Contents

Protection of Personal Data

CLiKC: A Privacy-Mindful Approach When Sharing Data                      3
Esma Aïmeur, Gilles Brassard, and Jonathan Rioux

Ransomware and the Legacy Crypto API                                        11
Aurélien Palisse, Hélène Le Bouder, Jean-Louis Lanet,
Colas Le Guernic, and Axel Legay

Risk and Security Analysis Methodology

A Formal Verification of Safe Update Point Detection in Dynamic Software Updating                                      31
Razika Lounas, Nisrine Jafri, Axel Legay, Mohamed Mezghiche,
and Jean-Louis Lanet

Analyzing the Risk of Authenticity Violation Based on the Structural and Functional Sizes of UML Sequence Diagrams                        46
Hela Hakim, Asma Sellami, and Hanène Ben Abddallah

Towards the Weaving of the Characteristics of Good Security Requirements                                      60
Sravani Teja Bulusu, Romain Laborde, Ahmad Samer Wazan,
Francois Barrère, and Abdelmalek Benzekri

Methodology for Security

Towards Empirical Evaluation of Automated Risk Assessment Methods                         77
Olga Gadyatskaya, Katsiaryna Labunets, and Federica Paci

An n-Sided Polygonal Model to Calculate the Impact of Cyber Security Events                                      87
Gustavo Gonzalez-Granadillo, Joaquin Garcia-Alfaro,
and Hervé Debar

Security and Formal Methods

SPTool – Equivalence Checker for SAND Attack Trees                                                    105
Barbara Kordy, Piotr Kordy, and Yoann van den Boom
Formal Verification of a Memory Allocation Module of Contiki
with FRAMA-C: A Case Study ........................................ 114
Frédéric Mangano, Simon Duquennoy, and Nikolai Kosmatov

Network Security

A Proactive Stateful Firewall for Software Defined Networking ........... 123
Salaheddine Zerkane, David Espes, Philippe Le Parc, and Frederic Cuppens

Protocol Reverse Engineering: Challenges and Obfuscation ............... 139
J. Duchène, C. Le Guernic, E. Alata, V. Nicomette, and M. Kaâniche

Detection and Monitoring

Detecting Anomalous Behavior in DBMS Logs .............................. 147
Muhammad Imran Khan and Simon N. Foley

Online Link Disclosure Strategies for Social Networks .................. 153
Younes Abid, Abdessamad Imine, Amedeo Napoli, Chedy Raïssi, and Michaël Rusinowitch

A Framework to Reduce the Cost of Monitoring and Diagnosis
Using Game Theory ...................................................... 169
Rui Abreu, César Andrés, and Ana R. Cavalli

Cryptography

High-Performance Elliptic Curve Cryptography by Using the CIOS Method
for Modular Multiplication ............................................. 185
Amine Mrabet, Nadia El-Mrabet, Ronan Lashermes, Jean-Baptiste Rigaud, Belgacem Bouallegue, Sihem Mesnager, and Mohsen Machhout

Improving Side-Channel Attacks Against Pairing-Based Cryptography .... 199
Damien Jauvart, Jacques J.A. Fournier, Nadia El-Mrabet, and Louis Goubin

A First DFA on PRIDE: From Theory to Practice .......................... 214
Benjamin Lac, Marc Beunardeau, Anne Canteaut, Jacques J.A. Fournier, and Renaud Sirdey

Author Index .............................................................. 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, N.; Lanet, J.-L.; Legay, A. (Eds.)
2017, VIII, 239 p. 67 illus., Softcover
ISBN: 978-3-319-54875-3