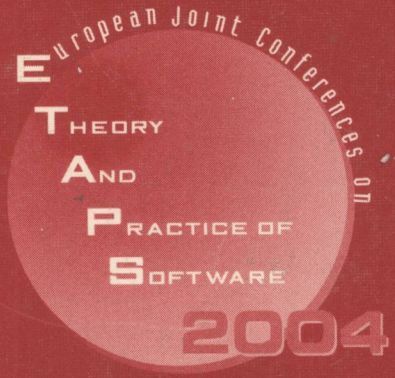
Igor Walukiewicz (Ed.)

LNCS 2987

Foundations of Software Science and Computation Structures

7th International Conference, FOSSACS 2004
Held as Part of the Joint European Conferences
on Theory and Practice of Software, ETAPS 2004
Barcelona, Spain, March/April 2004, Proceedings



Springer

Igor Walukiewicz (Ed.)

Foundations of Software Science and Computation Structures

7th International Conference, FOSSACS 2004
Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2004
Barcelona, Spain, March 29 – April 2, 2004
Proceedings

Springer

Volume Editor

Igor Walukiewicz
LaBRI, Domaine Universitaire, bâtiment A30
351, cours de la Libération, 33405 Talence Cedex, France
E-mail: igw@labri.fr

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): F.3, F.4.2, F.1.1, D.3.3-4, D.2.1

ISSN 0302-9743
ISBN 3-540-21298-1 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10991442 06/3142 5 4 3 2 1 0

Foreword

ETAPS 2004 was the seventh instance of the European Joint Conferences on Theory and Practice of Software. ETAPS is an annual federated conference that was established in 1998 by combining a number of existing and new conferences. This year it comprised five conferences (FOSSACS, FASE, ESOP, CC, TACAS), 23 satellite workshops, 1 tutorial, and 7 invited lectures (not including those that are specific to the satellite events).

The events that comprise ETAPS address various aspects of the system development process, including specification, design, implementation, analysis and improvement. The languages, methodologies and tools that support these activities are all well within its scope. Different blends of theory and practice are represented, with an inclination towards theory with a practical motivation on the one hand and soundly based practice on the other. Many of the issues involved in software design apply to systems in general, including hardware systems, and the emphasis on software is not intended to be exclusive.

ETAPS is a loose confederation in which each event retains its own identity, with a separate program committee and independent proceedings. Its format is open-ended, allowing it to grow and evolve as time goes by. Contributed talks and system demonstrations are in synchronized parallel sessions, with invited lectures in plenary sessions. Two of the invited lectures are reserved for "unifying" talks on topics of interest to the whole range of ETAPS attendees. The aim of cramming all this activity into a single one-week meeting is to create a strong magnet for academic and industrial researchers working on topics within its scope, giving them the opportunity to learn about research in related areas, and thereby to foster new and existing links between work in areas that were formerly addressed in separate meetings.

ETAPS 2004 was organized by the LSI Department of the Catalonia Technical University (UPC), in cooperation with:

European Association for Theoretical Computer Science (EATCS)
European Association for Programming Languages and Systems (EAPLS)
European Association of Software Science and Technology (EASST)
ACM SIGACT, SIGSOFT and SIGPLAN

The organizing team comprised

Jordi Cortadella (Satellite Events), Nikos Mylonakis, Robert Nieuwenhuis, Fernando Orejas (Chair), Edelmira Pasarella, Sonia Perez, Elvira Pino, Albert Rubio

and had the assistance of TILESA OPC.
ETAPS 2004 received generous sponsorship from:

UPC, Spanish Ministry of Science and Technology (MCYT), Catalan Department for Universities, Research and Information Society (DURSI), IBM, Intel.

Overall planning for ETAPS conferences is the responsibility of its Steering Committee, whose current membership is:

Ratislav Bodik (Berkeley), Maura Cerioli (Genoa), Evelyn Duesterwald (IBM, Yorktown Heights), Hartmut Ehrig (Berlin), José Fiadeiro (Leicester), Marie-Claude Gaudel (Paris), Andy Gordon (Microsoft Research, Cambridge), Roberto Gorrieri (Bologna), Nicolas Halbwachs (Grenoble), Görel Hedin (Lund), Kurt Jensen (Aarhus), Paul Klint (Amsterdam), Tiziana Margaria (Dortmund), Ugo Montanari (Pisa), Hanne Riis Nielson (Copenhagen), Fernando Orejas (Barcelona), Mauro Pezzè (Milan), Andreas Podelski (Saarbrücken), Mooly Sagiv (Tel Aviv), Don Sannella (Edinburgh), Vladimiro Sassone (Sussex), David Schmidt (Kansas), Bernhard Steffen (Dortmund), Perdita Stevens (Edinburgh), Andrzej Tarlecki (Warsaw), Igor Walukiewicz (Bordeaux), Michel Wermelinger (Lisbon)

I would like to express my sincere gratitude to all of these people and organizations, the program committee chairs and PC members of the ETAPS conferences, the organizers of the satellite events, the speakers themselves, and finally Springer-Verlag for agreeing to publish the ETAPS proceedings. This year, the number of submissions approached 600, making acceptance rates fall to 25%. I congratulate the authors who made it into the final program! I hope that all the other authors still found a way of participating in this exciting event and I hope you will continue submitting.

In 2005, ETAPS will be organized by Don Sannella in Edinburgh. You will be welcomed by another "local": my successor as ETAPS Steering Committee Chair – Perdita Stevens. My wish is that she will enjoy coordinating the next three editions of ETAPS as much as I have. It is not an easy job, in spite of what Don assured me when I succeeded him! But it is definitely a very rewarding one. One cannot help but feel proud of seeing submission and participation records being broken one year after the other, and that the technical program reached the levels of quality that we have been witnessing. At the same time, interacting with the organizers has been a particularly rich experience. Having organized the very first edition of ETAPS in Lisbon in 1998, I knew what they were going through, and I can tell you that each of them put his/her heart, soul, and an incredible amount of effort into the organization. The result, as we all know, was brilliant on all counts! Therefore, my last words are to thank Susanne Graf (2002), Andrzej Tarlecki and Paweł Urzyczyn (2003), and Fernando Orejas (2004) for the privilege of having worked with them.

Leicester, January 2004

José Luiz Fiadeiro
ETAPS Steering Committee Chair

Preface

This volume contains the proceedings of the international conference *Foundations of Software Science and Computation Structures* (FOSSACS 2004), held in Barcelona, Spain, 30 March–2 April, 2004. FOSSACS is an event of the *Joint Conferences on Theory and Practice of Software* (ETAPS). The previous six FOSSACS conferences took place in Lisbon (1998), Amsterdam (1999), Berlin (2000), Genoa (2001), Grenoble (2002) and Warsaw (2003).

FOSSACS presents original papers on foundational research with clear significance to software science. The Program Committee invited papers on theories and methods to support the analysis, integration, synthesis, transformation, and verification of programs and software systems. In particular, we have identified the following topics: algebraic models; automata and language theory; behavioral equivalences; categorical models; computation processes over discrete and continuous data; infinite state systems; computation structures; logics of programs; modal, spatial, and temporal logics; models of concurrent, reactive, distributed, and mobile systems; process algebras and calculi; semantics of programming languages; software specification and refinement; type systems and type theory.

FOSSACS 2004 attracted over 130 submissions from which the program committee selected 34, the maximum that could fit into the available time. Unfortunately many good papers had to be turned away. This proceedings contains additionally two invited contributions: by the FOSSACS 2004 invited speaker Hubert Comon-Lundh, and by the ETAPS 2004 unifying speaker Robin Milner.

I thank all the authors for submitting their papers to FOSSACS. I am grateful to the reviewers who contributed nearly 400 informed and detailed reports. I sincerely thank the members of the Program Committee for very active participation in the electronic meeting and for coping with the additional challenges arising from the substantial increase in the number of submissions.

To administer the submission and evaluation process, we relied on a fine Web-based tool provided by METAFrame Technologies, Dortmund; thanks to Martin Karusseit and Tiziana Margaria of METAFrame for their timely support. Finally, thanks are due to the ETAPS 2004 Organizing Committee chaired by Fernando Orejas and to the ETAPS Steering Committee chaired by José Luiz Fiadeiro for their efficient coordination of all the activities leading up to FOSSACS 2004.

Bordeaux, January 2004 Igor Walukiewicz

Program Committee

Parosh Aziz Abdulla (Sweden)
Roberto Di Cosmo (France)
Anuj Dawar (UK)
Paul Gastin (France)
Roberto Gorrieri (Italy)
Andrew D. Gordon (UK)
Dietrich Kuske (Germany)
Ugo Montanari (Italy)
Mogens Nielsen (Denmark)
Vincent van Oostrom (Netherlands)
Jens Palsberg (USA)
Alberto Rubio (Spain)
Davide Sangiorgi (Italy)
Vladimiro Sassone (UK)
Philippe Schnoebelen (France)
Helmut Seidl (Germany)
Andrzej Tarlecki (Poland)
Thomas Wilke (Germany)
Igor Walukiewicz (France, Chair)

Referees

M. Abadi
L. Aceto
K. Aehlig
A. Aldini
E. Asarin
A. Atserias
C. Baier
V. Balat
M. Baldamus
P. Baldan
J. Beauquier
M. Bednarczyk
N. Benton
S. Berardi
R. Berghammer
J. Berstel
D. Berwanger
L. Birkedal
S. Bloom
L. Boasson
B. Bollig
M. Boreale
A. Borzyszkowski
T. Borzyszkowski
A. Bouajjani
A.-J. Bouquet
P. Bouyer
M. Bravetti
X. Briand
F. van Breugel
R. Bruni
M. Bugliesi
M. Buscemi
N. Busi
T. Cachat
L. Caires
C. Calcagno
M. Carbone
P. Caspi
P. Catuscia
D. Caucal
C. Choffrut
J. Chroboczeck
P. Chrząstowski-Wachtel
M. Clerbout
C.S. Coen
A. Compagnoni
M. Coppo
A. Corradini
F. Corradini
J. Cortadella
V. Cortier
J.-M. Couvreur
S. Crafa
U. Dal Lago
O. Danvy
A. Datta
P. Degano
D. Delahaye
C. Delporte
S. Demri
J. Desharnais
P. Di Gianantonio
A. Di Pierro
L. Durante
P. Dybjer
A. Edalat
H. Ehrig
M. Engel
T. Erhard
J. Ernits
K. Etessami
E. Fersman
A. Finkel
R. Focardi
C. Fournet
M. Gabbrielli
F. Gadducci
N. Gambino
P. Gastin
S. Gaubert
S. Gay
P. Gerhardy
D. Ghica
L. Giordano
G. Godoy
M. Gordon
J. Goubault-Larrecq
P. Habermehl
R. Harmer

R. Hasegawa
R. Heckel
R. Heckmann
C. Hermida
R. Hoellerer
P. Hoffman
P. Hunter
M. Huth
F. Jacquemard
P. Jancar
M. Jantzen
B. Jean
A. Jeffrey
B. Jonsson
A. Jung
M. Jurdzinski
Y. Jurski
M. Kacprzak
F. Klaedtke
B. Klin
B. Konikowska
P. Krcal
J.-L. Krivine
K. Krukow
R. Kuesters
N. Kumar
A. Kurz
A. Labella
G. Lagorio
U. Lago
Y. Lakhnech
C. Laneve
F. Laroussinie
S. Lasota
O. Laurent
R. Lazic
M. Lenisa
M. Leucker
F. Levi
C. Lhoussaine
S. Limet
C. Loeding
M. Loreti
G. Lowe
E. Lozes
G. Luettgen
B. Luttik
S. Maffeis
J. Mairesse
C. Marche
B. Marco
G. Marczynski
N. Markey
S. Martini
N. Marti-Oliet
R. Mayr
G. McCusker
P.-A. Mellies
C. Meyssonnier
N. Mezzetti
M. Miculan
J. Midtgaard
E. Moggi
F. Moller
S. Mooly
R. Morin
P. Mosses
N. Mueller
M. Mukund
A. Muscholl
M. Narciso
F. Nardelli
Z. Nemeth
F. Neven
P. Niebert
D. Niwiński
M. Nygaard
P. Oliva
L. Ong
F. Orejas
J. d'Orso
S. Orzan
E. Palmgren
P. Panangaden
L. Paolini
D. Pattinson
W. Pawłowski
C. Pech
A. Peron
M. Petreczky
A. Philippou
S. Pinchinat
A. Piperno
F. Pottier
J. Power
L. Prensa
R. Pugliese
A. Ramanathan
T. Regan
H. Reichel
D. Remy
E. Robinson
P. Rossmanith
M. Rusinowitch
C. Sacerdoti
P. Samarati
D. Sands
D. Sangorgi
K. Schmidt
P. Schobbens
L. Schröder
A. Schubert
C. Schuermann
N. Schweikardt
R. Segala
H. Seki
B. Sengupta
P. Shankar
M. Sighireanu
M. Simone
V. Simonet
A. Slissenko
P. Sobocinski
M. Soerensen
J. Srba
T. Streicher
G. Sutre
C. Talcott
P.S. Thiagarajan
P. Thiemann
S. Tini
A. Troina
E. Tuosto
I. Ulidowski
T. Uustalu

F. Valencia
G. Valiente
D. Varacca
K. Verma
B. Victor
J. Vouillon
F.-J. de Vries
P. Weil
H. Wiklicky
L. Wildman
L. Wischik
U. Wolter
M. Yamashita
W. Yi
S. Yu
N. Zappa
G. Zavattaro
M. Zeitoun
W. Zielonka

Lecture Notes in Computer Science 2987

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Lecture Notes in Computer Science

For information about Vols. 1–2868

please contact your bookseller or Springer-Verlag

Vol. 2996: V. Diekert, M. Habib (Eds.), STACS 2004. XVI, 658 pages. 2004.

Vol. 2993: R. Alur, G.J. Pappas (Eds.), Hybrid Systems: Computation and Control. XII, 674 pages. 2004.

Vol. 2992: E. Bertino, S. Christodoulakis, D. Plexousakis, V. Christophides, M. Koubarakis, K. Böhm, E. Ferrari (Eds.), Advances in Database Technology - EDBT 2004. XVIII, 877 pages. 2004.

Vol. 2991: R. Alt, A. Frommer, R.B. Kearfott, W. Luther (Eds.), Numerical Software with Result Verification. X, 315 pages. 2004.

Vol. 2987: I. Walukiewicz (Ed.), Foundations of Software Science and Computation Structures. XIII, 529 pages. 2004.

Vol. 2985: E. Duesterwald (Ed.), Compiler Construction. X, 313 pages. 2004.

Vol. 2983: S. Istrail, M. Waterman, A. Clark (Eds.), Computational Methods for SNPs and Haplotype Inference. IX, 153 pages. 2004. (Subseries LNBI).

Vol. 2982: N. Wakamiya, M. Solarski, J. Sterbenz (Eds.), Active Networks. XI, 308 pages. 2004.

Vol. 2981: C. Müller-Schloer, T. Ungerer, B. Bauer (Eds.), Organic and Pervasive Computing – ARCS 2004. XI, 339 pages. 2004.

Vol. 2980: A. Blackwell, K. Marriott, A. Shimojima (Eds.), Diagrammatic Representation and Inference. XV, 448 pages. 2004. (Subseries LNAI).

Vol. 2978: R. Groz, R.M. Hierons (Eds.), Testing of Communicating Systems. XII, 225 pages. 2004.

Vol. 2976: M. Farach-Colton (Ed.), LATIN 2004: Theoretical Informatics. XV, 626 pages. 2004.

Vol. 2973: Y. Lee, J. Li, K.-Y. Whang, D. Lee (Eds.), Database Systems for Advanced Applications. XXIV, 925 pages. 2004.

Vol. 2970: F. Fernández Rivera, M. Bubak, A. Gómez Tato, R. Doallo (Eds.), Grid Computing. XI, 328 pages. 2004.

Vol. 2964: T. Okamoto (Ed.), Topics in Cryptology – CT-RSA 2004. XI, 387 pages. 2004.

Vol. 2963: R. Sharp, Higher Level Hardware Synthesis. XVI, 195 pages. 2004.

Vol. 2962: S. Bistarelli, Semirings for Soft Constraint Solving and Programming. XII, 279 pages. 2004.

Vol. 2961: P. Eklund (Ed.), Concept Lattices. IX, 411 pages. 2004. (Subseries LNAI).

Vol. 2960: P.D. Mosses, CASL Reference Manual. XVII, 528 pages. 2004.

Vol. 2958: L. Rauchwerger (Ed.), Languages and Compilers for Parallel Computing. XI, 556 pages. 2004.

Vol. 2957: P. Langendoerfer, M. Liu, I. Matta, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. XI, 307 pages. 2004.

Vol. 2954: F. Crestani, M. Dunlop, S. Mizzaro (Eds.), Mobile and Ubiquitous Information Access. X, 299 pages. 2004.

Vol. 2953: K. Konrad, Model Generation for Natural Language Interpretation and Analysis. XIII, 166 pages. 2004. (Subseries LNAI).

Vol. 2952: N. Guelfi, E. Astesiano, G. Reggio (Eds.), Scientific Engineering of Distributed Java Applications. X, 157 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2949: R. De Nicola, G. Ferrari, G. Meredith (Eds.), Coordination Models and Languages. X, 323 pages. 2004.

Vol. 2947: F. Bao, R. Deng, J. Zhou (Eds.), Public Key Cryptography – PKC 2004. XI, 455 pages. 2004.

Vol. 2946: R. Focardi, R. Gorrieri (Eds.), Foundations of Security Analysis and Design II. VII, 267 pages. 2004.

Vol. 2943: J. Chen, J. Reif (Eds.), DNA Computing. X, 225 pages. 2004.

Vol. 2941: M. Wirsing, A. Knapp, S. Balsamo (Eds.), Radical Innovations of Software and Systems Engineering in the Future. X, 359 pages. 2004.

Vol. 2940: C. Lucena, A. Garcia, A. Romanovsky, J. Castro, P.S. Alencar (Eds.), Software Engineering for Multi-Agent Systems II. XII, 279 pages. 2004.

Vol. 2939: T. Kalker, I.J. Cox, Y.M. Ro (Eds.), Digital Watermarking. XII, 602 pages. 2004.

Vol. 2937: B. Steffen, G. Levi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 325 pages. 2004.

Vol. 2934: G. Lindemann, D. Moldt, M. Paolucci (Eds.), Regulated Agent-Based Social Systems. X, 301 pages. 2004. (Subseries LNAI).

Vol. 2930: F. Winkler (Ed.), Automated Deduction in Geometry. VII, 231 pages. 2004. (Subseries LNAI).

Vol. 2926: L. van Elst, V. Dignum, A. Abecker (Eds.), Agent-Mediated Knowledge Management. XI, 428 pages. 2004. (Subseries LNAI).

Vol. 2923: V. Lifschitz, I. Niemelä (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 365 pages. 2004. (Subseries LNAI).

Vol. 2919: E. Giunchiglia, A. Tacchella (Eds.), Theory and Applications of Satisfiability Testing. XI, 530 pages. 2004.

Vol. 2917: E. Quintarelli, Model-Checking Based Data Retrieval. XVI, 134 pages. 2004.

Vol. 2916: C. Palamidessi (Ed.), Logic Programming. XII, 520 pages. 2003.

Vol. 2915: A. Camurri, G. Volpe (Eds.), Gesture-Based Communication in Human-Computer Interaction. XIII, 558 pages. 2004. (Subseries LNAI).

Vol. 2914: P.K. Pandya, J. Radhakrishnan (Eds.), FST TCS 2003: Foundations of Software Technology and Theoretical Computer Science. XIII, 446 pages. 2003.

Vol. 2913: T.M. Pinkston, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2003. XX, 512 pages. 2003. (Subseries LNAI).

Vol. 2911: T.M.T. Sembok, H.B. Zaman, H. Chen, S.R. Urs, S.H. Myaeng (Eds.), Digital Libraries: Technology and Management of Indigenous Knowledge for Global Access. XX, 703 pages. 2003.

Vol. 2910: M.E. Orlowska, S. Weerawarana, M.M.P. Papazoglou, J. Yang (Eds.), Service-Oriented Computing - ICSOC 2003. XIV, 576 pages. 2003.

Vol. 2909: K. Jansen, R. Solis-Oba (Eds.), Approximation and Online Algorithms. VIII, 269 pages. 2004.

Vol. 2909: R. Solis-Oba, K. Jansen (Eds.), Approximation and Online Algorithms. VIII, 269 pages. 2004.

Vol. 2908: K. Chae, M. Yung (Eds.), Information Security Applications. XII, 506 pages. 2004.

Vol. 2907: I. Lirkov, S. Margenov, J. Wasniewski, P. Yalamov (Eds.), Large-Scale Scientific Computing. XI, 490 pages. 2004.

Vol. 2906: T. Ibaraki, N. Katoh, H. Ono (Eds.), Algorithms and Computation. XVII, 748 pages. 2003.

Vol. 2905: A. Sanfeliu, J. Ruiz-Shulcloper (Eds.), Progress in Pattern Recognition, Speech and Image Analysis. XVII, 693 pages. 2003.

Vol. 2904: T. Johansson, S. Maitra (Eds.), Progress in Cryptology - INDOCRYPT 2003. XI, 431 pages. 2003.

Vol. 2903: T.D. Gedeon, L.C.C. Fung (Eds.), AI 2003: Advances in Artificial Intelligence. XVI, 1075 pages. 2003. (Subseries LNAI).

Vol. 2902: F.M. Pires, S.P. Abreu (Eds.), Progress in Artificial Intelligence. XV, 504 pages. 2003. (Subseries LNAI).

Vol. 2901: F. Bry, N. Henze, J. Ma luszyński (Eds.), Principles and Practice of Semantic Web Reasoning. X, 209 pages. 2003.

Vol. 2900: M. Bidoit, P.D. Mosses (Eds.), Casl User Manual. XIII, 240 pages. 2004.

Vol. 2899: G. Ventre, R. Canonico (Eds.), Interactive Multimedia on Next Generation Networks. XIV, 420 pages. 2003.

Vol. 2898: K.G. Paterson (Ed.), Cryptography and Coding. IX, 385 pages. 2003.

Vol. 2897: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. XI, 240 pages. 2003.

Vol. 2896: V.A. Saraswat (Ed.), Advances in Computing Science – ASIAN 2003. VIII, 305 pages. 2003.

Vol. 2895: A. Ohori (Ed.), Programming Languages and Systems. XIII, 427 pages. 2003.

Vol. 2894: C.S. Laih (Ed.), Advances in Cryptology - ASIACRYPT 2003. XIII, 543 pages. 2003.

Vol. 2893: J.-B. Stefani, I. Demeure, D. Hagimont (Eds.), Distributed Applications and Interoperable Systems. XIII, 311 pages. 2003.

Vol. 2892: F. Dau, The Logic System of Concept Graphs with Negation. XI, 213 pages. 2003. (Subseries LNAI).

Vol. 2891: J. Lee, M. Barley (Eds.), Intelligent Agents and Multi-Agent Systems. X, 215 pages. 2003. (Subseries LNAI).

Vol. 2890: M. Broy, A.V. Zamulin (Eds.), Perspectives of System Informatics. XV, 572 pages. 2003.

Vol. 2889: R. Meersman, Z. Tari (Eds.), On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops. XIX, 1071 pages. 2003.

Vol. 2888: R. Meersman, Z. Tari, D.C. Schmidt (Eds.), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. XXI, 1546 pages. 2003.

Vol. 2887: T. Johansson (Ed.), Fast Software Encryption. IX, 397 pages. 2003.

Vol. 2886: I. Nyström, G. Sanniti di Baja, S. Svensson (Eds.), Discrete Geometry for Computer Imagery. XII, 556 pages. 2003.

Vol. 2885: J.S. Dong, J. Woodcock (Eds.), Formal Methods and Software Engineering. XI, 683 pages. 2003.

Vol. 2884: E. Najm, U. Nestmann, P. Stevens (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 293 pages. 2003.

Vol. 2883: J. Schaeffer, M. Müller, Y. Björnsson (Eds.), Computers and Games. XI, 431 pages. 2003.

Vol. 2882: D. Veit, Matchmaking in Electronic Markets. XV, 180 pages. 2003. (Subseries LNAI).

Vol. 2881: E. Horlait, T. Magedanz, R.H. Glitho (Eds.), Mobile Agents for Telecommunication Applications. IX, 297 pages. 2003.

Vol. 2880: H.L. Bodlaender (Ed.), Graph-Theoretic Concepts in Computer Science. XI, 386 pages. 2003.

Vol. 2879: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. XXXIV, 1003 pages. 2003.

Vol. 2878: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. XXXIII, 819 pages. 2003.

Vol. 2877: T. Böhme, G. Heyer, H. Unger (Eds.), Innovative Internet Community Systems. VIII, 263 pages. 2003.

Vol. 2876: M. Schroeder, G. Wagner (Eds.), Rules and Rule Markup Languages for the Semantic Web. VII, 173 pages. 2003.

Vol. 2875: E. Aarts, R. Collier, E.v. Loenen, B.d. Ruyter (Eds.), Ambient Intelligence. XI, 432 pages. 2003.

Vol. 2874: C. Priami (Ed.), Global Computing. XIX, 255 pages. 2003.

Vol. 2871: N. Zhong, Z.W. Raś, S. Tsumoto, E. Suzuki (Eds.), Foundations of Intelligent Systems. XV, 697 pages. 2003. (Subseries LNAI).

Vol. 2870: D. Fensel, K.P. Sycara, J. Mylopoulos (Eds.), The Semantic Web - ISWC 2003. XV, 931 pages. 2003.

Vol. 2869: A. Yazici, C. Şener (Eds.), Computer and Information Sciences - ISCIS 2003. XIX, 1110 pages. 2003.

Table of Contents

Invited Contributions

Contributed Papers

Intruder Theories (Ongoing Work)

Hubert Comon-Lundh*

Laboratoire Spécification et Vérification, CNRS
Ecole Normale Supérieure de Cachan,
comon@lsv.ens-cachan.fr

1 Context

The specification of security protocols usually comes in two parts:

- A finite number of processes called *roles*, each of which is parametrized by agent identities and consists of a sequence of name generation, the *nonces* and a finite sequence of rules $u \Rightarrow v$, which should be read as "upon receiving a message matching u, send the corresponding message v."
- A description of intruder capabilities, sometimes given as a proof system, which we call hereafter the *offline intruder theory*.

The roles can be replicated and instanciated by agent names any number of times. Each such instance is called a *session*. The roles and the offline intruder theory define a transition system whose states are, for each agent name a local state and a set of messages called the *intruder knowledge*. The peculiarity of security protocols is the synchronization mechanism: the only effect of sending a message m is to increase the intruder knowledge with m, while any message that can be forged, i.e. deduced, by the intruder using his knowledge and the offline theory can be received. This models the fact that the intruder controls the public network: he can intercept messages, forge new messages and send them through the network. In addition, dishonest (or compromised) agents communicate all their private data, increasing the intruder knowledge.

As far as confidentiality is concerned, there is an *attack* on the security protocol if there is a reachable state in which the intruder knowledge contains a message which is supposed to remain a secret shared by honest agents.

One of the most well-known offline intruder theory is now called the *Dolev-Yao model*, and relies on the *perfect cryptography assumption*, which roughly states that nothing can be learned on a plain text from its encrypted version, without knowing the decryption key. The verification of such protocols is undecidable in this model. This remains undecidable when there is no name generation (see e.g. [3]) or when the size of messages is bounded [6]. It becomes decidable (and co-NP-complete) when the number of sessions is bounded [10].

* This work is partly supported by the RNTL project PROUVÉ and the ACI Rossignol

I. Walukiewicz (Ed.): FOSSACS 2004, LNCS 2987, pp. 1–4, 2004.