

1. Record Nr.	UNISA996203270903316
Titolo	Principles of Security and Trust [[electronic resource]] : Third International Conference, POST 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014, Proceedings / / edited by Martín Abadi, Steve Kremer
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
ISBN	3-642-54792-3
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XVIII, 307 p. 48 illus.)
Collana	Security and Cryptology ; ; 8414
Disciplina	005.8
Soggetti	Computer security Computer communication systems Data encryption (Computer science) E-commerce Management information systems Computer science Algorithms Systems and Data Security Computer Communication Networks Cryptology e-Commerce/e-business Management of Computing and Information Systems Algorithm Analysis and Problem Complexity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and author index.
Nota di contenuto	A Reduced Semantics for Deciding Trace Equivalence Using Constraint Systems -- Stateful Applied Pi Calculus -- Computational Soundness Results for ProVerif: Bridging the Gap from Trace Properties to Uniformity -- A Secure Key Management Interface with Asymmetric Cryptography -- Quantitative Aspects of Information Flow Abstract Channels and Their Robust Information-Leakage Ordering --

Quantitative Information Flow in Boolean Programs -- When Not All Bits Are Equal: Worth-Based Information Flow -- Leakage Resilience against Concurrent Cache Attacks -- Information Flow Control in WebKit's JavaScript Bytecode -- A Separation Logic for Enforcing Declarative Information Flow Control Policies -- Defining and Enforcing Referential Security -- Extending and Applying a Framework for the Cryptographic Verification of Java Programs -- Compiling CAO: From Cryptographic Specifications to C Implementations -- Decentralized Composite Access Control -- Temporal Logics for Hyperproperties -- Time-Dependent Analysis of Attacks.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third International Conference on Principles of Security and Trust, POST 2014, held as part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, in April 2014. The 15 papers presented in this volume were carefully reviewed and selected from 55 submissions. They are organized in topical sections named: analysis of cryptographic protocols; quantitative aspects of information flow; information flow control in programming languages; cryptography in implementations and policies and attacks.
