ICETE 2012
Final Program and Book of Abstracts

9th International Joint Conference on
e-Business and Telecommunications

Rome, Italy
24 – 27 July, 2012

Sponsored by
INSTICC – Institute for Systems and Technologies of Information, Control and Communication

Technically Co-sponsored by
IEEE Systems Council

In Cooperation with
ACM – Association for Computing Machinery
ACM SIGMM – ACM Special Interest Group on Multimedia
ACM SIGMIS – ACM Special Interest Group on Management Information Systems

Printed in Portugal
http://www.icete.org
icete.secretariat@insticc.org

Table of Contents

Foreword

We warmly welcome you to ICETE 2012 - the International Joint Conference on e-Business and Telecommunications, which is held in Rome, Italy.

This conference reflects a growing effort to increase the dissemination of new results among researchers and professionals in the fields of information and communication technologies, including data communication networking, e-business, optical communication systems, wireless networks and information systems, security and cryptography, signal processing and multimedia applications. These are the main knowledge areas that define the six ICETE component conferences, namely: DCNET, ICE-B, OPTICS, SECRYPT, SIGMAP and WINSYS, which together form the ICETE joint conference.

ICETE 2012 is sponsored by INSTICC (the Institute for Systems and Technologies of Information, Control and Communication), technically co-sponsored by the IEEE Systems Council and held in cooperation with ACM SIGMM (Special Interest Group on Multimedia) and ACM SIGMIS (Special Interest Group on Management Information Systems).

ICETE program includes a plenary distinguished panel, distinguished keynote lectures, research papers, and posters which presents the widest possible view on its technical areas. With its six tracks, we expect it to appeal to a global audience of the engineers, scientists, business practitioners and policy experts, interested in R&D on Telecommunication Systems and Services. All tracks focus on research related to real world applications and rely on contributions not only from academia, but also from industry, business and government with different solutions for end-user applications and enabling technologies, in a diversity of communication environments. The accepted papers demonstrate a number of new and innovative solutions and the vitality of these research areas.

ICETE 2012 received 403 papers in total, with contributions from 56 different countries, in all continents, which demonstrate its success and global dimension. To evaluate each submission, a double-blind paper evaluation method was used: each paper was blindly reviewed by at least two experts from the International Program Committee. In fact, most papers had 3 reviews or more. The selection process followed strict criteria in all tracks so only 45 papers were accepted and orally presented at ICETE as full papers (11% of submissions) and 77 as short papers (19% of submissions). Additionally, 50 papers were accepted for poster presentation. With these acceptance ratios, ICETE 2012 continues the tradition of previous ICETE conferences, a quality conference of high calibre. The extended versions of selected best papers of the conference will be invited to appear in a post-conference book that will be published by Springer.

We would like to emphasize that ICETE 2012 includes several outstanding keynote lectures, which are relevant to today's lines of research, development and technical innovation of today. These talks are presented by distinguished researchers who are internationally renowned experts in one or more of the ICETE areas.

A successful conference involves more than paper presentations; it is also a meeting place, where ideas about new research projects and other ventures are discussed and debated. Therefore, a social event including a conference diner/banquet has been planned for the evening of July 26 in order to promote this kind of social networking.

We would like to express our thanks to all colleagues involved in supporting this conference. First of all, we thank all authors including those whose papers were not included in the program. We also would like to thank all members of the international program committee and reviewers, who provided an invaluable help with their expertise, dedication and time. We would also like to thank the panelists and invited speakers for their invaluable contribution, in sharing their vision and knowledge.

Finally, a word of appreciation for the hard work of the INSTICC team; organizing a conference of this level is a task that can only be achieved by the collaborative effort of a dedicated and highly capable team.

We hope that the papers accepted and included in the proceedings may be a helpful reference in future works for all those who need to address the areas of e-business and telecommunications.

Enjoy the program and your stay in Rome.

Mohammad S. Obaidat, Monmouth University, U.S.A

ICETE Organizing and Steering Committees

ICETE Conference Chair

Mohammad S. Obaidat, Monmouth University, U.S.A.

DCNET Program Co-chairs

Mohammad S. Obaidat, Monmouth University, U.S.A.
José Sevillano, University of Seville, Spain
Zhaoyang Zhang, Zhejiang University, China

ICE-B Program Co-chairs

David A. Marca, University of Phoenix, U.S.A.
Marten van Sinderen, University of Twente, The Netherlands

OPTICS Program Co-chairs

Jose L. Marzo, University of Girona, Spain
Petros Nicopolitidis, Aristotle University, Greece

SECRYPT Program Chair

Pierangela Samarati, Universita' degli Studi di Milano, Italy

SECRYPT Program Co-chairs

Wenjing Lou, Virginia Polytechnic Institute and State University, U.S.A.
Jianying Zhou, Institute For Infocomm Research, Singapore

SIGMAP Program Co-chairs

Enrique Cabello, Universidad Rey Juan Carlos, Spain
Maria Virvou, University of Piraeus, Greece

WINSYS Program Co-chairs

Mohammad S. Obaidat, Monmouth University, United States
Rafael Caldeirinha, Polytechnic Institute of Leiria, Portugal
Hong Ji, Beijing University of Post and Telecommunications (BUPT), China
Dimitrios D. Vergados, University of Piraeus, Greece

Proceedings Production

Helder Coelhas, INSTICC, Portugal
Patricia Duarte, INSTICC, Portugal
Bruno Encarnação, INSTICC, Portugal
Liliana Medina, INSTICC, Portugal
Andreia Moita, INSTICC, Portugal
Carla Mota, INSTICC, Portugal
Raquel Pedrosa, INSTICC, Portugal
Vitor Pedrosa, INSTICC, Portugal
Claúdia Pinto, INSTICC, Portugal
José Varela, INSTICC, Portugal

CD-ROM Production

Pedro Varela, INSTICC, Portugal

Graphics Production and Webdesigner

Daniel Pereira, INSTICC, Portugal

Secretariat

Marina Carvalho, INSTICC, Portugal

Webmaster

Susana Ribeiro, INSTICC, Portugal

DCNET Program Committee

Julio Barbancho, Universidad de Sevilla, Spain
Alejandro Linares Barranco, University of Seville, Spain
Fernando Beltrán, University of Auckland, New Zealand
Christos Bouras, Research Academic Computer Technology Institute, N. Kazantzaki, University Campus; University of Patras, Greece
Roberto Bruschi, CNIT, Italy
Christian Callegari, University of Pisa, Italy
Periklis Chatzimisios, Alexander TEI of Thessaloniki, Greece
Hala ElAarag, Stetson University, U.S.A.
Sebastià Galmés, Universitat de les Illes Balears, Spain
Katja Gilly, Miguel Hernandez University, Spain
Abdelhakim Hafid, University of Montreal, Canada
Aun Haider, National Institute of Information and Communication Technology (NICT), Pakistan
Zbigniew Kalbarczyk, University of Illinois at Urbana-Champaign, U.S.A.
Dimitris Kanellopoulos, University of Patras, Greece
Randi Karlsen, University of Tromso, Norway
Abdallah Khreishah, Temple University, U.S.A.
Michael Kounavis, Intel Corporation, U.S.A.
Andy (Zhenjiang) Li, Cisco Systems Inc., U.S.A.
Pascal Lorenz, University of Haute Alsace, France
S. Kami Makki, Lamar University, U.S.A.
Carlos León de Mora, University of Seville, Spain
Petros Nicopolitidis, Aristotle University, Greece
Ibrahim Onyuksel, Northern Illinois Univ., U.S.A.
Elena Pagani, Universita' Degli Studi Di Milano, Italy
José Pelegri-Sebastia, Universidad Politécnica de Valencia, Spain
Juan-Carlos Ruiz-Garcia, Universidad Politécnica de València, Spain
José Luis Sevillano, University of Seville, Spain
Hangguan Shan, Zhejiang University, China
Kenji Suzuki, University of Chicago, U.S.A.
Vicente Traver, ITACA, Universidad Politécnica de Valencia, Spain
Pere Vilà, Universitat de Girona, Spain
Luis Javier Garcia Villalba, Universidad Complutense de Madrid, Spain
Manuel Villen-Altamirano, Universidad Politecnica de Madrid, Spain
Wei Wang, Zhejiang University, China
Bernd E. Wolfinger, University of Hamburg, Germany
Hirozumi Yamaguchi, Osaka University, Japan
Zhaoyang Zhang, Zhejiang University, China
Caijun Zhong, Zhejiang University, China
Cliff C. Zou, University of Central Florida, U.S.A.

DCNET Auxiliary Reviewer

Nader Chaabouni, University ofMontreal, Canada

ICE-B Program Committee

Anteneh Ayanso, Brock University, Canada
Ladjel Belllatreche, ENSMA, France
Morad Benyoucef, University of Ottawa, Canada
Indranil Bose, Indian Institute of Management Calcutta, India
Rebecca Bulander, Pforzheim University of Applied Science, Germany
Wojciech Cellary, Poznan University of Economics, Poland
Dickson Chiu, Dickson Computer Systems, China
Soon Chun, City University of New York, U.S.A.
Michele Colajanni, University of Modena and Reggio Emilia, Italy
Rafael Corchuelo, University of Sevilla, Spain
Peter Dolog, Aalborg University, Denmark
Yanqing Duan, University of Bedfordshire, U.K.
Erwin Fielt, Queensland University of Technology, Australia
José María García, University of Sevilla, Spain
Andreas Holzinger, Medical University Graz, Austria
Ela Hunt, ETH Zurich, Switzerland
Arun Iyengar, IBM Research, U.S.A.
Yung-Ming Li, National Chiao Tung University, Taiwan
Liping Liu, University of Akron, U.S.A.
David Marca, University of Phoenix, U.S.A.
Tokuro Matsuo, Yamagata University, Japan
Brian Mennecke, Iowa State University, U.S.A.
Adrian Mocan, SAP AG, Germany
Ali Reza Montazemi, Mcmaster University, Canada
Maurice Mulvenna, University of Ulster, U.K.
Daniel O'Leary, University of Southern California, U.S.A.
Krassie Petrova, Auckland University of Technology, New Zealand
Pak-Lok Poon, The Hong Kong Polytechnic University, China
Philippos Pouyioutas, University of Nicosia, Cyprus
Bijan Raahemi, University of Ottawa, Canada
Sofia Reino, CICTourGUNE, Spain
Ana Paula Rocha, LIACC-NIAD&R / FEUP, Portugal
Gustavo Rossi, University of La Plata, Argentina
Jarogniew Rykowski, The Poznan University of Economics (PUE), Poland
Marten van Sinderen, University of Twente, The Netherlands
Thompson Teo, National University of Singapore, Singapore
Michael Weiss, Carleton University, Canada
Qi Yu, Rochester Institute of Technology, U.S.A.
Lina Zhou, University of Maryland, Baltimore County, U.S.A.

OPTICS Program Committee

Anjali Agarwal, Telcordia Technologies, U.S.A.
Víctor López Álvarez, University Autónoma de Madrid, Spain
Adolfo Cartaxo, Instituto de Telecomunicações, Instituto Superior Técnico, Portugal
Walter Cerroni, Università di Bologna, Italy
Jitender Deogun, University of Nebraska-Lincoln, U.S.A.
Marco Genoves, INRIM, Italy
Masahiko Jinno, Nippon Telegraph and Telephone Corp., Japan
Miroslaw Klinkowski, National Institute of Telecommunications, Poland
Franko Küppers, University of Arizona, U.S.A.
David Q. Liu, Indiana Univ. - Purdue Univ. Fort Wayne, U.S.A.
Anna Manolova, Technical University of Denmark, Denmark
Jose L. Marzo, University of Girona, Spain
Amalia Miliou, Aristotle University of Thessaloniki, Greece
Petros Nicopolitidis, Aristotle University, Greece
Jordi Perelló, Universitat Politècnica de Catalunya (UPC), Spain
João Rebola, Instituto de Telecomunicações, ISCTE-IUL, Portugal
Enrique Rodriguez-Colina, Universidad Autónoma Metropolitana, Mexico
Sarah Ruepp, Technical University of Denmark, Denmark
Mehdi Shadaram, University of Texas at San Antonio, U.S.A.
Surinder Singh, Sant Longowal Instituite of Eng. & Tech., Longowal, Sangrur, Punjab, India
Wolfgang Sohler, University of Paderborn, Germany
Salvatore Spadaro, Universitat Politecnica de Catalunya, Spain
Naoya Wada, National Institute of Information and Communications Technology, Japan
Changyuan Yu, National University of Singapore, Singapore

SECRYPT Program Committee

Claudio Ardagna, Universita‘ degli Studi di Milano, Italy
Ken Barker, University of Calgary, Canada
Carlo Blundo, Università di Salerno, Italy
David Chadwick, University of Kent, U.K.
Aldar Chan, Institute for Infocomm Research, Singapore
Ee-chien Chang, School of Computing, National University of Singapore, Singapore
Yingying Chen, Stevens Institute of Technology, U.S.A.
Cheng-Kang Chu, Institute for Infocomm Research, Singapore
Marco Cova, University of Birmingham, U.K.
Jorge Cuellar, Siemens AG, Germany
Frederic Cuppens, TELECOM Bretagne, France
Reza Curtmola, New Jersey Institute of Tech, U.S.A.
Tassos Dimitriou, Athens Information Technology, Greece
Josep Domingo-ferrer, Rovira I Virgili University of Tarragona, Spain
Eduardo B. Fernandez, Florida Atlantic University, U.S.A.
Eduardo Fernández-medina, University of Castilla-La Mancha, Spain
Alberto Ferrante, University of Lugano, Switzerland
Josep-Lluis Ferrer-Gomila, Balearic Islands University, Spain
Simone Fischer-Hübner, Karlstad University, Sweden
Sara Foresti, Universita’ degli Studi di Milano, Italy
Keith Frikken, Miami University of Ohio, U.S.A.
Steven Furnell, Plymouth University, U.K.
Mark Gondree, Naval Postgraduate School,U.S.A.
Dimitris Gritzalis, AUEB, Greece
Yong Guan, Iowa State University, U.S.A.
Xinyi Huang, Fujian Normal University, China
Michael Huth, Imperial College London, U.K.
Cynthia Irvine, Naval Postgraduate School, U.S.A.
Sokratis Katsikas, University of Piraeus, Greece
Stefan Katzenbeisser, Technische Universität Darmstadt, Germany
Shinsaku Kiyomoto, KDDI R&D Laboratories Inc., Japan
Costas Lambrinoudakis, University of Piraeus, Greece
Bo Lang, Beijing University of Aeronautics and Astronautics, China
Loukas Lazos, University of Arizona, U.S.A.
Adam J. Lee, University of Pittsburgh, U.S.A.
Patrick P. C. Lee, Chinese University of Hong Kong, Hong Kong
Albert Levi, Sabanci University, Turkey
Jiguo Li, Hohai University, China
Ming Li, Utah State University, U.S.A.
Giovanni Livraga, Universita degli Studi di Milano, Italy
Javier Lopez, University of Malaga, Spain
Emil Lupu, Imperial College, U.K.
Luigi Mancini, University of Rome La Sapienza, Italy
Olivier Markowitch, Université Libre de Bruxelles, Belgium
Vashek Matyas, Masaryk University, Czech Republic
Carlos Maziero, UTFPR - Federal University of Technology - Paraná state, Brazil
Chris Mitchell, Royal Holloway, University of London, U.K.
Atsuko Miyaji, Japan Advaned Institute of Science and Technology, Japan
Marco Casassa Mont, Hewlett-Packard Laboratories, U.K.
David Naccache, Ecole Normale Superieure, France
Guevara Noubir, Northeastern University, U.S.A.
Eiji Okamoto, University of Tsukuba, Japan
Rolf Oppliger, eSECURITY Technologies, Switzerland
Stefano Paraboschi, University of Bergamo, Italy
Gerardo Pelosi, Politecnico di Milano, Italy
Günther Pernul, University of Regensburg, Germany

Raphael C.-w. Phan, Loughborough University, U.K.
Roberto Di Pietro, Universita' di Roma Tre, Italy
Joachim Posegga, Institute of IT Security and Security Law, Germany
Jian Ren, Michigan State University, U.S.A.
Kui Ren, Illinois Institute of Technology, U.S.A.
Sushmita Ruj, University of Ottawa, Canada
Gokay Saldamli, Bogazici University, Turkey
Pierangela Samarati, Università degli Studi di Milano, Italy
Martin Schläffer, Graz University of Technology, Austria
Miguel Soriano, UPC, Spain
Cosimo Stallo, University of Rome Tor Vergata, Italy
Neeraj Suri, Technische Universität Darmstadt, Germany
Willy Susilo, University of Wollongong, Australia
Chiu Tan, Temple University, U.S.A.
Juan Tapiador, Universidad Carlos III de Madrid, Spain
Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy
Guilin Wang, University of Wollongong, Australia
Haining Wang, The College of William and Mary, U.S.A.
Lingyu Wang, Concordia University, Canada
Xinyuan (Frank) Wang, George Mason University, U.S.A.
Osman Yagan, Carnegie Mellon University, U.S.A.
Danfeng Yao, Virginia Tech, U.S.A.
Alec Yasinsac, University of South Alabama, U.S.A.
Shucheng Yu, University of Arkansas at Little Rock, U.S.A.
Futai Zhang, Nanjing Normal University, China
Wensheng Zhang, Iowa State University, U.S.A.
Wen Tao Zhu, Graduate University of Chinese Academy of Sciences, China

SECRYPT Auxiliary Reviewers

Onur Aciicmez, Samsung Information Systems America, U.S.A.
Cristina Alcaraz, National Institute of Standards and Technology, U.S.A.
Andrew Blaich, Samsung, U.S.A.
Abian Blome, Siemens, Germany
Ning Cao, Worcester Polytechnic Institute, U.S.A.
Richard Chow, Samsung, U.S.A.
Prokopios Drogkaris, Department of Information and Communication Systems Engineering, Greece
Dimitris Geneiatakis, University of Peloponesse, Greece
Mario Kirschbaum, TU Graz - IAIK, Austria
Thomas Korak, IAIK, Austria
David Nuñez, Universidad de Málaga, Spain
Martin Ochoa, Siemens, Germany
Evangelos Reklitis, University of the Aegean, Greece
Lu Shi, University of Arkansas at Little Rock, U.S.A.
Nikos Vrakas, University of Piraeus, Greece
Boyang Wang, Xidian University, Canada
Mu-En Wu, Academic Sinica, Taiwan
Jiawei Yuan, University of Arkansas at Little Rock, U.S.A.

SIGMAP Program Committee

João Ascenso, Instituto Superior de Engenharia de Lisboa, Portugal
Arvind Bansal, Kent State University, U.S.A.
Alejandro Linares Barranco, University of Seville, Spain
Adrian Bors, University of York, U.K.
Enrique Cabello, Universidad Rey Juan Carlos, Spain
Wai-Kuen Cham, The Chinese University of Hong Kong, China
Chin-Chen Chang, Feng Chia University, Taiwan
Shu-Ching Chen, Florida International University, U.S.A.
Wei Cheng, Garena Online Pte. Ltd., Singapore
Ryszard S. Choras, University of Technology & Life Sciences, Poland
Cristina Conde, University Rey Juan Carlos, Spain
Isaac Martín De Diego, Universidad Rey Juan Carlos, Spain
Rob Evans, University of Melbourne, Australia
Jianping Fan, It College, the University of North Carolina at Charlotte, U.S.A.
Quanfu Fan, IBM, U.S.A.
Wu-Chi Feng, Portland State University, U.S.A.
William Grosky, University of Michigan - Dearborn, U.S.A.
Malka Halgamuge, The University of Melbourne, Australia
Hermann Hellwagner, Klagenfurt University, Austria
Wolfgang Hürst, Utrecht University, The Netherlands
Razib Iqbal, Amdocs, Canada
Mohan Kankanhalli, National University of Singapore, Singapore
Sokratis Katsikas, University of Piraeus, Greece
Brigitte Kerherve, Université du Québec à Montréal, Canada
Constantine Kotropoulos, Aristotle University of Thessaloniki, Greece
Tayeb Lemlouma, IUT of Lannion (University of Rennes I) / IRISA, France
Jing Li, University of Sheffield, U.K.
Zhu Liu, AT&T, U.S.A.
Hong Man, Stevens Institute of Technology, U.S.A.
Daniela Moctezuma, Rey Juan Carlos University, Spain
Arturo Morgado-Estevez, University of Cadiz, Spain
Chamin Morikawa, The University of Tokyo, Japan
Alejandro Murua, University of Montreal, Canada
Mokhtar Nibouche, University of the West of England, U.K.
Ioannis Paliokas, University of Western Macedonia, Greece
Maria Paula Queluz, Instituto Superior Técnico - Instituto de Telecomunicações, Portugal
Rudolf Rabenstein, University Erlangen-Nuremberg, Germany
Matthias Rauterberg, Eindhoven University of Technology, The Netherlands
Pedro Real, Universidad de Sevilla, Spain
Luis Alberto Morales Rosales, Instituto Tecnológico Superior de Misantla, Mexico
Javier Del Ser, TECNALIA, Spain
Mei-Ling Shyu, University of Miami, U.S.A.
Oscar S. Siordia, Universidad Rey Juan Carlos, Spain
George Tsihrintzis, University of Piraeus, Greece
Andreas Uhl, University of Salzburg, Austria
Steve Uhlig, TU Berlin/Deutsche Telekom Laboratories, Germany
Maria Virvou, University of Piraeus, Greece
Michael Weber, University of Ulm, Germany
Xiao-Yong Wei, Sichuan University, China
Lei Wu, University of Pittsburgh, U.S.A.
Kim-hui Yap, Nanyang Technological Univrsity, Singapore
Chengcui Zhang, University of Alabama at Birmingham, U.S.A.
Tianhao Zhang, University of Pennsylvania, U.S.A.
Yongxin Zhang, Qualcomm R&D, U.S.A.

SIGMAP Auxiliary Reviewers

Mariana Lobato Baez, Instituto Tecnologico Superior de Libres, Mexico
Eduardo López Domínguez, LANIA, Mexico
Elisavet Konstantinou, University of the Aegean, Greece

WINSYS Program Committee

Ali Abedi, University of Maine, U.S.A.
Dharma Agrawal, University of Cincinnati, U.S.A.
Vicente Alarcon-Aquino, Universidad de las Americas Puebla, Mexico
Josephine Antoniou, University of Cyprus, Cyprus
Francisco Barcelo Arroyo, Universitat Politecnica de Catalunya, Spain
Novella Bartolini, Università La Sapienza, Roma, Italy
Bert-Jan van Beijnum, University of Twente, The Netherlands
Luis Bernardo, Universidade Nova de Lisboa, Portugal
Matthias R. Brust, Louisiana Tech University, U.S.A.
Periklis Chatzimisios, Alexander TEI of Thessaloniki, Greece
Cheng-Fu Chou, National Taiwan University, Taiwan
Iñigo Cuiñas, Universidade de Vigo, Spain
Christos Douligeris, University of Piraeus, Greece
Amit Dvir, BME-HIT, Hungary
Val Dyadyuk, CSIRO, Australia
Marco Di Felice, University of Bologna, Italy
David Ferreira, Instituto de Telecomunicações and Polytechnic Institute of Leiria, Portugal
Mohammad Ghavami, London South Bank University - Faculty of Engineering, Science and The Built Environment, U.K.
Hong Ji, Beijing University of Post and Telecommunications (BUPT), China
Jehn-Ruey Jiang, National Central University, Taiwan
Abdelmajid Khelil, Technische Universität Darmstadt, Germany
Hsi-pin Ma, National Tsing Hua University, Taiwan
Imad Mahgoub, Florida Atlantic University, U.S.A.
S. Kami Makki, Lamar University, U.S.A.
Maja Matijasevic, University of Zagreb, Croatia
Luis Mendes, Instituto de Telecomunicações and Polytechnic Institute of Leiria, Portugal
Paul Patras, Hamilton Institute, National University of Ireland Maynooth, Ireland
Symon Podvalny, Voronezh State Technical University, Russian Federation
António Rodrigues, Instituto Superior Técnico, Portugal
Jörg Roth, University of Applied Sciences Nuremberg, Germany
Manuel García Sánchez, Universidade de Vigo, Spain
Christian Schindelhauer, University of Freiburg, Germany
Kuei-Ping Shih, Tamkang University, Taiwan
Shensheng Tang, Missouri Western State University, U.S.A.
George Tombras, National and Kapodistrian University of Athens, Greece, Greece
Cesar Vargas-Rosales, ITESM-Monterrey, Mexico
Dimitrios D. Vergados, University of Piraeus, Greece
Natalija Vlajic, York University, Canada

WINSYS Auxiliary Reviewers

Luca Bedogni, University of Bologna, Italy
Xiaojing Huang, CSIRO ICT Centre, Australia
Nikos Miridakis, University of Piraeus, Greece
Stefanos Nikolidakis, University of Piraeus, Greece
Pravin Amrut Pawar, University of Twente, The Netherlands

Panel

Tuesday, 24
9:15 – 10:30
Room: Plenary

Title: *"Recent Advances in the Security of Telecommunication and Network Systems"*

Panel Chair

Mohammad S. Obaidat, Fellow of IEEE, Fellow of SCS, Immediate Past President of the Society for Modeling &Simulation International (SCS), Editor-in-Chief, Wiley International Journal of Communication Systems, and Professor in Monmouth University, U.S.A.

Panelists

Venu Govindaraju, SUNY at Buffalo, USA
Geoffrey Fox, Indiana University, USA
Sushil Jajodia, George Mason University, USA
Pierangela Samarati, Universita' degli Studi di Milano, Italy
Andreas Holzinger, Medical University Graz, Austria
Luis M. Correia, Technical University of Lisbon, Portugal

Keynote Lectures

Tuesday 24
12:15 – 13:15
Room: Plenary

A Perspective of the Networks of the Future and Smart Cities

Luis M. Correia
IST/IT-Technical University of Lisbon
Portugal

A parallel in the evolution between mobile and wireless communications and other areas (computers and cars) will be presented, in an attempt to identify possible directions for systems future evolution. A look into already existing technologies will enable to establish a perspective for future user interface devices and services (e.g., information access, Internet of Things, and geo-location). Then, potential services are identified, after which research challenges for mobile and wireless communications networks are addressed (e.g., network virtualisation, cloud networking, and networks of information). Smart Cities are taken as an integration example, as well as a perspective of application to other key sectors (e.g., health, transport, and energy). The link with other areas, and impact on regulation, standardisation, and policy matters are presented at the end.

Luis M. Correia was born in Portugal, on October 1958. He received the Ph.D. in Electrical and Computer Engineering from IST-TUL (Technical University of Lisbon) in 1991, where he is currently a Professor in Telecommunications, with his work focused in Wireless/Mobile Communications in the areas of propagation, channel characterisation, radio networks, traffic, and applications. He has acted as a consultant for Portuguese mobile communications operators and the telecommunications regulator, besides other public and private entities. Besides being responsible for research projects at the national level, he has been active in various ones within the European frameworks of RACE, ACTS, IST, ICT and COST (where he also served as evaluator and auditor), having coordinated two COST projects, and taken leadership responsibilities at various levels in many others. He has supervised more than 150 M.Sc. and Ph.D. students, having authored more than 300 papers in international and national journals and conferences, for which he has served also as a reviewer, editor, and board member. He was part of the COST Domain Committee on ICT. He was the Chairman of the Technical Programme Committee of several conferences, namely PIMRC'2002. He is part of the Expert Advisory Group and of the Steering Board of the European Net!Works platform, and was the Chairman of its Working Group on Applications.

Tuesday 24
16:45 – 17:45
Room: Plenary

A Mission-centric Framework for Cyber Situational Awareness

Sushil Jajodia
George Mason University Fairfax
U.S.A.

Today, when a security incident occurs, the top three questions security administrators would ask are in essence: What has happened? Why did it happen? What should I do? Answers to the first two questions form the core of Cyber Situational Awareness. Whether the last question can be satisfactorily answered is greatly dependent upon the cyber situational awareness capability of an enterprise. In my talk, I will describe a framework to securely operate missions within networks that are imperfect and vulnerable to multiple types of cyber attacks. The key elements of the framework are as follows: First, we introduce the notion of generalized dependency graph which captures how network components, at different levels of abstraction, depend on each other. Second, we extend the classical definition of attack graph to incorporate probabilistic knowledge of the attacker's behavior. Finally, we introduce the notion of attack scenario graph which integrates dependency and attack graphs.

Sushil Jajodia is University Professor, BDM International Professor, and the director of Center for Secure Information Systems in the Volgenau School of Engineering at the George Mason University, Fairfax, Virginia. He served as the chair of the Department of Information and Software Engineering during 1998-2002. He joined Mason after serving as the director of the Database and Expert Systems Program within the Division of Information, Robotics, and Intelligent Systems at the National Science Foundation. Before that he was the head of the Database and Distributed Systems Section in the Computer Science and Systems Branch at the Naval Research Laboratory, Washington and Associate Professor of Computer Science and Director of Graduate Studies at the University of Missouri, Columbia. He has also been a visiting professor at the University of Milan, Italy; Sapienza University of Rome, Italy; Isaac Newton Institute for Mathematical Sciences, Cambridge University, England; and King's College, London, England. Dr. Jajodia received his PhD from the University of Oregon, Eugene. The scope of his current research interests encompasses information secrecy, privacy, integrity, and availability problems in military, civil, and commercial sectors. He has authored or coauthored six books, edited 38 books and conference proceedings, and published more than 400 technical papers in the refereed journals and conference proceedings. He is also a holder of eight patents and has several patent applications pending. He received the 1996 IFIP TC 11 Kristian Beckman award, 2000 Volgenau School of Engineering Outstanding Research Faculty Award, 2008 ACM SIGSAC Outstanding Contributions Award, and 2011 IFIP WG 11.3 Outstanding Research Contributions Award. He was recognized for the most accepted papers at the 30th anniversary of the IEEE Symposium on Security and Privacy. He has supervised 26 doctoral dissertations. His h-index is 70 and Erdos number is 2. Dr. Jajodia has served in different capacities for various journals and conferences. He serves on the editorial boards of IET Information Security, International Journal of Information and Computer Security, and International Journal of Information Security and Privacy. He was the founding editor-in-chief of the Journal of Computer Security (1992-2010) and a past editor of ACM Transactions on Information and Systems Security (1999-2006), International Journal of Cooperative Information Systems (1992-2011), and IEEE Transactions on Knowledge and Data Engineering. He is the consulting editor of the Springer International Series on Advances in Information Security. He has been named a Golden Core member for his service to the IEEE Computer Society, and received International Federation for Information Processing (IFIP) Silver Core Award "in recognition of outstanding services to IFIP" in 2001. He is a past chair of the ACM Special Interest Group on Security, Audit, and Control (SIGSAC), IEEE Computer Society Technical Committee on Data Engineering, and IFIP WG 11.5 on Systems Integrity and Control. He is a senior member of the IEEE and a member of IEEE Computer Society and Association for Computing Machinery. The URL for his web page is http://csis.gmu.edu/jajodia.

Wednesday 25
12:15 – 13:15
Room: Plenary

Making Sense of All Things Handwritten - From Postal Addresses to Tablet Notes

Venu Govindaraju
University at Buffalo
U.S.A.

The handwritten address interpretation system pioneered in our lab at UB is widely regarded as one of the key success stories in AI. It integrated the document processing steps of binarization, segmentation, recognition, and combination of classifiers with carefully handcrafted rules. Advances in machine learning (ML) in the past decade, made possible by the abundance of training data, storage, and processing power, have facilitated the development of principled approaches for many of the same modules.

Venu Govindaraju is a SUNY Distinguished Professor of Computer Science and Engineering at the University at Buffalo (SUNY Buffalo). He has authored over 325 scientific papers and supervised the doctoral dissertation of 25 students. His seminal work in handwriting recognition was at the core of the first handwritten address interpretation system used by the US Postal Service. Dr. Govindaraju has won several awards for his scholarship including the IEEE Technical Achievement Award (2010). He is a Fellow of the AAAS, ACM, IAPR and IEEE.

Thursday 26
12:15 – 13:15
Room: Plenary

On Knowledge Discovery and Interactive Intelligent Visualization of Biomedical Data - Challenges in Human–Computer Interaction & Biomedical Informatics

Andreas Holzinger
Medical University Graz
Austria

Biomedical Informatics can be defined as “the interdisciplinary field that studies and pursues the effective use of biomedical data, information and knowledge for scientific inquiry, problem solving, and decision Making, motivated by efforts to improve human health.” However, professionals in the life sciences are facing an increasing quantity of highly complex, multi-dimensional and weakly structured data. While researchers in Human-Computer Interaction (HCI) and Knowledge Discovery in Databases (KDD) have for long been working independently to develop methods that can support expert end users to identify, extract and understand information out of this data, it is obvious that an interdisciplinary approach to bring these two fields closer together can yield synergies in the application of these methods to weakly structured complex medical data sets. The aim is to support end users to learn how to interactively analyse information properties and to visualize the most relevant parts – in order to gain knowledge, and finally wisdom, to support a smarter decision making. The danger is not only to get overwhelmed by increasing masses of data, moreover, there is the risk of modelling artifacts.

Andreas Holzinger is head of the Research Unit Human–Computer Interaction, Institute of Medical Informatics, Statistics and Documentation, Medical University Graz, Associate Professor of Applied Informatics at the Faculty of Computer Science, Institute of Information Systems and Computer Media and Lecturer at the Faculty of Electrical and Information Engineering, Institute of Genomics and Bioinformatics at Graz University of Technology. He is chair of the Workgroup Human–Computer Interaction and Usability Engineering (HCI&UE) of the Austrian Computer Society, and founder and leader of the Special Interest Group HCI4MED. Since November 2009 he is Austrian Representative in the International Federation of Information Processing (IFIP), Technical Committee TC 13 Human-Computer Interaction. He serves as consultant for the Austrian, German and Dutch Government and for the German Excellence Initiative and as national expert in the European Commission (Lisbon Delegate 2000). Andreas, born 1963, started as an apprentice in Information Technology in 1978; while working as an industrial engineer, he resumed a parallel second-chance education, finished his PhD in cognitive science in 1997 and completed his second doctorate (habilitation) in applied informatics in 2003. Since 1999 participation in leading positions in 29 R&D multi-national projects, budget 2,8 MEUR; to date 314 publications, 2029 citations; h-index = 23, g-Index = 41; Andreas was Visiting Professor in Berlin, Innsbruck, London, Vienna and Aachen. His research field is in Computing and Information Sciences with application in Life and Medical Sciences and emphasis on Knowledge Management, Multimedia Information Systems, Human-Computer Interaction, Knowledge Discovery/Information Retrieval and Usability Engineering. Homepage: http://www.hci4all.at; Current main lecture: http://genome.tugraz.at/medical_informatics.shtml.

Friday 27
11:15 – 12:15
Room: Plenary

Cyberinfrastructure for eScience and eBusiness from Clouds to Exascale

Geoffrey Charles Fox
Indiana University
U.S.A.

We analyze scientific computing into classes of applications and their suitability for different architectures covering both compute and data analysis cases and both high end and long tail (many small) users. We identify where commodity systems (clouds) coming from eBusiness and eCommunity are appropriate and where specialized systems are needed. We cover both compute and data (storage) issues and propose an architecture for next generation Cyberinfrastructure and outline some of the research and education challenges. We discuss FutureGrid project that is a testbed for these ideas.

Geoffrey Charles Fox (gcf@indiana.edu, http:// www.infomall.org, http://www.futuregrid.org). Fox received a Ph.D. in Theoretical Physics from Cambridge University and is now distinguished professor of Informatics and Computing, and Physics at Indiana University where he is director of the Digital Science Center and Associate Dean for Research and Graduate Studies at the School of Informatics and Computing. He previously held positions at Caltech, Syracuse University and Florida State University. He has supervised the PhD of 64 students and published over 600 papers in physics and computer science with an index of 61 and over 19500 citations. He currently works in applying computer science to Bioinformatics, Defense, Earthquake and Ice-sheet Science, Particle Physics and Chemical Informatics. He is principal investigator of FutureGrid – a facility to enable development of new approaches to computing. He is involved in several projects to enhance the capabilities of Minority Serving Institutions.

Awards

Best Paper Awards

A "Best Paper Award" and a "Best Student Paper Award" will be conferred to the author(s) of a full paper presented at the conference, selected by the Program/Conference Chairs based on the best combined marks of paper reviewing, assessed by the Program Committee, and paper presentation quality, assessed by session chairs at the conference venue.

The "Best Student Paper Award" will be given to a paper in which the first author is a registered MSc or PhD student.

The awards will be announced and bestowed at the conference closing session.

Selected Papers Book

A number of selected papers presented at ICETE 2012 will be published by Springer-Verlag in a CCIS Series book. This selection will be done by the Conference Chair and Program Co-chairs, among the papers actually presented at the conference, based on a rigorous review by the ICETE 2012 Program Committee members.

Social Event and Banquet

Venue: Bus Tour in Rome followed by a Dinner at the "Il Borgo di Tragliata"
Date: Thursday 26, 18:15 - 23:30

Located at the entrance to Rome, "IL borgo di Tragliata," rises above an impressive tufa buttress. Archeological sources provide evidence that this area has been inhabited since ancient times. The discovery of the famous, "Oinochoe of Tagliatella" vase confirms the existence of human settlements since the Etruscan era within an area subject to control by either Ceri or Veio. The place name "Tragliata" takes note of the place names, Talianum Tagliata or Terlata, during medieval times and appears to be derived from "Tagliata, (meaning, "cut"), which is the word given to the paths dug into the tufa by the Etruscans.

The presence of several tombs dug into the tufa along the East slope of the hill on which the village sits, along with several clay artifacts found in the area, are evidence which suggest the presence of a small agricultural settlement. In addition, other documentation reports the findings of the remains of a Roman villa on Tragliata property. It is also known that the two marble memorial stones found in this area have inscriptions dating back to the third century AD.

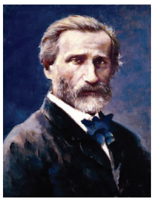
Midway through the eighth century, this area of the Roman countryside saw a period of repopulation thanks to the intelligence and will of Pope San Zaccaria (741-752) and Pope Adriano I (772-793). Encouraged by political and religious motives, these two Pontiffs presented an energetic revival and control of the territory.

During ninth and tenth centuries the historical scene began to change, the Roman countryside, with less support for the Papacy by the Carolugian empire, was made subject to continual and bloody raids by the Saracen pirates. The system of the “Domuscultae” entered into definite crisis, superceded by a strong defense system of towers and small castles; several coastal light towers were constructed to be used as bright defense signals to alert the inland region upon the pirates' approach.

The construction of Tragliata's small castle and tower date back to the ninth century, according to sources at the nearby Boccea castle.

The estate still belongs to the Vatican Basilica, even if time after time it was more or less controlled directly by others. In 1201, for example, it was ruled by a certain Jocobus de Traliata who occupied it, possibly as a lord. Several years later Tragliata, together with nearby “castium” Loterni, became subject to the interests of the turbulent Normanni family.

In 1885, the Chapter granted the Tragliata estate to Mr. Nicola Santovetti as the perpetual leaseholder. Consequently, Santovetti sold the lease to Mr. Domenico Lanza in 1917, (the great grand father of the present proprietor, Andrea de Gallo di Roccagiovane) who then took over as a tenant to finally gain possession of the estate in the following years.



General Information

Welcome Desk/On-site Registration
Monday 23 – Open from 15:00 to 17:30
Tuesday 24 – Open from 8:30 to 17:45
Wednesday 25 – Open from 8:30 to 17:30
Thursday 26 – Open from 8:30 to 17:30
Friday 27 – Open from 9:00 to 12:30

Opening Session
Tuesday 24, at 9:00 in the Plenary room.

Welcome Cocktail
Tuesday 24, at 17:45 in the Picasso Foyer.

Closing Session
Friday 27, at 12:15 in the Plenary room.

Farewell Drink
Friday 27, at 12:30 in the Picasso Foyer.

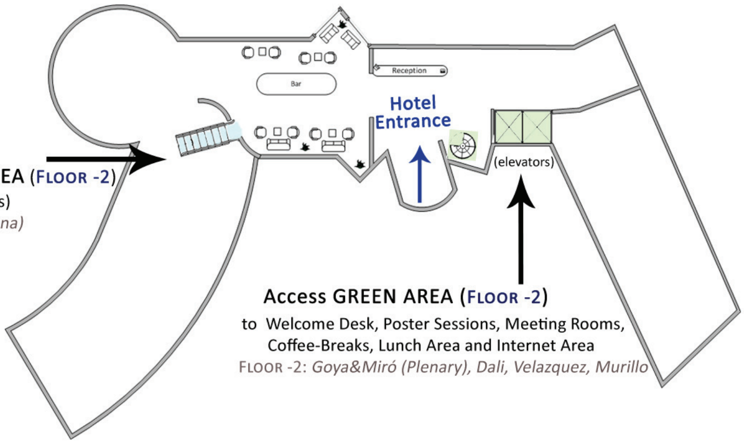
Meals
Coffee-breaks will be served in the Picasso Foyer next to the conference rooms to all registered participants.
Lunches will be served in the Murillo room from 13:15 to 14:30 to all registered participants.

Communications
Wireless access will be provided free of charge to all registered participants, during the conference business hours.

Secretariat Contacts
ICETE Secretariat
Address: Av. D. Manuel I, 27A 2º Esq.
2910-595 Setúbal, Portugal
Tel.: +351 265 520 185
Fax: +44 203 014 5432
e-mail: icete.secretariat@insticc.org
website: http://www.icete.org

Rooms Layout

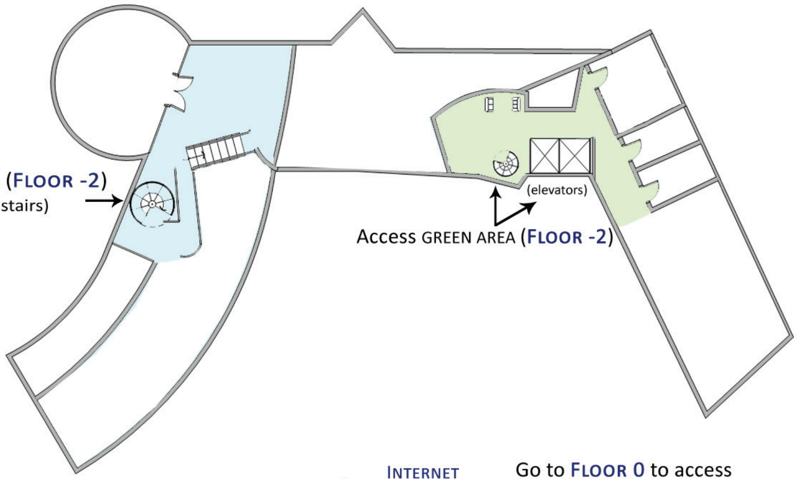
FLOOR 0



Access Meeting Rooms BLUE AREA (FLOOR -2)
through FLOOR -1 (only by stairs)
(Sevilla, Valencia, Madrid, Barcelona)

Access GREEN AREA (FLOOR -2)
to Welcome Desk, Poster Sessions, Meeting Rooms, Coffee-Breaks, Lunch Area and Internet Area
FLOOR -2: *Goya&Miró (Plenary), Dali, Velazquez, Murillo*

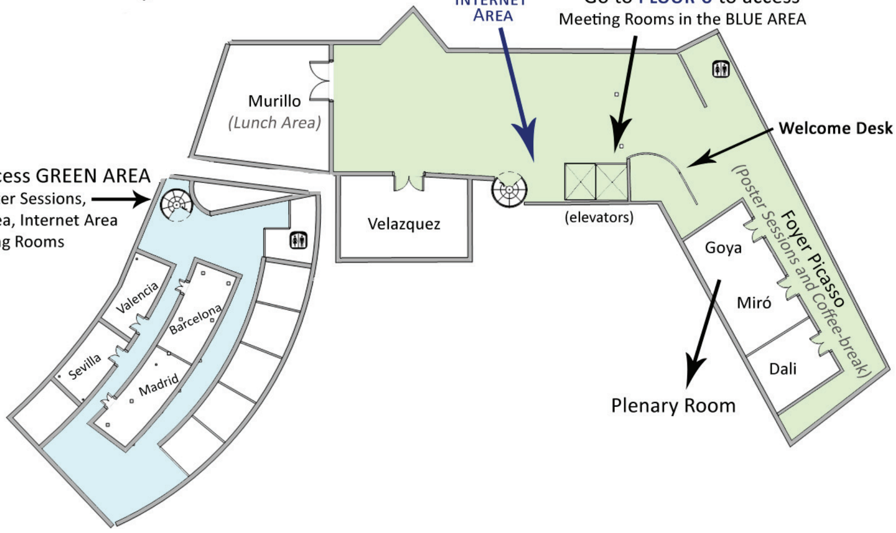
FLOOR -1



Access Meeting Rooms (FLOOR -2)
BLUE AREA (only by stairs)

Access GREEN AREA (FLOOR -2)

FLOOR -2



INTERNET AREA

Go to FLOOR 0 to access
Meeting Rooms in the BLUE AREA

Welcome Desk

Go to FLOOR 0 to access GREEN AREA
Welcome Desk, Poster Sessions,
Coffee-Breaks, Lunch Area, Internet Area
and other Meeting Rooms

Plenary Room

Program Layout

Monday 23		Tuesday 24		Wednesday 25		Thursday 26		Friday 27	
		08:30	Welcome Desk / Registration	08:30	Welcome Desk / Registration	08:30	Welcome Desk / Registration		
		09:00	Opening Session	09:00	Session 3	09:00	Session 6	09:00	WD / Registration
		09:15	Panel					09:15	Session 9
								10:15	Posters Session 3
		10:30	Coffee-Break	10:30	Coffee-Break	10:30	Coffee-Break	10:30	C.-Break
		10:45	Session 1	10:45	Session 4	10:45	Session 7	10:45	
								11:15	Keynote Lecture Geoffrey Charles Fox
		12:15	Keynote Lecture Luis M. Correia	12:15	Keynote Lecture Venu Govindaraju	12:15	Keynote Lecture Andreas Holzinger	12:15	Closing Session
								12:30	Farewell Cocktail
								13:00	
		13:15	Lunch	13:15	Lunch	13:15	Lunch		
		14:30	Session 2	14:30	Session 5	14:30	Session 8		
15:00	Welcome Desk / Registration								
		16:30	Coffee-Break	16:30	C.-Break	16:30	C.-Break		
		16:45	Keynote Lecture Sushil Jajodia	16:45	Posters Session 1	16:45	Posters Session 2		
17:30				17:30		17:30			
		17:45	Welcome Cocktail						
		18:15				18:15	Buses to Banquet		
							Social Event and Banquet		
						23:30	Buses back to hotel		

Final Program and Book of Abstracts

Contents

Contents

Tuesday Sessions

Opening Session ICETE
09:00 - 09:15 Room Plenary

Panel ICETE
09:15 - 10:30 Room Plenary

Paper 24 ICE-B
10:45 - 12:15 Room Dali
Parallel Session 1

3D Communities as Platforms for Developing Social Capital

Claudia Loebbecke
University of Cologne, Cologne, Germany

Paolo Depaoli
University of Urbino, Urbino, Italy

Marco De Marco
University Guglielmo Marconi, Rome, Italy

Keywords: Social Community, Social Capital, 3D, Empirical Analysis.

Abstract: 3D virtual communities, a particular form of platforms, have gained remarkable attention in theory and practice. Similarly, the well established concept of social capital, which describes resources becoming accessible and available through the connection and interaction between individuals on a platform, has regained prominence with the boom of social media. In this study, we investigate the development of social capital in 3D virtual communities. Adapting the model of Adler and Kwon (2002), we analyze the role of motivation, ability, opportunity, and integration fir constituting social capital in 3D virtual communities. Our empirical investigation conducted in 2008 and 2009 among users of two 3D virtual communities, one networking platform and one online gaming platform, suggests that only motivation and ability are generally important. We conclude that the sources of social capital depend on the specific type and user audience of a 3D virtual community as well as on the sophistication of the available tools in the particular 3D environment and the cultural openness of the network.

Paper 29 ICE-B
10:45 - 12:15 Room Dali
Parallel Session 1

Search Engine Optimization Meets e-Business A Theory-based Evaluation: Findability and Usability as Key Success Factors

Andreas Auinger, Patrick Brandtner
Upper Austria University of Applied Sciences, Steyr, Austria

Petra Großdeßner
BMD System Software, Steyr, Austria

Andreas Holzinger
Research Unit Human-Computer Interaction, Graz, Austria

Keywords: Search Engine Optimization, Usability, ISO Criteria, Eye Tracking, Usability Evaluation.

Abstract: What can not be found, can not be used. Consequently, the success of a Website depends, apart from its content, on two main criteria: its top-listing by search engines and its usability. Hence, Website usability and search engine optimization (SEO) are two topics of great relevance. This paper focusses on analysing the extent that selected SEO-criteria, which were experimentally applied to a Website, affect the website's usability, measured by DIN EN ISO 9241-110 criteria. Our approach followed (i) a theory-based comparison of usability-recommendations and SEO-measures and (ii) a scenario- and questionnaire-based usability evaluation study combined with an eye-tracking analysis. The findings clearly show that Website usability and SEO are closely connected and compatible to a wide extent. The theory-based measures for SEO and Web Usability could be confirmed by the results of the conducted usability evaluation study and a positive correlation between search engine optimization and Website usability could be demonstrated.

Paper 25 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 1

VLR Group Signatures How to Achieve Both Backward Unlinkability and Efficient Revocation Checks

Julien Bringer[1] and Alain Patey[1,2]
[1] *Morpho, Safran Group, Paris, France*
[2] *Télécom ParisTech, Paris, France*

Keywords: Group Signatures, Verifier-Local Revocation, Backward Unlinkability, Efficiency, Revocation Check.

Abstract: Verifier-Local Revocation (VLR) group signatures are a particular case of dynamic group signature schemes where the revocation process does not influence the activity of the signers. The verifiers use a Revocation List and in all known schemes, checking a signature requires a computational time linear in the number of revoked members. Usually, it requires one pairing per revoked user. Recently, Chen and Li proposed a scheme where Revocation Check uses exponentiations instead of pairings. In this paper, we first propose a correction of their scheme to enable a full proof of the traceability property and we succeed with a constant additional cost only to extend this tweaked scheme to ensure Backward Unlinkability (BU). This important property prevents the loss of anonymity of past signatures when a user is revoked. We thus obtain the scheme with the most efficient Revocation Check among VLR schemes enabling BU.

Paper 50	SECRYPT
10:45 - 12:15	Room Valencia
Parallel Session 1	

Security Policies in Dynamic Service Compositions

Julian Schütte[1], Hervais Simo Fhom[2] and Mark Gall[1]

[1] *Fraunhofer Institution for Applied and Integrated Security AISEC, Garching near Munich, Germany*

[2] *Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany*

Keywords: Service Composition, Policy Composition, Pervasive Systems.

Abstract: The paradigm of service composition emerged in the context of service oriented architectures, where it mainly referred to creating value-added services by combinitions of individual services. Nowadays, service composition is getting more and more dynamic and becomes part of pervasive systems. One of the major challenges in this context is to fulfill the security requirements of all involved parties without requiring human interaction to negotiate protection level agreements. In this paper, we propose an approach for composing access control decisions and obligations required by equitable policy domains on the fly. We show that our approach allows a policy-compliant collaboration without requiring the peers to reveal their individual rules and confirm its practicability by a prototype.

Paper 61	SECRYPT
10:45 - 12:15	Room Valencia
Parallel Session 1	

Towards Pervasive Cryptographic Access Control Models

Mikko Kiviharju

Finnish Defence Forces Technical Research Centre, Lakiala, Finland

Keywords: Cryptographic Access Control, CAC, Permissions, Access Control, CBIS.

Abstract: Access control lies at the heart of any technical information security and information assurance system. Access control is traditionally enforced by reference monitors, which are assumed to be able to reliably monitor and mediate all traffic from users to objects. An alternative view to enforcement is cryptography, referred to as cryptographic access control (CAC). CAC has gained popularity with the emergence of distributed computing, especially cloud computing and "everything as a service". CAC is not a formal model, but an enforcement paradigm. In this paper we propose an extension to the current CAC framework and discuss the limits, where it is in general feasible to extend CAC as a paradigm over reference monitors.

Paper 62	SECRYPT
10:45 - 12:15	Room Valencia
Parallel Session 1	

Cryptographic Enforcement of Access Control while Mitigating Key Sharing

Keith B. Frikken

Miami University, Oxford, U.S.A.

Keywords: Hierarchical-based Access Control, Cryptographic Enforcement, Mitigating Key Sharing.

Abstract: In this paper, we consider the well-studied problem of cryptographic enforcement of hierarchical-based access control. While this problem is well-studied, a significant drawback to prior approaches is that if a corrupt user shares his key, then any user can access the content of the corrupt user. This is particularly damaging since it is not possible to determine the identity of the corrupt user, and almost all previous schemes require some rekeying in order to revoke a key. To mitigate this key sharing attack, we propose a new model for cryptographic enforcement: Identity-based key management (IBKM). In this framework, each key is associated with an identity and this identity is required to access content. This allows the system to trace the source of key leakage and to revoke users without rekeying. The main disadvantage of this framework is the scheme does not have the ability to provide anonymous access, but it can be used to provide pseudonymous access. The main contributions of this paper are formal definitions for IBKM and schemes for achieving IBKM.

Paper 47	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 1	

Consumer Propensity and Location Analysis based Real-time Location Tracing Advertisement Service Design and Implementation Real-time Location based Advertisement System

Daehee Won, Yoonsoo Kim, Hangki Joh, Intae Ryoo and Doungyung Suh

Kyunghee University, Yong-in, Korea, Republic of

Keywords: Advertisement Service, Location based Service, Consumer Propensity, Real Time Location based Service.

Abstract: While distributing Android free of charge, Google intended to expose its advertisements on the platforms to seize users' eyes and make profits. However, smart phones are kept in bags or pockets during most of the time instead of showing screens in front of users' eyes. If the time during which users' eyes cannot be seized becomes longer advertisement effects will decrease as much. In this study, in order to solve these problems, consumers' movement paths are grasped using continuous screens based on the results of analyses of consumer propensity to replay advertisement images. Advertisement image replay lists are composed of related advertisements based on the key words set by consumers. The relevant project was named as shADow meaning Advertisements that follow like shadows.

Paper 80	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 1	

Centroid-based Clustering for Student Models in Computer-based Multiple Language Tutoring

Maria Virvou, Efthymios Alepis and Christos Troussas

University of Piraeus, Piraeus, Greece

Keywords: User Modelling, User Clustering, Multiple Language Learning, Intelligent Tutoring Systems, K-means Algorithm.

Abstract: This paper proposes an approach for the initialization and the construction of student models in an intelligent tutoring system that teaches multiple foreign languages. The basic concept for the construction of the initial user models is to assign each new student to a model with similar characteristics. As it is quite easy to understand that a tutoring system has rather little information about its new users, our effort is to provide as much information as possible for each specific user relying on the user's initial data. To this end, a machine learning algorithm, namely k-means, is responsible for creating clusters relying on the system's pre-entered past data and as a next step, each new entry is assigned to the nearest centroid.

Paper 81	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 1	

Influence of Different Phoneme Mappings on the Recognition Accuracy of Electrolaryngeal Speech

Petr Stanislav and Josef V. Psutka

University of West Bohemia, Pilsen, Czech Republic

Keywords: Automatic Speech Recognition, Laryngectomees, Electrolaryngeal Speech, Phoneme Mapping.

Abstract: This paper presents the initial steps towards building speech recognition system that is able to efficiently process electrolaryngeal substitute speech produced by laryngectomees. Speakers after total laryngectomy are characterized by restricted aero-acoustic properties in comparison with normal speakers and their speech is therefore far less intelligible. We suggested and tested several approaches to acoustic modeling within the ASR system that would be able to cope with this lower intelligibility. Comparative experiments were also performed on the healthy speakers. We tried several mappings that unify unvoiced phonemes with their voiced counterparts in the acoustic modeling process both on monophone and triphone level. Systems using zerogram and trigram language models were evaluated and compared in order to increase the credibility of the results.

Paper 82	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 1	

Large Scale Similar Song Retrieval using Beat-aligned Chroma Patch Codebook with Location Verification

Yijuan Lu
Texas State University, San Marcos, U.S.A.

Joseph E. Cabrera
Texas A&M University, College Station, U.S.A.

Keywords: Music Information Retrieval, Similar Song Search.

Abstract: With the popularity of song search applications on Internet and mobile phone, large scale similar song search has been attracting more and more With the popularity of song search applications on Internet and mobile phone, large scale similar song search has been attracting more and more attention in recent years. Similar songs are created by altering the volume levels, timing, amplification, or layering other songs on top of an original song. Given the large scale of songs uploaded on the Internet, it is demanding but challenging to identify these similar songs in a timely manner. Recently, some state-of-the-art large scale music retrieval approaches represent songs with a bag of audio words by quantizing local features, such as beat-chroma patches, solely in the feature space. However, feature quantization reduces the discriminative power of local features, which causes many false audio words matches. In addition, the location clues among audio words in a song is usually ignored or exploited for full location verification, which is computationally expensive. In this paper, we focus on similar song retrieval, and propose to utilize beat-aligned chroma patches for large scale similar song retrieval and apply location coding scheme to encode the location relationships among beat-aligned chroma patches in a song. Our approach is both efficient and effective to discover true matches of beat chroma patches between songs with low computational cost. Experiments in similar songs search on a large song database reveal the promising results of our approach.

Paper 6	WINSYS
10:45 - 12:15	Room Velazquez
Parallel Session 1	

Quality of Experience Evaluation for Data Services over Cellular Networks

Gerardo Gómez, Esther de Torres
University of Malaga, Malaga, Spain

Javier Lorca, Raquel García, Quiliano Pérez, Estefanía Arias
Telefonica I+D, Madrid, Spain

Keywords: Quality of Experience, MOS, Performance Evaluation, Quality of Service.

Abstract: This paper presents an end-to-end service performance evaluation method that is able to estimate both the Quality of Service (QoS) and Quality of Experience (QoE) associated to different data services over cellular networks. A set of performance indicators are evaluated at each layer of the terminal's protocol stack following a bottom-up process from the physical layer up to the application layer. Then, specific utility functions for each data service are used to map QoS into QoE in terms of Mean Opinion Score (MOS). Three different data services (web browsing, video YouTube and Skype-based voice over IP) have been evaluated in this paper under different network and terminal configurations. Performance results show that the MOS associated to a particular data service is largely affected by the radio level performance (error rate, throughput and delay), so proper protocols' configuration is a key issue to maximize the QoE.

Paper 7	WINSYS
10:45 - 12:15	Room Velazquez
Parallel Session 1	

Authentication Optimization for Vertical Handover in Heterogeneous Wireless Networks

Ikram Smaoui[1], Faouzi Zarai[1], Mohammad S. Obaidat[2] and Lotfi Kamoun[1]
[1] *University of Sfax, Sfax, Tunisia*
[2] *Monmouth University, West Long Branch, U.S.A.*

Keywords: Authentication, Seamless Handover, Security, EAP-AKA Protocol, Heterogeneous Networks.

Abstract: In this paper, we present a scheme for reducing vertical handover delay in heterogeneous wireless networks by optimizing the network access authentication procedure as it is a heavy burden due to its latencies and overhead. Indeed, optimizing the authentication procedure while at the same time providing the same or best level of security represents a key factor in the design of the next generation of heterogeneous wireless networks. In this context, the aim of our work in this paper is to provide a security framework accounting for heterogeneity in wireless access networks without degrading the security level currently provided by each wireless system. We also demonstrate using simulation analysis the handover performance improvement provided by our proposed security frame work.

Paper 53 WINSYS
10:45 - 12:15 Room Velazquez
Parallel Session 1

Knowledge Acquisition System based on JSON Schema Implementation of a HCI for Actuation of Biosignals Acquisition Systems

Nuno Costa[1], Tiago Araujo[1,2], Neuza Nunes[2] and Hugo Gamboa[1,2]

[1] *Universidade Nova de Lisboa, Lisbon, Portugal*

[2] *PLUX - Wireless Biosignals, S.A., Lisbon, Portugal*

Keywords: Knowledge Acquisition System, Human Computer Interaction, Ontology, Schema Language.

Abstract: Large amounts of data, increasing every day, are stored and transferred through the internet. These data are normally weakly structured making information disperse, uncorrelated, non-transparent and difficult to access and share. Semantic Web, proposed by the World Wide Web Consortium (W3C), addresses this problem by promoting semantic structured data, like ontologies, enabling machines to perform more work involved in finding, combining, and acting upon information on the web. Pursuing this vision, a Knowledge Acquisition System was created, written in JavaScript using JavaScript Object Notation (JSON) as the data structure and JSON Schema to define that structure, enabling new ways of acquiring and storing knowledge semantically structured. A novel Human Computer Interaction framework was developed with this knowledge system, enabling the end user to, practically, configure all kinds of electrical devices and control them. With the data structured by a Schema, the software becomes robust, error – free and human readable. To show the potential of this tool, the end user can configure an electrostimulator, surpassing the specific use of many Electrophysiology software. Therefore, we provide a tool for clinical, sports and investigation where the user has the liberty to produce their own protocols by sequentially compile electrical impulses.

12:15 - 13:15 Room Plenary
A Perspective of the Networks of the Future and Smart Cities
Keynote Speaker: Luis M. Correia

A Perspective of the Networks of the Future and Smart Cities

Luis M. Correia

IST/IT-Technical University of Lisbon, Lisbon, Portugal

Abstract: A parallel in the evolution between mobile and wireless communications and other areas (computers and cars) will be presented, in an attempt to identify possible directions for systems future evolution. A look into already existing technologies will enable to establish a perspective for future user interface devices and services (e.g., information access, Internet of Things, and geo-location). Then, potential services are identified, after which research challenges for mobile and wireless communications networks are addressed (e.g., network virtualisation, cloud networking, and networks of information). Smart Cities are taken as an integration example, as well as a perspective of application to other key sectors (e.g., health, transport, and energy). The link with other areas, and impact on regulation, standardisation, and policy matters are presented at the end.

Tuesday, 24

Paper 5 DCNET
14:30 - 16:30 Room Sevilla
Parallel Session 2

A Cross-layer Design for Video Transmission with TFRC in MANETs

George Adam[1,2], Christos Bouras[1,2], Apostolos Gkamas[3], Vaggelis Kapoulas[1,2] and Georgios Kioumourtzis[4]

[1] *Computer Technology Institute & Press "Diophantus", Patras, Greece*

[2] *Univ. of Patras, Patras, Greece*

[3] *University Ecclesiastical Academy of Vella, Ioannina, Greece*

[4] *Center for Security Studies, Athens, Greece*

Keywords: MANETs, Multimedia, Video Transmission, TFRC, Cross-layer, AODV, SNR.

Abstract: Mobile Ad hoc NETworks (MANETs) are becoming more essential to wireless communications due to growing popularity of mobile devices. However, MANETs do not seem to effectively support multimedia applications and especially video transmission. In this work, we propose a cross-layer design that aims to improve the performance of video transmission using TCP Friendly Rate Control (TFRC). Our design provides priority to video packets and exploits information from the MAC layer in order to improve TFRC's performance. The proposed cross-layer mechanism utilizes Signal to Noise Ratio (SNR) measurements along the routing path, in order to make the route reconstruction procedure more efficient. Simulation results show that both the use of traffic categorization and the SNR utilization lead to important improvements of video transmission over the mobile Ad hoc network. More specifically, simulations indicate increased average Peak Signal to Noise Ratio (PSNR) for the received video, increased throughput and packet delivery ration, as well as reduced average end-to-end delay.

Paper 9 DCNET
14:30 - 16:30 Room Sevilla
Parallel Session 2

Study on a Fast OSPF Route Reconstruction Method under Network Failures

Hiroki Doi

Central Research Institute of Electric Power Industry, Komae-shi, Japan

Keywords: OSPF, Router Dead Interval, Delay Time, Route, Designated Router.

Abstract: The Great East Japan Earthquake occurred onMarch 11, 2011. Many Japanese people and Japanese companies were damaged by the disaster. Also, network failures occurred over a wide area because many facilities of commercial ISPs (Internet Service Providers) were damaged. Thus, there is a need to reexamine the disaster estimation and reconstruct a robust network system against disasters in Japan. The network must have higher reliability and fast recovery. Although OSPF (Open Shortest Path First) is used widely on networks, it has a router dead interval problem. If a (backup) designated router has stopped operation due to failure, the other OSPF routers miss the designated router and try to find it by multiple hello packets. The OSPF routers await a hello packet acknowledgment from the designated router for the router dead interval. After the router dead interval, those routers can recognize that the designated router has ceased the operation. The router dead interval is 40 seconds. This interval time is not only long for many real-time applications but also involves huge buffering of data and a burst of traffic after the router reconstruction. To avoid the router dead interval, we propose a fast method of designated router detection by enhanced OSPF. In this report, we show how our method reduces the route reconstruction time from 45 seconds to 10 or less on OSPF networks.

Paper 11 DCNET
14:30 - 16:30 Room Sevilla
Parallel Session 2

Computational Intelligence Applied to Monitor Bird Behaviour

D. F. Larios[1], C. Rodríguez[2], J. Barbancho[1], M. Baena[3], F. Simón[1], J. Marín[2], C. León[1] and J. Bustamante[2]

[1] *University of Seville, Seville, Spain*
[2] *Doñana Biological Station (EDB-CSIC), Seville, Spain*
[3] *Doñana Biological Station, Seville, Spain*

Keywords: Neuronal Network, Computational Intelligence, Data Fusion, Environmental Monitoring, Sensor Networks.

Abstract: The best way to obtain relevant information about the behaviour of animals is direct observation (of individuals). However, traditional close-up observations can interfere on the behaviour, and taking biometric measurements requires the capture of individuals, which also causes stress. This paper describes an automatic motoring system for birds breeding in nest boxes. The main goal is to significantly increase the amount and quality of data acquired on bird behaviour without stressing the individuals or interfering. This system is based in an interconnected embedded sensor network, which permits sharing this valuable information with researchers all over the world through the internet. Each device of the network is a smart nest-box that allows a cross-validation of sensor information and data quality. This system has been evaluated for the specific case of a lesser kestrel breeding colony in Southern Spain. The lesser kestrel is an insectivorous migratory falcon that readily accepts nest-boxes. The system has been named HORUS and the results obtained from a year experiment demonstrate the efficiency of this approach.

Paper 26 ICE-B
14:30 - 16:30 Room Dali
Parallel Session 2

The User-journey in Online Search An Empirical Study of the Generic-to-Branded Spillover Effect based on User-level Data

Florian Nottorf, Andreas Mastel and Burkhardt Funk

Leuphana University, Lüneburg, Germany

Keywords: Online Search, Online Advertising, Consumer Behavior, Query Log, Spillover.

Abstract: Traditional metrics in online advertising such as the click-through rate often take into account the users' search activities separately and do not consider any interactions between them. In understanding online search behavior, this fact may favor a certain group of search type and, therefore, may mislead managers in allocating their financial spending efficiently. We analyzed a large query log for the occurrence of user-specific interaction patterns within and across three different industries (clothing, healthcare, hotel) and were able to show that users' online search behavior is indeed a multi-stage process, whereas e.g. a product search for sneakers typically begins with general, often referred to as generic, keywords which becomes narrowed as it proceeds by including more specific, e.g. brand-related ("sneakers adidas"), keywords. Our method to analyze the development of users' search process within query logs helps managers to identify the role of specific activities within a respective industry and to allocate their financial spending in paid search advertising accordingly.

Paper 34	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 2	

On the Development of Smart Adaptive User Interfaces for Mobile e-Business Applications Towards Enhancing User Experience – Some Lessons Learned

Andreas Holzinger, Michael Geier and Panagiotis Germanakos

Medical University Graz, Graz, Austria

Keywords: Adaptive User Interfaces, Smart Adaptation, Mobile e-Business Applications, Performance.

Abstract: Mobile end users usually work in complex and hectic environments, consequently for mobile e-Business applications the design and development of context aware, smart, adaptive user interfaces is getting more and more important. The main goal is to make the user interface so simple that the end users can concentrate on their tasks – not on the handling of the application, the main challenge is its adaptation to the context. A possible solution is smart adaptation. Consequently, developers need to know the limits of both context and systems and must be aware of mobile end users different interaction. In this paper, we follow the hypothesis that simple user interfaces enhance performance and we report about some lessons learned during the design, development and evaluation of a smart, adaptive user interface for an e-Business application.

Paper 51	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 2	

Strategic Planning in Highly Dinamic Competitive Contexts A Study of Italian Mobile Network Operators

Antonio Ghezzi[1], Marcelo Nogueira Cortimiglia[2], Alejandro Germán Frank[2] and Raffaello Balocco[1]

[1] *Politecnico di Milano, Milan, Italy*

[2] *Federal University of Rio Grande do Sul, Porto Alegre, Brazil*

Keywords: Strategic Management, Technology Management, Mobile Telephony.

Abstract: Strategic management formulation and implementation in highly dynamic competitive scenarios is a challenging task. This is the case of the Mobile Telephony segment of the Information and Communication Technology (ICT) industry. In this competitive setting, potentially disruptive changes in both marketing and technological dimensions are the norm, as attested by the recent decrease in voice-related revenues by Mobile Network Operators (MNO) and the consequent rise in mobile data traffic. In this context, this paper aims to contribute to the literature on Strategic Technology Management by proposing an interpretative framework to support strategic decision making in dynamic, competitive contexts characterized by disruptive changes in both technology and business dimensions. The proposed framework is based on empirical research conducted at the four MNOs operating in Italy and allows identifying drivers of potentially disruptive change and their implications on a firm's business model. The framework use is illustrated through the analysis of the Italian Mobile Telephony industry. Finally, the research also highlighted the main strategic routes MNOs have at their disposal to face the turbulent competitive times ahead. These include specific strategic actions to cope with the issues of mobile bandwidth scarcity and decreasing voice-related revenues. A summary of MNOs future strategic positioning options is also provided.

Paper 40	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 2	

Constructing Secure-channel Free Searchable Encryption from Anonymous IBE with Partitioned Ciphertext Structure

Keita Emura

National Institute of Information and Communications Technology (NICT), Tokyo, Japan

Mohammad Shahriar Rahman

University of Asia Pacific, Dhaka, Bangladesh

Keywords: Adaptive Secure-channel Free Public Key Encryption Scheme with Keyword Search, IBE with Partitioned Ciphertext Structure.

Abstract: As an extension of public key encryption with keyword search (PEKS), secure channel free PEKS (SCF-PEKS) has been considered. Generic construction of SCF-PEKS (with adaptive security) from strongly existentially unforgeable one-time signature, selective-tag CCA secure tag-based encryption (TBE) and anonymous identity-based encryption (IBE) has been proposed in ISC2011. Since this construction follows the double encryption, where a ciphertext of anonymous IBE is encrypted by TBE, hybrid encryption is applied because usually the ciphertext space of IBE is not equal to the plaintext space of TBE. In this paper, we show that hybrid encryption is not necessary as long as previously-known anonymous IBE schemes are used as a building tool of adaptive SCF-PEKS. Our result leads to a composability of IBE schemes whether they can be applied for constructing adaptive SCF-PEKS or not. Moreover, since we can exclude DEM part, our construction is efficient compared to the original one.

Paper 66	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 2	

High-throughput Hardware Architectures of the JH Round-three SHA-3 Candidate An FPGA Design and Implementation Approach

George S. Athanasiou[1], Chara I. Chalkou[1], D. Bardis[1], Harris E. Michail[2], George Theodoridis[1] and Costas E. Goutis[1]

[1] *University of Patras, Patras, Greece*

[2] *Cyprus University of Technology, Lemesos, Cyprus*

Keywords: Security, Cryptography, Hash Functions, SHA-3, JH, High-throughput Implementation, Hardware, FPGA.

Abstract: Hash functions are exploited by many cryptographic primitives that are incorporated in crucial cryptographic schemes and commercial security protocols. Nowadays, there is an active international competition, launched by the National Institute of Standards and Technology (NIST), for establishing the new hash standard, SHA-3. One of the semi-finalists is the JH algorithm. In this paper, two high throughput hardware architectures of the complete JH algorithm are presented. The difference between them is the existence of 3 pipeline stages at the second one. They both are designed to support all the possible versions of the algorithm and are implemented in Xilinx Virtex-4, Virtex-5, and Virtex-6 FPGAs. Based on the experimental results, the proposed architectures outperform the existing ones in terms of Throughput/Area factor, regarding all FPGA platforms and JH algorithm's versions.

Paper 72	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 2	

Private Outsourcing of Matrix Multiplication over Closed Semi-rings

Mikhail J. Atallah[1], Keith B Frikken[2] and Shumiao Wang[1]

[1] *Purdue University, West Lafayette, U.S.A.*

[2] *Miami University, Oxford, U.S.A.*

Keywords: Privacy-preserving Protocols, Private Outsourcing.

Abstract: Many protocols exist for a client to outsource the multiplication of matrices to a remote server without revealing to the server the input matrices or the resulting product, and such that the server does all of the super-linear work whereas the client does only work proportional to the size of the input matrices. These existing techniques hinge on the existence of additive and multiplicative inverses for the familiar matrix multiplication over the $(+,*)$ ring, and they fail when one (or both) of these inverses do not exist, as happens for many practically important algebraic structures (including closed semi-rings) when one or both of the two operations in the matrix multiplication is the "$\min$" or "max" operation. Such matrix multiplications are very common in optimization. We give protocols for the cases of $(+, \min)$ multiplication, $(\min, max)$ multiplication, and of $(\min, +)$ multiplication; the last two cases are particularly important primitives in many combinatorial optimization problems.

Paper 91 SECRYPT
14:30 - 16:30 Room Valencia
Parallel Session 2

DDoS Detection with Information Theory Metrics and Netflows A Real Case

Domenico Vitali[1], Antonio Villani[2], Angelo Spognardi[1], Roberto Battistoni[1] and Luigi V. Mancini[1]

[1] *"Sapienza" University of Rome, Rome, Italy*

[2] *University of Roma Tre, Rome, Italy*

Keywords: DDoS, Attack Detection, Information Divergence, Relative Entropy, Autonomous System, Internet Security.

Abstract: Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) constitute one of the main issues for critical Internet services. The widespread availability and simplicity of automated stressing tools has also promoted the voluntary participation to extensive attacks against known websites. Today the most effective (D)DoS detection schemes are based on information theory metrics, but their effectiveness is often evaluated with synthetic network traffic. In this work we present a comparison of the main metrics proposed in the literature carried on a huge dataset formed by real netflows. This comparison considers the ability of each metric to detect (D)DoS attacks at an early stage, in order to launch effective and timely countermeasures. The evaluation is based on a large dataset, collected from an Italian transit tier II Autonomous System (AS) located in Rome. This AS network is connected to all the three main network infrastructures present in Italy (Commercial, Research and Public Administration networks), and to several international providers (even for Internet transit purposes). Many attempted attacks to Italian critical IT infrastructures can be observed inside the network traffic of this AS. Several publicly declared attacks have been traced and many other malicious activities have been found by ex-post analysis.

Paper 10 WINSYS
14:30 - 16:30 Room Velazquez
Parallel Session 2

From Farm to Fork: Traceability based on RFID A Proposal for Complete Traceability in the Wine Sector

Iñigo Cuiñas, Isabel Expósito, José Antonio Gay-Fernández, Ana V. Alejos and Manuel G. Sánchez

Universidade de Vigo, Vigo, Spain

Keywords: RFID, Traceability, Tag, Wine.

Abstract: This paper highlights the objectives and activities of the European project "RFID from Farm to Fork", which is focused on the food industry traceability. The final goal is to extend the traceability information to the final consumer, so these persons could feel the confidence on the food origin like our grandparents did when they lived in a less globalised World. The activities of the project in a winery at Ribeiro denomination of origin (Spain) at both vineyards (by means of wireless sensor networks) and the wine production process (by RFID technology) are also presented along the paper, in order to show some of the project outcomes.

Paper 14 WINSYS
14:30 - 16:30 Room Velazquez
Parallel Session 2

Using Radio Frequency Identification Technology to Track Individual Wine Bottles

Isabel Expósito, Iñigo Cuiñas and Paula Gómez

Universidade de Vigo, Vigo, Spain

Keywords: Radio Frequency Identification, Wine Traceability, Bottle Tracking, Tag Readability.

Abstract: Radio Frequency Identification (RFID) technology has been tested and it is now proposed to be used in applications as food traceability, instead of the traditional barcode, as that could get advantages of its inherent characteristics: automatic management and distance readability. Among food industries, wine production represents an added value sector and so it would be a target to implement RFID. Wine bottles present some problems to the radio propagation, as liquids are not electromagnetically friend materials. Thus, a large radio electric measurement campaign has been performed in order to deal with the possible mismatches in using this technology to trace wine bottles from the wine cellars to the final consumer. The performance of different RFID tag models, as well as the effect of the wine content within the bottle, is analysed along the paper, trying to identify the better technological solution. The tests indicate that the use of RFID methods would be suitable to allow the consumer to obtain complete traceability information from each wine bottle, and the producer to track its products. The proposal opens the door to new possibilities in the relationship between consumer and producer, by demonstrating the possibility of using a new technology in a traditional market.

Paper 23	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 2	

Performance Evaluation for TCP in Tactical Mobile Ad Hoc Networks

Jonas Karlsson[1], Velizar G. Dimitrov[2], Andreas Kassler[1], Anna Brunstrom[1], Jan Nilsson[3] and Anders Hansson[3]

[1] *Karlstad University, Karlstad, Sweden*

[2] *Technical University of Sofia, Sofia, Bulgaria*

[3] *Swedish Defence Research Agency (FOI), Linköping, Sweden*

Keywords: MANET, TCP, Tactical Networks, TDMA.

Abstract: Tactical networks are used in military and rescue operations to provide timely and accurate information to operating teams. Tactical networks have traditionally used long distance narrow band radio links. However, although these links provide robust real-time communication the limited bandwidth makes them less suited for high data-rate applications. To support high-data rate TCP applications such as providing digital images and maps, emerging tactical networks use shorter range but higher data-rate wide band radio links and multihop. Due to the requirement of cheap up-front cost, most MANET research has focused on Carrier Sense Multiple Access (CSMA) networks. However, in tactical networks, where bounded delays are important, Time Division Multiple Access (TDMA) can give better possibility to support the Quality of Service needed for real-time communication. The purpose of this paper is to assess and compare the throughput of three state-of-the-art TCP versions and two routing protocols over TDMA based MANETs.

Paper 25	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 2	

Design of Soft Computing based Black Hole Detection in MANET

D. Vydeki, K. S. Sujatha

Easwari Engineering College, Ramapuram, Chennai, India

R. S. Bhuvaneswaran

Anna Univesity, Chennai, India

Keywords: Intrusion Detection, Black Hole, Fuzzy Logic, Genetic Algorithm.

Abstract: Mobile Ad hoc Networks (MANETs) are more vulnerable to attacks than the generic wireless network due to the lack of an underlying infrastructure and shared medium. Intrusion Detection System (IDS) provides an enhanced level of security to such networks. Application of Soft computing techniques to the detection process is proved to be more suitable as they have human-like decision-making capabilities. This paper proposes a hybrid intrusion detection system for MANETs that detects black hole attack, by combining anomaly and specification-approaches of IDS. The proposed system aims at designing two different IDS using the two fundamental soft computing mechanisms such as, Fuzzy and Genetic Algorithm (GA). The design of each IDS is tested with simulated MANETs for various traffic conditions. The performance of each system is compared based on the true and false positive rates. The experimental results show that the fuzzy based system produces 81.8% true positive rate and the GA based system results in a 100% efficient detection.

Paper 32	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 2	

Improved NetArgus A Suite of Wi-fi Positioning & SNMP Monitor

Tryfon Theodorou[1], George Violettas[1], Antigoni Polychroniadou[2] and Christos Georgiadis[1]

[1] *University of Macedonia, Thessaloniki, Greece*

[2] *Royal Holloway University of London, Egham, U.K.*

Keywords: Wi-fi Positioning, Kalman Filter, SNMP, FSPL, RTLS.

Abstract: In this paper, field research was conducted in order to enrich and strengthen the “NetArgus” application that is able to monitor either a wired or a wireless network with all its possible aspects. Original algorithms were implemented in an effort to find the position of a moving station utilizing the

signal level of wireless local area network (WLAN) devices. Exhausting sampling and research were done, in order to resolve various practical problems associated with the signal level of the wireless stations as well as the involved hardware. Various flaws and omissions of 802.11x protocols were discovered, such as the lack of definition of the signal level and its width range. Moreover, a plethora of positioning practical problems has been adequately managed. Hence, an application was constructed to draw paths and manipulate proper information from various network moving clients, using the Simple Network Management Protocol (SNMP) as well as low level operating system libraries. Last but not least, "Kalman Filter" was implemented and fully tested in order to correct the positioning unavoidable mistakes.

16:45 - 17:45 Room Plenary
A Mission-centric Framework for Cyber Situational Awareness
Keynote Speaker: Sushil Jajodia

A Mission-centric Framework for Cyber Situational Awareness

Sushil Jajodia

George Mason University Fairfax, Fairfax, U.S.A.

Abstract: Today, when a security incident occurs, the top three questions security administrators would ask are in essence: What has happened? Why did it happen? What should I do? Answers to the first two questions form the core of Cyber Situational Awareness. Whether the last question can be satisfactorily answered is greatly dependent upon the cyber situational awareness capability of an enterprise.

In my talk, I will describe a framework to securely operate missions within networks that are imperfect and vulnerable to multiple types of cyber attacks. The key elements of the framework are as follows: First, we introduce the notion of generalized dependency graph which captures how network components, at different levels of abstraction, depend on each other. Second, we extend the classical definition of attack graph to incorporate probabilistic knowledge of the attacker's behavior. Finally, we introduce the notion of attack scenario graph which integrates dependency and attack graphs.

Wednesday Sessions

Paper 16 ICE-B
09:00 - 10:30 Room Dali
Parallel Session 3

Resilient Sustainable Supply Chain Management A Conceptual Framework

Maruf H. Chowdhury, Mohammed Naim A. Dewan and Mohammed A. Quaddus
Curtin University, Perth, Australia

Keywords: Resilience, Sustainability, Supply Chain, Disruption.

Abstract: A resilient-sustainable supply chain has become a unanimously important research agenda in business as global supply chain is facing an increased number of risks and disruptions. In such a situation in order to be competitive and sustainable a supply chain needs to be resilient. Literature related to supply chain sustainability and resilience in an integrated fashion is sparse, rather issues are presented separately and no empirical work has yet been done to develop a resilient-sustainable supply chain management (RSSCM) framework. A resilient-sustainable supply chain management (RSSCM) framework is formulated and measurement scale for resilience and sustainability is developed in this study. The study combines the stakeholder theory and resource based view in line with sustainability and resilience in developing a theoretically grounded, comprehensive framework of resilient-sustainable supply chain management.

Paper 39 ICE-B
09:00 - 10:30 Room Dali
Parallel Session 3

Developing a Conceptual Framework to Structure an IT Organization using an Ontology Engineering Methodology

Nelson Gama[1], Lukasz Ostrowski[2] and Miguel Mira da Silva[1]
[1] *Instituto Superior Técnico, Lisboa, Portugal*
[2] *Dublin City University, Dublin, Ireland*

Keywords: IT Organization, Alignment, Conceptual Framework, Ontology Engineering Process, Concept Definition, Concept Maps.

Abstract: Organizations are struggling to adopt practices that allow the best results trying to achieve alignment between IT and an organization's concepts and dimensions, pursuing efficiency and effectiveness. Therefore, the structure of an IT organization is fundamental. However, despite the recognized importance of IT organizational structure and the efforts made in the development of disparate perspectives and relationships, no relevant references about its structure are found, and the existent ones are far from satisfactory. There is neither a single framework nor one relating to what we consider to be relevant or clearly dominant. This paper proposes the use of ontology engineering methodology to identify and enumerate concepts and develop a conceptual framework in order to structure and establish a relationship among concepts within an IT organization, which will allow the definition of an IT organization.

Paper 47 ICE-B
09:00 - 10:30 Room Dali
Parallel Session 3

Evaluation of Maturity Models for Business Process Management Maturity Models for Small and Medium-sized Enterprises

Johannes Britsch
University of Mannheim, Mannheim, Germany

Rebecca Bulander, Frank Morelli
Pforzheim University of Applied Sciences, Pforzheim, Germany

Keywords: Business Process Management, Maturity Model, Evaluation, Small and Medium-sized Enterprises, Anything Relationship Management.

Abstract: This paper contains an appraisal of selected maturity models for BPM. Business process maturity models in general offer precise process definitions, repeatable process operations, the integration and interaction with linked processes, as well as the measurability and controlling of the process flows. Maturity models provide small and medium-sized enterprises (SMEs) with clear structures for organizational changes. The intention of the analysis is to support SMEs by choosing an appropriate framework that helps to design "to-be" business processes based on a continuous and comprehensive assessment concept. However, due to their size and limited resources, SMEs also have special requirements regarding maturity models. The paper describes the evaluation results of well-known maturity models for SMEs and the advantages and dis-advantages of the models relating to a concrete scenario in the area of Anything Relationship Management.

Paper 50 ICE-B
09:00 - 10:30 Room Dali
Parallel Session 3

Leveraging the Software Ecosystem Towards a Business Model Framework for Marketplaces

Tobias Weiblen, Andrea Giessmann, Amir Bonakdar and Uli Eisert

SAP Research, St. Gallen, Switzerland

Keywords: Business Model, Marketplace, Software Industry, Software Ecosystems, e-Commerce.

Abstract: Software platforms in the form of marketplaces like Salesforce.com‘s AppExchange, Netsuite‘s SuiteApp or SAP‘s Commercial Platform are changing the way how software and services are distributed, consumed, and priced. Technical innovations in the underlying platforms receive high attention, while innovative business models that build on and commercialize a flourishing ecosystem are neglected. In this paper we investigate the question which marketplace business model options are available to software platform owners that want to commercialize their ecosystem’s products and services. We present a framework of ten possible models that is derived from both theory and practice. The options are clustered by the required level of product/service standardization to guide the choice of business model. The framework may serve decision makers as a starting point for their business model innovation plans.

Paper 58 SECRYPT
09:00 - 10:30 Room Valencia
Parallel Session 3

Homomorphic Primitives for a Privacy-friendly Smart Metering Architecture

Benjamin Vetter, Osman Ugus, Dirk Westhoff

HAW Hamburg, Hamburg, Germany

Christoph Sorge

University of Paderborn, Paderborn, Germany

Keywords: PET for Smart Metering, Homomorphic MACs, Homomorphic Encryption.

Abstract: We propose a privacy-friendly smart metering architecture which is yet flexible enough to serve various future third party energy services. Our secure architecture may be deployed as a cloud service and allows processing of SQL queries on encrypted measurements, providing aggregated results in a most flexible manner. A combination of homomorphic encryption and homomorphic MACs provides confidentiality of the users’ energy consumptions, allowing integrity checks and enhanced SQL-queries on encrypted data. Our extensive performance analysis shows that our approach is promising with respect to storage and computational overhead.

Paper 59 SECRYPT
09:00 - 10:30 Room Valencia
Parallel Session 3

Flexible Redactable Signature Schemes for Trees Extended Security Model and Construction

Henrich C. Pöhls, Kai Samelin, Hermann de Meer and Joachim Posegga

University of Passau, Passau, Germany

Keywords: Redactable Signatures, Malleable Signatures, Trees.

Abstract: At ISPEC’12, *Samelin* et al. show that the redactable signature scheme introduced at VLDB’08 by *Kundu* and *Bertino* does not always preserve the structural integrity of the tree signed. In particular, they show how redaction of non-leaves promotes descendants and allows a third party to add new edges to the signed tree. This alters the semantic meaning of the tree and is not acceptable in certain scenarios. We generalize the model, such that it offers the signer the flexibility to sign trees where every node is transparently redactable. This includes intermediates nodes, i.e, to allow redacting a hierarchy, but also the tree’s root. We present a provably secure construction, where this possibility is given, while remaining under explicit control of the signer. Our security model is as strong as *Brzuska* et al.’s introduced at ACNS’10. We have implemented our secure construction and present a detailed performance analysis.

Paper 73 SECRYPT
09:00 - 10:30 Room Valencia
Parallel Session 3

Extension of de Weger’s Attack on RSA with Large Public Keys

Nicolas T. Courtois, Theodosis Mourouzis

University College London, London, U.K.

Pho V. Le

University College London, London, U.S.A.

Keywords: RSA, Cryptanalysis, Weak Keys, Exponent Blinding, Wiener’s Attack, de Weger’s Attack, Large Public Keys.

Abstract: RSA cryptosystem (Rivest et al., 1978) is the most widely deployed public-key cryptosystem for both encryption and digital signatures. Since its invention, lots of cryptanalytic efforts have been made which helped us to improve it, especially in the area of key selection. The security of RSA relies on the computational hardness of factoring large integers and most of the attacks exploit bad choice parameters or flaws in implementations. Two very important cryptanalytic efforts in this area have been made by Wiener (Wiener, 1990) and de Weger (Weger, 2002) who developed attacks based on small secret keys (Hinek, 2010). The main idea of Wiener's attack is to approximate the fraction $\frac{e}{\varphi(N)}$ by $\frac{e}{N}$ for large values of N and then make use of the continued fraction algorithm to recover the secret key d by computing the convergents of the fraction $\frac{e}{N}$. He proved that the secret key d can be efficiently recovered if $d < \frac{1}{3}N^{\frac{1}{4}}$ and $e < \varphi(N)$ and then de Weger extended this attack from $d < \frac{1}{3}N^{\frac{1}{4}}$ to $d < N^{\frac{3}{4}-\beta}$, for any $\frac{1}{4} < \beta < \frac{1}{2}$ such that $|p-q| < N^{\beta}$. The aim of this paper is to investigate for which values of the variables σ and $\Delta = |p-q|$, RSA which uses public keys of the special structure $E = e + \sigma\varphi(N)$, where $e < \varphi(N)$, is insecure against cryptanalysis. Adding multiples of $\varphi(N)$ either to e or to d is called Exponent Blinding and it is widely used especially in case of encryption schemes or digital signatures implemented in portable devices such as smart cards (Schindler and Itoh, 2011). We show that an extension of de Weger's attack from public keys $e < \varphi(N)$ to $E > \varphi(N)$ is possible if the security parameter σ satisfies $\sigma \leq N^{\frac{1}{2}}$.

Paper 49	SECRYPT
09:00 - 10:30	Room Velazquez
Parallel Session 3a	

Building the Security Foundation to Embrace Public Software-as-a-Service (SaaS) Security Policies for SaaS Data Protection

Yuyu Chou[1], Jan Oetting[2] and Olga Levina[1]

[1] *Berlin Institute of Technology, Berlin, Germany*

[2] *Consileon Business Consultancy GmbH, Karlsruhe, Germany*

Keywords: Software as a Service, Cloud Computing, Security Policy, Data Protection, Security Management.

Abstract: To mitigate the risk of confidentiality breaches when adapting public SaaS solutions, enterprises should build their security policies by setting up a system of security awareness. This paper presents a systematic approach to developing security policies, which includes the method and process used during the public SaaS system development life cycle. Hence, all employees will have the well-grounded concept to protect confidential data in the cloud.

Paper 110	SECRYPT
09:00 - 10:30	Room Velazquez
Parallel Session 3a	

Key Management as a Service

Liran Lerman, Olivier Markowitch and Jorge Nakahara Jr

Université Libre de Bruxelles, Bruxelles, Belgium

Keywords: Cloud Computing, Key Management, Threshold Cryptosystem, Protocol.

Abstract: In this paper we consider the security issues related to the key management in cloud computing. We focus on the difficulty of managing cryptographic keys necessary to maintain for example the confidentiality of information stored in the clouds. In this framework, we present a threshold cryptosystem as well as three protocols, based on cooperation between cloud providers and a random number generator which is a trusted third party, that covers the issue of key management.

Paper 129	SECRYPT
09:00 - 10:30	Room Velazquez
Parallel Session 3a	

Data Repository for Security Information and Event Management in Service Infrastructures

Igor Kotenko, Olga Polubelova and Igor Saenko

St. Petersburg Institute for Informatics and Automation (SPIIRAS), Saint-Petersburg, Russian Federation

Keywords: Security Repository, Security Information and Event Management, Security Ontology, Data Model, Data Representation, Logical Inference, Service Infrastructure.

Abstract: Design and implementation of the repository is a critical problem in advanced security information and event management (SIEM) systems, which are SIEM systems of service infrastructures. The paper discusses several innovations which are realized to address this challenge. These include the application of an ontological approach for repository data modeling and a hybrid approach to its development, meaning the combined use of relational databases, XML databases and storage of triplets.

Wednesday, 25

Paper 137 SECRYPT
09:00 - 10:30 Room Velazquez
Parallel Session 3a

Quantifying the Benefits of File Size Information for Forensic Hash Matching

Johan Garcia
Karlstad University, Karlstad, Sweden

Keywords: Hashing, Digital Forensics, File Size Distributions.

Abstract: Hashing is a widely used technique in the digital forensic practice. By using file size information in addition to hashes, hash matching can potentially be made more effective since there is no need to calculate a hash value if there is no file in the hash set that has the same file size as the file being examined. Based on an examination of 36 million file sizes from five different data sets, this paper provides a quantification of the obtainable improvements. For the evaluated data sets the file reduction, i.e the fraction of files that can be skipped without hash calculations, ranged from 0.009 to 0.525. The byte reduction, i.e. the fraction of bytes that can be skipped, ranged from 0.514 to 0.992. Simulation results showed that these reductions in many cases could decrease the time necessary for hash scanning by 50% or more.

Paper 18 SIGMAP
09:00 - 10:30 Room Sevilla
Parallel Session 3

Adaptive Rate Control Scheme for Improving Quality of Multimedia in Broadband Wireless Networks

Dooyeol Yoon, Dongchil Kim and Kwangsue Chung
Kwangwoon University, Seoul, Korea, Republic of

Keywords: Quality Adaptation Scheme, Video Streaming, Rate Control.

Abstract: In order to improve quality of streaming services in broadband wireless networks, many researches are in progress. However, existing schemes do not guarantee a user perceived quality, because most of these schemes do not consider both wireless channel states and video characteristics. To cope with these problems, this paper proposes a NB-RC (Network and Buffer-aware Rate Control) scheme. The proposed scheme adjusts the video transmission rate according to the wireless channel states. It also controls the video quality based on buffer occupancy of clients. Through the simulation results, we prove that our scheme improves the media quality.

Paper 57 SIGMAP
09:00 - 10:30 Room Sevilla
Parallel Session 3

Time-frequency Filtering of Gaussian and Impulse Noise for Spread Spectrum Power Line Communication

Gaoyong Luo
Guangzhou University, Guangzhou, Guangdong, China
Buckinghamshire New University, Buckinghamshire, U.K.

Keywords: Power Line Communication, Spread Spectrum System, Impulse Noise Detection and Mitigation, Time-frequency Filtering, Fast Computation.

Abstract: The affluence of impulse noise is one of the challenging problems of the power line communication (PLC) as a communication channel. However, current methods for impulse noise reduction are either not effective or requiring heavy computing for detecting impulse noise accurately. This paper presents a time-frequency filter design method for impulse and Gaussian noise mitigation by a reliable noise detector in the wavelet domain with local variance analysis. The filtering is applied only to the detected noisy samples with others unchanged in an effort to reduce the noise level by adapting its operation in accordance with variance characteristics. The received corrupted signal from spread spectrum system is decomposed into time-frequency domain by fast implementation of lifting wavelet transform for real-time filtering of mixed Gaussian and impulse noise. Experimental results demonstrate that the proposed method can significantly reduce impulse noise and improve bit error rate (BER) without introducing distortion, leading to better quality of service.

Paper 75 SIGMAP
09:00 - 10:30 Room Sevilla
Parallel Session 3

Spaxels, Pixels in Space
A Novel Mode of Spatial Display

Horst Hörtner, Matthew Gardiner, Roland Haring, Christopher Lindinger and Florian Berger
Ars Electronica Futurelab, Linz, Austria

Keywords: Space Pixel, Spaxel, Voxel, Pixel, Media Display Technology, Spatial Imaging, 3D Visualization.

Abstract: We introduce a novel visual display paradigm through the use of controllable moving visible objects in physical space. Spaxels is a conjugation of "space" and "pixels". It takes the notion of a pixel, and frees it from the confines of a static two-dimensional matrix of a screen or projection surface to move three dimensionally in space. Spaxels extend the notion of Voxels, volumetric pixels, in that a Spaxel can physically move, as well as transition in colour and shape. Our current applied research is based on the control of a swarm of unmanned aerial vehicles equipped with RGB lighting and a positioning system that can be coordinated in three dimensions to create a morphing floating display. This paper introduces Spaxels as a novel concept and paradigm as a new kind of spatial display.

Paper 42 ICE-B
10:45 - 12:15 Room Dali
Parallel Session 4

Planning, Designing and Evaluating Multiple eGovernment Interventions

Fabrizio d'Amore, Luigi Laura
Sapienza Univ. of Rome, Rome, Italy

Luca Luciani, Fabio Pagliarini
INVITALIA Agenzia Nazionale per l'Attrazione degli Investimenti e lo Sviluppo d'Impresa S.p.A, Rome, Italy

Keywords: eGovernment, Interventions Planning.

Abstract: We consider the scenario where an organ of a public administration, which we refer as the *decisionmaker*, is requested to plan one or more interventions in some framework related to the Information Society or the eGovernment set of actions. We propose a methodology to support the decisionmaker in orienting, planning, and evaluating multiple (partially overlapping) interventions. In particular, we address two main problems: first, how to decide the structure of the interventions and how to determine the relevant parameters involved; second, how to set up a scoring system for comparing single interventions and its extension to the case of multiple interventions. The methodology unexpectedly shows that *it is not always the case that the best outcome is the one obtained by the best projects*. We formally model the problem and discuss its computational complexity. Our approach is also effective in process of selecting, from a set of submitted proposals, the ones to be funded.

Paper 61 ICE-B
10:45 - 12:15 Room Dali
Parallel Session 4

Geographic Information System using ArcGIS 10 and Open Source MapWindow Methodology and Comparative Study

Balqies Sadoun, Omar Al-Bayari, Jalal Al-Azizi and Samih Al Rawashdeh
AL-Balqa' Applied University, Al-Salt, Jordan

Keywords: GIS, ArcGIS 10, Open Source MapWindow, GIS Client, Spatial Database System.

Abstract: Geographic Information System (GIS) is an IT system capable of capturing, storing, analyzing, and displaying geographically data. We present a comparison between ArcGIS 10 and MapWindow 4.0 in creating a (GIS) for a study area to clarify the similarities and the differences. Upon the application of the GIS system using the two mentioned different software tools, we will provide the methodology and a related comparison. The *ESRI®ArcGIS* is an integrated geographic information system (GIS) for managing a digital database, working with maps and geographic information. It provides an infrastructure for making maps, analysis, presentations of geographic information available for organizations, communities and openly on the Web. emphMapWindow is free of charge, extensible geographic information System (GIS) that can be used as an open-source alternative to desktop GIS to develop and distribute custom spatial data analysis tools. It is a "Programmable Geographic Information System" that supports manipulation, analysis, and viewing of geospatial data and associated attribute data in several standard GIS data formats. It is also considered a mapping tool, a GIS modeling system, and a GIS application programming interface (API); all in one convenient redistributable package. It was developed by MapWindow Open Source Team to address the need for a GIS programming tool that could be used in engineering research, without requiring end users to purchase a complete GIS system, or become GIS experts.

We had used MapWindow in many applications and always proved efficient. We found Open Source MapWindow GIS as efficient as the commercial GIS system for important applications (Mapping, Navigation, Tracking etc.) in addition to its being free of charge. We had been using it in our applications and research work such as: OSGIS for BAU and in Navigation and Tracking to be used by interested users on the web.

Paper 9 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 4

Reversible Steganographic Scheme with High Embedding Capacity using Dual Cover Images

Nagaraj V. Dharwadkar and B. B. Amberker
National Institute of Technology, Warangal, India

Keywords: Reversible, Steganography, Dual Cover Images, Embedding Capacity, Stegoimage, Stego-key, Secret Communication.

Abstract: The advances in Internet technology and digital image representation helped the user to easily exchange the secret message. On Internet the transmission of the secret message is conducted using digital images which created new needs, issues and opportunities to the researcher. The basic objective of secret message communication is to transmit a message securely by embedding it into a cover-image such that unintended observers are unable to detect it. The image steganographic schemes are used in secret message communication. In this paper, we have proposed reversible steganographic scheme for gray-scale images. This scheme uses dual cover images to hide secret image and generates the perceptually similar dual stegoimages. Further, to extract the secret image the knowledge of dual stegoimages and stego-key are necessary which improved the security of this scheme. The experimental results show that the scheme provides a higher embedding capacity and robustness with un-noticeable distortions in the stegoimages. The performance of the scheme is analyzed for various types of image processing attacks on stegoimage. The proposed scheme was found rigid to the image processing attacks.

Paper 27 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 4

Tampering with Java Card Exceptions The `Exception` Proves the Rule

Guillaume Barbu[1,2], Philippe Hoogvorst[1] and Guillaume Duc[1]
[1] *Institut Mines-Télécom / Télécom ParisTech, CNRS LTCI, Paris Cedex 13, France*
[2] *Oberthur Technologies, Innovation Group, Pessac, France*

Keywords: Java Card, Java Exceptions, Software Attacks, Fault Attacks, Combined Attacks.

Abstract: Many publications have studied the various issues concerning Java Cards security regarding software and/or hardware attacks. However, it is surprising to notice that the particular case of exception-related mechanisms has not been tackled yet in the literature. In this article, we fill this gap by proposing several attacks against Java Card platforms based on both exception handling and exception throwing. In addition, this study allows us to point out that a weakness known by the web-oriented Java community for more than a decade still passes the different steps of the state-of-the-art Java Card application deployment process (namely conversion and verification). This appears all the more important as the Java Card 3 *Connected Edition* specifications have started to bridge the gap between the two worlds that are Java Cards and Java web services.

Paper 81 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 4

Voice Passwords Revisited

Chenguang Yang[1], Ghaith Hammouri[2] and Berk Sunar[1]
[1] *Worcester Polytechnic Institute, Worcester, U.S.A.*
[2] *Claveo Software, Santa Barbara, U.S.A.*

Keywords: Voice, Entropy, Mel Frequency Cepstral Coefficients, Gaussian Mixture Model.

Abstract: We demonstrate an attack on basic voice authentication technologies. Specifically, we show how one member of a voice database can manipulate his voice in order to gain access to resources by impersonating another member in the same database. The attack targets a voice authentication system build around parallel and independent speech recognition and speaker verification modules and assumes that adapted Gaussian Mixture Model (GMM) is used to model basic Mel-frequency cepstral coefficients (MFCC) features of speakers. We experimentally verify our attack using the YOHO database. The experiments conclude that in a database of 138 users an attacker can impersonate anyone in the database with a 98% success probability after at most nine authorization attempts. The attack still succeeds, albeit at lower success rates, if fewer attempts are permitted. The attack is quite practical and highlights the limited amount of entropy that can be extracted from the human voice when using MFCC features.

Paper 44	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 4	

Diffusion Tracking Algorithm for Image Segmentation

Lassi Korhonen and Keijo Ruotsalainen
University of Oulu, Oulu, Finland

Keywords: Spectral Clustering, Image Segmentation, Diffusion.

Abstract: Different clustering algorithms are widely used for image segmentation. In recent years, spectral clustering has risen among the most popular methods in the field of clustering and has also been included in many image segmentation algorithms. However, the classical spectral clustering algorithms have their own weaknesses, which affect directly to the accuracy of the data partitioning. In this paper, a novel clustering method, that overcomes some of these problems, is proposed. The method is based on tracking the time evolution of the connections between data points inside each cluster separately. This enables the algorithm proposed to perform well also in the case when the clusters have different inner geometries. In addition to that, this method suits especially well for image segmentation using the color and texture information extracted from small regions called patches around each pixel. The nature of the algorithm allows to join the segmentation results reliably from different sources. The color image segmentation algorithm proposed in this paper takes advantage from this property by segmenting the same image several times with different pixel alignments and joining the results. The performance of our algorithm can be seen from the results provided at the end of this paper.

Paper 58	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 4	

Optimisation of Smoothing Parameter of Diffeomorphism Kernel Estimate for Bounded Random Data

Molka Troudi
ENIT, Tunis, Tunisia

Faouzi Ghorbel
ENSI, La Manouba, Tunisia

Keywords: Diffeomorphisme Kernel Estimate, Plug-in Algorithm, Banwidth.

Abstract: The Diffeomorphism Kernel Density Estimator (DKDE) requires the estimation of an optimal value of the bandwidth to ensure a reliable pdf estimation of bounded distributions. In this paper, we suggest to approach the optimal bandwidth value by adapting Plug-in algorithm to DKDE estimator. We will show that the pro-posal method allows better density estimation in the MISE sense. Otherwise, the Gibbs phenomenon com-pletely disappears. These results are illustrated by some bounded and semi bounded distributions simulations.

Paper 60	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 4	

Development of Computer Algorithms to Control a Weelchair through the Movement of the Head by Artificial Vision

Ricardo Fuentes Covarrubias, Andrés Gerardo Fuentes Covarrubias
Universidad de Colima, Colima, Mexico

Cristina Conde Vilda, Isaac Martin de Diego, Enrique Cabello
Universidad Rey Juan Carlos (URJC), Mostoles, Madrid, Spain

Keywords: Biometry, Machine Vision, Automatic Recognition.

Abstract: The Purpose of this project is the control of motion and direction in real time of a wheel chair, using machine vision algorithms. The main goal of this project is the signal acquisition from the video camera and collision sensors for post processing in the C# algorithms and later obtaining motor control in the traction mechanism of the wheelchair. The C# algorithm has several tasks. The first is to obtain the real time image from web cam and later processing for the identification of the direction of movement of the human face. The second is to calculate the speed of the movement for generation of the PWM output for motor movement. This information output using the RS232C driver to a microcontroller card attached to a motor control box in the wheel chair mechanism. The final task is to obtain the collision sensor status for security implementation, all in real time. The main reason for development of an implementation of this solution is the use of open source software tools for a more stable platform in the base system due to the characteristics of the end use of the system. The end user of the system will be quadriplegic people.

Paper 17 WINSYS
10:45 - 12:15 Room Velazquez
Parallel Session 4

Implementation of the COST 273 Directional Channel Model in Microcell Scenarios

Ivo Sousa, Maria Paula Queluz and António Rodrigues
Technical University of Lisbon, Lisbon, Portugal

Keywords: COST 273 Directional Channel Model, Microcells, Wireless Communications.

Abstract: This paper presents a tutorial on how to implement the COST 273 Directional Channel Model (DCM) for microcell scenarios. Special care has been taken to present all the parameters models and values required by the DCM, being some of them proposed in this work because they were missing in the related literature and are essential. The results and comparison with experimental data of an implementation example are also presented, which prove that this DCM is suitable for wireless systems development, especially those that exploit spatial aspects of radio channels, like for example Multiple-Input Multiple-Output (MIMO) systems.

Paper 51 WINSYS
10:45 - 12:15 Room Velazquez
Parallel Session 4

Sustainable Rural Areas Network-based Architecture

Farnaz Farid, Chun Ruan and Seyed Shahrestani
University of Western Sydney, Sydney, Australia

Keywords: Cellular Systems, ICT, Network-based Architecture, Wireless Networking.

Abstract: Communication technologies and broadband networks offer interesting solutions for improving human quality of life. However, the improvements are less prominent in the rural areas and in developing countries. Partially, this may be related to cultural and social acceptance of such technologies in rural areas. It can also be associated with the lack of a proper architecture for utilization of such technologies in those areas. This work in progress is an attempt in developing such architecture. It is based on mapping of existing or upcoming information and communication technologies to services and applications needed for sustainable rural areas. Based on analysis of the existing infrastructure and technical requirements, we show that wireless and cellular technologies are the most suitable choices for this purpose. Integrating these points, a network-based architecture, referred to as eVillage, is designed. To investigate the underlying issues, simulation studies for several interactive services in such an environment, using OPNET are then carried out. These studies show that the proposed architecture is capable of supporting a reasonable number of clients while meeting basic Quality of Service requirements.

Paper 52 WINSYS
10:45 - 12:15 Room Velazquez
Parallel Session 4

QoE – Based Scheduling in WiMAX Networks

Kalypso Magklara[1], Aggeliki Sgora[1,2], Dimitrios D. Vergados[1] and Dimitris J. Vergados[3,2]
[1] *University of Piraeus, Piraeus, Greece*
[2] *Technological Educational Institute of Western Macedonia, Kastoria, Greece*
[3] *National Technical University of Athens, Athens, Greece*

Keywords: WiMAX, Networks, Scheduling, rtPS, Quality of Service (QoS), Quality of Experience (QoE).

Abstract: Worldwide Interoperability for Microwave Access (WiMAX) networks provide wireless broadband internet access, interoperability, while decrease the entrance barrier in mobile communications sector, and offer services comparable to those of the emerging 4G technology. The standard 802.16, upon which WiMAX networks are based, has not designated any particular scheduling algorithm, allowing each provider to develop its own. However, existing scheduling algorithms take into account the Quality of Service (QoS), fairness and other parameters, but do not provide Quality of Experience (QoE). For this reason, in this paper two different approaches are proposed in order to provide QoE, especially for the rtPS WiMAX service. Simulation results show that by applying different policies the QoE provided to the WiMAX users is improved.

12:15 - 13:15 Room Plenary
Making Sense of All Things Handwritten - From Postal Addresses to Tablet Notes
Keynote Speaker: Venu Govindaraju

Making Sense of All Things Handwritten From Postal Addresses to Tablet Notes

Venu Govindaraju
University at Buffalo, Amherst, U.S.A.

Abstract: The handwritten address interpretation system pioneered in our lab at UB is widely regarded as one of the key success stories in AI. It integrated the document processing steps of binarization, segmentation, recognition, and combination of classifiers with carefully handcrafted rules. Advances in machine learning (ML) in the past decade, made possible by the abundance of training data, storage, and processing power, have facilitated the development of principled approaches for many of the same modules.

Paper 6 DCNET
14:30 - 16:30 Room Sevilla
Parallel Session 5

Digital Signature of Network Segment using Flow Analysis

Alexandro M. Zacaron, Luiz F. Carvalho, Mario H. A. C. Adaniya, Taufik Abrão and Mario Lemes Proença Jr.

State University of Londrina, Londrina, Brazil

Keywords: DSNSF, Baseline, NetFlow, K-means, Ant Colony Optimization.

Abstract: This paper presents two models for building Digital Signature of Network Segment using flow analysis (DSNSF). The DSNSF can be classified as a characterization of the traffic or as a baseline of the analyzed network segment. In this work two types of signatures of network segment are presented. The first is built applying K-means clustering algorithm and the second using optimized clustering by metaheuristic Ant Colony Optimization (ACO). The signatures provide characterization of the traffic segments analyzed using NetFlow v9 protocols TCP and UDP. The results achieved show that the two models presented using k-means Clustering and metaheuristic Ant Colony Optimization obtained good results for the creation of DSNSF or traffic characterization of the segments analyzed.

Paper 10 DCNET
14:30 - 16:30 Room Sevilla
Parallel Session 5

Mobile Broadband Traffic Forecasts in Korea

Chanwoo Cho and Sungjoo Lee

Ajou University, Suwon, Korea, Republic of

Keywords: Mobile Traffic, Forecast, Smart-Phone, Smart-TV, PC, Patterns of Use.

Abstract: During many years, the dominant traffic in mobile broadband networks was voice. However, with the introduction of diverse mobile broadband equipment, the situation has changed. Since mobile broadband devices can allow users to access information instant and connect to web quickly, the mobile world has been revolutionized, where global mobile data traffic has been increasing dramatically. And the changes in the patterns of usage for mobile devices have started to cause traffic jams on the mobile broadband networks. As a result, forecasting the future traffic needs is in urgent need to provide high-quality mobile broadband services. To meet this need, this research aims to suggest a new forecasting method for future mobile broadband traffic. For the purpose, three-round Delphi survey was conducted to identify devices and applications that would affect in the future mobile broadband traffic, and their expected growth rates of users and changes in the patterns of use for each device. Then the total amount of mobile broadband traffic was forecasted based on survey results. The research results are expected to provide the basic research data for a further study.

Paper 19 DCNET
14:30 - 16:30 Room Sevilla
Parallel Session 5

Towards a CDN over ICN

Byungjoon Lee, Hongseok Jeon, Seunghyun Yoon and Hoyoung Song

ETRI, Daejeon, Korea, Republic of

Keywords: Information-Centric Networking (ICN), Content Delivery Network (CDN).

Abstract: The development of Information-Centric Networking (ICN) concepts is one of the significant results of different international Future Internet research activities. In the approaches, the networking paradigm shifts from the host-to-host communication to the information-based communication. The ICN concept is receiving huge attention because of the increasing demand for highly scalable and efficient distribution of information. Meanwhile, the Content Delivery Network (CDN) has been an important patch to the existing IP network that enables the fast delivery of content. Though the CDN architecture relies on the traditional host-to-host communication model, it has been widely deployed to solve the content availability and on-time delivery issues. In this paper, we cover issues and requirements to implement CDN over ICN technologies, and suggest an architecture called IICN which enables an easy transition from IP-based CDN to ICN-based CDN. In IICN, it is possible to incrementally replace IP nodes with ICN-capable nodes. We believe that IICN suggests an important ICN application that leads to an Information-Centric Internet.

Paper 20	DCNET
14:30 - 16:30	Room Sevilla
Parallel Session 5	

Improving Network Performane Management of Nonlinear Dynamics

Seyed Shahrestani
University of Western Sydney, Sydney, Australia

Keywords: AQM/RED, Bifurcation Analysis, Delay Control, Internet, Nonlinear Dynamics.

Abstract: To manage the huge amount of traffic that is to be carried using the limited bandwidth and other resources, large networks and the Internet are heavily dependent on the use of protocols, and in particular, on TCP/IP protocol suite. While the utilization of TCP/IP is of significant practical value, for most large complex networks it can be inefficient, as it fails to fully take into consideration the importance of the major parts of the system. To overcome this, more complicated congestion control mechanisms, such as AQM/RED are widely utilized. However, these complex mechanisms exhibit nonlinear dynamics, which are not well understood and are usually unaccounted for. As a result of this, to avoid oscillatory behavior or loss of stability, the parameters of these systems are often set too conservatively. In turn, this will lead to unnecessary underutilization of the network resources. On the other hand, through the analysis and management of nonlinearities, the operability regions for the networked systems can be expanded, while its performance is also improved. This paper presents our visionary works of applying these ideas to networked systems, resulting in higher loading and throughput, and avoiding oscillatory or unstable behavior.

Paper 21	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 5	

The Relative Importance of Teenagers' Personal Characteristics on Technology Addiction

Chan Jung Park and Jung Suk Hyun
Jeju National University, Jeju-si, Korea, Republic of

Keywords: Ethics Education, Internet Addiction, Mobile Phone Addiction, Self-Efficacy, Time Perspective, Dominance Analysis.

Abstract: As the Internet becomes the major means to conduct business, new types of agenda arise in e-Business arena. One of them is Ethics. Compared to other topics, ethics education for e-services takes long time because of its characteristics. Thus, Cyberethics education is required from childhood. In this paper, we examine the status of the Korean teenagers' technology addiction, their personal characteristics, and their environmental factors composed of parents, friends, and media to diagnose their behavior and to boost their morality. In order to achieve our research goals, we survey 1,421 primary and secondary school students, and then do factor, regression, and dominance analyses. Also, we examine the relationships between the students' characteristics and their technology addiction. We focus on the Internet and mobile phone addiction as technology addiction. Based on this study, we summarize a few issues to be solved for our adolescents to do their right actions on e-environment.

Paper 22	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 5	

The Use of Internet as a Marketing Tool Evaluating the Websites of Spain's Top Restaurants

F. J. Miranda, S. Rubio, A. Chamorro and M. S. Janita
Extremadura University, Badajoz, Spain

Keywords: World Wide Web, Restaurant Websites, Tourism Marketing, Content Analysis, Web Design, Internet, Research Paper.

Abstract: The haute cuisine catering sector in Spain is faced with two facts that underscore the importance today of their presence on the Internet. On the one hand, the quality and recognition of Spanish cuisine are fostering the development of culinary tourism, both domestic in origin and from abroad. And on the other, an ever greater proportion of tourists are using the Internet to obtain information and make decisions about activities to include in their trips. Given this context, the present work describes a comparative analysis of the Websites of Spanish restaurants which have at least one Michelin star in order to assess the quality of those Web pages and provide some guidance to their designers to facilitate their use as a marketing tool. The instrument used is the Web Assessment Index (WAI). This has been validated in other studies in the literature, and measures the quality of a Website based on 4 dimensions: visibility, speed, navigability, and content. The results showed the quality of the Website to be positively correlated with the category of the corresponding restaurant.

Paper 48 ICE-B
14:30 - 16:30 Room Dali
Parallel Session 5

ArchaeoApp Rome Edition (AARE): Making Invisible Sites Visible e-Business Aspects of Historic Knowledge Discovery via Mobile Devices

Katharina Holzinger, Gabi Koiner
Karl-Franzens University Graz, Graz, Austria

Primoz Kosec, Markus Fassold, Andreas Holzinger
Institute for Medical Informatics, Statistics and Documentation, Graz, Austria

Keywords: Information Retrieval on Mobile devices, Knowledge Management, e-Business, Archaeology, Classics, History, e-Business, Tourists.

Abstract: Rome is visited by 7 to 10 million tourists per year, many of them interested in historical sites. Most sites that are described in tourist guides (printed or online) are archaeological sites; we can call them visible archaeological sites. Unfortunately, even visible archaeological sites in Rome are barely marked – and invisible sites are completely ignored. In this paper, we present the ArchaeoApp Rome Edition (AARE). The novelty is not just to mark the important, visible, barely known sites, but to mark the invisible sites, consequently introducing a completely novel type of site to the tourist guidance: historical invisible sites. One challenge is to get to reliable, historic information on demand. A possible approach is to retrieve the information from Wikipedia directly. The second challenge is that most of the end users have no Web-access due to the high roaming costs. The third challenge is to address a balance between the best platform available and the most used platform. For e-Business purposes, it is of course necessary to support the highest possible amount of various mobile platforms (Android, iOS and Windows Phone). The advantages of AARE include: no roaming costs, data update on demand (when connected to Wi-Fi, e.g. at a hotel, at a public hotspot, etc. ... for free), automatic nearby notification of invisible sites (markers) with a Visual-Auditory-Tactile technique to make invisible sites visible.

Paper 55 ICE-B
14:30 - 16:30 Room Dali
Parallel Session 5

Pattern Characterization in Multivariate Data Series using Fuzzy Logic Applications to e-Health

W. Fajardo, M. Molina-Solana and M. C. Valenza
University of Granada, Granada, Spain

Keywords: Health Care, Data Series, Fuzzy Logic.

Abstract: The application of classic models to represent and analyze time-series imposes strict restrictions to the data that do not usually fit well with real-case scenarios. This limitation is mainly due to the assumption that data are precise, not noisy. Therefore, classic models propose a preprocessing stage for noise removal and data conversion. However, there are real applications where this data preprocessing stage dramatically lowers the accuracy of the results, since these data being filtering out are of great relevance. In the case of the real problem we propose in this research, the diagnosis of cardiopulmonary pathologies by means of fitness tests, detailed fluctuations in the data (usually filtered out by preprocessing methods) are key components for characterizing a pathology. We plan to model time-series data from fitness tests in order to characterize more precise and complete patterns than those being currently used for the diagnosis of cardiopulmonary pathologies. We will develop similarity measures and clustering algorithms for the automatic identification of novel, refined, types of diagnoses; classification algorithms for the automatic assignment of a diagnosis to a given test result.

Paper 56 ICE-B
14:30 - 16:30 Room Dali
Parallel Session 5

Measurement and Concepts of Individual Application Capability of e-Business

Chui Young Yoon and Sung Koo Hong
Korea National University of Transportation, Chungju city, Korea, Republic of

Keywords: e-Business, e-Business Competency, Measurement Tool, Measurement Item.

Abstract: Understanding measurement and concepts for an individual application capability of e-business is important to manage and improve their work ability in an e-business environment. This study presents a 17-item tool to measure an individual application capability of e-business with the measurement items, process, and method

based on the previous literature. The developed tool construct were verified by factor and reliability analysis with the questionnaire survey. This tool has four measurement factors and seventeen items. The utilization of the developed tool was confirmed by applying it to a case study.

Paper 63 SECRYPT
14:30 - 16:30 Room Valencia
Parallel Session 5

Verifying Privacy by Little Interaction and No Process Equivalence

Denis Butin
Dublin City University, Dublin 9, Ireland

Giampaolo Bella
Università di Catania, Catania, Italy
De Montfort University, Leicester, U.K.

Keywords: e-Voting, Privacy, Inductive Method.

Abstract: While machine-assisted verification of classical security goals such as confidentiality and authentication is well-established, it is less mature for recent ones. Electronic voting protocols claim properties such as voter privacy. The most common modelling involves indistinguishability, and is specified via trace equivalence in cryptographic extensions of process calculi. However, it has shown restrictions. We describe a novel model, based on unlinkability between two pieces of information. Specifying it as an extension to the Inductive Method allows us to establish voter privacy without the need for approximation or session bounding. The two models and their latest specifications are contrasted.

Paper 64 SECRYPT
14:30 - 16:30 Room Valencia
Parallel Session 5

A Security Analysis of Emerging Web Standards HTML5 and Friends, from Specification to Implementation

Philippe De Ryck, Lieven Desmet, Frank Piessens and Wouter Joosen
KU Leuven, Leuven, Belgium

Keywords: HTML5, Web Application Security, Standards, Specification.

Abstract: Over the past few years, a significant effort went into the development of a new generation of web standards, centered around the HTML5 specification. Given the importance of the web in our society, it is essential that these new standards are scrutinized for potential security problems. This paper reports on a systematic analysis of ten important, recent specifications with respect to two generic security goals: (1) new web mechanisms should not break the security of existing web applications, and (2) different newly proposed mechanisms should interact with each other gracefully. In total, we found 45 issues, of which 12 are violations of the security goals and 31 issues concern under-specified features. Additionally, we found that 6 out of 11 explicit security considerations have been overlooked/overruled in major browsers, leaving secure specifications vulnerable in the end. All details can be found in an extended version of this paper (De Ryck et al., 2012).

Paper 75 SECRYPT
14:30 - 16:30 Room Valencia
Parallel Session 5

Biometric Identification in Virtual Worlds using Biometric Fusion Techniques

Ahmed Al-Khazzar and Nick Savage
University of Portsmouth, Portsmouth, U.K.

Keywords: Biometric Fusion, Biometric Recognition, Identification, Virtual Worlds, Games, Behavioural Biometric.

Abstract: The use of virtual worlds is becoming popular in many fields such as education, economy, space, and games. With the widespread use of virtual worlds, establishing the security of these systems becomes more important. In this paper a behavioural biometric system is implemented to identify users of a virtual environment. This research suggests the use of a score level fusion technique to improve the identification performance of the system. The identification is achieved by analysing user interactions within the virtual environments and comparing these interactions with the previously recorded interactions in the database. The results showed that using score level biometric fusion in behavioural biometric systems similar to the one presented in this research is a promising tool to improve the performance of these systems. The use of biometric fusion technique enhanced the performance of the implemented biometric system up to 7.5%. An average equal error rate of up to 22.7% was achieved in this work.

Paper 79	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 5	

On the Development of Totally Self-checking Hardware Design for the SHA-1 Hash Function

Harris E. Michail[1], George S. Athanasiou[2], Andreas Gregoriades[3], George Theodoridis[2] and Costas E. Goutis[2]

[1] *Cyprus University of Technology, Lemesos, Cyprus*
[2] *University of Patras, Patras, Greece*
[3] *European University of Cyprus, Nicosia, Cyprus*

Keywords: Cryptography, Hash Functions, SHA-1, Totally Self-checking, Concurrent Error Detection.

Abstract: Hash functions are among the major blocks of modern security schemes, used in many applications to provide authentication services. To meet the applications' real-time constraints, they are implemented in hardware offering high-performance and increased security solutions. However, faults occurred during their operation result in the collapse of the authentication procedure, especially when they are used in security-critical applications such as military or space ones. In this paper, a Totally Self-Checking (TSC) design is introduced for the currently most-used hash function, namely the SHA-1. A detailed description concerning the TSC development of the data- and control-path is provided. To the best of authors' knowledge, it is the first time that a TSC hashing core is presented. The proposed design has been implemented in 0.18μm CMOS technology and experiments on fault caverage, performance, and area have been performed. It achieves 100% coverage in the case of odd erroneous bits. The same coverage is also achieved for even erroneous bits, if they are appropriately spread. Compared to the corresponding Duplicated-with-Checking (DWC) design, the proposed one is more area-efficient by almost 15% keeping the same frequency.

Paper 116	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 5	

Some Remarks on Keystroke Dynamics Global Surveillance, Retrieving Information and Simple Countermeasures

Marek Klonowski, Piotr Syga and Wojciech Wodo

Wrocław University of Technology, Wroclaw, Poland

Keywords: User Identification, Keystroke Dynamics, Digraphs, Distribution, Impersonation.

Abstract: In this paper we discuss some security issues related to keystroke dynamics. Up to now these methods have been used mainly for supporting authentication protocols. We point out that they can be also used against privacy and potentially lead to some other malicious behavior like for example impersonation. We also present some simple fairly realistic and usable countermeasures. We discuss fundamental issues about efficient and accurate representation of user's profile in keystroke dynamic methods. More precisely, we discuss statistics of so–called timings used for building user's profile. We give some observations about distributions of timings that substantially differ from assumptions used in numerous papers. Some of our theories are supported by experimental results.

Paper 1	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 5	

Optimal MAC PDU Size in ARQ-enabled Connections in IEEE 802.16e/WiMAX Systems

Oran Sharon

Netanya Academic College, Netanya, Israel

Yaron Alpert

Intel Corporation, Haifa, Israel

Keywords: WiMAX, Bursts, FEC Blocks, Data Blocks, Goodput.

Abstract: In this paper we address an aspect of the mutual influence between the PHY layer budding blocks (FEC blocks) and the MAC level allocations in the Uplink and Downlink of IEEE 802.16e/WiMAX systems, In these systems it is possible to transmit MAC level frames, denoted MAC PDUs, such that a PDU contains an integral number of fixed size Data Blocks. We compute the optimal size of a PDU that maximizes the Goodput of the PDU. The Goodput depends on the success probability of the PDU, which in turn depends on the FEC blocks over which the PDU is allocated. We then compare among the maximum PDU Goodputs in different sizes of the FEC blocks and the Data Blocks. The main outcome is that the PDU Goodput is sensitive only in the case where Data Blocks are very large. We also give guidelines on how to choose the best Modulation/Coding Scheme (MCS) to use in a scenario where the Signal-to-Noise Ratio (SNR) can change significantly during transmissions, in order to maximize the PDU Goodput.

Paper 19	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 5	

Improving the Reliability of a Train Positioning System through the Use of Full Coverage Radio Communication Technologies Performance Study of a TETRA Network to Transmit Position Information

Roberto Carballedo, Pablo Fernández, Unai Hernández Jayo and Asier Perallos

University of Deusto, Bilbao, Spain

Keywords: Wireless Communications, Terrestrial Trunked Radio, Train Positioning System, Railway Industry.

Abstract: Today, it is common for trains to incorporate autonomous positioning systems based on geo-location technologies similar to those used on road transportation. These positioning systems represent a cost effective solution for railway companies operating in not evolved regions. Furthermore, these positioning systems can enhance the reliability of positioning systems based on the occupation of the tracks (which are most used in the most developed regions). Autonomous positioning systems calculate the position of the train, but the position has to be sent from the train to the control center. GPRS/3G mobile technologies and WiFi radio technologies are the most common technologies for transmitting the position to the control centers. These technologies do not guarantee 100% coverage in certain areas such as tunnels or mountainous regions. This paper presents the results of the tests on an autonomous positioning system to add a new communications technology in order to increase its coverage. This technology is TETRA, which is a radio technology that has been traditionally used for voice transmission, but it can be a good complement to GPRS/3G when there is no coverage.

Paper 24	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 5	

Investigation of a Radio Propagation Model for Vegetation Scatter Dynamic Channels at BFWA Frequencies

Sérgio Morgadinho[1,2], Juergen Richter[2], Rafael F. S. Caldeirinha[1,3,2] and Telmo R. Fernandes[1,3]

[1] *Instituto de Telecomunicações, Leiria, Portugal*

[2] *University of Glamorgan, Pontypridd, U.K.*

[3] *Polytechnic Institute of Leiria, Leiria, Portugal*

Keywords: Radio Propagation Model, Radiative Energy Transfer (RET), Time-variant Channel, Vegetation Scatter, Dynamic Effects, BWA Frequency.

Abstract: The successful deployment of wireless technologies in the micro- and millimetre frequencies relies on the understanding of radio channel propagation and accurate radio propagation models. To this extent, the dynamic effects of vegetation on radio signals are investigated, as a function of wind direction, receiver location and vegetation depth. Furthermore, a radio propagation model, based on the RET, is investigated as an approach to predict the channel dynamic effects of vegetation scatter at 20 GHz. The model is evaluated for a structured forest medium, and its performance is assessed through the use of primary, secondary and error quantification statistics.

Paper 2	WINSYS
14:30 - 16:30	Room Velazquez
Parallel Session 5	

Efficient Coupled PHY and MAC Use of Physical Bursts in WiMAX/IEEE 802.16e Networks

Oran Sharon

Netanya Academic College, Netanya, Israel

Gassan Tabajah, Yaron Alpert

Intel Corporation, Haifa, Israel

Keywords: WiMAX, Bursts, FEC Blocks, Scheduling, Goodput.

Abstract: We address several issues related to the efficient use of Bursts in WiMAX/IEEE 802.16e systems. We look on the relation between the PHY layer budding blocks (FEC blocks) and the allocation of MAC level frames (PDUs) over these FEC blocks. In particular, we show how to transmit a given amount of MAC level data bits over a given Burst in order to maximize the number of successfully transmitted data bits in the Burst. We also compute, given an amount of data bits to transmit, what is the Burst size that maximizes each of the following three performance criterion: the number of successfully transmitted data bits in the Burst, the maximum ratio between the number of successfully transmitted data bits to the Burst size, and the number of successfully transmitted data bits per PHY slot. For the first problem the paper shows how to optimally divide the Burst into PDUs and shows that sometimes it is more efficient to use less reliable Modulation/Coding schemes. For the second problem the paper shows that using the PHY slots efficiently is the best criterion to consider.

Paper 3	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

TRAFIL
A Tool for Enhancing Simulation TRAce FILes Processing

Christos Bouras[1,2], Savvas Charalambides[1,2], George Kioumourztis[3] and Kostas Stamos[1,2,4]

[1] *Computer Technology Institute and Press, Rio, Greece*

[2] *University of Patras, Patras, Greece*

[3] *Center for Security Studies, Athens, Greece*

[4] *Technological Educational Institute of Patras, Patras, Greece*

Keywords: Simulation Analysis Tool, Trace File, NS-2.

Abstract: NS-2 (Network Simulator) is one of the most popular discrete event simulators used for network simulation. Trace files produced by NS-2 provide very useful information for post simulation analysis. This paper presents the architecture and development considerations for a TRAce FILe analysis tool, which intends to simplify the management of trace files generated during network simulations. The tool is focused on NS-2 trace files, but can be extended to handle a variety of simulation trace files formats. Its purpose is to make the execution of a large number of network simulations faster, and the extraction of results from a large amount of data more flexible and productive. TRAFIL introduces a novel way of interpreting, parsing, reading and eventually utilizing NS-2 trace files by using "metafiles" and "sub-metafiles" during the trace file recognition and process procedures, making the overall operations more abstract, substantially efficient and faster than alternative approaches. Furthermore, TRAFIL facilitates the whole trace file analysis task, offering the opportunity to store each trace file as well as every measurement produced for each trace file. The tool aims to aid the analysis of simulation results offering features that other tools in this area have been missing.

Paper 8	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Hash Algorithms for 8051-based Sensornodes

Manuel Koschuch, Matthias Hudler and Michael Krüger

University of Applied Science, Vienna, Austria

Keywords: Efficient Implementation, Hash Algorithms, Sensor Networks, Sensor Nodes, SHA-1, SHA-3, Tiger Hash.

Abstract: Wireless Sensors Networks are still an emerging technology. Their special architecture allows for unique applications that would be impossible, or at least very difficult, to implement using other technologies. But the wireless data transmission between the single nodes poses new challenges from a security point of view: the single messages have to be secured against eavesdropping and manipulation, as well as the individual nodes have to be secured against capture and extraction of their secret key. Cryptographic hash functions are an integral part of most cryptographic network protocols, whether they are used for signatures or message integrity. In this position paper, we describe a preliminary performance evaluation of three very different hash-functions on a Texas Instruments CC2530 sensor node, based on an 8051 microcontroller: Tiger, representing a hash designed for 64-bit architectures, the current standard SHA-1, and Grøstl, a SHA-3 finalist. Our preliminary results indicate that even without any major optimizations hash algorithms that were clearly not designed to run on constrained devices can be adapted to these environments with quite acceptable results, thereby giving designers of sensor network security protocols new implementation options.

Paper 17	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Strictness of Rate-latency Service Curves

Ulrich Klehmet and Kai-Steffen Hielscher

University Erlangen, Erlangen, Germany

Keywords: Network Calculus, Blind Multiplexing, Strict Service Curve, Non-strict Service Curve.

Abstract: Network Calculus (NC) offers powerful methods for performance evaluation of queueing systems, especially for the worst-case analysis of communication networks. It is often used to obtain QoS guarantees in packet switched communication systems. One issue of nowadays' research is the applicability of NC for multiplexed flows, in particular, if the FIFO property cannot be assumed when merging the individual flows. If a node serves the different flows using another schedule than FIFO, the terms 'strict' or 'non-strict' service curves play an important role. In this paper, we are dealing with the problems of strict and non-strict service curves in connection with aggregate scheduling. In the literature, the strictness of the service curve of the aggregated flow is reported as a fundamental precondition to get a service curve for the single individual flows at demultiplexing, if the service node process the input flows in Non-FIFO manner. The important strictness-property is assumed to be a unique feature of the service curve alone. But we will show here that this assumption is not true in general. Only the connection with the concrete input allows to classify a service as curve strict or non-strict.

Paper 38	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

A Mobile Information System for Improved Navigation in Public Transport User Centered Design, Development, Evaluation and e-Business Scenarios of a Mobile Roadmap Application

Bernhard Peischl
Softnet Autstria, Graz, Austria

Martina Ziefle
RWTH Aachen University, Aachen, Germany

Andreas Holzinger
Medical University Graz, Graz, Austria

Keywords: Mobile User Interfaces, User-centered Design, Ubiquity, m-Business Models.

Abstract: End-user friendly interface design is of tremendous importance for the success of mobile applications which are of increasing interest in the e-Business area. In this paper, we present an empirical evaluation of a mobile information system for improving navigation of public transport. High air pollution and respiratory dust, along with other threats to environmental conditions in urban areas, make the use of public transport system less and less a matter of choice. The central hypothesis of this study is that useful, useable and accessible navigation contributes towards making public transport systems more attractive.

Paper 49	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Collaborative Security Management Services for Port Information Systems

Theodoros Ntouskas and Nineta Polemi
University of Piraeus, Piraeus, Greece

Keywords: Security Management, Commercial Ports, Critical Infrastructures, Collaboration, S-Port project.

Abstract: Ports Information and Communication Technology (PICT) systems offer critical services and host sensitive data. However the current maritime legislation, standardization and technological efforts do not sufficiently cover the PICT security. Identifying these needs, we propose the collaborative environment S-Port offering security management services.

Paper 8	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

AMO-OFDM Signal Delivery of 20 Gbit/S throughput in 20-Km Single Loopback Fiber Link Employing Baseband I/Q Separation Adaptive Optical OFDM Modulation and Separate I/Q Baseband Signal Transmission with Remotely-fed RSOAs for Colorless ONU in Next-generation WDM Access

Jeong-Min Joo, Moon-Ki Hong, Dung Tien Pham and Sang-Kook Han
Yonsei University, Seoul, Korea, Republic of

Keywords: Adaptively Modulated Optical Orthogonal Frequency Division Multiplexing, Separate I/Q Baseband Transmission, Remotely-fed, Bandwidth-limited, Reflective Semiconductor Optical Amplifier, Colorless Optical Network Unit, Next-generation Access, Wavelength Division Multiplexed Passive Optical Network.

Abstract: We demonstrated a novel scheme to transmit 20-Gb/s adaptively modulated optical orthogonal frequency division multiplexed (AMO OFDM) signal employing separate in-phase (I) and quadrature (Q) channel baseband delivery in a 20-km single loopback fiber link based on 1-GHz reflective semiconductor optical amplifiers (RSOAs) for a colorless optical network unit (ONU). Adaptive loading process was applied to the OFDM signals to overcome the bandwidth limitation of RSOAs. The I and Q channel data streams in the OFDM signals were separately carried on individual optical carriers with different wavelengths without Hermitian

Symmetry for baseband transmission. Our proposed scheme was experimentally demonstrated using a periodic property of free spectral range (FSR) in a wavelength multiplexer. The separated optical "dual" carriers were provided by the same port of a wavelength multiplexer to reduce the number of used WDM channels for a upstream.

Paper 12	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Flexible Group Key Exchange with On-demand Computation of Subgroup Keys Supporting Subgroup Key Randomization

Keita Emura

National Institute of Information and Communications Technology (NICT), Koganei, Japan

Takashi Sato

Japan Advanced Institute of Science and Technology (JAIST), Nomi, Japan

Keywords: Group Key Exchange, On-demand Computation of Subgroup Keys.

Abstract: In AFRICACRYPT2010, Abdalla, Chevalier, Manulis, and Pointcheval proposed an improvement of group key exchange (GKE), denoted by GKE+S, which enables on-demand derivation of independent secret subgroup key for all potential subsets. On-demand derivation is efficient (actually, it requires only one round) compared with GKE for subgroup (which requires two or more rounds, usually) by re-using values which was used for the initial GKE session for superior group. In this paper, we improve the Abdalla et al. GKE+S protocol to support key randomization. In our GKE+S protocol, the subgroup key derivation algorithm is probabilistic, whereas it is deterministic in the original Abdalla et al. GKE+S protocol. All subgroup member can compute the new subgroup key (e.g., for countermeasure of subgroup key leakage) with just one-round additional complexity. Our subgroup key establishment methodology is inspired by the "essential idea" of the NAXOS technique. Our GKE+S protocol is authenticated key exchange (AKE) secure under the Gap Diffie-Hellman assumption in the random oracle model.

Paper 26	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

On Secure Communication over Wireless Sensor Networks

Stefan Rass

Universität Klagenfurt, Klagenfurt, Austria

Michał Koza

Wrocław University of Technology, Wrocław, Poland

Keywords: Wireless Sensor Network, Security: Secrecy, Secret Sharing, Perfectly Secure Message Transmission.

Abstract: This paper investigates (perfectly) secure message transmission over a wireless sensor network. Using a layered network architecture and a very simple form of routing, we show how to construct an arbitrarily secure communication channel over a given infrastructure of wireless devices. Our construction is computationally cheap and requires no cryptographic primitive beyond symmetric encryption on the channels. The security of the transmission can be made arbitrarily strong (in an information-theoretic sense).

Paper 87	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Attack Modelling and Security Evaluation for Security Information and Event Management

Igor Kotenko, Andrey Chechulin and Evgenia Novikova

St. Petersburg Institute for Informatics and Automation (SPIIRAS), Saint-Petersburg, Russian Federation

Keywords: Attack Modelling, Security Evaluation, Security Information and Event Management Systems, Attack Graph, Service Dependences Graph, Zero Day Vulnerabilities.

Abstract: The paper considers an approach to attack modelling in Security Information and Event Management (SIEM) systems. The suggested approach incorporates usage of service dependency graphs and zero-day vulnerabilities to produce attack graph, calculation of security metrics based on attack graph and service dependencies and advanced any-time techniques for attack graph generation and security evaluation, etc.

Paper 135	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

The Concept of Compatibility between Identity-based and Certificateless Encryption Schemes

Antigoni Polychroniadou

University of London, Egham, U.K.

Konstantinos Chalkias, George Stephanides

University of Macedonia, Thessaloniki, Greece

Keywords: Compatibility, Identity-based Encryption, Certificateless Encryption, Protocol Classification, Efficiency Comparison.

Abstract: This paper introduces the concept of compatibility and presents an extended classification of two IBE-related schemes, the Identity-Based Encryption (IBE) and the Certificate-Less Encryption (CLE) in order to implement compatible systems. It cannot be denied that IBE, which can be extended to support a plethora of encryption models, gains widespread adoption day by day as it solves problems within conventional public key schemes and it results in a simplified key management, making it much more lightweight to deploy. Based on the fact that a number of different encryption schemes stemmed from IBE, an implementation of an IBE-related compatible system enables a number of different encryptions on-the-fly based on the user's needs at a specific moment. Our approach categorizes known concrete constructions from two IBE-related types into classes and analyzes similarities concerning public settings, used keys, protocol structures and provided model of provable security. Therefore, we consider compatibility issues between CLE and IBE and we conclude that a significant number of them are closely related. Therefore, the concept of compatibility can be put into practice.

Paper 143	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

iSATS: Leveraging Identity based Sender Authentication for Spam Mitigation

Sufian Hameed, Tobias Kloht and Xiaoming Fu

University of Göttingen, Göttingen, Germany

Keywords: Email Sender Authentication, Spam Prevention, Identity based Cryptography.

Abstract: A vast majority of spam emails today are sent from botnets with forged sender addresses. This has attracted researchers over the years to develop email sender authentication mechanism as a promising way to verify identity of the senders. In this paper we introduce *iSATS*, a new email sender authentication system based on Identity-based public key cryptography. *iSATS* leverages an identity based signature scheme to provide a reliable and easy way to bind the identity of legitimate sender to an email. Unlike the popular existing solutions like SPF and DKIM, it is hard for the spammer to adopt *iSATS*.

Paper 160	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Defense Against TCP Flooding Attack

Seungyong Yoon, Jintae Oh, Ikkyun Kim and Jongsoo Jang

Electronics and Telecommunications Research Institute, Daejeon, Korea, Republic of

Keywords: DDoS, TCP Flooding Attack.

Abstract: This paper generally relates to a DDoS attack prevention method, more particularly, to a Transmission Control Protocol (TCP) flooding attack prevention method which defines several session states based on the type and direction of a packet, tracks the session state for each flow, and detects and responds to a flooding attack. An anti-DDoS system with a capacity of 20Gbps throughput, we call 'ALADDIN' system, was implemented in FPGA based reconfigurable hardware. The possibility of high-speed hardware implementation was shown in this paper. The system was tested using existing DDoS attack tools in 8Gbps of background traffic. According to the test results, TCP flooding attacks could be defended through our proposed method rapidly and accurately.

Paper 167	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Network-based Executable File Extraction and Analysis for Malware Detection

Byoungkoo Kim[1,2], Ikkyun Kim[1] and Tai-Myoung Chung[2]

[1] *Electronics and Teletcommunicatons Research Institute, Daejeon, Korea, Republic of*

[2] *Sungkyunkwan University, Suwon, Gyeonggi-do, Korea, Republic of*

Keywords: Network Packet, Malware Detection, Region Analysis, Executable File.

Abstract: The injury by various computer viruses is over the time comprised of the tendency to increase. Therefore, various methodologies for protecting the computer system from the threats of new malicious software are actively studied. In this paper, we present a network-based executable file extraction and analysis technique for malware detection. Here, an executable file extraction is processed by executable file specific session and pattern matching in reconfiguring hardware. Next, malware detection is processed by clustering analysis technique about an executable file which is divided into many regions. In other words, it detects a malware by measuring the byte distribution similarity between malicious executable files and normal executable files. The proposed technique can detect not only the known malicious software but also the unknown malicious software. Most of all, it uses network packets as analysis source unlike the existing host anti-virus techniques. Besides, the proposed detection technique easily can detect malicious software without complicated command analysis. Therefore, our approach can minimize the load on the system execution despite the load on the additional network packet processing.

Paper 7	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Computer Games Sound Effects Recording, Postproduction and Existing Database

Bartosz Ziółko, Martyna Gromotka and Mariusz Ziółko

AGH University of Science and Technology, Kraków, Poland

Keywords: Video Games, Signal Processors, Audio Edition.

Abstract: The paper describes the process of building a new database of sound effects recordings for computer games and the first version of such product. Ways of applying signal processors for postproduction is described, as well as differences in audio edition for films and games. Some aspects of using sounds in games are also mentioned as well as the first version of the list of possible tags of the audio files in the database. Both the language of the tags and the datatabse will be substanially enlarged.

Paper 11	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

MPEG-4/AVC versus MPEG-2 in IPTV

Stefan Paulsen, Tadeus Uhl

Flensburg University of Applied Sciences, Flensburg, Germany

Krzysztof Nowicki

Gdansk University of Technology, Gdansk, Poland

Keywords: Communication Networks, Communication Services, Communication Protocols, Multimedia Applications, IPTV, QoE, PEVQ, MPEG-4/AVC, MPEG-2, ISO/IEC 13818-1 Transport Stream.

Abstract: This paper is essentially a treatment of the theoretical and practical aspects of the new IPTV service. The central part of the paper constitutes a detailed presentation of analysis scenarios and results, and addresses the following issues in particular: What influence does the encoding rate have of on QoE values? What effect does the most obtrusive impairment factor in a network, i.e. packet loss, have on QoE in IPTV? Is the MPEG-2 Transport Stream suitable for encapsulation and transport of MPEG-4/AVC content? Are there alternatives to the ISO/IEC 13818-1 Transport Stream? If so, how do they affect quality of service (QoE)?.

Paper 45	ICETE
16:30 - 17:30	Foyer
Poster Session 1	

Optimal Multidimensional Signal Processing in Wireless Sensor Networks

Anatoli Torokhti and Stan Miklavcic

University of South Australia, Mawson Lakes, Australia

Keywords: Multidimensional Signal Processing.

Abstract: Wireless sensor networks involve a set of spatially distributed sensors and a fusion center. Three methods for finding models of the sensors and the fusion center are proposed.

Paper 3 ICETE
16:30 - 17:30 Foyer
Poster Session 1

Differential Space Time Block Codes for High Mobility Scenarios

Benigno Rodríguez
Universidad de la República, Montevideo, Uruguay

Keywords: OFDM, MIMO, DSTBCs,WiMAX, LTE,Wireless Broadband Mobile Networks.

Abstract: In this paper the advantages of using a particular class of Differential Space Time Block Codes (DSTBCs) in high mobility scenarios are reported. This is a high bandwidth efficiency technique with specially good performance when the mobile terminal velocity is high. For Orthogonal Frequency Division Multiplexing (OFDM) based systems in high mobility scenarios, as the ones that can be considered for Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE), the analyzed technique reports improvements of up to 14 dB with respect to the use of 64PSK in DSTBCs.

Paper 12 ICETE
16:30 - 17:30 Foyer
Poster Session 1

Bandwidth Analysis of the Ubiquitous Video Conferencing Application

Neil Arellano, Aleksander Milshteyn, Eric Diaz, Sergio Mendoza, Helen Boussalis and Charles Liu
California State University, Los Angeles, U.S.A.

Keywords: Ubiquitous Video Conferencing (UVC), Semantic Information System Network, Tuple Space, Client-server Model, Bandwidth Metrics.

Abstract: The CSULA SPACE Center has endeavoured to develop the Semantic Information System (SIS) Network for real-time project collaboration. However, the lack of uniform, real-time communication platform application poses an inconvenience to the project collaborators, as they would be driven towards third-party communication applications, such as Skype, MSN, Yahoo Messenger, etc. The use of these commercial products does not incorporate moderation features between the network participants. In addition, these applications have various conference capacity limitations and their simultaneous multi-device sign-in feature can lead to possible concerns with information security (Alegre, 2009). The Ubiquitous Video Conferencing (UVC) application has been designed specifically for the SIS Network in order to provide its participants with dedicated multimedia channels and interactive communication. It is built on the integration of Qt libraries, audio/video codec libraries of FFMPEG, and the image-processing library Open Computer Vision. This paper presents the UVC application within the Semantic Information System Model and focuses on issues related to real-time bandwidth regulation.

Paper 42 ICETE
16:30 - 17:30 Foyer
Poster Session 1

New Mobility Metric based on MultiPoint Relay Life Duration

Ali Ouacha, Noureddine Lakki, Ahmed Habbani and Jamal El Abbadi
Université Mohammed, Rabat, Morocco

Keywords: Age of Death, MPR Selection, Link Duration, Mobility Metric, OLSR and Routing Protocols.

Abstract: Optimized Link State Routing (OLSR) is a proactive protocol designed to operate inMobile Ad Hoc Networks (MANET). In this protocol, the topology is based on MultiPoint Relay (MPR) Mechanism. However, the loss of one or many MPRs caused by their movement affects the link state of the network. Therefore, the contribution of this paper is to keep the network links between the nodes and MPRs in stable state as long as possible. It was done by calculating a new parameter named Average Age of Death which estimates the life duration ofMPRs. The experimental results illustrate that this parameter is affected by the environment (speed of node, network density and others). This result provides to use this parameter as a new mobility metric that can be used in the MPR sets Calculation.

Paper 46 ICETE
16:30 - 17:30 Foyer
Poster Session 1

Student Experience Issues of Wireless Access and Cloud Deployment in Higher Education

Vladlena Benson
Kingston University, London, U.K.

Stephanie Morgan
Kingston Business School, London, U.K.

Keywords: Mobile Applications, Wireless Networks, eLearning, Higher Education, Student Experience, Information Security, Cloud Computing.

Abstract: Universal move to wireless learning enabled through mobile apps has been evident over the last eighteen months in the higher education (HE) sector. Penetration rate of smart phones amongst students have reached a record high. Universities are investing in mobile applications enabling wireless access to current Learning Management Systems (LMS), while carefully considering benefits of the cloud for secure and flexible provision of LMS services. Capabilities of wireless devices present issues of access, presentation and compatibility of e-learning materials, while cloud infrastructure as a service raises concerns of security as data is hosted by third parties outside of the corporate firewalls. The research questions are presented for discussion through the lens of the student experience. A case of a successful move to mobile learning enablement and cloud deployment concludes the paper and opens a discussion on critical success factors in wireless e-learning operations.

Thursday Sessions

Thursday, 26

Paper 7 SECRYPT
09:00 - 10:30 Room Valencia
Parallel Session 6

Practical Applications of Homomorphic Encryption

Michael Brenner, Henning Perl and Matthew Smith
Leibniz Universitt Hannover, Hannover, Germany

Keywords: Homomorphic Encryption, Private Information Retrieval, Encrypted Search.

Abstract: Homomorphic cryptography has been one of the most interesting topics of mathematics and computer security since Gentry presented the first construction of a fully homomorphic encryption (FHE) scheme in 2009. Since then, a number of different schemes have been found, that follow the approach of bootstrapping a fully homomorphic scheme from a somewhat homomorphic foundation. All existing implementations of these systems clearly proved, that fully homomorphic encryption is not yet practical, due to significant performance limitations. However, there are many applications in the area of secure methods for cloud computing, distributed computing and delegation of computation in general, that can be implemented with homomorphic encryption schemes of limited depth. We discuss a simple algebraically homomorphic scheme over the integers that is based on the factorization of an approximate semiprime integer. We analyze the properties of the scheme and provide a couple of known protocols that can be implemented with it. We also provide a detailed discussion on searching with encrypted search terms and present implementations and performance figures for the solutions discussed in this paper.

Paper 34 SECRYPT
09:00 - 10:30 Room Valencia
Parallel Session 6

Quantitative Assessment of Cloud Security Level Agreements A Case Study

Jesus Luna Garcia, Hamza Ghani, Tsvetoslava Vateva and Neeraj Suri
Technische Universität Darmstadt, Darmstadt, Germany

Keywords: Cloud security, security assessment, security benchmarks, Security Level Agreements, security metrics.

Abstract: The users of Cloud Service Providers (CSP) often motivate their choice of providers based on criteria such as the offered service level agreements (SLA) and costs, and also recently based on security aspects (i.e., due to regulatory compliance). Unfortunately, it is quite uncommon for a CSP to specify the security levels associated with their services, hence impeding users from making security relevant informed decisions. Consequently, while the many economic and technological advantages of Cloud computing are apparent, the migration of key sector applications has been limited, in part, due to the lack of security assurance on the CSP. In order to achieve this assurance and create trustworthy Cloud ecosystems, it is desirable to develop metrics and techniques to compare, aggregate, negotiate and predict the trade-offs (features, problems and the economics) of security. This paper contributes with a quantitative security assessment case study using the CSP information found on the Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR). Our security assessment rests on the notion of Cloud Security Level Agreements — SecLA — and, a novel set of security metrics used to quantitatively compare SecLAs.

Paper 124 SECRYPT
09:00 - 10:30 Room Valencia
Parallel Session 6

Secure File Allocation and Caching in Large-scale Distributed Systems

Alessio Di Mauro
Technical University of Denmark, Lyngby, Denmark

Alessandro Mei
Sapienza University of Rome, Rome, Italy

Sushil Jajodia
George Mason University, Fairfax, U.S.A.

Keywords: Load Balancing, Distributed Systems, Secure File Allocation.

Abstract: In this paper, we present a file allocation and caching scheme that guarantees high assurance, availability, and load balancing in a large-scale distributed file system that can support dynamic updates of authorization policies. The scheme uses fragmentation and replication to store files with high security requirements in a system composed of a majority of low-security servers. We develop mechanisms to fragment files, to allocate them into multiple servers, and to cache them as close as possible to their readers while preserving the security requirement of the files, providing load-balancing, and reducing delay of read operations. The system offers a trade-off between performance and security that is dynamically tunable according to the current level of threat. We validate our mechanisms with extensive simulations in an Internet-like network.

Paper 33	SIGMAP
09:00 - 10:30	Room Sevilla
Parallel Session 6	

The Effect of Multi-media Contents in Reducing Sensible Temperature

Shuhei Yamamoto, Akira Tomono

School of Information and Telecommunication Engineering, Tokai University, Minato-ku, Tokyo, Japan

Hajime Katsuyama

Tokai University, Hiratsuka-shi, Kanagawa, Japan

Keywords: Kansei Multimedia, Sensible Temperature, Aroma, Energy Saving, Information Extraction Analysis.

Abstract: In this paper, the effect of multi-media contents such as visual images, scent, and their combinations on sensible temperature is investigated. For this purpose, a new definition of sensible temperature which takes into account the effect of visual images and scent is proposed. Using this definition, the effectiveness of multi-media contents in reducing sensible temperature was quantitatively measured. It turned out that visual images with lemon aroma is more effective in reducing sensible temperature than visual images alone.

Paper 34	SIGMAP
09:00 - 10:30	Room Sevilla
Parallel Session 6	

Image Presentation with Smell for Digital Signage and the Effect on Eye Catching

Keisuke Tomono[1], Hajime Katsuyama[2], Shuhei Yamamoto[1] and Akira Tomono[1]

[1] *Tokai University, Minato-ku, Tokyo, Japan*

[2] *Tokai University, Hiratsuka-shi, Kanagawa, Japan*

Keywords: Image, Smell, Gaze Detection, Inhalation, Tactile.

Abstract: This paper describes the effect on eye catching by digital signage that releases smell from screen and the method of smell presentation to human olfactory receptor. The effect on eye catching is investigated by analyzing movements of eye with and without smell using a detector. Visual image of foods is presented to a viewer, and his or her gazing time on a food object is detected. This experiment reveals advertisement accompanied with smell is more attracted to a viewer. The proposed method for smell presentation is to induce a person inhalation by tactile sensation caused by airflow and released smell at a time of inhalation. This experiment discusses the possibility of inducing subjects to receive smell efficiently.

Paper 42	SIGMAP
09:00 - 10:30	Room Sevilla
Parallel Session 6	

Architectural Model for Visualization of High Definition Images on Mobile Devices

Germán Corredor, Daniel Martínez, Eduardo Romero

Universidad Nacional de Colombia, Bogotá D.C., Colombia

Marcela Iregui

Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Keywords: Architecture, Decoding, Images, Interaction, JPEG2000, Mobile Devices, Protocol, Multimedia, Streaming, Visualization.

Abstract: In recent years, the mobile device demand has largely increased because of the accessibility, ubiquity and portability of such devices, which are being used not only for personal purposes but also in several applications like education, science, entertainment, commerce and industry, among others. Visualization and interaction with high definition multimedia content, like large images and videos, using mobile devices, represents a challenge because of their very limited machine resources and bandwidth. For such application, this content requires special treatment so that users can properly access and interact. In this article, it is proposed an architectural model for efficient streaming and visualization of very large images on mobile devices using the JPEG2000 standard and an adapted image transfer protocol. Results show that the introduced architecture is effective for visualizing regions of large images and presents good performance, both for transmission and decoding processes, allowing a simple and dynamic interaction between user and images.

Paper 77	SIGMAP
09:00 - 10:30	Room Sevilla
Parallel Session 6	

Content Meets Semantics: Smarter Exploration of Image Collections Presentation of Relevant Use Cases

Ilaria Bartolini

Università di Bologna, Bologna, Italy

Keywords: Image Databases, Visual Content, Semantics, Browsing.

Abstract: Current techniques for the management of image collections exploit either user-provided annotations or automatically-extracted visual features. Although effective, the approach based on annotations cannot be efficient since the manual process of data tagging prevents its scalability. On the other hand, the organization and search grounded on visual features, such as color and texture, is known to be a powerful (since it can be made fully automatic), yet imprecise, retrieval paradigm, because of the semantic gap problem. This position paper advocates the combination of visual content and semantics as a critical binomial for effectively and efficiently managing and browsing image databases satisfying users' expectations in quickly locating images of interest.

Paper 10 OPTICS
10:45 - 12:15 Room Dali
Parallel Session 7

Channel-encoded and SVD-assisted MIMO Multimode Transmission Schemes with Iterative Detection

Sebastian Aust, Andreas Ahrens and Steffen Lochmann

Hochschule Wismar, University of Technology, Business and Design, Wismar, Germany

Keywords: Multiple-input Multiple-output (MIMO) System, Singular-value Decomposition (SVD), Bit Allocation, Optical Fibre Transmission, Multimode Fiber (MMF), Bit-interleaved Coded Modulation (BICM).

Abstract: In this contribution a coherent (2 × 2) MIMO (multiple input multiple output) transmission with iterative detection over a measured multimode fiber channel at 1325 nm as well as at 1570 nm operating wavelength is studied. For the channel measurements a fibre length of 1,4 km were chosen. Extrinsic information transfer (EXIT) charts are used for analyzing and optimizing the convergence behaviour of the iterative demapping and decoding. Our results show that in order to achieve the best bit-error rate, not necessarily all MIMO layers have to be activated.

Paper 13 OPTICS
10:45 - 12:15 Room Dali
Parallel Session 7

High Repetition Frequency Mode-locked Semiconductor Disk Laser

Yanrong Song, Peng Zhang, Jinrong Tian

Beijing University of Technology, Beijing, China

Zhigang Zhang

Peking University, Beijing, China

Hark Hoe Tan, C. Jagadish

The Australian National University, Canberra, Australia

Keywords: Lasers, Diode-pumped, Ultrafast Lasers, Semiconductor Lasers.

Abstract: A compact passively mode-locked semiconductor disk laser with a high repetition frequency of 3GHz is demonstrated. 4.9ps pulse duration and 30mW average output power are obtained with 1.4W of 808nm incident pump power. The gain chip consists of 16 compressively strained InGaAs symmetrical step quantum wells in the active region.

Paper 20 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 7

Identity-based Password-Authenticated Key Exchange for Client/Server Model

Xun Yi

Victoria University, Melbourne, Australia

Raylin Tso

National Chengchi University, Taipei, Taiwan

Eiji Okamoto

University of Tsukuba, Tsukuba, Japan

Keywords: PAKE, Client/Server Model, Identity-based Encryption, Decisional Diffie-Hellman Problem.

Abstract: Password-Authenticated Key Exchange for Client/Server model (PAKE-CS) is where a client and a server, based only on their knowledge of a password, establish a cryptographic key for secure communication. In this paper, we propose a PAKE-CS protocol on the basis of identity-based encryption, where the client needs to remember a password only while the server keeps the password in addition to a private key related to his identity, where the private key is generated by multiple private key generators. Our protocol takes advantage of the features of client/server model and is more efficient than other PAKE-CS protocols in terms that it achieves explicit authentication with two-round communications only. In order to analyze the security of our protocol, we construct an ID-based formal model of security for PAKE-CS by embedding ID-based model into PAKE model. If the underlying identity-based encryption scheme has provable security without random oracle, we can provide a rigorous proof of security for our protocol without random oracles.

Paper 42 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 7

SIMD-based Implementations of Eta Pairing Over Finite Fields of Small Characteristics

Anup Kr. Bhattacharya, Abhijit Das, Dipanwita Roychowdhury
Indian Institute of Technology Kharagpur, Kharagpur, India

Bhargav Bellur, Aravind Iyer
General Motors Technical Centre India, Bangalore, India

Keywords: Supersingular Elliptic Curves, Eta Pairing, Software Implementation, SIMD, SSE Intrinsics.

Abstract: Eta pairing on supersingular elliptic curves defined over fields of characteristics two and three is a popular and practical variant of pairing used in many cryptographic protocols. In this paper, we study SIMD-based implementations of eta pairing over these fields. Our implementations use standard SIMD-based vectorization techniques which we call horizontal and vertical vectorization. To the best of our knowledge, we are the first to study vertical vectorization in the context of curves over fields of small characteristics. Our experimentation using SSE2 intrinsics reveals that vertical vectorization outperforms horizontal vectorization.

Paper 128 SECRYPT
10:45 - 12:15 Room Valencia
Parallel Session 7

Formal Analysis of the TLS Handshake Protocol

Hanane Houmani and Mourad Debbabi
Concordia University, Montreal, Canada

Keywords: TLS/SSL Protocol, Formal Analysis, Confidentiality, Secrecy.

Abstract: Most applications in the Internet as e-banking, e-commerce, e-maling, etc., use the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol to protect the communication channel between the client and the server. That is why it is paramount to ensure the security objectives such as confidentiality, authentication and integrity of the SSL/TLS protocol. In this paper we prove the confidentiality (secrecy) property of the SSL/TLS handshake protocol which consititues the main core of the SSL/TLS protocol. To perform this analysis, we introduce a new funcion called DINEK function that safeltly estimates the security level of messages. More precisely, this function which shares a conceptual origin with the idea of a rank function, allows to estimate a security level of a message (including the unknown messages) according to the interaction between the protocol and the intruder. This function could not be used only to verify the TLS protocol as we will show in this paper, but also to verify the secrecy property for large class of protocols and in particular Key Agreement protocols. The verification using the DINEK function is proven in this paper for unbounded number of sessions and unbounded number of nouces.

Paper 59 SIGMAP
10:45 - 12:15 Room Sevilla
Parallel Session 7

Keywords-based Automatic Multimedia Authoring in the Cloud

Abdelkader Outtagarts, Sylvain Squedin and Olivier Martimot
Alcatel-Lucent Bell Labs, Nozay, France

Keywords: Automatic Video Editing, Authoring, Mashups, Speech2text, Annotation, Reasoning, Collaboration, Web 2.0.

Abstract: In this paper, we describe our work on automatic multimedia authoring or editing. Our approach is based on keyword extracted from the audio embedded in videos. A model approach of mashup based on keywords is proposed. A video editing testbed has been designed and implemented. Using speech2text keywords generator component, the audio files uploaded in the video editing testbed are transcribed and analyzed in order to extract keywords. The keywords are used to edit automatically videos in order to produce mashups.

Paper 56 SIGMAP
10:45 - 12:15 Room Sevilla
Parallel Session 7

Autonomous Constructing Everyday Projected Displays

Cui Xie, Qi Wang and Wei Cheng
Ocean University of China, Qingdao, China

Keywords: Projector-based Display, Image Warping, Automatic Geometric Correction, Non-Planar Surface.

Abstract: This paper presents an autonomous geometric correction method to support constructing a projector-based large display for everyday use, which includes offline and online processing phase. The offline process is focus on an automatic, fast and robust approach for the geometric registration of projector-camera system. The online stage is mainly the implementing real-time image warping via modern graphics hardware to achieve the final corrected images without first acquiring geometric information of the screen's surface. Since a simple checkerboard pattern is used to facilitate building the mapping of the corner correspondences of projector-camera image, and a perspective projection invariant rational Bezier patch is used to approximately represent the mapping, our method saves a lot of computing time and become easier and robust. Therefore, the achieved transformation can be used for online image warping for actual projection. As a result, a layman user can get a corrected image displayed on a non-planar surface for the point of view of the camera easily.

Paper 79	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 7	

Next Generation TV through Automatic Multimedia Annotation Systems A Hybrid Approach

Joël Dumoulin[1], Marco Bertini[2], Alberto Del Bimbo[2], Elena Mugellini[1], Omar Abou Khaled[1] and Maria Sokhn[1]

[1] *HES-SO, Fribourg, Switzerland*

[2] *University of Florence, Florence, Italy*

Keywords: Automatic Video Annotation, High Level Content Annotation, Multimedia Information Retrieval, Social Video Retrieval, Tag Suggestion, User-generated Content, Smart TV.

Abstract: After the advent of smartphones, it is time for television to see its next big evolution, to become smart TVs. But to provide a richer television user experience, multimedia content first has to be enriched. In recent years, the evolution of technology has facilitated the way to take and store multimedia assets, like photographs or videos. This causes an increased difficulty in multimedia resources retrieval, mainly because of the lack of methods that handle non-textual features, both in annotation systems and search engines. Moreover, multimedia sharing websites like Flickr or YouTube, in addition to information provided by Wikipedia, offer a tremendous source of knowledge interesting to be explored. In this position paper, we address the automatic multimedia annotation issue, by proposing a hybrid system approach. We want to use unsupervised methods to find relationships between multimedia elements, referred as *hidden topics*, and then take advantage of social knowledge to label these resulting relationships. Resulting enriched multimedia content will allow to bring new user experience possibilities to the next generation television, allowing for instance the creation of recommender systems that merge this information with user profiles and behavior analysis.

Paper 85	SIGMAP
10:45 - 12:15	Room Sevilla
Parallel Session 7	

A New Tool for the Analysis of Heart Rate Variability of Long Duration Records

Ricardo Chorão[1], Joana Sousa[2], Tiago Araújo[1,2] and Hugo Gamboa[1,2]

[1] *FCT-UNL, Lisbon, Portugal*

[2] *PLUX Wireless Biosignals S.A., Lisbon, Portugal*

Keywords: ECG, Heart Rate Variability, Interactive Tool.

Abstract: The increased masses of data confronting us, originate a pressing need for the creation of a user interface for better handling and extracting knowledge from it. In this work we developed such a tool for the analysis of Heart Rate Variability (HRV). The analysis of HRV in patients with neuromuscular diseases, sleep disorders and cardiorespiratory problems has a strong impact on clinical practice. It has been widely used for monitoring the autonomic nervous system (ANS), whose regulatory effect controls the cardiac activity. These patients need to be continuously monitored, which originates data with huge sizes. Our interactive tool can perform a fast analysis of HRV from such data. It provides the analysis of HRV in time and frequency domains, and from non-linear methods. The tool is suitable to be run in a web environment, rendering it highly portable. It includes a programming feature, which enables the user to perform additional analysis of the data by giving direct access to the signals in a signal processing programming environment. We also added a report generation functionality, which is extremely important from a clinical standpoint, on which the evolution in time of relevant HRV parameters is depicted.

12:15 - 13:15 Room Plenary
On Knowledge Discovery and Interactive Intelligent Visualization of Biomedical Data - Challenges in Human–Computer Interaction & Biomedical Informatics
Keynote Speaker: Andreas Holzinger

On Knowledge Discovery and Interactive Intelligent Visualization of Biomedical Data Challenges in Human–Computer Interaction & Biomedical Informatics

Andreas Holzinger

Medical University Graz, Graz, Austria

Abstract: Biomedical Informatics can be defined as “the interdisciplinary field that studies and pursues the effective use of biomedical data, information and knowledge for scientific inquiry, problem solving, and decision making, motivated by efforts to improve human health.” However, professionals in the life sciences are faced with an increasing quantity of highly complex, multi-dimensional and weakly structured data. While researchers in Human-Computer Interaction (HCI) and Information Retrieval/Knowledge Discovery in Databases (IR/KDD) have long been independently working to develop methods that can support expert end users to identify, extract and understand information out of this data, it is obvious that an interdisciplinary approach to bring these two fields closer together can yield synergies in the application of these methods to weakly structured complex medical data sets. The aim is to support end users to learn how to interactively analyse information properties and to visualize the most relevant parts – in order to gain knowledge, and finally wisdom, to support a smarter decision making. The danger is not only to get overwhelmed by increasing masses of data, moreover there is the risk of modelling artifacts.

Paper 8 ICE-B
14:30 - 16:30 Room Dali
Parallel Session 8

Three Dimensional Elements for Sustainable e-Business Modelling

Mohammed Naim A. Dewan, Maruf Hossan Chowdhury and Mohammed A. Quaddus

Curtin University, Perth, Australia

Keywords: e-Business, Sustainability, Business Model, Blended Value.

Abstract: e-business modelling is a prevalent term now days as it converts technology into economic value. The sustainability of the business is another global contemporary issue. Although e-business modelling and sustainability are the two major global trends now but still there is no common understanding about the elements that need to be used for a sustainable e-business model. Surprisingly, none of the e-business modelling approaches even consider sustainability as a major element. In this paper, therefore, after extensive literature review on e-business modelling and sustainability of the business we carefully identify and determine the required elements for a sustainable e-business model. The elements are three dimensional and selected from customer value area, business value area, and process value area so that the modelling elements safeguard the interests of all stakeholders (customer, business, society, and environment) while maintaining the sustainability.

Paper 44 ICE-B
14:30 - 16:30 Room Dali
Parallel Session 8

Evaluating Disseminators for Time-critical Information Diffusion on Social Networks

Yung-Ming Li and Lien-Fa Lin

National Chiao Tung University, Hsinchu, Taiwan

Keywords: Social Networks, Information Diffusion, Time-critical.

Abstract: In recent years, information diffusion in social networks has received significant attention from the Internet research community driven by many potential applications such as viral marketing and sales promotions. One of the essential problems in information diffusion process is how to select a set of influential nodes as the initial nodes to disseminate the information through their social network. Most of the existing solutions aim at how to maximize the influence effectiveness of the initially selected "influential nodes", but pay little attention on how the influential nodes selection could minimize the cost of the diffusion. Diffusion effectiveness is important for the applications such as innovation and new technology diffusion. However, many applications, such as disseminating disaster information or product promotions, have the mission to deliver messages in a minimal time. In this paper, we design and implement an efficiently k-best social sites selected mechanism in such that the total diffusion “social cost” required for each user in this social network to receive the diffusion critical time information is minimized.

Paper 27	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 8	

A Framework for Performance Measurement in Service Oriented Virtual Organizations A Value Network Approach to Collaborative Performance Measurement

S. M. Amin Kamali, Greg Richards, Mohammad H. Danesh and Bijan Raahemi

University of Ottawa, Ottawa, Canada

Keywords: Virtual Organizations, Performance Measurement, Service Oriented Architecture, Value Networks.

Abstract: Management of Virtual Organizations faces unique challenges which traditional approaches cannot address. Based on service oriented architecture, this paper proposes a performance measurement framework that aligns the work of partners in a virtual organization at three different layers. The first layer is designed for partners' strategic alignment through coordination of the value creation network. In the second layer, five performance dimensions of partners' collaboration are defined which can be mapped onto the service choreography model. The third layer focuses on assessing effectiveness and efficiency of partners' domain specific services which is designed based on ITIL V3 service level management guidelines. In order to consolidate the proposed framework, these three layers are integrated using a procedure for extracting service choreography and SLA aggregation patterns from the value network. We propose an integrated solution for decentralized performance measurement without the need for a central authority. The proposed framework provides flexibility, scalability, and interoperability and enhances transparency of partners' performance information at an agreed-upon level as a basis for mutual trust.

Paper 33	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 8	

Identifying Emerging Technologies in the e-Business Industry A Needs-driven Approach

Kyungpyo Lee[1], Youngkeun Song[2] and Sungjoo Lee[1]

[1] *Ajou University, Yeongtong-Gu Suwon, Korea, Republic of*

[2] *ETRI, Daejeon, Korea, Republic of*

Keywords: Mobile Communications, Technological Characteristics, Market Characteristics, Emerging Technology, Methodology, Applications.

Abstract: Over the last few years, there have been huge efforts to forecast the technological future and emerging technologies, as an attempt to increase R&D efficiency within a limited budget. Therefore, this research purposes to develop a methodology for identifying new and promising technologies and apply it to the field of e-business. Unlike the previous studies taking a technology-driven approach, we take a needs-driven approach starting from future needs and derive a necessary technology to meet the needs. For this purpose, we firstly consider the future major using STEEP analysis. Secondly, the prospective social needs are derived from each major issue and then, the technologies required to meet the core needs are deduced to be a candidate of emerging technologies. Finally, the candidate technologies are evaluated from the viewpoint of feasibility and issues-relatedness, based on which the top 10 most important emerging technologies are determined. The suggested methodology is expected to be utilized as a valuable tool for discovering emerging technologies when considering IT is evolved not only in the form of technology-driven but also in the form of market-driven.

Thursday, 26

Paper 58	ICE-B
14:30 - 16:30	Room Dali
Parallel Session 8	

Local Governments and Cloud Computing Security

Inita Kindzule
Information Technology Centre of the Riga City, Riga, Latvia

Edzus Zeiris
ZZ Dats Ltd., Riga, Latvia

Maris Ziema
Riga Technical University, Riga, Latvia

Keywords: Local Governments, Enterprise Architecture, Cloud Computing Security, Risks Assessment, SOA, Systems Architecture.

Abstract: The Cloud computing solution has enormous potential to provide companies, industries and economy in general with remarkable benefits but there are certain challenges that have to be taken into account when choosing this solution. The purpose of this paper is to provide results of research about local governments' Cloud computing security, assisting them in making appropriate risk-based security decisions about how to securely embrace Cloud computing. To ensure that managing information of system-related security risks is consistent with the organization's mission/business objectives, and that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes.

Paper 15	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 8	

Improved "Partial Sums"-based Square Attack on AES

Michael Tunstall
University of Bristol, Bristol, U.K.

Keywords: Cryptanalysis, Square Attack, Advanced Encryption Standard.

Abstract: The Square attack as a means of attacking reduced round variants of AES was described in the initial description of the Rijndael block cipher. This attack can be applied to AES, with a relatively small number of chosen plaintext-ciphertext pairs, reduced to less than six rounds in the case of AES-128 and seven rounds otherwise and several extensions to this attack have been described in the literature. In this paper we describe new variants of these attacks that have a smaller time complexity than those present in the literature. Specifically, we demonstrate that the quantity of chosen plaintext-ciphertext pairs can be halved producing the same reduction in the time complexity. We also demonstrate that the time complexity can be halved again for attacks applied to AES-128 and reduced by a smaller factor for attacks applied to AES-192. This is achieved by eliminating hypotheses on-the-fly when bytes in consecutive subkeys are related because of the key schedule.

Paper 18	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 8	

Two Dragons
A Family of Fast Word-based Stream Ciphers

Matt Henricksen
*A*STAR, Singapore, Singapore*

Keywords: Dragon, Stream Ciphers, AES-NI, Cryptology.

Abstract: The EU eSTREAMcompetition selected two portfolios of stream ciphers, from among thirty-four candidates, with members that were either fast in software or compact in hardware. Dragon was among the eight finalists in the software category. While meeting the performance requirement of being faster than the Advanced Encryption Standard (AES) on many platforms, it was less efficient than the four ciphers selected for the portfolio. Cryptanalysis revealed some less-than-ideal properties. In this paper, we provide some new insights into Dragon, and propose two modifications: Black Dragon, which is tailored for efficient implementation in modern SIMD architectures; and Yellow Dragon, which utilizes recent developments in Chinese block ciphers. We show the improved security and performance of these two variants.

Paper 38	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 8	

Privacy-preserving Targeted Advertising Scheme for IPTV using the Cloud

Leyli Javid Khayati[1], Erkay Savaş[1], Berkant Ustaoğlu[2] and Cengiz Örencik[1]
[1] *Sabancı University, Istanbul, Turkey*
[2] *Izmir Institute of Technology, Izmir, Turkey*

Keywords: IPTV, Targeted Advertising, Privacy, Cryptography, Cloud Server.

Abstract: In this paper, we present a privacy-preserving scheme for targeted advertising via the

Internet Protocol TV (IPTV). The scheme uses a communication model involving a collection of viewers/subscribers, a content provider (IPTV), an advertiser, and a cloud server. To provide high quality directed advertising service, the advertiser can utilize not only demographic information of subscribers, but also their watching habits. The latter includes watching history, preferences for IPTV content and watching rate, which are published on the cloud server periodically (e.g. weekly) along with anonymized demographics. Since the published data may leak sensitive information about subscribers, it is safeguarded using cryptographic techniques in addition to the anonymization of demographics. The techniques used by the advertiser, which can be manifested in its queries to the cloud, are considered (trade) secrets and therefore are protected as well. The cloud is oblivious to the published data, the queries of the advertiser as well as its own responses to these queries. Only a legitimate advertiser, endorsed with a so-called *trapdoor* by the IPTV, can query the cloud and utilize the query results. The performance of the proposed scheme is evaluated with experiments, which show that the scheme is suitable for practical usage.

Paper 74	SECRYPT
14:30 - 16:30	Room Valencia
Parallel Session 8	

On Securing Communication from Profilers

Sandra Díaz-Santiago and Debrup Chakraborty
CINVESTAV IPN, Col. San Pedro Zacatenco, Mexico

Keywords: Data Encryption, Profiling Adversary, User Profiling, CAPTCHA, Secret Sharing.

Abstract: A profiling adversary is an adversary which aims to classify messages into pre-defined profiles and thus gain useful information regarding the sender or receiver of such messages. Usual chosen-plaintext secure encryption schemes are capable of securing information from profilers, but these schemes provide more security than required for this purpose. In this paper we study the requirements for an encryption algorithm to be secure only against profilers and finally give a precise notion of security for such schemes. We also present a full protocol for secure (against profiling adversaries) communication, which neither requires a key exchange nor a public key infrastructure. Our protocol guarantees security against non-human profilers and is constructed using CAPTCHAs and secret sharing schemes.

Paper 112	SECRYPT
14:30 - 16:30	Room Velazquez
Parallel Session 8a	

Secure and Seamless Session Management in Mobile and Heterogeneous Environment

Ali Hammami and Noëmie Simoni
Telecom ParisTech, Paris Cedex 13, France

Keywords: Security as a Service, Device as a Service, Mobility and Heterogeneity, Secure and Unique Session, Security Continuity, Token, SIP+, Virtual Private Device Network.

Abstract: The Next Generation Network and Services (NGN/NGS) environment becomes more and more heterogeneous and mobile. Furthermore, today user seeks to access his services within a secured session ensuring the continuity and the quality of service. This rapid evolution and requirements raise the issue of guarantying the continuity of user-centric session in an advanced mobility context. This work targets particularly access control and security aspects based on Service Oriented Architecture in mobile and heterogeneous environments. To address the aforementioned challenges, we propose a secure and seamless session management solution that is based on several concepts and mechanisms. First, this solution ensures security management that overcomes session security and uniqueness challenges by gathering ubiquitous, mutualisable, autonomous and stateless service components. Second, we present a multiple and heterogeneous terminal composition by proposing a Virtual Private Device Network (VPDN) concept that is based on secure and auto-managed components. Finally, in addition to these proposed architecture components and concepts, we introduce SIP+ in order to ensure the security continuity within a seamless session during user mobility.

Paper 113	SECRYPT
14:30 - 16:30	Room Velazquez
Parallel Session 8a	

A Collaborative Firewall for Wireless Ad-Hoc Social Networks

Leonardo Maccari
University of Trento, Povo, Italy

Keywords: Collaborative Firewall, Wireless Ad-Hoc Networks, Security, Privacy.

Abstract: A collaborative firewall can be realized in a multi-hop distributed wireless network when all or some of the nodes in the network agree on a filtering policy and enforce it when routing a packet.

Cooperative firewalling introduces many challenges, how to distribute the rules, how to enforce them, how to reduce the global rule-set in order to limit the impact on the network performance. This paper studies the performance of a collaborative firewall when only a subset of the nodes of the ad-hoc network filter the packets. In order to achieve higher performances the integration with OLSR protocol is proposed. Simulations on realistic scenarios are performed and the source code of the simulator is released.

Paper 130	SECRYPT
14:30 - 16:30	Room Velazquez
Parallel Session 8a	

Distributed Threshold Certificate based Encryption Scheme with No Trusted Dealer

Apostolos P. Fournaris
University of Patras, Patra, Greece

Keywords: Threshold Cryptography, Certificate based Encryption, Elliptic Curve Cryptography, Pairing based Cryptography, Distributed System, Certificate Authority.

Abstract: Generating certified keys and managing certification information in a fully distributed manner can find a wide range of applications in the increasingly distributed IT environment. However, the prohibition of trusted entities within the distributed system and the high complexity certificate management and revocation mechanism, hinder the adoption of this approach in a large scale. Threshold cryptography offers an elegant solution to these issues through Shamir's secret sharing scheme, where a secret (the Certificate Authority's (CA) master key) is split and shared among all participants. Combining this approach with the reasonable certificate service requirements of Certificate based encryption (CBE) schemes could result in a functional and efficient distributed security scheme. However, centralized entities, denoted as trusted dealers, are needed in most threshold cryptography schemes even those few that support CBE, while the static way in which the system's functionality is viewed, considerably limits possible applications (i.e. dynamic environments like p2p, Ad- Hoc networks, MANETS). In this paper, we explore the potentials of combining the latest developments in distributed key generation threshold cryptography schemes with efficient yet highly secure certificate based encryption schemes in order to provide a solution that matches the above concerns. We draft a fully distributed Threshold Certificate Based Encryption Scheme that has no need for any centralized entity at any point during its operating cycle, has few requirements concerning certificate management due to CBE and does not need any trusted dealer to create, and split secrets or distribute certificates. The proposed scheme has an easy participant addition-removal procedure to support dynamic environments.

Paper 131	SECRYPT
14:30 - 16:30	Room Velazquez
Parallel Session 8a	

Improving Cloud Survivability through Dependency based Virtual Machine Placement

Min Li[1], Yulong Zhang[1], Kun Bai[2], Wanyu Zang[1], Meng Yu[1] and Xubin He[1]
[1] *Virginia Commonwealth University, Richmond, U.S.A.*
[2] *IBM T.J. Watson Research Center, Cambridge, U.S.A.*

Keywords: Cloud Computing, Virtual Machine Placement, Security, Survivability.

Abstract: Cloud computing is becoming more and more popular in computing infrastructure and it also introduces new security problems. For example, a physical server shared by many virtual machines can be taken over by an attacker if the virtual machine monitor is compromised through one of the virtual machines. Thus, collocating with vulnerable virtual machines, or “bad neighbours”, on the same physical server introduces additional security risks. Moreover, the connections between virtual machines, such as the network connection between a web server and its back end database server, are natural paths of attacks. Therefore, both virtual machine placement and connections among virtual machines in the cloud have great impact over the overall security of cloud. In this paper, we quantify the security risks of cloud environments based on virtual machine vulnerabilities and placement schemes. Based on our security evaluation, we develop techniques to generate virtual machine placement that can minimize the security risks considering the connections among virtual machines. According to the experimental results, our approach can greatly improve the survivability of most virtual machines and the whole cloud. The computing costs and deployment costs of our techniques are also practical.

Paper 132 SECRYPT
14:30 - 16:30 Room Velazquez
Parallel Session 8a

PPiTTA - Preserving Privacy in TV Targeted Advertising

Tzachy Reinman[1,2] and Erez Waisbard[3,2]
[1] *The Hebrew University of Jerusalem, Jerusalem, Israel*
[2] *NDS Technologies Ltd, Jerusalem, Israel*
[3] *Bar Ilan University, Ramat Gan, Israel*

Keywords: Privacy, Targeted Advertising.

Abstract: Targeted advertising involves using a person's personal data to determine the most promising commercials to show that person. While the benefits are clear, the price paid in terms of loss of privacy may be high. In this work we bridge what seems at first to be contradicting requirements – the ability to personalize data and the need to maintain privacy, especially while reporting back the impressions to the advertiser. We provide two schemes that achieve this, each in its own adversarial model. We put an emphasis on modern TV systems and describe the architecture for supporting it.

Paper 140 SECRYPT
14:30 - 16:30 Room Velazquez
Parallel Session 8a

Improved Detection of Probe Request Attacks Using Neural Networks and Genetic Algorithm

Deepthi N. Ratnayake, Hassan B. Kazemian
Faculty of Computing, London Metropolitan University, London, U.K.
Syed A. Yusuf
University of Portsmouth, Portsmouth, U.K.

Keywords: Wlan Security, Probe Request Flooding Attacks, Neural Networks, Genetic Algorithms.

Abstract: The Media Access Control (MAC) layer of the wireless protocol, Institute of Electrical and Electronics Engineers (IEEE) 802.11, is based on the exchange of request and response messages. Probe Request Flooding Attacks (PRFA) are devised based on this design flaw to reduce network performance or prevent legitimate users from accessing network resources. The vulnerability is amplified due to clear beacon, probe request and probe response frames. The research is to detect PRFA of Wireless Local Area Networks (WLAN) using a Supervised Feedforward Neural Network (NN). The NN converged outstandingly with train, valid, test sample percentages 70, 15, 15 and hidden neurons 20. The effectiveness of an Intruder Detection System depends on its prediction accuracy. This paper presents optimisation of the NN using Genetic Algorithms (GA). GAs sought to maximise the performance of the model based on Linear Regression (R) and generated R > 0.95. Novelty of this research lies in the fact that the NN accepts user and attacker training data captured separately. Hence, security administrators do not have to perform the painstaking task of manually identifying individual frames for labelling prior training. The GA provides a reliable NN model and recognises the behaviour of the NN for diverse configurations.

Paper 13 SIGMAP
14:30 - 16:30 Room Sevilla
Parallel Session 8

Fast Algorithm of Short-time DCT for Low Resolution Signal Processing

Vitaly Kober
CICESE, Ensenada, Mexico

Keywords: Discrete Cosine Transform, Fast Algorithm.

Abstract: A fast algorithm for computing the discrete cosine transform (DCT) in a window running on a signal with a step higher than one is proposed. The algorithm is based on a second-order recursive relation between DCT spectra computed in windows which are equally spaced with a given distance. The computational complexity of the proposed algorithm is compared with that of common fast and running DCT algorithms. A fast inverse DCT transform is also presented.

Paper 38 SIGMAP
14:30 - 16:30 Room Sevilla
Parallel Session 8

Sphere Decoding Complexity Reduction using an Adaptive SD-OSIC Algorithm

Bora Kim, Sangmi Moon, Saransh Malik, Cheolhong Kim and Intae Hwang
Chonnam National University, Gwangju, Korea, Republic of

Keywords: Link Adaptation, MIMO, OSIC, SNR, Sphere Decoding.

Abstract: Sphere decoding is a technique able to achieve the optimal performance of the maximum likelihood decoder, but its high and variable complexity can make the practical implementation infeasible. In this paper, we present an adaptive system, called adaptive SD-OSIC, as a way of reducing the decoding complexity while maintaining the error performance of conventional sphere

decoding.

Paper 46	SIGMAP
14:30 - 16:30	Room Sevilla
Parallel Session 8	

Finding a Tradeoff between Compression and Loss in Motion Compensated Video Coding

Thomas Guthier[1,2], Adrian Sosic[1], Volker Willert[1] and Julian Eggert[2]

[1] *TU Darmstadt, Darmstadt, Germany*

[2] *Honda Research Institute Europe, Offenbach, Germany*

Keywords: Video Coding, Polynomial Motion Model, Quadtree Segmentation, Model Selection.

Abstract: In video coding, affine motion models combined with a quadtree decomposition have often been suggested as an extension to the mostly used translational models combined with a blockwise decomposition. What is missing so far is a thorough analysis to judge the tradeoff between using more complex motion models or more elaborate decomposition methods in terms of data compression and information loss. In this paper, we compare different polynomial motion models with a quadtree decomposition concerning motion model complexity and granularity of decomposition. We provide a statistical evaluation based on optical flow databases to quantitatively find a tradeoff between bitrate and reconstruction error.

Paper 54	SIGMAP
14:30 - 16:30	Room Sevilla
Parallel Session 8	

New Two-step Motion Estimation using Adjustable Partial Distortion Search Advanced Selected Search Point and Early Termination for Two Step Motion Search

Yonghoon Kim and Jechang Jeong

Hanyang University, Seoul, Korea, Republic of

Keywords: Video Coding, Fast Motion Estimation, Two-step Motion Search.

Abstract: In this paper, we proposed an advanced two-step motion estimation using adjustable partial distortion for fast motion estimation. We improve the two-step search by using relationship between neighboring and current block. The proposed algorithm is 187 times faster than FS and 2.7 times faster than TS-EPDS without negligible PSNR degradation. Therefore, it is suitable for real-time video implementation.

Paper 55	SIGMAP
14:30 - 16:30	Room Sevilla
Parallel Session 8	

Video Foreground/Background Segmentation using Spatially Distributed Model and Edge-based Shadow Cancellation

Shian-De Tsai, Jin-Jang Leou and Han-Hui Hsiao

National Chung Cheng University, Chiayi, Taiwan

Keywords: Video Foreground/Background Segmentation, Spatially Distributed Model, Edge-based Shadow Cancellation.

Abstract: Video foreground/background segmentation is to extract relevant objects (the foreground) from the background of a video sequence, which is an important step in many computer vision applications. In this study, the spatially distributed model is built by a splitting process using Gaussian probability distribution functions in spatial and color spaces. Then, edge-based shadow cancellation is employed to obtain more robust segmentation results. The proposed approach can well handle illumination variations, shadow effect, and dynamic scenes in video sequences. Based on experimental results obtained in this study, as compared with two comparison approaches, the proposed approach provides the better video segmentation results.

Paper 61	SIGMAP
14:30 - 16:30	Room Sevilla
Parallel Session 8	

Raw Camera Image Demosaicing using Finite Impulse Response Filtering on Commodity GPU Hardware using CUDA

Patrik Goorts, Sammy Rogmans and Philippe Bekaert

Hasselt University, Diepenbeek, Belgium

Keywords: Demosaicing, Bayer, Finite Impulse Response Filtering, GPU, CUDA.

Abstract: In this paper, we investigate demosaicing of raw camera images on parallel architectures using CUDA. To generate high-quality results, we use the method of Malvar et al., which incorporates the gradient for edgesensing demosaicing. The method can be implemented as a collection of finite impulse response filters, which can easily be mapped to a parallel architecture. We investigated different trade-offs between memory operations and processor occupation to acquire maximum performance, and found a clear difference in optimization principles between different GPU architecture designs. We show that trade-offs are still important and not

straightforward when using systems with massive fast processors and slower memory.

Paper 62	SIGMAP
14:30 - 16:30	Room Sevilla
Parallel Session 8	

A Dataflow Description of ACC-JPEG Codec

Khaled Jerbi[1,2], Tarek Ouni[1] and Mohamed Abid[1]

[1] *National Engineering School of Sfax, Sfax, Tunisia*

[2] *IETR/INSA, UMR CNRS 6164, Rennes, France*

Keywords: Video Compression, Accordeon, Dataflow, MPEG RVC.

Abstract: Video codec standards evolution raises two major problems. The first one is the design complexity which makes very difficult the video coders implementation. The second is the computing capability demanding which requires complex and advanced architectures. To decline the first problem, MPEG normalized the Reconfigurable Video Coding (RVC) standard which allows the reutilization of some generic image processing modules for advanced video coders. However, the second problem still remains unsolved. Actually, technology development becomes incapable to answer the current standards algorithmic increasing complexity. In this paper, we propose an efficient solution for the two problems by applying the RVC methodology and its associated tools on a new video coding model called Accordion based video coding. The main advantage of this video coding model consists in its capacity of providing high compression efficiency with low complexity which is able to resolve the second video coding problem.

Paper 3	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

Analysing E-Business Applications with Business Provenance

Sergio Manuel Serra da Cruz

Universidade Federal Rural do Rio de Janeiro, Seropédica, Brazil

Laci Mary Manhães, Raimundo Costa, Jorge Zavaleta

Universidade Federal Rio de Janeiro, Ilha do Fundão, Brazil

Keywords: Business Provenance, Web Services, SOA, E-Business.

Abstract: Business Provenance provides important documentation that is an essential to increase the trustworthiness and traceability of end-to-end business operations. This paper presents two data marts that allows multidimensional analysis of business provenance metadata collected from a real e-business scenario. Provenance was collected with the aid of an architecture named BizProv. We conclude the paper with the identification of the challenges that will drive future research of BizProv.

Paper 6	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

IS Employees' Stress and Outcomes at Work

Huichih Wang

National Chiao Tung University, Hsinchu, Taiwan

Sheng-Jim Fan

National Chung Cheng University, Chiayi, Taiwan

Her-Sen Doong

National Chiayi University, Chiayi, Taiwan

Keywords: Information Systems, Absenteeism, Occupational Stress.

Abstract: The problem of excessive occupational stress faced by IS employees may accelerate their intention to quit, which may ultimately cause companies difficulty in finding skilled professionals and a huge cost in training newcomers. A handful of past studies in the information system discipline have examined this connection from the perspective of job satisfaction to some extent. However, employees' behavioral outcomes resulting from their excessive stress are not limited to intention to quit: job performance and absenteeism, which were significantly associated with organizational effectiveness, were unfortunately overlooked in the IS studies. To broaden the knowledge in IS personnel management, the current study has incorporated the literature from psychology and organizational behavior to propose a theoretically based model. Findings will be able to provide fruitful implications for future researchers and practitioners.

Paper 10	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

A Study on Older Adult Students' Behavioural Intention and Learning Satisfaction of Blended e-Learning Course at the Active Aging University

Horng-Jyh Chen[1], Chien-Jen Liu[2], Chien-Liang Lin[3], Yi-Fang Chen[2] and Hung-Liang Chen[4]

[1] *Kao-Yuan University, Kaohsiung, Taiwan*

[2] *National Sun Yat-sen University, Kaohsiung, Taiwan*

[3] *National Cheng Chi University, Taipei, Taiwan*

[4] *Chia-Nan University, Tainan, Taiwan*

Keywords: Active Aging University, Blended e-Learning, Behavioural Intention, Learning Satisfaction, Structural Equation Model (SEM).

Abstract: Recently, the blended e-learning is implemented in many fields more and more popularly. In this paper, the program of ceramics teaching at the Active Aging University is also applied blended e-learning without exception in order to raise older adult students' behavioural intention and learning satisfaction. Because of the unfamiliar with IT technology application for these older adult students the different results from most of younger students in this investigation are expected. In this study, the questionnaire is designed for 44 older adult students whose ages are all over 55 years old. The teaching experiment of blended e-learning for ceramics teaching course is performed at the Active Aging University in the southern of Taiwan. And the Structural Equation Model (SEM) quantitative analysis is carried out that the conclusions are got with the perceived usefulness of learning contents has positive relationship with learning satisfaction. Also, the perceived ease of use for interfaces has positive relationship with the perceived usefulness of learning contents and learning satisfaction. Therefore, these conclusions could be applied to develop and design for all the blended e-learning programs at the Active Aging University with the best teaching and learning strategy in the future.

Paper 13	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

Factors that Influence e-Business Application in Tertiary Education

Andreas Ahrens, Sebastian Aust

University of Technology, Business and Design, Wismar, Germany

Jeļena Zaščerinska

Centre for Education and Innovation Research, Riga, Latvia

Keywords: e-Business Application, Tertiary Education, External Factors, Internal Factors.

Abstract: e-Business has dramatically influenced progress in all the dimensions of modern life in the context of globalisation. Education is one of these dimensions. Moreover, e-Business and tertiary education are interdependent. However, success in application of e-Business technologies in tertiary education can be changed by its factors. Aim of the present paper is to analyze factors that influence e-Business application in tertiary education. The meaning of the key concepts of *e-business technologies* and factors is studied. Moreover, the study demonstrates how the key concepts are related to the idea of *tertiary education* and shows a potential model for development, indicating how the steps of the process are related following a logical chain: *e-business technologies* → the role of e-business application in tertiary education → factors → empirical study within a multicultural environment. The results of the present research show that the external factors and, particularly, factors forming communication influence e-business application in tertiary education. Directions of further research are proposed.

Paper 22	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

lmRNG: A Lightweight Pseudorandom Number Generator for Wireless Sensor Networks

Anna Sojka and Krzysztof Piotrowski

IHP, Frankfurt (Oder), Germany

Keywords: Wireless Sensor Network, Pseudorandom Number Generator, Lightweight Security.

Abstract: Wireless sensor networks (WSN) are often used in the areas where the data security is very important. The cryptographic protocols developed for WSN need to be as computationally inexpensive as possible due to the energy and computational constraints of WSN. The same requirements concern also the elements of these protocols, e.g. the random number generator. In this paper we present our work on a pseudorandom number generator for wireless sensor networks. It uses a modification of the LogisticMap, which is adapted to be used in the constrained environment of the WSN. In our approach we combine a non-deterministic seed source with the deterministic function to get the pseudorandom number generator. We present the results of the tests confirming that our approach fulfils the requirements of randomness and is a candidate to be used for cryptographic purposes.

Paper 68	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

Non-repudiation of Forwarding Traceability of Confidential Data Via Multiple Recipients

Rainer Schick and Christoph Ruland

University of Siegen, Siegen, Germany

Keywords: Non-repudiation, Data Leakage Protection, Security Service, Data Tracking, Evidence Generation.

Abstract: Nowadays, it can be assumed that valuable private data can be securely transmitted from one sender to one (or more) recipients. An unsolved problem following the transmission is addressed by this paper. The sender of some confidential information does not know what happens with the data after the transmission. If the message appears in a place it should not, the originator does not know who published it unauthorized. In order to solve this problem, this paper introduces a new non-repudiation service that allows tracking the way of protected data via several recipients.

Paper 106	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

Sevigator: Network Confinement of Malware Applications and Untrusted Operating Systems

Denis Efremov and Nikolay Pakulin

Institute for System Programming, Moscow, Russian Federation

Keywords: Virtualization-based Security, Network Access Control, Hypervisor, Virtual Machine Monitor, Virtualization, Security, Privacy Protection.

Abstract: This project is an attempt to combine the advantages of software flexibility and security of hardware firewalls. It aims at the implementation of these advantages in the hypervisor source code for the purpose of creating user data confidentiality protection against its leakage from the personal computer through the network. The hypervisor implementation is based on the hardware virtualization extensions of both processors and motherboards. This constitutes a key feature, which enables hypervisor to combine the following advantages: the advantages of access to the OS environment and hardware protection against various intruders' methods of compromise, including those capable of exploiting OS kernel resources for performing the malicious actions.

Paper 120	ICETE
16:30 - 17:30	Foyer
Poster Session 2	

Development of a Snort IPv6 Plugin Detection of Attacks on the Neighbor Discovery Protocol

Martin Schütte, Thomas Scheffler

Beuth University of Applied Sciences, Berlin, Germany

Bettina Schnor

Potsdam University, Potsdam, Germany

Keywords: IPv6, Neighbor Discovery, Intrusion Detection System.

Abstract: This paper describes the implementation and use of a preprocessor module for the open source Intrusion Detection System Snort. Our implementation utilizes preprocessor APIs for the extension of Snort and provides several new IPv6-specific rule options that make the definition of IPv6-specific attack signatures possible. The preprocessor detects attacks against the IPv6 Neighbor Discovery Protocol and can identify suspicious activity in local IPv6 networks. This includes misconfigured network elements, as well as malicious activities from attackers on the network. To our knowledge this is the first such implementation in an Open Source IDS.

Paper 153 ICETE
16:30 - 17:30 Foyer
Poster Session 2

Adaptive Speech Watermarking in Wavelet Domain based on Logarithm

Mehdi Fallahpour, David Megias
Universitat Oberta de Catalunya, Barcelona, Spain

Hossein Najaf-Zadeh
Advanced Audio Systems, Communications Research Centre Canada (CRC), Ottawa, Spain

Keywords: Speech Watermarking, Data Hiding, Wavelet Transform, Logarithm.

Abstract: Considering the fact that the human auditory system requires more precision at low amplitudes, the use of a logarithmic quantization algorithm is an appropriate design strategy. Logarithmic quantization is used for the approximation coefficients of a wavelet transform to embed the secret bits. To improve robustness, the approximation coefficients are packed into frames and each secret bit is embedded into a frame. The experimental results show that the distortion caused by the embedding algorithm is adjustable and lower than that introduced by a standard ITU-T G.723.1 codec. Therefore, the marked signal has high quality (PESQ-MOS score around 4.0) and the watermarking scheme is transparent. The capacity is adjustable and ranges from very low bit-rates to 4000 bits per second. The scheme is shown to be robust against different attacks such as ITU-T G.711 (a-law and u-law companding), amplification and low-pass RC filters.

Paper 163 ICETE
16:30 - 17:30 Foyer
Poster Session 2

An Application of a Group Signature Scheme with Backward Unlinkability to Biometric Identity Management

Julien Bringer[1], Hervé Chabanne[1,2] and Alain Patey[1,2]
[1] *Morpho, Issy-Les-Moulineaux, France*
[2] *Télécom ParisTech, Paris, France*

Keywords: Group Signatures, Identity Management, Derivation, Cascade Revocation, Biometrics, Anonymity.

Abstract: We introduce a new identity management process in a setting where users' identities are credentials for anonymous authentications. Considering identity domains organized in a tree structure, where applying for a new identity requires to previously own the parent identity, we enable a cascade revocation process that takes into account this structure while ensuring anonymity for non-revoked users, in particular, towards the providers of other identity domains. Our construction is based on the group signature scheme of (Bringer and Patey, 2012).

Paper 164 ICETE
16:30 - 17:30 Foyer
Poster Session 2

A Novel Fuzzy Vault Scheme for Secret Key Exchange

Lin You
Hangzhou Dianzi University, Hangzhou, China

Jie Lu
Zhejiang Wellcom Technology Co., Ltd, Hangzhou, China

Keywords: Fuzzy Vault, Secret Key Exchange, Finite Group, Biometrics, Polynomial Interpolation.

Abstract: Based on the classical fuzzy vault and the Diffie-Hellman key exchange scheme, a novel fuzzy vault scheme for the secret key exchange is proposed. In this fuzzy vault scheme, the two users can respectively use their biometric features to unlock the fuzzy vault to get their shared secret key without running the risk of disclosure of their biometric features. The security of our scheme is based on the polynomial reconstruction problem and the discrete logarithm problem in a given finite group.

Paper 173 ICETE
16:30 - 17:30 Foyer
Poster Session 2

HoneyCloud: Elastic Honeypots On-attack Provisioning of High-interaction Honeypots

Patrice Clemente, Jean-Francois Lalande
ENSI de Bourges, LIFO, Bourges, France

Jonathan Rouzaud-Cornabas
INRIA, ENS Lyon, Lyon, France

Keywords: Honeypot, Cloud Computing, Security.

Abstract: This paper presents HoneyCloud: a large-scale high-interaction honeypots architecture based on a cloud infrastructure. The paper shows how to setup and deploy on-demand virtualized honeypot hosts on a private cloud. Each attacker is elastically assigned to a new virtual honeypot instance. HoneyCloud offers a high scalability. With a small number of public IP addresses, HoneyCloud can multiplex thousands of attackers. The attacker can perform malicious activities on the honeypot and launch new attacks from the compromised host. The HoneyCloud architecture is designed to collect operating system logs about attacks, from various IDS, tools and sensors. Each virtual honeypot instance includes network and especially system sensors that gather more useful information than traditional network oriented honeypots. The paper shows how are collected the activities of attackers into the cloud storage mechanism for further forensics. HoneyCloud also addresses efficient attacker's session storage, long term session management, isolation between attackers and fidelity of hosts.

Paper 174 ICETE
16:30 - 17:30 Foyer
Poster Session 2

A Proposed Framework for Analysing Security Ceremonies

Marcelo Carlomagno Carlos[1], Jean Everson Martina[2], Geraint Price[1] and Ricardo Felipe Custódio[2]

[1] *Royal Holloway University of London, Egham, U.K.*

[2] *Universidade Federal de Santa Catarina, Florianópolis, Brazil*

Keywords: Security Ceremonies, Security Protocols, Formal Methods, Cognitive Human Formalisation.

Abstract: The concept of a ceremony as an extension of network and security protocols was introduced by Ellison. There are no currently available methods or tools to check correctness of the properties in such ceremonies. The potential application for security ceremonies are vast and fill gaps left by strong assumptions in security protocols. Assumptions include the provision of cryptographic keys and correct human interaction. Moreover, no tools are available to check how knowledge is distributed among human peers nor their interaction with other humans and computers in these scenarios. The key component of this position paper is the formalisation of human knowledge distribution in security ceremonies. By properly enlisting human expectations and interactions in security protocols, we can minimise the ill-described assumptions we usually see failing. Taking such issues into account when designing or verifying protocols can help us to better understand where protocols are more prone to break due to human constraints.

Paper 8 ICETE
16:30 - 17:30 Foyer
Poster Session 2

Complexity Analysis of Video Frames by Corresponding Audio Features

SeungHo Shin and TaeYong Kim

Chung-Ang University, Seoul, Korea, Republic of

Keywords: Video Complexity Analysis, Video Indexing, Audio Indexing, Rate-control.

Abstract: In this paper, we propose a method to estimate the video complexity by using audio features based on human synesthesia factors. By analyzing the features of audio segments related to video frames, we initially estimate the complexity of the video frames and can improve the performance of video compression. The effectiveness of proposed method is verified by applying it to an actual H.264/AVC Rate-Control.

Paper 12 ICETE
16:30 - 17:30 Foyer
Poster Session 2

Design of Short Irregular LDPC Codes for a Markov-modulated Gaussian Channel

W. Proß[1,2], M. Otesteanu[1] and F. Quint[2]

[1] *Politehnica University of Timisoara, Timisoara, Romania*

[2] *University of Applied Sciences, Karlsruhe, Germany*

Keywords: Irregular LDPC Codes, Density-evolution, Downhill-simplex, Markov-modulated Gaussian Channel.

Abstract: This paper deals with the design of short irregular Low-Density Parity-Check (LDPC) codes. An optimization method for the underlying symbol-node degree-distribution (SNDD) of an irregular LDPC code is introduced, which is based on the Downhill-Simplex (DHS) algorithm. In order to compare our method with the optimization described in (Hu et al., 2005), which is based on a simplified version of the DHS algorithm, we first designed a rate 0.5 irregular LDPC code of length $n = 504$ for an Additive White Gaussian Noise Channel (AWGNC). The proposed optimization method was then used to design an irregular LDPC code for a Markov-modulated Gaussian Channel (MMGC). The decoding performance of the resulting LDPC code is then compared to the design based on the Density-Evolution (DE) method.

Paper 40 ICETE
16:30 - 17:30 Foyer
Poster Session 2

Enhancing Photoware in the Social Networks Environment

Ombretta Gaggi
University of Padua, Padua, Italy

Keywords: Digital Photo Management, Social Network.

Abstract: This paper presents *SMIL PhotoShow*, an authoring tool for photo books, which allows the creation of enhanced multimedia presentations, enriched with audio (music or spoken) comments, transition effects and animations in a very simple way. Our tool allows to create a digital counterpart of a printed photo book with the aim to bridge the gap between digital web albums and printed photo books. Since authoring a photo book is a time consuming activity, *SMIL PhotoShow* provides the users also the possibility to create, with only three clicks, an engaging slideshows with transition effects and background music.

Paper 51 ICETE
16:30 - 17:30 Foyer
Poster Session 2

Search Range Adjustment and Motion Vector Prediction for Fast Motion Estimation Using Neighbouring Motion Vectors and Distortions for Adjustment of a Search Range and a Starting Point

Do-Kyung Lee and Je-Chang Jeong
Hanyang University, Seoul, Korea, Republic of

Keywords: Fast Motion Estimation, Search Range Adjustment, Motion Vector Prediction, Partial Distortion Search, Block Matching Algorithm.

Abstract: The block matching algorithm has been widely used for motion estimation, but it suffers from heavy computational complexity. Many researchers in video processing area have proposed fast motion estimation algorithms by adopting various ways to reduce its complexity. In this paper, we introduce a conventional method controlling a search range and defining a new starting point, and also discuss our proposed method which supplements previous work by using neighbouring block's motion vectors and distortions. Consequently, we obtained remarkable performance about 80 times faster than full search and 2.6 times faster than conventional algorithm with small video quality improvement in terms of PSNR. Therefore, the proposed method can be applied for real-time video processing applications.

Paper 65 ICETE
16:30 - 17:30 Foyer
Poster Session 2

Friction Sources Characterization for Fricative Consonants of Arabic

Fazia Karaoui and Amar Djéradi
Université des Sciences et Technologies Houari Boumediene, Beb Ezzouar Alger, Algeria

Keywords: Fricatives Consonants, Vocal Tract Transfer Function, Noise Source Model.

Abstract: The objective of this work is the acoustic characterization of the friction source for Arabic voiced consonants [v], [z], $[Z]$, [h], $[\varsigma]$ and unvoiced ones [s], [f], $[S]$, $[\hbar]$, employing vocal tract transfer function obtained from a direct measurement by the Pseudo Random Excitation of the human vocal tract and the signal spectrum radiated at the lips. Assuming the separability of the source of the vocal tract considered as a linear filter, the sources spectrum is obtained by the ratio of the output signal spectrum of the vocal tract transfer function. The results are derived from data produced by two female and two male subjects.

Friday Sessions

Paper 41 ICE-B
09:15 - 10:15 Room Dali
Parallel Session 9

Usability of Mobile Applications Dissemination of Usability Engineering in Small and Medium Enterprises

Britta Fuchs, Thomas Ritz and Jakob Strauch
FH Aachen, Aachen, Germany

Keywords: Usability Engineering, Mobile Applications, SME, User-centred Development.

Abstract: This paper starts from the idea that mobile enterprise software has great potential in the future but needs to fulfil usability requirements to be successful. Following mobile enterprise software Mobile enterprise software is explained with the established software engineering processes. Related to this topic usability engineering is presented with relevance to the utilization in small and medium-sized enterprises (SMEs). The relevance of the target group SMEs is demonstrated using the example of Germany. The integrated user-centered method for mobile enterprise software development integrating usability is presented. The paper closes with an analysis of the needed future research in this field.

Paper 43 ICE-B
09:15 - 10:15 Room Dali
Parallel Session 9

A Dimension Integration Method for a Heterogeneous Data Warehouse Environment

Marius-Octavian Olaru and Maurizio Vincini
University of Modena, Modena, Italy

Keywords: Multidimensional Schema Matching, Dimension Merging.

Abstract: Data Warehousing is the main Business Intelligence instruments that allows the extraction of relevant, aggregated information from the operational data, in order to support the decision making process inside complex organizations. Following recent trends in Data Warehousing, companies realized that there is a great potential in combining their information repositories in order to offer all participants a broader view of the economical market. Unfortunately, even though Data Warehouse integration has been defined from a theoretical point of view, until now no complete, widely used methodology has been proposed to support Data Warehouse integration. This paper proposes a method that is able to achieve both *schema* and *instance* level integration of heterogeneous Data Warehouse dimensions attributes by exploiting the topology of dimensions and the *dimension-chase* procedure.

Paper 60 ICE-B
09:15 - 10:15 Room Dali
Parallel Session 9

e-Business An Online Shop in the Area of Technical and Scientific Publications

José António S. Pereira, Paulo Pita, Élsio Santos and Joaquim Filipe
Polithecnical Institute of Setúbal, Setúbal, Portugal

Keywords: e-Commerce, User Profiling, Context-based Software, Machine Learning, Data Mining, Recommender Systems, Intelligent Systems.

Abstract: The explosive growth of the world-wide-web and the emergence of e-commerce enabled the development of recommender systems that became to an independent emerged research area in the mid-1990s. The recommender systems are used to solve the prediction problem or the top-N recommendation problem. However, recommendation systems feel ever more the pressure related to a change on users habits. In order to capture users interests it is necessary a representation of information about an individual user. Our Online Shop in the Area of Technical and Scientific Publications intends to add the best of the user-based collaborative filtering and content-based collaborative filtering methodologies into a single hybrid methodology in order to answer some issues raised about new users and new items added to the recommender system. And also try to combine inference and prediction to assist the user in finding content that is of personal interest or even combine data mining techniques to provide recommendations.

Paper 15 OPTICS
09:15 - 10:15 Room Sevilla
Parallel Session 9

Budget Extension Schemes for Nx10 Gbit/s DPSK-based TDM/WDM PON

A. Emsia, Q. T. Le, T. von Lerber, D. Briggmann and F. Kueppers
TU Darmstadt, Darmstadt, Germany

Keywords: Wavelength-Division-Multiplexed Passive Optical Network (WDM PON), Differential-Phase-Shift-Keying (DPSK), Semiconductor Optical Amplifier (SOA), Delay Line Interferometer (DLI), Saturated Collision Amplifier (SCA).

Abstract: We present a new TDM/WDM PON scheme utilizing PSK (phase shift-keying) at 10

Gbit/s per λ-channel as the modulation format along the feeder line and an SOA (semiconductor optical amplifier) as the amplifying component at the remote node. One single DLI (Delay Line Interferometer) converts all λ-channels from PSK to OOK (on-off keying), the modulation format which is used along the access line and one single SOA are experimentally demonstrated to be sufficient providing a power budget increase of up to 46.8 dB.

Paper 16	OPTICS
09:15 - 10:15	Room Sevilla
Parallel Session 9	

Success Probability Evaluation of Quantum Circuits based on Probabilistic CNOT-Gates

Amor Gueddana, Rihab Chatta and Noureddine Boudriga

Engineering School of Communication of Tunis (SUP'COM), Ariana, Tunisia

Keywords: $CNOT$, C^kNOT, Abstract Probabilistic $CNOT$, Quantum $CNOT$-based Circuit.

Abstract: In this paper, we study the effect of non deterministic CNOT gates on the success probability of Quantum CNOT-based circuits. Based on physical implementation, we define an abstract probabilistic model of the CNOT gate that takes into consideration error sources and realizability constraints. Using the proposed model, we simulate a three-qubit quantum adder and show the evolution of the probability of realizing correctly the SUM operation depending on the success probability and errors of the CNOT gates.

Paper 22	OPTICS
09:15 - 10:15	Room Sevilla
Parallel Session 9	

All-optical Multi-wavelength Virtual Memory Architecture Design and Performances Analysis

SelmaBatti Selma Batti, Mourad Zghal and Noureddine Boudriga

University of Carthage, Ariana, Tunisia

Keywords: Optical Buffering, All-optical Memory, Fiber Bragg Grating, Tunable Wavelength Conversion.

Abstract: As all-optical memory represents one of the most important lacks in evolution of optical networks; this paper presents an all-optical virtual memory based on a recirculation loop, with the goal of providing optical data unit storage in all-optical switching networks. The concept of multi-wavelength signal buffering is adopted, to realize a shared buffer with an important storage capacity. We propose the organization of the buffer in two loops, the first as a delay loop and the second as an amplification loop, to improve the buffering duration and performances. The memory implementation is demonstrated using optical components such as fiber Bragg gratings (FBG), circulator and tunable wavelength converter. An all-optical control unit is designed to provide a dynamic and automatic signal buffer managing. An analytical model is implemented and a simulations set is done to prove that the proposed architecture is able to confine several signals for a relatively long time as a memory and signals can leave the architecture for a reasonably short delay after the departure decision is taken. The low penalty observed shows good system reliability.

Paper 16	SECRYPT
09:15 - 10:15	Room Valencia
Parallel Session 9	

Analysis of Some Natural Variants of the PKP Algorithm

Rodolphe Lampe and Jacques Patarin

University of Versailles Saint-Quentin, Versailles, France

Keywords: Public-key Cryptography, Identification Scheme, Zero Knowledge, Permuted Kernel Problem.

Abstract: In 1989, (Shamir, 1989) proposed a new zero-knowledge identification scheme based on a NP-complete problem called PKP for Permuted Kernel Problem. For a given prime p, a given matrix A and a given vector V, the problem is to find a permutation π such that the permuted vector V_π verifies $A\cdot V_\pi$=0 mod p. This scheme is still in 2011 known as one of the most efficient identification scheme based on a combinatorial problem. However, we will see in this paper that it is possible to improve this scheme significantly by combining new ideas in order to reduce the total number of computations to be performed and to improve very efficiently the security against side channel attacks using precomputations. We will obtain like this a new scheme that we have called SPKP. Moreover, if we use precomputed values in the scheme SPKP, then the prover will need to perform no computations (i.e. only selection and transmission of precomputed values). This is very interesting for security against side channel attacks because our scheme is zero-knowledge and we don't perform any computations using the key during the identification so we prove that any attacker (even using side channel attacks) being successfully identified implies that he has a solution to the NP-complete problem PKP.

Paper 45 SECRYPT
09:15 - 10:15 Room Valencia
Parallel Session 9

Securing In-vehicle Communication and Redefining the Role of Automotive Immobilizer

Constantinos Patsakis
Universitat Rovira i Virgili Department of Computer Engineering and Maths, Tarragona, Spain

Kleanthis Dellios
University of Piraeus, Piraeus, Greece

Keywords: Immobilizer, In-vehicle Communication, Security, Authentication.

Abstract: Automotive conventional anti-theft devices fail to prevent from unauthorized actions against vehicles. Information technologies and evolved microelectronics are currently being developed and widely adopted in controlling many mechanical parts of the vehicles. One of the most common means of restricting access to unauthorized drivers is immobilizer. In current work we discuss some common vulnerability issues that vehicles and immobilizer technology confronts, leading us to propose a redefinition of its role in vehicle security and the physical vehicle environment. Our proposal meets current trends of IT and computer science in embedding systems in vehicles and if properly implemented, may provide more secure vehicles.

Paper 123 SECRYPT
09:15 - 10:15 Room Valencia
Parallel Session 9

An Improved Public-key Tracing Scheme with Sublinear Ciphertext Size

Chiara Valentina Schiavo and Andrea Visconti
Universitá degli Studi di Milano, Milano, Italy

Keywords: Traitor Tracing Schemes, Piracy, Digital Content Distribution Systems, Pirate Decoders, Traitors.

Abstract: To overcome the piracy problem in digital content distribution systems, a number of traitor tracing schemes have been suggested by researchers. The goal of these schemes is to enable the tracer to identify at least one of the traitors. In this context, Matsushita and Imai (2004) proposed a black-box tracing scheme with sublinear header size that is able to perform tracing of self-defensive pirate decoders. Kiayias and Pehlivanoglu (2009) proved that this scheme is vulnerable to an attack which allows an illicit decoder to recognize normal ciphertext to tracing ones and distinguish two consecutive tracing ciphertexts. For making the scheme no more susceptible to such attack, authors modified the encryption phase and assumed that traitors belong to the same user group. In this paper, we present a solution that has no traitors restrictions, repairing the scheme totally. In particular, we modified the tracing scheme proving that (a) a pirate decoder is not able to recognize normal ciphertext to tracing ones with sufficiently high probability, and (b) the statistical distance between two consecutive tracing operations is negligible under Decision Diffie Hellman assumption.

Paper 139 SECRYPT
09:15 - 10:15 Room Valencia
Parallel Session 9

Inverting Thanks to SAT Solving An Application on Reduced-step MD*

Florian Legendre[1], Gilles Dequen[2] and Michaël Krajecki[1]
[1] *University of Reims Champagne-Ardennes, Reims, France*
[2] *University of Picardie Jules Verne, Amiens, France*

Keywords: Logic, Cryptanalysis, Hash Function, MD5, Satisfiability.

Abstract: The SAT isfiability Problem is a core problem in mathematical logic and computing theory. The last decade progresses have led it to be a great and competitive approach to practically solve a wide range of industrial and academic problems. Thus, the current SAT solving capacity allows the propositional formalism to be an interesting alternative to tackle cryptanalysis problems. This paper deals with an original application of the SAT problem to cryptanalysis. We thus present a principle, based on a propositional modeling and solving, and provide details on logical inferences, simplifications, learning and pruning techniques used as a preprocessor with the aim of reducing the computational complexity of the SAT solving and hence weakening the associated cryptanalysis. As cryptographic hash functions are central elements in modern cryptography we choose to illustrate our approach with a dedicated attack on the second preimage of the well-known MD⋆ hash functions. We finally validate this reverse-engineering process, thanks to a generic SAT solver achieving a weakening of the inversion of MD⋆. As a result, we present an improvement of the current limit of best practical attacks on step-reduced MD4 and MD5 second preimage, respectively up to 39 and 28 inverted rounds.

Paper 23	ICETE
10:15 - 11:15	Foyer
Poster Session 3	

The Road to a Responsible and Sustainable e-Business

Norberto Patrignani and Marco De Marco

Catholic University of Milano, Milano, Italy

Keywords: Corporate Social Responsibility, Business Ethics, Computer Ethics, Information Systems, Big Data.

Abstract: This paper introduces a definition of a responsible and sustainable e-business organization. Today every company has to take into account the growing role of the stakeholders (employees, suppliers, customers, and general society) and this has increased the importance of the Corporate Social Responsibility (CSR). Also, they have to expose the impact of their operations on the environment in terms of supply-chain, power consumption and waste management. Both these dimensions are becoming important also for organizations that concentrate their activities on electronic channels. For them, information systems and communication channels (ICT) represent the fundamental infrastructure. This paper concentrates on the questions: how to harmonize the CSR strategy with the important decisions that has to be taken in the computing areas? How to keep aligned the Business Ethics with the Computer Ethics strategies?.

Paper 32	ICETE
10:15 - 11:15	Foyer
Poster Session 3	

Paths of Business Model Evolution Findings from Business Model Patents

Woori Han, Bomi Song and Yongtae Park

Seoul National University, Seoul, Korea, Republic of

Keywords: Business Model Evolution, Business Model (BM) Patent, Technology based Business Model.

Abstract: All firms have business models (BMs) and they continuously modify their BMs to adjust to dynamic environment. The objective of this paper is to find paths of technology based BM evolution by investigating BM patents which are representative data source of technical BMs. The paper begins by reviewing the BM and BM patents, and provides a description and justification of the proposed evolutionary paths of BM - major (origination, transplant, mutation) and minor (variation, alternation, addition or subtraction) evolutionary stream. The paper concludes by highlighting the key findings and drawing limitation and further research.

Paper 36	ICETE
10:15 - 11:15	Foyer
Poster Session 3	

Comparison Study of Some Collaborative Tools Use in Virtual Teams

Cosmina Carmen Aldea and Anca Draghici

”Politehnica” University of Timisoara, Timişoara, Romania

Keywords: Virtual Teams, Teamwork, Human Resource, Trust, Communication Tools.

Abstract: This article describes the connectivity and networking of virtual team members (based on the reference review and some structured interview organized with members of virtual project teams) and new perspectives in virtual teams' collaboration, to underline the actual trends and to identify their future development. Introduction of new communication tools with multiple options and functionalities that better support collaborative work and learning processes will also, facilitate the integration of new members, the communication and working processes and they will increase trust between members of virtual teams. The tools used for communication and real time research-work will increase competitiveness, too by optimizing the resources dedicated to different projects, teams and management systems. There are software tools that facilitate communication, collaboration and coordination of virtual teams. Choosing the right software has to consider the specific virtual teams' needs and requirements. The best frame is one in which the characteristics are well defined so that they cover all aspects of collaborative activities and overall project management.

Paper 41	ICETE
10:15 - 11:15	Foyer
Poster Session 3	

Self-ad-MCNHA-SLOS A Self-adaptive Minimum-Cost Network Hardening Algorithm based on Stochastic Loose Optimize Strategy

Yonglin Sun, Yongjun Wang and Yi Zhang

National University of Defense Technology (NUDT), Changsha, China

Keywords: Minimum-cost Network Hardening, Stochastic Loose Optimize, Self-adaptive, Network Vulnerability, Attack Graph.

Abstract: Given a network, it inevitable contains various vulnerabilities, which could be exploited by malicious attackers. It is an effective way to harden a network by searching and remedying those critical vulnerabilities. That is the so-called Minimum-Cost Network Hardening (MCNH) problem, but there haven't any effective enough method to address this problem yet, especially, when facing large-scale network. We proposed Self-ad-MCNHA-SLOS, an algorithm using Stochastic Loose Optimize Strategy (SLOS) and self-adaptive parameter adjustment method ingeniously, to meet the problem. Experiment results show that it has the merits of high-efficiency, controllable, asymptotically optimal, and suitable for large-scale network.

Paper 44 ICETE
10:15 - 11:15 Foyer
Poster Session 3

ADQL: A Flexible Access Definition and Query Language to Define Access Control Models

Andreas Sonnenbichler and Andreas Geyer-Schulz
Karlsruhe Institute of Technology, Karlsruhe, Germany

Keywords: Access Control, ADQL, Formal Language, Meta Language, Access Control Service.

Abstract: We suggest a full specified formal language, the Access Definition and Query Language (ADQL). It has been designed to define access control models, facts, policies, and queries. ADQL, therefore, has the features of a meta language: It can be configured to act like known access control models e.g. as Bell-LaPadula, RBAC and its extensions and applications (e.g. SAP R/3), but also it can implement new models. Because of this, ADQL is highly flexible. Nevertheless, ADQL is not only a meta-language, but also allows to define facts, policies and queries. It has been implemented as a software service. It can be used as external authorization component for other applications and services. Through its flexibility many access control models can be supported.

Paper 35 ICETE
10:15 - 11:15 Foyer
Poster Session 3

Performance Analysis of New SNR Estimation Methodology based on Preamble Approach

Sangmi Moon, Saransh Malik, Bora Kim, Cheolhong Kim and Intae Hwang
Chonnam National University, Gwangju, Korea, Republic of

Keywords: CSI, MIMO, OFDM, Preamble, SNR.

Abstract: The latest wireless communication systems focus on developing MIMO-OFDM systems that allow the transmission of very high data rates in fading environments. We can optimize these systems even further by setting the modulation and coding adaptively according to the channel conditions, and by using sub-carrier frequency and power allocation techniques. The overall system performance depends on the accuracy and delay of the channel state information (CSI). In this paper, we propose a signal-to-noise ratio (SNR) estimation algorithm based on preamble transmission. Through simulations of several channel environments, we prove that our proposed algorithm is more accurate than conventional algorithms.

Paper 36 ICETE
10:15 - 11:15 Foyer
Poster Session 3

Novel Channel Estimation Algorithm using Various Filter Design in LTE-Advanced System

Saransh Malik, Sangmi Moon, Bora Kim, Cheolhong Kim and Intae Hwang
Chonnam National University, Buk-Gu, Gwangju, Korea, Republic of

Keywords: Channel Estimation, OFDM, LTE-Advanced.

Abstract: Channel estimation is a major issue in communication system. In this paper, we propose a new idea for channel estimation that uses a Kalman Filter (KF) approach to predict the channel in OFDM symbols with pilot subcarriers where channel affected is by high doppler spread. We design the algorithm considering the lattice-type arrangement of pilot subcarriers in a LTE-Advanced system from 3GPP. In further advancement, we use the filtering of channel impulse response and application of a Wiener Filter for the estimation of the channel frequency response in the rest of the subcarriers.

Paper 48 ICETE
10:15 - 11:15 Foyer
Poster Session 3

Semi-dynamic Calibration for Eye Gaze Pointing System based on Image Processing

Kohichi Ogata and Kohei Matsumoto
Kumamoto University, Kumamoto, Japan

Keywords: Eye Gaze, Iris, Calibration, Image Processing.

Abstract: In this paper, we propose two semi-dynamic calibration methods for compensating for user's head movements for an eye gaze pointing system. Since the user perceives degradation in pointing accuracy during use, an effective compensatory calibration by the user which does not require additional apparatus or high cost calculation can be a useful solution for the problem. The proposed semi-dynamic calibration methods lead the user to gaze at 1 or 3 points on the computer screen and reduce the gap between the true eye gaze direction and the position of the mouse pointer. Experimental results showed that the proposed methods were capable of pointing the mouse pointer within 20 pixels at a distance of about 60 cm between the user and the display.

Paper 76	ICETE
10:15 - 11:15	Foyer
Poster Session 3	

Simulated Annealing based Parameter Optimization of Time-frequency ε-filter Utilizing Correlation Coefficient

Tomomi Matsumoto[1], Mitsuharu Matsumoto[2] and Shuji Hashimoto[1]

[1] *Waseda University, Tokyo, Japan*

[2] *University of Electro-communications, Tokyo, Japan*

Keywords: Simulated Annealing, Parameter Optimization, Noise Reduction, ε-filter, Nonlinear Filter, Time-frequency ε-filter.

Abstract: Time-Frequency ε-filter (TF ε-filter) can reduce different types of noise from a single-channel noisy signal while preserving the signal that varies drastically such as a speech signal. It can reduce not only small stationary noise but also large nonstationary noise. However, it has some parameters whose values are set empirically. So far, there are few studies to optimize the parameter of TF ε-filter automatically. In this paper, we employ the correlation coefficient of the filter output and the difference between the filter input and output as the evaluation function of the parameter optimization. We also propose an algorithm to set the optimal parameter of TF ε-filter automatically. The experimental results show that we can obtain the adequate parameter in TF ε-filter automatically by using the proposed method.

11:15 - 12:15	Room Plenary
Cyberinfrastructure for eScience and eBusiness from Clouds to Exascale	
Keynote Speaker: Geoffrey Charles Fox	

Cyberinfrastructure for eScience and eBusiness from Clouds to Exascale

Geoffrey Charles Fox

Indiana University, Indianapolis, U.S.A.

Abstract: We analyze scientific computing into classes of applications and their suitability for different architectures covering both compute and data analysis cases and both high end and long tail (many small) users. We identify where commodity systems (clouds) coming from eBusiness and eCommunity are appropriate and where specialized systems are needed. We cover both compute and data (storage) issues and propose an architecture for next generation Cyberinfrastructure and outline some of the research and education challenges. We discuss FutureGrid project that is a testbed for these ideas.

Closing Session	ICETE
12:15 - 12:30	Room Plenary

Friday, 27