2011 Ninth Annual International Conference on Privacy, Security and Trust

(PST 2011)

Montreal, Quebec, Canada
19 – 21 July 2011

IEEE Catalog Number: CFP1104F-PRT
ISBN: 978-1-4577-0582-3

Table of Contents

Pseudonymised Communication in Delay Tolerant Networks 1
Naveed Ahmad, Haitham Cruickshank, Zhili Sun and Muhammad Asif

Trust Bootstrapping Services and Service Providers 7
Zainab M. Aljazzaf, Miriam A. M. Capretz and Mark Perry

Safe Realization of the Generalization Privacy Mechanism 16
Tristan Allard, Benjamin Nguyen and Philippe Pucheral

The ultimate invasion of privacy: identity theft 24
Esma Aïmeur and David Schönfeld

Towards machine-assisted formal procedures for the collection of digital evidence 32
Martín Barrere, Gustavo Betarte and Marcelo Rodríguez

On Re-use of Randomness in Broadcast Encryption 36
Paolo Gasti and Alessio Merlo

Extraction and Comprehension of Moodle's Access Control Model: A case study 44
François Gauthier, Dominic Letarte, Thierry Lavoie and Ettore Merlo

Modelling of security properties in Alloy 52
Lilia Georgieva

Privacy Data Envelope: Concept and Implementation 55
Mahmoud Ghorbel, Armen Aghasaryan, Stéphane Betgé-Brezetz, Marie-Pascale Dupont, Guy-Bertrand Kamga and Sophie Piekarec

A Trust-based Approach against IP-spoofing Attacks 63
Jesus Gonzalez, Mohd Anwar and James B.D. Joshi

Improving the Use of Advisor Networks for Multi-Agent Trust Modelling 71
Joshua Gorner, Jie Zhang and Robin Cohen

I-RBAC: Isolation Enabled Role-Based Access Control 79
Nagajyothi Gunti, Weiqing Sun and Mohammed Niamat

Transparent Non-Intrusive Multimodal Biometric System For Video Conference Using The Fusion Of Face And Ear Recognition 87
Abbas Javadtalab, Laith Abbadi, Mona Omidyeganeh, Carlisle Adams, Shervin Shirmohammadi and Abdulmotaleb El Saddik

A Hamming Distance-like Filtering in Keystroke Dynamics 93
Yoshihiro Kaneko, Yuji Kinpara and Yuta Shiomi

Ensuring Tight Computational Security Against Higher-Order DPA Attacks 96
Dakshita Khurana and Aditya Gaurav

Forward Secure Identity-based Key Agreement for Dynamic Groups 102
Nick Mailloux, Ali Miri and Monica Nevins

UPBA: User-Authenticated Property-Based Attestation 112
Mark Manulis and Marion Steiner

On the Need for Data Flow Graph Visualization of Forensic Lucid Programs and Encoded Evidence, and their Evaluation by GIPSY 120
Serguei Mokhov, Joey Paquet and Mourad Debbabi

Delegation of access rights in a privacy preserving access control model 124
Md. Moniruzzaman and Ken Barker

Improving Security and Usability of Low Cost RFID Tags. 134
Ali Noman, Sk. Md. Mizanur Rahman and Carlisle Adams

Model-Based Systems Security Quantification 142
Samir Ouchani, Yosr Jarraya and Otmane Ait Mohamed

A Probabilistic-Based Approach towards Trust Evaluation using Poisson Hidden Markov Models and Bonus Malus Systems 150
Kevin Ouyang, Binod Vaidya and Dimitrios Makrakis

Validation of Security for Participant Control Exchanges in Multicast Content Distribution 156
Mohammad Parham and John William Atwood

Cryptographic Security Models for eHealth P2P Database Management Systems Network 164
Sk. Md. Mizanur Rahman, Md. Mehedi Masud, Carlisle Adams, Khalil El-Khatib, Hussein Mouftah and Eiji Okamoto

Detecting P2P Botnets through Network Behavior Analysis and Machine Learning 174
Sherif Saad, Issa Traore, Ali Ghorbani, Bassam Sayed, David Zhao, Wei Lu, John Felix and Payman Hakimian

Data Preprocessing for Distance-based Unsupervised Intrusion Detection 181
Dina Said, Lisa Stirling, Peter Federolf and Ken Barker

Risk-based Decision Method for Access Control Systems 189
Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo and Serge Mankovski

Advantages of a Non-Technical XACML Notation in Role-Based Models 193
Bernard Stepien, Amy Felty and Stan Matwin

A Diffie-Hellman based Privacy Protocol for Car-to-X Communication 201
Hagen Stübing, Murat Ceven and Sorin A. Huss

Secure communication with secret sharing in static computer networks with partition in mistrust parties 205
Johannes Viehmann

Privacy Challenges of Open APIs: Case Location Based Services 213
Alberto Vila Tena and Yrjö Raivio

General Secure Function Evaluation Using Standard Trusted Computing Hardware 221
Roopa Vishwanathan and Steve Tate

Beyond Privacy Policies - Assessing Inherent Privacy Risks of Consumer Health Services 229
Jens H. Weber-Jahnke and James Williams

An Implementation of a Verification Condition Generator for Foundational Proof-Carrying Code . . . 238
Jiangong Weng and Amy Felty

Performance Analysis of QKD Based Key Distribution for IEEE 802.11 Networks 246
Shirantha Wijesekera, Xu Huang and Dharmendra Sharma

Privacy-Preserving Matchmaking For Mobile Social Networking Secure Against Malicious Users . . 252
Qi Xie and Urs Hengartner

Online Information Privacy: Agent-Mediated Payoff 260
Abdulsalam Yassine, Ali Asghar Nazari Shirehjini, Shervin Shirmohammadi and Thomas T.Tran

RC4 State and Its Applications 264
Qian Yu and Chang N. Zhang