

# Contents

## Protection of Personal Data

<i>CLiKC: A Privacy-Mindful Approach When Sharing Data</i> . . . . .	3
<i>Esma Aïmeur, Gilles Brassard, and Jonathan Rioux</i>	
<i>Ransomware and the Legacy Crypto API</i> . . . . .	11
<i>Aurélien Palisse, Hélène Le Boudier, Jean-Louis Lanet, Colas Le Guernic, and Axel Legay</i>	

## Risk and Security Analysis Methodology

<i>A Formal Verification of Safe Update Point Detection in Dynamic Software Updating</i> . . . . .	31
<i>Razika Lounas, Nisrine Jafri, Axel Legay, Mohamed Mezghiche, and Jean-Louis Lanet</i>	
<i>Analyzing the Risk of Authenticity Violation Based on the Structural and Functional Sizes of UML Sequence Diagrams</i> . . . . .	46
<i>Hela Hakim, Asma Sellami, and Hanène Ben Abdallah</i>	
<i>Towards the Weaving of the Characteristics of Good Security Requirements</i> . . . . .	60
<i>Stravani Teja Bulusu, Romain Laborde, Ahmad Samer Wazan, Francois Barrère, and Abdelmalek Benzekri</i>	

## Methodology for Security

<i>Towards Empirical Evaluation of Automated Risk Assessment Methods</i> . . . .	77
<i>Olga Gadyatskaya, Katsiaryna Labunets, and Federica Paci</i>	
<i>An n-Sided Polygonal Model to Calculate the Impact of Cyber Security Events</i> . . . . .	87
<i>Gustavo Gonzalez-Granadillo, Joaquin Garcia-Alfaro, and Hervé Debar</i>	

## Security and Formal Methods

<i>SPTool – Equivalence Checker for SAND Attack Trees</i> . . . . .	105
<i>Barbara Kordy, Piotr Kordy, and Yoann van den Boom</i>	

Formal Verification of a Memory Allocation Module of Contiki with FRAMA-C: A Case Study . . . . .	114
<i>Frédéric Mangano, Simon Duquennoy, and Nikolai Kosmatov</i>	
<b>Network Security</b>	
A Proactive Stateful Firewall for Software Defined Networking . . . . .	123
<i>Salaheddine Zerkane, David Espes, Philippe Le Parc, and Frederic Cuppens</i>	
Protocol Reverse Engineering: Challenges and Obfuscation . . . . .	139
<i>J. Duchêne, C. Le Guernic, E. Alata, V. Nicomette, and M. Kaâniche</i>	
<b>Detection and Monitoring</b>	
Detecting Anomalous Behavior in DBMS Logs . . . . .	147
<i>Muhammad Imran Khan and Simon N. Foley</i>	
Online Link Disclosure Strategies for Social Networks . . . . .	153
<i>Younes Abid, Abdessamad Imine, Amedeo Napoli, Chedy Raïssi, and Michaël Rusinowitch</i>	
A Framework to Reduce the Cost of Monitoring and Diagnosis Using Game Theory . . . . .	169
<i>Rui Abreu, César Andrés, and Ana R. Cavalli</i>	
<b>Cryptography</b>	
High-Performance Elliptic Curve Cryptography by Using the CIOS Method for Modular Multiplication . . . . .	185
<i>Amine Mrabet, Nadia El-Mrabet, Ronan Lashermes, Jean-Baptiste Rigaud, Belgacem Bouallegue, Sihem Mesnager, and Mohsen Machhout</i>	
Improving Side-Channel Attacks Against Pairing-Based Cryptography . . . . .	199
<i>Damien Jauvart, Jacques J.A. Fournier, Nadia El-Mrabet, and Louis Goubin</i>	
A First DFA on PRIDE: From Theory to Practice . . . . .	214
<i>Benjamin Lac, Marc Beunardeau, Anne Canteaut, Jacques J.A. Fournier, and Renaud Sirdey</i>	
<b>Author Index</b> . . . . .	239

Risks and Security of Internet and Systems

11th International Conference, CRiSIS 2016, Roscoff,  
France, September 5-7, 2016, Revised Selected Papers  
Cuppens, F.; Cuppens-Boulahia, N.; Lanet, J.-L.; Legay,  
A. (Eds.)

2017, VIII, 239 p. 67 illus., Softcover

ISBN: 978-3-319-54875-3