1. Record Nr. UNISA996476470403316

Titolo	Revista Argentina de investigación educativa
Pubbl/distr/stampa	Ciudad Autónoma de Buenos Aires, Argentina : , : Universidad Pedagógica Nacional
ISSN	2796-7433
Descrizione fisica	1 online resource (volumes)
Disciplina	370.982
Soggetti	Education Education and state - Argentina Education - Periodicals Periodicals. Argentina
Lingua di pubblicazione	Spagnolo
Formato	Materiale a stampa
Livello bibliografico	Periodico
Note generali	Each volume bears also a thematic title.
Sommario/riassunto	Devoted to research and scholarship in education.

2. Record Nr. UNINA9910484546603321

Titolo	Computer Security -- ESORICS 2015 : 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part II / / edited by Günther Pernul, Peter Y A Ryan, Edgar Weippl
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-24177-X
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVII, 665 p. 124 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 9327
Disciplina	005.8
Soggetti	Data protection Cryptography Data encryption (Computer science) Electronic data processing - Management Algorithms Computers and civilization Data and Information Security Cryptology IT Operations Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Foreword -- Organization -- Contents - Part II -- Contents - Part I -- Privacy -- FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting -- 1 Introduction -- 2 Related Work -- 2.1 Fingerprinting -- 2.2 Countermeasures -- 3 Determining the Fingerprint Surface -- 3.1 Limitations of Preventing Fingerprint Tracking -- 3.2 Fingerprint Vectors -- 3.3 Fingerprint Surface -- 4 Design -- 4.1 Balancing Usability vs. Privacy -- 4.2 Generating Web Identities -- 5 Development and Implementation -- 5.1 Development -- 5.2 Implementation -- 6 Experiments and Validation -- 7 Conclusions -- References -- Mind-Reading: Privacy Attacks Exploiting Cross-App KeyEvent Injections -- 1 Introduction -- 2 Background and

Adversary Model -- 2.1 IME and Personalized User Dictionary -- 2.2 Adversary Model -- 3 Vulnerability Analysis -- 3.1 Android KeyEvent Processing Flow -- 3.2 Cross-App KeyEvent Injection Vulnerability -- 4 Attack -- 4.1 Enumerating Entries from Dictionary -- 4.2 Attack in Stealthy Mode -- 4.3 Case Study of IMEs for Non-Latin Languages -- 5 Evaluation -- 5.1 Scope of Attack -- 5.2 Experiment on Word Completion Attack Mode -- 5.3 Experiment on Next-Word Prediction Attack Mode -- 6 Defense -- 7 Related Works -- 8 Conclusion -- References -- Enabling Privacy-Assured Similarity Retrieval over Millions of Encrypted Records -- 1 Introduction -- 2 Related Works -- 3 Preliminaries -- 4 Notations and Definitions -- 5 Our Proposed Schemes -- 5.1 Main Scheme -- 5.2 Dynamic Scheme -- 6 Security Analysis -- 7 Implementation and Evaluation -- 8 Conclusion -- A Definition of Locality-Sensitive Hashing -- B Simulation-Based Security Definition -- C Security Proofs -- D Comparison with Prior Work -- E Bandwidth Consumption Switch Appendix D with Appendix E -- References -- Privacy-Preserving Link Prediction in Decentralized Online Social Networks.
1 Introduction -- 2 Related Work -- 3 System Model and Privacy Goals -- 3.1 Network Abstraction -- 3.2 Training Goal -- 3.3 Prediction Goal -- 4 Methodology -- 4.1 ADMM -- 4.2 Two-Tier Training -- 4.3 Complexity Analysis -- 4.4 Protecting Prior Knowledge -- 5 Experimentation and Evaluation -- 5.1 Wikipedia RfA Dataset -- 5.2 Experimental Setup -- 5.3 Evaluation Metrics -- 5.4 Results -- 6 Conclusion -- A Appendix: Link Reconstruction Attack -- A.1 Experimental Setup -- A.2 Results -- References -- Privacy-Preserving Observation in Public Spaces -- 1 Introduction -- 2 Related Work -- 2.1 Privacy-Preserving Billing -- 2.2 Threat Model -- 3 Collusion Attack -- 3.1 Model -- 3.2 Collusion Strategy -- 3.3 Analysis -- 4 Privacy-Preserving Spot Checking -- 4.1 Setup and Registration -- 4.2 Security Properties -- 4.3 Protocol -- 4.4 Optimization -- 4.5 Efficiency Analysis -- 4.6 Rate Limiting -- 4.7 Disposal -- 5 Example Application -- 6 Conclusions -- A Privacy vs. Penalty Analysis -- A.1 Variables -- A.2 Analysis -- References -- Privacy-Preserving Context-Aware Recommender Systems: Analysis and New Solutions -- 1 Introduction -- 1.1 State-of-the-Art -- 1.2 Our Contribution -- 1.3 Organization -- 2 Analysis of JPH Protocols -- 2.1 Preliminary of JPH Protocols -- 2.2 JPH Online Protocol -- 2.3 JPH Offline Protocol -- 3 New Formulation of Recommender System -- 3.1 Computing Predicted Ratings -- 3.2 Threat Model -- 4 New Privacy-Preserving Recommender Protocols -- 4.1 Recommendation Protocol for Single Prediction -- 4.2 Recommendation Protocol for Top-N Items -- 5 Evaluating the Proposed Protocols -- 6 Conclusion -- References -- Cloud Security -- Rich Queries on Encrypted Data: Beyond Exact Matches -- 1 Introduction -- 2 Preliminaries -- 3 Range Queries -- 4 Substring Queries -- 4.1 Basic SSE Substring Search -- 4.2 Wildcards and Phrase Queries.
4.3 Substring Protocol Extensions -- 5 Security Analysis -- A Implementation and Performance -- References -- Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data -- 1 Introduction -- 2 Related Work -- 3 Proposed Revocable Cloud Data Encryption Model -- 3.1 System Overview -- 3.2 Notations -- 3.3 Extended Proxy-Assisted User Revocation Approach -- 3.4 Formulation of Revocable Cloud Data Encryption -- 4 Our Construction -- 4.1 Construction Details -- 4.2 Functional Analysis -- Features -- 4.3 Security Analysis -- 5 Implementation of Our Construction -- 5.1 Proof-of-Concept -- 5.2 Performance Results -- 6 Conclusion -- References -- Batch Verifiable Computation of

Polynomials on Outsourced Data -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Overview of the Constructions -- 1.3 Related Work -- 1.4 Organization -- 2 Preliminaries -- 2.1 Batch Verifiable Computation on Outsourced Data -- 2.2 A Lemma -- 3 Constructions -- 3.1 The First Construction -- 3.2 The Second Construction -- 4 Analysis -- 5 Concluding Remarks -- A Proof of Lemma 1 -- References -- CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud -- 1 Introduction -- 2 Problem Formulation: Outsourcing Computation of Biometric Identification -- 2.1 System Model and Assumptions -- 2.2 Threat Model -- 3 Privacy-Preserving Biometric Identification: An Examination of the State-of-the-Art -- 3.1 The Biometric Identification Scheme of Huang et al. -- 3.2 The Biometric Identification Scheme of Yuan et al. -- 4 Our Construction: The New and Improved Solutions -- 4.1 CloudBI-I: The Basic Scheme -- 4.2 CloudBI-II: The Enhanced Scheme -- 5 Implementation and Evaluation -- 5.1 Complexity Analysis -- 5.2 Experimental Evaluation -- 6 Concluding Remarks -- A Attack on Yuan et al. by Eliminating Randomness.
B Attack on Yuan et al. by Exploiting Euclidian Distance Results -- References -- Protocols and Attribute-based Encryption -- Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment -- 1 Introduction -- 2 Messages, Formats and the Intruder Model -- 2.1 Messages -- 2.2 Formats -- 2.3 Intruder Knowledge and Deduction Rules -- 3 Protocol Semantics -- 3.1 Symbolic Constraints -- 3.2 Operational Strands -- 3.3 Goal Predicates in the Geometric Fragment -- 4 Constraint Solving -- 4.1 From Geometric Fragment to Symbolic Constraints -- 4.2 Constraint Reduction -- 5 Typed Model -- 5.1 Message Patterns -- 6 Parallel Composition -- 7 Tool Support -- 8 Conclusions and Related Work -- A Appendix: Proofs of the Technical Results -- References -- Checking Trace Equivalence: How to Get Rid of Nonces? -- 1 Introduction -- 2 Model for Security Protocols -- 2.1 Term Algebra -- 2.2 Process Algebra -- 2.3 Semantics -- 2.4 Trace Equivalence -- 3 Main Contribution: Getting Rid of Nonces -- 3.1 Our Hypotheses -- 3.2 Our Transformation -- 3.3 Main Result -- 3.4 Sketch of Proof -- 4 Scope of Our Result -- 4.1 Simple Processes -- 4.2 Adequate Theories -- 5 Application of Our Result -- 5.1 Is Our Abstraction Precise Enough? -- 5.2 Proof Technique -- 6 Conclusion -- A Appendix -- References -- Attribute Based Broadcast Encryption with Short Ciphertext and Decryption Key -- 1 Introduction -- 2 Preliminaries -- 2.1 Bilinear Map on Prime Order Groups -- 2.2 The Viete's formulas -- 2.3 Access Structure -- 2.4 KP-ABBE Definition -- 2.5 CP-ABBE Definition -- 3 KP-ABBE Scheme -- 4 CP-ABBE Scheme -- 5 Security Analysis -- 6 Conclusion -- References -- Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Our Technique.
1.3 Related Work -- 1.4 Organization -- 2 Background -- 2.1 Notation -- 2.2 Access Policy -- 2.3 Linear Secret-Sharing Schemes -- 2.4 Composite Order Bilinear Groups -- 2.5 Complexity Assumptions -- 2.6 Zero-Knowledge Proof of Knowledge of Discrete Log -- 3 Accountable Authority CP-ABE with White-Box Traceability and Public Auditing -- 3.1 Definition -- 3.2 Security -- 4 Our System -- 4.1 Construction -- 4.2 IND-CPA Security -- 4.3 DishonestAuthority Security -- 4.4 DishonestUser Security -- 4.5 Key Sanity Check Proof -- 5 Conclusion and Future Work -- A Proof of Lemma 2 -- B Proof of Theorem 2 -- C Proof Sketch of Theorem 3 -- D Proof of Theorem 4 -- References -- Code Analysis and Side-Channels -- DexHunter: Toward

Extracting Hidden Code from Packed Android Applications -- 1 Introduction -- 2 Analysis of Packing Services -- 2.1 Common Techniques Used by Packing Services -- 2.2 Packers Under Investigation -- 3 DexHunter: Goal and Basic Idea -- 3.1 Basic Idea -- 3.2 ART -- 3.3 DVM -- 4 DexHunter: Design and Implementation -- 4.1 Architecture -- 4.2 Locating and Dumping Dex Files -- 4.3 Proactive Class Loading and Initialization -- 4.4 Identifying Packers -- 4.5 Extracting the Values of location_ and fileName -- 5 Evaluation -- 5.1 Overhead Introduced by Packers -- 5.2 DexHunter's Effectiveness -- 5.3 DexHunter's Efficiency -- 6 Discussion -- 7 Related Work -- 8 Conclusion -- References -- Identifying Arbitrary Memory Access Vulnerabilities in Privilege-Separated Software -- 1 Introduction -- 2 Problem Overview -- 2.1 Motivating Example -- 2.2 Problem Definition -- 2.3 Memory Access Patterns to Detect DUIs -- 3 Design -- 3.1 Overview -- 3.2 Suspicious Instruction Shortlisting -- 3.3 Dereference Behavior Analysis -- 4 Implementation -- 4.1 Taint Propagation -- 4.2 Access Formula Generation -- 5 Evaluation -- 5.1 Efficacy -- 5.2 Performance.
5.3 Security Implications.

Sommario/riassunto

The two-volume set, LNCS 9326 and LNCS 9327 constitutes the refereed proceedings of the 20th European Symposium on Research in Computer Security, ESORICS 2015, held in Vienna, Austria, in September 2015. The 59 revised full papers presented were carefully reviewed and selected from 298 submissions. The papers address issues such as networks and Web security; system security; crypto application and attacks; risk analysis; privacy; cloud security; protocols and attribute-based encryption; code analysis and side-channels; detection and monitoring; authentication; policies; and applied security.

3.

Record Nr.	UNISA996684481703316
Autore	FAUCEGLIA, Giuseppe
Titolo	[Ammortamento di assegno circolare in bianco e terzo in buona fede] / [Giuseppe Fauceglia]
Pubbl/distr/stampa	Milano, : Giuffrè, [1986]
Descrizione fisica	327-332 p. ; 24 cm
Disciplina	332
Soggetti	Assegni circolari - Ammortamento - Sentenze - Annotazione
Collocazione	XVI.7.Misc. 169
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Titolo dell'intitolazione Nome dell'autore a p. 330 Estratto da: Giurisprudenza di merito : rivista bimestrale di giurisprudenza dei giudici di merito, anno 18, n. 2 (mar.-apr. 1986) Contiene: Titoli di credito, assegno circolare, sottrazione di moduli, ammortamento, inammissibilità : Tribunale di Roma, 25 luglio 1984, Pres. Pannunzio, Est. Ferraro, Credito italiano spa.