1. Record Nr.	UNINA9910484580203321
Titolo	Foundations and Practice of Security : 6th International Symposium, FPS 2013, La Rochelle, France, October 21-22, 2013, Revised Selected Papers / / edited by Jean Luc Danger, Mourad Debbabi, Jean-Yves Marion, Joaquin Garcia-Alfaro, Nur Zincir Heywood
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-05302-7
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XIII, 444 p. 134 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 8352
Disciplina	005.8
Soggetti	Cryptography
	Data encryption (Computer science)
	Data protection
	Coding theory
	Information theory
	Cryptology
	Data and Information Security
	Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	On the Efficiency of Mathematics in Intrusion Detection: The NetEntropy Case -- On the Feasibility of a Censorship Resistant Decentralized Naming System -- A General Framework for Group Authentication and Key Exchange Protocols -- Modelling Simultaneous Mutual Authentication for Authenticated Key Exchange -- Model-Based Specification and Validation of Security and Dependability Patterns -- Enforcing Information Flow by Combining Static and Dynamic Analysis -- Fault Injection to Reverse Engineer DES-like Cryptosystems -- Software Camouflage -- Investigation of Parameters Influencing the Success of Optical Fault Attacks -- ONTIDS: A Highly Flexible Context-Aware and Ontology-Based Alert Correlation Framework -- Quantitative Evaluation of Enforcement Strategies -- Collusion Resistant Inference Control for Cadastral Databases -- Leveraging Ontologies upon a

Holistic Privacy-Aware Access Control Model -- Formal Modelling of Content-Based Protection and Release for Access Control in NATO Operations -- Computational Soundness of Symbolic Blind Signatures under Active Attacker -- Improved Davies-Murphys Attack on DES Revisited -- Yet Another Fault-Based Leakage in Non-Uniform Faulty Ciphertexts -- A Hierarchal Anti-Counterfeit Mechanism: Securing the Supply Chain using RFIDs -- A More Realistic Model For Verifying Route Validity in Ad-Hoc Networks -- On the Security of a Privacy-Preserving Key Management Scheme for Location Based Services in VANETs -- CheR: Cheating Resilience in the Cloud via Smart Resource Allocation -- Evaluation of Software-Oriented Block Ciphers on Smartphones -- Don't Push it: Breaking iButton Security -- Discovering Flaws in IDS through Analysis of their Inputs -- On the Reverse Engineering of the Citadel Botnet -- The Carna Botnet Through the Lens of a Network Telescope.

| Sommario/riassunto | This book constitutes the carefully refereed post-proceedings of the 6th Symposium on Foundations and Practice of Security, FPS 2013, held in La Rochelle, France, in October 2013. The 25 revised full papers presented together with a keynote address were carefully reviewed and selected from 65 submissions. The papers are organized in topical sections on security protocols, formal methods, physical security, attack classification and assessment, access control, cipher attacks, ad-hoc and sensor networks, resilience and intrusion detection. |