## Contents

### Cyber-Physical Systems Security

A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures ................................. 3  
*Hayretdin Bahşi and Olaf Manuel Maennel*

A Survey of Industrial Control System Testbeds ................................. 11  
*Hannes Holm, Martin Karresand, Arne Vidström, and Erik Westring*

The Timed Decentralised Label Model ............................................ 27  
*Martin Leth Pedersen, Michael Hedegaard Sørensen, Daniel Lux, Ulrik Nyman, and René Rydhof Hansen*

### Privacy

Resilient Collaborative Privacy for Location-Based Services .................. 47  
*Hongyu Jin and Panos Papadimitratos*

Design of a Privacy-Preserving Document Submission and Grading System ................................. 64  
*Benjamin Greschbach, Guillermo Rodríguez-Cano, Tomas Ericsson, and Sonja Buchegger*

Towards Perfectly Secure and Deniable Communication Using an NFC-Based Key-Exchange Scheme .................. 72  
*Daniel Bosk, Martin Kjellqvist, and Sonja Buchegger*

### Cryptography

Faster Binary Curve Software: A Case Study ................................. 91  
*Billy Bob Brumley*

WHIRLBOB, the Whirlpool Based Variant of STRIBOB: Lighter, Faster, and Constant Time ................................. 106  
*Markku–Juhani O. Saarinen and Billy Bob Brumley*

An Efficient Traceable Attribute-Based Authentication Scheme with One-Time Attribute Trees .................. 123  
*Huihui Yang and Vladimir A. Oleshchuk*
Trust and Fraud

FIDO Trust Requirements ........................................... 139
   Ijlal Loutfi and Audun Jøsang

Using the RetSim Fraud Simulation Tool to Set Thresholds for Triage
of Retail Fraud .......................................................... 156
   Edgar Alonso Lopez-Rojas and Stefan Axelsson

IncidentResponseSim: An Agent-Based Simulation Tool for Risk
Management of Online Fraud ........................................ 172
   Dan Gorton

Network and Software Security

Challenges in Managing Firewalls ..................................... 191
   Artem Voronkov, Stefan Lindskog, and Leonardo A. Martucci

Multi-layer Access Control for SDN-Based Telco Clouds. ......... 197
   Bernd Jäger, Christian Röpke, Iris Adam, and Thorsten Holz

Guaranteeing Dependency Enforcement in Software Updates ....... 205
   Luigi Catuogno, Clemente Galdi, and Giuseppe Persiano

Electronic Citizen Identities and Strong Authentication ............ 213
   Sanna Suoranta, Lari Haataja, and Tuomas Aura

Author Index ............................................................ 231
Secure IT Systems
20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19-21, 2015, Proceedings
Buchegger, S.; Dam, M. (Eds.)
2015, X, 231 p. 47 illus. in color., Softcover
ISBN: 978-3-319-26501-8