

Contents

Attacks and Vulnerabilities

- On Acoustic Covert Channels Between Air-Gapped Systems 3
Brent Carrara and Carlisle Adams
- Location-Dependent EM Leakage of the ATxmega Microcontroller 17
Thomas Korak

Privacy

- Privacy-Preserving Public Auditing in Cloud Computing
with Data Deduplication. 35
Naelah Alkhajandi and Ali Miri
- A Maximum Variance Approach for Graph Anonymization 49
Hiep H. Nguyen, Abdessamad Imine, and Michaël Rusinowitch
- Privacy by Design: On the Conformance Between Protocols
and Architectures 65
Vinh-Thong Ta and Thibaud Antignac

Software Security and Malware Analysis

- Moving Target Defense Against Cross-Site Scripting
Attacks (Position Paper). 85
Joe Portner, Joel Kerr, and Bill Chu
- Combining High-Level and Low-Level Approaches to Evaluate
Software Implementations Robustness Against Multiple Fault
Injection Attacks. 92
*Lionel Rivi re, Marie-Laure Potet, Thanh-Ha Le, Julien Bringer,
Herv  Chabanne, and Maxime Puy *
- Malware Message Classification by Dynamic Analysis 112
Guillaume Bonfante, Jean-Yves Marion, and Thanh Dinh Ta

Network Security and Protocols

- A Game Approach for an Efficient Intrusion Detection System
in Mobile Ad Hoc Networks 131
Myria Bouhaddi, Mohammed Sa d Radjef, and Kamel Adi

Optimizing TLS for Low Bandwidth Environments	147
<i>Diego A. Ortiz-Yepes</i>	
Automating MAC Spoofer Evidence Gathering and Encoding for Investigations	168
<i>Serguei A. Mokhov, Michael J. Assels, Joey Paquet, and Mourad Debbabi</i>	
Access Control Models and Policy Analysis	
HGABAC: Towards a Formal Model of Hierarchical Attribute-Based Access Control	187
<i>Daniel Servos and Sylvia L. Osborn</i>	
Logical Method for Reasoning About Access Control and Data Flow Control Models.	205
<i>Luigi Logrippo</i>	
A Formal Approach to Verify Completeness and Detect Anomalies in Firewall Security Policies	221
<i>Ahmed Khoumsi, Wadie Krombi, and Mohammed Erradi</i>	
Protocol Verification	
Debating Cybersecurity or Securing a Debate? (Position Paper)	239
<i>Fabio Martinelli and Francesco Santini</i>	
Formal Verification of e-Reputation Protocols.	247
<i>Ali Kassem, Pascal Lafourcade, and Yassine Lakhnech</i>	
(In)Corruptibility of Routing Protocols.	262
<i>Raphaël Jamet and Pascal Lafourcade</i>	
Cryptographic Technologies	
Decentralized CRT-Based Efficient Verifiable (n, t, n) Multi-secret Sharing Scheme	279
<i>Wen Wen, Binod Vaidya, Dimitrios Makrakis, and Carlisle Adams</i>	
Composable Oblivious Extended Permutations	294
<i>Peeter Laud and Jan Willemson</i>	
Benchmarking Encrypted Data Storage in HBase and Cassandra with YCSB	311
<i>Tim Waage and Lena Wiese</i>	

Short Papers

Data Confirmation for Botnet Traffic Analysis	329
<i>Fariba Haddadi and A. Nur Zincir-Heywood</i>	
Detection of Illegal Control Flow in Android System: Protecting Private Data Used by Smartphone Apps	337
<i>Mariem Graa, Nora Cuppens-Boulahia, Frédéric Cuppens, and Ana Cavalli</i>	
A Responsive Defense Mechanism Against DDoS Attacks	347
<i>Negar Mosharraf, Anura P. Jayasumana, and Indrakshi Ray</i>	
Automated Extraction of Vulnerability Information for Home Computer Security	356
<i>Sachini Weerawardhana, Subhojeet Mukherjee, Indrajit Ray, and Adele Howe</i>	
A Formal Approach to Automatic Testing of Security Policies Specified in XACML	367
<i>Mohamed H.E. Aouadi, Khalifa Toumi, and Ana Cavalli</i>	
Author Index	375

Foundations and Practice of Security

7th International Symposium, FPS 2014, Montreal, QC,
Canada, November 3-5, 2014. Revised Selected Papers
Cuppens, F.; Garcia-Alfaro, J.; Zinic-Heywood, N.; Fong,
P.W.L. (Eds.)

2015, XIII, 375 p. 98 illus., Softcover

ISBN: 978-3-319-17039-8