

2020 IEEE International Conference on Intelligence and Security Informatics (ISI 2020)

**Arlington, Virginia, USA
9 – 10 November 2020**



**IEEE Catalog Number: CFP20ITI-POD
ISBN: 978-1-7281-8801-0**

**Copyright © 2020 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:	CFP20ITI-POD
ISBN (Print-On-Demand):	978-1-7281-8801-0
ISBN (Online):	978-1-7281-8800-3

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

Table of Contents

<hr/>	
Adversarial Machine Learning	
<hr/>	
Automated Adversary Emulation for Cyber-Physical Systems via Reinforcement Learning	1
<i>Arnab Bhattacharya, Thiagarajan Ramachandran, Sandeep Banik, Chase Dowling and Shaunak Bopardikar</i>	
Detecting Cyber-Adversarial Videos in Traditional Social media	7
<i>Bingyan Du, Pranay Singhal, Victor Benjamin and Weifeng Li</i>	
Evaluating Effectiveness of Adversarial Examples on state of art License Plate Recognition Models	10
<i>Kanishk Rana and Rahul Madaan</i>	
Assessing GAN-based approaches for generative modeling of crime text reports	13
<i>Samira Khorshidi, George Mohler and Jeremy Carter</i>	
<hr/>	
COVID-19's Impact on Cybersecurity	
<hr/>	
Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses	19
<i>Mir Mehedi Ahsan Pritom, Kristin Schweitzer, Raymond Bateman, Min Xu and Shouhuai Xu</i>	
Data-Driven Characterization and Detection of COVID-19 Themed Malicious Websites	25
<i>Mir Mehedi Ahsan Pritom, Kristin Schweitzer, Raymond Bateman, Min Xu and Shouhuai Xu</i>	
Analyzing the Evolutionary Characteristics of the Cluster of COVID-19 under Anti-contagion Policies	31
<i>Pu Miao, Hu Tian, Xingwei Zhang, Saike He, Xiaolong Zheng, Daniel Zeng and Wu Desheng Dash</i>	
The Four-Stages Strategies on Social Media to Cope with "Infodemic" and Repair Public Trust: Covid-19 Disinformation and Effectiveness of Government Intervention in China	37
<i>Yonghan Zhu and Yuqiao Jiang</i>	
<hr/>	
Cyber Threat Intelligence	
<hr/>	
Malware Family Fingerprinting Through Behavioral Analysis	42
<i>Aaron Walker and Shamik Sengupta</i>	
Knowledge Enrichment by Fusing Representations for Malware Threat Intelligence and Behavior	47
<i>Aritran Piplai, Sudip Mittal, Mahmoud Abdelsalam, Maanak Gupta, Anupam Joshi and Tim Finin</i>	
Multi-Dimensional Anomalous Entity Detection via Poisson Tensor Factorization	53
<i>Maksim Eren, Juston Moore and Boian Alexandrov</i>	
Detection of Malicious Domains Using Passive DNS with XGBoost	59
<i>Marcos Rogério Silveira, Adriano Mauro Cansian and Hugo Koji Kobayashi</i>	

Cybersecurity Threat Intelligence Augmentation and Embedding Improvement - A Healthcare Usecase	62
<i>Matthew Sills, Priyanka Ranade and Sudip Mittal</i>	
Scalable Malware Clustering using Multi-Stage Tree Parallelization	68
<i>Muqheet Ali, Josiah Hagen and Jonathan Oliver</i>	
A KG-based Enhancement Framework for Fact Checking Using Category Information	74
<i>Shuai Wang, Lei Wang and Wenji Mao</i>	
XGBoosted Misuse Detection in LAN-Internal Traffic Dataset	80
<i>Zhiqing Zhang, Pawissakan Chirupphapa, Hiroshi Esaki and Hideya Ochiai</i>	
<hr/> Cybersecurity for Cyberinfrastructure <hr/>	
Identifying Vulnerable GitHub Repositories and Users in Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach	86
<i>Ben Lazarine, Sagar Samtani, Mark Patton, Hongyi Zhu, Steven Ullman, Benjamin Ampel and Hsinchun Chen</i>	
APIN: Automatic Attack Path Identification in Computer Networks	92
<i>Eric Ficke and Shouhuai Xu</i>	
Fraud Prevention Within the Brazilian Governmental Public-Key Infrastructure	98
<i>Fernanda Oliveira Gomes, Bruno Machado Agostinho and Jean Everson Martina</i>	
Adaptive and Predictive SDN Control During DDoS Attacks	104
<i>Jagannadh Vempati, Ram Dantu, Syed Badruddoja and Mark Thompson</i>	
Efficient and Secure Implementation of BLS Multisignature Scheme on TPM	110
<i>Mustapha Hedabou and Yunusa Simpa Abdulsalam</i>	
Performance Analysis of Secure Real-time Transport Protocol Using Elliptic Curves	116
<i>Nilanjan Sen, Ram Dantu and Mark Thompson</i>	
A Comparative Study on Contemporary Intrusion Detection Datasets for Machine Learning Research	123
<i>Smirti Dwibedi, Medha Pujari and Weiqing Sun</i>	
Effective Voice Fuzzing Method for Finding Vulnerabilities in AI Speech Recognition Devices	129
<i>So-Hyun Park and Il-Gu Lee</i>	
Smart Vulnerability Assessment for Scientific Cyberinfrastructure: An Unsupervised Graph Embedding Approach	135
<i>Steven Ullman, Sagar Samtani, Ben Lazarine, Hongyi Zhu, Benjamin Ampel, Mark Patton and Hsinchun Chen</i>	
Discerning User Activity in Extended Reality Through Side-Channel Accelerometer Observations	141
<i>Tiago Martins Andrade, Max Smith-Creasey and Jonathan Francis Roscoe</i>	

Dark Web Analytics

Labeling Hacker Exploits for Proactive Cyber Threat Intelligence: A Deep Transfer Learning Approach	144
<i>Benjamin Ampel, Sagar Samtani, Hongyi Zhu, Steven Ullman and Hsinchun Chen</i>	
An Expert System for Classifying Harmful Content on the Dark Web.....	150
<i>Hanae Kobayashi, Masashi Kadoguchi, Shota Hayashi, Akira Otsuka and Masaki Hashimoto</i>	
Identifying Proficient Cybercriminals Through Text and Network Analysis.....	156
<i>Jan William Johnsen and Katrin Franke</i>	
Deep Self-Supervised Clustering of the Dark Web for Cyber Threat Intelligence.....	163
<i>Masashi Kadoguchi, Hanae Kobayashi, Shota Hayashi, Akira Otsuka and Masaki Hashimoto</i>	
A Generative Adversarial Learning Framework for Breaking Text-Based CAPTCHA in the Dark Web.....	169
<i>Ning Zhang, Mohammadreza Ebrahimi, Weifeng Li and Hsinchun Chen</i>	
Improving the Data Quality for Credit Card Fraud Detection.....	175
<i>Rongrong Jing, Hu Tian, Yidi Li, Xingwei Zhang, Xiaolong Zheng, zhu zhang and Daniel Zeng</i>	
Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web.....	181
<i>Yizhi Liu, Fang Yu Lin, Zara Ahmad-Post, Mohammadreza Ebrahimi, Ning Zhang, James Lee Hu, Jingyu Xu, Weifeng Li and Hsinchun Chen</i>	
<hr/> Deep Learning Applications for Cybersecurity <hr/>	
Sentimental LIAR: Extended Corpus and Deep Learning Models for Fake Claim Classification.....	187
<i>Bibek Upadhayay and Vahid Behzadan</i>	
Political Fake Statement Detection via Multistage Feature-assisted Neural Modeling.....	193
<i>Fuad Mire Hassan and Mark Lee</i>	
DeepGuard: Deep Generative User-behavior Analytics for Ransomware Detection	199
<i>Gaddisa Olani Ganfure, Chun-Feng Wu, Yuan-Hao Chang and Wei-Kuan Shih</i>	
A virtual simulation environment using deep learning for autonomous vehicles obstacle avoidance	205
<i>Leila Haj Meftah and Rafik Braham</i>	
From Word Embedding to Cyber-Phrase Embedding: Comparison of Processing Cybersecurity Texts.....	212
<i>Moumita Das Purba, Bill Chu and Ehab Al-Shaer</i>	
Weaponizing Unicodes with Deep Learning - Identifying Homoglyphs with Weakly Labeled Data	218
<i>Perry Deng, Cooper Linsky and Matthew Wright</i>	

Phishcasting: Deep Learning for Time Series Forecasting of Phishing Attacks.....	224
<i>Syed Hasan Amin Mahmood, Syed Mustafa Ali Abbasi, Ahmed Abbasi and Fareed Zaffar</i>	
<hr/> Socio-technical Perspectives of Cybersecurity <hr/>	
Is the user identity perception influenced by the blockchain technology?	230
<i>Andreea-Elena Panait</i>	
Conceptual Models for Counter-Terrorism and Intelligence Knowledge Bases.....	233
<i>Antonio Badia</i>	
An Ordinal Approach to Modeling and Visualizing Phishing Susceptibility.....	236
<i>David G. Dobolyi, Ahmed Abbasi, F. Mariam Zahedi and Anthony Vance</i>	
A Bootstrapped Model to Detect Abuse and Intent in White Supremacist Corpora	242
<i>David Skillicorn and Benjamin Simons</i>	
A Proxy-Based Encrypted Online Social Network With Fine-Grained Access.....	248
<i>Fabian Schillinger and Christian Schindelbauer</i>	
A Survey of Real-Time Social-Based Traffic Detection.....	253
<i>Hashim Abu-Gellban</i>	
Twitter Bot Detection with Reduced Feature Set	259
<i>Jefferson Abreu, Célia Ralha and João Gondim</i>	
Towards a Story Scheme Ontology of Terrorist MOs	265
<i>Joeri Peters and Floris Bex</i>	
A Human-Network-Security-Interface for an Average Joe	271
<i>Rajasekhar Ganduri, Ram Dantu, Mark Thompson, Samuel Evans and Logan Widick</i>	
Heuristic Phishing Detection and URL Checking Methodology Based on Scraping and Web Crawling.....	277
<i>Rômulo Almeida and Carla Westphall</i>	
Social Emotion Cause Extraction from Online Texts.....	283
<i>Xinglin Xiao, Lei Wang, Qingchao Kong and Wenji Mao</i>	