

Lecture Notes in Computer Science

5376

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Daniel Ortiz-Arroyo
Henrik Legind Larsen Daniel Dajun Zeng
David Hicks Gerhard Wagner (Eds.)

Intelligence and Security Informatics

First European Conference, EuroISI 2008
Esbjerg, Denmark, December 3-5, 2008
Proceedings

Volume Editors

Daniel Ortiz-Arroyo
Computer Science Department
Aalborg University Esbjerg, Denmark
E-mail: do@cs.aau.dk

Henrik Legind Larsen
Computer Science Department
Aalborg University Esbjerg, Denmark
E-mail: hll@sis-rc.org

Daniel Dajun Zeng
MIS Department
University of Arizona, Tucson, AZ, USA
E-mail: zeng@email.arizona.edu

David Hicks
Computer Science Department
Aalborg University Esbjerg, Denmark
E-mail: hicks@cs.aau.dk

Gerhard Wagner
European Commission
Joint Research Centre, Ispra, Italy
E-mail: gerhard.wagner@jrc.it

Library of Congress Control Number: 2008940518

CR Subject Classification (1998): H.4, H.3, C.2, H.2, D.4.6, K.4.1, K.5, K.6

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-89899-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-89899-3 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12582617 06/3180 5 4 3 2 1 0

Preface

This volume constitutes the proceedings of the First European Conference on Intelligence and Security Informatics, EuroISI 2008, held in Esbjerg Denmark, December 3–5, 2008.

Intelligence and security informatics (ISI) is a multidisciplinary field encompassing methodologies, models, algorithms, and advanced tools for intelligence analysis, homeland security, terrorism research as well as security-related public policies. EuroISI 2008 was the first European edition of the series of ISI symposiums that have been held annually in the USA since 2003, and more recently in Asia. These meetings gather together people from previously disparate communities to provide a stimulating forum for the exchange of ideas and results. Participants have included academic researchers (especially in the fields of information technologies, computer science, public policy, and social and behavioral studies), law enforcement and intelligence experts, as well as information technology companies, industry consultants and practitioners in the relevant fields.

These proceedings contain 25 original papers, out of 48 submissions received, related to the topics of intelligence and security informatics. The papers cover a broad range of fields such as: social network analysis, knowledge discovery, web-based intelligence and analysis, privacy protection, access control, digital rights management, malware and intrusion detection, surveillance, crisis management, and computational intelligence, among others. Additionally to the main conference, a poster section was organized.

With the organization of EuroISI 2008, we hope to have fostered important collaborations, not only among the European-based researchers and practitioners but also among researchers from other regions of the world. We believe that this is particularly important at this stage where the ISI core set of research methodologies and approaches is beginning to mature.

We wish to thank all contributors for their excellent papers and the referees, publisher and sponsors for their efforts. Special thanks also to the invited speakers and members of the Program Committee. They made the success of EuroISI 2008 possible.

December 2008

Daniel Ortiz-Arroyo
Henrik Legind Larsen
Daniel Dajun Zeng
David Hicks
Gerhard Wagner

Organization

EuroISI 2008 was organized by Aalborg University, the European Joint Research Centre, and the University of Arizona.

Executive Committee

Conference Chair	Daniel Ortiz-Arroyo (Aalborg University, Denmark)
Co-chair	David Hicks (Aalborg University, Denmark)
Co-chair	Gerhard Wagner (European Commission, Joint Research Centre, Italy)
Honorary Chair	Hsinchun Chen (University of Arizona, USA)
Program Chair	Henrik Legind Larsen (Aalborg University, Denmark)
Program Co-chair	Daniel Dajun Zeng (University of Arizona, USA and Chinese Academy of Sciences, China)
Organizing Chair	Akbar Hussain (Aalborg University, Denmark)
Organizing Co-chair	Andrea Valente (Aalborg University, Denmark)
Local Arrangements and Web Site	Sandra Del-Villar Lazcano

Program Committee

Conference Chair	Daniel Ortiz-Arroyo (Aalborg University, Denmark)
Program Chair	Henrik Legind Larsen (Aalborg University, Denmark)
Program Co-chair	Daniel Dajun Zeng (University of Arizona, USA and Chinese Academy of Sciences, China)

Referees

Ajith Abraham, Norway	Marek Druzdziel, Poland
Tayfur Altioek, USA	Dennis Egan, USA
Dragos Arotaritei, Romania	Vladimir Estivill-Castro, Australia
Antonio Badia, USA	Uwe Glasser, Canada
Patrick Bosc, France	Nazli Goharian, USA
Debrup Chakraborty, Mexico	Mark Goldberg, USA
Richard Chbeif, France	Paul Hofmann, USA
Guy De Tre, Belgium	Dil Hussain, Denmark
Kevin C. Desouza, USA	Janusz Kacprzyk, Poland

Paul Kantor, USA	Antonio Sanfilippo, USA
Juha Knuuttila, Finland	Charles Shoniregun, UK
Don Kraft, USA	Joshua Sinai, USA
Henrik Legind Larsen, Denmark	David B. Skillicorn, Canada
Seok-Won Lee, USA	Randy Smith, USA
Gondy Leroy, USA	Nicolas Spyrtos, France
Ee-peng Lim, Singapore	Clark Thomborson, New Zealand
Sushmita Mitra, India	Paul Thompson, USA
Guillermo Morales-Luna, Mexico	Scott Tousley, USA
Robert Moskovitch, Israel	Cedric Ulmer, USA
Fredrick Mtenzi, Ireland	Nalini Venkatasubramanian, USA
Clifford Neuman, USA	Alan Wang, USA
Daniel Ortiz-Arroyo, Denmark	Fei-Yue Wang, China
Gabriella Pasi, Italy	Jennifer Xu, USA
Warren Powell, USA	Chris Yang, Hong Kong
Yael Radlauer, Israel	Slawomir Zadrozny, Poland
Victor Ralevich, Canada	Daniel Zeng, USA
Francisco Rodríguez-Henriquez, Mexico	Nan Zhang, USA
Elie Sanchez, France	Lina Zhou, USA
	Willam Zhu, China

Sponsoring Institutions

Aalborg University, Esbjerg Institute of Technology, Denmark
The Obel Family Foundation, Aalborg, Denmark
XSI ApS, Virum, Denmark
IEEE Systems Man and Cybernetics Society
European Joint Research Centre

Table of Contents

Abstracts of Plenary Talks

Intelligent Social Network Modeling and Analysis for Security Informatics	1
<i>Ronald R. Yager</i>	
Nature Inspired Online Real Risk Assessment Models for Security Systems	3
<i>Ajith Abraham</i>	
Homeland Security Data Mining Using Social Network Analysis	4
<i>Hsinchun Chen</i>	

Criminal and Social Network Analysis

The Automatic Identification and Prioritisation of Criminal Networks from Police Crime Data	5
<i>Richard Adderley, Atta Badii, and Chaorin Wu</i>	
An Information Theory Approach to Identify Sets of Key Players	15
<i>Daniel Ortiz-Arroyo and D.M. Akbar Hussain</i>	
Locating Key Actors in Social Networks Using Bayes' Posterior Probability Framework	27
<i>D.M. Akbar Hussain and Daniel Ortiz-Arroyo</i>	
Computational Modeling of Criminal Activity	39
<i>Uwe Glässer and Mona Vajihollahi</i>	

Intelligence Analysis and Knowledge Discovery

SPYWatch, Overcoming Linguistic Barriers in Information Management	51
<i>Federico Neri and Angelo Priamo</i>	
Dissecting the Meaning of an Encrypted Message: An Approach to Discovering the Goals of an Adversary	61
<i>Aaron Hunter</i>	
Buzz Monitoring in Word Space	73
<i>Magnus Sahlgren and Jussi Karlgren</i>	

Web-Based Intelligence Monitoring and Analysis

Nuclear Threat Detection Via the Nuclear Web and Dark Web: Framework and Preliminary Study 85
Hsinchun Chen

Mapping Dark Web Geolocation 97
Clinton Mielke and Hsinchun Chen

Jihadi Video and Auto-radicalisation: Evidence from an Exploratory YouTube Study 108
Maura Conway and Lisa McInerney

Privacy Protection, Access Control, and Digital Rights Management

Access Control of Federated Information Systems 119
Aneta Poniszewska-Maranda

Designing Information Systems Which Manage or Avoid Privacy Incidents 131
Giannakis Antoniou, Lynn Batten, and Udaya Parampalli

Secure Computation for Privacy Preserving Biometric Data Retrieval and Authentication 143
Bon Sy

Digital Audio Watermarking for Copyright Protection Based on Multiwavelet Transform 155
Prayoth Kumsawat, Kittit Attakitmongcol, and Arthit Srikaew

Problem Analyses and Recommendations in DRM Security Policies 165
Youngseek Kim, Jessica Howard, Sharad Ravindranath, and Joon S. Park

Malware and Intrusion Detection

A Distributed Framework for the Detection of New Worm-Related Malware 179
Boris Rozenberg, Ehud Gudes, and Yuval Elovici

Optimization of NIDS Placement for Protection of Intercommunicating Critical Infrastructures 191
Rami Puzis, Marius David Klippel, Yuval Elovici, and Shlomi Dolev

Unknown Malcode Detection Using OPCODE Representation 204
Robert Moskovitch, Clint Feher, Nir Tzachar, Eugene Berger, Marina Gitelman, Shlomi Dolev, and Yuval Elovici

Surveillance and Crisis Management

Mobile and Stationary Sensors for Local Surveillance: System Architecture and Applications	216
<i>Sandro Leuchter, Thomas Partmann, and Lothar Berger</i>	
Fuzzy Distributed Workflows for Crisis Management Decision Makers...	226
<i>Jean-Francois Landry, Cedric Ulmer, and Laurent Gomez</i>	
Reconfigurable Radio Systems for Public Safety Based on Low-Cost Platforms	237
<i>Gianmarco Baldini, Raimondo Giuliani, and Dimitrios Symeonidis</i>	
An Information Systems Design Theory for Supporting WMD Knowledge Reachback	248
<i>Steven R. Haynes, Jonathan M. Singel, and Thomas George Kannampallil</i>	
Rampart: A Service and Agent-Based Architecture for Anti-Terrorism Planning and Resource Allocation.....	260
<i>Steven R. Haynes, Thomas George Kannampallil, Mark A. Cohen, Andrey Soares, and Frank E. Ritter</i>	

Posters

Evaluative Word Locations in Semantic Networks from News Stories about Al Qaeda and Implications for Optimal Communication Messages in Anti-Terrorism Campaigns	271
<i>James A. Danowski</i>	
Methodology for Experimental ICT Industrial and Critical Infrastructure Security Tests	274
<i>Igor Nai Fovino and Marcelo Masera</i>	
Author Index	277