2019 17th International Conference on Privacy, Security and Trust (PST 2019)

Fredericton, New Brunswick, Canada
26 – 28 August 2019

IEEE Catalog Number: CFP1904F-POD
ISBN: 978-1-7281-3266-2

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:	CFP1904F-POD
ISBN (Print-On-Demand):	978-1-7281-3266-2
ISBN (Online):	978-1-7281-3265-5
ISSN:	2574-139X

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

Table of Contents

Geographic Hints for Passphrase Authentication 1
Alaadin Addas, Julie Thorpe, and Amirali Salehi-Abari

Compromising Speech Privacy under Continuous Masking in Personal Spaces 10
S Abhishek Anand, Payton Walker, and Nitesh Saxena

Competitive Selfish Mining 20
Hamid Azimy and Ali Ghorbani

RZcash: A Privacy Protection Scheme for the Account-Based Blockchain 28
Xue Bai, Licheng Wang, Lijing Zhou, Sijia Yang, and Lixiang Li

Security and Privacy Functionalities in IoT 37
Elahe Fazeldehkordi, Olaf Owe, and Josef Noll

Prying into Private Spaces using Mobile Device Motion Sensors 49
Zakery Fyke, Isaac Griswold-Steiner, and Abdul Serwadda

Hardware-Assisted Remote Runtime Attestation for Critical Embedded Systems 59
Munir Geden and Kasper Rasmussen

Onboarding and Software Update Architecture for IoT Devices 69
Hemant Gupta and Paul C. van Oorschot

A Blockchain-Based Loan Over-Prevention Mechanism 80
Xiaoya Hu, Licheng Wang, Lijing Zhou, Lixiang Li, and Sijia Yang

A New Multisignature Scheme with Public Key Aggregation for Blockchain 89
Duc-Phong Le, Guomin Yang, and Ali Ghorbani

Victim or Attacker? A Multi-Dataset Domain Classification of Phishing Attacks 96
Sophie Le Page and Guy-Vincent Jourdan

SplitSecond: Flexible Privilege Separation of Android Apps 106
Jehyun Lee, Akshaya Venkateswara Raja, and Debin Gao

Achieving Privacy-Preserving Edit Distance Query in Cloud and Its Application to Genomic Data 116
Jason Chang and Rongxing Lu

Privacy-Preserving Tax-Case Processing 125
Espen Kjellstadli Lund, Mariusz Nowostawski, Abylay Satybaldy and Nader Aeinehchi

Extensive Examination of XOR Arbiter PUFs as Security Primitives for Resource-Constrained IoT Devices 135
Khalid T. Mursi, Yu Zhuang, Mohammed Saeed Alkatheiri, and Ahmad O. Aseeri

End-Users and Service Providers: Trust and Distributed Responsibility for Account Security 144
Yomna Abdelaziz, Daniela Napoli, and Sonia Chiasson

Brain Hemorrhage: When Brainwaves Leak Sensitive Medical Conditions and Personal Information 150
Ajaya Neupane, Kiavash Satvat, Mahshid Hosseini, and Nitesh Saxena

Stethoscope: Crypto Phones with Transparent & Robust Fingerprint Comparisons using Inter Text-Speech Transformations 160
Maliheh Shirvanian and Nitesh Saxena

ZEMFA: Zero-Effort Multi-Factor Authentication Based on Multi-Modal Gait Biometrics..................... 170
Babins Shrestha, Manar Mohamed, and Nitesh Saxena

"*It's a Generally Exhausting Field*" A Large-Scale Study of Security Incident Management Workflows and Pain Points 180
Jessica Staddon and Noelle Easterday

A Framework for Evaluating Image Obfuscation under Deep Learning-Assisted Privacy Attacks 192
Jimmy Tekli, Bechara Al Bouna, Raphaël Couturier, Gilbert Tekli, Zeinab Al Zein, and Marc Kamradt

Forward Secure and Fine-Grained Data Sharing for Mobile Crowdsensing 202
Liang Xue, Jianbing Ni, Cheng Huang, Xiaodong Lin, and Xuemin (Sherman) Shen

Ari: *A P2P Optimization for Blockchain Systems* 211
Xin Yang and Lei Shi

Geographical Security Questions for Fallback Authentication 217
Alaadin Addas, Amirali Salehi-Abari, and Julie Thorpe

Semantic Modeling Approach for Software Vulnerabilities Data Sources 223
Sultan S. Alqahtani and Juergen Rilling

Analysis, Implications, and Challenges of an Evolving Consumer IoT Security Landscape................ 230
Christopher Bellman and Paul C. van Oorschot

A Fair Anonymous Auction Scheme Utilizing Trusted Hardware and Blockchain 237
Batnyam Enkhtaivan, Takao Takenouchi, and Kazue Sako

EVChain: A Blockchain-Based Credit Sharing in Electric Vehicles Charging 242
Mahdi Daghmehchi Firoozjaei, Ali Ghorbani, Hyoungshick Kim, and Jaeseung Song

Enhancing Security and Privacy of Next-Generation Edge Computing Technologies 247
Matthew Hagan, Fahad Siddiqui, and Sakir Sezer

A Novel Permutational Sampling Technique for Cooperative Network Scanning 252
Jafar Haadi Jafarian and Kuntal Das

GlassMasq: Adversarial Examples Masquerading in Face Identification Systems with Feature Extractor 258
Kazuya Kakizaki, Kosuke Yoshida, and Tsubasa Takahashi

On the Null Relationship between Personality Types and Passwords.. 265
Amit Maraj, Miguel Vargas Martin, Matthew Shane, and Mohammad Mannan

Machine Learning Model for Smart Contracts Security Analysis 272
Pouyan Momeni, Yu Wang, and Reza Samavi

Exploring Automation in Proofs of Attribute-Based Encryption in the Standard Model 278
Guruprasad Eswaraiah, Lalitha Muthu Subramanian, and Roopa Vishwanathan

Rebalancing in Acyclic Payment Networks 283
Lalitha Muthu Subramanian, Guruprasad Eswaraiah, and Roopa Vishwanathan

Model Checking the IKEv2 Protocol using Spin 288
Tristan Ninet, Axel Legay, Romaric Maillard, Louis-Marie Traonouez, and Olivier Zendra

Privacy in the Internet of Things: A Study to Protect User's Data in LPR Systems using Blockchain 295
Iago Ochôa, Leonardo Calbusch, Karize Viecelli, Juan De Paz, Valderi Leithardt,, and Cesar Zeferino

On Embedding Backdoor in Malware Detectors using Machine Learning 300
Shoichiro Sasaki, Seira Hidano, Toshihiro Uchibayashi, Takuo Suganuma, Masahiro Hiji, and Shinsaku Kiyomoto

Time Synchronization Attack Scenarios and Analysis of Effective Self-Detection Parameters in a Distributed Industrial Wireless Sensor Network 305
Meriem Smache, Alexis Olivereau, Thibault Franco-Rondisson, and Assia Tria

Website Identity Notification: Testing the Simplest Thing That Could Possibly Work 310
Milica Stojmenović, Eric Spero, Temitayo Oyelowo, and Robert Biddle

Privacy-Preserving Multi-Party Conditional Random Selection 317
Stefan Wüller, Benjamin Assadsolimani, Ulrike Meyer, Fabian Förg, and Susanne Wetzel

Detecting Exploit Websites using Browser-Based Predictive Analytics 324
May Almousa and Mohd Anwar

Automated Extraction of Security Concerns from Bug Reports 327
Sultan S. Alqahtani

Automated Threat-Alert Screening for Battling Alert Fatigue with Temporal Isolation Forest............. 330
Muhamad Erza Aminanto, Lei Zhu, Tao Ban, Ryoichi Isawa, Takeshi Takahashi,, and Daisuke Inoue

Contemporary Sequential Network Attacks Prediction using Hidden Markov Model 333
Timothy Chadza, Konstantinos G. Kyriakopoulos, and Sangarapillai Lambotharan

User Authentication using Keystroke Dynamics via Crowdsourcing.. 336
Andrew Foresi and Reza Samavi

Evaluation Framework for Future Privacy Protection Systems: A Dynamic Identity Ecosystem Approach 339
David Liau, Razieh Nokhbeh Zaeem, and K. Suzanne Barber

Mixed Pictures: Mental Models of Malware 342
Eric Spero, Milica Stojmenović, Zahra Hassanzadeh, Sonia Chiasson, and Robert Biddle

Blockchain-Based Marketplace for Software Testing 345
Yu Wang, Reza Samavi,, and Nitin Sood