Sokratis Katsikas
Javier Lopez
Günther Pernul (Eds.)

LNCS 3184

Trust and Privacy in Digital Business

First International Conference, TrustBus 2004
Zaragoza, Spain, August/September 2004
Proceedings

Springer

Sokratis Katsikas Javier Lopez
Günther Pernul (Eds.)

Trust and Privacy in Digital Business

First International Conference, TrustBus 2004
Zaragoza, Spain, August 30 - September 1, 2004
Proceedings

Springer

Volume Editors

Sokratis Katsikas
University of the Aegean
Department of Information and Communication Systems Engineering
Karlovassi, 83200 Samos, Greece
E-mail: ska@aegean.gr

Javier Lopez
University of Malaga, Computer Science Department
Campus de Teatinos, 29071 Málaga, Spain
E-mail: jlm@lcc.uma.es

Günther Pernul
University of Regensburg, Department of Information Systems
Universitätsstr. 31, 93053 Regensburg, Germany
E-mail: pernul@wiwi.uni-regensburg.de

Library of Congress Control Number: 2004110771

CR Subject Classification (1998): K.4.4, K.4, K.6, E.3, C.2, D.4.6, J.1

ISSN 0302-9743
ISBN 3-540-22919-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11312376 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3184

Lecture Notes in Computer Science

For information about Vols. 1–3066

please contact your bookseller or Springer

Vol. 3194: R. Camacho, R. King, A. Srinivasan (Eds.), Inductive Logic Programming. XI, 361 pages. 2004. (Subseries LNAI).

Vol. 3184: S. Katsikas, J. Lopez, G. Pernul (Eds.), Trust and Privacy in Digital Business. XI, 299 pages. 2004.

Vol. 3178: W. Jonker, M. Petkovic (Eds.), Secure Data Management. VIII, 219 pages. 2004.

Vol. 3177: Z.R. Yang, H. Yin, R. Everson (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2004. VXIII, 852 pages. 2004.

Vol. 3174: F. Yin, J. Wang, C. Guo (Eds.), Advances in Neural Networks - ISNN 2004. XXXV, 1021 pages. 2004.

Vol. 3172: M. Dorigo, M. Birattari, C. Blum, L. M.Gambardella, F. Mondada, T. Stützle (Eds.), Ant Colony, Optimization and Swarm Intelligence. XII, 434 pages. 2004.

Vol. 3166: M. Rauterberg (Ed.), Entertainment Computing – ICEC 2004. XXIII, 617 pages. 2004.

Vol. 3158: I. Nikolaidis, M. Barbeau, E. Kranakis (Eds.), Ad-Hoc, Mobile, and Wireless Networks. IX, 344 pages. 2004.

Vol. 3157: C. Zhang, H. W. Guesgen, W.K. Yeap (Eds.), PRICAI 2004: Trends in Artificial Intelligence. XX, 1023 pages. 2004. (Subseries LNAI).

Vol. 3156: M. Joye, J.-J. Quisquater (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2004. XIII, 455 pages. 2004.

Vol. 3155: P. Funk, P.A. González Calero (Eds.), Advanced in Case-Based Reasoning. XIII, 822 pages. 2004. (Subseries LNAI).

Vol. 3154: R.L. Nord (Ed.), Software Product Lines. XIV, 334 pages. 2004.

Vol. 3153: J. Fiala, V. Koubek, J. Kratochvíl (Eds.), Mathematical Foundations of Computer Science 2004. XIV, 902 pages. 2004.

Vol. 3152: M. Franklin (Ed.), Advances in Cryptology – CRYPTO 2004. XI, 579 pages. 2004.

Vol. 3150: G.-Z. Yang, T. Jiang (Eds.), Medical Imaging and Augmented Reality. XII, 378 pages. 2004.

Vol. 3149: M. Danelutto, M. Vanneschi, D. Laforenza (Eds.), Euro-Par 2004 Parallel Processing. XXXIV, 1081 pages. 2004.

Vol. 3148: R. Giacobazzi (Ed.), Static Analysis. XI, 393 pages. 2004.

Vol. 3146: P. Érdi, A. Esposito, M. Marinaro, S. Scarpetta (Eds.), Computational Neuroscience: Cortical Dynamics. XI, 161 pages. 2004.

Vol. 3144: M. Papatriantafilou, P. Hunel (Eds.), Principles of Distributed Systems. XI, 246 pages. 2004.

Vol. 3143: W. Liu, Y. Shi, Q. Li (Eds.), Advances in Web-Based Learning – ICWL 2004. XIV, 459 pages. 2004.

Vol. 3142: J. Diaz, J. Karhumäki, A. Lepistö, D. Sannella (Eds.), Automata, Languages and Programming. XIX, 1253 pages. 2004.

Vol. 3140: N. Koch, P. Fraternali, M. Wirsing (Eds.), Web Engineering. XXI, 623 pages. 2004.

Vol. 3139: F. Iida, R. Pfeifer, L. Steels, Y. Kuniyoshi (Eds.), Embodied Artificial Intelligence. IX, 331 pages. 2004. (Subseries LNAI).

Vol. 3138: A. Fred, T. Caelli, R.P.W. Duin, A. Campilho, D.d. Ridder (Eds.), Structural, Syntactic, and Statistical Pattern Recognition. XXII, 1168 pages. 2004.

Vol. 3137: P. De Bra, W. Nejdl (Eds.), Adaptive Hypermedia and Adaptive Web-Based Systems. XIV, 442 pages. 2004.

Vol. 3136: F. Meziane, E. Métais (Eds.), Natural Language Processing and Information Systems. XII, 436 pages. 2004.

Vol. 3134: C. Zannier, H. Erdogmus, L. Lindstrom (Eds.), Extreme Programming and Agile Methods - XP/Agile Universe 2004. XIV, 233 pages. 2004.

Vol. 3133: A.D. Pimentel, S. Vassiliadis (Eds.), Computer Systems: Architectures, Modeling, and Simulation. XIII, 562 pages. 2004.

Vol. 3131: V. Torra, Y. Narukawa (Eds.), Modeling Decisions for Artificial Intelligence. XI, 327 pages. 2004. (Subseries LNAI).

Vol. 3130: A. Syropoulos, K. Berry, Y. Haralambous, B. Hughes, S. Peter, J. Plaice (Eds.), TeX, XML, and Digital Typography. VIII, 265 pages. 2004.

Vol. 3129: Q. Li, G. Wang, L. Feng (Eds.), Advances in Web-Age Information Management. XVII, 753 pages. 2004.

Vol. 3128: D. Asonov (Ed.), Querying Databases Privately. IX, 115 pages. 2004.

Vol. 3127: K.E. Wolff, H.D. Pfeiffer, H.S. Delugach (Eds.), Conceptual Structures at Work. XI, 403 pages. 2004. (Subseries LNAI).

Vol. 3126: P. Dini, P. Lorenz, J.N.d. Souza (Eds.), Service Assurance with Partial and Intermittent Resources. XI, 312 pages. 2004.

Vol. 3125: D. Kozen (Ed.), Mathematics of Program Construction. X, 401 pages. 2004.

Vol. 3124: J.N. de Souza, P. Dini, P. Lorenz (Eds.), Telecommunications and Networking - ICT 2004. XXVI, 1390 pages. 2004.

Vol. 3123: A. Belz, R. Evans, P. Piwek (Eds.), Natural Language Generation. X, 219 pages. 2004. (Subseries LNAI).

Vol. 3122: K. Jansen, S. Khanna, J.D.P. Rolím, D. Ron (Eds.), Approximation, Randomization, and Combinatorial Optimization. IX, 428 pages. 2004.

Vol. 3121: S. Nikoletseas, J.D.P. Rolim (Eds.), Algorithmic Aspects of Wireless Sensor Networks. X, 201 pages. 2004.

Vol. 3120: J. Shawe-Taylor, Y. Singer (Eds.), Learning Theory. X, 648 pages. 2004. (Subseries LNAI).

Vol. 3118: K. Miesenberger, J. Klaus, W. Zagler, D. Burger (Eds.), Computer Helping People with Special Needs. XXIII, 1191 pages. 2004.

Vol. 3116: C. Rattray, S. Maharaj, C. Shankland (Eds.), Algebraic Methodology and Software Technology. XI, 569 pages. 2004.

Vol. 3114: R. Alur, D.A. Peled (Eds.), Computer Aided Verification. XII, 536 pages. 2004.

Vol. 3113: J. Karhumäki, H. Maurer, G. Paun, G. Rozenberg (Eds.), Theory Is Forever. X, 283 pages. 2004.

Vol. 3112: H. Williams, L. MacKinnon (Eds.), Key Technologies for Data Management. XII, 265 pages. 2004.

Vol. 3111: T. Hagerup, J. Katajainen (Eds.), Algorithm Theory - SWAT 2004. XI, 506 pages. 2004.

Vol. 3110: A. Juels (Ed.), Financial Cryptography. XI, 281 pages. 2004.

Vol. 3109: S.C. Sahinalp, S. Muthukrishnan, U. Dogrusoz (Eds.), Combinatorial Pattern Matching. XII, 486 pages. 2004.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 3107: J. Bosch, C. Krueger (Eds.), Software Reuse: Methods, Techniques and Tools. XI, 339 pages. 2004.

Vol. 3106: K.-Y. Chwa, J.I. Munro (Eds.), Computing and Combinatorics. XIII, 474 pages. 2004.

Vol. 3105: S. Göbel, U. Spierling, A. Hoffmann, I. Iurgel, O. Schneider, J. Dechau, A. Feix (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. XVI, 304 pages. 2004.

Vol. 3104: R. Kralovic, O. Sykora (Eds.), Structural Information and Communication Complexity. X, 303 pages. 2004.

Vol. 3103: K. Deb, e. al. (Eds.), Genetic and Evolutionary Computation – GECCO 2004. XLIX, 1439 pages. 2004.

Vol. 3102: K. Deb, e. al. (Eds.), Genetic and Evolutionary Computation – GECCO 2004. L, 1445 pages. 2004.

Vol. 3101: M. Masoodian, S. Jones, B. Rogers (Eds.), Computer Human Interaction. XIV, 694 pages. 2004.

Vol. 3100: J.F. Peters, A. Skowron, J.W. Grzymała-Busse, B. Kostek, R.W. Świniarski, M.S. Szczuka (Eds.), Transactions on Rough Sets I. X, 405 pages. 2004.

Vol. 3099: J. Cortadella, W. Reisig (Eds.), Applications and Theory of Petri Nets 2004. XI, 505 pages. 2004.

Vol. 3098: J. Desel, W. Reisig, G. Rozenberg (Eds.), Lectures on Concurrency and Petri Nets. VIII, 849 pages. 2004.

Vol. 3097: D. Basin, M. Rusinowitch (Eds.), Automated Reasoning. XII, 493 pages. 2004. (Subseries LNAI).

Vol. 3096: G. Melnik, H. Holz (Eds.), Advances in Learning Software Organizations. X, 173 pages. 2004.

Vol. 3095: C. Bussler, D. Fensel, M.E. Orlowska, J. Yang (Eds.), Web Services, E-Business, and the Semantic Web. X, 147 pages. 2004.

Vol. 3094: A. Nürnberger, M. Detyniecki (Eds.), Adaptive Multimedia Retrieval. VIII, 229 pages. 2004.

Vol. 3093: S. Katsikas, S. Gritzalis, J. Lopez (Eds.), Public Key Infrastructure. XIII, 380 pages. 2004.

Vol. 3092: J. Eckstein, H. Baumeister (Eds.), Extreme Programming and Agile Processes in Software Engineering. XVI, 358 pages. 2004.

Vol. 3091: V. van Oostrom (Ed.), Rewriting Techniques and Applications. X, 313 pages. 2004.

Vol. 3089: M. Jakobsson, M. Yung, J. Zhou (Eds.), Applied Cryptography and Network Security. XIV, 510 pages. 2004.

Vol. 3087: D. Maltoni, A.K. Jain (Eds.), Biometric Authentication. XIII, 343 pages. 2004.

Vol. 3086: M. Odersky (Ed.), ECOOP 2004 – Object-Oriented Programming. XIII, 611 pages. 2004.

Vol. 3085: S. Berardi, M. Coppo, F. Damiani (Eds.), Types for Proofs and Programs. X, 409 pages. 2004.

Vol. 3084: A. Persson, J. Stirna (Eds.), Advanced Information Systems Engineering. XIV, 596 pages. 2004.

Vol. 3083: W. Emmerich, A.L. Wolf (Eds.), Component Deployment. X, 249 pages. 2004.

Vol. 3080: J. Desel, B. Pernici, M. Weske (Eds.), Business Process Management. X, 307 pages. 2004.

Vol. 3079: Z. Mammeri, P. Lorenz (Eds.), High Speed Networks and Multimedia Communications. XVIII, 1103 pages. 2004.

Vol. 3078: S. Cotin, D.N. Metaxas (Eds.), Medical Simulation. XVI, 296 pages. 2004.

Vol. 3077: F. Roli, J. Kittler, T. Windeatt (Eds.), Multiple Classifier Systems. XII, 386 pages. 2004.

Vol. 3076: D. Buell (Ed.), Algorithmic Number Theory. XI, 451 pages. 2004.

Vol. 3075: W. Lenski (Ed.), Logic versus Approximation. IX, 205 pages. 2004.

Vol. 3074: B. Kuijpers, P. Revesz (Eds.), Constraint Databases and Applications. XII, 181 pages. 2004.

Vol. 3073: H. Chen, R. Moore, D.D. Zeng, J. Leavitt (Eds.), Intelligence and Security Informatics. XV, 536 pages. 2004.

Vol. 3072: D. Zhang, A.K. Jain (Eds.), Biometric Authentication. XVII, 800 pages. 2004.

Vol. 3071: A. Omicini, P. Petta, J. Pitt (Eds.), Engineering Societies in the Agents World. XIII, 409 pages. 2004. (Subseries LNAI).

Vol. 3070: L. Rutkowski, J. Siekmann, R. Tadeusiewicz, L.A. Zadeh (Eds.), Artificial Intelligence and Soft Computing - ICAISC 2004. XXV, 1208 pages. 2004. (Subseries LNAI).

Vol. 3068: E. André, L. Dybkjær, W. Minker, P. Heisterkamp (Eds.), Affective Dialogue Systems. XII, 324 pages. 2004. (Subseries LNAI).

Vol. 3067: M. Dastani, J. Dix, A. El Fallah-Seghrouchni (Eds.), Programming Multi-Agent Systems. X, 221 pages. 2004. (Subseries LNAI).

Preface

Sincerely welcome to proceedings of the 1st International Conference on Trust and Privacy in Digital Business, Zaragoza, Spain, held from August 30th to September 1st, 2004. This conference was an outgrowth of the two successful TrustBus international workshops, held in 2002 and 2003 in conjunction with the DEXA conferences in Aix-en-Provence and in Prague. Being the first of a planned series of successful conferences it was our goal that this event would initiate a forum to bring together researchers from academia and commercial developers from industry to discuss the state of the art of technology for establishing trust and privacy in digital business. We thank you all the attendees for coming to Zaragoza to participate and debate the new emerging advances in this area.

The conference program consisted of one invited talk and nine regular technical papers sessions. The invited talk and keynote speech was delivered by Ahmed Patel from the Computer Networks and Distributed Systems Research Group, University College Dublin, Ireland on "Developing Secure, Trusted and Auditable Services for E-Business: An Autonomic Computing Approach". A paper covering his talk is also contained in this book.

The regular paper sessions covered a broad range of topics, from access control issues to electronic voting, from trust and protocols to digital rights management. The conference attracted close to 100 submissions of which the program committee accepted 29 papers for presentation and inclusion in the conference proceedings. The authors of the accepted papers come from 12 different countries. The proceedings contain the revised versions of all accepted papers.

We would like to express our thanks to the people who helped put together the program: the program committee members and external reviewers for their timely and rigorous reviews, the DEXA organizing committee, in particular Mrs. Gabriela Wagner for her help in the administrative work, and, last but not least, Mr. Christian Schläger who was the main organizational force behind most of the involved tasks in making the conference possible.

Finally we would like to thank all authors who submitted papers, those who presented papers, and the attendees who made this event an intellectually stimulating one. We hope they enjoyed the conference.

Athens, Malaga, Regensburg
August 2004

Sokratis Katsikas
Javier Lopez
Günther Pernul

Program Committee

General Chairperson

Sokratis Katsikas, University of the Aegean, Greece

Conference Program Chairpersons

Javier Lopez, University of Malaga, Spain
Guenther Pernul, University of Regensburg, Germany

Program Committee Members

Peter Bramhall, HP Labs, Bristol, UK
Mike Burmester, Florida State University, USA
David W. Chadwick, University of Salford, UK
Frederic Cuppens, ENST Bretagne, France
Jorge Davila, Polytechnic Univ. of Madrid, Spain
Ed Dawson, Queensland University of Technology, Australia
Hannes Federrath, University of Regensburg, Germany
Eduardo B. Fernandez, Florida Atlantic University, USA
Elena Ferrari, University of Como, Italy
Simone Fischer-Huebner, Karlstad University, Sweden
Steven Furnell, University of Plymouth, UK
Rüdiger Grimm, University of Technology, Ilmenau, Germany
Stefanos Gritzalis, University of the Aegean, Greece
Dimitrios Gritzalis, Athens Univ. of Economics and Business, Greece
Ehud Gudes, Ben-Gurion University, Israel
Sigrid Guergens, Fraunhofer, Germany
Sushil Jajodia, George Mason University, USA
Kamal Karlapalem, IIIT Hyderabad, India
Dipak Khakhar, Lund University, Sweden
Hiroaki Kikuchi, Tokai University, Japan
Antonio Lioy, Politecnico di Torino, Italy
Diego Lopez, RedIRIS, Spain
Peter Lory, University of Regensburg, Germany
Masahiro Mambo, Tohoku University, Japan
Olivier Markowitch, Université Libre de Bruxelles, Belgium
Martin Olivier, University of Pretoria, South Africa
Eiji Okamoto, Universisty of Tsukuba, Japan
Rolf Oppliger, eSecurity Technologies, Switzerland
Ahmed Patel, University College Dublin, Ireland
Andreas Pfitzmann, University of Technology, Dresden, Germany
Birgit Pfitzmann, IBM Zurich Research Lab., Switzerland
Hartmut Pohl, FH Bonn-Rhein-Sieg, Germany
Karl Posch, University of Technology, Graz, Austria
Bart Preneel, Katholieke Universiteit Leuven, Belgium
Gerald Quirchmayr, University of Vienna, Austria
Kai Rannenberg, University of Frankfurt, Germany

Arnon Rosenthal, MITRE Corporation, USA
Carsten Rudolph, Fraunhofer, Germany
Pierangela Samarati, University of Milan, Italy
Jose M. Sierra, Univ. Carlos III, Spain
Mikko T. Siponen, University of Oulu, Finland
Adrian Spalka, University of Bonn, Germany
Leon Strous, De Nederlandsche Bank, Netherlands
Stephanie Teufel, University of Fribourg, Switzerland
Bhavani Thuraisingham, MITRE Corporation, USA
Ivan Visconti, ENS, France
Michael Waidner, IBM Zurich Research Lab., Switzerland
Marianne Winslett, University of Illinois, USA
Jianying Zhou, I2R, Singapore

External Reviewers

Angelis, George
Balopoulos, Thodoris
Bergmann, Mike
Boehme, Rainer
Bouabdallah, Ahmed
Boyd, Colin
Chen, Shiping
Clauss, Sebastian
D'Arco, Paolo
Erat, Andreas
Franz, Elke
Gilberg, Jörg
Guo, Huiping
Iliadis, John
Julisch, Klaus
Klimant, Herbert
Koepsell, Stefan
Kriegelstein, Thomas
Kühn, Ulrich
Lambrinoudakis, Costas
Martucci, Leonardo
Monahan, Brian
Muschall, Björn
Nikova, Svetla
Olson, Lars
Otenko, Sassa
Paul, Souradyuti
Pearson, Siani
Peng, Kun
Plank, Kilian
Priebe, Torsten
Proudler, Graeme
Rossnagel, Heiko
Rosulek, Mike
Roy, Sankardas
Schläger, Christian
Schlienger, Thomas
Schmidt, Nikita
Steinbrecher, Sandra
Steinert, Martin
Wang, Guilin
Westfeld, Andreas
Woelfl, Thomas
Yao, Chao
Zuccato, Albin

Table of Contents

Invited Talk

Trust

Access Control

e-Business Issues

Privacy

e-Voting

Protocols

Copyright Protection

Multicast

PKI, Signature Schemes

Developing Secure, Trusted and Auditable Services for e-Business: An Autonomic Computing Approach

Ahmed Patel

Computer Networks and Distributed Systems Research Group,
Department of Computer Science,
University College Dublin,
Belfield, Dublin 4, Ireland
apatel@cnds.ucd.ie

Abstract. Why have e-business trust and security often been evasive and unsuccessful? This keynote paper attempts to answer this question by looking at an autonomic approach to communications services for on-line businesses. It reviews the issues and challenges, and presents a rationale for security, privacy, interception, forensics of digital evidence and trust in an autonomic communications and computing environment. A combination of security, privacy enhancing technologies, trustworthy computing interfaces and techniques, advocacy, and greater understanding of the socio-economic and technical aspects of this new electronic phenomena must be covered to establish a sound e-business operating environment on a global level. Some possible solutions pertaining to this environment are also reviewed and examples of some key research areas outlined. Finally a brief overview of directions for innovative research is presented and followed by concluding remarks.

1 Introduction

The e-business industry has changed dramatically in recent years. The explosive growth of the Internet, the proliferation of mobile networks and the increasing difficulty in managing multi-vendor environments and the services that they are meant to provide have altered forever the dynamics of this industry, the expectations of its customers and the business models under which it operates. The impact of Moore's Law has had a profound effect across all sectors of the industry – equipment manufacturers, network operators, service providers and e-businesses continually strive to rapidly deploy the latest technology in order to gain competitive advantage. Although recent economic upheavals have had a drastic effect on certain sectors, the level of innovation has been impressive and the industry is again poised to drive another wave of economic growth. Further, as much as e-business rests on the benefits obtained from personalisation and customisation, it also requires that client and system privacy and security risks be effectively minimised. Eradicating these risks and maximising the client's confidence level is a key e-business requirement, as it not only influences the acceptance of e-business by clients, but also opens the avenues for effective design of e-business processes and supporting systems.

S. Katsikas, J. Lopez, and G. Pernul (Eds.): TrustBus 2004, LNCS 3184, pp. 1–10, 2004.

However, the challenges posed by the complexity of modern communications environments, which link businesses and clients, are potentially overwhelming. A gulf has emerged between the communications infrastructure and the capabilities of the services and applications deployed across it. This is manifested in the inflexible nature of current service offerings: they are rigidly defined, closely coupled to the network, possess static functionality, and are prone to a variety of security breaches and mandatory interception of traffic. Critically, current service offerings are manually deployed and managed, requiring highly labour intensive support structures, with a consequent inflexibility and significant time to market constraints.

The heart of this problem is the inability of service providers, communications operators and e-business applications to adapt, in a dynamic fashion, their offered services to the changing needs of their customers in a seamless and secure fashion. An approach to solving this problem is through envisaging an Autonomic Communications Environment (ACE) underpinning or supporting an autonomic computing user base, an idealistic service-centric environment exhibiting self-governing behaviour with independent auditability. Within an ACE, services will be created that are self-aware and self-healing. In their deployment, they will be self-adapting, self-optimising and self-configuring, and in operation they will be self-protecting, self-managing and self-composing. These features enable ACE services and the associated resources to adapt to changing business needs and environmental conditions without manual intervention. The proposed answer is the development of a secure, trusted and auditable Autonomic Communications Framework (ACF), whose mission is to support the development of different ACEs targeted at different business needs but in a global e-business interlaced Net environment.

At the heart of the ACF will be a new methodology for managing objects. It is required because different stakeholders have different views of a managed object, and current approaches do not take this into account. For example, the business analyst looks at a 'Service Level Agreement' object and sees an entity that represents a contractual agreement, whereas a network administrator looks at the same object and sees the different network services that must be supported using different vendor-specific functions, such as interception and audit rules, security functions and other algorithms such as queuing, routing, etc. This methodology cannot be built in either private industry or fora, and requires the combination of academic, scientific, technical and industrial advances which must be produced through a combination of fundamental basic, applied and strategic research.

The security issues that are of concern and urgent today will be even more urgent in the new world of autonomic systems that will also bring new and as yet undefined security issues of its own, issues that may not be significant or present at all today. It is envisaged that autonomic technology will offer new opportunities – new ways and means of securing e-business systems against attacks and with a level of trust that will minimise the level of tolerance in loss of revenue or non-economic function.

The growing awareness, coupled with an expanding number of new initiatives in the area internationally, is leading to a great deal of exciting research and development in the areas of security, privacy enhancing technologies, trustworthy computing interfaces and techniques, advocacy, and greater understanding of the socio-economic and technical aspects of the these new electronic phenomena.

This keynote presentation attempts to explore with you what are the issues, possible solutions and directions for research in this challenging area.

2 Issues and Challenges

The autonomic communications approach, proposed as a facilitator of e-business development on the Internet and other networks (mobile, 3G), is intrinsically tied to a variety of security challenges. The term 'security' is understood here in the broad sense and includes protection from unauthorised intervention, privacy, trust and forensics. Security in an ACE plays a dual role: to *protect autonomic facilities* of the ACE and to *offer security services to e-businesses*. Therefore, it can no longer be developed as an afterthought; it must be built in from the outset.

System and network security are vital parts of any autonomic computing solution, key to the achievement of the goals of self-protection, self-healing, and self-optimisation. Additional security challenges arising in autonomic systems include the establishment of trustworthy identities, automatically handling changes in system and network configuration, and greatly increased configuration complexity. Elements of autonomic systems will need to both establish and follow security policies in an understandable and fail-safe manner.

The fields of information technology security and telecommunications security are characterised by the existence of many technologies, services and concepts with little, if any, cohesive architecture. Furthermore, many existing protocols and systems were designed without security. In addition, there are complex interactions between society's needs (as expressed in laws, regulations etc.) and what is technologically possible. Conflicts arise between users' reasonable expectations of privacy and other reasonable expectations of law enforcement, network owners and similar stakeholders to access and control information in the telecommunications system [8]. At present, these areas are developing in an *ad hoc* manner without a clear model of how the different issues relate to one another, and how the telecommunications infrastructure should address them.

Security and reliability issues are rarely considered at the initial stages of system development. In fact, security technology is still erroneously considered as supplementary, and engineering of security techniques are not integrated within software engineering processes, with negative consequences. As a result of recent computer security crises, operating system designers have realised this need for integrated security but are constrained by the original design of their systems and the networks they are connected to – a fundamental change in system security design is needed. It is no longer sufficient to rely on rigid traffic filtering and periodic updates to protect systems from computer intruders and virus infections. Increased awareness of service and network level activities is needed to enable human analysts and automated agents to detect and respond to major problems. However, to reduce the latency between detection and response, a more organic approach to security must be developed. In addition to improving our awareness of system activities at the macro level, we need services to be resilient (self-aware and self-healing) to defend themselves against injury at the micro level to protect individuals against identity theft, privacy violation and financial loss [2,4,9].

Modern telecommunication systems are very challenging from a security and privacy perspective due to their complexity, distributed nature, diverse components, and rapid growth. Managing security is even more difficult when systems are being regularly altered to provide improved or new services. The associated lack of control over these systems must be compensated by identifying and mitigating weaknesses prior to an incident and detecting problems when prevention is not successful.

Existing approaches to security management (reconfiguration, dissemination of updates) are designed for relatively static computing environments and are not well suited to a dynamic system such as the ACE. Therefore, new security management techniques and tools must be developed for resilient autonomic systems. Similarly, vulnerability assessment must be rethought when dealing with systems that adapt and protect themselves.

Little attention has so far been paid to the usability of secure services. At present it is often the case that *'secure'* equates to *'too complicated for the average user'*. Security that is too complicated for the average user is likely to be turned off, undermining the protective mechanisms. In the future, security must be present as default behaviour without special knowledge or actions by users.

For the concept of autonomic communications to succeed, its target environments must be *secure enough to be trustworthy* in the eyes of their users. They must also provide services such as privacy protection and authentication to their users in an autonomic fashion, i.e. with minimum human involvement. While no functioning system is perfectly secure, the goal for ACEs is to be secure enough that their benefits outweigh the risks. The autonomic systems infrastructure must provide reliable identity verification, integrity and access control. To satisfy privacy policies and laws, the system and its elements must also appropriately protect private and personal information that comes into their possession. Data segregation according to their origin or purpose is needed to satisfy policy and legal requirements [6].

3 Possible Solutions

As discussed above, the challenges can be classified into three main groups: provision of *security services* to ACE users, maintaining the *security of an ACE* itself, and ensuring *usability* and transparency of security mechanisms to the end user.

3.1 Security Services in an Autonomic Communications Environment

Business scenarios envisaged in an ACE will depend on a variety of security services provided by the environment. Such services include reliable authentication (and single sign-on) of users, confidentiality (e.g. when sensitive information such as financial data or credit card numbers is transmitted), proof and non-repudiation of transactions, and trust management. Given the power of information, access to it must be protected to preserve our freedom and to defend against abuse. Since some autonomic systems deal with personal information about individuals, they need to be able to represent and demonstrably obey privacy policies required by national and international law and reinforced by proper business ethics. More powerful authorisation methods, that are context-aware and policy-driven, are required.

A methodology needs to be defined to incorporate single sign-on, as well as authentication, authorisation, accounting, and auditing of services delivered and resources used. Particular emphasis will be placed on federating security resources and services into a set of 'zones' that each provides security according to the business requirements of their context as policy-based. This combination facilitates a distributed architecture for supporting the special security needs of users. Management of end-user privacy and profiles will enable the end-user to control what information should be provided to what resource when, where, why and how.

A major challenge in the specific to ACE is to make its security services autonomic. Autonomic computing offers a host of new abilities that include ways and means to make our systems more secure and our private data better protected. Building and administering secure computing systems is well known to be a difficult task, especially so if they are heterogeneous and highly distributed. Autonomic systems offer us the opportunity to semi-automate such processes.

Making security resources and services autonomic depends largely on the underlying model of the autonomic communications architecture. For instance, they can be modelled through some kind of 'resource abstraction layer', like any other services and resources in autonomic networks. However, it is important to ensure that specific requirements of security services are met: for instance, that autonomic service management mechanisms will not undermine security of the managed services.

3.2 Security of an Autonomic Communications Environment

The aim is to create resilient systems that enable the ACE to bounce back and self-heal after an injury. This type of resilience exists in biological systems in the form of adaptive immune systems [1,5]. The concept of self-healing communication systems harks back to the early conceptions of the Internet but was not fully accomplished because sensing and response capabilities were not integrated. Our aim is to implement this resilience in more complex global, mobile communication environments, where security problems are compounded by increasing distribution and openness, with a design goal of allowing anyone to connect from anywhere.

In part resilience in ACE depends on internal sensors and alarms but also on internal triggers and responses similar to antibodies in biological systems. A biological analogy can be further explored by considering nervous and immune systems. A nervous system is responsible for sensing (and problem detection) and self-protection through reflexes and smart responses. An immune system is responsible for anomaly detection ('self' vs 'not self', 'legitimate' vs 'illegal' or 'harmless' vs 'harmful') and self-healing. The success depends on integration, reliable data, and proper response.