

2020 IEEE Conference on Communications and Network Security (CNS 2020)

**Avignon, France
29 June – 1 July 2020**



**IEEE Catalog Number: CFP20CNM-POD
ISBN: 978-1-7281-4761-1**

**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:	CFP20CNM-POD
ISBN (Print-On-Demand):	978-1-7281-4761-1
ISBN (Online):	978-1-7281-4760-4

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

SYMBION: INTERLEAVING SYMBOLIC WITH CONCRETE EXECUTION.....	1
<i>Fabio Gritti, Lorenzo Fontana, Eric Gustafson, Fabio Pagani, Andrea Continella, Christopher Kruegel, Giovanni Vigna</i>	
ATTACKS ON DYNAMIC PROTOCOL DETECTION OF OPEN SOURCE NETWORK SECURITY MONITORING TOOLS	11
<i>Jan Grashöfer, Christian Titze, Hannes Hartenstein</i>	
WHEN THE NETWORK OF A SMART CITY IS NOT SO SMART	20
<i>Ali Tabaja, Reuven Cohen</i>	
TRUST.IO: PROTECTING PHYSICAL INTERFACES ON CYBER-PHYSICAL SYSTEMS	29
<i>Chad Spensky, Aravind Machiry, Marcel Busch, Kevin Leach, Rick Housley, Christopher Kruegel, Giovanni Vigna</i>	
A RULE REORDERING METHOD VIA PAIRING DEPENDENT RULES	38
<i>Takashi Harada, Ken Tanaka, Ryohei Ogasawara, Kenji Mikawa</i>	
EVOLVING ADVANCED PERSISTENT THREAT DETECTION USING PROVENANCE GRAPH AND METRIC LEARNING.....	47
<i>Gbadebo Ayoade, Khandakar Ashrafi Akbar, Pracheta Sahoo, Yang Gao, Anmol Agarwal, Kangkook Jee, Latifur Khan, Anoop Singhal</i>	
EXPLORING ABSTRACTION FUNCTIONS IN FUZZING	56
<i>Christopher Salls, Aravind Machiry, Adam Doupe, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna</i>	
OTDA: A UNSUPERVISED OPTIMAL TRANSPORT FRAMEWORK WITH DISCRIMINANT ANALYSIS FOR KEYSTROKE INFERENCE	65
<i>Kun Jin, Chaoyue Liu, Cathy Xia</i>	
FAST AND SECURE KNN QUERY PROCESSING IN CLOUD COMPUTING	74
<i>Xinyu Lei, Guan-Hua Tu, Alex X. Liu, Tian Xie</i>	
QUERY-CRAFTING DOS THREATS AGAINST INTERNET DNS	83
<i>Sang-Yoon Chang, Younghee Park, Nikhil Vijayakumar Kengalahalli, Xiaobo Zhou</i>	
MAILTO: ME YOUR SECRETS: ON BUGS AND FEATURES IN EMAIL END-TO-END ENCRYPTION.....	92
<i>Jens Müller, Marcus Brinkmann, Damian Poddebniak, Sebastian Schinzel, Jörg Schwenk</i>	
SECUREAIS - SECURING PAIRWISE VESSELS COMMUNICATIONS.....	101
<i>Ahmed Aziz, Pietro Tedeschi, Savio Sciancalepore, Roberto Di Pietro</i>	
ORDER-OPTIMAL SCALING OF COVERT COMMUNICATION OVER MIMO AWGN CHANNELS.....	110
<i>Ahmed Bendary, C. Emre Koksall</i>	
TOWARDS A BELIEVABLE DECOY SYSTEM: REPLAYING NETWORK ACTIVITIES FROM REAL SYSTEM.....	119
<i>Jianhua Sun, Kun Sun, Qi Li</i>	

COMPACT AND RESILIENT CRYPTOGRAPHIC TOOLS FOR DIGITAL FORENSICS	128
<i>Efe U. A. Seyitoglu, Attila A. Yavuz, Muslum Ozgur Ozmen</i>	
FORENSIC INVESTIGATION OF INDUSTRIAL CONTROL SYSTEMS USING DETERMINISTIC REPLAY	137
<i>Gregory Walkup, Sriharsha Etigowni, Dongyan Xu, Vincent Urias, Han W. Lin</i>	
A MACHINE LEARNING APPROACH TO CLASSIFY SECURITY PATCHES INTO VULNERABILITY TYPES	146
<i>Xinda Wang, Shu Wang, Kun Sun, Archer Batcheller, Sushil Jajodia</i>	
NEXTSTEP: AN EXTENSIBLE TESTBED FOR NETWORK COVERT CHANNELS	155
<i>Olga Chen, Aaron D. Jaggard, Catherine Meadows, Michael C. Shlanta</i>	
SCIBORG: SECURE CONFIGURATIONS FOR THE IOT BASED ON OPTIMIZATION AND REASONING ON GRAPHS	164
<i>Hamed Soroush, Massimiliano Albanese, Milad Asgari Mehrabadi, Ibifubara Iganibo, Marc Mosko, Jason H. Gao, David J. Fritz, Shantanu Rane, Eric Bier</i>	
A QUANTITATIVE FRAMEWORK TO MODEL RECONNAISSANCE BY STEALTHY ATTACKERS AND SUPPORT DECEPTION-BASED DEFENSES	174
<i>Luan Huy Pham, Massimiliano Albanese, Ritu Chadha, Cho-Yu J. Chiang, Sridhar Venkatesan, Charles Kamhoua, Nandi Leslie</i>	
TOWARDS DATA-DRIVEN CHARACTERIZATION OF BRUTE-FORCE ATTACKERS	183
<i>Florian Wilkens, Mathias Fischer</i>	
CATCHING FALLING DOMINOES: CLOUD MANAGEMENT-LEVEL PROVENANCE ANALYSIS WITH APPLICATION TO OPENSTACK	192
<i>Azadeh Tabiban, Yosr Jarraya, Mengyuan Zhang, Makan Pourzandi, Lingyu Wang, Mourad Debbabi</i>	
CUMULATIVE MESSAGE AUTHENTICATION CODES FOR RESOURCE-CONSTRAINED NETWORKS	201
<i>He Li, Vireshwar Kumar, Jung-Min Jerry Park, Yaling Yang</i>	
SWEET: SECURE WIRELESS ENERGY TRANSFER WITH ELECTRIC VEHICLES IN VEHICULAR ENERGY NETWORKS	210
<i>Yuntao Wang, Zhou Su, Ning Zhang, Abderrahim Benslimane</i>	
EARS: ENABLING PRIVATE FEEDBACK UPDATES IN ANONYMOUS REPUTATION SYSTEMS	219
<i>Vishnu Teja Kilari, Ruozhou Yu, Satyajayant Misra, Guoliang Xue</i>	
EXPLORING ADVERSARIAL PROPERTIES OF INSIDER THREAT DETECTION	228
<i>Duc C. Le, Nur Zincir-Heywood</i>	
DEEPBLOC: A FRAMEWORK FOR SECURING CPS THROUGH DEEP REINFORCEMENT LEARNING ON STOCHASTIC GAMES	237
<i>Alireza Tahsini, Noah Dunstatter, Mina Guirguis, Chuadhry Mujeeb Ahmed</i>	
A MACHINE LEARNING-BASED APPROACH FOR AUTOMATED VULNERABILITY REMEDATION ANALYSIS	246
<i>Fengli Zhang, Philip Huff, Kylie McClanahan, Qinghua Li</i>	

HYBRID ANALYSIS OF ANDROID APPS FOR SECURITY VETTING USING DEEP LEARNING.....	255
<i>Dewan Chaulagain, Prabesh Poudel, Prabesh Pathak, Sankardas Roy, Doina Caragea, Guojun Liu, Xinming Ou</i>	
RUMBA-MOUSE: RAPID USER MOUSE-BEHAVIOR AUTHENTICATION USING A CNN-RNN APPROACH.....	264
<i>Shen Fu, Dong Qin, Daji Qiao, George T Amariuca</i>	
AUGMENTED RANDOMNESS FOR SECURE KEY AGREEMENT USING PHYSIOLOGICAL SIGNALS	273
<i>Beste Seymen, Duygu Karaoglan Altop, Albert Levi</i>	
PRIVACY PROTECTION AND EFFICIENT INCUMBENT DETECTION IN SPECTRUM SHARING BASED ON FEDERATED LEARNING	282
<i>Ning Wang, Junqing Le, Weiwei Li, Long Jiao, Zhihao Li, Kai Zeng</i>	
LEARNING THE ASSOCIATIONS OF MITRE ATT&CK ADVERSARIAL TECHNIQUES.....	291
<i>Rawan Al-Shaer, Jonathan M. Spring, Eliana Christou</i>	
PHISHZIP: A NEW COMPRESSION-BASED ALGORITHM FOR DETECTING PHISHING WEBSITES	300
<i>Rizka Purwanto, Arindam Pal, Alan Blair, Sanjay Jha</i>	
DYNAMIC RISK-AWARE PATCH SCHEDULING.....	309
<i>Fengli Zhang, Qinghua Li</i>	
EFFICIENT PHYSICAL LAYER GROUP KEY GENERATION IN 5G WIRELESS NETWORKS.....	318
<i>Long Jiao, Pu Wang, Ning Wang, Songlin Chen, Amir Alipour-Fanid, Junqing Le, Kai Zeng</i>	
A LARGE-SCALE ANALYSIS OF CLOUD SERVICE ABUSE.....	327
<i>Naoki Fukushi, Daiki Chiba, Mitsuaki Akiyama, Masato Uchida</i>	
EAUTHENTICATION: A CHEWING-BASED AUTHENTICATION METHOD	336
<i>Mattia Carlucci, Stefano Ceconello, Mauro Conti, Piero Romare</i>	
GAME THEORETIC APPROACH FOR SECURE AND EFFICIENT HEAVY-DUTY SMART CONTRACTS	345
<i>Pinglan Liu, Wensheng Zhang</i>	
OFF IS NOT OFF: ON THE SECURITY OF PARKED VEHICLES.....	354
<i>Kyong-Tak Cho, Kang Shin, Yu Seung Kim, Byung-Ho Cha</i>	
DODGETRON: TOWARDS AUTONOMOUS CYBER DECEPTION USING DYNAMIC HYBRID ANALYSIS OF MALWARE	363
<i>Md Sajidul Islam Sajid, Jinpeng Wei, Md Rabbi Alam, Ehsan Aghaei, Ehab Al-Shaer</i>	
RAPID: ROBUST AND ADAPTIVE DETECTION OF DISTRIBUTED DENIAL-OF-SERVICE TRAFFIC FROM THE INTERNET OF THINGS.....	372
<i>Samuel Mergendahl, Jun Li</i>	
HEKA: A NOVEL INTRUSION DETECTION SYSTEM FOR ATTACKS TO PERSONAL MEDICAL DEVICES.....	381
<i>Akm Iqtidar Newaz, Amit Kumar Sikder, Leonardo Babun, A. Selcuk Uluagac</i>	

SECURE END-TO-END SENSING IN SUPPLY CHAINS	390
<i>Jan Pennekamp, Fritz Alder, Roman Matzutt, Jan Tobias Mühlberg, Frank Piessens, Klaus Wehrle</i>	
MODELLING ADVERSARIAL FLOW IN SOFTWARE-DEFINED INDUSTRIAL CONTROL NETWORKS USING A QUEUEING NETWORK MODEL	396
<i>Linivus Obiora Nweke, Stephen D. Wolthusen</i>	
MACHINE LEARNING IN ACTION: SECURING IAM API BY RISK AUTHENTICATION DECISION ENGINE.....	402
<i>Nebojsa Djosic, Bojan Nokovic, Salah Sharieh</i>	
AUTONOMOUS SPACE RESUPPLY VEHICLE SYSTEMS SECURITY DESIGN PRINCIPLE CASE STUDY	406
<i>Logan O. Mailloux, Robert F. Mills</i>	
A SECURITY REFERENCE MODEL FOR AUTONOMOUS VEHICLES IN MILITARY OPERATIONS	414
<i>Federico Mancini, Solveig Bruvoll, John Melrose, Frederick Leve, Logan Mailloux, Raphael Ernst, Kellyn Rein, Stefano Fioravanti, Diego Merani, Robert Been</i>	
FINGERPRINTING VOICE APPLICATIONS ON SMART SPEAKERS OVER ENCRYPTED TRAFFIC	422
<i>Shriti Naraparaju</i>	
GENERATION OF REALISTIC SIGNAL STRENGTH MEASUREMENTS FOR A 5G ROGUE BASE STATION ATTACK SCENARIO.....	424
<i>Mohammad Saedi, Adrian Moore, Philip Perry, Mohammad Shojafar, Hanif Ullah, Jonathan Synnott, Ruth Brown, Ian Herwono</i>	
ETAREE: AN EFFECTIVE TREND-AWARE REPUTATION EVALUATION ENGINE FOR WIRELESS MEDICAL SENSOR NETWORKS	431
<i>Muhammad Shadi Hajar, M. Omar Al-Kadri, Harsha Kalutarage</i>	
ADAPTIVE LATENCY REDUCTION IN LORA FOR MISSION CRITICAL COMMUNICATIONS IN MINES	440
<i>Ahasanun Nessa, Fatima Hussain, Xavier Fernando</i>	
ON THE FEASIBILITY OF EXPLOITING TRAFFIC COLLISION AVOIDANCE SYSTEM VULNERABILITIES.....	447
<i>Paul M. Berges, Basavesh Ammanaghatta Shivakumar, Timothy Graziano, Ryan Gerdes, Z. Berkay Celik</i>	
ARBITRARILY VARYING WIRETAP CHANNELS WITH AND WITHOUT NON-CAUSAL SIDE INFORMATION AT THE JAMMER.....	453
<i>Carsten Rudolf Janda, Eduard A. Jorswieck, Moritz Wiese, Holger Boche</i>	
PHYSICAL LAYER AUTHENTICATION TECHNIQUES BASED ON MACHINE LEARNING WITH DATA COMPRESSION.....	459
<i>Linda Senigagliesi, Marco Baldi, Ennio Gambi</i>	
SECURE STRONG COORDINATION	465
<i>Giulia Cervia, Germán Bassi, Mikael Skoglund</i>	
REDIREKT: EXTRACTING MALICIOUS REDIRECTIONS FROM EXPLOIT KIT TRAFFIC	471
<i>Jonah Burgess, Domhnall Carlin, Philip O’Kane, Sakir Sezer</i>	

PERTURBING INPUTS TO PREVENT MODEL STEALING	480
<i>Justin Grana</i>	
OPTIMAL MECHANISMS UNDER MAXIMAL LEAKAGE.....	489
<i>Benjamin Wu, Aaron B. Wagner, G. Edward Suh</i>	
MODELING TEMPERATURE BEHAVIOR IN THE HELPER DATA FOR SECRET-KEY BINDING WITH SRAM PUFs	495
<i>Lieneke Kusters, Alexandros Rikos, Frans M. J. Willems</i>	
STEALTHY PRIVACY ATTACKS AGAINST MOBILE AR APPS	501
<i>Sarah M. Lehman, Abrar S. Alrumayh, Haibin Ling, Chiu C. Tan</i>	
ADVERSARIAL MULTIPLE ACCESS CHANNELS AND A NEW MODEL OF MULTIMEDIA FINGERPRINTING CODING.....	506
<i>Grigory Kabatiansky, Elena Egorova</i>	
NOTES ON COMMUNICATION AND COMPUTATION IN SECURE DISTRIBUTED MATRIX MULTIPLICATION.....	511
<i>Rafael G. L. D'Oliveira, Salim El Rouayheb, Daniel Heinlein, David Karpuk</i>	
AUTHENTICATION AND PARTIAL MESSAGE CORRECTION OVER ADVERSARIAL MULTIPLE-ACCESS CHANNELS.....	517
<i>Allison Beemer, Eric Graves, Joerg Kliewer, Oliver Kosut, Paul Yu</i>	
QUANTITATIVE VERIFICATION OF CERTIFICATE TRANSPARENCY GOSSIP PROTOCOLS.....	523
<i>Michael Oxford, David Parker, Mark Ryan</i>	
SECURITY VULNERABILITIES OF SERVER-CENTRIC WIRELESS DATACENTERS.....	532
<i>Sayed Ashraf Mamun, Amlan Ganguly, Panos P. Markopoulos, Andres Kwasinski, Minseok Kwon</i>	
THE QUEST FOR SECURE AND PRIVACY-PRESERVING CLOUD-BASED INDUSTRIAL COOPERATION.....	541
<i>Martin Henze</i>	
CLOUD-BASED FACE AND SPEECH RECOGNITION FOR ACCESS CONTROL APPLICATIONS.....	546
<i>Nathalie Tkauc, Thao Tran, Kevin Hernandez-Diaz, Fernando Alonso-Fernandez</i>	
SPARSEIDS: LEARNING PACKET SAMPLING WITH REINFORCEMENT LEARNING	554
<i>Maximilian Bachl, Fares Meghdouri, Joachim Fabini, Tanja Zseby</i>	
MAXIMAL α -LEAKAGE AND ITS PROPERTIES	563
<i>Jiachun Liao, Lalitha Sankar, Oliver Kosut, Flavio P. Calmon</i>	
INSIDER ATTACK DETECTION FOR SCIENCE DMZS USING SYSTEM PERFORMANCE DATA.....	569
<i>Ross Gegan, Brian Perry, Dipak Ghosal, Matt Bishop</i>	
ENCRYPTED-INPUT PROGRAM OBFUSCATION: SIMULTANEOUS SECURITY AGAINST WHITE-BOX AND BLACK-BOX ATTACKS	578
<i>Giovanni Di Crescenzo, Lisa Bahler, Allen McIntosh</i>	
PLATOON HANDOVER AUTHENTICATION IN 5G-V2X : IEEE CNS 20 POSTER.....	587
<i>Guanjie Li, Chengzhe Lai</i>	

AUTOMATED POST-BREACH PENETRATION TESTING THROUGH REINFORCEMENT LEARNING.....	589
<i>Sujita Chaudhary, Austin O'Brien, Shengjie Xu</i>	
WEBSITE CRYPTOJACKING DETECTION USING MACHINE LEARNING : IEEE CNS 20 POSTER	591
<i>Venkata Sai Krishna Avinash Nukala</i>	
IDENTIFYING P2P COMMUNITIES IN NETWORK TRAFFIC USING MEASURES OF COMMUNITY CONNECTIONS : IEEE CNS 20 POSTER.....	593
<i>Harshvardhan P. Joshi, Rudra Dutta</i>	
CYBER SECURITY DECISION MAKING INFORMED BY CYBER THREAT INTELLIGENCE (CYDETI) : IEEE CNS 20 POSTER	595
<i>Aliyu Aliyu, Ying He, Iryna Yevseyeva, Cunjin Luo</i>	
MEMBERSHIP INFERENCE ATTACKS AGAINST MEMGUARD : IEEE CNS 20 POSTER.....	597
<i>Ben Niu, Yahong Chen, Likun Zhang, Fenghua Li</i>	

Author Index