

2018 IEEE International Conference on Intelligence and Security Informatics (ISI 2018)

**Miami, Florida, USA
8 – 10 November 2018**



**IEEE Catalog Number: CFP18ITI-POD
ISBN: 978-1-5386-7849-7**

**Copyright © 2018 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:	CFP18ITI-POD
ISBN (Print-On-Demand):	978-1-5386-7849-7
ISBN (Online):	978-1-5386-7848-0

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

CURRAN ASSOCIATES INC.
proceedings
.com

TECHNICAL PAPERS

Day 1 - November 8, 2018

Threat Intelligence

Using Entropy and Mutual Information to Extract Threat Actions from Cyber Threat Intelligence	1
<i>Ghaith Husari, Xi Niu, Bill Chu, Ehab Al-Shaer</i>	

Mining Threat Intelligence about Open-Source Projects and Libraries from Code Repository Issues and Bug Reports	7
<i>Lorenzo Neil, Sudip Mittal, Anupam Joshi</i>	

Cyberattacks - I

Spatial Patterns of Offender Groups	13
<i>Mohammad A. Tayebi, Hamed Yaghoubi Shahr, Uwe Glässer, Patricia L. Brantingham</i>	

Adaptive Anomaly Detection on Network Data Streams	19
<i>Elizabeth Riddle-Workman, Marina Evangelou, Niall M. Adams</i>	

Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights	25
<i>Md Ariful Haque, Gael Kamdem De Teyou, Sachin Shetty, Bheshaj Krishnappa</i>	

DARKMENTION: A Deployed System to Predict Enterprise-Targeted External Cyberattacks	31
<i>Mohammed Almukaynizi, Ericsson Marin, Eric Nunes, Paulo Shakarian, Gerardo I. Simari, Dipsy Kapoor, Timothy Siedlecki</i>	

Cyberattacks - II

A Study of Data Fusion for Predicting Novel Activity in Enterprise Cyber-Security	37
<i>Jack Hogan, Niall M. Adams</i>	

Correlation-based Dynamics and Systemic Risk Measures in the Cryptocurrency Market	43
<i>Jiaqi Liang, Linjing Li, Daniel Zeng, Yunwei Zhao</i>	

Extracting and Evaluating Similar and Unique Cyber Attack Strategies from Intrusion Alerts	49
<i>Stephen Moskal, Shanchieh Jay Yang, Michael E. Kuhl</i>	

[Short Paper] Attacklets: Modeling High Dimensionality in Real World Cyberattacks	55
<i>Cuneyt G. Akcora, Jonathan Z. Bakdash, Yulia R. Gel, Murat Kantarcioglu, Laura R. Marusich, Bhavani Thuraisingham</i>	

Cybercrime Prediction

Leveraging Intra-Day Temporal Variations to Predict Daily Cyberattack Activity	58
<i>Gordon Werner, Shanchieh Yang, Katie Mcconky</i>	

DAbR: Dynamic Attribute-based Reputation scoring for Malicious IP Address Detection	64
<i>Arya Renjan, Karuna Pande Joshi, Sandeep Nair Narayanan, Anupam Joshi</i>	

Identifying, Collecting, and Presenting Hacker Community Data: Forums, IRC, Carding Shops, and DNMs	70
<i>Po-Yi Du, Ning Zhang, Mohammadreza Ebrahimi, Sagar Samtani, Ben Lazarine, Nolan Arnold, Rachael Dunn, Sandeep Sunwal, Guadalupe Angeles, Robert Schweitzer, Hsinchun Chen</i>	

[Short Paper] Evaluation of Crime Topic Models: Topic Coherence vs Spatial Crime Concentration	76
<i>Ritika Pandey, George O. Mohler</i>	

Day 2 - November 9, 2018

Darkweb

Analysis of Hacking Related Trade in the Darkweb	79
<i>Othmane Cherqi, Ghita Mezzour, Mounir Ghogho, Mohammed El Koutbi</i>	

Detecting Cyber Threats in Non-English Dark Net Markets: A Cross-Lingual Transfer Learning Approach	85
<i>Mohammadreza Ebrahimi, Mihai Surdeanu, Sagar Samtani, Hsinchun Chen</i>	

[Short Paper] Finding Cryptocurrency Attack Indicators using Temporal Logic and Darkweb Data	91
<i>Mohammed Almukaynizi, Vivin Paliath, Malay Shah, Malav Shah, Paulo Shakarian</i>	

IoT & Smartcities

Incremental Hacker Forum Exploit Collection and Classification for Proactive Cyber Threat Intelligence: An Exploratory Study	94
<i>Ryan Williams, Sagar Samtani, Mark Patton, Hsinchun Chen</i>	

Benchmarking Vulnerability Assessment Tools for Enhanced Cyber-Physical System (CPS) Resiliency	100
<i>Emma McMahon, Mark Patton, Sagar Samtani, Hsinchun Chen</i>	

Identifying Privacy Functional Requirements for Crowdsourcing Applications in Smart Cities	106
<i>Mônica da Silva, José Viterbo, Flavia Bernardini, Cristiano Maciel</i>	

Effect of Imbalanced Datasets on Security of Industrial IoT using Machine Learning	112
<i>Maede Zolanvari, Marcio A. Teixeira, Raj Jain</i>	

Threat Intelligence

Copresence Networks	118
<i>David Skillicorn, Christian Leuprecht</i>	

Political Bots and the Swedish General Election	124
<i>Johan Fernquist, Lisa Kaati, Ralph Schroeder</i>	

Lifting the Smokescreen: Detecting Underlying Anomalies during a DDoS Attack	130
<i>Brian Ricks, Bhavani Thuraisingham, Patrick Tague</i>	

Putting all Eggs in a Single Basket: A Cross-Community Analysis of 12 Hacking Forums	136
<i>Richard Frank, Myfanwy Thomson, Alexander Mikhaylov, Andrew Park</i>	

Vulnerability & Anomaly Detection

Measuring the Effectiveness of Network Deception	142
<i>Shridatt Sugrim, Sridhar Venkatesan, Jason A. Youzwak, Cho-Yu J. Chiang, Ritu Chadha, Massimiliano Albanese, Hasan Cam</i>	
Vulnerability Assessment, Remediation, and Automated Reporting: Case Studies of Higher Education Institutions	148
<i>Christopher R. Harrell, Mark Patton, Hsinchun Chen, Sagar Samtani</i>	
Analysing Indicator of Compromises for Ransomware: Leveraging IOCs with Machine Learning Techniques	154
<i>Mayank Verma, Ponnurangam Kumarguru, Shuva Brata Deb, Anuradha Gupta</i>	
[Short Paper] A Temporal Recurrent Neural Network Approach to Detecting Market Anomaly Attacks	160
<i>Yifan Huang, Wingyan Chung, Xinlin Tang</i>	

Day 3 - November 10, 2018

Threat Intelligence

Detecting Saturation Attacks in Software-Defined Networks	163
<i>Zhiyuan Li, Weijia Xing, Dianxiang Xu</i>	
Early Identification of Pathogenic Social Media Accounts	169
<i>Hamidreza Alvari, Elham Shaabani, Paulo Shakarian</i>	
Exploratory Data Analysis of a Network Telescope Traffic and Prediction of Port Probing Rates	175
<i>Mehdi Zakroum, Abdellah Houmz, Mounir Ghogho, Ghita Mezzour, Abdelkader Lahmadi, Jérôme François, Mohammed El Koutbi</i>	
Privacy Preserving on Trajectories Created by Wi-Fi Connections in a University Campus	181
<i>Fernanda Oliveira Gomes, Douglas Simões Silva, Bruno Machado Agostinho, Jean Everson Martina</i>	

Big Data

SPERG: Scalable Political Event Report Geoparsing in Big Data	187
<i>Aswin Krishna Gunasekaran, Maryam Bahojb Imani, Latifur Khan, Christan Grant, Patrick T. Brandt, Jennifer S. Holmes</i>	
From Public Gatherings to the Burst of Collective Violence: An Agent-based Emotion Contagion Model	193
<i>Lida Huang, Guoray Cai, Hongyong Yuan, Jianguo Chen</i>	
Security Analysis of the RaSTA Safety Protocol	199
<i>Markus Heinrich, Jannik Vieten, Tolga Arul, Stefan Katzenbeisser</i>	
Directed Digital Hate	205
<i>Björn Pelzer, Lisa Kaati, Nazar Akrami</i>	
[Short Paper] Attention-based Multi-hop Reasoning for Knowledge Graph	211
<i>Zikang Wang, Linjing Li, Daniel Dajun Zeng, Yue Chen</i>	

Text and Social Media

Joint Learning with Keyword Extraction for Event Detection in Social Media	214
<i>Guandan Chen, Wenji Mao, Qingchao Kong, Han Han</i>	

PhishMon: A Machine Learning Framework for Detecting Phishing Webpages	220
<i>Amirreza Niakanlahiji, Bei-Tseng Chu, Ehab Al-Shaer</i>	

A Broker Architecture, Push-Pull Database System for Intelligence Analysis	226
<i>Antonio Badia</i>	

A Partition and Interaction Combined Model for Social Event Popularity Prediction	232
<i>Guandan Chen, Qingchao Kong, Wenji Mao, Daniel Zeng</i>	

Final Session

Using Deep Neural Networks to Translate Multi-lingual Threat Intelligence	238
<i>Priyanka Ranade, Sudip Mittal, Anupam Joshi, Karuna Joshi</i>	

[Short Paper] Extracting Textual Features of Financial Social Media to Detect Cognitive Hacking	244
<i>Wingyan Chung, Jinwei Liu, Xinlin Tang, Vincent S.K. Lai</i>	