

# **2014 IEEE Joint Intelligence and Security Informatics Conference**

**(JISIC 2014)**

**The Hague, Netherlands  
24 – 26 September 2014**



**IEEE Catalog Number: CFP1432Y-POD**  
**ISBN: 978-1-4799-6365-2**

# 2014 IEEE Joint Intelligence and Security Informatics Conference

## JISIC 2014

### Table of Contents

Message from General Chairs .....	.xi
Message from Program Chairs .....	.xii
Conference Organization.....	.xiii
Program Committee.....	.xiv
Keynotes .....	.xvii

---

### Long Papers

Aegis: A Lightweight Tool for Prevent Frauds in Web Browsers .....	1
<i>Carlo Marcelo Revoredo da Silva, José Lutiano Costa da Silva, Rodrigo Elia Assad, and Ruy José Guerra Barretto de Queiroz Vinicius Cardoso Garcia</i>	
DNSSEC Misconfigurations: How Incorrectly Configured Security Leads to Unreachability .....	9
<i>Niels L. M. van Adrichem, Antonio Reyes Lua, Xin Wang, Muhammad Wasif, Ficky Fatturrahman, and Fernando A. Kuipers</i>	
Overcoming Limited Collaboration Channels in Distributed Intelligence Analysis: Visualization Tools and Design Seeds .....	17
<i>Brian Prue, Michael Jenkins, Lauren D. Stern, and Jonathan Pfautz</i>	
Time-to-Event Modeling for Predicting Hacker IRC Community Participant Trajectory .....	25
<i>Victor Benjamin and Hsinchun Chen</i>	
Authorship Analysis of Inspire Magazine through Stylometric and Psychological Features .....	33
<i>Jennifer Sikos, Peter David, Nizar Habash, and Reem Faraj</i>	
The Nature of Communications and Emerging Communities on Twitter Following the 2013 Syria Sarin Gas Attacks .....	41
<i>Yulia Tyshchuk, William A. Wallace, Hao Li, Heng Ji, and Sue E. Kase</i>	

Twitter Sentiment Analysis for Security-Related Information Gathering .....	48
<i>Anna Jurek, Yaxin Bi, and Maurice Mulvenna</i>	
Descriptive Analytics: Examining Expert Hackers in Web Forums .....	56
<i>Ahmed Abbasi, Weifeng Li, Victor Benjamin, Shiyu Hu, and Hsinchun Chen</i>	
Identifying Top Sellers In Underground Economy Using Deep Learning-Based Sentiment Analysis .....	64
<i>Weifeng Li and Hsinchun Chen</i>	
Time Critical Disinformation Influence Minimization in Online Social Networks .....	68
<i>Chuan Luo, Kainan Cui, Xiaolong Zheng, and Daniel Zeng</i>	
A Selective Defense for Application Layer DDoS Attacks .....	75
<i>Yuri Gil Dantas, Vivek Nigam, and Iguatemi E. Fonseca</i>	
Time Profiles for Identifying Users in Online Environments .....	83
<i>Fredrik Johansson, Lisa Kaati, and Amendra Shrestha</i>	
ALPD: Active Learning Framework for Enhancing the Detection of Malicious PDF Files .....	91
<i>Nir Nissim, Aviad Cohen, Robert Moskovitch, Assaf Shabtai, Mattan Edry, Oren Bar-Ad, and Yuval Elovici</i>	
Predicting Popularity of Forum Threads for Public Events Security .....	99
<i>Qingchao Kong, Wenji Mao, Daniel Zeng, and Lei Wang</i>	
Predicting Links in Multi-relational Networks .....	107
<i>Bisharat Rasool Memon and Uffe Kock Wil</i>	
Practical Interception of DECT Encrypted Voice Communication in Unified Communications Environments .....	115
<i>Iwen Coisel and Ignacio Sanchez</i>	
Mining the Web for Sympathy: The Pussy Riot Case .....	123
<i>Anders Westling, Joel Brynielsson, and Tove Gustavi</i>	
Resource-Based Event Reconstruction of Digital Crime Scenes .....	129
<i>Yi-Ching Liao and Hanno Langweg</i>	
Inferring itineraries of containerized cargo through the application of Conditional Random Fields .....	137
<i>Pedro Chahuara, Luca Mazzola, Michail Makridis, Claudio Schifanella, Aris Tsois, and Mauro Pedone</i>	
Trusted Detection of Sensitive Activities on Mobile Phones Using Power Consumption Measurements .....	145
<i>Mordechai Guri, Gabi Kedma, Boris Zadov, and Yuval Elovici</i>	
Resilience of Anti-malware Programs to Naïve Modifications of Malicious Binaries .....	152
<i>Mordechai Guri, Gabi Kedma, Assaf Kachlon, and Yuval Elovici</i>	

On the Usability of Augmented Reality for Information Exchange in Teams from the Security Domain .....	160
<i>Dragoş Datcu, Marina Cidota, Heide Lukosch, and Stephan Lukosch</i>	
Understanding the Factors Affecting UX and Technology Acceptance in the Context of Automated Border Controls .....	168
<i>Mari Ylikauppila, Sirra Toivonen, Minna Kulju, and Minna Jokela</i>	
Addressing the Increasing Volume and Variety of Digital Evidence Using an Ontology .....	176
<i>Owen Brady, Richard Overill, and Jeroen Keppens</i>	
Modelling and Analysis of Identity Threat Behaviors through Text Mining of Identity Theft Stories .....	184
<i>Yongpeng Yang, Monisha Manoharan, and K. Suzanne Barber</i>	
Maritime Situation Analysis: A Multi-vessel Interaction and Anomaly Detection Framework .....	192
<i>Hamed Yaghoubi Shahir, Uwe Glässer, Narek Nalbandyan, and Hans Wehn</i>	
On the Adequacy of Performance Models in an Adaptive Border Inspection Management System .....	200
<i>Jesse Musgrove, Bojan Cukic, and Vittorio Cortellessa</i>	

## Short Papers

Land Border Permeability and Irregular Migration Using Geospatial Intelligence from Satellite Data .....	208
<i>A. C. van den Broek, R. M. Schoemaker, and R. J. Dekker</i>	
Studies of Integration Readiness Levels: Case Shared Maritime Situational Awareness System .....	212
<i>Rauno Pirinen</i>	
Threat Detection in Tweets with Trigger Patterns and Contextual Cues .....	216
<i>Martijn Spitters, Pieter T. Eendebak, Daniël T. H. Worm, and Henri Bouma</i>	
Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services .....	220
<i>Martijn Spitters, Stefan Verbruggen, and Mark van Staalduinen</i>	
A Case Study in Opportunity Reduction: Mitigating the Dirt Jumper Drive-Smart Attack .....	224
<i>Joel Lathrop and James B. O'Kane</i>	
Security Components in a One-Stop-Shop Border Control System .....	228
<i>Axel Weissenfeld, Andreas Kriechbaum-Zabini, and Lukasz Szklarski</i>	

Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT) .....	232
<i>Mark Patton, Eric Gross, Ryan Chinn, Samantha Forbis, Leon Walker, and Hsinchun Chen</i>	
Ranking Online Memes in Emergency Events Based on Transfer Entropy .....	236
<i>Saike He, Xiaolong Zheng, Xiuguo Bao, Hongyuan Ma, Daniel Zeng, Bo Xu, Guanhua Tian, and Hongwei Hao</i>	
Challenges to a Smooth-Running Data Security Audits. Case: A Finnish National Security Auditing Criteria KATAKRI .....	240
<i>Jyri Rajamäki</i>	
Three Statistical Approaches to Sessionizing Network Flow Data .....	244
<i>Patrick Rubin-Delanchy, Daniel J. Lawson, Melissa J. Turcotte, Nicholas Heard, and Niall M. Adams</i>	
Statistical Frameworks for Detecting Tunnelling in Cyber Defence Using Big Data .....	248
<i>Daniel J. Lawson, Patrick Rubin-Delanchy, Nicholas Heard, and Niall M. Adams</i>	
Adaptive Change Detection for Relay-Like Behaviour .....	252
<i>Dean Adam Bodenham and Niall M. Adams</i>	
An Approximate Framework for Flexible Network Flow Screening .....	256
<i>Niall M. Adams and Daniel J. Lawson</i>	
Causal Inference in Social Media Using Convergent Cross Mapping .....	260
<i>Chuan Luo, Xiaolong Zheng, and Daniel Zeng</i>	
Exfiltration of Information from Air-Gapped Machines Using Monitor's LED Indicator .....	264
<i>Vitali Sepetnitsky, Mordechai Guri, and Yuval Elovici</i>	
Filtering Automated Polling Traffic in Computer Network Flow Data .....	268
<i>Nick Heard, Patrick Rubin-Delanchy, and Daniel J. Lawson</i>	
Modelling New Edge Formation in a Computer Network through Bayesian Variable Selection .....	272
<i>Silvia Metelli and Nicholas Heard</i>	
Automatic Timeline Construction and Analysis for Computer Forensics Purposes .....	276
<i>Yoan Chabot, Aurélie Bertaux, Christophe Nicolle, and Tahar Kechadi</i>	
A Service-Independent Model for Linking Online User Profile Information .....	280
<i>Matthew John Edwards, Awais Rashid, and Paul Rayson</i>	
Exploring Opinion Dynamics in Security-Related Microblog Data .....	284
<i>Yuhao Zhang, Wenji Mao, Daniel Zeng, Ning Zhao, and Xiuguo Bao</i>	
Multiagent Models for Police Resource Allocation and Dispatch .....	288
<i>Ricardo Guedes, Vasco Furtado, and Tarcísio Pequeno</i>	

Application of a Linear Time Method for Change Point Detection to the Classification of Software .....	292
<i>Alexander Bolton and Nicholas Heard</i>	
How Analysts Think (?): Early Observations .....	296
<i>B. L. William Wong</i>	
Optical Security Document Simulator for Black-Box Testing of ABC Systems .....	300
<i>Michael Gschwandtner, Svorad Štolc, and Franz Daubner</i>	
Forecasting Country Stability in North Africa .....	304
<i>Steven Banaszak, Elizabeth Bowman, John P. Dickerson, and V. S. Subrahmanian</i>	
AccountabilityFS: A File System Monitor for Forensic Readiness .....	308
<i>Rune Nordvik, Yi-Ching Liao, and Hanno Langweg</i>	
Foraging Online Social Networks .....	312
<i>Gijs Koot, Mirjam A. A. Huis in 't Veld, Joost Hendricksen, Rianne Kaptein, Arnout de Vries, and Egon L. van den Broek</i>	

## Posters

CAPER: Collaborative Information, Acquisition, Processing, Exploitation and Reporting for the Prevention of Organised Crime .....	316
<i>Gila Molcho, Sebastian Maier, Felipe Melero, and Carlo Aliprandi</i>	
Detecting Threats of Violence in Online Discussions Using Bigrams of Important Words .....	319
<i>Hugo Lewi Hammer</i>	
Learning to Classify Hate and Extremism Promoting Tweets .....	320
<i>Ashish Sureka and Swati Agarwal</i>	
Recommending Documents for Complex Question Exploration by Analyzing Browsing Behavior .....	321
<i>Alya Abbott and Olga Simek</i>	
Passwords are Dead: Alternative Authentication Methods .....	322
<i>Michael Bachmann</i>	
Sensemaking and Cognitive Bias Mitigation in Visual Analytics .....	323
<i>Margit Pohl, Lisa-Christina Winter, Chris Pallaris, Simon Attfield, and B. L. William Wong</i>	
Metal Oxide Gas Sensors Technologies for Hidden People Detection .....	324
<i>Andrea Ponzoni, Dario Zappa, Cristina Cerqui, Elisabetta Comini, and Giorgio Sberveglieri</i>	
Towards a Methodology for Cybersecurity Risk Management Using Agents Paradigm .....	325
<i>Edgar Toshiro Yano, Parth Bhatt, Per M Gustavsson, and Rose-Mharie Åhlfeldt</i>	

Computational Approach for Detection of Illegal Activity over the Internet .....	326
<i>Rasim Alguliyev, Davud Rustamov, and Mirza Rzayev</i>	
POLAR-An Interactive Patterns of Life Visualisation Tool for Intelligence Analysis .....	327
<i>Neesha Kodagoda, Simon Attfield, Phong H. Nguyen, Leishi Zhang, Kai Xu, B L William Wong, Adrian Wagstaff, Graham Phillips, James Bulloch, John Marshall, and Stewart Bertram</i>	
Modeling Flash Mobs in Cybernetic Space: Evaluating Threats of Emerging Socio-Technical Behaviors to Human Security .....	328
<i>Samer Al-khateeb and Nitin Agarwal</i>	
Military Geospatial Profiling Analysis .....	329
<i>Herman-Dick Giok Tjiang Oey</i>	
Robust Navigation and Communication in the Maritime Domain: The TRITON Project .....	331
<i>Marco Pini, Luca Pilosu, Lene Vesterlund, David Blanco, Fredrik Lindström, and Emiliano Spaltro</i>	
Detection of Olfactory Traces by Orthogonal Gas Identification Technologies - DOGGIES .....	332
<i>I. Daniilidis, J.-J. Filippi, W. Vautz, E. Dalcanale, S. Zampolli, G. Leventakis, I. Kauppinen, S. Sinisalo, V. Tsoukias, V. Kassouras, M. Carras, B. Gerard, R. Pinalli, A. Ragnoni, L. Dujourdy, D. Zavali, M. Brun, V. Grizis, A. Argyris, and D. Syvridis</i>	
When Counting is Not Enough: Limitations of NSA's Effectiveness Assessment of Surveillance Technology .....	333
<i>Michelle Cayford, Coen van Gulijk, and P.H.A.J.M. van Gelder</i>	
DOCSCOPE: ID Printing Techniques Signatures .....	334
<i>Marc Michel Pic, Clarisse Mandridake, Mathieu Hoarau, and Kevin Win-Lime</i>	
<b>Author Index</b> .....	<b>335</b>