2016 IEEE Conference on Intelligence and Security Informatics (ISI 2016)

Tucson, Arizona, USA
28-30 September 2016

IEEE Catalog Number: CFP16ITI-POD
ISBN: 978-1-5090-3866-4

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP16ITI-POD
ISBN (Print-On-Demand): 978-1-5090-3866-4
ISBN (Online): 978-1-5090-3865-7

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

TECHNICAL PAPERS

Part I: Long Papers

Cybersecurity Analytics and Threat Intelligence

Rights Management to Enable a True Internet of Things 1
Robert Newman, Pat Doody, Mira Trebar, Uchenna Okeke

Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence 7
Eric Nunes, Ahmad Diab, Andrew Gunn, Ericsson Marin, Vineet Mishra, Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, Paulo Shakarian

Exploring Key Hackers and Cybersecurity Threats in Chinese Hacker Communities 13
Zhen Fang, Xinyi Zhao, Qiang Wei, Guoqing Chen, Yong Zhang, Chunxiao Xing, Weifeng Li, Hsinchun Chen

AZSecure Hacker Assets Portal: Cyber Threat Intelligence and Malware Analysis 19
Sagar Samtani, Kory Chinn, Cathy Larson, Hsinchun Chen

Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques 25
Sagar Samtani, Shuo Yu, Hongyi Zhu, Mark Patton, Hsinchun Chen

PhishMonger: A Free and Open Source Public Archive of Real-World Phishing Websites 31
David G. Dobolyi, Ahmed Abbasi

Using Cyber Defense Exercises to Obtain Additional Data for Attacker Profiling 37
Joel Brynielsson, Ulrik Franke, Muhammad Adnan Tariq, Stefan Varga

Mining Hospital Data Breach Records: Cyber Threats to U.S. Hospitals 43
Travis Floyd, Matthew Grieco, Edna F. Reid

Data Science and Analytics in Security Informatics

Bayesian Nonparametric Relational Learning with the Broken Tree Process 49
Justin Sahs

Activating Topic Models from a Cognitive Perspective 55
Jie Bai, Linjing Li, Daniel Zeng

Meme Extraction and Tracing in Crisis Events 61
Saike He, Xiaolong Zheng, Jiaojiao Wang, Zhijun Chang, Yin Luo, Daniel Zeng

Predictability of NetFlow Data 67
Marina Evangelou, Niall M. Adams

Effective Prioritization of Network Intrusion Alerts to Enhance Situational Awareness 73
E. Allison Newcomb, Robert J. Hammell II, Steve Hutchinson

Identifying Features for Detecting Fraudulent Loan Requests on P2P Platforms 79
Jennifer Xu, Dongyu Chen, Michael Chau

Measuring Online Affects in a White Supremacy Forum 85
Léo Figea, Lisa Kaati, Ryan Scrivens

Model-Based Clustering and New Edge Modelling in Large Computer Networks 91
Silvia Metelli, Nicholas Heard

Chinese Underground Market Jargon Analysis Based on Unsupervised Learning 97
Kangzhi Zhao, Yong Zhang, Chunxiao Xing, Weifeng Li, Hsinchun Chen

Automated Big Text Security Classification 103
Khudran Alzhrani, Ethan M. Rudd, Terrance E. Boult, C. Edward Chow

Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content 109
Ahmed T. Zulkarnine, Richard Frank, Bryan Monk, Julianna Mitchell, Garth Davies

Activity Monitoring Using Topic Models 115
Boshra Nabaei, Martin Ester

Automatic Detection of Xenophobic Narratives: A Case Study on Swedish Alternative Media 121
Lisa Kaati, Amendra Shrestha, Katie Cohen, Sinna Lindquist

Spatial-Temporal Patterns and Drivers of Illicit Tobacco Trade in Changsha County, China 127
Jiaojiao Wang, Saike He, Yiyuan Xu, Zhidong Cao, Lei Wang, Daniel Dajun Zeng

A Non-Parametric Learning Approach to Identify Online Human Trafficking 133
Hamidreza Alvari, Paulo Shakarian, J.E. Kelly Snyder

Near Real-time Atrocity Event Coding 139
Mohiuddin Solaimani, Sayeed Salam, Ahmad M. Mustafa, Latifur Khan, Patrick T. Brandt, Bhavani Thuraisingham

Exploring the Online Underground Marketplaces through Topic-Based Social Network and Clustering 145
Shin-Ying Huang, Hsinchun Chen

Discovering Structure in Islamist Postings Using Systemic Nets 151
N. Alsadhan, D.B. Skillicorn

Social Media Account Linkage Using User-Generated Geo-Location Data 157
Xiaohui Han, Lianhai Wang, Lijuan Xu, Shuihui Zhang

Human Behavior and Factors in Security Applications

Trust and Distrust as Distinct Constructs: Evidence from Data Theft Environments 163
Steven J. Simon

Phishing Susceptibility: The Good, the Bad, and the Ugly 169
Ahmed Abbasi, F. Mariam Zahedi, Yan Chen

Organizational, National, and International Issues in Counter-Terrorism and Other Security Applications

Identifying the Socio-Spatial Dynamics of Terrorist Attacks in the Middle East 175
Ze Li, Duoyong Sun, Hsinchun Chen, Shin-Ying Huang

The Impact of US Cyber Policies on Cyber-Attacks Trend 181
Sumeet Kumar, Matthew Benigni, Kathleen M. Carley

Part II: Short Papers
Cybersecurity Analytics and Threat Intelligence

Product Offerings in Malicious Hacker Markets 187
Ericsson Marin, Ahmad Diab, Paulo Shakarian

Topic Modelling of Authentication Events in an Enterprise Computer Network 190
Nick Heard, Konstantina Palla, Maria Skoularidou

Shodan Visualized 193
Vincent J. Ercolani, Mark W. Patton, Hsinchun Chen

SCADA Honeypots: An In-depth Analysis of Conpot 196
Arthur Jicha, Mark Patton, Hsinchun Chen

Identifying Devices across the IPv4 Address Space 199
Ryan Jicha, Mark W. Patton, Hsinchun Chen, Cathy Larson

Data Science and Analytics in Security Informatics

New Words Enlightened Sentiment Analysis in Social Media 202
Chiyu Cai, Linjing Li, Daniel Zeng

Identifying Language Groups within Multilingual Cybercriminal Forums 205
Victor Benjamin, Hsinchun Chen

Poisson Factorization for Peer-Based Anomaly Detection 208
Melissa Turcotte, Juston Moore, Nick Heard, Aaron McPhall

Social Role Clustering with Topic Model 211
Jie Bai, Linjing Li, Daniel Zeng, Junjie Lin

Competitive Perspective Identification via Topic Based Refinement for Online Documents 214
Junjie Lin, Wenji Mao, Daniel Zeng

Part III: Poster Papers
Cybersecurity Analytics and Threat Intelligence

Anonymous Port Scanning: Performing Network Reconnaissance Through Tor 217
Rodney Rohrmann, Mark W. Patton, Hsinchun Chen

DDoS Cyber-Attacks Network: Who's Attacking Whom 218
Sumeet Kumar, Kathleen M. Carley

Data Science and Analytics in Security Informatics

Identifying Top Listers in Alphabay Using Latent Dirichlet Allocation 219
John Grisham, Calvin Barreras, Cyrus Afarin, Mark Patton, Hsinchun Chen

Part IV: Workshop Papers
Big Data Analytics for Cybersecurity Computing

Network-Wide Anomaly Detection via the Dirichlet Process 220
Nick Heard, Patrick Rubin-Delanchy

Parallel Massive Data Monitoring and Processing Using Sensor Networks 225
Hamid Reza Naji, Najmeh Rezaee

Understanding DDoS Cyber-Attacks Using Social Media Analytics 231
Sumeet Kumar, Kathleen M. Carley

IoT Security Development Framework for Building Trustworthy Smart Car Services 237
Jesus Pacheco, Shalaka Satam, Salim Hariri, Clarisa Grijalva, Helena Berkenbrock

Disassortativity of Computer Networks 243
Patrick Rubin-Delanchy, Niall M. Adams, Nicholas A. Heard

Activity-Based Temporal Anomaly Detection in Enterprise-Cyber Security 248
Mark Whitehouse, Marina Evangelou, Niall M. Adams

Cybersecurity Education & Workforce

An Undergraduate Cyber Operations Curriculum in the Making: A 10^{+} Year Report 251
Shiva Azadegan, Michael O'Leary

Engaging Females in Cybersecurity: K through Gray 255
Xiang Liu, Diane Murphy

Using Eye-tracking to Investigate Content Skipping: A Study on Learning Modules in Cybersecurity 261
Sagar Raina, Leon Bernard, Blair Taylor, Siddharth Kaza

Cybersecurity Workforce Development: A Peer Mentoring Approach 267
Vandana P. Janeja, Carolyn Seaman, Kerrie Kephart, Aryya Gangopadhyay, Amy Everhart

Design and Implementation of a Multi-Facet Hierarchical Cybersecurity Education Framework 273
Wei Wei, Arti Mann, Kewei Sha, T. Andrew Yang

Smart Augmented Reality Glasses in Cybersecurity and Forensic Education 279
Nikitha Kommera, Faisal Kaleem, Syed Mubashir Shah Harooni

CySCom: CyberSecurity COMics 282
Brian Ledbetter Jr., Zach Wallace, Adam Harms, Ambareen Siraj

Challenges, Lessons Learned and Results from Establishing a CyberCorps: Scholarship for Service Program Targeting Undergraduate Students 285
Shiva Azadegan, Josh Dehlinger, Siddharth Kaza, Blair Taylor, Wei Yu

Women in Cybersecurity

Intruder Detector: A Continuous Authentication Tool to Model User Behavior 286
Leslie C. Milton, Atif Memon

An Immune Inspired Unsupervised Intrusion Detection System for Detection of Novel Attacks 292
Manjari Jha, Raj Acharya

Automatic Clustering of Malware Variants 298
Rima Asmar Awad, Kirk D. Sayre

Doctoral Consortium

Soft Computing and Hybrid Intelligence for Decision Support in Forensics Science 304
Andrii Shalaginov

Approaches to Understanding the Motivations Behind Cyber Attacks 307
Sumeet Kumar, Kathleen M. Carley

Topic Modeling of Small Sequential Documents: Proposed Experiments for Detecting Terror Attacks 310
Brandon W. Jones, Wingyan Chung

Detecting Radicalization Trajectories Using Graph Pattern Matching Algorithms 313
Benjamin W.K. Hung, Anura P. Jayasumana, Vidarshana W. Bandara

Modeling Cyber-Attacks on Industrial Control Systems 316
Vivin Paliath, Paulo Shakarian

Using Social Network Analysis to Identify Key Hackers for Keylogging Tools in Hacker Forums 319
Sagar Samtani, Hsinchun Chen

Targeting Key Data Breach Services in Underground Supply Chain 322
Weifeng Li, Junming Yin, Hsinchun Chen