

| | |
|-------------------------|---|
| 1. Record Nr. | UNINA9910483855203321 |
| Titolo | Security and Trust Management : 11th International Workshop, STM 2015, Vienna, Austria, September 21-22, 2015, Proceedings // edited by Sara Foresti |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015 |
| ISBN | 3-319-24858-8 |
| Edizione | [1st ed. 2015.] |
| Descrizione fisica | 1 online resource (X, 293 p. 68 illus. in color.) |
| Collana | Security and Cryptology, , 2946-1863 ; ; 9331 |
| Disciplina | 005.8 |
| Soggetti | Data protection Electronic data processing - Management Cryptography Data encryption (Computer science) Algorithms Computers and civilization Data and Information Security IT Operations Cryptology 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 -- Preface -- Organization -- Contents -- Security Metrics and Classification -- Digital Waste Sorting: A Goal-Based, Self-Learning Approach to Label Spam Email Campaigns -- 1 Introduction -- 2 Related Work -- 3 Digital Waste Sorting -- 3.1 Definition of Classes -- 3.2 Feature Extraction -- 3.3 DWS Classification Workflow -- 4 Results -- 4.1 Classifier Selection -- 4.2 DWS Application -- 5 Conclusion and Future Directions -- References -- Integrating Privacy and Safety Criteria into Planning Tasks -- 1 Introduction -- 2 Related Work -- 3 Approach -- 4 The Analytic Hierarchy Process -- 4.1 AHP Hierarchy -- 4.2 Relative Importance of Criteria -- 4.3 Ranking of Alternative Plans -- 5 Criteria -- 5.1 Utility -- 5.2 Unsatisfied Safety Preferences (USP) -- 5.3 Willingness-to-Share-Data (WSD) -- 6 The Influence of Criteria |

Importance Ratios -- 7 Discussion -- 8 Conclusion and Future Work --
References -- Security Metrics, Secure Elements, and Operational
Measurement Trust in Cloud Environments -- 1 Introduction -- 2
Background and Related Work -- 2.1 Terminology -- 2.2 Related Work
-- 3 Threat Model -- 4 Operational Measurement Trust -- 4.1 Trusted
Monitoring Base -- 4.2 Secure Elements and Measurement Data -- 5
Levels of Operational Trust -- 5.1 Trusted Monitoring Base -- 5.2
Probes -- 5.3 Quantifying Overall Confidence -- 6 Operational
Measurement Trust and Security Metrics -- 7 Discussion -- 8
Conclusion -- References -- Data Protection -- A Declarative
Framework for Specifying and Enforcing Purpose-Aware Policies -- 1
Introduction -- 2 Running Example -- 3 A Declarative Framework for
Purpose-Aware Policies -- 3.1 Semantics of Purpose-Aware Policies --
4 Policies Verification -- 4.1 Purpose Achievement Problem -- 4.2
Runtime Policies Verification -- 5 Discussion and Related Work --
References -- How to Trust the Re-use of Data -- 1 Introduction.
2 Klaim with Goals -- 2.1 Syntax -- 2.2 Semantics -- 3 Analysis -- 3.1
Over Approximation -- 3.2 Well-Behaved Processes -- 4 Conclusion --
A Appendix: Proofs -- References -- Towards Balancing Privacy and
Efficiency: A Principal-Agent Model of Data-Centric Business -- 1
Personal Data Markets and Privacy -- 2 Related Work -- 3 Principal-
Agent Model of the Privacy Problems in Data-Centric Business -- 3.1
Assumptions and Background -- 3.2 Principal-Agent Model -- 4
Towards Balancing Privacy and Efficiency -- 4.1 S1: Privacy is Not
Considered a Competitive Factor by Users -- 4.2 S3: Markets for Data-
Centric Services Are Currently Monopolistic -- 4.3 S2: Privacy is
Perceived as a Competitive Factor by Users But They are Unable to
Determine Providers' Level of "Privacy-Friendliness" -- 5 Conclusion
-- References -- Intrusion Detection and Software Vulnerabilities --
The AC-Index: Fast Online Detection of Correlated Alerts -- 1
Introduction -- 2 Preliminaries and Problem Formalization -- 3 The
AC-Index -- 4 Experimental Results -- 5 Related Work -- 6
Conclusions -- References -- Intrusion Detection System for
Applications Using Linux Containers -- 1 Introduction -- 2 Related
Work -- 3 Real-Time Intrusion Detection -- 4 System Evaluation -- 4.1
Environment Setup -- 4.2 Generating Normal Workload -- 4.3
Simulating Malicious Behavior -- 4.4 Collecting Container-Behavior
Data -- 4.5 Training Classifier -- 4.6 Classifier Evaluation -- 4.7
Evaluation Results -- 4.8 Complexity Analysis -- 5 Conclusion and
Future Work -- References -- SUDUTA: Script UAF Detection Using
Taint Analysis -- 1 Introduction -- 2 Background -- 2.1 UAF
Vulnerabilities -- 2.2 Undangle -- 2.3 Formalizing Taint Policy Rules --
3 SUDUTA -- 3.1 Taint Policy -- 3.2 On-line Dynamic Taint Analysis --
3.3 Custom Memory Allocator Monitoring -- 4 Evaluation -- 5 Related
Work -- 6 Conclusion.
References -- Cryptographic Protocols -- Two-Factor Authentication
for the Bitcoin Protocol -- 1 Introduction -- 2 Bitcoin Protocol -- 3
Threshold Signatures -- 3.1 Two-Party ECDSA -- 3.2 Threshold
Signature Support in Bitcoin -- 4 Two-Factor Bitcoin Wallets -- 4.1
Description of the Prototype -- 5 Implementation Aspects -- 5.1
Runtime Analysis -- 6 Future Work -- 7 Conclusion -- References --
Private Proximity Testing on Steroids: An NTRU-based Protocol -- 1
Introduction -- 2 Related Work -- 2.1 NTRU -- 2.2 Private Proximity
Testing -- 2.3 The Protocol of Narayanan et al. -- 3 The Proposed
Protocol -- 3.1 Threat Model -- 3.2 Main Actors and Desiderata -- 3.3
The Protocol -- 3.4 Protocol Correctness -- 3.5 Security Analysis -- 4
Comparison/Experimental Results -- 5 Conclusions -- References --
Selecting a New Key Derivation Function for Disk Encryption -- 1

Introduction -- 2 Requirements for a Key Derivation Function -- 2.1 Environment for Disk Encryption -- 2.2 Requirements for a Disk Encryption Application -- 3 KDF Building Blocks -- 3.1 Cryptographic Primitives -- 3.2 Concepts to Utilize Resources During Computation -- 3.3 Ingredients -- 3.4 Processing Unlimited Input and Output -- 4 PHC Candidates as KDF Algorithms -- 4.1 Argon -- 4.2 Battcrypt -- 4.3 Catena -- 4.4 Lyra2 -- 4.5 Yescrypt -- 4.6 Algorithms Not Selected for Further Testing -- 4.7 Overview -- 5 Run-Time Test -- 5.1 Specific Use Case Measurement -- 5.2 Fixed Implementation Issues -- 6 Conclusions and Open Issues -- A Appendix -- A.1 PHC Candidate Implementation and Benchmarking Tests -- A.2 PHC Test Report -- References -- Controlling Data Release -- It's My Privilege: Controlling Downgrading in DC-Labels -- 1 Introduction -- 2 Background -- 3 Security Definitions -- 4 Enforcement for Robust Privileges -- 5 Interaction Among Restricted Privileges -- 6 Case Studies.

6.1 Calendar Case Study -- 6.2 Restricted Privileges in Existing Applications -- 7 Related Work -- 8 Conclusion -- References -- Obligations in PTaCL -- 1 Introduction -- 2 PTaCL -- 2.1 Syntax and Semantics -- 2.2 Additional Operators -- 3 Obligations in PTaCL -- 3.1 Defining Obligations in PTaCL -- 3.2 Computing Obligations in PTaCL -- 3.3 Computing Obligations for Derived Policy Operators -- 4 Indeterminacy in PTaCL -- 4.1 Failure of Target Evaluation -- 4.2 Failure of Policy Retrieval -- 5 XACML and Other Related Work -- 6 Conclusion -- References -- Content and Key Management to Trace Traitors in Broadcasting Services -- 1 Introduction -- 1.1 Background -- 1.2 Related Works -- 1.3 Our Contributions -- 2 Preparation: Traitor Tracing Mechanism in [1] -- 3 Proposal: Content and Key Management (CKM) -- 3.1 Content Comparison Attack -- 3.2 Content Management: Slight Modification of Coded Content -- 3.3 Content and Key Management Method -- 3.4 Actual Content and Key Management System -- 3.5 Content and Key Management Method for TTE -- 4 Discussion and Security Analysis -- 4.1 Simplicity of CKM -- 4.2 Security -- 4.3 Transmission Bit Rate -- 5 Conclusion -- References -- Security Analysis, Risk Management, and Usability -- In Cyber-Space No One Can Hear You SCREAM -- 1 Introduction -- 2 Methods -- 3 SCREAM: An RCA for Computer Security -- 3.1 Adapting CREAM as an RCA Technique for Security -- 3.2 Using SCREAM -- 4 Building the Catalog of Attack Modes -- 5 Discussion -- 6 Conclusion -- References -- A Socio-Technical Investigation into Smartphone Security -- 1 Introduction -- 2 Methodology -- 2.1 Interview Protocol -- 2.2 Participants -- 2.3 Analysis -- 3 Results -- 3.1 Lack of Awareness -- 3.2 Lack of Concern -- 3.3 Lack of Self-Efficacy -- 3.4 Lack of Compulsion -- 3.5 Lack of Perseverance -- 4 Model of Precaution Adoption -- 5 Related Work.

6 Conclusions and Future Work -- References -- A Game Theoretic Framework for Modeling Adversarial Cyber Security Game Among Attackers, Defenders, and Users -- Abstract -- 1 Introduction -- 2 Cyber Security Game -- 2.1 Player Objectives -- 2.2 User -- Defender Game -- 2.3 User-Attacker Game -- 2.4 Attacker-Defender Game -- 3 Related Work -- 4 Conclusions -- Acknowledgments -- References -- Design, Demonstration, and Evaluation of an Information Security Contract and Trading Mechanism to Hedge Information Security Risks -- 1 Introduction -- 2 Related Work -- 3 Requirements for ISC and TM -- 4 Design and Development of ISC and TM -- 4.1 Information Security Contract -- 4.2 Trading Mechanism -- 5 Demonstration: ISC to Hedge Underlying Risk -- 6 Evaluation -- 7 Conclusion -- References -- Author Index.

International Workshop on Security and Trust Management, STM 2015, held in Vienna, Austria, in September 2015, in conjunction with the 20th European Symposium Research in Computer Security, ESORICS 2015. The 15 revised full papers were carefully reviewed and selected from 38 submissions. They are organized in topical sections as security metrics and classification; data protection; intrusion detection and software vulnerabilities; cryptographic protocols; controlling data release; and security analysis, risk management and usability.
