

2019 IEEE Conference on Communications and Network Security (CNS 2019)

**Washington, DC, USA
10 – 12 June 2019**



**IEEE Catalog Number: CFP19CNM-POD
ISBN: 978-1-5386-7118-4**

**Copyright © 2019 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:	CFP19CNM-POD
ISBN (Print-On-Demand):	978-1-5386-7118-4
ISBN (Online):	978-1-5386-7117-7

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

DRAKE: DISTRIBUTED RELAY-ASSISTED KEY ESTABLISHMENT	1
<i>Savio Sciancalepore ; Roberto Di Pietro</i>	
EFFICIENT AND ACCOUNTABLE OBLIVIOUS CLOUD STORAGE WITH THREE SERVERS	10
<i>Qiunao Ma ; Wensheng Zhang</i>	
LOCATION LEAKAGE FROM NETWORK ACCESS PATTERNS	19
<i>Trishita Tiwari ; Avraham Klausner ; Mikhail Andreev ; Ari Trachtenberg ; Arkady Yerukhimovich</i>	
RECOGNIZING EMAIL SPAM FROM META DATA ONLY	28
<i>Tim Krause ; Rafael Uetz ; Tim Kretschmann</i>	
BOTSIFTER: AN SDN-BASED ONLINE BOT DETECTION FRAMEWORK IN DATA CENTERS	37
<i>Zili Zha ; An Wang ; Yang Guo ; Doug Montgomery ; Songqing Chen</i>	
COLLUSIVEHIJACK: A NEW ROUTE HIJACKING ATTACK AND COUNTERMEASURES IN OPPORTUNISTIC NETWORKS	46
<i>Ala Altaweel ; Radu Stoleru ; Guofei Gu ; Arnab Kumar Maity</i>	
FILECRYPT: TRANSPARENT AND SCALABLE PROTECTION OF SENSITIVE DATA IN BROWSER-BASED CLOUD STORAGE	55
<i>Peiyi Han ; Chuanyi Liu ; Yingfei Dong ; Hezhong Pan ; Qiyang Song ; Binxing Fang</i>	
TOPOLOGY-AGNOSTIC RUNTIME DETECTION OF OSPF ROUTING ATTACKS	64
<i>Nurit Devir ; Orna Grumberg ; Shaul Markovitch ; Gabi Nakibly</i>	
SECURING TASK ALLOCATION IN MOBILE CROWD SENSING: AN INCENTIVE DESIGN APPROACH	73
<i>Mingyan Xiao ; Ming Li ; Linke Guo ; Miao Pan ; Zhu Han ; Pan Li</i>	
MANIPULATING DRONE POSITION CONTROL	82
<i>Wenxin Chen ; Yingfei Dong ; Zhenhai Duan</i>	
SHERLOCK HOLMES OF CACHE SIDE-CHANNEL ATTACKS IN INTEL'S X86 ARCHITECTURE	91
<i>Maria Mushtaq ; Ayaz Akram ; Muhammad Khurram Bhatti ; Usman Ali ; Vianney Lapotre ; Guy Gogniat</i>	
CHARACTERIZING LOCATION-BASED MOBILE TRACKING IN MOBILE AD NETWORKS	100
<i>Boyang Hu ; Qicheng Lin ; Yao Zheng ; Qiben Yan ; Matthew Troglia ; Qingyang Wang</i>	
I CAN HEAR YOUR ALEXA: VOICE COMMAND FINGERPRINTING ON SMART HOME SPEAKERS	109
<i>Sean Kennedy ; Haipeng Li ; Chenggang Wang ; Hao Liu ; Boyang Wang ; Wenhai Sun</i>	
RANDEX: MITIGATING RANGE INJECTION ATTACKS ON SEARCHABLE ENCRYPTION	118
<i>Hanyu Quan ; Hao Liu ; Boyang Wang ; Ming Li ; Yuqing Zhang</i>	
VACCINE:: OBFUSCATING ACCESS PATTERN AGAINST FILE-INJECTION ATTACKS	127
<i>Hao Liu ; Boyang Wang ; Nan Niu ; Shomir Wilson ; Xuetao Wei</i>	
DYNAMIC TRAFFIC FEATURE CAMOUFLAGING VIA GENERATIVE ADVERSARIAL NETWORKS	136
<i>Jie Li ; Lu Zhou ; Huaxin Li ; Lu Yan ; Haojin Zhu</i>	
DETECTING ADS-B SPOOFING ATTACKS USING DEEP NEURAL NETWORKS	145
<i>Xuhang Ying ; Joanna Mazer ; Giuseppe Bernieri ; Mauro Conti ; Linda Bushnell ; Radha Poovendran</i>	
ENERGY-AWARE DIGITAL SIGNATURES FOR EMBEDDED MEDICAL DEVICES	154
<i>Muslum Ozgur Ozmen ; Attila A. Yavuz ; Rouzbeh Behnia</i>	
SQL-IDENTIFIER INJECTION ATTACKS	163
<i>Cagri Cetin ; Dmitry Goldgof ; Jay Ligatti</i>	
IT'S NOT WHAT IT LOOKS LIKE: MEASURING ATTACKS AND DEFENSIVE REGISTRATIONS OF HOMOGRAPH DOMAINS	172
<i>Florian Quinkert ; Tobias Lauinger ; William Robertson ; Engin Kirda ; Thorsten Holz</i>	
DESIGN OF A ROBUST RF FINGERPRINT GENERATION AND CLASSIFICATION SCHEME FOR PRACTICAL DEVICE IDENTIFICATION	181
<i>Xinyu Zhou ; Aiqun Hu ; Guyue Li ; Linning Peng ; Yuexiu Xing ; Jiabao Yu</i>	
PRIVACY AND LINKABILITY OF MINING IN ZCASH	190
<i>Alex Biryukov ; Daniel Feher</i>	
A USABLE AUTHENTICATION SYSTEM USING WRIST-WORN PHOTOPLETHYSMOGRAPHY SENSORS ON SMARTWATCHES	196
<i>Jiacheng Shang ; Jie Wu</i>	

CAPNET: A DEFENSE AGAINST CACHE ACCOUNTING ATTACKS ON CONTENT DISTRIBUTION NETWORKS	205
<i>Ghada Almashaqbeh ; Kevin Kelley ; Allison Bishop ; Justin Cappos</i>	
CAPTURE: CYBERATTACK FORECASTING USING NON-STATIONARY FEATURES WITH TIME LAGS	214
<i>Ahmet Okutan ; Shanchieh Jay Yang ; Katie McConky ; Gordon Werner</i>	
SUPPORTING BOTH RANGE QUERIES AND FREQUENCY ESTIMATION WITH LOCAL DIFFERENTIAL PRIVACY	223
<i>Xiaolan Gu ; Ming Li ; Yang Cao ; Li Xiong</i>	
TOWARDS SECURE SLICING: USING SLICE ISOLATION TO MITIGATE DDOS ATTACKS ON 5G CORE NETWORK SLICES	232
<i>Danish Sattar ; Ashraf Matrawy</i>	
“WHAT”, “WHERE”, AND “WHY” CYBERSECURITY CONTROLS TO ENFORCE FOR OPTIMAL RISK MITIGATION	241
<i>Ashutosh Dutta ; Ehab Al-Shaer</i>	
GEE: A GRADIENT-BASED EXPLAINABLE VARIATIONAL AUTOENCODER FOR NETWORK ANOMALY DETECTION	250
<i>Quoc Phong Nguyen ; Kar Wai Lim ; Dinil Mon Divakaran ; Kian Hsiang Low ; Mun Choon Chan</i>	
WRISTUNLOCK: SECURE AND USABLE SMARTPHONE UNLOCKING WITH WRIST WEARABLES	259
<i>Lili Zhang ; Dianqi Han ; Ang Li ; Tao Li ; Yan Zhang ; Yanchao Zhang</i>	
I KNOW WHAT YOU ENTER ON GEAR VR	268
<i>Zhen Ling ; Zupai Li ; Chen Chen ; Junzhou Luo ; Wei Yu ; Xinwen Fu</i>	
BOTFLOWMON: LEARNING-BASED, CONTENT-AGNOSTIC IDENTIFICATION OF SOCIAL BOT TRAFFIC FLOWS	277
<i>Yebo Feng ; Jun Li ; Lei Jiao ; Xintao Wu</i>	
JOINT DATA AND TAG PRECODER OPTIMIZATION FOR MIMO PHYSICAL LAYER AUTHENTICATION WITH EMBEDDED FINGERPRINTING	286
<i>Batu K. Chalise ; Brian M. Sadler</i>	
SPOOFING ATTACK DETECTION IN MM-WAVE AND MASSIVE MIMO 5G COMMUNICATION	291
<i>Ning Wang ; Jie Tang ; Kai Zeng</i>	
SECURITY RISK-AWARE RESOURCE PROVISIONING SCHEME FOR CLOUD COMPUTING INFRASTRUCTURES	296
<i>Talal Halabi ; Martine Bellaiche</i>	
ROBUSTNESS ANALYSIS OF CNN-BASED MALWARE FAMILY CLASSIFICATION METHODS AGAINST VARIOUS ADVERSARIAL ATTACKS	305
<i>Seok-Hwan Choi ; Jin-Myeong Shin ; Peng Liu ; Yoon-Ho Choi</i>	
LINEAR PRECODING WITH FRIENDLY JAMMING IN OVERLOADED MU-MIMO WIRETAP NETWORKS	311
<i>Peyman Siyari ; Marwan Krunz</i>	
JAM-ME: EXPLOITING JAMMING TO ACCOMPLISH DRONE MISSION	316
<i>Roberto Di Pietro ; Gabriele Oligeri ; Pietro Tedeschi</i>	
DISTRIBUTED LEDGER FOR SPAMMERS' RESUME	323
<i>Anudeep Sai Muttavarapu ; Ram Dantu ; Mark Thompson</i>	
SER -CONSTRAINED SYMBOL-LEVEL PRECODING FOR PHYSICAL-LAYER SECURITY	332
<i>Abderrahmane Mayouche ; Danilo Spano ; Christos G. Tsinos ; Symeon Chatzinotas ; Björn Ottersten</i>	
DEEP-LEARNING-BASED NETWORK INTRUSION DETECTION FOR SCADA SYSTEMS	337
<i>Huan Yang ; Liang Cheng ; Mooi Choo Chuah</i>	
SECURE AND RELIABLE DECENTRALIZED TRUTH DISCOVERY USING BLOCKCHAIN	344
<i>Yifan Tian ; Jiawei Yuan ; Houbing Song</i>	
MACHINE LEARNING-BASED DELAY-AWARE UAV DETECTION OVER ENCRYPTED WI-FI TRAFFIC	352
<i>Amir Alipour-Fanid ; Monireh Dabaghchian ; Ning Wang ; Pu Wang ; Liang Zhao ; Kai Zeng</i>	
PRESERVING LOCATION PRIVACY IN CYBER-PHYSICAL SYSTEMS	359
<i>Ismail Butun ; Patrik Österberg ; Mikael Gidlund</i>	
USING STRUCTURAL DIVERSITY TO ENFORCE STRONG AUTHENTICATION OF MOBILES TO THE CLOUD	365
<i>Samy Kambou ; Ahmed Bouabdallah</i>	
SAFETY ANALYSIS OF AMI NETWORKS THROUGH SMART FRAUD DETECTION	374
<i>A H M Jakaria ; Mohammad Ashiqur Rahman ; Md Golam Moula Mehedi Hasan</i>	

PRIVACY-PRESERVING CONTROL OF VIDEO TRANSMISSIONS FOR DRONE-BASED INTELLIGENT TRANSPORTATION SYSTEMS	381
<i>Kemal Akkaya ; Vashish Baboolal ; Nico Saputro ; Selcuk Uluagac ; Hamid Menouar</i>	
DEANONYMIZING CRYPTOCURRENCY WITH GRAPH LEARNING: THE PROMISES AND CHALLENGES	388
<i>Anil Gaihre ; Santosh Pandey ; Hang Liu</i>	
POLYNOMIAL-BASED LIGHTWEIGHT KEY MANAGEMENT IN A PERMISSIONED BLOCKCHAIN	391
<i>Ashwag Albakri ; Lein Harn ; Mahesh Maddumala</i>	
FIGHTING FAKE NEWS PROPAGATION WITH BLOCKCHAINS	400
<i>Muhammad Saad ; Ashar Ahmad ; Aziz Mohaisen</i>	
A BLOCKCHAIN-ENABLED DECENTRALIZED TIME BANKING FOR A NEW SOCIAL VALUE SYSTEM	404
<i>Xuheng Lin ; Ronghua Xu ; Yu Chen ; J. Koji Lum</i>	
SECURE AND PRIVACY-PRESERVING WARNING MESSAGE DISSEMINATION IN CLOUD-ASSISTED INTERNET OF VEHICLES	409
<i>Qinlong Huang ; Nan Li ; Zhicheng Zhang ; Yixian Yang</i>	
FINGERPRINT EMBEDDING AUTHENTICATION WITH ARTIFICIAL NOISE: MISO REGIME	417
<i>Jake Bailey Perazzone ; Paul L. Yu ; Brian M. Sadler ; Rick S. Blum</i>	
GPU ALGORITHMS FOR K-ANONYMITY IN MICRODATA	422
<i>Roberto Di Pietro ; Leonardo Jero ; Flavio Lombardi ; Agustí Solanas</i>	
ENABLING SECURE AND PRIVACY PRESERVING IDENTITY MANAGEMENT VIA SMART CONTRACT	431
<i>Yaoqing Liu ; Guchuan Sun ; Stephanie Schuckers</i>	
SECURE WIRELESS COMMUNICATION USING SUPPORT VECTOR MACHINES	439
<i>Tiep M. Hoang ; Trung Q. Duong ; Sangarapillai Lambotharan</i>	
SECURE DELEGATION TO A SINGLE MALICIOUS SERVER: EXPONENTIATION IN RSA-TYPE GROUPS	444
<i>Giovanni Di Crescenzo ; Matluba Khodjaeva ; Delaram Kahrobaei ; Vladimir Shpilrain</i>	
A FRAMEWORK ARCHITECTURE FOR AGENTLESS CLOUD ENDPOINT SECURITY MONITORING	453
<i>Asem Ghaleb ; Issa Traore ; Karim Ganame</i>	
AUTHENTICATION AGAINST A MYOPIC ADVERSARY	462
<i>Allison Beemer ; Oliver Kosut ; Joerg Kliewer ; Eric Graves ; Paul Yu</i>	
SECRET KEY AND PRIVATE KEY CAPACITIES OVER AN UNAUTHENTICATED PUBLIC CHANNEL	467
<i>Wenwen Tu ; Lifeng Lai</i>	
Author Index	