2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2020)

Virtual Conference
1 – 3 December 2020

IEEE Catalog Number: CFP20V08-POD
ISBN: 978-1-7281-8544-6

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:	CFP20V08-POD
ISBN (Print-On-Demand):	978-1-7281-8544-6
ISBN (Online):	978-1-7281-8543-9

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

2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)

TPS-ISA 2020

Table of Contents

Message from the General Chairs and PC Chairs x
Organizing Committee xii
Technical Program Committee xiii
Steering Committee xiv
Plenary Panel xv
Plenary Panel for Pandemics xx
Conference Keynote xxvi

TPS Vision Session 1: Security and Privacy in Intelligent Systems and Applications

A Queueing Solution to Reduce Delay in Processing of Disclosed Vulnerabilities 1
Andrew Feutrill (CSIRO/Data61; University of Adelaide), Matthew Roughan (University of Adelaide), Joshua Ross (University of Adelaide), and Yuval Yarom (University of Adelaide; CSIRO/Data61)

Security and Privacy for a Sustainable Internet of Things 12
Helge Janicke (Edith Cowan University & Cyber Security Cooperative Research Centre), Sharif Abuadbba (CSIRO's Data61; CSCRC), and Surya Nepal (CSIRO's Data6; CSCRC)

An Exploratory Analysis on Users' Contributions in Federated Learning 20
Jiyue Huang (Delft University of Technology), Rania Talbi (INSA-Lyon), Zilong Zhao (Delft University of Technology), Sara Boucchenak (INSA-Lyon), Lydia Y. Chen (Delft University of Technology), and Stefanie Roos (Delft University of Technology)

Utility-Optimized Synthesis of Differentially Private Location Traces 30
M. Emre Gursoy (Koc University), Vivekanand Rajasekar (Georgia Institute of Technology), and Ling Liu (Georgia Institute of Technology)

Big Data Privacy Management: A Vision Paper 40
Xiaofeng Meng (Renmin University of China) and Xiaojian Zhang (Henan University of Economics and Law)

TPS Research Session 1: Authentication and Adversarial Learning

A Needle in a Haystack: Finding a Suitable Lightweight IoT Authentication Protocol and Improving Its Usability 46

Nan Li (The University of Newcastle), Dongxi Liu (Data61, CSIRO), Surya Nepal (Data61, CSIRO), and Guangyu Pei (Boeing)

Towards IoT Security Automation and Orchestration 55

Yifeng Zheng (CSIRO's Data61; CSCRC), Arindam Pal (CSIRO's Data61; CSCRC), Sharif Abuadbba (CSIRO's Data61; CSCRC), Shiva Raj Pokhrel (Deakin University), Surya Nepal (CSIRO's Data61; CSCRC), and Helge Janicke (Edith Cowan University & Cyber Security Cooperative Research Centre)

imdpGAN: Generating Private and Specific Data with Generative Adversarial Networks 64

Saurabh Gupta (Indraprastha Institute of Information Technology Delhi), Arun Balaji Buduru (Indraprastha Institute of Information Technology Delhi), and Ponnurangam Kumaraguru (Indraprastha Institute of Information Technology Delhi)

BCB-X3DH: a Blockchain Based Improved Version of the Extended Triple Diffie-Hellman Protocol 73

Armando Ruggeri (University of Messina), Antonio Celesti (University of Messina), Maria Fazio (University of Messina), Antonino Galletta (University of Messina), and Massimo Villari (University of Messina)

Handling Incomplete Information in Policy Evaluation using Attribute Similarity 79

Sowmya Ravidas (Eindhoven University of Technology), Indrakshi Ray (Colorado State University), and Nicola Zannone (Eindhoven University of Technology)

TPS Vision Session 2: Security in Intelligent Systems and Application

Requirements and Challenges for Secure and Trustworthy UAS Collaboration 89

Marco Anisetti (Università degli Studi di Milano Milan), Claudio A. Ardagna (Università degli Studi di Milano Milan), Barbara Carminati (Università degli Studi dell'Insubria Varese), Elena Ferrari (Università degli Studi dell'Insubria Varese), and Cora Lisa Perner (Airbus Cybersecurity GmbH Munich)

MultiModal Deception Detection: Accuracy, Applicability and Generalizability 99

Vibha Belavadi (University of Texas at Dallas), Yan Zhou (University of Texas at Dallas), Jonathan Z. Bakdash (U.S. Army Combat Capabilities Development Command, Army Research Lab South at University of Texas at Dallas), Murat Kantarcioglu (University of Texas at Dallas), Daniel C. Krawczyk (University of Texas at Dallas), Linda Nguyen (University of Texas at Dallas), Jelena Rakic (University of Texas at Dallas), and Bhavani Thuriasingham (University of Texas at Dallas)

Energy Attacks on Mobile Devices 107

Ashish Kundu (Senior Member, IEEE), Zhiqiang Lin (Ohio State University), and Joshua Hammond (University of Texas, Dallas)

From Blue-Sky to Practical Adversarial Learning 118
Aminollah Khormali (University of Central Florida), Ahmed Abusnaina (University of Central Florida), Songqing Chen (George Mason University), DaeHun Nyang (Ewha Womans University), and David Mohaisen (University of Central Florida)

Quantum Adversarial Machine Learning: Status, Challenges and Perspectives 128
DeMarcus Edwards (Howard University) and Danda B. Rawat (Howard University)

TPS Vision Session 3: Privacy and Access Control in Intelligent Systems and Applications

Privacy in the Era of 5G, IoT, Big Data and Machine Learning 134
Elisa Bertino (Purdue University)

A Framework for Privacy-Preserving Genomic Data Analysis Using Trusted Execution Environments 138
Aref Asvadishirehjini (University of Texas at Dallas), Murat Kantarcioglu (University of Texas at Dallas), and Bradley Malin (Vanderbilt University Medical Center)

Convergent Access Control to Enable Secure Smart Communities 148
Smriti Bhatt (Texas A&M University-San Antonio) and Ravi Sandhu (University of Texas at San Antonio)

Maintaining Privacy and Utility in IoT System Analytics 157
Daniel Mossé (University of Pittsburgh), Henrique Pötter (University of Pittsburgh), and Stephen Lee (University of Pittsburgh)

Towards Dynamic Access Control for Privacy 165
Chinmay Kundu (KIIT University)

TPS Research Session 2: Access Control and Authentication

A Model for the Administration of Access Control in Software Defined Networking using Custom Permissions 169
Abdullah Al-Alaj (The University of Texas at San Antonio), Ravi Sandhu (The University of Texas at San Antonio), and Ram Krishnan (The University of Texas at San Antonio)

Role-Based Access Control Models for Android 179
Samir Talegaon (The University of Texas at San Antonio) and Ram Krishnan (The University of Texas at San Antonio)

AuthN-AuthZ: Integrated, User-Friendly and Privacy-Preserving Authentication and Authorization 189

Tyler Phillips (Indiana University-Purdue University Indianapolis), Xiaoyuan Yu (Indiana University-Purdue University Indianapolis), Brandon Haakenson (Indiana University-Purdue University Indianapolis), Shreya Goyal (Indiana University-Purdue University Indianapolis), Xukai Zou (Indiana University-Purdue University Indianapolis), Saptarshi Purkayastha (Indiana University-Purdue University Indianapolis), and Huanmei Wu (Indiana University-Purdue University Indianapolis)

MAFIA: Multi-Layered Architecture for IoT-Based Authentication 199

Pranut Jain (University of Pittsburgh), Henrique Pötter (University of Pittsburgh), Adam J. Lee (University of Pittsburgh), and Daniel Mósse (University of Pittsburgh)

A Survival Game Analysis to Personal Identity Protection Strategies 209

David Liau (The University of Texas at Austin), Razieh Nokhbeh Zaeem (The University of Texas at Austin), and K. Suzanne Barber (The University of Texas at Austin)

A Modern Implementation of System Call Sequence Based Host-Based Intrusion Detection Systems 218

Jeffrey Byrnes (California State University, Sacramento), Thomas Hoang (California State University, Sacramento), Nihal Nitin Mehta (California State University, Sacramento), and Yuan Cheng (California State University, Sacramento)

TPS Research Session 3: Authentication and Adversarial Learning

Revisiting Secure Computation Using Functional Encryption: Opportunities and Research Directions 226

Runhua Xu (IBM Research - Almaden) and James Joshi (University of Pittsburgh)

Adversarial Deception in Deep Learning: Analysis and Mitigation 236

Wenqi Wei (Georgia Institute of Technology, USA), Ling Liu (Georgia Institute of Technology, USA), Margaret Loper (Georgia Tech Research Institute, USA), Ka-Ho Chow (Georgia Institute of Technology, USA), Mehmet Emre Gursoy (Georgia Institute of Technology, USA), Stacey Truex (Georgia Institute of Technology, USA), and Yanzhao Wu (Georgia Institute of Technology, USA)

MoNet: Impressionism as a Defense against Adversarial Examples 246

Huangyi Ge (Purdue University), Sze Yiu Chau (The Chinese University of Hong Kong), and Ninghui Li (Purdue University)

Is Your Phone You? How Privacy Policies of Mobile Apps Allow the Use of Your Personally Identifiable Information 256

Kai Chih Chang (The University of Texas at Austin), Razieh Nokhbeh Zaeem (The University of Texas at Austin), and K. Suzanne Barber (The University of Texas at Austin)

Adversarial Objectness Gradient Attacks in Real-Time Object Detection Systems .263
Ka-Ho Chow (Georgia Institute of Technology), Ling Liu (Georgia Institute of Technology), Margaret Loper (Georgia Tech Research Institute), Juhyun Bae (Georgia Institute of Technology), Mehmet Emre Gursoy (Georgia Institute of Technology), Stacey Truex (Georgia Institute of Technology), Wenqi Wei (Georgia Institute of Technology), and Yanzhao Wu (Georgia Institute of Technology)

Physics Reasoning for Intrusion Detection in Industrial Networks .273
Mohammad Yahya (Oakland University), Nasir Sharaf (Oakland University), Julian L. Rrushi (Oakland University), Ho Ming Tay (Fortinet), Bing Liu (Fortinet), and Kai Xu (Fortinet)

TPS Vision Session 4: Security Incident Managements in Cloud Applications

Security-Aware Energy Management in Clouds .284
Jianzhou Mao (Auburn University), Ting Cao (Auburn University), Xiaopu Peng (Auburn University), Tathagata Bhattacharya (Auburn University), Wei-Shinn Ku (Auburn University), and Xiao Qin (Auburn University)

StackVault: Protection from Untrusted Functions .294
Qi Zhang (IBM Thomas J. Watson Research Center), Zehra Sura (Bloomberg LP), Ashish Kundu (Ciphense), Gong Su (IBM Thomas J. Watson Research Center), Arun Iyengar (IBM Thomas J. Watson Research Center), and Ling Liu (Georgia Institute of Technology)

Envisioning a Cyber-Security Incident Managed Campus Environment .307
Sean Thorpe (University of Technology), Julian Jarrett (University of Technology), and Tyrone Grandison (University of Technology)

Data Security and Malware Detection in Cloud Storage Services .310
Ting Cao (Auburn University), Jianzhou Mao (Auburn University), Tathagata Bhattacharya (Auburn University), Xiaopu Peng (Auburn University), Wei-Shinn Ku (Auburn University), and Xiao Qin (Auburn University)

Toward Automated Enforcement of Cyber-Physical Security Requirements for Energy Delivery Systems .319
Carlos E. Rubio-Medrano (Texas A&M University - Corpus Christi), Ziming Zhao (University at Buffalo), and Gail-Joon Ahn (Arizona State University)

Author Index 323