Contents

Privacy

O-PSI: Delegated Private Set Intersection on Outsourced Datasets .................................. 3
   Aydin Abadi, Sotirios Terzis, and Changyu Dong

Flexible and Robust Privacy-Preserving Implicit Authentication ................................. 18
   Josep Domingo-Ferrer, Qianhong Wu, and Alberto Blanco-Justicia

Towards Relations Between the Hitting-Set Attack and the Statistical Disclosure Attack .................................................. 35
   Dang Vinh Pham and Dogan Kesdogan

POSN: A Personal Online Social Network ................................................................. 51
   Esra Erdin, Eric Klukovich, Gurhan Gunduz, and Mehmet Hadi Gunes

Strategic Noninterference .......................................................................................... 67
   Wojciech Jamroga and Masoud Tabatabaei

Verifying Observational Determinism ........................................................................ 82
   Jaber Karimpour, Ayaz Isazadeh, and Ali A. Noroozi

Web Security

Cache Timing Attacks Revisited: Efficient and Repeatable Browser History, OS and Network Sniffing .......................................................... 97
   Chetan Bansal, Sören Preibusch, and Natasa Milic-Frayling

Enforcing Usage Constraints on Credentials for Web Applications ........................ 112
   Jinwei Hu, Heiko Mantel, and Sebastian Ruhleder

A Survey of Alerting Websites: Risks and Solutions .................................................. 126
   Amrit Kumar and Cédric Lauradoux

Access Control, Trust and Identity Management

A Generalization of ISO/IEC 24761 to Enhance Remote Authentication with Trusted Product at Claimant .................................................. 145
   Asahiko Yamada

Enhancing Passwords Security Using Deceptive Covert Communication .............. 159
   Mohammed H. Almeshekah, Mikhail J. Atallah, and Eugene H. Spafford
Information Sharing and User Privacy in the Third-party Identity Management Landscape. .......................................................... 174
Anna Vapen, Niklas Carlsson, Anirban Mahanti, and Nahid Shahmehri

An Iterative Algorithm for Reputation Aggregation in Multi-dimensional and Multinomial Rating Systems ........................................ 189
Mohsen Rezvani, Mohammad Allahbakhsh, Lorenzo Vigentini, Aleksandar Ignjatovic, and Sanjay Jha

A Comparison of PHY-Based Fingerprinting Methods Used to Enhance Network Access Control .................................................. 204
Timothy J. Carbino, Michael A. Temple, and Juan Lopez Jr.

Model-Driven Integration and Analysis of Access-control Policies in Multi-layer Information Systems ............................................ 218
Salvador Martínez, Joaquin Garcia-Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia, and Jordi Cabot

Network Security

Authenticated File Broadcast Protocol ................................................ 237
Simão Reis, André Zúquete, Carlos Faneca, and José Vieira

Automated Classification of C&C Connections Through Malware URL Clustering ................................................................. 252
Nizar Kheir, Gregory Blanc, Hervé Debar, Joaquin Garcia-Alfaro, and Dingqi Yang

B.Hive: A Zero Configuration Forms Honeypot for Productive Web Applications ................................................................. 267
Christoph Pohl, Alf Zugenmaier, Michael Meier, and Hans-Joachim Hof

Security Management and Human Aspects of Security

Investigation of Employee Security Behaviour: A Grounded Theory Approach ................................................................. 283
Lena Connolly, Michael Lang, and J.D. Tygar

Practice-Based Discourse Analysis of InfoSec Policies .................. 297
Fredrik Karlsson, Göran Goldkuhl, and Karin Hedström

Understanding Collaborative Challenges in IT Security Preparedness Exercises ................................................................. 311
Maria B. Line and Nils Brede Moe

Social Groupings and Information Security Obedience Within Organizations ................................................................. 325
Teodor Sommestad
Attack Trees with Sequential Conjunction ........................................... 339
  Ravi Jhawar, Barbara Kordy, Sjouke Mauw, Saša Radomirović,
  and Rolando Trujillo-Rasua

Enhancing the Security of Image CAPTCHAs Through Noise Addition .... 354
  David Lorenzi, Emre Uzun, Jaideep Vaidya, Shamik Sural,
  and Vijayalakshmi Atluri

Software Security

SHRIFT System-Wide HybRid Information Flow Tracking ...................... 371
  Enrico Lovat, Alexander Fromm, Martin Mohr, and Alexander Pretschner

ISboxing: An Instruction Substitution Based Data Sandboxing
for x86 Untrusted Libraries .......................................................... 386
  Liang Deng, Qingkai Zeng, and Yao Liu

Exploit Generation for Information Flow Leaks
in Object-Oriented Programs ....................................................... 401
  Quoc Huy Do, Richard Bubel, and Reiner Hähnle

Memoized Semantics-Based Binary Diffing with Application
to Malware Lineage Inference .................................................... 416
  Jiang Ming, Dongpeng Xu, and Dinghao Wu

Mitigating Code-Reuse Attacks on CISC Architectures
in a Hardware Approach .............................................................. 431
  Zhijiao Zhang, Yashuai Lü, Yu Chen, Yongqiang Lü, and Yuanchun Shi

Integrity for Approximate Joins on Untrusted Computational Servers .... 446
  Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia,
  Stefano Paraboschi, and Pierangela Samarati

Applied Cryptography

Fast Revocation of Attribute-Based Credentials for Both Users
and Verifiers ................................................................. 463
  Wouter Lueks, Gergely Alpár, Jaap-Henk Hoepman, and Pim Vullers

Chaotic Chebyshev Polynomials Based Remote User Authentication
Scheme in Client-Server Environment ........................................ 479
  Toan-Thanh Truong, Minh-Triet Tran, Anh-Duc Duong, and Isao Echizen

A Secure Exam Protocol Without Trusted Parties ........................... 495
  Giampaolo Bella, Rosario Giustolisi, Gabriele Lenzini,
  and Peter Y.A. Ryan
Mobile and Cloud Services Security

ApkCombiner: Combining Multiple Android Apps to Support Inter-App Analysis .................................................. 513
Li Li, Alexandre Bartel, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon

Assessment of the Susceptibility to Data Manipulation of Android Games with In-app Purchases .................................................. 528
Francisco Vigário, Miguel Neto, Diogo Fonseca, Mário M. Freire, and Pedro R.M. Inácio

An Empirical Study on Android for Saving Non-shared Data on Public Storage .................................................. 542
Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li, and Kehuan Zhang

The Dual-Execution-Environment Approach: Analysis and Comparative Evaluation .................................................. 557
Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah

On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps .................................................. 571
Konstantin Knorr, David Aspinall, and Maria Wolters

A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration .................................................. 585
Alevtina Dubovitskaya, Visara Urovi, Matteo Vasirani, Karl Aberer, and Michael I. Schumacher

Cyber-physical Systems and Critical Infrastructures Security

Application of a Game Theory Based Approach in Smart Sensor Data Trustworthiness Problems .................................................. 601
Konstantinos Maraslis, Theodoros Spyridopoulos, George Oikonomou, Theo Tryfonas, and Mo Haghighi

Securing BACnet’s Pitfalls .................................................. 616
Jaspreet Kaur, Jernej Tonejc, Steffen Wendzel, and Michael Meier

On the Secure Distribution of Vendor-Specific Keys in Deployment Scenarios .................................................. 630
Nicolai Kuntze, Andreas Fuchs, and Carsten Rudolph

Erratum to: On the Secure Distribution of Vendor-Specific Keys in Deployment Scenarios .................................................. E1
Nicolai Kuntze, Andreas Fuchs, and Carsten Rudolph

Author Index .................................................. 645
ICT Systems Security and Privacy Protection
30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings
Federrath, H.; Gollmann, D. (Eds.)
2015, XVI, 646 p. 156 illus., Hardcover
ISBN: 978-3-319-18466-1