

Hsinchun Chen Reagan Moore
Daniel D. Zeng John Leavitt (Eds.)



dandelion.com

© 2008 AGI Information Management Consultants
May be used for personal purposes only or by
libraries associated to dandelion.com network.

Intelligence and Security Informatics

Second Symposium on
Intelligence and Security Informatics, ISI 2004
Tucson, AZ, USA, June 10-11, 2004
Proceedings



Springer

Table of Contents

Part I: Full Papers

Bioterrorism and Disease Informatics

Aligning Simulation Models of Smallpox Outbreaks	1
<i>Li-Chiou Chen, Boris Kaminsky, Tiffany Tummino, Kathleen M. Carley, Elizabeth Casman, Douglas Fridsma, and Alex Yahja</i>	

Data Analytics for Bioterrorism Surveillance	17
<i>Donald J. Berndt, Sunil Bhat, John W. Fisher, Alan R. Hevner, and James Studnicki</i>	

West Nile Virus and Botulism Portal: A Case Study in Infectious Disease Informatics	28
<i>Daniel Zeng, Hsinchun Chen, Chunju Tseng, Catherine Larson, Millicent Eidson, Ivan Gotham, Cecil Lynch, and Michael Ascher</i>	

Data Access Control, Privacy, and Trust Management

A Novel Policy and Information Flow Security Model for Active Network .	42
<i>Zhengyou Xia, Yichuan Jiang, Yiping Zhong, and Shiyong Zhang</i>	

A Novel Autonomous Trust Management Model for Mobile Agents	56
<i>Yichuan Jiang, Zhengyou Xia, Yiping Zhong, and Shiyong Zhang</i>	

Privacy-Preserving Inter-database Operations	66
<i>Gang Liang and Sudarshan S. Chawathe</i>	

Data Management and Mining

Finding Unusual Correlation Using Matrix Decompositions	83
<i>David B. Skillicorn</i>	

Generating Concept Hierarchies from Text for Intelligence Analysis	100
<i>Jeng-Haur Wang, Chien-Chung Huang, Jei-Wen Teng, and Lee-Feng Chien</i>	

Interactive Query Languages for Intelligence Tasks	114
<i>Antonio Badia</i>	

Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach
to Addressing the Threats of Terrorism 125
*Edna Reid, Jialun Qin, Wingyan Chung, Jennifer Xu, Yilu Zhou,
Rob Schumaker, Marc Sageman, and Hsinchun Chen*

The Architecture of the Cornell Knowledge Broker 146
Alan Demers, Johannes Gehrke, and Mirek Riedewald

Deception Detection

Computer-Based Training for Deception Detection: What Users Want? ... 163
*Jinwei Cao, Ming Lin, Amit Deokar, Judee K. Burgoon,
Janna M. Crews, and Mark Adkins*

Identifying Multi-ID Users in Open Forums 176
Hung-Ching Chen, Mark Goldberg, and Malik Magdon-Ismael

Self-efficacy, Training Effectiveness, and Deception Detection:
A Longitudinal Study of Lie Detection Training 187
Kent Marett, David P. Biros, and Monti L. Knode

Information Assurance and Infrastructure Protection

Composite Role-Based Monitoring (CRBM)
for Countering Insider Threats 201
Joon S. Park and Shuyuan Mary Ho

Critical Infrastructure Integration Modeling and Simulation 214
*William J. Tolone, David Wilson, Anita Raja, Wei-ning Xiang,
Huili Hao, Stuart Phelps, and E. Wray Johnson*

Mining Normal and Intrusive Activity Patterns
for Computer Intrusion Detection 226
Xiangyang Li and Nong Ye

The Optimal Deployment of Filters to Limit Forged Address Attacks
in Communication Networks 239
Enock Chisonge Mofya and Jonathan Cole Smith

Monitoring and Surveillance

A Tool for Internet Chatroom Surveillance 252
Ahmet Çamtepe, Mukkai S. Krishnamoorthy, and Bülent Yener

ChatTrack: Chat Room Topic Detection Using Classification 266
Jason Bengel, Susan Gauch, Eera Mittur, and Rajan Vijayaraghavan

SECRETS: A Secure Real-Time Multimedia Surveillance System 278
Naren Kodali, Csilla Farkas, and Duminda Wijesekera

Studying E-Mail Graphs for Intelligence Monitoring and Analysis in the Absence of Semantic Information	297
<i>Petros Drineas, Mukkai S. Krishnamoorthy, Michael D. Sofka, and Bülent Yener</i>	

THEMIS: Threat Evaluation Metamodel for Information Systems	307
<i>Csilla Farkas, Thomas C. Wingfield, James B. Michael, and Duminda Wijesekera</i>	

Security Policies and Evaluation

Balancing Security and Privacy in the 21 st Century	322
<i>Chris C. Demchak and Kurt D. Fenstermacher</i>	

IT Security Risk Management under Network Effects and Layered Protection Strategy	331
<i>Wei T. Yue, Metin Cakanyildirim, Young U. Ryu, and Dengpan Liu</i>	

Mind the Gap: The Growing Distance between Institutional and Technical Capabilities in Organizations Performing Critical Operations	349
<i>Gene I. Rochlin</i>	

Social Network Analysis

Analyzing and Visualizing Criminal Network Dynamics: A Case Study	359
<i>Jennifer Xu, Byron Marshall, Siddharth Kaza, and Hsinchun Chen</i>	

Discovering Hidden Groups in Communication Networks	378
<i>Jeff Baumes, Mark Goldberg, Malik Magdon-Ismail, and William Al Wallace</i>	

Generating Networks of Illegal Drug Users Using Large Samples of Partial Ego-Network Data	390
<i>Ju-Sung Lee</i>	

Part II: Short Papers

Deception Detection

Using Speech Act Profiling for Deception Detection	403
<i>Douglas P. Twitchell, Jay F. Nunamaker Jr., and Judee K. Burgoon</i>	

Testing Various Modes of Computer-Based Training for Deception Detection	411
<i>Joey F. George, David P. Biros, Mark Adkins, Judee K. Burgoon, and Jay F. Nunamaker Jr.</i>	

Data/Text Management and Mining

The Use of Data Mining Techniques in Operational Crime Fighting	418
<i>Richard Adderley</i>	
Spatial Forecast Methods for Terrorist Events in Urban Environments	426
<i>Donald Brown, Jason Dalton, and Heidi Hoyle</i>	
Web-Based Intelligence Notification System: Architecture and Design	436
<i>Alexander Dolotov and Mary Strickler</i>	
Cross-Lingual Semantics for Crime Analysis Using Associate Constraint Network	449
<i>Christopher C. Yang and Kar Wing Li</i>	

Information Assurance and Infrastructure Protection

Experimental Studies Using Median Polish Procedure to Reduce Alarm Rates in Data Cubes of Intrusion Data	457
<i>Jorge Levera, Benjamin Barán, and Robert Grossman</i>	
Information Sharing and Collaboration Policies within Government Agencies	467
<i>Homa Atabakhsh, Catherine Larson, Tim Petersen, Chuck Violette, and Hsinchun Chen</i>	
Intrusion-Tolerant Intrusion Detection System	476
<i>Myung-Kyu Yi and Chong-Sun Hwang</i>	
Optimal Redundancy Allocation for Disaster Recovery Planning in the Network Economy	484
<i>Benjamin B.M. Shao</i>	
Semantic Analysis for Monitoring Insider Threats	492
<i>Svetlana Symonenko, Elizabeth D. Liddy, Ozgur Yilmazel, Robert Del Zoppo, Eric Brown, and Matt Downey</i>	
Towards a Social Network Approach for Monitoring Insider Threats to Information Security	501
<i>Anand Natarajan and Liaquat Hossain</i>	

Part III: Extended Abstracts for Posters

Policy-Based Information Sharing with Semantics	508
<i>Eric Hughes, Amy Kazura, and Arnie Rosenthal</i>	
Determining the Gender of the Unseen Name through Hyphenation	510
<i>Robert H. Warren and Christopher Leurer</i>	

A Framework for a Secure Federated Patient Healthcare System	512
<i>Raj Sharman, Himabindu Challapalli, Raghav H. Rao, and Shambhu Upadhyaya</i>	
Vulnerability Analysis and Evaluation within an Intranet	514
<i>Eungki Park, Jung-Taek Seo, Eul Gyu Im, and Cheol-Won Lee</i>	
Security Informatics: A Paradigm Shift in Information Technology Education	516
<i>Susan M. Merritt, Allen Stix, and Judith E. Sullivan</i>	
Research of Characteristics of Worm Traffic	518
<i>Yufeng Chen, Yabo Dong, Dongming Lu, and Zhengtao Xiang</i>	
Part IV: Panel Discussion Papers	
MIPT: Sharing Terrorism Information Resources	520
<i>James O. Ellis III</i>	
Post-9/11 Evolution of Al Qaeda	526
<i>Rohan Gunaratna</i>	
Utilizing the Social and Behavioral Sciences to Assess, Model, Forecast and Preemptively Respond to Terrorism	531
<i>Joshua Sinai</i>	
Author Index	535