1. Record Nr. UNINA9910483083703321

Titolo	Information security and cryptology : second SKLOIS conference, Inscrypt 2006, Beijing, China, November 29-December 1, 2006 : proceedings / / Helger Lipmaa, Moti Yung, Dongdai Lin (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, c2006
ISBN	3-540-49610-6
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 308 p.)
Collana	LNCS sublibrary. SL 4, Security and cryptology Lecture notes in computer science, , 0302-9743 ; ; 4318
Altri autori (Persone)	LipmaaHelger YungMoti LinDongdai
Disciplina	005.8/2
Soggetti	Computer security Cryptography
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	Digital Signature Schemes -- Cryptanalysis of Two Signature Schemes Based on Bilinear Pairings in CISC '05 -- Identity-Based Key-Insulated Signature with Secure Key-Updates -- Efficient Intrusion-Resilient Signatures Without Random Oracles -- Sequences and Stream Ciphers -- New Constructions of Large Binary Sequences Family with Low Correlation -- On the Rate of Coincidence of Two Clock-Controlled Combiners -- Symmetric-Key Cryptography -- Designing Power Analysis Resistant and High Performance Block Cipher Coprocessor Using WDDL and Wave-Pipelining -- OPMAC: One-Key Poly1305 MAC -- A General Construction of Tweakable Block Ciphers and Different Modes of Operations -- Cryptographic Schemes -- Dynamic Threshold and Cheater Resistance for Shamir Secret Sharing Scheme -- Efficient Short Signcryption Scheme with Public Verifiability -- A Revocation Scheme Preserving Privacy -- Network Security -- Deterministic Packet Marking with Link Signatures for IP Traceback -- Survey and Taxonomy of Feature Selection Algorithms in Intrusion Detection System -- A Network Security Policy Model and Its Realization Mechanism -- Packet Marking Based Cooperative Attack Response Service for Effectively

Handling Suspicious Traffic -- Access Control -- A Verifiable Formal Specification for RBAC Model with Constraints of Separation of Duty -- Design and Implementation of Fast Access Control That Supports the Separation of Duty -- Computer and Applications Security -- A Practical Alternative to Domain and Type Enforcement Integrity Formal Models -- Return Address Randomization Scheme for Annuling Data-Injection Buffer Overflow Attacks -- Application and Evaluation of Bayesian Filter for Chinese Spam -- Web and Media Security -- Batch Decryption of Encrypted Short Messages and Its Application on Concurrent SSL Handshakes -- An Enterprise Security Management System as a Web-Based Application Service for Small/Medium Businesses -- Obtaining Asymptotic Fingerprint Codes Through a New Analysis of the Boneh-Shaw Codes.

Sommario/riassunto

The second SKLOIS Conference on Information Security and Cryptology 2006 (Inscrypt, formerly CISC) was organized by the State Key Laboratory of Inf- mation Security of the Chinese Academy of Sciences. This international conf- ence was held in Beijing, China and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate University of Chinese Academy of Sciences and the National Natural Science Foundations of China. The c- ference proceedings, with contributed papers, are published by Springer in this volume of Lecture Notes in Computer Science (LNCS). The research areas covered by Inscrypt have been gaining increased visibility recently since modern computing and communication infrastructures and app- cations require increased security, trust and safety. Indeed important fundam- tal, experimental and applied work has been done in wide areasof cryptography and information security research in recent years. Accordingly, the program of Inscrypt 2006 covered numerous ?elds of research within these areas. The International Program Committee of the conference received a total of 225 submissions, from which only 23 submissions were selected for presentation at the regular papers track and are part of this volume. In addition to this track, the conference also hosted a short paper track of 13 presentations that were carefully selected as well. All anonymous submissions were reviewed by experts in the relevant areas and based on their ranking, technical remarks and strict selection criteria the papers were selected to the various tracks.