Table of Contents

ASIACCS 2010 Conference Organization .................................................................................. viii

External Reviewers .................................................................................................................. x

Sponsor & Supporters ............................................................................................................... xi

Keynote Addresses

• Data Protection in Outsourcing Scenarios: Issues and Directions ............................................. 1
  Pierangela Samarati, Sabrina De Capitani di Vimercati (Università degli Studi di Milano)

• A Lattice-based Approach to Mashup Security .................................................................. 15
  Jonas Magazinius (Chalmers), Aslan Askarov (Cornell University),
  Andrei Sabelfeld (Chalmers)

Session 1: Privacy

• Towards Publishing Recommendation Data With Predictive Anonymization ...................... 24
  Chih-Cheng Chang, Brian Thompson (Rutgers University),
  Hui Wang (Stevens Institute of Technology), Danfeng Yao (Rutgers University)

• Restoring Compromised Privacy in Micro-data Disclosure ............................................... 36
  Lei Zhang, Alexander Brodsky, Sushil Jajodia (George Mason University)

• Securely Outsourcing Linear Algebra Computations ....................................................... 48
  Mikhail Atallah (Purdue University), Keith Frikken (Miami University)

Session 2: Applied Cryptography

• Attribute-based Signature and its Application .................................................................... 60
  Jin Li (Illinois Institute of Technology),
  Man Ho Au, Willy Susilo (University of Wollongong),
  Dongqing Xie (Guangzhou University), Kui Ren (Illinois Institute of Technology)

• Dynamic Fully Forward-Secure Group Signatures .......................................................... 70
  Benoit Libert (Universite Catholique de Louvain),
  Moti Yung (Google & Columbia University)

• Identity-Based Encryption based on DHIES .................................................................. 82
  Yu Chen (Peking University),
  Manuel Charlemagne (Dublin City University, Ireland),
  Zhi Guan, Jianbin Hu, Zhong Chen (Peking University)
Session 3: Network Security

• Region-based BGP Announcement Filtering for Improved BGP Security ..........................89
  Fernando Sanchez, Zhenhai Duan (Florida State University)

• Fast-flux Service Network Detection Based on Spatial Snapshot Mechanism for Delay-free Detection .................................................................101
  Si-Yu Huang, Ching-Hao Mao, Hahn-Ming Lee
  (National Taiwan University of Science and Technology)

• Securing Wireless Sensor Networks against Large-scale Node Capture Attacks .............112
  Tuan Manh Vu, Reihaneh Safavi-Naini, Carey Williamson (University of Calgary)

Session 4: Systems Security – I

• Preventing Drive-by Download via Inter-Module Communication Monitoring ...............124
  Chengyu Song, Jianwei Zhuge, Xinhui Han, Zhiyuan Ye (Peking University)

• A Solution for the Automated Detection of Clickjacking Attacks ..................................135
  Marco Balduzzi (Institute Eurecom), Manuel Egele (Technical University, Vienna),
  Engin Kirda, Davide Balzarotti (Institute Eurecom),
  Christopher Kruegel (University of California, Santa Barbara)

• PARiCheck: An Efficient Pointer Arithmetic Checker for C Programs ..........................145
  Yves Younan, Pieter Philippaerts (Katholieke Universiteit Leuven),
  Lorenzo Cavallaro (University of California, Santa Barbara),
  R. Sekar (Stony Brook University),
  Frank Piessens, Wouter Joosen (Katholieke Universiteit Leuven)

Session 5: Access Control – I

• An Opportunistic Authority Evaluation Scheme for Data Security in Crisis Management Scenarios .................................................................157
  Enrico Scalavino (Imperial College London), Giovanni Russello (Create-Net),
  Rudi Ball, Vaibhav Gowadia, Emil Lupu (Imperial College London)

• Effective Trust Management Through a Hybrid Logical and Relational Approach .......... N/A
  Adam J. Lee (University of Pittsburgh), Ting Yu (North Carolina State University),
  Yann Le Gall (University of Pittsburgh)

• Toward Practical Authorization-dependent User Obligation Systems .........................180
  Murillo Pontual, Omar Chowdhury, William H. Winsborough,
  (The University of Texas at San Antonio),
  Ting Yu (North Carolina State University), Keith Irwin (Winston-Salem State University)
Session 6: Security Protocols

- Cap Unification: Application to Protocol Security modulo Homomorphic Encryption .................................................. 192
  Siva Anantharaman (LIFO, University of Orleans), Hai Lin (Clarkson University),
  Christopher Lynch (Clarkson University), Paliath Narendran (University at Albany-SUNY)
  Michael Rusinowitch (LORIA - INRIA Lorraine)

- SSLOCK: Sustaining the Trust on Entities Brought by SSL ............................................................ 204
  Adonis P.H. Fung, K.W. Cheung (The Chinese University of Hong Kong)

- Computationally Secure Two-Round Authenticated Message Exchange .................................................. 214
  Klaas Ole Kürtz, Henning Schnoor, Thomas Wilke (Christian-Albrechts-Universität zu Kiel)

- Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting ................................ 226
  Guan Wang, Tongbo Luo (Syracuse University),
  Michael T. Goodrich (University of California, Irvine),
  Wenliang Du, Zutao Zhu (Syracuse University)

Session 7: Access Control – II

- A Logic for Authorization Provenance ........................................................................................................ 238
  Jinwei Hu (Huazhong University of Science and Technology),
  Yan Zhang (University of Western Sydney),
  Ruixuan Li, Zhengding Lu (Huazhong University of Science and Technology)

- Risk-based Access Control Systems Built on Fuzzy Inferences .................................................. 250
  Qun Ni, Elisa Bertino (Purdue University), Jorge Lobo (IBM T.J. Watson Research Center)

- Attribute Based Data Sharing with Attribute Revocation .................................................. 261
  Shucheng Yu (Worcester Polytechnic Institute),
  Cong Wang, Kui Ren (Illinois Institute of Technology),
  Wenjing Lou (Worcester Polytechnic Institute)

Session 8: Systems Security – II

- binOb+: A Framework for Potent and Stealthy Binary Obfuscation .................................................. 271
  Byoungyoung Lee, Yuna Kim, Jong Kim (POSTECH)

- Secure Provenance: The Essential of Bread and Buffer of Data Forensics in Cloud Computing .................................................. 282
  Rongxing Lu (University of Waterloo),
  Xiaodong Lin (University of Ontario Institute of Technology),
  Xiaohui Liang, Xuemin (Sherman) Shen (University of Waterloo)

- RunTest: Assuring Integrity of Dataflow Processing in Cloud Computing Infrastructures .................................................. 293
  Juan Du, Wei Wei, Xiaohui Gu, Ting Yu (North Carolina State University)
Session 9: Short Papers – I

- **K-anonymous Association Rule Hiding** ................................................................. 305
  Zutao Zhu, Wenliang Du (Syracuse University)

- **Controlling Data Disclosure in Computational PIR Protocols** .................. 310
  Ning Shang, Gabriel Ghinita, Yongbin Zhou, Elisa Bertino (Purdue University)

- **Cryptographic Role-based Security Mechanisms based on Role-Key Hierarchy** .......... 314
  Yan Zhu (Peking University), Gail-Joon Ahn, Hongxin Hu (Arizona State University),
  Huaixi Wang (Peking University)

- **PriMa: An Effective Privacy Protection Mechanism for Social Networks** ........ 320
  Anna Squicciarini (The Pennsylvania State University),
  Federica Paci (University of Trento),
  Smitha Sundareswaran (The Pennsylvania State University)

- **Oblivious Enforcement of Hidden Information Release Policies** ................. 324
  Brian Wongchaowart, Adam Lee (University of Pittsburgh)

Session 10: Short Papers – II

- **Apex: Extending Android Permission Model and Enforcement with**
  **User-defined Runtime Constraints** ................................................................. 328
  Mohammad Nauman (Institute of Management Sciences, Pakistan),
  Sohail Khan (NUST, Pakistan), Xinwen Zhang (Samsung Information Systems America)

- **A Hotspot-based Protocol for Attack Traceback in Mobile Ad Hoc Networks** ........ 333
  Hungyuan Hsu, Sencun Zhu (The Pennsylvania State University),
  Ali Hurson (Missouri University of Science and Technology)

- **Practical ID-based Encryption for Wireless Sensor Network** ......................... 337
  Cheng-Kang Chu (Singapore Management University),
  Joseph K. Liu, Jianying Zhou, Feng Bao (Institute for Infocomm Research, Singapore),
  Robert H. Deng (Singapore Management University)

- **A Game Theoretic Model for Digital Identity and Trust in Online Communities** ...... 341
  Tansu Alpcan (Deutsche Telekom Laboratories),
  Cengiz Örencik, Albert Levi, Erkay Savas (Sabanci University, Turkey)

- **Scene Tagging: Image-Based CAPTCHA Using Image Composition**
  **and Object Relationships** .................................................................................... 345
  Peter Matthews, Cliff Zou (University of Central Florida)

**Author Index** ............................................................................................................. 351