1. Record Nr. UNINA9910483667703321

Titolo	Information Security : 9th International Conference; ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings / / edited by Sokratis K. Katsikas, Michael Backes, Stefanos Gritzalis, Bart Preneel
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-38343-3
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 548 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4176
Altri autori (Persone)	KatsikasSokratis K
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Operating systems (Computers) Algorithms Computer networks Computers, Special purpose Electronic data processing - Management Cryptology Operating Systems Computer Communication Networks Special Purpose and Application-Based Systems IT Operations
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 index.
Nota di contenuto	Software Security -- Extending .NET Security to Unmanaged Code -- Transparent Run-Time Prevention of Format-String Attacks Via Dynamic Taint and Flexible Validation -- Privacy and Anonymity -- Low Latency Anonymity with Mix Rings -- Breaking Four Mix-Related Schemes Based on Universal Re-encryption -- Weak k-Anonymity: A Low-Distortion Model for Protecting Privacy -- Protecting Data Privacy Through Hard-to-Reverse Negative Databases -- Block Ciphers and Hash Functions -- Related-Key Rectangle Attack on 42-Round SHACAL-2 -- On the Collision Resistance of RIPEMD-160 -- Digital

Signatures -- Blind Ring Signatures Secure Under the Chosen-Target-CDH Assumption -- Multi-party Concurrent Signatures -- Formal Security Model of Multisignatures -- Cryptanalysis of Variants of UOV -- Stream Ciphers -- Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles -- Cryptanalysis of the Bluetooth E 0 Cipher Using OBDD's -- Encryption I -- A Partial Key Exposure Attack on RSA Using a 2-Dimensional Lattice -- On the Integration of Public Key Data Encryption and Public Key Encryption with Keyword Search -- Collusion-Free Policy-Based Encryption -- Pervasive Computing -- Using Multiple Smart Cards for Signing Messages at Malicious Terminals -- Diverging Keys in Wireless Sensor Networks -- Encryption II -- A Generic Transformation from Symmetric to Asymmetric Broadcast Encryption -- Transparent Image Encryption Using Progressive JPEG -- Network Security -- Preserving TCP Connections Across Host Address Changes -- A Security Architecture for Protecting LAN Interactions -- Simulation of Internet DDoS Attacks and Defense -- SNOOZE: Toward a Stateful NetwOrk prOtocol fuzZEr -- Watermarking and DRM -- Rights Protection for Data Cubes -- An Efficient Probabilistic Packet Marking Scheme (NOD-PPM) -- IntrusionDetection and Worms -- Resistance Analysis to Intruders' Evasion of Detecting Intrusion -- A Wireless Intrusion Detection System for Secure Clustering and Routing in Ad Hoc Networks -- Anomaly Intrusion Detection Based on Clustering a Data Stream -- Robust Reactions to Potential Day-Zero Worms Through Cooperation and Validation -- Key Exchange -- An Authentication and Key Exchange Protocol for Secure Credential Services -- A Non-malleable Group Key Exchange Protocol Robust Against Active Insiders -- Security Protocols and Formal Methods -- Formalising Receipt-Freeness -- Enhancing the Security and Efficiency of 3-D Secure -- Designing and Verifying Core Protocols for Location Privacy -- Information Systems Security -- Delegation in a Distributed Healthcare Context: A Survey of Current Approaches -- Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness.

Sommario/riassunto

th This volume contains the papers presented at the 9 Information Security Conference (ISC 2006) held on Samos Island, Greece, during August 30 – September 2, 2006. The Conference was organized by the University of the Aegean, Greece. ISC was first initiated as a workshop, ISW in Japan in 1997, ISW 1999 in Mal- sia, ISW 2000 in Australia and then changed to the current name ISC when it was held in Spain in 2001 (ISC 2001). The latest conferences were held in Brazil (ISC 2002), UK (ISC 2003), USA (ISC 2004), and Singapore (ISC 2005). ISC 2006 provided an international forum for sharing original research results and application experiences among specialists in fundamental and applied problems of - formation security. In response to the Call for Papers, 188 papers were submitted. Each paper was - viewed by three members of the PC, on the basis of their significance, novelty, and technical quality. Of the papers submitted, 38 were selected for presentation, with an acceptance rate of 20%.