2017 15th Annual Conference on Privacy, Security and Trust (PST 2017)

Calgary, Alberta, Canada
28 – 30 August 2017

IEEE

IEEE Catalog Number:	**CFP1704F-POD**
ISBN:	**978-1-5386-2488-3**

Copyright © 2017 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:	CFP1704F-POD
ISBN (Print-On-Demand):	978-1-5386-2488-3
ISBN (Online):	978-1-5386-2487-6

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

2017 15th Annual Conference on Privacy, Security and Trust

PST 2017

Table of Contents

Preface xii
Conference Organization xiii
Steering Committee xiv
Program Committee xv
Reviewers xvii
Sponsors xviii

Keynote

Transaction Immutability and Reputation Traceability: Blockchain as a Platform for Access Controlled IoT and Human Interactivity 3
David W. Kravitz (Crypto Systems Research DarkMatter San Jose)

Blockchain and Applications

Lelantos: A Blockchain-Based Anonymous Physical Delivery System 15
Riham AlTawy (University of Waterloo), Muhammad ElSheikh (Concordia University), Amr M. Youssef (Concordia University), and Guang Gong (University of Waterloo)

Transforming Face-to-Face Identity Proofing into Anonymous Digital Identity Using the Bitcoin Blockchain 25
Daniel Augot (INRIA), Hervé Chabanne (OT-Morpho), Olivier Clémot (OT-Morpho), and William George (Laboratoire LIX)

A Nonoutsourceable Puzzle Under GHOST Rule 35
Gongxian Zeng (University of Hong Kong), Siu Ming Yiu (University of Hong Kong), Jun Zhang (University of Hong Kong), Hiroki Kuzuno (SECOM), and Man Ho Au (Hong Kong Polytechnic University)

An Identity Management System Based on Blockchain 44
Yuan Liu (Software Colledge Northeastern University), Zheng Zhao (Software Colledge Northeastern University), Guibing Guo (Software Colledge Northeastern University), Xingwei Wang (Software Colledge Northeastern University), Zhenhua Tan (Software Colledge Northeastern University), and Shuang Wang (Software Colledge Northeastern University)

The Internet of Things

OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame 57
Hyunsung Lee (Korea University Seoul), Seong Hoon Jeong (Korea University Seoul), and Huy Kang Kim (Korea University Seoul)

A Precedence Graph-Based Approach to Detect Message Injection Attacks in J1939 Based Networks 67
Subhojeet Mukherjee (Colorado State University), Jacob Walkery (Colorado State University), Indrakshi Rayz (Colorado State University), and Jeremy Daily (University of Tulsa)

Context Sensitive and Secure Parser Generation for Deep Packet Inspection of Binary Protocols 77
Ali ElShakankiry (Queen's University School of Computing) and Thomas Dean (Queen's University)

A New Segmentation Method for Integrated ICS (Short Paper) 87
Khaoula Es-Salhi (IMT Atlantique Cesson Sevigne), David Espes (University of Western Brittany Brest), and Nora Cuppens (IMT Atlantique Cesson Sevigne)

Data Privacy

SORTaki: A Framework to Integrate Sorting with Differential Private Histogramming Algorithms 95
Stylianos Doudalis (University of California - Irvine) and Sharad Mehrotra (University of California - Irvine)

Differentially Private Instance-Based Noise Mechanisms in Practice 105
Sébastien Canard (Orange Labs), Baptiste Olivier (Orange Labs), and Tony Quertier (Orange Labs)

Model Inversion Attacks for Prediction Systems: Without Knowledge of Non-Sensitive Attributes 115
Seira Hidano (KDDI Research), Takao Murakami (National Institute of Advanced Industrial Science and Technology), Shuichi Katsumata (The University of Tokyo), Shinsaku Kiyomoto (KDDI Research), and Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology)

Authentication

What Your Brain Says About Your Password: Using Brain-Computer Interfaces to Predict Password Memorability 127
Ruba Alomari (University of Ontario Institute of Technology), Miguel Vargas Martin (University of Ontario Institute of Technology), Shane MacDonald (University of Ontario Institute of Technology), Christopher Bellman (University of Ontario Institute of Technology), Ramiro Liscano (University of Ontario Institute of Technology), and Amit Maraj (University of Ontario Institute of Technology)

System-Assigned Passwords You Can't Write Down, But Don't Need To 137
Zeinab Joudaki (University of Ontario Institute of Technology), Julie Thorpe (University of Ontario Institute of Technology), and Miguel Vargas Marti (University of Ontario Institute of Technology)

Smartphone Continuous Authentication Using Deep Learning Autoencoders 147
Mario Parreño Centeno (School of Computing Science Newcastle University), Aad van Moorsel (School of Computing Science Newcastle University), and Stefano Castruccio (School of Mathematics & Statistics Newcastle University)

Best Paper Awards

No (Privacy) News is Good News: An Analysis of New York Times and Guardian Privacy News from 2010–2016 159
Karthik Sheshadri (North Carolina State University), Nirav Ajmeri (North Carolina State University), and Jessica Staddon (North Carolina State University)

RandHeap: Heap Randomization for Mitigating Heap Spray Attacks in Virtual Machines 169
Abhinav Jangda (University of Massachusetts Amherst) and Mohit Mishra (ZotOut Inc.)

Understanding Privacy

Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things 181
Meredydd Williams (University of Oxford), Jason R. C. Nurse (University of Oxford), and Sadie Creese (University of Oxford)

Cross-National Privacy Concerns on Data Collection by Government Agencies (Short Paper) 191
Rebecca Cooper (Carleton University), Hala Assal (Carleton University), and Sonia Chiasson (Carleton University)

How Much Privacy Does $3,165 Buy You? 197
Jeremy Martin (United States Naval Academy), Dane Brown (United States Naval Academy), Kris Merrion (Center for Measurement and Analysis of Network Data), Lamont Brown (United States Naval Academy), and Travis Mayberry (United States Naval Academy)

Security and Privacy in Multi-party Computation

Privacy-Preserving Multi-Party Bartering Secure Against Active Adversaries 205
Stefan Wüller (RWTH Aachen University), Ulrike Meyer (RWTH Aachen University), and Susanne Wetzel (Stevens Institute of Technology)

A Taxonomy of Secure Two-Party Comparison Protocols and Efficient Constructions 215
Nuttapong Attrapadung (National Institute of Advanced Industrial Science and Technology), Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology), Shinsaku Kiyomoto (KDDI Research Inc.), Tomoaki Mimoto (KDDI Research Inc.), and Jacob C. N. Schuldt (National Institute of Advanced Industrial Science and Technology)

Conditionally Secure Multiparty Computation using Secret Sharing Scheme for n < 2k-1 (Short Paper) .225…………………………………………………………………………………………………
Ahmad Akmal Aminuddin Mohd Kamal (Tokyo University of Science) and Keiichi Iwamura (Tokyo University of Science)

Mobile Security

Towards a Network-Based Framework for Android Malware Detection and Characterization .233……
Arash Habibi Lashkari (Canadian Institute for Cybersecurity), Andi Fitriah A.Kadir (Canadian Institute for Cybersecurity), Hugo Gonzalez (Canadian Institute for Cybersecurity), Kenneth Fon Mbah (Canadian Institute for Cybersecurity), and Ali A. Ghorbani (Canadian Institute for Cybersecurity)

Automated Static Analysis and Classification of Android Malware using Permission and API Calls Models .243…………………………………………………………………………………………………
Anastasia Skovoroda (Lomonosov Moscow State University) and Dennis Gamayunov (Lomonosov Moscow State University)

Real-Time Detection and Reaction to Activity Hijacking Attacks in Android Smartphones (Short Paper) .253…………………………………………………………………………………………………
Anis Bkakria (IMT Atlantique), Mariem Graa (IMT Atlantique), Nora Cuppens-Boulahia (IMT Atlantique), Frédéric Cuppens (IMT Atlantique), and Jean-Louis Lanet (Campus de Beaulieu)

On Return Oriented Programming Threats in Android Runtime .259…………………………………………
Akshaya Venkateswara Raja (Singapore Management University), Jehyun Lee (Singapore Management University), and Debin Gao (Singapore Management University)

How Much Privilege Does an App Need? Investigating Resource Usage of Android Apps (Short Paper) .268…………………………………………………………………………………………………
Nurul Momen (Karlstad University), Tobias Pulls (Karlstad University), Lothar Fritsch (Karlstad University), and Stefan Lindskog (Karlstad University)

Cloud Computing and Encrypted Data

Evidence-Based Trust Mechanism Using Clustering Algorithms for Distributed Storage Systems (Short Paper) .277…………………………………………………………………………………………………
Giulia Traverso (Technical University of Darmstadt), Carlos Garcia Cordero (Technical University of Darmstadt), Mehrdad Nojoumiany (Florida Atlantic University), Reza Azarderakhshy (Florida Atlantic University), Denise Demirel (Technical University of Darmstadt), Sheikh Mahbub Habib (Technical University of Darmstadt), and Johannes Buchmann (Technical University of Darmstadt)

Running Compression Algorithms in the Encrypted Domain: A Case-Study on the Homomorphic Execution of RLE .283…………………………………………………………………………………………………
Sebastien Canard (Orange Labs), Sergiu Carpov (CEA LIST), Donald Nokam Kuate (Orange Labs), and Renaud Sirdey (CEA LIST)

A Privacy-Preserving Multi-Pattern Matching Scheme for Searching Strings in Cloud Database 293
Meiqi He (University of Hong Kong), Jun Zhang (University of Hong Kong), Gongxian Zeng (University of Hong Kong), and Siu Ming Yiu (University of Hong Kong)

Information Leakage Analysis of Inner-Product Functional Encryption Based Data Classification 303
Damien Ligier (CEA LIST), Sergiu Carpov (CEA LIST), Caroline Fontaine (CNRS/Lab-STICC and UBL), and Renaud Sirdey (CEA LIST)

Social Network

Reputation Schemes for Pervasive Social Networks with Anonymity (Short Paper) 311
Lydia Garms (Information Security Group), Keith Martin (Information Security Group), and Siaw–Lynn Ng (Information Security Group)

ABnews: A Fast Private Social Messaging System Using Untrusted Storage and Attribute-Based Encryption 317
Yasushi Shinjo (University of Tsukuba), Sota Naito (University of Tsukuba), Xiao Kunyao (University of Tsukuba), and Akira Sato (University of Tsukuba)

Modeling Exposure in Online Social Networks 327
Andrew Cortese (University at Albany - SUNY) and Amirreza Masoumzadeh (University at Albany - SUNY)

From Tag to Protect: A Tag-Driven Policy Recommender System for Image Sharing 337
Anna Cinzia Squicciarini (Pennsylvania State University), Andrea Novelli (Pennsylvania State University), Dan Lin (Missouri S&T), Cornelia Caragea (University of North Texas), and Haoti Zhong (Pennsylvania State University)

Applied Cryptography and Web Security

Classification and Distribution of RBAC Privilege Protection Changes in Wordpress Evolution (Short Paper) 349
Marc-André Laverdière (Tata Consultancy Services) and Ettore Merlo (École Polytechnique de Montréal)

Hiding Behind the Shoulders of Giants: Abusing Crawlers for Indirect Web Attacks 355
Apostolis Zarras (Technical University of Munich) and Federico Maggi (Trend Micro Inc.)

Performance Analysis and Comparison of Different Elliptic Curves on Smart Cards 365
Petr Dzurenda (Brno University of Technology), Sara Ricci (Universitat Rovira i Virgili), Jan Hajny (Brno University of Technology), and Lukas Malina (Brno University of Technology)

On the Additional Chi-Square Tests for the IID Assumption of NIST SP 800-90B 375
Ju-Sung Kang (Kookmin University), Hojoong Park (Kookmin University), and Yongjin Yeom (Kookmin University)

Posters

An Analysis of the Security of Compressed Sensing Using an Artificial Neural Network 385
Shadan Ghaffaripour (Ryerson University), Fadi Younis (Ryerson University), Hoi Ting Poon (Ryerson University), and Ali Miri (Ryerson University)

Information-Flow Control with Fading Labels 388
Andrew Bedford (Université Laval)

A Certified Core Policy Language 391
Bahman Sistany (Irdeto Canada Corporation) and Amy Felty (University of Ottawa)

Optimized Secure Data Aggregation in Wireless Sensor Networks 394
Scott A. Thompson (Montclair State University) and Bharath K. Samanthula (Montclair State University)

A Post-Quantum One Time Signature Using Bloom Filter 397
Masoumeh Shafieinejad (University of Calgary) and Reihaneh Safavi-Naini (University of Calgary)

Alice in Blockchains: Surprising Security Pitfalls in PoW and PoS Blockchain Systems 400
Thomas P. Keenan (University of Calgary)

Author Index 403