

1. Record Nr.	UNISA996466225403316
Titolo	Information Security [[electronic resource]] : 16th International Conference, ISC 2013, Dallas, Texas, November 13-15, 2013, Proceedings / / edited by Yvo Desmedt
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-27659-X
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIV, 418 p. 52 illus. in color.)
Collana	Security and Cryptology ; ; 7807
Disciplina	005.8
Soggetti	Software engineering Computer logic Programming languages (Electronic computers) Mathematical logic Artificial intelligence Computer communication systems Software Engineering Logics and Meanings of Programs Programming Languages, Compilers, Interpreters Mathematical Logic and Formal Languages Artificial Intelligence Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- ISC 2013 -- Contents -- Security of Operating Systems -- Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection -- 1 Introduction -- 2 Related Work -- 3 Integrity Checking for Function Pointers -- 3.1 Environment -- 3.2 HookLocator Architecture -- 4 Implementation -- 5 Evaluation -- 5.1 Extraction Module -- 5.2 Search Module -- 5.3 Learning Module and Pool Monitor -- 5.4 Performance Overhead of HookLocator -- 6 Conclusion -- References -- Lightweight Attestation and Secure Code Update for Multiple Separated Microkernel Tasks -- 1 Introduction -- 2

Related Work -- 3 Attestation Scenario and Attacker Model -- 3.1
 Scenario for the Attestation of Multiple Tasks -- 3.2 Attacker Model --
 4 Microkernel-Based System Architecture with a Multi-context HSM --
 5 Integrity Verification of Multiple Microkernel Tasks as Basis for a
 Secure Code Update -- 5.1 Notation -- 5.2 Cryptographic Keys -- 5.3
 Integrity Verification and Attestation of Multiple Tasks -- 5.4 Updating
 a Task After Verifying the Integrity of Existing Tasks -- 6 Security
 Analysis -- 6.1 Analysis of the Attestation Protocol -- 6.2 Formal
 Verification of the Attestation Protocol -- 6.3 Analysis of the Code
 Update Protocol -- 7 Conclusion -- A ProVerif Code for the Attestation
 Mechanism -- References -- Secret Sharing -- The Security Defect of a
 Multi-pixel Encoding Method -- 1 Introduction -- 2 Preliminaries -- 3
 The Security Defect of MPEM -- 3.1 Our Discovery of MPEM's Security
 Defect -- 3.2 Using Variance to Explain the Above Security Defect -- 4
 Future Researches -- 5 Conclusions -- References -- Encrypted Secret
 Sharing and Analysis by Plaintext Randomization -- 1 Introduction --
 1.1 Plaintext Randomization -- 1.2 Our Contributions -- 2
 Cryptographic Security and Games -- 2.1 Multi-user CCA Security -- 3
 Plaintext Randomization.
 4 Hybrid Encryption -- 5 Secret Sharing with Encrypted Shares -- 6
 Conclusions -- References -- Encryption -- Round-Efficient Private
 Stable Matching from Additive Homomorphic Encryption -- 1
 Introduction -- 1.1 Related Work -- 1.2 Contribution -- 2 Preliminaries
 -- 3 Private Stable Matching -- 3.1 Gale-Shapley Algorithm -- 3.2
 Golle and Franklin--Gondree--Mohassel Private Stable Matching -- 4
 Main Proposal -- 4.1 New Bid Design -- 4.2 New Private Stable
 Matching -- 4.3 Complexity Analysis -- 5 Experimental
 Implementation -- 5.1 Implemented Version of Our Protocol -- 5.2
 Experimental Settings -- 5.3 Experimental Results -- A Initialization of
 the Proposed Protocol -- B Correctness of the Proposed Protocol -- C
 Security of the Proposed Protocol -- References -- Efficient and Fully
 Secure Forward Secure Ciphertext-Policy Attribute-Based Encryption --
 1 Introduction -- 2 Preliminaries -- 2.1 Composite Order Bilinear Maps
 and Assumptions -- 2.2 Access Structures and Linear Secret Sharing
 Schemes -- 3 Fully Secure Forward Secure Ciphertext-Policy Attribute-
 Based Encryption -- 3.1 The Model of FS-CP-ABE -- 3.2 Security Model
 for FS-CP-ABE -- 4 Ciphertext-Policy Attribute-Based Encryption with
 Augmented Hierarchy (CP-ABE-AH) -- 4.1 The Model of CP-ABE-AH --
 4.2 Security Model for CP-ABE-AH -- 4.3 CP-ABE-AH: Construction --
 5 Construction of FS-CP-ABE from CP-ABE-AH -- 6 Efficiency --
 References -- Reducing Public Key Sizes in Bounded CCA-Secure KEMs
 with Optimal Ciphertext Length -- 1 Introduction -- 1.1 Background --
 1.2 Our Contribution -- 1.3 Related Works -- 2 Preliminaries -- 2.1
 Notation -- 2.2 Syntax and Security Notions -- 2.3 Number Theoretic
 Assumptions -- 2.4 Cover Free Family and Its Two-Dimensional
 Representation -- 3 Construction from the CBDH Assumption -- 3.1
 Construction -- 3.2 Security -- 4 Construction from the Factoring
 Assumption.
 4.1 CDH Assumption on QRN and BBS Pseudo-Random Number
 Generator -- 4.2 Construction -- 4.3 Security -- References --
 Malware and Critical Infrastructures -- 4GMOP: Mopping Malware
 Initiated SMS Traffic in Mobile Networks -- 1 Introduction -- 2 Mobile
 Malware Traffic -- 2.1 Traffic During Infection -- 2.2 Traffic During
 Execution -- 3 The 4GMOP Sensor -- 3.1 Architecture Overview -- 3.2
 Sensor Placement -- 4 The SMS-Mv1.0 Corpus -- 4.1 SMS Usage in
 Mobile Malware Samples -- 4.2 Building the SMS-Mv1.0 Corpus -- 5
 An Example Classifier -- 5.1 Feature Selection -- 5.2 Evaluation -- 6
 Conclusion -- References -- Design and Analysis of a Sophisticated

Malware Attack Against Smart Grid -- 1 Introduction -- 2 Smart Grid Architecture -- 3 Smart Grid Blackout Attack -- 3.1 Phase 1: Initial Penetration -- 3.2 Phase 2: Espionage -- 3.3 Phase 3: Development of Malware for the Deceptive Attack -- 3.4 Phase 4: Deceptive Attack -- 3.5 Phase 5: Cleanup and Aftermath -- 4 Concluding Remarks -- References -- Multi-round Attacks on Structural Controllability Properties for Non-complete Random Graphs -- 1 Introduction -- 2 Multi-round Threat Model -- 3 Attack Scenarios on Structural Controllability -- 3.1 SCN-1 and SCN-2: Exploitation of Links and Vertices in Graphs -- 3.2 SCN3: Exploitation of Links and Vertices in Power-Law Subgraphs -- 4 Conclusions -- References -- Cryptanalysis -- Improved Meet-in-the-Middle Attacks on Round-Reduced ARIA -- 1 Introduction -- 2 Preliminary -- 2.1 A Short Description of ARIA -- 2.2 Notations -- 3 New 4-Round Meet-in-the-Middle Distinguisher of ARIA -- 4 Meet-in-the-Middle Attacks on Round-Reduced ARIA -- 4.1 7-Round Attack on ARIA-192/256 -- 4.2 Extension to 8-Round Attack on ARIA-256 -- 4.3 Attack on 7-Round ARIA-128 -- 4.4 9-Round Attack on ARIA-256 -- 5 Conclusion -- References.

Establishing Equations: The Complexity of Algebraic and Fast Algebraic Attacks Revisited -- 1 Introduction -- 2 Preliminaries -- 3 Algebraic Attacks -- 3.1 Simple Method: Polynomial Multiplication -- 3.2 Improved Method: Shift and Update from the Feedback Polynomial -- 3.3 New Method: Frobenius Form of the Monomial State Rewriting Matrix -- 4 Fast Algebraic Attacks -- 4.1 Simple Method: Polynomial Multiplication -- 4.2 Improved Method: Shift and Update from the Feedback Polynomial -- 4.3 New Method: Frobenius Form of the Monomial State Rewriting Matrix -- 5 General Algebraic and Fast Algebraic Attacks -- 5.1 Simple Method: Polynomial Multiplication -- 5.2 Improved Method: Shift and Update from the Feedback Polynomial -- 5.3 New Method: Frobenius Form of the Monomial State Rewriting Matrix -- 6 Conclusion -- References -- Factoring a Multiprime Modulus N with Random Bits -- 1 Introduction -- 2 Algorithm to Factor a Multiprime Modulus N -- 3 Behavior and Complexity of the Algorithm to Factor N -- 3.1 Number of Incorrect Roots Lifted from a Good Root (G) -- 3.2 Number of Incorrect Roots Lifted from an Incorrect Root (B) -- 3.3 Number of Incorrect Roots Lifted at Level j (X_j) -- 3.4 Complexity of the Algorithm to Factor -- 4 Implementation and Performance -- 5 Concluding Remarks -- References -- Block Ciphers and Stream Ciphers -- Faster 128-EEA3 and 128-EIA3 Software -- 1 Preliminaries -- 2 Software Optimizations -- 3 Results -- 3.1 Hexagon Architecture -- 3.2 Performance -- 4 Conclusion -- References -- Merging the Camellia, SMS4 and AES S-Boxes in a Single S-Box with Composite Bases -- 1 Introduction -- 2 Notation and Mathematical Representations -- 3 Mathematical Representation of the Camellia, AES and SMS4 S-Boxes -- 3.1 Merging the Camellia, AES and SMS4 S-Boxes by Using Composite Fields -- 4 Results and Comparisons -- 5 Conclusions -- References.

Entity Authentication -- Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards -- 1 Introduction -- 2 System Architecture and Adversary Models -- 2.1 System Architecture of Two-Factor Authentication -- 2.2 Adversary Models for Smart-card-based Authentication and for Common-memory-based Authentication -- 3 Cryptanalysis of Hsieh-Leu's Scheme -- 3.1 A Brief Review of Hsieh-Leu's Scheme -- 3.2 Offline Dictionary Attack -- 4 Cryptanalysis of PSCAV from SEC 2012 -- 4.1 A Brief Review of PSCAV -- 4.2 Offline Dictionary Attack -- 5 Conclusion -- References -- Self-blindable Credential: Towards Anonymous Entity Authentication Upon Resource Constrained Devices -- 1 Introduction -- 2 Modeling of Self-blindable

Credential -- 3 Self-blindable Credential with Verifier-Local Revocation
-- 3.1 Design Rationale -- 3.2 Construction Details -- 3.3 Security
Analysis -- 4 Self-blindable Credential with Forward Unlinkability and
Scalable Revocation -- 4.1 Forward Unlinkable Self-blindable Credential
-- 4.2 Scalable Revocation -- References -- Practical and Provably
Secure Distance-Bounding -- 1 Introduction -- 2 Model for Distance-
Bounding Protocols -- 3 Practical and Secure Distance-Bounding
Protocols -- References -- Usability and Risk Perception -- On the
Viability of CAPTCHAs for use in Telephony Systems: A Usability Field
Study -- 1 Introduction -- 2 Related Work -- 3 Hypotheses -- 4
Studied Audio CAPTCHAs -- 5 Usability Evaluation -- 6 Study Results
-- 6.1 Captcha Inconvenience -- 6.2 Hypotheses Validation -- 7
Discussion -- 8 Guidelines -- References -- Cars, Condoms, and
Facebook -- 1 Introduction -- 2 Background and Related Work -- 3
Methodology -- 4 Results -- 5 Discussion -- 6 Conclusion and Future
Work -- References -- Access Control -- Achieving Revocable Fine-
Grained Cryptographic Access Control over Cloud Data -- 1
Introduction.
2 Synopsis.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 16th International Conference on Information Security, ISC 2013, held in Dallas, Texas, in November 2013. The 16 revised full papers presented together with 14 short papers were carefully reviewed and selected from 70 submissions. The papers cover a wide range of topics in the area of cryptography and cryptanalysis and are organized in the following topical sections: security of operating systems; secret sharing; encryption; malware and Critical infrastructures; cryptanalysis; block ciphers and stream ciphers; entity authentication; usability & risk perception; access control; computer security; privacy attacks; cryptography.
