1. Record Nr. UNISA996466469903316

Titolo	Computer Security -- ESORICS 2015 [[electronic resource]] : 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I / / edited by Günther Pernul, Peter Y A Ryan, Edgar Weippl
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-24174-5
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVIII, 543 p. 114 illus. in color.)
Collana	Security and Cryptology ; ; 9326
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Management information systems Computer science Algorithms Computers and civilization Systems and Data Security Cryptology Management of Computing and Information Systems Algorithm Analysis and Problem Complexity 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 I -- Contents - Part II -- Networks and Web Security -- Towards Security of Internet Naming Infrastructure -- 1 Introduction -- 2 Related Work -- 2.1 Understanding the DNS Infrastructure -- 2.2 Misconfigured Networks -- 2.3 DNS Security -- 3 Studying DNS Name Servers -- 3.1 Recursive Authoritative Name Servers -- 3.2 Why Use Server-Side Caches? -- 3.3 Who Operates and Uses RANS? -- 3.4 Methodology for Detecting RANSes -- 4 Evaluating (in)Security of RANSes -- 4.1 Services Coresidence -- 4.2 Source Port Randomisation -- 4.3 DNSSEC -- 4.4 Implications of Vulnerable RANSes -- 5 Conclusions -- A Overview:

DNS and DNSSEC -- References -- Waiting for CSP -- Securing Legacy Web Applications with JSAgents -- 1 Introduction -- 2 Related Work -- 3 JSAgents Architecture -- 3.1 Building Blocks -- 3.2 JSAgents Core Library -- 3.3 JSAgents Modules -- 3.4 JSAgents Policy Files -- 4 Security Evaluation -- 5 Performance Evaluation -- 6 Future Work -- A Comparable Approaches -- A.1 From XSS Filters to CSP 1.0 -- A.2 Content Security Policy -- References -- Analyzing the BrowserID SSO System with Primary Identity Providers Using an Expressive Model of the Web -- 1 Introduction -- 2 The Web Model -- 2.1 Communication Model -- 2.2 Web System -- 2.3 Web Browsers -- 3 General Security Properties -- 4 The BrowserID System -- 4.1 Overview -- 4.2 Implementation Details -- 5 Analysis of BrowserID: Authentication Properties -- 5.1 Modeling of BrowserID with Primary IdPs -- 5.2 Authentication Properties of the BrowserID System -- 5.3 Identity Injection Attack on BrowserID with Primary IdPs -- 5.4 Security of the Fixed System -- 6 Privacy of BrowserID -- 6.1 Privacy Attacks on BrowserID -- 6.2 Fixing the Privacy of BrowserID -- 7 Related Work -- 8 Conclusion -- A Browser Model -- A.1 Browser State: Zp and sp0. A.2 Web Browser Relation Rp -- B Additional Privacy Attack Variants -- References -- System Security -- A Practical Approach for Adaptive Data Structure Layout Randomization -- 1 Introduction -- 2 Overview -- 2.1 Threat Model -- 2.2 System Overview -- 3 Design and Implementation of SALADS -- 3.1 Extraction Component -- 3.2 Randomization Component -- 3.3 De-randomization Component -- 3.4 Other Practical Issues -- 4 Evaluation -- 4.1 Effectiveness of DSSR Application Programs -- 4.2 Effectiveness of DSSR Kernel and DSSR Hypervisor -- 4.3 Performance Overhead -- 4.4 Memory Overhead -- 5 Discussion -- 5.1 Analysis of Effectiveness -- 5.2 Limitations -- 6 Related Work -- 7 Conclusion -- A Details of Lmbench Results -- References -- Trustworthy Prevention of Code Injection in Linux on Embedded Devices -- 1 Introduction -- 2 Background -- 2.1 The Prosper Hypervisor -- 2.2 The Attack Model -- 2.3 Formal Model of the Hypervisor -- 3 Design -- 4 Formal Model of MProsper -- 5 Verification Strategy -- 6 Evaluation -- 7 Related Work -- 8 Concluding Remarks -- References -- Practical Memory Deduplication Attacks in Sandboxed Javascript -- 1 Introduction -- 2 Background -- 2.1 Shared Memory -- 2.2 Page-Deduplication Attacks -- 3 Description of Our Javascript-Based Attack -- 4 Practical Attacks and Evaluation -- 4.1 Cross-VM Attack on Private Clouds -- 4.2 Attack on Personal Computers and Smartphones -- 5 Countermeasures -- 6 Conclusion -- References -- Cryptography -- Computational Soundness for Interactive Primitives -- 1 Introduction -- 2 Related Work -- 3 Review of the CoSP Framework for Equivalence -- 4 Review of the UC Framework -- 5 Ideal Functionalities in the Symbolic Model -- 6 Ideal Functionalities in the Computational Model -- 7 Real Protocols in CoSP -- 8 Computational Soundness for Interactive Primitives -- 9 Case Study: Untraceable Payments.
A Protocol Conditions -- References -- Verifiably Encrypted Signatures: Security Revisited and a New Construction -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Work -- 1.3 Outline -- 2 Preliminaries -- 2.1 Digital Signatures -- 2.2 Structure-Preserving Signatures on Equivalence Classes -- 2.3 Verifiably Encrypted Signatures -- 3 The Importance of Resolution Independence -- 3.1 Counterexample -- 3.2 Filling the Gap -- 4 Verifiably Encrypted Signatures from SPS-EQ-R -- 5 Public-Key Encryption from SPS-EQ-R -- 6 Conclusion -- References -- A Omitted Proofs -- Interleaving Cryptanalytic Time-Memory Trade-Offs on Non-uniform Distributions -- 1 Introduction -- 2 Cryptanalytic Time-Memory Trade-Offs -- 2.1 Hellman Scheme -- 2.2 Oechslin

Scheme -- 2.3 Related Works -- 3 Interleaving -- 3.1 Description -- 3.2 Analysis -- 4 Order of Visit -- 4.1 Discussion -- 4.2 Analysis -- 5 Input Set Partition and Memory Allocation -- 5.1 Input Set Partition -- 5.2 Memory Allocation -- 6 Results -- 6.1 Statistics -- 6.2 RockYou -- 6.3 10 Million Combos -- 6.4 Discussion -- 7 Conclusion -- A Proof of Theorem -- B Subsets of 10 Million Combos -- References -- Efficient Message Authentication Codes with Combinatorial Group Testing -- 1 Introduction -- 2 Preliminaries -- 3 MAC for Corruption Identification -- 3.1 Combinatorial Group Testing -- 3.2 MAC for Extended Vector Space -- 3.3 Efficient Group Testing MAC -- 3.4 Security Notions -- 3.5 Remarks -- 3.6 Provable Security of GTM -- 4 Experimental Implementation -- 5 Concluding Remarks -- References -- Symmetric-Key Based Proofs of Retrievability Supporting Public Verification -- 1 Introduction -- 1.1 Related Work -- 2 Preliminaries -- 2.1 Proofs of Retrievability -- 2.2 Obfuscation Preliminaries -- 2.3 Puncturable PRFs -- 3 Security Definitions -- 3.1 Security Definitions on Static PoR.
3.2 Security Definitions on Dynamic PoR -- 4 Constructions -- 4.1 Static Publicly Verifiable PoR Scheme -- 4.2 PoR Scheme Supporting Efficient Dynamic Updates -- 4.3 Security Proofs -- 5 Analysis and Comparisons -- 6 Conclusions -- A Discussions and Future Directions Towards i O -- A.1 Outsourced and Joint Generation of Indistinguishability Obfuscation -- A.2 Reusability and Universality of Indistinguishability Obfuscation -- A.3 Obfuscation for Specific Functions -- References -- DTLS-HIMMO: Achieving DTLS Certificate Security with Symmetric Key Overhead -- 1 Introduction -- 2 Preliminaries -- 2.1 Security Standards in the Internet (of Things) -- 2.2 DTLS-PSK -- 2.3 Attack Model and Security Goals -- 3 HIMMO and HIMMO Extensions -- 3.1 HIMMO Operation -- 3.2 Implicit Certification and Verification of Credentials -- 3.3 Enhancing Privacy by Using Multiple TTPs -- 4 Implementation and Performance -- 5 (D)TLS-HIMMO -- 5.1 DTLS-HIMMO Configurations -- 5.2 (D)TLS-HIMMO Handshake -- 5.3 Privacy Protection -- 5.4 TTP Infrastructure -- 5.5 Security Considerations of (D)TLS-HIMMO -- 6 Performance of DTLS-HIMMO and Comparison with Existing (D)TLS Alternatives -- 7 Conclusions -- References -- Short Accountable Ring Signatures Based on DDH -- 1 Introduction -- 2 Defining Accountable Ring Signatures -- 2.1 Ring and Group Signatures from Accountable Ring Signatures -- 3 Preliminaries -- 4 Constructing Accountable Ring Signatures -- 5 Efficient Instantiation -- A Proof of Theorem 1 -- B Security Proofs of Our -Protocols -- B.1 Proof of Lemma 1 -- B.2 Proof of Lemma 2 -- B.
3 Proof of Lemma 3 -- B.4 Proof of Lemma 5 -- References -- Updatable Hash Proof System and Its Applications -- 1 Introduction -- 1.1 Our Results -- 1.2 Related Work -- 2 Preliminaries -- 3 Updatable Hash Proof System -- 4 Building CML-PKE from UHPS -- 4.1 A CPA-Secure Scheme.
4.2 CCA-Secure Schemes -- 4.3 PKE Schemes with Leakage During Key Update -- 5 Instantiations of Updatable Hash Proof System -- 5.1 Instantiation from the SXDH Assumption -- 5.2 Parameters -- A Omitted Constructions in Sect.4.2 -- References -- Server-Aided Revocable Identity-Based Encryption -- 1 Introduction -- 2 Preliminaries -- 3 Definition and Security of SR-IBE -- 4 Construction of SR-IBE Scheme -- 4.1 The Node Selection Algorithm: KUNodes -- 4.2 The Construction -- 5 Security Proof -- 6 Conclusion -- A Proof of Theorem 2 -- References -- Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Roadmap -- 2 Preliminaries -- 2.1 Commitment Schemes -- 2.2 Zero-Knowledge Proofs and -Protocols -- 2.3 Learning with Errors -- 2.4 Rejection

Sampling -- 3 Commitments from Ring-LWE -- 4 Zero-Knowledge of Proofs of Knowledge -- 4.1 Preimage Proofs -- 4.2 Proving Linear Relations -- 4.3 Proving Multiplicative Relations -- 5 Conclusion -- A Proofs -- A.1 Proofs of Theorem 4.5 -- A.2 Proofs of Theorem 4.6 -- References -- Making Any Identity-Based Encryption Accountable, Efficiently -- 1 Introduction -- 2 Generic Construction of A-IBE with Constant Size Ciphertext -- 2.1 Detailed Construction -- 2.2 Security Analysis -- 3 Generic Construction of A-IBE Allowing Public Traceability and Identity Reuse -- 3.1 A General Framework Allowing Identity Re-use -- 3.2 Building Blocks for Public Traceability -- 3.3 Concrete Construction and Security Analysis -- 4 Conclusions and Open Problems -- A Preliminaries -- References -- Practical Threshold Password-Authenticated Secret Sharing Protocol -- 1 Introduction -- 2 Definition of Security -- 3 Our TPASS Protocol -- 3.1 Description of Our Protocol -- 3.2 Correctness and Efficiency -- 4 Security Analysis -- 5 Conclusion.
References.

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. .

2. Record Nr. UNINA9910148960503321

Autore	Iles Greg <1960->
Titolo	Devil's Punchbowl (Penn Cage, Book 3)
Pubbl/distr/stampa	HarperCollins UK
ISBN	0-00-731643-7
Disciplina	813/.54
Lingua di pubblicazione	Inglese
Formato	Musica
Livello bibliografico	Monografia
Sommario/riassunto	The disturbing new thriller from the king of southern gothic.When he was a prosecuting attorney Penn Cage sent hardened killers to death row. But it is as mayor of his hometown, Natchez, Mississippi, that Penn willface his most dangerous threat.Urged by old friends to try to restore the town to its former glory, Penn has ridden into office on a tide of support for change. But in its quest for new jobs and fresh money, Natchez has turned to casino gambling. Five fantastical steamboats float on the river beside the old slave market like props from Gone With the Wind. But one boat isn't like the others. Rumour has it that the Magnolia Queen has found a way to pull the big players from Las Vegas. And with them comes an unquenchable taste for one thing: blood sport, and the dark vices that go with it.When a childhood friend of Penn's who brings him evidence of these crimes is brutally murdered, the full weight of Penn's failure to protect this city hits home. So begins his quest to find the men responsible. But it's a hunt he begins alone, for the local authorities have been corrupted by the money and power of his hidden enemy. With his family's life at stake, Penn realizes his only allies in his one-man war are those bound to him by blood or honour: