1. Record Nr. UNISA996465956303316

| | |
|---|---|
| Titolo | Cyberspace Safety and Security [[electronic resource] ] : 4th International Symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012, Proceedings / / edited by Yang Xiang, Javier Lopez, C.-C. Jay Kuo, Wanlei Zhou |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012 |
| ISBN | 3-642-35362-2 |
| Edizione | [1st ed. 2012.] |
| Descrizione fisica | 1 online resource (XIV, 510 p. 226 illus.) |
| Collana | Security and Cryptology ; ; 7672 |
| Disciplina | 005.8 |
| Soggetti | Computer security<br>Computer communication systems<br>Data encryption (Computer science)<br>Algorithms<br>Application software<br>Management information systems<br>Computer science<br>Systems and Data Security<br>Computer Communication Networks<br>Cryptology<br>Algorithm Analysis and Problem Complexity<br>Information Systems Applications (incl. Internet)<br>Management of Computing and Information Systems |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | International conference proceedings. |
| Nota di bibliografia | Includes bibliographical references and author index. |
| Nota di contenuto | CSS 2012 Regular Papers -- Session 1: Mobile Security -- Identity and Its Authentication Protocol for Secure Mobile Commerce Applications -- SafeCode – Safeguarding Security and Privacy of User Data on Stolen iOS Devices -- Protection Aspects of Iconic Passwords on Mobile Devices -- Detecting Control Flow in Smarphones: Combining Static and Dynamic Analyses -- Session 2: Cyberspace Attacks and Defense -- A Multi-tier Ensemble Construction of Classifiers for Phishing Email |

Detection and Filtering -- Chattering-Free Terminal Sliding-Mode Observer for Anomaly Detection -- Detecting Illicit Drugs on Social Media Using Automated Social Media Intelligence Analysis (ASMIA) -- Improving Content Availability in the I2P Anonymous File-Sharing Environment -- Session 3: Security Applications and Systems -- V2GPriv: Vehicle-to-Grid Privacy in the Smart Grid -- A Secure Architecture for Smart Meter Systems -- A Novel Identity-Based Key Management and Encryption Scheme for Distributed System -- An Anomaly Based Approach for HID Attack Detection Using Keystroke Dynamics -- Robust Authentication of Public Access Points Using Digital Certificates – A Novel Approach -- Session 4: Network and Cloud Security -- General Transformation from KP-ABE to Searchable Encryption -- Supporting Security and Consistency for Cloud Database -- Proxy Re-encryption in a Privacy-Preserving Cloud Computing DRM Scheme -- Collaborative Behavior Visualization and Its Detection by Observing Darknet Traffic -- SSH – Somewhat Secure Host -- Session 5: Security Models -- Physical Access Control Administration Using Building Information Models -- Multiple Factors Based Evaluation of Fingerprint Images Quality -- A Leakage-Resilient Zero Knowledge Proof for Lattice Problem -- MDSE@R: Model-Driven Security Engineering at Runtime -- Session 6: Wireless Security -- A Hash Chains Based Key Management Scheme for Wireless Sensor Networks -- An Event-Based Packet Dropping Detection Scheme for Wireless Mesh Networks -- A State-Aware RFID Privacy Model with Reader Corruption -- An Improved Anti-collision Algorithm for ISO15693 RFID Systems -- Session 7: Security Protocols -- Near-Optimal Collusion-Secure Fingerprinting Codes for Efficiently Tracing Illegal Re-distribution -- A Forward-Secure Certificate-Based Signature Scheme in the Standard Model -- Policy-Based Vulnerability Assessment for Virtual Organisations -- Constant-Ciphertext-Size Dual Policy Attribute Based Encryption -- Session 8: Industry Track: Future of Cyberspace Security and Safety -- Sophisticated Phishers Make More Spelling Mistakes: Using URL Similarity against Phishing -- Secure Mobility Management Based on Session Key Agreements -- Taxonomy and Proposed Architecture of Intrusion Detection and Prevention Systems for Cloud Computing -- Portability Evaluation of Cryptographic Libraries on Android Smartphones -- Secure Middleware Patterns -- Intrusion Detection Using Disagreement-Based Semi-supervised Learning: Detection Enhancement and False Alarm Reduction -- Towards Effective Algorithms for Intelligent Defense Systems.

Sommario/riassunto

This book constitutes the refereed proceedings of the 4th International Symposium on Cyberspace Safety and Security (CSS 2012), held in Melbourne, Australia, in December 2012. The 30 revised full papers presented together with 7 invited talks were carefully reviewed and selected from 105 submissions. The papers cover the following topics: mobile security, cyberspace attacks and defense, security application adn systems, network and cloud security, wireless security, security protocols and models.