

Table of Contents

Verifying Cryptographic Code in C: Some Experience and the Csec Challenge	1
<i>Mihhail Aizatulin, François Dupressoir, Andrew D. Gordon, and Jan Jürjens</i>	
Better Security and Privacy for Web Browsers: A Survey of Techniques, and a New Implementation	21
<i>Willem De Groef, Dominique Devriese, and Frank Piessens</i>	
Differential Privacy: On the Trade-Off between Utility and Information Leakage	39
<i>Mário S. Alvim, Miguel E. Andrés, Konstantinos Chatzikokolakis, Pierpaolo Degano, and Catuscia Palamidessi</i>	
On-the-Fly Inlining of Dynamic Dependency Monitors for Secure Information Flow	55
<i>Luciano Bello and Eduardo Bonelli</i>	
Min-Entropy Leakage of Channels in Cascade	70
<i>Barbara Espinoza and Geoffrey Smith</i>	
Secure Recharge of Disposable RFID Tickets	85
<i>Riccardo Focardi and Flaminia L. Luccio</i>	
Avoiding Delegation Subterfuge Using Linked Local Permission Names	100
<i>Simon N. Foley and Samane Abdi</i>	
Verifiable Control Flow Policies for Java Bytecode	115
<i>Arnaud Fontaine, Samuel Hym, and Isabelle Simplot-Ryl</i>	
Concepts and Proofs for Configuring PKCS#11	131
<i>Sibylle Fröschle and Nils Sommer</i>	
Service Automata	148
<i>Richard Gay, Heiko Mantel, and Barbara Sprick</i>	
Analysing Applications Layered on Unilaterally Authenticating Protocols	164
<i>Thomas Gibson-Robinson and Gavin Lowe</i>	
Type-Based Enforcement of Secure Programming Guidelines — Code Injection Prevention at SAP	182
<i>Robert Grabowski, Martin Hofmann, and Kegin Li</i>	

TBA : A Hybrid of Logic and Extensional Access Control Systems 198
 Timothy L. Hinrichs, William C. Garrison III, Adam J. Lee,
 Skip Saunders, and John C. Mitchell

Diffie-Hellman without Difficulty 214
 Sebastian Mödersheim

Is Cryptyc Able to Detect Insider Attacks? 230
 Behnam Sattarzadeh and Mehran S. Fallah

Formal Analysis of Anonymity in ECC-Based Direct Anonymous
Attestation Schemes 245
 Ben Smyth, Mark Ryan, and Liqun Chen

Risk Balance in Optimistic Non-repudiation Protocols 263
 Mohammad Torabi Dashti, Jan Cederquist, and Yanjing Wang

Author Index 279