2018 IEEE Security and Privacy Workshops (SPW 2018)

San Francisco, California, USA 24 May 2018



IEEE Catalog Number: ISBN: CFP18SPX-POD 978-1-5386-8277-7

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:	CFP18SPX-POD
ISBN (Print-On-Demand):	978-1-5386-8277-7
ISBN (Online):	978-1-5386-8276-0

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



2018 IEEE Symposium on Security and Privacy Workshops SPW 2018

Table of Contents

Message from the Workshops General Chair x
Message from the DLS Organizers .xi
DLS Committees xii
Message from the SADFE Organizers xiii
SADFE Committees .xiv.
Message from the WRIT Organizers xvi
WRIT Committees .xvii
Message from the BioStar Organizers xviii
BioStar Committees xix
Message from the LangSec Organizers xx
LangSec Committees xxi

DLS: Deep Learning and Security Workshop

Audio Adversarial Examples: Targeted Attacks on Speech-to-Text .1 Nicholas Carlini (University of California) and David Wagner (University of California)
A Deep Learning Approach to Fast, Format-Agnostic Detection of Malicious Web Content .8 Joshua Saxe, Richard Harang (Sophos), Cody Wild (Sophos), and Hillary Sanders (Sophos)
Mouse Authentication Without the Temporal Aspect – What Does a 2D-CNN Learn? .15 Penny Chong (ST Electronics-SUTD Cyber Security Laboratory), Yi Xiang Marcus Tan (ST Electronics-SUTD Cyber Security Laboratory), Juan Guarnizo (ST Electronics-SUTD Cyber Security Laboratory), Yuval Elovici (ST Electronics-SUTD Cyber Security Laboratory), and Alexander Binder (ST Electronics-SUTD Cyber Security Laboratory)
Detecting Homoglyph Attacks with a Siamese Neural Network .22 Jonathan Woodbridge (Endgame), Hyrum S. Anderson (Endgame), Anjum Ahuja (Endgame), and Daniel Grant (Endgame)
Machine Learning DDoS Detection for Consumer Internet of Things Devices .29 Rohan Doshi (Princeton University), Noah Apthorpe (Princeton University), and Nick Feamster (Princeton University)
Adversarial Examples for Generative Models .36. Jernej Kos (National University of Singapore), Ian Fischer (Google), and Dawn Song (University of California)
Learning Universal Adversarial Perturbations with Generative Models .43 Jamie Hayes (ac.uk) and George Danezis (UCL)

Black-Box Generation of Adversarial Text Sequences to Evade Deep Learning Classifiers .50 Ji Gao (University of Virginia), Jack Lanchantin (University of Virginia), Mary Lou Soffa (Unversity of Virginia), and Yanjun Qi (University of Virginia)
Exploring the Use of Autoencoders for Botnets Traffic Representation .5.7 Ruggiero Dargenio (MIT CSAIL), Shashank Srikant (MIT CSAIL), Erik Hemberg (MIT CSAIL), and Una-May O'Reilly (MIT CSAIL)
The Good, the Bad and the Bait: Detecting and Characterizing Clickbait on YouTube .63 Savvas Zannettou (Cyprus University of Technology), Sotirios Chatzis (Cyprus University of Technology), Kostantinos Papadamou (Cyprus University of Technology), and Michael Sirivianos (Cyprus University of Technology)
Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection .70 Maria Rigaki (Czech Technical University in Prague) and Sebastian Garcia (Czech Technical University in Prague)
Adversarial Deep Learning for Robust Detection of Binary Encoded Malware .76 Abdullah Al-Dujaili (MIT CSAIL), Alex Huang (MIT CSAIL), Erik Hemberg (MIT CSAIL), and Una-May O'Reilly (MIT CSAIL)
Extending Detection with Privileged Information via Generalized Distillation .83 Z. Berkay Celik (Pennsylvania State University) and Patrick McDaniel (Pennsylvania State University)
Detecting Deceptive Reviews Using Generative Adversarial Networks .89 Hojjat Aghakhani (University of California), Aravind Machiry (University of California), Shirin Nilizadeh (Carnegie Mellon University), Christopher Kruegel (University of California), and Giovanni Vigna (University of California)
Background Class Defense Against Adversarial Examples .96 Michael McCoyd (University of California) and David Wagner (University of California)
Time Series Deinterleaving of DNS Traffic .103 Amir Asiaee T. (Ohio State University), Hardik Goel (Microsoft Corporation), Shalini Ghosh (SRI International), Vinod Yegneswaran (SRI International), and Arindam Banerjee (University of Minnesota)
HeNet: A Deep Learning Approach on Intel® Processor Trace for Effective Exploit Detection .109 Li Chen (Intel Labs), Salmin Sultana (Intel Labs), and Ravi Sahita (Intel Labs)
Deep Reinforcement Fuzzing .116 Konstantin Böttinger (Fraunhofer Institute for Applied and Integrated Security), Patrice Godefroid (Microsoft Research), and Rishabh Singh (Microsoft Research)
Security Risks in Deep Learning Implementations .123 Qixue Xiao (Qihoo 360 Security Research Labs), Kang Li (University of Georgia), Deyue Zhang (Qihoo 360 Security Research Labs), and Weilin Xu (University of Virginia)

SADFE: Systematic Approaches to Digital Forensic Engineering

Evaluating Automated Facial Age Estimation Techniques for Digital Forensics .129 Felix Anda (University College Dublin), David Lillis (University College Dublin), Nhien-An Le-Khac (University College Dublin), and Mark Scanlon (University College Dublin)
 File Fragment Classification Using Grayscale Image Conversion and Deep Learning in Digital Forensics.140 Qian Chen (Harbin Institute of Technology, Shenzhen), Qing Liao (Harbin Institute of Technology, Shenzhen), Zoe L. Jiang (Harbin Institute of Technology, Shenzhen), Junbin Fang (Guangdong Provincial Engineering Technology Research Center on VLC), Siuming Yiu (The University of Hong Kong), Guikai Xi (Guangdong Provincial Engineering Technology Research Center on VLC), Rong Li (Guangdong Provincial Engineering Technology Research Center on VLC), Zhengzhong Yi (Harbin Institute of Technology, Shenzhen), Xuan Wang (Harbin Institute of Technology, Shenzhen), Lucas C.K. Hui (Hong Kong Applied Science and Technology Research Institute), Dong Liu (Henan Normal University, Xinxiang), and En Zhang (Henan Normal University, Xinxiang)
Forensic-Aware Anti-DDoS Device .148. <i>Chi Yuen Tseung (The University of Hong Kong) and Kam Pui Chow (The</i> <i>University of Hong Kong)</i>
A Dynamic Taint Analysis Tool for Android App Forensics .160 Zhen Xu (Iowa State University), Chen Shi (Iowa State University), Chris Chao-Chun Cheng (Iowa State University), Neil Zhengqiang Gong (Iowa State University), and Yong Guan (Iowa State University)
Fingerprinting Cryptographic Protocols with Key Exchange Using an Entropy Measure .170 Shoufu Luo (City University of New York), Jeremy D. Seideman (City University of New York), and Sven Dietrich (City University of New York)
Forensic Analysis of Ransomware Families Using Static and Dynamic Analysis .180 Kul Prasad Subedi (University of Memphis), Daya Ram Budhathoki (University of Memphis), and Dipankar Dasgupta (University of Memphis)
Forensic Analysis of Immersive Virtual Reality Social Applications: A Primary Account .186 Ananya Yarramreddy (University of New Haven), Peter Gromkowski (University of New Haven), and Ibrahim Baggili (University of New Haven)

WRIT: Workshop on Research for Insider Threat

SOFIT: Sociotechnical and Organizational Factors for Insider Threat .197.....
Frank Greitzer (PsyberAnalytix), Justin Purl (Human Resources Research Organization), Yung Mei Leong (Independent Consultant), and D.E. (Sunny) Becker (Human Resources Research Organization)
Insider Threat Cybersecurity Framework Webtool & Methodology: Defending Against Complex
Cyber-Physical Threats .207.....
Michael Mylrea (Pacific Northwest National Laboratory), Sri Nikhil
Gupta Gourisetti (Pacific Northwest National Laboratory), Curtis
Larimer (Pacific Northwest National Laboratory), and Christine Noonan (Pacific Northwest National Laboratory)

Detection of Masqueraders Based on Graph Partitioning of File System Access Events .2.17 Flavio Toffalini (Singapore University of Technology and Design), Ivan Homoliak (Singapore University of Technology and Design), Athul Harilal (Singapore University of Technology and Design), Alexander Binder (Singapore University of Technology and Design), and Martin Ochoa (Universidad del Rosario)
Simulated User Bots: Real Time Testing of Insider Threat Detection Systems .228 Preetam Dutta (Columbia University), Gabriel Ryan (Columbia University), Aleksander Zieba (Columbia University), and Salvatore Stolfo (Columbia University)
 Balancing Organizational Incentives to Counter Insider Threat .237 Andrew P. Moore (Software Engineering Institute), Tracy M. Cassidy (Software Engineering Institute), Michael C. Theis (Software Engineering Institute), Daniel Bauer (Software Engineering Institute), Denise M. Rousseau (Carnegie Mellon University), and Susan B. Moore (Life Dimensions Coaching and Counseling)
Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump Start an Insider Threat Program .247 Derrick Spooner (Software Engineering Institute), George Silowash (Norwich University), Daniel Costa (Software Engineering Institute),

and Michael Albrethsen (Software Engineering Institute)

BioStar: Workshop on Bio-inspired Security, Trust, Assurance and Resilience

S.P.O.O.F Net: Syntactic Patterns for identification of Ominous Online Factors 258 Vysakh S Mohan (Amrita School of Engineering, Coimbatore), Vinayakumar R (Amrita School of Engineering, Coimbatore), Soman KP (Amrita School of Engineering, Coimbatore), and Prabaharan Poornachandran (Amrita School of Engineering, Amritapuri)
 WACA: Wearable-Assisted Continuous Authentication .264. Abbas Acar (Florida International University), Hidayet Aksu (Florida International University), A. Selcuk Uluagac (Florida International University), and Kemal Akkaya (Florida International University)
Evaluating Insider Threat Detection Workflow Using Supervised and Unsupervised Learning .270 Duc C. Le (Dalhousie University) and A. Nur Zincir-Heywood (Dalhousie University)
Towards Human Bio-Inspired Defence Mechanism for Cyber Security .2.76 Nanda Kumar Thanigaivelan (University of Turku), Ethiopia Nigussie (University of Turku), Seppo Virtanen (University of Turku), and Jouni Isoaho (University of Turku)
A Case Study in Tailoring a Bio-Inspired Cyber-Security Algorithm: Designing Anomaly Detection for Multilayer Networks .281 Gonzalo Suárez (Rutgers University), Lazaros Gallos (Rutgers University), and Nina Fefferman (University of Tennessee)

Diversity-Based Moving-Target Defense for Secure Wireless Vehicular Communications .287
Esraa M. Ghourab (Alexandria University, Egypt), Effat Samir
(Alexandria University, Egypt), Mohamed Azab (Informatics Research
Institute), and Mohamed Eltoweissy (Virginia Military Institute)

Biologically Inspired Safety and Security for Smart Built Environments: Position Paper .293..... Denis Gracanin (Virginia Tech), Adam D'Amico (Virginia Tech), Mark Manuel (Virginia Tech), Walter Carson (Virginia Tech), Mohamed Eltoweissy (Virginia Military Institute), and Liang Cheng (Lehigh University)

LangSec: Workshop on Language-theoretic Security and Applications

Redesigning Secure Protocols to Compel Grammatical Compliance Checking .299 Keith Irwin (Winston-Salem State University)
A Binary Analysis Approach to Retrofit Security in Input Parsing Routines .306 Jayakrishna Menon (University of Southern California), Christophe Hauser (University of Southern California), Yan Shoshitaishvili (Arizona State University), and Stephen Schwab (University of Southern California)
A Mathematical Modeling of Exploitations and Mitigation Techniques Using Set Theory .323 Rodrigo Branco (Intel Corp), Kekai Hu (Intel Corp), Henrique Kawakami (Intel Corp), and Ke Sun (Intel Corp)
LangSec Revisited: Input Security Flaws of the Second Kind .329 Erik Poll (Radboud University, Nijmegen)

Author Index 335