

Contents

Privacy

O-PSI: Delegated Private Set Intersection on Outsourced Datasets	3
<i>Aydin Abadi, Sotirios Terzis, and Changyu Dong</i>	
Flexible and Robust Privacy-Preserving Implicit Authentication	18
<i>Josep Domingo-Ferrer, Qianhong Wu, and Alberto Blanco-Justicia</i>	
Towards Relations Between the Hitting-Set Attack and the Statistical Disclosure Attack	35
<i>Dang Vinh Pham and Dogan Kesdogan</i>	
POSN: A Personal Online Social Network	51
<i>Esra Erdin, Eric Klukovich, Gurhan Gunduz, and Mehmet Hadi Gunes</i>	
Strategic Noninterference	67
<i>Wojciech Jamroga and Masoud Tabatabaei</i>	
Verifying Observational Determinism	82
<i>Jaber Karimpour, Ayaz Isazadeh, and Ali A. Noroozi</i>	

Web Security

Cache Timing Attacks Revisited: Efficient and Repeatable Browser History, OS and Network Sniffing	97
<i>Chetan Bansal, Sören Preibusch, and Natasa Milic-Frayling</i>	
Enforcing Usage Constraints on Credentials for Web Applications	112
<i>Jinwei Hu, Heiko Mantel, and Sebastian Ruhleder</i>	
A Survey of Alerting Websites: Risks and Solutions	126
<i>Amrit Kumar and Cédric Lauradoux</i>	

Access Control, Trust and Identity Management

A Generalization of ISO/IEC 24761 to Enhance Remote Authentication with Trusted Product at Claimant	145
<i>Asahiko Yamada</i>	
Enhancing Passwords Security Using Deceptive Covert Communication	159
<i>Mohammed H. Almeshekeh, Mikhail J. Atallah, and Eugene H. Spafford</i>	

Information Sharing and User Privacy in the Third-party Identity Management Landscape.	174
<i>Anna Vapen, Niklas Carlsson, Anirban Mahanti, and Nahid Shahmehri</i>	
An Iterative Algorithm for Reputation Aggregation in Multi-dimensional and Multinomial Rating Systems	189
<i>Mohsen Rezvani, Mohammad Allahbakhsh, Lorenzo Vigentini, Aleksandar Ignjatovic, and Sanjay Jha</i>	
A Comparison of PHY-Based Fingerprinting Methods Used to Enhance Network Access Control	204
<i>Timothy J. Carbino, Michael A. Temple, and Juan Lopez Jr.</i>	
Model-Driven Integration and Analysis of Access-control Policies in Multi-layer Information Systems.	218
<i>Salvador Martínez, Joaquín García-Alfaro, Frédéric Cuppens, Nora Cuppens-Boulahia, and Jordi Cabot</i>	
Network Security	
Authenticated File Broadcast Protocol.	237
<i>Simão Reis, André Zúquete, Carlos Faneca, and José Vieira</i>	
Automated Classification of C&C Connections Through Malware URL Clustering	252
<i>Nizar Kheir, Gregory Blanc, Hervé Debar, Joaquín García-Alfaro, and Dingqi Yang</i>	
B.Hive: A Zero Configuration Forms Honeypot for Productive Web Applications	267
<i>Christoph Pohl, Alf Zugenmaier, Michael Meier, and Hans-Joachim Hof</i>	
Security Management and Human Aspects of Security	
Investigation of Employee Security Behaviour: A Grounded Theory Approach	283
<i>Lena Connolly, Michael Lang, and J.D. Tygar</i>	
Practice-Based Discourse Analysis of InfoSec Policies	297
<i>Fredrik Karlsson, Göran Goldkuhl, and Karin Hedström</i>	
Understanding Collaborative Challenges in IT Security Preparedness Exercises	311
<i>Maria B. Line and Nils Brede Moe</i>	
Social Groupings and Information Security Obedience Within Organizations	325
<i>Teodor Sommestad</i>	

Attack Trees with Sequential Conjunction	339
<i>Ravi Jhawar, Barbara Kordy, Sjouke Mauw, Saša Radomirović, and Rolando Trujillo-Rasua</i>	

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

Software Security

SHRIFT System-Wide HybRid Information Flow Tracking	371
<i>Enrico Lovat, Alexander Fromm, Martin Mohr, and Alexander Pretschner</i>	

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

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

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

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

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

Applied Cryptography

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

Chaotic Chebyshev Polynomials Based Remote User Authentication Scheme in Client-Server Environment	479
<i>Toan-Thinh Truong, Minh-Triet Tran, Anh-Duc Duong, and Isao Echizen</i>	

A Secure Exam Protocol Without Trusted Parties	495
<i>Giampaolo Bella, Rosario Giustolisi, Gabriele Lenzini, and Peter Y.A. Ryan</i>	

Mobile and Cloud Services Security

ApkCombiner: Combining Multiple Android Apps to Support Inter-App Analysis	513
<i>Li Li, Alexandre Bartel, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon</i>	
Assessment of the Susceptibility to Data Manipulation of Android Games with In-app Purchases	528
<i>Francisco Vigário, Miguel Neto, Diogo Fonseca, Mário M. Freire, and Pedro R.M. Inácio</i>	
An Empirical Study on Android for Saving Non-shared Data on Public Storage	542
<i>Xiangyu Liu, Zhe Zhou, Wenrui Diao, Zhou Li, and Kehuan Zhang</i>	
The Dual-Execution-Environment Approach: Analysis and Comparative Evaluation	557
<i>Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah</i>	
On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps	571
<i>Konstantin Knorr, David Aspinall, and Maria Wolters</i>	
A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration	585
<i>Alevtina Dubovitskaya, Visara Urovi, Matteo Vasirani, Karl Aberer, and Michael I. Schumacher</i>	

Cyber-physical Systems and Critical Infrastructures Security

Application of a Game Theoretic Approach in Smart Sensor Data Trustworthiness Problems	601
<i>Konstantinos Maraslis, Theodoros Spyridopoulos, George Oikonomou, Theo Tryfonas, and Mo Haghghi</i>	
Securing BACnet's Pitfalls	616
<i>Jaspreet Kaur, Jernej Tonejc, Steffen Wendzel, and Michael Meier</i>	
On the Secure Distribution of Vendor-Specific Keys in Deployment Scenarios	630
<i>Nicolai Kuntze, Andreas Fuchs, and Carsten Rudolph</i>	
Erratum to: On the Secure Distribution of Vendor-Specific Keys in Deployment Scenarios	E1
<i>Nicolai Kuntze, Andreas Fuchs, and Carsten Rudolph</i>	
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