Sushil Jajodia
Chandan Mazumdar (Eds.)

Information Systems Security

LNCS 3803

First International Conference, ICISS 2005
Kolkata, India, December 2005
Proceedings

Springer

Sushil Jajodia Chandan Mazumdar (Eds.)

Information Systems Security

First International Conference, ICISS 2005
Kolkata, India, December 19-21, 2005
Proceedings

Springer

Volume Editors

Sushil Jajodia
George Mason University
Center for Secure Information Systems
Fairfax, VA 22030-4444, USA
E-mail: jajodia@gmu.edu

Chandan Mazumdar
Jadavpur University
Department of Computer Science and Engineering
Kolkata - 700032, India
E-mail: chandanm@cse.jdvu.ac.in

Library of Congress Control Number: 2005936358

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

ISSN 0302-9743
ISBN-10 3-540-30706-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-30706-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11593980 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3803

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

Editorial Board

Preface

The 1st International Conference on Information Systems Security (ICISS 2005) was held December 19–21, 2005 at Jadavpur University, Kolkata, India. The objectives of the conference were to discuss in depth the current state of the research and practice in information systems security, enable participants to benefit from personal contact with other researchers and expand their knowledge, and disseminate the research results.

This volume contains 4 invited papers, 19 refereed papers that were presented at the conference, and 5 ongoing project summaries. The refereed papers, which were selected from the 72 submissions, were rigorously reviewed by the Program Committee members. The volume provides researchers with a broad perspective of recent developments in information systems security.

A special note of thanks goes to the many volunteers whose efforts made this conference a success. We wish to thank Prem Chand, Ernesto Damiani, Patrick McDaniel, R. Sekar, and Vijay Varadharajan for agreeing to deliver the invited talks, the authors for their worthy contributions, and the referees for their time and effort in reviewing the papers. We are grateful to Arun Majumdar and Aditya Bagchi for serving as the General Chairs.

Last, but certainly not least, our thanks go to Vijay Kowtha of the U.S. Office of Naval Research Global and Michael Cheetham of the INDO-US Science & Technology Forum for providing the generous financial support.

December 2005

Sushil Jajodia and Chandan Mazumdar
Program Chairs

General Chairs' Message

It was our great pleasure to organize the 1st International Conference on Information Systems Security in Kolkata, India. Though such conferences are held in different parts of the globe, a conference dedicated to data security issues only has not been organized before in India. That way it is a unique event. It gives us great satisfaction to admit that our colleagues in different countries have extended all possible help in making it a success. As members of the Program Committee, they have extended all possible cooperation. We are very much grateful to our keynote speakers for accepting our invitation and for delivering lectures on frontier topics in the area of data security. We are thankful to the tutorial speakers for providing interesting tutorials. We are also grateful to the authors of the submitted papers for showing interest in this conference and sincerely hope that they would do the same in future years as well. We hope that the participants have found this conference informative enough and would also join in coming years.

In this connection, we take the opportunity to express our great appreciation to the wonderful work done by our Program Chairs Prof. S. Jajodia and Prof. C. Mazumdar. Only because of their untiring effort has the conference achieved an enviable acdemic level in its first year.

We are also very grateful to Jadavpur University for hosting the first conference as part of their Golden Jubilee celebration program. The Organizing Committee under the leadership of Prof. A. Kar has also done a wonderful job.

To organize such an event, we need money. Fundraising is not an easy job. The Finance Chair managed the show very well. We are very grateful to all our sponsors. Only because of their help could we make the conference a success.

Aditya Bagchi and Arun K. Majumdar

Organization

General Chairs:	Arun K. Majumdar, Indian Institute of Technology, Kharagpur, India
	Aditya Bagchi, Indian Statistical Institute, Kolkata, India
Program Chairs:	Sushil Jajodia, George Mason University, Fairfax, VA, USA
	Chandan Mazumdar, Jadavpur University, Kolkata, India
Organizing Chairs:	Avijit Kar, Jadavpur University, Kolkata, India
	Samir Basu, Department of Information Technology, Government of India
Tutorial Chairs:	Sarmistha Neogy, Jadavpur University, Kolkata, India
	R.T. Goswami, Birla Institute of Technology, Mesra, Ranchi, India
Finance Chair:	Mridul S. Barik, Bengal Engineering & Science University, Howrah, India
Publicity Chairs:	B.B. Pant, Birla Institute of Technology, Mesra, Ranchi, India
	Anil K. Kaushik, Department of Information Technology, Government of India
Industry Chair:	Kushal Banerjee, TCS, Kolkata, India

Program Committee

S. Arunkumar	Indian Institute of Technology, Bombay, India
Vijay Atluri	Rutgers University, USA
Mridul S. Barik	Bengal Engineering & Science University, India
Joachim Biskup	University of Dortmund, Germany
Frédéric Cuppens	ENST, France
Ernesto Damiani	University of Milan, Italy
Neil Daswani	DoCoMo USA Labs, USA
Deborah Frincke	PNNL and University of Idaho, USA
K. Gopinath	Indian Institute of Science, India
B.N. Jain	Indian Institute of Technology, Delhi, India
Christopher Kruegel	TU Vienna, Austria
Michiharu Kudo	IBM Tokyo Research Laboratory, Japan
Yingjiu Li	Singapore Management University, Singapore
Fabio Massacci	University of Trento, Italy
Patrick McDaniel	Pennsylvania State University, USA
Sharad Mehrotra	University of California, Irvine, USA

Sukumar Nandi	Indian Institute of Technology, Guwahati, India
Brajendra Panda	University of Arkansas, USA
Arun K. Pujari	University of Hyderabad, India
Indrakshi Ray	Colorado State University, USA
Indrajit Ray	Colorado State University, USA
Bimal Roy	Indian Statistical Institute, Kolkata, India
Pierangela Samarati	University of Milan, Italy
A.K. Sarje	Indian Institute of Technology, Roorkee, India
R. Sekar	State University of New York, Stoney Brook, USA
Indranil Sengupta	Indian Institute of Technology, Kharagpur, India
Shiuh-Pyng Shieh	Chiao Tung University, Taiwan
Shamik Sural	Indian Institute of Technology, Kharagpur, India
Vijay Varadharajan	Macquarie University, Australia
Alec Yasinsac	Florida State University, USA
Bill Yurcik	University of Illinois, USA

Advisory Committee

Prof. A.N. Basu	Vice Chancellor, Jadavpur University, Chairman
Prof. Shyamal K. Sanyal	Pro Vice Chancellor, Jadavpur University
Prof. A.R. Thakur	Vice Chancellor, West Bengal University of Technology
Prof. S.K. Pal	Director, Indian Statistical Institute
Prof. S.K. Mukherjee	Vice Chancellor, Birla Institute of Technology, Mesra, Ranchi (D.U.)
Shri K.V.S.S. Prasad Rao	Chief Controller, R&D (Technical), Ministry of Defence, Govt. of India
Shri A.K. Chakravarti	Adviser, Department of Information Technology, MCIT, Govt. of India
Shri N. Sitaram	Director, Centre for A. I. & Robotics, Bangalore, DRDO, Govt. of India
Shri Pankaj Aggarwala	Joint Secretary, Department of IT, Govt. of India
Dr. M.S. Rao	Director-cum-Chief Forensic Scientist of India, Ministry of Home Affairs, Govt. of India

Sponsoring Institutions

Center for Secure Information Systems, George Mason University, USA
Center For Distributed Computing, Jadavpur University, Kolkata, India
Birla Institute of Technology (D.U.), Mesra, Ranchi, India
INDO-US Science & Technology Forum, New Delhi, India
U.S. Office of Naval Research Global, USA

Lecture Notes in Computer Science

For information about Vols. 1–3704

please contact your bookseller or Springer

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Subseries LNAI).

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Subseries LNAI).

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Subseries LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Subseries LNAI).

Vol. 3785: K.-K. Lau, R. Banach (Eds.), Formal Methods and Software Engineering. XIV, 496 pages. 2005.

Vol. 3784: J. Tao, T. Tan, R.W. Picard (Eds.), Affective Computing and Intelligent Interaction. XIX, 1008 pages. 2005.

Vol. 3781: S.Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, D. Zhang (Eds.), Advances in Biometric Person Authentication. XI, 250 pages. 2005.

Vol. 3780: K. Yi (Ed.), Programming Languages and Systems. XI, 435 pages. 2005.

Vol. 3779: H. Jin, D. Reed, W. Jiang (Eds.), Network and Parallel Computing. XV, 513 pages. 2005.

Vol. 3777: O.B. Lupanov, O.M. Kasim-Zade, A.V. Chaskin, K. Steinhöfel (Eds.), Stochastic Algorithms: Foundations and Applications. VIII, 239 pages. 2005.

Vol. 3775: J. Schönwälder, J. Serrat (Eds.), Ambient Networks. XIII, 281 pages. 2005.

Vol. 3773: A. Sanfeliu, M.L. Cortés (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XX, 1094 pages. 2005.

Vol. 3772: M. Consens, G. Navarro (Eds.), String Processing and Information Retrieval. XIV, 406 pages. 2005.

Vol. 3771: J.M.T. Romijn, G.P. Smith, J. van de Pol (Eds.), Integrated Formal Methods. XI, 407 pages. 2005.

Vol. 3770: J. Akoka, S.W. Liddle, I.-Y. Song, M. Bertolotto, I. Comyn-Wattiau, W.-J. van den Heuvel, M. Kolp, J. Trujillo, C. Kop, H.C. Mayr (Eds.), Perspectives in Conceptual Modeling. XXII, 476 pages. 2005.

Vol. 3768: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part II. XXVIII, 1088 pages. 2005.

Vol. 3767: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part I. XXVIII, 1022 pages. 2005.

Vol. 3766: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 231 pages. 2005.

Vol. 3765: Y. Liu, T. Jiang, C. Zhang (Eds.), Computer Vision for Biomedical Image Applications. X, 563 pages. 2005.

Vol. 3764: S. Tixeuil, T. Herman (Eds.), Self-Stabilizing Systems. VIII, 229 pages. 2005.

Vol. 3762: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops. XXXI, 1228 pages. 2005.

Vol. 3761: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part II. XXVII, 653 pages. 2005.

Vol. 3760: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part I. XXVII, 921 pages. 2005.

Vol. 3759: G. Chen, Y. Pan, M. Guo, J. Lu (Eds.), Parallel and Distributed Processing and Applications - ISPA 2005 Workshops. XIII, 669 pages. 2005.

Vol. 3758: Y. Pan, D.-x. Chen, M. Guo, J. Cao, J.J. Dongarra (Eds.), Parallel and Distributed Processing and Applications. XXIII, 1162 pages. 2005.

Vol. 3757: A. Rangarajan, B. Vemuri, A.L. Yuille (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 666 pages. 2005.

Vol. 3756: J. Cao, W. Nejdl, M. Xu (Eds.), Advanced Parallel Processing Technologies. XIV, 526 pages. 2005.

Vol. 3754: J. Dalmau Royo, G. Hasegawa (Eds.), Management of Multimedia Networks and Services. XII, 384 pages. 2005.

Vol. 3753: O.F. Olsen, L.M.J. Florack, A. Kuijper (Eds.), Deep Structure, Singularities, and Computer Vision. X, 259 pages. 2005.

Vol. 3752: N. Paragios, O. Faugeras, T. Chan, C. Schnörr (Eds.), Variational, Geometric, and Level Set Methods in Computer Vision. XI, 369 pages. 2005.

Vol. 3751: T. Magedanz, E.R. M. Madeira, P. Dini (Eds.), Operations and Management in IP-Based Networks. X, 213 pages. 2005.

Vol. 3750: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part II. XL, 1018 pages. 2005.

Vol. 3749: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part I. XXXIX, 942 pages. 2005.

Vol. 3748: A. Hartman, D. Kreische (Eds.), Model Driven Architecture – Foundations and Applications. IX, 349 pages. 2005.

Vol. 3747: C.A. Maziero, J.G. Silva, A.M.S. Andrade, F.M.d. Assis Silva (Eds.), Dependable Computing. XV, 267 pages. 2005.

Vol. 3746: P. Bozanis, E.N. Houstis (Eds.), Advances in Informatics. XIX, 879 pages. 2005.

Vol. 3745: J.L. Oliveira, V. Maojo, F. Martín-Sánchez, A.S. Pereira (Eds.), Biological and Medical Data Analysis. XII, 422 pages. 2005. (Subseries LNBI).

Vol. 3744: T. Magedanz, A. Karmouch, S. Pierre, I. Venieris (Eds.), Mobility Aware Technologies and Applications. XIV, 418 pages. 2005.

Vol. 3740: T. Srikanthan, J. Xue, C.-H. Chang (Eds.), Advances in Computer Systems Architecture. XVII, 833 pages. 2005.

Vol. 3739: W. Fan, Z.-h. Wu, J. Yang (Eds.), Advances in Web-Age Information Management. XXIV, 930 pages. 2005.

Vol. 3738: V.R. Syrotiuk, E. Chávez (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XI, 360 pages. 2005.

Vol. 3735: A. Hoffmann, H. Motoda, T. Scheffer (Eds.), Discovery Science. XVI, 400 pages. 2005. (Subseries LNAI).

Vol. 3734: S. Jain, H.U. Simon, E. Tomita (Eds.), Algorithmic Learning Theory. XII, 490 pages. 2005. (Subseries LNAI).

Vol. 3733: P. Yolum, T. Güngör, F. Gürgen, C. Özturan (Eds.), Computer and Information Sciences - ISCIS 2005. XXI, 973 pages. 2005.

Vol. 3731: F. Wang (Ed.), Formal Techniques for Networked and Distributed Systems - FORTE 2005. XII, 558 pages. 2005.

Vol. 3729: Y. Gil, E. Motta, V. R. Benjamins, M.A. Musen (Eds.), The Semantic Web – ISWC 2005. XXIII, 1073 pages. 2005.

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3726: L.T. Yang, O.F. Rana, B. Di Martino, J.J. Dongarra (Eds.), High Performance Computing and Communications. XXVI, 1116 pages. 2005.

Vol. 3725: D. Borrione, W. Paul (Eds.), Correct Hardware Design and Verification Methods. XII, 412 pages. 2005.

Vol. 3724: P. Fraigniaud (Ed.), Distributed Computing. XIV, 520 pages. 2005.

Vol. 3723: W. Zhao, S. Gong, X. Tang (Eds.), Analysis and Modelling of Faces and Gestures. XI, 4234 pages. 2005.

Vol. 3722: D. Van Hung, M. Wirsing (Eds.), Theoretical Aspects of Computing – ICTAC 2005. XIV, 614 pages. 2005.

Vol. 3721: A.M. Jorge, L. Torgo, P.B. Brazdil, R. Camacho, J. Gama (Eds.), Knowledge Discovery in Databases: PKDD 2005. XXIII, 719 pages. 2005. (Subseries LNAI).

Vol. 3720: J. Gama, R. Camacho, P.B. Brazdil, A.M. Jorge, L. Torgo (Eds.), Machine Learning: ECML 2005. XXIII, 769 pages. 2005. (Subseries LNAI).

Vol. 3719: M. Hobbs, A.M. Goscinski, W. Zhou (Eds.), Distributed and Parallel Computing. XI, 448 pages. 2005.

Vol. 3718: V.G. Ganzha, E.W. Mayr, E.V. Vorozhtsov (Eds.), Computer Algebra in Scientific Computing. XII, 502 pages. 2005.

Vol. 3717: B. Gramlich (Ed.), Frontiers of Combining Systems. X, 321 pages. 2005. (Subseries LNAI).

Vol. 3716: L. Delcambre, C. Kop, H.C. Mayr, J. Mylopoulos, Ó. Pastor (Eds.), Conceptual Modeling – ER 2005. XVI, 498 pages. 2005.

Vol. 3715: E. Dawson, S. Vaudenay (Eds.), Progress in Cryptology – Mycrypt 2005. XI, 329 pages. 2005.

Vol. 3714: H. Obbink, K. Pohl (Eds.), Software Product Lines. XIII, 235 pages. 2005.

Vol. 3713: L.C. Briand, C. Williams (Eds.), Model Driven Engineering Languages and Systems. XV, 722 pages. 2005.

Vol. 3712: R. Reussner, J. Mayer, J.A. Stafford, S. Overhage, S. Becker, P.J. Schroeder (Eds.), Quality of Software Architectures and Software Quality. XIII, 289 pages. 2005.

Vol. 3711: F. Kishino, Y. Kitamura, H. Kato, N. Nagata (Eds.), Entertainment Computing - ICEC 2005. XXIV, 540 pages. 2005.

Vol. 3710: M. Barni, I. Cox, T. Kalker, H.J. Kim (Eds.), Digital Watermarking. XII, 485 pages. 2005.

Vol. 3709: P. van Beek (Ed.), Principles and Practice of Constraint Programming - CP 2005. XX, 887 pages. 2005.

Vol. 3708: J. Blanc-Talon, W. Philips, D.C. Popescu, P. Scheunders (Eds.), Advanced Concepts for Intelligent Vision Systems. XXII, 725 pages. 2005.

Vol. 3707: D.A. Peled, Y.-K. Tsay (Eds.), Automated Technology for Verification and Analysis. XII, 506 pages. 2005.

Vol. 3706: H. Fuks, S. Lukosch, A.C. Salgado (Eds.), Groupware: Design, Implementation, and Use. XII, 378 pages. 2005.

Vol. 3705: R. De Nicola, D. Sangiorgi (Eds.), Trustworthy Global Computing. VIII, 371 pages. 2005.

Table of Contents

Authorization and Trust Enhanced Security for Distributed Applications

Vijay Varadharajan

Professor and Microsoft Chair in Computing,
Macquarie University, NSW 2109, Australia
vijay@ics.mq.edu.au

Abstract. This paper addresses the issues of authorization and trust in a federated distributed environment. We describe some of design principles involved in the development of authorization service for practical large scale distributed systems. We present the design of web services authorization architecture and discuss its implementation within the .NET framework. Then we discuss the notion of trusted computing and presented our approach and architecture to enhancing the distributed authorization service using trusted platforms technologies.

1 Introduction

Security issues are becoming even more significant in the age of pervasive mobile networked computing where we have different types of information being used by mobile and fixed large scale distributed applications interacting over wireless and wired networks to deliver useful services to enterprises and users, fixed and mobile. (see Figure 1). We also have mobile software agents that move from place to place doing some work on behalf of the applications and users. The applications themselves are varied in their characteristics ranging from simple dedicated ones to large scale applications in finance, telecommunications and healthcare. In terms of computing platforms, we have systems ranging from big and powerful computers to cluster of computers to PCs to PDAs to dedicated information appliances. In terms of distributed middleware, we have technologies ranging from distributed remote programming to distributed object systems to web services and service oriented architecture platforms. Perhaps the key component in Figure 1 is the Users component and the main reason for all these technologies is to provide the users with the ability to perform their tasks more conveniently, more securely and more effectively from anywhere and at anytime.

The heterogeneous pervasive mobile networked computing and information infrastructure outlined above poses many security and privacy challenges. Not only there are different technology components such as computing hardware operating systems, middleware, networks and protocols, databases and applications and users but also there are different platforms in each of these technologies and different providers developing them with different security services and mechanisms. There will also be different security policies and requirements from users and organizations using these

S. Jajodia and C. Mazumdar (Eds.): ICISS 2005, LNCS 3803, pp. 1 – 20, 2005.

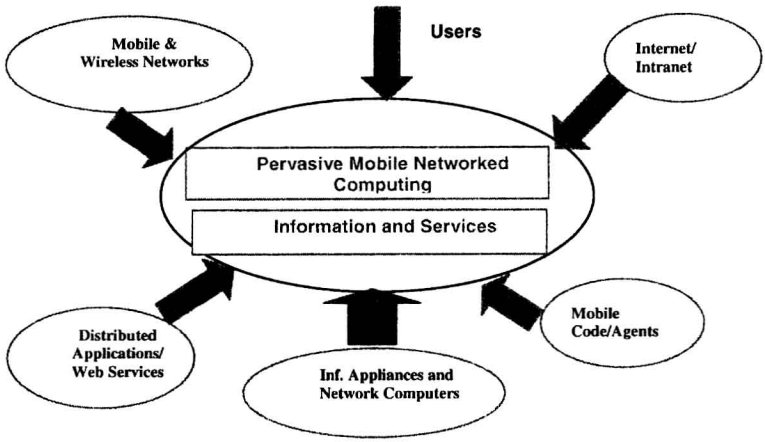

Fig. 1. Pervasive Mobile Networked Computing Environment

platforms and applications are likely to have their own security requirements. Furthermore, nowadays there are numerous standards that relate to security ranging from mechanisms to services to protocols in different networks, systems and applications; compliance and conformance to security standards, though they are claimed by different vendors and developers, are difficult to prove and are not often achieved. All these imply that the design and management of secure systems and applications and their interoperability pose several major challenges both in research and in practice.

One of the emerging areas in the middleware space in this pervasive mobile networked computing that is key to businesses and applications is that of web services or more generally service oriented architectures. Web services provide the pillars for evolving the Internet into a service-oriented integration platform of unprecedented scale and agility. The foundation of this technology lies in the modularization and virtualization of system functions as services that can be described, advertised and discovered using (XML-based) standard languages, and that interoperate through standard Internet protocols. These services aim to use standard formats and protocols to promote interoperability and extensibility among applications and to enable complex operations. Traditionally, distributed computing mechanisms have typically evolved around technical architectures rather than broader problems of application integration. On the other hand, web services have evolved around the problem of application integration using standard open technologies. Web services can pose significant security challenges as they can offer a decentralized architecture and administration with heterogeneous technologies across multiple enterprises in a federated environment. Furthermore, as web services may operate in highly autonomous and dynamic environments, security concerns are more pronounced and challenging in service oriented architectures than in conventional distributed computing architectures.

In general, security for web services is a broad and complex area covering a range of technologies. At present, there are several efforts underway that are striving for the provision of security services such as authentication between participating entities,

confidentiality and integrity of communications. A variety of existing technologies can contribute to this area such as TLS/SSL [1] and IPSEC [2]. Security functionality based on XML Signature and XML Encryption standard efforts [3] are currently being done at W3C. There are also natural extensions of these to integrate security features in technologies such as SOAP and WSDL [4]. There is also work as part of XKMS [5] defining interfaces to key management and trust services based on SOAP and WSDL. These primarily target the "transport" level. There are also draft standards being developed in the areas of web services policy, trust and federation. At this stage, they are primarily concentrating on message structures and exchange formats, rather than policy modeling, specification and enforcement. However there are some fundamental architectural and design issues in the areas of distributed authorization, trust establishment and management, which need to be addressed for the development and deployment of secure large scale web services based applications in the future.

In this paper, we will consider some specific research issues in the areas of authorization and trust in a distributed environment. In particular, we will look at the design and management of authorization policies for enterprise wide distributed applications and introduce the notion of trust enhanced authorization to improve security decision making. The paper is organized as follows. In section 2, we begin by outlining some of the design principles involved in distributed authorization. Section 3 presents the design and development of distributed authorization architecture for web services. Section 4 discusses the notion of trust in "trusted computing" and presents our approach to enhancing the authorization using trusted platforms in distributed applications.

2 Distributed Authorization

In a distributed system, when one principal requests a service from another, the receiving principal needs to address at least two questions. Is the requesting principal the one it claims to be and does the requesting principal have appropriate privileges for the requested service? These two basic questions relate to the issues of authentication and authorization. There are also other security concerns such as auditing, secure communication, availability and accountability. The authorization requirements in distributed applications are much richer than the authentication both in terms of the types of privileges required and the nature and degree of interactions between participating entities. In this paper, our focus is on the design and management of distributed authorization and will not address the issue of authentication.

2.1 Authorization Architecture Framework

In general, the authorization architectural framework should be aimed at addressing the needs of several classes of users. These include the developers, administrators, policy setters and the end users.

From a developer point of view, much of authorization security today is still often implemented as part of the programming effort. The authorization logic is written for each application, which is often based on developers' knowledge and skill level. We

believe from an architectural point of view, it is important to separate out the authorization logic from the application logic as much as possible. This can be accomplished by defining appropriate authorization attributes and formulating rules that specify how the authorization decision is computed and processed outside the application logic. There are several benefits that arise from this strict separation. An important practical consequence is that it results in a consistent application programming interface across all applications and platforms thereby allowing common policies across them. Furthermore, checking of access rights is abstracted away from a particular application. This enables the developers to concentrate on the business logic instead of reinventing the security portion of the application.

From an administrator point of view, often each application is administered separately. This often leads to custom security processes for administering the required security information, such as user names and privilege capabilities. Enterprise wide security policies are become difficult to implement consistently across all applications and these policies are even more difficult to verify. Certain security tasks require more than one administrator to check the correctness of the task. It will be useful if the architecture is able to consolidate security management. This can provide a consistent view of principals and their privileges for a given application.

From the end user point of view, in large systems, they suffer most from the fact that each system and each application implements its own security mechanisms. When each application provides its own authorization facilities, the user can get confused by the different policies in the application. For example, why is a bank manager's limit in one banking application is $1500 and in a related application it is $2000? It may be necessary for the security related attributes of a user to be consistent throughout the range of similar applications.

Furthermore, policy setters and managers require facilities and tools to ensure that the policies are correctly specified and implemented. Hence there is a need for the authorization architecture to be a way of structuring and grouping principals and resources, establish and manage privileges, check and test for consistency and validate the correctness and completeness of policies.

2.2 Authorization Service Design Principles

The design of any security service involves at least the following aspects: security information used in the provision of the security service, the security mechanisms that are required to support the service and the authorities involved in the management of the service. In the case of authorization service, the security information used ranges from user identities to group identities to role information to location information to actions and parameters associated with the actions. From an architecture point of view, it is important to recognize the characteristics of the different types of the authorization security information. At an informal conceptual level, we can classify the various types of information as follows: Some security information is generic and static in nature. For instance, typically identity based information falls into this category. Then there is security information that is specific but still somewhat static in nature. For instance, role based access information falls into this category. Roles are specific to organizations and they are reasonably static in the sense that they are unlikely to change on a day to day or even on a monthly (or even yearly) basis. In