1.	Record Nr.	UNISA996466008803316
	Titolo	Information Security [[electronic resource]] : Third International Workshop, ISW 2000, Wollongong, Australia, December 20-21, 2000. Proceedings / / edited by Josef Pieprzyk, Eiji Okamoto, Jennifer Seberry
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
	ISBN	3-540-44456-4
	Edizione	[1st ed. 2000.]
	Descrizione fisica	1 online resource (X, 322 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1975
	Disciplina	005.8
	Soggetti	Data encryption (Computer science)
		Computer communication systems
		Algorithms
		Operating systems (Computers)
		Management information systems
		Computer science
		Cryptology
		Computer Communication Networks
		Algorithm Analysis and Problem Complexity
		Operating Systems
		Management of Computing and Information Systems
	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 at the end of each chapters and index.
	Nota di contenuto	Multimedia Copyright Protection -- A Watermarking Scheme Based on the Characteristic of Addition among DCT Coefficients -- Affine Invariant Watermarks for 3D Polygonal and NURBS Based Models -- A Steganographic Framework for Reference Colour Based Encoding and Cover Image Selection -- Spatial-Domain Image Watermarking Robust against Compression, Filtering, Cropping, and Scaling -- Region-Based Watermarking by Distribution Adjustment -- Hiding Information in Color Images Using Small Color Palettes -- An Approach to the Objective and Quantitative Evaluation of Tamper-Resistant Software -- Characteristics of Some Binary Codes for Fingerprinting -- E-

Commerce -- An Anonymous Auction Protocol with a Single Non-trusted Center Using Binary Trees -- Unlinkable Divisible Electronic Cash -- Weighted One-Way Hash Chain and Its Applications -- Linkability in Practical Electronic Cash Design -- Towards a Practical Secure Framework for Mobile Code Commerce -- Key Management -- Probabilistic Methods in Multicast Key Management -- Classification of Authentication Protocols: A Practical Approach -- Exploring Fair Exchange Protocols Using Specification Animation -- A Practical Implementation of Hierarchically Structured Key Predistribution System and Its Evaluation -- Network Security and Access Control -- An Efficient Protocol for Certified Electronic Mail -- Performance Analysis of Secure Web Server Based on SSL -- Sherlock: Commercial High Assurance Network Computing Extended Abstract -- The Role of the Development Process in Operating System Security -- Cryptographic Systems -- Threshold Fail-Stop Signature Schemes Based on Discrete Logarithm and Factorization -- A Signcryption Scheme Based on Integer Factorization.

Sommario/riassunto	The third International Workshop on Information Security was held at the U- versity of Wollongong, Australia. The conference was sponsored by the Centre for Computer Security Research, University of Wollongong. The main themes of the conference were the newly emerging issues of Information Security. Mul- media copyright protection and security aspects of e-commerce were two topics that clearly re?ect the focus of the conference. Protection of the copyright of electronic documents seems to be driven by strong practical demand from the industry for new, e cient and secure solutions. Although e-commerce is already booming, it has not reached its full potential in terms of new, e cient and secure e-commerce protocols with added properties. There were 63 papers submitted to the conference. The program committee accepted 23. Of those accepted, six papers were from Australia, ve from Japan, two each from Spain, Germany and the USA, and one each from Finland and Sweden. Four papers were co-authored by international teams from Canada and China, Korea and Australia, Taiwan and Australia, and Belgium, France and Germany, respectively. Final versions of the accepted papers were gathered using computing and other resources of the Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland. We are especially grateful to Jerzy Urbanowicz and Andrzej Pokrzywa for their help during preparation of the proceedings.