

2021 IEEE Conference on Communications and Network Security (CNS 2021)

**Tempe, Arizona, USA
4 – 6 October 2021**



**IEEE Catalog Number: CFP21CNM-POD
ISBN: 978-1-6654-4497-2**

**Copyright © 2021 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:	CFP21CNM-POD
ISBN (Print-On-Demand):	978-1-6654-4497-2
ISBN (Online):	978-1-6654-4496-5

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

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

A MODEL OBFUSCATION APPROACH TO IOT SECURITY.....	1
<i>Yunqi Guo, Zhaowei Tan, Kaiyuan Chen, Songwu Lu, Ying Nian Wu</i>	
MITIGATING ENERGY DEPLETION ATTACKS IN IOT VIA RANDOM TIME-SLOTTED CHANNEL ACCESS.....	10
<i>Savio Sciancalepore, Pietro Tedeschi, Usman Riasat, Roberto Di Pietro</i>	
LICE: LIGHTWEIGHT CERTIFICATE ENROLLMENT FOR IOT USING APPLICATION LAYER SECURITY	19
<i>Joel Höglund, Shahid Raza</i>	
DEVICE-CENTRIC DETECTION AND MITIGATION OF DIAMETER SIGNALING ATTACKS AGAINST MOBILE CORE	29
<i>Zhaowei Tan, Boyan Ding, Zhehui Zhang, Qianru Li, Yunqi Guo, Songwu Lu</i>	
CUPS HIJACKING IN MOBILE RAN SLICING: MODELING, PROTOTYPING, AND ANALYSIS	38
<i>Rupendra Nath Mitra, Mohamed M. Kassem, Jon Larrea, Mahesh K. Marina</i>	
A GAME-THEORETIC APPROACH FOR PROBABILISTIC COOPERATIVE JAMMING STRATEGIES OVER PARALLEL WIRELESS CHANNELS	47
<i>Zhifan Xu, Melike Baykal-Gürsoy, Predrag Spasojevic</i>	
VERY PWNABLE NETWORK: CISCO ANYCONNECT SECURITY ANALYSIS.....	56
<i>Gerbert Roitburd, Matthias Ortmann, Matthias Hollick, Jiska Classen</i>	
PRIVACY, SECURITY, AND UTILITY ANALYSIS OF DIFFERENTIALLY PRIVATE CPES DATA.....	65
<i>Md Tamjid Hossain, Shahriar Badsha, Haoting Shen</i>	
HIDING THE TOPOLOGY OF AN IEEE 802.15.4 NETWORK WITH LIMITED ENERGY	74
<i>Sara Beatriz Schwarz, Dimitrios-Georgios Akestoridis, Patrick Tague, Hanan Hibshi</i>	
ON GAME-THEORETIC COMPUTATION POWER DIVERSIFICATION IN THE BITCOIN MINING NETWORK	83
<i>Suhan Jiang, Jie Wu</i>	
SPON: ENABLING RESILIENT INTER-LEDGERS PAYMENTS WITH AN INTRUSION-TOLERANT OVERLAY	92
<i>Lucian Trestioreanu, Cristina Nita-Rotaru, Aanchal Malhotra, Radu State</i>	
CONMAN: A CONNECTION MANIPULATION-BASED ATTACK AGAINST BITCOIN NETWORKING	101
<i>Wenjun Fan, Sang-Yoon Chang, Xiaobo Zhou, Shouhuai Xu</i>	
TRANSLATING INTRUSION ALERTS TO CYBERATTACK STAGES USING PSEUDO-ACTIVE TRANSFER LEARNING (PATRL).....	110
<i>Stephen Moskal, Shanchieh Jay Yang</i>	
GADOT: GAN-BASED ADVERSARIAL TRAINING FOR ROBUST DDOS ATTACK DETECTION.....	119
<i>Maged Abdelaty, Sandra Scott-Hayward, Roberto Doriguzzi-Corin, Domenico Siracusa</i>	

A HIERARCHICAL ARCHITECTURE AND PROBABILISTIC STRATEGY FOR COLLABORATIVE INTRUSION DETECTION.....	128
<i>Christoph Hardegen, Mike Petersen, Chukwuebuka Ezele, Timo Geier, Sebastian Rieger, Ulrich Buehler</i>	
DREVAN: DEEP REINFORCEMENT LEARNING-BASED VULNERABILITY-AWARE NETWORK ADAPTATIONS FOR RESILIENT NETWORKS	137
<i>Qisheng Zhang, Jin-Hee Cho, Terrence J. Moore, Frederica Free Nelson</i>	
A SYMMETRIC CIPHER RESPONSE-BASED CRYPTOGRAPHY ENGINE ACCELERATED USING GPGPU.....	146
<i>Jordan Wright, Zane Fink, Michael Gowanlock, Christopher Philabaum, Brian Donnelly, Bertrand Cambou</i>	
CONTEXT-AWARE IOT DEVICE FUNCTIONALITY EXTRACTION FROM SPECIFICATIONS FOR ENSURING CONSUMER SECURITY	155
<i>Upakar Paudel, Andy Dolan, Suryadipta Majumdar, Indrakshi Ray</i>	
AN UNEVEN GAME OF HIDE AND SEEK: HIDING BOTNET CNC BY ENCRYPTING IPS IN DNS RECORDS	164
<i>Martin Fejrskov, Jens Myrup Pedersen, Leon Böck, Emmanouil Vasilomanolakis</i>	
CHIMERA: AUTONOMOUS PLANNING AND ORCHESTRATION FOR MALWARE DECEPTION.....	173
<i>Md Mazharul Islam, Ashutosh Dutta, Md Sajidul Islam Sajid, Ehab Al-Shaer, Jinpeng Wei, Sadegh Farhang</i>	
PORTFILER: PORT-LEVEL NETWORK PROFILING FOR SELF-PROPAGATING MALWARE DETECTION	182
<i>Talha Ongun, Oliver Spohngellert, Benjamin Miller, Simona Boboila, Alina Oprea, Tina Eliassi-Rad, Jason Hiser, Alastair Nottingham, Jack Davidson, Malathi Veeraraghavan</i>	
ETHCLIPPER: A CLIPBOARD MEDDLING ATTACK ON HARDWARE WALLETS WITH ADDRESS VERIFICATION EVASION.....	191
<i>Nikolay Ivanov, Qiben Yan</i>	
IATTACKGEN: GENERATIVE SYNTHESIS OF FALSE DATA INJECTION ATTACKS IN CYBER-PHYSICAL SYSTEMS	200
<i>Md Hasan Shahriar, Alvi Ataur Khalil, Mohammad Ashiqur Rahman, Mohammad Hossein Manshaei, Dong Chen</i>	
HIVEGUARD: A NETWORK SECURITY MONITORING ARCHITECTURE FOR ZIGBEE NETWORKS.....	209
<i>Dimitrios-Georgios Akestoridis, Patrick Tague</i>	
HONEYBOG: A HYBRID WEBSHELL HONEYPOT FRAMEWORK AGAINST COMMAND INJECTION.....	218
<i>Songsong Liu, Pengbin Feng, Kun Sun</i>	
“X-PHISH: DAYS OF FUTURE PAST”: ADAPTIVE & PRIVACY PRESERVING PHISHING DETECTION.....	227
<i>Shalin Kumar Deval, Meenakshi Tripathi, Bruhadeshwar Bezawada, Indrakshi Ray</i>	
VIBE: AN IMPLICIT TWO-FACTOR AUTHENTICATION USING VIBRATION SIGNALS.....	236
<i>Eric Husa, Reza Tourani</i>	

ARTIFICIAL PACKET-PAIR DISPERSION (APPD): A BLACKBOX APPROACH TO VERIFYING THE INTEGRITY OF NFV SERVICE CHAINS	245
<i>A S M Asadujjaman, Momen Oqaily, Yosr Jarraya, Suryadipta Majumdar, Makan Pourzandi, Lingyu Wang, Mourad Debbabi</i>	
AUTOMATIC DETECTION OF ANDROID STEGANOGRAPHY APPS VIA SYMBOLIC EXECUTION AND TREE MATCHING	254
<i>Wenhao Chen, Li Lin, Jennifer Newman, Yong Guan</i>	
UNDERSTANDING AND MITIGATING PRIVACY LEAKS FROM THIRD-PARTY SMART SPEAKER APPS.....	263
<i>Abrar S. Alrumayh, Sarah M. Lehman, Chiu C. Tan</i>	
UNCONDITIONAL AUTHENTICATION FOR CONSTRAINED APPLICATIONS VIA STRONG PUFs	272
<i>Ahmed Bendary, C. Emre Koksal, Daniel Canaday, Andrew Pomerance</i>	
COMPKEY: EXPLOITING COMPUTER’S ELECTROMAGNETIC RADIATION FOR SECRET KEY GENERATION	281
<i>Fangfang Yang, Mohammad A. Islam, Fan Wu, Shaolei Ren</i>	
SECURING APIS AND CHAOS ENGINEERING	290
<i>Salah Sharieh, Alexander Ferworn</i>	
THE QUANTUM COMMUNICATIONS AND NETWORKING PROJECT AT THE INFORMATION TECHNOLOGY LABORATORY OF NIST	295
<i>Oliver Slattery, Xiao Tang, Lijun Ma, Thomas Gerrits, Anouar Rahmouni, Sumit Bhushan</i>	
EVALUATING THE EAVESDROPPER ENTROPY VIA BLOCH-MESSIAH DECOMPOSITION	301
<i>Micael A. Dias, Francisco M. Assis</i>	

Author Index