1. Record Nr.	UNISA996466251403316
Titolo	Information security : 11th international conference, ISC 2008, Taipei, Taiwan, September 15-18, 2008, proceedings / / Tzong-Chen Wu [and three others] (editors)
Pubbl/distr/stampa	Berlin ; ; Heidelberg : , : Springer, , [2008] ©2008
ISBN	3-540-85886-5
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XV, 504 p.)
Collana	Lecture notes in computer science ; ; 5222
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Trusted Computing -- Property-Based TPM Virtualization -- A Demonstrative Ad Hoc Attestation System -- Property-Based Attestation without a Trusted Third Party -- The Reduced Address Space (RAS) for Application Memory Authentication -- Database and System Security -- An Efficient PIR Construction Using Trusted Hardware -- Athos: Efficient Authentication of Outsourced File Systems -- BotTracer: Execution-Based Bot-Like Malware Detection -- Intrusion Detection -- Towards Automatically Generating Double-Free Vulnerability Signatures Using Petri Nets -- Distinguishing between FE and DDoS Using Randomness Check -- Network Security -- Antisocial Networks: Turning a Social Network into a Botnet -- Compromising Anonymity Using Packet Spinning -- Behavior-Based Network Access Control: A Proof-of-Concept -- Path-Based Access Control for Enterprise Networks -- Cryptanalysis -- Cryptanalysis of Rabbit -- Algebraic Attack on HFE Revisited -- Revisiting Wiener’s Attack – New Weak Keys in RSA -- Deterministic Constructions of 21-Step Collisions for the SHA-2 Hash Family -- Digital Signatures -- Proxy Re-signatures in the Standard Model -- An RSA-Based (t,n) Threshold Proxy Signature Scheme without Any Trusted Combiner -- Certificate-Based Signature Schemes without Pairings or Random Oracles -- AES Special Session -- Improved Impossible Differential Attacks on Large-Block Rijndael -- A Five-Round Algebraic Property of the Advanced Encryption Standard --

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Conference on Information Security Conference, ISC 2008, held in Taipei, Taiwan, September 15-18, 2008. The 33 revised full papers presented were carefully reviewed and selected from 134 submissions. The papers are organized in topical sections on trusted computing, database and system security, intrusion detection, network security, cryptanalysis, digital signatures, AES, symmetric cryptography and hash functions, authentication as well as security protocols.