

# Contents

## Attacks and Mitigation

An Attack Possibility on Time Synchronization Protocols Secured with TESLA-Like Mechanisms . . . . .	3
<i>Kristof Teichel, Dieter Sibold, and Stefan Milius</i>	
Practical DoS Attacks on Embedded Networks in Commercial Vehicles. . . . .	23
<i>Subhojeet Mukherjee, Hossein Shirazi, Indrakshi Ray, Jeremy Daily, and Rose Gamble</i>	

## Authentication

Secure Lightweight User Authentication and Key Agreement Scheme for Wireless Sensor Networks Tailored for the Internet of Things Environment . . . . .	45
<i>Srinivas Jangirala, Dheerendra Mishra, and Sourav Mukhopadhyay</i>	
SPOSS: Secure Pin-Based-Authentication Obviating Shoulder Surfing . . . . .	66
<i>Ankit Maheshwari and Samrat Mondal</i>	

## Authorization and Information Flow Control

Building a Fair System Using Access Rights . . . . .	89
<i>Nada Essaouini, Frédéric Cuppens, and Nora Cuppens-Boulahia</i>	
Collaborative Access Decisions: Why Has My Decision Not Been Enforced? . . . . .	109
<i>Jerry den Hartog and Nicola Zannone</i>	
Data Loss Prevention Based on Text Classification in Controlled Environments . . . . .	131
<i>Kyrre Wahl Kongsgård, Nils Agne Nordbotten, Federico Mancini, and Paal E. Engelstad</i>	
Defining Abstract Semantics for Static Dependence Analysis of Relational Database Applications . . . . .	151
<i>Angshuman Jana and Raju Halder</i>	

## Cryptosystem and Protocols

An Efficient Certificateless Signature Scheme in the Standard Model. . . . .	175
<i>Sébastien Canard and Viet Cuong Trinh</i>	

Constant-Size Ciphertext Attribute-Based Encryption from Multi-channel Broadcast Encryption. . . . .	193
<i>Sébastien Canard and Viet Cuong Trinh</i>	
Enhanced Modulo Based Multi Secret Image Sharing Scheme . . . . .	212
<i>Maroti Deshmukh, Neeta Nain, and Mushtaq Ahmed</i>	
Performance Evaluation of Modified Henon Map in Image Encryption . . . . .	225
<i>S.J. Sheela, K.V. Suresh, and Deepaknath Tandur</i>	
<b>Network Security and Intrusion Detection</b>	
Network Counter-Attack Strategy by Topology Map Analysis . . . . .	243
<i>Hidema Tanaka</i>	
Network Vulnerability Analysis Using a Constrained Graph Data Model . . . . .	263
<i>Mridul Sankar Barik, Chandan Mazumdar, and Amarnath Gupta</i>	
Secured Dynamic Scheduling Algorithm for Real-Time Applications on Grid . . . . .	283
<i>Surendra Singh, Sachin Tripathi, and Suvadip Batabyal</i>	
<b>Privacy</b>	
A Framework for Analyzing Associativity and Anonymity in Conventional and Electronic Summative Examinations . . . . .	303
<i>Kissan Gauns Dessai and Venkatesh Kamat</i>	
On the Security of “Verifiable Privacy-Preserving Monitoring for Cloud-Assisted mHealth Systems” . . . . .	324
<i>Hardik Gajera, Shruti Naik, and Manik Lal Das</i>	
Privacy Preserving Network Analysis of Distributed Social Networks . . . . .	336
<i>Varsha Bhat Kukkala, Jaspal Singh Saini, and S.R.S. Iyengar</i>	
<b>Software Security</b>	
Exploiting Block-Chain Data Structure for Auditorless Auditing on Cloud Data . . . . .	359
<i>Sanat Ghoshal and Goutam Paul</i>	
Risk Evaluation of X.509 Certificates – A Machine Learning Application . . . . .	372
<i>Varsharani Hawanna, Vrushali Kulkarni, Rashmi Rane, and Pooja Joshi</i>	

## Wireless, Mobile and IoT Security

A Secure Routing Scheme for Wireless Mesh Networks . . . . .	393
<i>Ashish Nanda, Priyadarsi Nanda, Xiangjian He, and Aruna Jamdagni</i>	
Digital Forensic Source Camera Identification with Efficient Feature Selection Using Filter, Wrapper and Hybrid Approaches . . . . .	409
<i>Venkata Udaya Sameer, S. Sugumaran, and Ruchira Naskar</i>	
Formal Verification of a Cross-Layer, Trustful Space-Time Protocol for Wireless Sensor Networks. . . . .	426
<i>Douglas Simões Silva, Davi Resner, Rick Lopes de Souza, and Jean Everson Martina</i>	
JITWORM: Jitter Monitoring Based Wormhole Attack Detection in MANET. . . . .	444
<i>Sudhir Bagade and Vijay Raisinghani</i>	

## Short Papers

A Solution to Detect Phishing in Android Devices . . . . .	461
<i>Sharvari Prakash Chorghe and Narendra Shekokar</i>	
Feature Selection for Effective Botnet Detection Based on Periodicity of Traffic . . . . .	471
<i>T. Harsha, S. Asha, and B. Soniya</i>	
Honeypot Deployment in Broadband Networks. . . . .	479
<i>Saurabh Chamotra, Rakesh Kumar Sehgal, Sanjeev Ror, and Bhupendra singh</i>	
Generic Construction of Certificateless Signcryption Scheme . . . . .	489
<i>Jayaprakash Kar and Kshirasagar Naik</i>	
Reed-Muller Code Based Symmetric Key Fully Homomorphic Encryption Scheme . . . . .	499
<i>RatnaKumari Challa and VijayaKumari Gunta</i>	
Towards Useful Anomaly Detection for Back Office Networks. . . . .	509
<i>Ömer Yüksel, Jerry den Hartog, and Sandro Etalle</i>	
Detection of SQLite Database Vulnerabilities in Android Apps. . . . .	521
<i>Vineeta Jain, M.S. Gaur, Vijay Laxmi, and Mohamed Mosbah</i>	
Discovering Vulnerable Functions by Extrapolation: A Control-Flow Graph Similarity Based Approach. . . . .	532
<i>Lokesh Jain, Aditya Chandran, Sanjay Rawat, and Kannan Srinathan</i>	
<b>Author Index</b> . . . . .	543

Information Systems Security

12th International Conference, ICISS 2016, Jaipur, India,

December 16-20, 2016, Proceedings

Ray, I.; Gaur, M.S.; Conti, M.; Sanghi, D.; Kamakoti, V.

(Eds.)

2016, XV, 544 p. 134 illus., Softcover

ISBN: 978-3-319-49805-8