Aditya Bagchi
Vijayalakshmi Atluri (Eds.)

Information Systems Security

LNCS 4332

Second International Conference, ICISS 2006
Kolkata, India, December 2006
Proceedings

Springer

Aditya Bagchi Vijayalakshmi Atluri (Eds.)

Information Systems Security

Second International Conference, ICISS 2006
Kolkata, India, December 19-21, 2006
Proceedings

Springer

Volume Editors

Aditya Bagchi
Indian Statistical Institute
Computer and Statistical Service Center
203, B.T. Road, Kolkata, 700108, India
E-mail: aditya@isical.ac.in

Vijayalakshmi Atluri
Rutgers University
Department of Management Science and Information Systems
180 University Avenue, Newark, NJ 07102, USA
E-mail: atluri@cimic.rutgers.edu

Library of Congress Control Number: 2006938424

CR Subject Classification (1998): C.2.0, D.4.6, E.3, H.2.0, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-68962-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-68962-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11961635 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4332

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

The 2nd International Conference on Information Systems Security (ICISS 2006) was held during December 19-21, 2006 at the Indian Statistical Institute, Kolkata, India. Following the success of the first conference also held at Kolkata, this conference attracted submissions from different parts of the globe. Besides India, the accepted papers are from Australia, Austria, France, Germany, Iran, Italy, Korea, New Zealand, Spain and USA. Out of the 20 full papers accepted for presentation, only 9 are from India. It shows that wihin two years, this conference has earned good acceptance among the research communities around the world.

The refereed papers, which were selected from 79 submissions, were rigorously reviewed by the Program Committee members. They did a wonderful job in selecting the best papers. The acceptance rate is 25%. Besides the 20 full papers, this volume also contains 4 invited papers, 5 short papers and 3 ongoing project summaries. The volume provides researchers with a broad perspective of recent developments in information systems security.

We are particularly grateful to Pierangela Samarati, Patrick McDaniel, Vipin Swarup and Nasir Memon for accepting our invitation to deliver invited talks at the conference. The conference was preceeded by four tutorials during December 17-18, 2006. We are thankful to Partha Pal, Ravi Mukkamala, Nasir Memon and Subhamoy Maitra for delivering the tutorial lectures. We are grateful to Birla Institute of Technology, Mesra, Ranchi for hosting the tutorials at their Kolkata Center. We are also grateful to Malay Kundu and Chandan Majumdar for serving as the General Chairs. We are indebted to the Director of the Indian Statistical Institute for hosting the conference this year as a part of the Platinum Jubilee Celebration of the institute.

Last, but certainly not least, our thanks go to all members of the Program Committee, volunteers and students of the Indian Statistical Institute and Rutgers University whose efforts made this conference a success.

December 2006

Aditya Bagchi
Vijayalakshmi Atluri
Program Chairs

General Chairs' Message

After the success of the 1st International Conference on Information Systems Security (ICISS 2005), it was our pleasure to organize the 2nd Conference, ICISS 2006, at the Indian Statistical Institute, Kolkata, India during December 19-21, 2006. We are grateful to the Director of the institute for allowing us to organize the conference as part of the Platinum Jubilee Celebration of the institute.

This is the only conference organized in this part of the globe which is totally dedicated to information systems security. The basic aim of this conference is to provide a forum for interaction among researchers working in areas of information and system security both in India and abroad. We are very happy to note that within the short span of two years, the conference has drawn the attention of the international research community. As a result, we received a good number of submissions from many countries.

The Program Chairs, V. Atluri and A. Bagchi, along with a very committed and dedicated Program Committee did a wonderful job and maintained the high academic standard achieved in the first conference. We are very grateful to all members of the Program Committee. We are thankful to the tutorial speakers for offering interesting tutorials. We are also very grateful to the keynote speakers for accepting our invitations and for delivering highly thought-provoking lectures covering the current state of research and practice in different areas of information systems security.

The Organizing Committee under the leadership of S.C. Kundu also did a wonderful job. Organizing a conference needs money. We are particularly grateful to the Indian Statistical Institute for sponsoring this conference from the Platinum Jubilee Celebration fund. We are also grateful to all other sponsors for their generous help. In this connection, we take the opportunity to also thank Mandar Maitra, the Finance Chair of the conference.

December 2006

Malay K. Kundu
Chandan Mazumdar

Organization

Advisory Committee Chair	S.K. Pal Director Indian Statistical Institute, Kolkata, India
General Chairs	Malay K. Kundu Indian Statistical Institute, Kolkata, India Chandan Mazumdar Jadavpur University, Kolkata, India
Program Chairs	Aditya Bagchi Indian Statistical Institute, Kolkata, India Vijayalakshmi Atluri Rutgers University, USA
Organizing Chair	S.C. Kundu Indian Statistical Institute, Kolkata, India
Tutorial Chair	Indrajit Ray Colorado State University, USA
Tutorial Coordinators	R.T. Goswami Birla Institute of Technology, Mesra, Ranchi, India Pinakpani Pal Indian Statistical Institute, Kolkata, India
Finance Chair	Mandar Mitra Indian Statistical Institute, Kolkata, India
Publicity Chair	B.B. Pant Birla Institute of Technology, Mesra, Ranchi, India
Industrial Track Chair	Kushal Banerjee Tata Consultancy Services, Kolkata, India

Steering Committee

Sushil Jajodia	George Mason University, USA, Chair
Arun K. Majumdar	Indian Institute of Technology, Kharagpur, India
Aditya Bagchi	Indian Statistical Institute, Kolkata, India
Chandan Mazumdar	Jadavpur University, Kolkata, India
Vijay Varadharajan	Macquarie University, Australia
Pieranjela Samarati	University of Milan, Italy
R. Sekar	Stony Brook University, USA
A.K. Chakrabarti	Adviser, Dept. of IT, Govt. of India
N. Sitaram	Director, CAIR, India
Prem Chand	V.P., Mahindra British Telecom, India

Program Committee

Mridul S. Barik	Jadavpur University, Kolkata, India
Rana Barua	Indian Statistical Institute, Kolkata, India
Joachim Biskup	University of Dortmund, Germany
B. Bruhadeshwar	IIIT, Hyderabad, India
Frdric Cuppens	ENST, France
Ernesto Damiani	University of Milan, Italy
Deborah Frincke	PNNL and University of Idaho, USA
K. Gopinath	Indian Institute of Science, India
Qijun Gu	Texas State University, USA
S.K. Gupta	Indian Institute of Technology, Delhi, India
Sushil Jajodia	George Mason University, USA
Christopher Kruegel	TU Vienna, Austria
Michiharu Kudo	IBM Tokyo Research Laboratory, Japan
Yingjiu Li	Singapore Management University, Singapore
Subhamoy Maitra	Indian Statistical Institute, Kolkata, India
A.K. Majumdar	Indian Institute of Technology, Kharagpur, India
Fabio Massacci	University of Trento, Italy
Patrick McDaniel	Pennsylvania State University, USA
Sharad Mehrotra	University of California, Irvine, USA
Ravi Mukkamala	Old Dominion University, USA
Sukumar Nandi	Indian Institute of Technology, Guwahati, India
Brajendra Panda	University of Arkansas, USA
Arun K. Pujari	University of Hyderabad, India
Indrajit Ray	Colorado State University, USA
Indrakshi Ray	Colorado State University, USA
Bimal Roy	Indian Statistical Institute, India
Pierangela Samarati	University of Milan, Italy
A.K. Sarje	Indian Institute of Technology, Roorkee, India
R. Sekar	Stony Brook University, USA
Indranil Sengupta	Indian Institute of Technology, Kharagpur, India
Basit Shafiq	Purdue University, USA
Shamik Sural	Indian Institute of Technology, Kharagpur, India
Kian-Lee Tan	National University of Singapore, Singapore
Patrick Traynor	Pennsylvania State University, USA
Jaideep Vaidya	Rutgers University, USA
Vijay Varadharajan	Macquarie University, Australia
Alec Yasinsac	Florida State University, USA
Meng Yu	Monmouth University, USA
Bill Yurcik	University of Illinois, USA

Advisory Committee

S.K. Pal	Director, Indian Statistical Institute
S.K. Sanyal	Vice Chancellor, Jadavpur University

A.R. Thakur	Vice Chancellor, West Bengal University of Technology
S.K. Mukherjee	Vice Chancellor, Birla Institute of Technology, Mesra, Ranchi
D. Dutta Mazumdar	Professor Emeritius, Indian Statistical Institute
B.B. Bhattacharya	Professor, Indian Statistical Institute
B. Chanda	Professor In-Charge, Computer and Communication Sciences Division, Indian Statistical Institute
P.K. Das	Chairman, IEEE Computer Chapter, Kolkata Section

Collaborating Institutions

Center for Secure Information Systems, George Mason University, USA
Center for Distributed Computing, Jadavpur University, India
Birla Institute of Technology, Mesra, Ranchi, India
IEEE Computer Chapter, Kolkata Section

Lecture Notes in Computer Science

For information about Vols. 1–4254

please contact your bookseller or Springer

Vol. 4355: J. Julliand, O. Kouchnarenko (Eds.), B 2007: Formal Specification and Development in B. XIII, 293 pages. 2006.

Vol. 4345: N. Maglaveras, I. Chouvarda, V. Koutkias, R. Brause (Eds.), Biological and Medical Data Analysis. XIII, 496 pages. 2006. (Sublibrary LNBI).

Vol. 4341: P.Q. Nguyen (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4338: P. Kalra, S. Peleg (Eds.), Computer Vision, Graphics and Image Processing. XV, 965 pages. 2006.

Vol. 4337: S. Arun-Kumar, N. Garg (Eds.), FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science. XIII, 430 pages. 2006.

Vol. 4333: U. Reimer, D. Karagiannis (Eds.), Practical Aspects of Knowledge Management. XII, 338 pages. 2006. (Sublibrary LNAI).

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4331: G. Min, B. Di Martino, L.T. Yang, M. Guo, G. Ruenger (Eds.), Frontiers of High Performance Computing and Networking – ISPA 2006 Workshops. XXXVII, 1141 pages. 2006.

Vol. 4330: M. Guo, L.T. Yang, B. Di Martino, H.P. Zima, J. Dongarra, F. Tang (Eds.), Parallel and Distributed Processing and Applications. XVIII, 953 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4328: D. Penkler, M. Reitenspiess, F. Tam (Eds.), Service Availability. X, 289 pages. 2006.

Vol. 4327: M. Baldoni, U. Endriss (Eds.), Declarative Agent Languages and Technologies IV. VIII, 257 pages. 2006. (Sublibrary LNAI).

Vol. 4326: S. Göbel, R. Malkewitz, I. Iurgel (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. X, 384 pages. 2006.

Vol. 4325: J. Cao, I. Stojmenovic, X. Jia, S.K. Das (Eds.), Mobile Ad-hoc and Sensor Networks. XIX, 887 pages. 2006.

Vol. 4320: R. Gotzhein, R. Reed (Eds.), System Analysis and Modeling: Language Profiles. X, 229 pages. 2006.

Vol. 4319: L.-W. Chang, W.-N. Lie (Eds.), Advances in Image and Video Technology. XXVI, 1347 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4317: S.K. Madria, K.T. Claypool, R. Kannan, P. Uppuluri, M.M. Gore (Eds.), Distributed Computing and Internet Technology. XIX, 466 pages. 2006.

Vol. 4316: M.M. Dalkilic, S. Kim, J. Yang (Eds.), Data Mining and Bioinformatics. VIII, 197 pages. 2006. (Sublibrary LNBI).

Vol. 4313: T. Margaria, B. Steffen (Eds.), Leveraging Applications of Formal Methods. IX, 197 pages. 2006.

Vol. 4312: S. Sugimoto, J. Hunter, A. Rauber, A. Morishima (Eds.), Digital Libraries: Achievements, Challenges and Opportunities. XVIII, 571 pages. 2006.

Vol. 4311: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks II. XI, 253 pages. 2006.

Vol. 4309: P. Inverardi, M. Jazayeri (Eds.), Software Engineering Education in the Modern Age. VIII, 207 pages. 2006.

Vol. 4308: S. Chaudhuri, S.R. Das, H.S. Paul, S. Tirthapura (Eds.), Distributed Computing and Networking. XIX, 608 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4306: Y. Avrithis, Y. Kompatsiaris, S. Staab, N.E. O'Connor (Eds.), Semantic Multimedia. XII, 241 pages. 2006.

Vol. 4305: A.A. Shvartsman (Ed.), Principles of Distributed Systems. XIII, 441 pages. 2006.

Vol. 4304: A. Sattar, B.-h. Kang (Eds.), AI 2006: Advances in Artificial Intelligence. XXVII, 1303 pages. 2006. (Sublibrary LNAI).

Vol. 4303: A. Hoffmann, B.-h. Kang, D. Richards, S. Tsumoto (Eds.), Advances in Knowledge Acquisition and Management. XI, 259 pages. 2006. (Sublibrary LNAI).

Vol. 4302: J. Domingo-Ferrer, L. Franconi (Eds.), Privacy in Statistical Databases. XI, 383 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4297: Y. Robert, M. Parashar, R. Badrinath, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2006. XXIV, 642 pages. 2006.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4295: J.D. Carswell, T. Tezuka (Eds.), Web and Wireless Geographical Information Systems. XI, 269 pages. 2006.

Vol. 4294: A. Dan, W. Lamersdorf (Eds.), Service-Oriented Computing – ICSOC 2006. XIX, 653 pages. 2006.

Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), MICAI 2006: Advances in Artificial Intelligence. XXVIII, 1232 pages. 2006. (Sublibrary LNAI).

Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part II. XXXII, 906 pages. 2006.

Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part I. XXXI, 916 pages. 2006.

Vol. 4290: M. van Steen, M. Henning (Eds.), Middleware 2006. XIII, 425 pages. 2006.

Vol. 4289: M. Ackermann, B. Berendt, M. Grobelnik, A. Hotho, D. Mladenič, G. Semeraro, M. Spiliopoulou, G. Stumme, V. Svatek, M. van Someren (Eds.), Semantics, Web and Mining. X, 197 pages. 2006. (Sublibrary LNAI).

Vol. 4288: T. Asano (Ed.), Algorithms and Computation. XX, 766 pages. 2006.

Vol. 4287: C. Mao, T. Yokomori (Eds.), DNA Computing. XII, 440 pages. 2006.

Vol. 4286: P. Spirakis, M. Mavronicolas, S. Kontogiannis (Eds.), Internet and Network Economics. XI, 401 pages. 2006.

Vol. 4285: Y. Matsumoto, R. Sproat, K.-F. Wong, M. Zhang (Eds.), Computer Processing of Oriental Languages. XVII, 544 pages. 2006. (Sublibrary LNAI).

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4282: Z. Pan, A. Cheok, M. Haller, R.W.H. Lau, H. Saito, R. Liang (Eds.), Advances in Artificial Reality and Tele-Existence. XXIII, 1347 pages. 2006.

Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), Theoretical Aspects of Computing - ICTAC 2006. XV, 371 pages. 2006.

Vol. 4280: A.K. Datta, M. Gradinariu (Eds.), Stabilization, Safety, and Security of Distributed Systems. XVII, 590 pages. 2006.

Vol. 4279: N. Kobayashi (Ed.), Programming Languages and Systems. XI, 423 pages. 2006.

Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II. XLV, 1004 pages. 2006.

Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part I. XLV, 1009 pages. 2006.

Vol. 4276: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II. XXXII, 752 pages. 2006.

Vol. 4275: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I. XXXI, 1115 pages. 2006.

Vol. 4274: Q. Huo, B. Ma, E.-S. Chng, H. Li (Eds.), Chinese Spoken Language Processing. XXIV, 805 pages. 2006. (Sublibrary LNAI).

Vol. 4273: I. Cruz, S. Decker, D. Allemang, C. Preist, D. Schwabe, P. Mika, M. Uschold, L. Aroyo (Eds.), The Semantic Web - ISWC 2006. XXIV, 1001 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4271: F.V. Fomin (Ed.), Graph-Theoretic Concepts in Computer Science. XIII, 358 pages. 2006.

Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), Interactive Technologies and Sociotechnical Systems. XVI, 547 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006. (Sublibrary LNAI).

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006. (Sublibrary LNAI).

Vol. 4263: A. Levi, E. Savaş, H. Yenigün, S. Balcısoy, Y. Saygın (Eds.), Computer and Information Sciences – ISCIS 2006. XXIII, 1084 pages. 2006.

Vol. 4262: K. Havelund, M. Núñez, G. Roşu, B. Wolff (Eds.), Formal Approaches to Software Testing and Runtime Verification. VIII, 255 pages. 2006.

Vol. 4261: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.), Advances in Multimedia Information Processing - PCM 2006. XXII, 1040 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006. (Sublibrary LNAI).

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), Web Information Systems – WISE 2006 Workshops. XIV, 320 pages. 2006.

Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), Web Information Systems – WISE 2006. XIV, 563 pages. 2006.

Table of Contents

Invited Papers

Data and Application Security

Access Control

Key Management and Security in Wireless Networks

Threat Analysis, Detection and Recovery

Cryptography and Encryption

Short Papers and Research Reports

Privacy in the Electronic Society

Sabrina De Capitani di Vimercati and Pierangela Samarati

Dipartimento di Tecnologie dell'Informazione
Università degli Studi di Milano
26013 Crema - Italy
samarati@dti.unimi.it

Abstract. Internet provides unprecedented opportunities for the collection and sharing of privacy-sensitive information from and about users. Information about users is collected every day, as they join associations or groups, shop for groceries, or execute most of their common daily activities. Such information is subsequently processed, exchanged and shared between different parties; with users often having users have often little control over their personal information once it has been disclosed to third parties. Privacy is then becoming an increasing concern. In this paper we discuss some problems to be addressed in the protection of information in our electronic society, surveying ongoing work and open issues to be investigated.

1 Introduction

We live today in a global information infrastructure connecting remote parties worldwide through the use of large scale networks, relying on application level protocols and services such as the World Wide Web. Human activities are increasingly based on the use of remote resources and services, and on the interaction between different, remotely located, and unknown parties. The vast amounts of personal information thus available has led to growing concerns about the privacy of users: effective information sharing and dissemination can take place only if there is assurance that, while releasing information, disclosure of sensitive information is not a risk.

Unfortunately, users' privacy is often poorly managed. For instance, personal information is often disclosed to third parties without the consent of legitimate data owners or that there are professional services specialized on gathering and correlating data from heterogeneous repositories, which permit to build user profiles and possibly to disclose sensitive information not voluntarily released by their owners. Ensuring proper privacy protection requires the investigation of different aspects. Among them, there we look at the following:

- *data protection requirements composition* to take into consideration requirements coming from the data owner, the data holder, and possible privacy law. These multiple authorities scenario should be supported from the administration point of view providing solutions for modular, large-scale, scalable policy composition and interaction.

A. Bagchi and V. Atluri (Eds.): ICISS 2006, LNCS 4332, pp. 1–21, 2006.

- *security and privacy specifications and secondary usage control* to identify under which conditions a party can trust others for their security and privacy. Trust models are one of the techniques be evaluated. In particular, *digital certificates* (statements certified by given entities) can be used to establish properties of their holder (such as identity, accreditation, or authorizations. Users should be given the ability to constraint possible secondary uses of their information.
- *inference and linking attacks protection* to ensure that released (sanitized) information is not open to channels allowing attackers to infer sensitive (not released, but related) information.

In this paper, we discuss these problems and illustrate some current approaches and ongoing research. The remainder of this paper is organized as follows. Section 2 addresses the problem of combining authorization specifications that may be independently stated. We describe the characteristics that a policy composition framework should have and illustrate some current approaches and open issues. Section 3 addresses the problem of defining policies in open environments such as the Internet. We then describe current approaches and open issues. Section 4 addresses the problem of protecting released data against inference and linking attacks. We describe the k-anonymity concept and illustrate some related current approaches and open issues. Finally, Section 5 concludes the paper.

2 Policy Composition

Traditionally, authorization policies have been expressed and managed in a centralized manner: one party administers and enforces the access control requirements. In many cases however, access control needs to combine restrictions independently stated that should be enforced as one, while retaining their independence and administrative autonomy. For instance, the global policy of a large organization can be the combination of the policies of its independent and geographically distributed departments. Each of these departments is responsible for defining access control rules to protect resources and each brings its own set of constraints. To address these issues, a *policy composition framework* by which different component policies can be integrated while retaining their independence should be designed. The framework should be flexible to support different kinds of composition, yet remain simple so to keep control over complex compound policies. It should be based on a solid formal framework and a clear semantics to avoid ambiguities and enable correctness proofs.

Some of the main requirements that a policy composition framework should have can be summarized as follows [11].

- *Heterogeneous policy support.* The composition framework should be able to combine policies expressed in arbitrary languages and possibly enforced by different mechanisms. For instance, a datawarehouse may collect data from different data sources where the security restrictions autonomously stated by

the sources and associated with the data are stated with different specification languages, or refer to different paradigms (e.g., open vs closed policy).

- *Support of unknown policies.* It should be possible to account for policies that may be not completely known or even be specified and enforced in external systems. These policies are like "black-boxes" for which no (complete) specification is provided, but that can be queried at access control time. Think, for instance, of a situation where given accesses are subject, in addition to other policies, to a policy P enforcing "central administration approval". Neither the description of P, nor the specific accesses that it allows might be available; whereas P can respond yes or no to each specific request. Runtime evaluation is therefore the only possible option for P. In the context of a more complex and complete policy including P as a component, the specification could be partially compiled, leaving only P (and its possible consequences) to be evaluated at run time.
- *Controlled interference.* Policies cannot always be combined by simply merging their specifications (even if they are formulated in the same language), as this could have undesired side effects. The accesses granted/denied might not correctly reflect the specifications anymore. As a simple example, consider the combination of two systems P_{closed}, which applies a closed policy, based on rules of the form "*grant access if* $(s, o, +a)$", and P_{open} which applies an open policy, based on rules of the form "*grant access if* $\neg(s, o, -a)$". Merging the two specifications would cause the latter decision rule to derive all authorizations not blocked by P_{open}, regardless of the contents of P_{closed}. Similar problems may arise from uncontrolled interaction of the derivation rules of the two specifications. Besides, if the adopted language is a logic language with negation, the merged program might not be stratified (which may lead to ambiguous or undefined semantics).
- *Expressiveness.* The language should be able to conveniently express a wide range of combinations (spanning from minimum privileges to maximum privileges, encompassing priority levels, overriding, confinement, refinement etc.) in a uniform language. The different kinds of combinations must be expressed without changing the input specifications (as it would be necessary even in most recent and flexible approaches) and without ad-hoc extensions to authorizations (like those introduced to support priorities). For instance, consider a policy P_1 regulating access to given documents and the central administration policy P_2. Assume that access to administrative documents can be granted only if authorized by both P_1 and P_2. This requisite can be expressed in existing approaches only by explicitly extending all the rules possibly referred to administrative documents to include the additional conditions specified by P_2. Among the drawbacks of this approach is the rule explosion that it would cause and the complex structure and loss of controls of two specifications; which, in particular, cannot be maintained and managed autonomously anymore.
- *Support of different abstraction levels.* The composition language should highlight the different components and their interplay at different levels of abstraction. This is important to: *i)* facilitate specification analysis and