LNCS 2240

Gian Pietro Picco (Ed.)

# Mobile Agents

5th International Conference, MA 2001
Atlanta, GA, USA, December 2001
Proceedings

Springer

Gian Pietro Picco (Ed.)

# Mobile Agents

5th International Conference, MA 2001
Atlanta, GA, USA, December 2-4, 2001
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Gian Pietro Picco
Politecnico di Milano, Dipartimento di Elettronica e Informazione
Piazza Leonardo da Vinci 32, 20133 Milano, Italy
E-mail: picco@elet.polimi.it

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Mobile agents : 5th international conference ; proceedings / MA 2000, Atlanta, GA, USA, December 2 - 4, 2001. Gian Pietro Picco (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2240)
ISBN 3-540-42952-2

CR Subject Classification (1998): C.2.4, D.1.3, D.2, D.4.4-7, I.2.11, K.6.5

ISSN 0302-9743
ISBN 3-540-42952-2 Springer-Verlag Berlin Heidelberg New York



Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de


Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna
Printed on acid-free paper SPIN: 10845850 06/3142 5 4 3 2 1 0

# Preface

Recent years have witnessed the appearance of new paradigms for designing distributed applications where the application components can be relocated dynamically across the hosts of the network. This form of *code mobility* lays the foundation for a new generation of technologies, architectures, models, and applications in which the location at which the code is executed comes under the control of the designer, rather than simply being a configuration accident.

Among the various flavors of mobile code, the *mobile agent* paradigm has become particularly popular. Mobile agents are programs able to determine autonomously their own migration to a different host, and still retain their code and state (or at least a portion thereof). Thus, distributed computations do not necessarily unfold as a sequence of requests and replies between clients and remote servers, rather they encompass one or more visits of one or more mobile agents to the nodes involved.

Mobile code and mobile agents hold the potential to shape the next generation of technologies and models for distributed computation. The first steps of this process are already evident today: Web applets provide a case for the least sophisticated form of mobile code, Java-based distributed middleware makes increasing use of mobile code, and the first commercial applications using mobile agents are starting to appear.

This volume contains the proceedings of the Fifth International Conference on Mobile Agents (MA 2001). MA 2001 took place in Atlanta, Georgia, USA, at the Georgia Center for Advanced Telecommunications Technology (GCATT), on December 2–4, 2001. The ambitious goal of MA 2001 was to gather researchers and practitioners from all over the world and shed some light on the open issues related to the exciting research topic of code mobility.

The first conference in this series was held in 1997 in Berlin, and since then it has been, by number of attendees and by quality and breadth of the research disseminated, among the top events for the community of researchers and practitioners interested in mobile code and mobile agents. The previous two conferences were held together with the International Symposium on Agent Systems and Applications (ASA) as joint ASA/MA events that aimed at gathering researchers interested in all the flavors of agent systems, e.g., including also intelligent and non-mobile agents. Although these joint events were very successful, MA 2001 was presented as a stand-alone event, entirely focused on the original target of mobile code and mobile agents. Our goal with this and future events is to strengthen the MA conference as the international venue at which the best and latest results in the topics of mobile code and mobile agents are disseminated and discussed.

The conference received 75 submissions from authors all over the world. The CyberChair system (`www.cyberchair.org`) greatly simplified the submission and review process. The Program Committee, composed of 20 of the most distinguished researchers in code mobility, reviewed all of the papers carefully. Each paper was assigned to at least three reviewers – four in the case of papers authored by Program Committee members. Reviewers were asked to declare in advance potential conflicts of interest, to allow a proper assignment of papers and ensure fair reviews. Moreover, this information was used at the Program Committee meeting, that took place in Milan at the end of May, where reviewers with a conflict of interest on a paper were asked to leave the room during the related discussion. After a full-day meeting, the Program Committee selected the 18 papers included in the technical program.

In addition to these papers, we were honored that two distinguished experts accepted our invitation to give keynote presentations. Fred Schneider (Cornell University, USA) shared his views about the past, present, and future of mobile agent research, while Aleta Ricciardi (Valaran Corporation, USA) reported on her first-hand experience in applying code mobility within a real-world industrial context. The program was completed by a "Posters and Research Demos" session, and by four tutorials by leading experts in the field.

Conferences are the result of the concerted efforts of several people. First of all, I would like to express, personally and on behalf of the rest of the Organizing Committee, my appreciation to the authors of the submitted papers, and sincerely thank the members of the Program Committee and the external reviewers for their fundamental contribution to ensuring the quality of this conference. I would also like to thank the General Chair of MA 2001, David Kotz, and the rest of the Organizing Committee for their work in making this event a success. Finally, I would like to acknowledge and thank the IEEE Technical Committee on the Internet and the IEEE Computer Society for sponsoring the event, and Nokia and Georgia Tech College of Engineering for supporting it.

September 2001 Gian Pietro Picco

# Organization

The Fifth International Conference on Mobile Agents (MA 2001) took place at the Georgia Center for Advanced Telecommunications Technology (GCATT) in Atlanta, Georgia, USA, on December 2–4, 2001.

GEORGIA CENTER FOR ADVANCED TELECOMMUNICATIONS TECHNOLOGY

## Executive Committee

| | |
|---|---|
| General Chair: | David Kotz (Dartmouth College, USA) |
| Program Chair: | Gian Pietro Picco (Politecnico di Milano, Italy) |
| Tutorials: | David Wong (Mitsubishi Electric Research Labs, USA) |
| Advertizing: | Marco Cremonini (Dartmouth College, USA) |
| Registration: | Lori A. Terino (Dartmouth College, USA) |
| Local Arrangements: | Ashraf Saad (Georgia Institute of Technology, USA) |
| Treasurer: | Robert S. Gray (Dartmouth College, USA) |
| Webmaster: | Guanling Chen (Dartmouth College, USA) |

## Program Committee

| | |
|---|---|
| Israel Ben-Shaul | Israel Institute of Technology, and Versedge Technologies, Israel |
| Lubomir F. Bic | University of California Irvine, USA |
| Luca Cardelli | Microsoft Research, UK |
| Rocco De Nicola | Università di Firenze, Italy |
| Andrzej Duda | LSR-IMAG, France |
| Robert S. Gray | Dartmouth College, USA |
| Shinichi Honiden | National Institute of Informatics, Japan |
| Günter Karjoth | IBM Zurich Research Laboratory, Switzerland |
| Dag Johansen | University of Tromsø, Norway |
| Danny B. Lange | Vocomo Software, USA |
| Thomas Magedanz | IKV++, Germany |
| Keith Marzullo | University of California San Diego, USA |
| José Meseguer | SRI International, USA |
| Amy L. Murphy | University of Rochester, USA |
| Kurt Rothermel | Universität Stuttgart, Germany |
| Niranjan Suri | University of West Florida, USA |
| Anand Tripathi | University of Minnesota, USA |
| Christian Tschudin | Uppsala University, Sweden |
| Giovanni Vigna | University of California Santa Barbara, USA |
| Franco Zambonelli | Università di Modena e Reggio Emilia, Italy |

## Steering Committee

| | |
|---|---|
| Robert S. Gray | Dartmouth College, USA |
| David Kotz | Dartmouth College, USA |
| Danny B. Lange | Vocomo Software, USA |
| Friedemann Mattern | ETH Zurich, Switzerland |
| Gian Pietro Picco | Politecnico di Milano, Italy |
| Kurt Rothermel | Universität Stuttgart, Germany |

## Sponsoring Organizations

MA 2001 was sponsored by the IEEE Technical Committee on the Internet and the IEEE Computer Society, and supported by Nokia and the Georgia Tech College of Engineering.

## Referees

Miki Abu
Yariv Aridor
Christian Becker
Lorenzo Bettini
Bozhena Bidyuk
Michele Boreale
Cora Burger
Michael Dillencourt
Jesus Favela
Eugene Gendleman
Yoad Gidron
Daniel Hagimont
Nguyen Hoa Binh
Fritz Hohl
Kjetil Jacobsen
Neeran Karnik
Hairong Kuang
Michele Loreti
Koji Noguchi
Lei Pan
Stefan Pleisch
Rosario Pugliese
Franck Rousseau
Ant Rowstron
Markus Straßer
Wolfgang Theilmann
Yaron Weinsberg

# Lecture Notes in Computer Science

For information about Vols. 1–2151
please contact your bookseller or Springer-Verlag

Vol. 2152: R.J. Boulton, P.B. Jackson (Eds.), Theore Proving in Higher Order Logics. Proceedings, 2001. X,395 pages. 2001.

Vol. 2153: A.L. Buchsbaum, J. Snoeyink (Eds.), Algorithm Engineering and Experimentation. Proceedings, 2001. VIII, 231 pages. 2001.

Vol. 2154: K.G. Larsen, M. Nielsen (Eds.), CONCUR 2001 – Concurrency Theory. Proceedings, 2001. XI, 583 pages. 2001.

Vol. 2155: H. Bunt, R.-J. Beun (Eds.), Cooperative Multimodal Communication. Proceedings, 1998. VIII, 251 pages. 2001. (Subseries LNAI).

Vol. 2156: M.I. Smirnov, J. Crowcroft, J. Roberts, F.Boavida (Eds.), Quality of Future Internet Services. Proceedings, 2001. XI, 333 pages. 2001.

Vol. 2157: C. Rouveirol, M. Sebag (Eds.), Inductive Logic Programming. Proceedings, 2001. X, 261 pages. 2001. (Subseries LNAI).

Vol. 2158: D. Shepherd, J. Finney, L. Mathy, N. Race (Eds.), Interactive Distributed Multimedia Systems. Proceedings, 2001. XIII, 258 pages. 2001.

Vol. 2159: J. Kelemen, P. Sosík (Eds.), Advances in Artificial Life. Proceedings, 2001. XIX, 724 pages. 2001. (Subseries LNAI).

Vol. 2161: F. Meyer auf der Heide (Ed.), Algorithms – ESA 2001. Proceedings, 2001. XII, 538 pages. 2001.

Vol. 2162: Ç. K. Koç, D. Naccache, C. Paar (Eds.), Cryptographic Hardware and Embedded Systems – CHES 2001. Proceedings, 2001. XIV, 411 pages. 2001.

Vol. 2163: P. Constantopoulos, I.T. Sølvberg (Eds.), Research and Advanced Technology for Digital Libraries. Proceedings, 2001. XII, 462 pages. 2001.

Vol. 2164: S. Pierre, R. Glitho (Eds.), Mobile Agents for Telecommunication Applications. Proceedings, 2001. XI, 292 pages. 2001.

Vol. 2165: L. de Alfaro, S. Gilmore (Eds.), Process Algebra and Probabilistic Methods. Proceedings, 2001. XII, 217 pages. 2001.

Vol. 2166: V. Matoušek, P. Mautner, R. Mouček, K. Taušer (Eds.), Text, Speech and Dialogue. Proceedings, 2001. XIII, 452 pages. 2001. (Subseries LNAI).

Vol. 2167: L. De Raedt, P. Flach (Eds.), Machine Learning: ECML 2001. Proceedings, 2001. XVII, 618 pages. 2001. (Subseries LNAI).

Vol. 2168: L. De Raedt, A. Siebes (Eds.), Principles of Data Mining and Knowledge Discovery. Proceedings, 2001. XVII, 510 pages. 2001. (Subseries LNAI).

Vol. 2169: M. Jaedicke, New Concepts for Parallel Object-Relational Query Processing. XI, 161 pages. 2001.

Vol. 2170: S. Palazzo (Ed.), Evolutionary Trends of the Internet. Proceedings, 2001. XIII, 722 pages. 2001.

Vol. 2171: R. Focardi, R. Gorrieri (Eds.), Foundations of Security Analysis and Design. VII, 397 pages. 2001.

Vol. 2172: C. Batini, F. Giunchiglia, P. Giorgini, M. Mecella (Eds.), Cooperative Information Systems. Proceedings, 2001. XI, 450 pages. 2001.

Vol. 2173: T. Eiter, W. Faber, M. Truszczynski (Eds.), Logic Programming and Nonmonotonic Reasoning. Proceedings, 2001. XI, 444 pages. 2001. (Subseries LNAI).

Vol. 2174: F. Baader, G. Brewka, T. Eiter (Eds.), KI 2001: Advances in Artificial Intelligence. Proceedings, 2001. XIII, 471 pages. 2001. (Subseries LNAI).

Vol. 2175: F. Esposito (Ed.), AI*IA 2001: Advances in Artificial Intelligence. Proceedings, 2001. XII, 396 pages. 2001. (Subseries LNAI).

Vol. 2176: K.-D. Althoff, R.L. Feldmann, W. Müller (Eds.), Advances in Learning Software Organizations. Proceedings, 2001. XI, 241 pages. 2001.

Vol. 2177: G. Butler, S. Jarzabek (Eds.), Generative and Component-Based Software Engineering. Proceedings, 2001. X, 203 pages. 2001.

Vol. 2178: R. Moreno-Díaz, B. Buchberger, J.-L. Freire (Eds.), Computer Aided Systems Theory – EUROCAST 2001. Proceedings, 2001. XI, 670 pages. 2001.

Vol. 2180: J. Welch (Ed.), Distributed Computing. Proceedings, 2001. X, 343 pages. 2001.

Vol. 2181: C. Y. Westort (Ed.), Digital Earth Moving. Proceedings, 2001. XII, 117 pages. 2001.

Vol. 2182: M. Klusch, F. Zambonelli (Eds.), Cooperative Information Agents V. Proceedings, 2001. XII, 288 pages. 2001. (Subseries LNAI).

Vol. 2183: R. Kahle, P. Schroeder-Heister, R. Stärk (Eds.), Proof Theory in Computer Science. Proceedings, 2001. IX, 239 pages. 2001.

Vol. 2184: M. Tucci (Ed.), Multimedia Databases and Image Communication. Proceedings, 2001. X, 225 pages. 2001.

Vol. 2185: M. Gogolla, C. Kobryn (Eds.), «UML» 2001 – The Unified Modeling Language. Proceedings, 2001. XIV, 510 pages. 2001.

Vol. 2186: J. Bosch (Ed.), Generative and Component-Based Software Engineering. Proceedings, 2001. VIII, 177 pages. 2001.

Vol. 2187: U. Voges (Ed.), Computer Safety, Reliability and Security. Proceedings, 2001. XVI, 249 pages. 2001.

Vol. 2188: F. Bomarius, S. Komi-Sirviö (Eds.), Product Focused Software Process Improvement. Proceedings, 2001. XI, 382 pages. 2001.

Vol. 2189: F. Hoffmann, D.J. Hand, N. Adams, D. Fisher, G. Guimaraes (Eds.), Advances in Intelligent Data Analysis. Proceedings, 2001. XII, 384 pages. 2001.

Vol. 2190: A. de Antonio, R. Aylett, D. Ballin (Eds.), Intelligent Virtual Agents. Proceedings, 2001. VIII, 245 pages. 2001. (Subseries LNAI).

Vol. 2191: B. Radig, S. Florczyk (Eds.), Pattern Recognition. Proceedings, 2001. XVI, 452 pages. 2001.

Vol. 2192: A. Yonezawa, S. Matsuoka (Eds.), Metalevel Architectures and Separation of Crosscutting Concerns. Proceedings, 2001. XI, 283 pages. 2001.

Vol. 2193: F. Casati, D. Georgakopoulos, M.-C. Shan (Eds.), Technologies for E-Services. Proceedings, 2001. X, 213 pages. 2001.

Vol. 2194: A.K. Datta, T. Herman (Eds.), Self-Stabilizing Systems. Proceedings, 2001. VII, 229 pages. 2001.

Vol. 2195: H.-Y. Shum, M. Liao, S.-F. Chang (Eds.), Advances in Multimedia Information Processing – PCM 2001. Proceedings, 2001. XX, 1149 pages. 2001.

Vol. 2196: W. Taha (Ed.), Semantics, Applications, and Implementation of Program Generation. Proceedings, 2001. X, 219 pages. 2001.

Vol. 2197: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. Proceedings, 2001. XI, 213 pages. 2001.

Vol. 2198: N. Zhong, Y. Yao, J. Liu, S. Ohsuga (Eds.), Web Intelligence: Research and Development. Proceedings, 2001. XVI, 615 pages. 2001. (Subseries LNAI).

Vol. 2199: J. Crespo, V. Maojo, F. Martin (Eds.), Medical Data Analysis. Proceedings, 2001. X, 311 pages. 2001.

Vol. 2200: G.I. Davida, Y. Frankel (Eds.), Information Security. Proceedings, 2001. XIII, 554 pages. 2001.

Vol. 2201: G.D. Abowd, B. Brumitt, S. Shafer (Eds.), Ubicomp 2001: Ubiquitous Computing. Proceedings, 2001. XIII, 372 pages. 2001.

Vol. 2202: A. Restivo, S. Ronchi Della Rocca, L. Roversi (Eds.), Theoretical Computer Science. Proceedings, 2001. XI, 440 pages. 2001.

Vol. 2204: A. Brandstädt, V.B. Le (Eds.), Graph-Theoretic Concepts in Computer Science. Proceedings, 2001. X, 329 pages. 2001.

Vol. 2205: D.R. Montello (Ed.), Spatial Information Theory. Proceedings, 2001. XIV, 503 pages. 2001.

Vol. 2206: B. Reusch (Ed.), Computational Intelligence. Proceedings, 2001. XVII, 1003 pages. 2001.

Vol. 2207: I.W. Marshall, S. Nettles, N. Wakamiya (Eds.), Active Networks. Proceedings, 2001. IX, 165 pages. 2001.

Vol. 2208: W.J. Niessen, M.A. Viergever (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2001. Proceedings, 2001. XXXV, 1446 pages. 2001.

Vol. 2209: W. Jonker (Ed.), Databases in Telecommunications II. Proceedings, 2001. VII, 179 pages. 2001.

Vol. 2210: Y. Liu, K. Tanaka, M. Iwata, T. Higuchi, M. Yasunaga (Eds.), Evolvable Systems: From Biology to Hardware. Proceedings, 2001. XI, 341 pages. 2001.

Vol. 2211: T.A. Henzinger, C.M. Kirsch (Eds.), Embedded Software. Proceedings, 2001. IX, 504 pages. 2001.

Vol. 2212: W. Lee, L. Mé, A. Wespi (Eds.), Recent Advances in Intrusion Detection. Proceedings, 2001. X, 205 pages. 2001.

Vol. 2213: M.J. van Sinderen, L.J.M. Nieuwenhuis (Eds.), Protocols for Multimedia Systems. Proceedings, 2001. XII, 239 pages. 2001.

Vol. 2214: O. Boldt, H. Jürgensen (Eds.), Automata Implementation. Proceedings, 1999. VIII, 183 pages. 2001.

Vol. 2215: N. Kobayashi, B.C. Pierce (Eds.), Theoretical Aspects of Computer Software. Proceedings, 2001. XV, 561 pages. 2001.

Vol. 2216: E.S. Al-Shaer, G. Pacifici (Eds.), Management of Multimedia on the Internet. Proceedings, 2001. XIV, 373 pages. 2001.

Vol. 2217: T. Gomi (Ed.), Evolutionary Robotics. Proceedings, 2001. XI, 139 pages. 2001.

Vol. 2218: R. Guerraoui (Ed.), Middleware 2001. Proceedings, 2001. XIII, 395 pages. 2001.

Vol. 2220: C. Johnson (Ed.), Interactive Systems. Proceedings, 2001. XII, 219 pages. 2001.

Vol. 2221: D.G. Feitelson, L. Rudolph (Eds.), Job Scheduling Strategies for Parallel Processing. Proceedings, 2001. VII, 207 pages. 2001.

Vol. 2224: H.S. Kunii, S. Jajodia, A. Sølvberg (Eds.), Conceptual Modeling – ER 2001. Proceedings, 2001. XIX, 614 pages. 2001.

Vol. 2225: N. Abe, R. Khardon, T. Zeugmann (Eds.), Algorithmic Learning Theory. Proceedings, 2001. XI, 379 pages. 2001. (Subseries LNAI).

Vol. 2226: K.P. Jantke, A. Shinohara (Eds.), Discovery Science. Proceedings, 2001. XII, 494 pages. 2001. (Subseries LNAI).

Vol. 2227: S. Boztaş, I.E. Shparlinski (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proceedings, 2001. XII, 398 pages. 2001.

Vol. 2229: S. Qing, T. Okamoto, J. Zhou (Eds.), Information and Communications Security. Proceedings, 2001. XIV, 504 pages. 2001.

Vol. 2230: T. Katila, I.E. Magnin, P. Clarysse, J. Montagnat, J. Nenonen (Eds.), Functional Imaging and Modeling of the Heart. Proceedings, 2001. XI, 158 pages. 2001.

Vol. 2232: L. Fiege, G. Mühl, U. Wilhelm (Eds.), Electronic Commerce. Proceedings, 2001. X, 233 pages. 2001.

Vol. 2233: J. Crowcroft, M. Hofmann (Eds.), Networked Group Communication. Proceedings, 2001. X, 205 pages. 2001.

Vol. 2234: L. Pacholski, P. Ružička (Eds.), SOFSEM 2001: Theory and Practice of Informatics. Proceedings, 2001. XI, 347 pages. 2001.

Vol. 2237: P. Codognet (Ed.), Logic Programming. Proceedings, 2001. XI, 365 pages. 2001.

Vol. 2239: T. Walsh (Ed.), Principles and Practice of Constraint Programming – CP 2001. Proceedings, 2001. XIV, 788 pages. 2001.

Vol. 2240: G.P. Picco (Ed.), Mobile Agents. Proceedings, 2001. XIII, 277 pages. 2001.

Vol. 2241: M. Jünger, D. Naddef (Eds.), Computational Combinatorial Optimization. IX, 305 pages. 2001.

Vol. 2242: C.A. Lee (Ed.), Grid Computing – GRID 2001. Proceedings, 2001. XII, 185 pages. 2001.

Vol. 2190: A. de Antonio, R. Aylett, D. Ballin (Eds.), Intelligent Virtual Agents. Proceedings, 2001. VIII, 245 pages. 2001. (Subseries LNAI).

Vol. 2191: B. Radig, S. Florczyk (Eds.), Pattern Recognition. Proceedings, 2001. XVI, 452 pages. 2001.

Vol. 2192: A. Yonezawa, S. Matsuoka (Eds.), Metalevel Architectures and Separation of Crosscutting Concerns. Proceedings, 2001. XI, 283 pages. 2001.

Vol. 2193: F. Casati, D. Georgakopoulos, M.-C. Shan (Eds.), Technologies for E-Services. Proceedings, 2001. X, 213 pages. 2001.

Vol. 2194: A.K. Datta, T. Herman (Eds.), Self-Stabilizing Systems. Proceedings, 2001. VII, 229 pages. 2001.

Vol. 2195: H.-Y. Shum, M. Liao, S.-F. Chang (Eds.), Advances in Multimedia Information Processing – PCM 2001. Proceedings, 2001. XX, 1149 pages. 2001.

Vol. 2196: W. Taha (Ed.), Semantics, Applications, and Implementation of Program Generation. Proceedings, 2001. X, 219 pages. 2001.

Vol. 2197: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. Proceedings, 2001. XI, 213 pages. 2001.

Vol. 2198: N. Zhong, Y. Yao, J. Liu, S. Ohsuga (Eds.), Web Intelligence: Research and Development. Proceedings, 2001. XVI, 615 pages. 2001. (Subseries LNAI).

Vol. 2199: J. Crespo, V. Maojo, F. Martin (Eds.), Medical Data Analysis. Proceedings, 2001. X, 311 pages. 2001.

Vol. 2200: G.I. Davida, Y. Frankel (Eds.), Information Security. Proceedings, 2001. XIII, 554 pages. 2001.

Vol. 2201: G.D. Abowd, B. Brumitt, S. Shafer (Eds.), Ubicomp 2001: Ubiquitous Computing. Proceedings, 2001. XIII, 372 pages. 2001.

Vol. 2202: A. Restivo, S. Ronchi Della Rocca, L. Roversi (Eds.), Theoretical Computer Science. Proceedings, 2001. XI, 440 pages. 2001.

Vol. 2204: A. Brandstädt, V.B. Le (Eds.), Graph-Theoretic Concepts in Computer Science. Proceedings, 2001. X, 329 pages. 2001.

Vol. 2205: D.R. Montello (Ed.), Spatial Information Theory. Proceedings, 2001. XIV, 503 pages. 2001.

Vol. 2206: B. Reusch (Ed.), Computational Intelligence. Proceedings, 2001. XVII, 1003 pages. 2001.

Vol. 2207: I.W. Marshall, S. Nettles, N. Wakamiya (Eds.), Active Networks. Proceedings, 2001. IX, 165 pages. 2001.

Vol. 2208: W.J. Niessen, M.A. Viergever (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2001. Proceedings, 2001. XXXV, 1446 pages. 2001.

Vol. 2209: W. Jonker (Ed.), Databases in Telecommunications II. Proceedings, 2001. VII, 179 pages. 2001.

Vol. 2210: Y. Liu, K. Tanaka, M. Iwata, T. Higuchi, M. Yasunaga (Eds.), Evolvable Systems: From Biology to Hardware. Proceedings, 2001. XI, 341 pages. 2001.

Vol. 2211: T.A. Henzinger, C.M. Kirsch (Eds.), Embedded Software. Proceedings, 2001. IX, 504 pages. 2001.

Vol. 2212: W. Lee, L. Mé, A. Wespi (Eds.), Recent Advances in Intrusion Detection. Proceedings, 2001. X, 205 pages. 2001.

Vol. 2213: M.J. van Sinderen, L.J.M. Nieuwenhuis (Eds.), Protocols for Multimedia Systems. Proceedings, 2001. XII, 239 pages. 2001.

Vol. 2214: O. Boldt, H. Jürgensen (Eds.), Automata Implementation. Proceedings, 1999. VIII, 183 pages. 2001.

Vol. 2215: N. Kobayashi, B.C. Pierce (Eds.), Theoretical Aspects of Computer Software. Proceedings, 2001. XV, 561 pages. 2001.

Vol. 2216: E.S. Al-Shaer, G. Pacifici (Eds.), Management of Multimedia on the Internet. Proceedings, 2001. XIV, 373 pages. 2001.

Vol. 2217: T. Gomi (Ed.), Evolutionary Robotics. Proceedings, 2001. XI, 139 pages. 2001.

Vol. 2218: R. Guerraoui (Ed.), Middleware 2001. Proceedings, 2001. XIII, 395 pages. 2001.

Vol. 2220: C. Johnson (Ed.), Interactive Systems. Proceedings, 2001. XII, 219 pages. 2001.

Vol. 2221: D.G. Feitelson, L. Rudolph (Eds.), Job Scheduling Strategies for Parallel Processing. Proceedings, 2001. VII, 207 pages. 2001.

Vol. 2224: H.S. Kunii, S. Jajodia, A. Sølvberg (Eds.), Conceptual Modeling – ER 2001. Proceedings, 2001. XIX, 614 pages. 2001.

Vol. 2225: N. Abe, R. Khardon, T. Zeugmann (Eds.), Algorithmic Learning Theory. Proceedings, 2001. XI, 379 pages. 2001. (Subseries LNAI).

Vol. 2226: K.P. Jantke, A. Shinohara (Eds.), Discovery Science. Proceedings, 2001. XII, 494 pages. 2001. (Subseries LNAI).

Vol. 2227: S. Boztaş, I.E. Shparlinski (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proceedings, 2001. XII, 398 pages. 2001.

Vol. 2229: S. Qing, T. Okamoto, J. Zhou (Eds.), Information and Communications Security. Proceedings, 2001. XIV, 504 pages. 2001.

Vol. 2230: T. Katila, I.E. Magnin, P. Clarysse, J. Montagnat, J. Nenonen (Eds.), Functional Imaging and Modeling of the Heart. Proceedings, 2001. XI, 158 pages. 2001.

Vol. 2232: L. Fiege, G. Mühl, U. Wilhelm (Eds.), Electronic Commerce. Proceedings, 2001. X, 233 pages. 2001.

Vol. 2233: J. Crowcroft, M. Hofmann (Eds.), Networked Group Communication. Proceedings, 2001. X, 205 pages. 2001.

Vol. 2234: L. Pacholski, P. Ružička (Eds.), SOFSEM 2001: Theory and Practice of Informatics. Proceedings, 2001. XI, 347 pages. 2001.

Vol. 2237: P. Codognet (Ed.), Logic Programming. Proceedings, 2001. XI, 365 pages. 2001.

Vol. 2239: T. Walsh (Ed.), Principles and Practice of Constraint Programming – CP 2001. Proceedings, 2001. XIV, 788 pages. 2001.

Vol. 2240: G.P. Picco (Ed.), Mobile Agents. Proceedings, 2001. XIII, 277 pages. 2001.

Vol. 2241: M. Jünger, D. Naddef (Eds.), Computational Combinatorial Optimization. IX, 305 pages. 2001.

Vol. 2242: C.A. Lee (Ed.), Grid Computing – GRID 2001. Proceedings, 2001. XII, 185 pages. 2001.

# Contents

## Security



## Models and Architectures



## Applications

## Communication



## Run-Time Support



## Quantitative Evaluation and Benchmarking

# On the Robustness of Some Cryptographic Protocols for Mobile Agent Protection

Volker Roth

Fraunhofer Institut für Graphische Datenverarbeitung
Rundeturmstraße 6, 64283 Darmstadt, Germany
vroth@igd.fhg.de

**Abstract.** Mobile agent security is still a young discipline and most naturally, the focus up to the time of writing was on inventing new cryptographic protocols for securing various aspects of mobile agents. However, past experience shows that protocols can be flawed, and flaws in protocols can remain unnoticed for a long period of time. The game of breaking and fixing protocols is a necessary evolutionary process that leads to a better understanding of the underlying problems and ultimately to more robust and secure systems. Although, to the best of our knowledge, little work has been published on breaking protocols for mobile agents, it is inconceivable that the multitude of protocols proposed so far are all flawless. As it turns out, the opposite is true. We identify flaws in protocols proposed by Corradi *et al.*, Karjoth *et al.*, and Karnik *et al.*, including protocols based on secure co-processors.

**Keywords**: mobile agent security, cryptanalysis, breaking security protocols.

## 1 Introduction

Analyzing cryptographic protocols for mobile agent protection means meeting old friends and foes. In [1,2], Abadi, Needham, and Anderson summarized some rules and principles of good and bad practice for designing cryptographic protocols. We show in this paper that their advice was not followed thoroughly in the design of some cryptographic protocols meant to protect mobile agents against certain attacks by malicious hosts. We first summarize the typical objectives of the protocols we analyze:

**Objective 1 (Confidentiality)** *Mobile agents shall reveal cleartext only while being on trusted hosts.*

**Objective 2 (Integrity)** *The agents shall be protected such that they can acquire new data on each host they visit, but any tampering with pre-existing data must be detected by the agent's owner (and possibly by other hosts on the agent's itinerary).*

The general objective here is to protect certain features of a mobile agent against malicious hosts. By assumption, the host of the agent's owner is always trusted. Some of the protocols address both objectives simultaneously, others address just one. All

G.P. Picco (Ed.): MA 2001, LNCS 2240, pp. 1–14, 2001.

protocols are targeted at protecting *free-roaming* mobile agents. In other words, mobile agents that are free to choose their respective next hop dynamically based on data they acquired in the course of their execution.

Unfortunately, these protocols expose hosts in a way that allows an attacker to abuse them as oracles for generating protocol data. This enables attacks on cryptographic protocols devised in [3,4,5,6]. In some cases this leads to a complete compromise of the protocol's security objectives. In other cases the adversary is able to forge and replace subsets of the protocol data in a way that makes it impossible for an agent's owner to detect the tampering. The important observation here is not that protocol data acquired by agents can be truncated (some authors already acknowledge this possibility) but that the attacker can exercise control over the data returned by an agent.

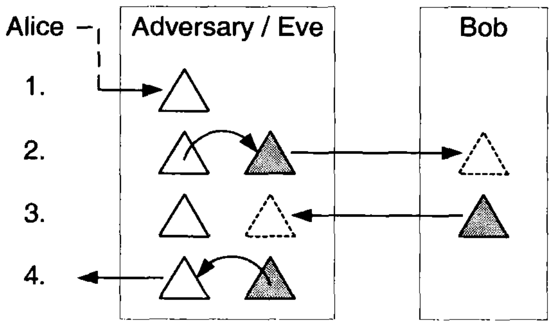


**Fig. 1.** Basic scheme of attacks we mount against various protocols. Triangles denote agents. Triangles shaded in gray denote agents created by the adversary Eve.

The attacks we mount on the analyzed protocols can best be described as *interleaving attack* [7, §10.5], which is "an impersonation or other deception involving selective combination of information from one or more previous or simultaneously ongoing protocol executions *(parallel sessions)*, including possible origination of one or more protocol executions by an adversary itself. Figure 1 illustrates the general scheme of attack: the adversary receives an agent, and copies protocol data back and forth between this agent and agents she sent herself.

## 2 Some Protocol Failures

We will write encryption of some *plaintext* into a *ciphertext* symbolically as $c = \{m\}_K$, where $K$ is the *key* being used. A digital signature will be written as an encryption with a private signing key $S^{-1}$. We will write $S^{-1}(m)$ when we refer to the bare signature rather than the union of the signature and the signed data. We assume that the identity of the signer can be extracted from her signature. A cryptographic hash of some input will be written $h(m)$. Unless noted otherwise, we assume that $h$ is *preimage resistant* and *collision resistant* [7, §9.2.2], which implies that $h$ must also be *2nd-preimage* *resistant* [7, §9.2.5]. When $A$ sends some message $m$ to $B$ we will write $A \rightarrow B : m$. We will write $A \rightarrow B : \{m\}_{K_{A,B}}$ when $m$ is sent over a confidential channel. Concatenation of $m_1$ and $m_2$ is written as $m_1 \parallel m_2$. For ease of reading, we refer to some entities by their nicknames, e.g., Alice, Bob, and Eve. In general, Eve will play the role of the adversary, Alice will play the role of the victim agent's owner, Bob and Dave will play the role of additional entities taking part in the protocols. The itinerary of Alice's agent is written as $i_0, \ldots, i_n$, where $i_0 =$ Alice and $i_n$ is the host currently visited by the agent.

## 2.1 Decrypting the Targeted State

In [3], Karnik and Tripathi propose a *targeted state* as a means to protect the confidentiality of data carried by an agent. The idea is to make this data available to the agent only when it is on a host that is trusted with respect to keeping this data confidential from other agents and hosts. In order to achieve this, the plaintext is encrypted with the public key of the trusted host. The targeted state looks like this:

$$\{\{m_1\}_{K_{i_1}}, \ldots, \{m_n\}_{K_{i_n}}\}_{S_A^{-1}}$$

The targeted state is signed by Alice, who is the originator of the agent owning the targeted state. Having received an agent, each host inspects the targeted state for ciphertexts it can decrypt. If so, the host decrypts it using its own private decryption key, and makes the cleartext available to the agent.

Below, we illustrate the attack on this protocol. Without loss of generality, we assume that the agent's targeted state contains a single ciphertext, which is encrypted with the public key of Bob. Alice first sends the agent to Eve from whom it hops to Bob and then returns to Alice. The protocol starts as follows (for simplicity, we assume here that an agent initially consists only of its targeted state and its program $\Pi_A$):

$$A \rightarrow E : \Pi_A, \{\{m\}_{K_B}\}_{S_A^{-1}}$$

The attack is straightforward. Eve strips off Alice's signature, copies $\{m\}_{K_B}$ into the targeted state of an agent of her own, signs this targeted state, and sends her agent to Bob:

$$E \rightarrow B : \Pi_E, \{\{m\}_{K_B}\}_{S_E^{-1}}$$
$$B : \Pi_E, \{\{m\}_{K_B}\}_{S_E^{-1}}, \{\{m\}_{K_B}\}_{K_B^{-1}} = m$$

Bob innocently decrypts the targeted state using his own private key and makes the resulting plaintext available to the agent. The agent then migrates back to Eve carrying the plaintext.

$$B \rightarrow E : \Pi_E, \{\{m\}_{K_B}\}_{S_E^{-1}}, m$$

Eve now is in possession of the plaintext which should be available only to Bob; Alice never detects the attack. The problem with this protocol is that, due to a lack of redundancy in the ciphertext, Bob can be abused as an oracle. Alice needs to include