2017 IEEE International Conference on Intelligence and Security Informatics (ISI 2017)

Beijing, China
22-24 July 2017

IEEE Catalog Number: CFP17ITI-POD
ISBN: 978-1-5090-6728-2

Copyright © 2017 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

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

IEEE Catalog Number: CFP17ITI-POD
ISBN (Print-On-Demand): 978-1-5090-6728-2
ISBN (Online): 978-1-5090-6727-5

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 Paper

Human Behavior and Factors in the Security Applications

Proactive Information Security Behavior and Individual Creativity: Effects of Group Culture and Decentralized IT Governance 1
Canchu Lin, Jenell L.S. Wittmer

A Novel Approach for Analysis of Attack Graph 7
Mehdi Yousefi, Nhamo Mtetwa, Yan Zhang, Huaglory Tianfield

Mobile Analytics in Security Informatics

Identifying Mobile Malware and Key Threat Actors in Online Hacker Forums for Proactive Cyber Threat Intelligence 13
John Grisham, Sagar Samtani, Mark Patton, Hsinchun Chen

Linking Social Network Accounts by Modeling user Spatiotemporal Habits 19
Xiaohui Han, Lianhai Wang, Shujiang Xu, Guangqi Liu, Dawei Zhao

Network Analytics in Security Informatics

Raising Flags: Detecting Covert Storage Channels using Relative Entropy 25
Josephine Chow, Xiangyang Li, Xenia Mountrouidou

Clustering and Monitoring Edge Behaviour in Enterprise Network Traffic 31
Christopher Schon, Niall Adams, Marina Evangelou

Tie Strength Still Matters: Investigating Interaction Patterns of Al-Qaeda Network in Terror Operations 37
Ze Li, Duoyong Sun, Kui Cai, Bo Li

End-to-end Encrypted Traffic Classification with One-dimensional Convolution Neural Networks 43
Wei Wang, Ming Zhu, Jinlin Wang, Xuewen Zeng, Zhongzhen Yang

Hierarchical Network Threat Situation Assessment Method for DDoS based on D-S Evidence Theory 49
Zihao Liu, Bin Zhang, Ning Zhu, Lixun Li

Hacking Social Network Data Mining 54
Yasmeen Alufaisan, Yan Zhou, Murat Kantarcioglu, Bhavani Thuraisingham

Predictive Analytics in Security Informatics

Recognizing Military Vehicles in Social Media Images using Deep Learning 60
Tuomo Hiippala

A Framework for Digital Forensics Analysis based on Semantic Role Labeling 66
Ravi Barreira, Vladia Pinheiro, Vasco Furtado

Security Analytics and Threat Intelligence

Phishing Detection: A Recent Intelligent Machine Learning Comparison based on Models Content and Features 72
Neda Abdelhamid, Fadi Thabtah, Hussein Abdel-jaber

Security Information Surveillance and Integration

Alignment-Free Indexing-First-One Hashing with Bloom Filter Integration 78
Yen-Lung Lai, Bok-Min Goi, Tong-Yuen Chai

Benchmarking Vulnerability Scanners: An Experiment on SCADA Devices and Scientific Instruments 83
Malaka El, Emma McMahon, Sagar Samtani, Mark Patton, Hsinchun Chen

Information Sharing & Cyber Threats 89
Sonya H.Y. Hsu, Steven J. Dick

Text Analytics in Security Informatics

Web-derived Emotional Word Detection in Social Media using Latent Semantic Information 95
Chiyu Cai, Linjing Li, Daniel Zeng

The Dynamics of Health Sentiments with Competitive Interactions in Social Media 101
Saike He, Xiaolong Zheng, Daniel Zeng

Prioritized Active Learning for Malicious URL Detection using Weighted Text-Based Features 107
Sreyasee Das Bhattacharjee, Ashit Talukder, Ehab Al-Shaer, Pratik Doshi

Mapping Users across Social Media Platforms by Integrating Text and Structure Information 113
Song Sun, Qiudan Li, Peng Yan, Daniel D. Zeng

Topic Evolution Modeling in Social Media Short Texts based on Recurrent Semantic Dependent CRP 119
Yuhao Zhang, Wenji Mao, Daniel Zeng

Part II: Short Paper

Human Behavior and Factors in the Security Applications

Impact of Human Mobility on Police Allocation 125
Carlos Caminha, Vasco Furtado

Behavior Enhanced Deep Bot Detection in Social Media 128
Chiyu Cai, Linjing Li, Daniel Zeng

Topic and User based Refinement for Competitive Perspective Identification 131
Junjie Lin, Wenji Mao, Daniel Zeng

Ranking Events based on user Relevant Query 134
Xiangfei Kong, Wenji Mao

Impact of Replacement Policies on Static-Dynamic Query Results Cache in Web Search Engines 137
Hongyuan Ma, Ou Tao, Chunlu Zhao, Pengxiao Li, Lihong Wang

Mobile Analytics in Security Informatics

An End-to-End Model for Android Malware Detection 140
Hongliang Liang, Yan Song, Da Xiao

Resolving Reflection Methods in Android Applications 143
Zhichao Cheng, Fanping Zeng, Xingqiu Zhong, Mingsong Zhou, Chengcheng Lv, Shuli Guo

The Impact of Different Perceived Dimensions of Mobile Media APP users on Customer Commitment and Customer Recommendation 146
Qian Li, Xiu-cun Wang

Network Analytics in Security Informatics

Reasoning Crypto Ransomware Infection Vectors with Bayesian Networks 149
Aaron Zimba, Zhaoshun Wang, Hongsong Chen

Analyzing Multimodal Public Sentiment based on Hierarchical Semantic Attentional Network 152
Nan Xu

Predictive Analytics In Security Informatics

Wavelet Transform and Unsupervised Machine Learning to Detect Insider Threat on Cloud File-Sharing 155
Wangyan Feng, Wenfeng Yan, Shuning Wu, Ningwei Liu

Efficient Parameter Selection for SVM: The Case of Business Intelligence Categorization 158
Hsin-Hsiung Huang, Zijing Wang, Wingyan Chung

An Attention-based Neural Popularity Prediction Model for Social Media Events 161
Guandan Chen, Qingchao Kong, Wenji Mao

Developing Curricular Modules for Cybersecurity Informatics: An Active Learning Approach 164
Wingyan Chung

Real-Time Prediction of Meme Burst 167
Jie Bai, Linjing Li, Lan Lu, Yanwu Yang, Daniel Zeng

Security Analytics and Threat Intelligence

On Man-in-the-Cloud (MITC) Attacks: The Analytical Case of Linux 170
Aaron Zimba, Zhaoshun Wang

A User-Centric Machine Learning Framework for Cyber Security Operations Center 173
Wangyan Feng, Shuning Wu, Ningwei Liu

Assessing Medical Device Vulnerabilities on the Internet of Things 176
Emma McMahon, Ryan Williams, Malaka El, Sagar Samtani, Mark Patton, Hsinchun Chen

Identifying Vulnerabilities of Consumer Internet of Things (IoT) Devices: A Scalable Approach 179
Ryan Williams, Emma McMahon, Sagar Samtani, Mark Patton, Hsinchun Chen

Security Information Surveillance and Integration

Online Event Detection and Tracking in Social Media based on Neural Similarity Metric Learning 182
Guandan Chen, Qingchao Kong, Wenji Mao

Large Scale Port Scanning Through Tor: Using Parallel Nmap Scans to Scan Large Portions of the IPv4 Range 185
Rodney R. Rohrmann, Vincent J. Ercolani, Mark W. Patton

Text Analytics in Security Informatics

Exploring Linguistic Features for Extremist Texts Detection (on the Material of Russian-Speaking Illegal Texts) 188
Dmitry Devyatkin, Ivan Smirnov, Margarita Ananyeva, Maria Kobozeva, Andrey Chepovskiy, Fyodor Solovyev

Criminal Intelligence Surveillance and Monitoring on Social Media: Cases of Cyber-Trafficking 191
Wingyan Chung, Elizabeth Mustaine, Daniel Zeng

Modeling Online Collective Emotions through Knowledge Transfer 194
Saike He, Xiaolong Zheng, Daniel Zeng

Part III: Poster

Human Behavior and Factors in the Security Applications

A New Approach to Security Informatics: Actionable Behavioral Rules Mining (ABRM) 197
Peng Su, Yuqin Zhao, Jian Yang, Zhenpeng Li

Research on the Relationship between Informatization Level and Global Competitiveness 198
Tian Beibei, Zheng Feifei, Cao Yuqi

An Identity-based One-Off Public Key Scheme for Privacy Preservation 199
Linpeng Chai, Bin Zhang

Mobile Analytics in Security Informatics

Static Detection on Android Malware based on Improved Random Forest Algorithm 200
Hou Su, Lu Tianliang, Du Yanhui, Guo Jing

Android app Protection using Same Identifier Attack Defensor 201
Jinseong Kim, Im Y. Jung

Research on High-Resolution Imaging Technology to Extract the Halftone-Dot-Information by iPhone 202
Luo Lu, Cao Peng, Mu Dazhong

Network Analytics in Security Informatics

Enhance the Robustness of Cyber-Physical Systems by Adding Interdependency 203
Pengshuai Cui, Peidong Zhu, Peng Xun, Zhuoqun Xia

Predictive Analytics In Security Informatics

Anti-DDoS Technique using Self-Learning Bloom Filter 204
C.Y. Tseung, K.P. Chow, X. Zhang

Security Analytics and Threat Intelligence

Attack Pattern Mining Algorithm based on Security Log 205
Keyi Li, Yang Li, Jianyi Liu, Ru Zhang, Xi Duan