2013 IEEE International Conference on Intelligence and Security Informatics

(ISI 2013)

Seattle, Washington, USA
4-7 June 2013
Table of Contents

Welcome Message from the Conference Co-Chairs .............................................................. xi
Conference Organizers ........................................................................................................ xii
Program Committee ........................................................................................................... xiii
Sponsors ................................................................................................................................. xv
Technical Papers ............................................................................................................... xvii

Part I: Technical Papers

Crime Linkage: A Fuzzy MCDM Approach ........................................................................ 1
  Fabrizio Albertetti, Paul Cotofrei, Lionel Grossrieder, Olivier Ribaux, Kilian Stoffel

Occupational Fraud Detection through Visualization ...................................................... 4
  Evmorfia N. Argyriou, Aikaterini A. Sotiraki, Antonios Symvonis

Flexible Creation of Indicators of Scientific and Technological Emergence: Emerging
Phenomena and Big Data .................................................................................................. 7
  Olga Babko-Malaya, Daniel Hunter, Andy Seidel, Fotis Barlos

Analyzing Security Threats as Reported by the United States Computer Emergency
Readiness Team (US-CERT) ............................................................................................ 10
  Yolanda S. Baker, Rajeev Agrawal, Sambit Bhattacharya

Detecting Collaboration from Behavior ............................................................................ 13
  Travis Bauer, Daniel Garcia, Rich Colbaugh, Kristin Glass

Evaluating Text Visualization: An Experiment in Authorship Analysis ....................... 16
  Victor Benjamin, Wingyan Chung, Ahmed Abbasi, Joshua Chuang,
  Catherine A. Larson, Hsinchun Chen

Machine Learning for Attack Vector Identification in Malicious Source Code ................ 21
  Victor A. Benjamin, Hsinchun Chen

How Analysts Cognitively “Connect the Dots” ................................................................. 24
  Lauren Bradel, Jessica Zeitz Self, Alex Endert, M. Shahriar Hossain,
  Chris North, Naren Ramakrishnan

Use of Latent Semantic Indexing to Identify Name Variants in Large Data Collections .... 27
  R.B. Bradford

Learning to Classify Emotional Content in Crisis-Related Tweets ................................ 33
  Joel Brynielsson, Fredrik Johansson, Anders Westling

From When and What to Where: Linking Spatio-Temporal Visualizations in Visual
Analytics ......................................................................................................................... 39
  Yingjie Victor Chen, Zhenyu Cheryl Qian
Dynamic Information-Theoretic Measures for Security Informatics ........................................... 45
Richard Colbaugh, Kristin Glass, Travis Bauer
Moving Target Defense for Adaptive Adversaries ................................................................. 50
Richard Colbaugh, Kristin Glass
Detecting Future Social Unrest in Unprocessed Twitter Data:
Emerging Phenomena and Big Data ........................................................................................ 56
Ryan Compton, Craig Lee, Tsai-Ching Lu, Lalinda De Silva, Michael Macy
SociAL Sensor Analytics: Measuring Phenomenology at Scale ............................................. 61
Courtney D. Corley, Chase Dowling, Stuart J. Rose, Taylor McKenzie
Dave DeBarr, Venkatesh Ramanathan, Harry Wechsler
Saudi Arabia’s Response to Cyber Conflict: A Case Study of the Shamoon Malware Incident .... 73
Zakariya Dehlawi, Norah Abokhodair
Side-View Face Authentication based on Wavelet and Random Forest with Subsets ............ 76
Sihao Ding, Qiang Zhai, Yuan F. Zheng, Dong Xuan
Effects of Fear Appeals and Point of Reference on the Persuasiveness of
IT Security Communications .................................................................................................... 82
Honglu Du, Heng Xu, Mary Beth Rosson, John M. Carroll
A Multi-Modality Attributes Representation Scheme for Group Activity
Characterization and Data Fusion .............................................................................................. 85
Vinayak Elangovan, Anjjad Alkilani, Amir Shirkhodaie
Towards Task-Centered Network Models through Semantic Workflows ................................. 91
Yolanda Gil
Cyber Friendly Fire: Research Challenges for Security Informatics ......................................... 94
Frank L. Greitzer, Thomas E. Carroll, Adam D. Roberts
Modeling and Detecting Anomalous Topic Access ................................................................. 100
Siddharth Gupta, Casey Hanson, Carl A. Gunter, Mario Frank, David Liebovitz, Bradley Malin
Towards a Network-of-Networks Framework for Cyber Security ........................................... 106
Mahamtesh Halappanavar, Sutanay Choudhury, Emilie Hogan, Peter Hui, John Johnson,
Indrajit Ray, Lawrence Holder
Stealthy Software: Next-Generation Cyber-Attacks and Defenses ......................................... 109
Kevin W. Hamlen
Building a Better Intelligence Machine: A New Approach to Capability
Review and Development ......................................................................................................... 113
Duncan Hodges, Sadie Creese
OCC Model-Based Emotion Extraction from Online Reviews .......................................................... 116
Luwen Huangfu, Wenji Mao, Daniel Zeng, Lei Wang

Information Graphs of Event Threads: Identifying and Building Forward and Backward Event Threads for Societal Events .................................................... 122
James R. Johnson

A Graph Analytic Metric for Mitigating Advanced Persistent Threat ........................................... 129
John R. Johnson, Emilie A. Hogan

Gamification of Emergency Response Training: A Public Health Example .................................. 134
Irfan E. Kanat, Sathananda Siloju, T.S. Raghu, Ajay S. Vinze

TALISON — Tensor Analysis of Social Media Data ................................................................. 137
Anne Kao, William Ferng, Stephen Poteet, Poteet Quach, Rod Tjoelker

Analyzing Users’ Web Surfing Patterns to Trace Terrorists and Criminals .................................. 143
Gabi Kedma, Mordehai Guri, Tom Sela, Yuval Elovici

Click Fraud Detection with Bot Signatures .................................................................................... 146
Brendan Kitts, Jing Ying Zhang, Albert Roux, Ron Mills

Click Fraud Botnet Detection by Calculating Mix Adjusted Traffic Value: A Method for De-Cloaking Click Fraud Attacks that is Resistant to Spoofing .................. 151
Brendan Kitts, Jing Ying Zhang, Gang Wu, Raj Mahato

Predicting User Participation in Social Networking Sites .......................................................... 154
Qingchao Kong, Wenji Mao, Daniel Zeng

An Interdisciplinary Approach to Studying and Improving Terrorism Analysis ......................... 157
Donald R. Kretz, Charles W. Granderson

Detecting Deception in Interrogation Settings ............................................................................. 160
C.E. Lamb, D.B. Skillicorn

Discovering Thematic Structure in Political Datasets .................................................................. 163
Minh-Tam Le, John Sweeney, Matthew F. Lawlor, Steven W. Zucker

Stochastic Game Model for Information Dissemination of Emergency Events in Social Network ............................................................................................................ 166
Li Liu, Yuanzhuo Wang, Jing Ding

Context Matters: Improving the Uses of Big Data for Forecasting Civil Unrest: Emerging Phenomena and Big Data ............................................................................ 169
Pedro Manrique, Hong Qi, Ana Morgenstern, Nicolás Velásquez, Tsai-Ching Lu, Neil Johnson

Layered Behavioral Trace Modeling for Threat Detection ......................................................... 173
Rudolph L. Mappus IV, Erica Briscoe
Differences between Individuals with and without Experience with Assault in Identifying Facial Signs of Imminent Aggression .................................................. 176
David Matsumoto, Hyisung C. Hwang

Efficient Anomaly Detection in Dynamic, Attributed Graphs: Emerging Phenomena and Big Data ................................................................. 179
Benjamin A. Miller, Nicholas Arcolano, Nadya T. Bliss

Identifying Groups of Interest through Temporal Analysis and Event Response Monitoring .......... 185
Jonathan Mugan, Eric McDermid, Abbey McGrew, Laura Hitt

Discovery of Persistent Threat Structures through Temporal and Geo-Spatial Characterization in Evolving Networks ......................................................... 191
Josephine M. Namayanja, Vandana P. Janeja

Improving Expert Judgment by Coherence Weighting ............................................. 197
Kenneth C. Olson, Christopher W. Karvetski

Detecting Unfolding Crises with Visual Analytics and Conceptual Maps: Emerging Phenomena and Big Data ...................................................... 200
Simon F. Pratt, Philippe J. Giabbanelli, Jean-Sébastien Mercier

Anomalies in Network Traffic .................................................................................. 206
Alan S. Rainer, Phillip Kelly

Exploring the Structural Characteristics of Social Networks in a Large Criminal Court Database ...................................................................................... 209
Andrew A. Reid, Mohammad A. Tayebi, Richard Frank

Crowdsourcing and Gamification Techniques in Inspire (AQAP Online Magazine) ....................... 215
Edna F. Reid

Sociolect-Based Community Detection .................................................................. 221
William N. Reynolds, William J. Salter, Robert M. Farber, Courtney Corley, Chase P. Dowling,
William O. Beeman, Beeman Smith-Lovin, Joon Nak Choi

Conceptual Framework to Enable Early Warning of Relevant Phenomena: Emerging Phenomena and Big Data ......................................................... 227
Bob G. Schlicher, Robert K. Abercrombie, Lee M. Hively

Maritime Situation Analysis ...................................................................................... 230
Hamed Yaghoubi Shahir, Uwe Glässer, Narek Nalbandyan, Hans Wehn

Behavioral Targeting with Social Regularization .................................................. 233
Yanmin Shang, Peng Zhang, Yanan Cao, Li Guo

Language Use in Inspire Magazine ....................................................................... 239
D.B. Skillicorn, E.F. Reid

The Edge Effect: Exploring High Crime Zones near Residential Neighborhoods ....................... 245
Justin Song, Valerie Spicer, Patricia Brantingham
A Model Docking System for Understanding Radicalization .................................................. 251
Lora Weiss, Erica Briscoe, Walter Wright, Sim Harbert, Keith Keith, John Horgan,
Lily Cushenbery, Casey Hilland

Improving Supply Chain Security using Big Data ................................................................. 254
David Zage, Kristin Glass, Richard Colbaugh

Auto-Highlighter: Identifying Salient Sentences in Text ....................................................... 260
Jessica Zeitz Self, Rebecca Zeitz, Chris North, Alan L. Breitler

How to use Experience in Cyber Analysis: An Analytical Reasoning Support System .......... 263
Chen Zhong, Deepak S. Kirubakaran, John Yen, Peng Liu, Steve Hutchinson, Hasan Cam

Jargon and Graph Modularity on Twitter .............................................................................. 381
Chase P Dowling, Courtney D Corley, Robert M Farber, William N Reynolds

Part II: Poster Papers

Unsupervised Ranking and Characterization of Differentiated Clusters ............................... 266
Luca Cazzanti, Courosh Mehanian, Julie Penzotti, Doug Scott, Oliver Downs

Identifying Threatening Networks from Transactional Data .................................................. 267
Laura Hilt, Matt McClain

Implementation of Framework to Identify Potential Phishing Websites ............................. 268
Doowon Kim, Chaitanya Achan, Jinsuk Baek, Paul S. Fisher

Armored Ads ......................................................................................................................... 269
Wesley Brandi, Brendan Kitts, Raj Mahato, Jing Ying Zhang

Assessment of Malicious Applications using Permissions and Enhanced User Interfaces on Android ........................................................................................................... 270
Sangho Lee, Da Young Ju

Exploring Trajectory Behavior Model for Anomaly Detection in Maritime Moving Objects .... 271
Po-Ruey Lei

Ensemble Classification over Stock Market Time Series and Economy News ..................... 272
Sadi Evren Seker, Cihan Mert, Khaled Al-Naami, Ugur Ayan, Nuri Ozalp

A New Pruning Method for Resolving Conflicts in Actionable Behavioral Rules ................ 274
Peng Su, Dan Zhu, Daniel Zeng
Part III: Workshop Papers

Workshop 1: Evaluating Visualization in Support of Analytical Reasoning and Decision Making for Cybersecurity
Organizing Institution: Innovative Analytics

Reflecting on Visualization for Cyber Security ............................................................................... 275
Carrie Gates, Sophie Engle

Investigating the Efficacy of Network Visualizations for Intelligence Tasks ............................... 278
Christopher W. Berardi, Erin T. Solovey, Mary L. Cummings

Capturing Human Cognition in Cyber-Security Simulations with NETS .................................. 284
Nicklaus A. Giacobe, Michael D. McNeese, Vincent F. Mancuso, Dev Minotra

Visualization Techniques for Efficient Malware Detection ....................................................... 289
John Donahue, Anand Paturi, Srinivas Mukkamala

Information Visualization Metrics and Methods for Cyber Security Evaluation ....................... 292
John T. Langton, Alex Baker

Christopher Alexander’s Fifteen Properties: Toward Developing Evaluation Metrics for Security Visualizations ......................................................................................... 295
Ziyad Alshaikh, Abdulrahman Alarifi, Mansour Alsaleh

Workshop 2: Signature Discovery for Intelligence and Security
Organizing Institution: Pacific Northwest National Laboratory

Research Towards a Systematic Signature Discovery Process ................................................. 301
Nathan A. Baker, Jonathan L. Barr, George T. Bonheyo, Cliff A. Joslyn, Kannan Krishnaswami,
Mark E. Oxley, Rich Quadrel, Landon H. Sego, Mark F. Tardiff, Adam S. Wynne

An Investigation into Label Fusion on Sparse Data .................................................................... 309
Alexander M. Venzin, Mark E. Oxley, Nathaniel Beagley

Graph Analytics for Signature Discovery ..................................................................................... 315
Emilie Hogan, John R. Johnson, Mahaniesh Halappanavar, Chaomei Lo

Lame’ Curve-Based Signature Discovery Learning Technique for Network Traffic Classification .................................................................................................................. 321
Shan Suthaharan, Laxmi Sunkara, Sweta Keshapagou

Capturing Signatures of Anomalous Behavior in Online Social Networks .............................. 327
Arun V. Sathanur, Vikram Jandhyala, Chuanjia Xing

A Generalized Bio-Inspired Method for Discovering Sequence-Based Signatures .................. 330
Elena Peterson, Darren Curtis, Aaron Phillips, Jeremy Teuton, Christopher Oehmen
Signature Discovery for Personalized Medicine .............................................. 333
Ka Yee Yeung

The Lifecycle of Bayesian Network Models Developed for Multi-Source
Signature Assessment of Nuclear Programs .................................................. 339

Assessing the Quality of Bioforensic Signatures ........................................ 346
Landon H. Sego, Aimee E. Holmes, Luke J. Gosink, Bobbie-Jo M. Webb-Robertson,
Helen W. Kreuzer, Richard M. Anderson, Alan J. Brothers, Courtney D. Corley, Mark R. Tardiff

The CommonGround Visual Paradigm for Biosurveillance .......................... 352
Yarden Livnat, Elizabeth Jurrus, Adi V. Gundlapalli, Per Gestland

Workshop 3: Social Media Analytics and Social Computing
Organizing Institution: Boeing, Chinese Academy of Sciences,
and the University of Arizona

PHYSENSE: Scalable Sociological Interaction Models for Influence
Estimation on Online Social Networks ....................................................... 358
Arun V. Sathanur, Vikram Jandhyala, Chuanjia Xing

Measuring Expertise and Bias in Cyber Security using
Cognitive and Neuroscience Approaches ................................................... 364
Daniel Krawczyk, James Bartlett, Murat Kantarcioglu, Kevin Hamlen, Bhavani Thuraisingham

Action Knowledge Extraction from Web Text ........................................... 368
Ansheng Ge, Wenji Mao, Daniel Zeng, Lei Wang

Discovering Seasonal Patterns of Smoking Behavior using Online Search Information .......... 371
Zhu Zhang, Xiaolong Zheng, Daniel Dajun Zeng, Kainan Cui, Chuan Luo, Saike He,
Scott Leischow

Discovering the Rating Pattern of Online Reviewers through Data Co-clustering .......... 374
Jie Wang, Xiwei Liang

Author Index ......................................................................................... 377

Jargon and Graph Modularity on Twitter ..................................................... 381
Chase P Dowling, Courtney D Corley, Robert M Farber, William N Reynolds