

1. Record Nr.	UNINA9910510559803321
Titolo	Protocols, strands, and logic : essays dedicated to Joshua Guttman on the the occasion of his 66.66th birthday / / Daniel Dougherty [and three others], editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-91631-6
Descrizione fisica	1 online resource (435 pages)
Collana	Lecture Notes in Computer Science ; ; 13066
Disciplina	005.8
Soggetti	Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Contents -- Securing Node-RED Applications -- 1 Introduction -- 2 Node-RED Vulnerabilities -- 2.1 Node-RED Platform -- 2.2 Platform-Level Isolation Vulnerabilities -- 2.3 Application-Level Context Vulnerabilities -- 3 Formalization -- 3.1 Language Syntax and Semantics -- 3.2 Security Condition and Enforcement -- 4 Related Work -- 5 Conclusion -- References -- Protocol Analysis with Time and Space -- 1 Introduction -- 1.1 Related Work -- 2 Two Time and Space Protocols -- 3 A Time and Space Process Algebra -- 3.1 New Syntax for Location -- 3.2 Time and Space Intruder Model -- 3.3 Time and Space Process Semantics -- 4 Time and Space Process Algebra into Untimed Process Algebra -- 5 Timed Process Algebra into Strands in Maude-NPA -- 6 Conclusions -- References -- Searching for Selfie in TLS 1.3 with the Cryptographic Protocol Shapes Analyzer -- 1 Introduction -- 2 Background -- 2.1 Cryptographic Protocol Shapes Analyser -- 2.2 TLS 1.3 Pre Shared Key Authentication -- 2.3 Selfie Attack -- 3 Modeling TLS 1.3 PSK Authentication -- 3.1 Models of the TLS 1.3 PSK Authentication -- 3.2 Modeling the Proposed Fixes to the Selfie Attack -- 4 Discussion -- 5 Conclusions -- A Appendix -- References -- A Tutorial-Style Introduction to DY -- 1 Introduction -- 2 The DY Framework -- 3 The ISO-DH Protocol -- 4 Modeling ISO-DH in DY -- 5 Security Analysis -- 5.1 Forward Secrecy -- 5.2 Authentication Properties -- 6 Conclusion -- References -- Security Protocols as

Choreographies -- 1 Introduction -- 2 The Envelope Protocol and Its Choreographic Description -- 3 Projection and Refinement -- 3.1 Projection -- 3.2 Refinement -- 4 Verification in Tamarin -- 5 Related Work -- 6 Conclusion -- References -- How to Explain Security Protocols to Your Children -- 1 Introduction -- 2 Storyboard -- 2.1 Our First Security Protocol. 2.2 How the Postman Steals Isabelle's Cake -- 2.3 A Fix: Asymmetric Encryption -- 2.4 Denial of Service? -- 3 When it Gets Really Dark -- 3.1 Challenge and Respond -- 3.2 Man in the Middle Attack -- 3.3 A Countermeasure -- 4 A Practical Session -- 4.1 The Material -- 4.2 A Typical Session -- 4.3 Long-Term Variants of the Design-Attack Parts (advanced) -- 5 Conclusion: Have Fun! -- References -- Verifying a Blockchain-Based Remote Debugging Protocol for Bug Bounty -- 1 Introduction -- 2 Background: VeriOSS -- 2.1 Workflow Overview -- 2.2 Challenge-Response Interaction -- 2.3 Remote Debugging, and Challenge Generation and Solution -- 3 Protocol Encoding -- 4 Verification in ProVerif -- 5 Conclusion -- References -- Quantum Machine Learning and Fraud Detection -- 1 Introduction -- 2 Detecting Fraudulent Transactions -- 2.1 Support Vector Machines -- 2.2 Quantum Matrix Inversion and Probabilistic Abstract Interpretation -- 3 Quantum Machine Learning -- 3.1 Quantum Support Vector Machines -- 3.2 Quantum Support Vector Machines as PAI -- 4 Implementation of Quantum Fraud Detection -- 4.1 Experiments on the IBM Quantum Platform -- 5 Conclusion -- References -- Model Finding for Exploration -- 1 Introduction -- 2 Foundations -- 2.1 Homomorphism Orderings -- 3 Approaches to Model Finding -- 4 Three Principles for Model Finding Assistants -- 4.1 Fitness -- 4.2 Exploration of Individual Models -- 4.3 Completeness -- 5 Geometric Logic -- 6 Direct Model Finding Methods -- 6.1 Chase-Based Approaches -- 6.2 cpsa -- 7 Programming Against a Solver: Theory -- 7.1 Building Blocks -- 7.2 Minimization -- 7.3 Set of Support -- 8 Programming Against a Solver: Practice -- 8.1 Constructing HomTo and HomFrom for Arbitrary Homomorphisms -- 8.2 Constructing HomTo and HomFrom for Submodel Morphisms -- 8.3 Constructing homTo and homFrom for Injective Morphisms -- 9 Conclusion. References -- Secure Key Management Policies in Strand Spaces -- 1 Introduction -- 2 Background and Related Work -- 2.1 The Strand Space Model -- 2.2 The CPSA Tool -- 2.3 Attacks on the PKCS#11 API -- 2.4 Related Work -- 3 Key Management Policies -- 4 Key Management APIs -- 4.1 An Untyped, Vulnerable API -- 4.2 A Secure, Typed API -- 4.3 Examples -- 5 Conclusion -- References -- A Declaration of Software Independence -- 1 Introduction -- 2 Formalizing Software Independence -- 2.1 Software Independence... of What? -- 2.2 Voting System and Its Software -- 2.3 Available Audits -- 3 Possibilistic Formulation of Software Independence -- 3.1 Basic Formulation -- 3.2 Relationship to End-to-End Verifiability -- 3.3 SI with Adaptive Audits -- 3.4 A Refinement -- 3.5 Software Resilience -- 3.6 Thought Experiment -- 3.7 Software Independence for Probabilistic Audits -- 4 Probabilistic/Game-Theoretic Definition -- 4.1 Terminology and Notation -- 4.2 Game-Theoretic Definition of SI -- 5 Conclusions -- References -- Formal Methods and Mathematical Intuition -- 1 Introduction -- 2 Formal Methods and Research at MITRE -- 3 Mathematical Intuition and Heuristics -- 4 Example: Development of Dimension Concepts and Dimension Theories -- 5 L. E. J. Brouwer's Breakthrough to Invariance of Dimension -- 6 Conclusion: Formal Methods, Mathematical Intuition, and Rigorous Mathematical Exposition -- References -- Establishing the Price of Privacy in Federated Data Trading -- 1 Introduction -- 2 Preliminaries -- 2.1 Differential Privacy

-- 2.2 Shapley Value -- 3 Related Works -- 4 Differentially Private Data Trading Mechanism -- 4.1 Mechanism Outline -- 4.2 Earning Splitting -- 5 Experimental Results -- 5.1 Experimental Environments -- 5.2 Number of Rounds Needed for Data Collection -- 5.3 Number of Free Riders by Penalty Scheme -- 5.4 Reduced Shapley Value Computation Time.

6 Conclusion -- A Proofs -- References -- On the Complexity of Verification of Time-Sensitive Distributed Systems -- 1 Introduction -- 2 Multiset Rewriting Systems -- 2.1 Progressing Timed Systems -- 3 Quantitative Temporal Properties -- 3.1 Critical Configurations and Compliant Traces -- 3.2 Time Sampling -- 3.3 Verification Problems -- 4 Relations Among Properties of Timed MSR -- 4.1 Relations Among Different Properties of Timed MSR and PTS -- 5 Complexity Results for PTSes -- 5.1 PSPACE-Completeness of Verification Problems for PTSes -- 6 Related and Future Work -- References -- Adapting Constraint Solving to Automatically Analyze UPI Protocols -- 1 Introduction -- 2 Background -- 3 Constraint Solving -- 4 CSolver -- 5 Modeling in the Constraint Solver -- 6 Representation of SMS -- 7 Implementation and Testing -- 8 Conclusion -- References -- Three Branches of Accountability -- 1 Introduction -- 2 The Agent Model -- 3 The Legislative Branch -- 4 The Executive Branch -- 5 The Judicial Branch -- 6 Security Based on Perfect Crimes -- 7 Løglog -- 8 Related Work and Conclusion -- References -- Benign Interaction of Security Domains -- 1 Introduction -- 2 Syntax -- 3 Local Security: Information Flow Type System -- 4 Global Security: Change of Security Domain -- 5 Taking Security Violations into Account -- 6 Conclusion -- A Semantics -- References -- Probabilistic Annotations for Protocol Models -- 1 Introduction -- 2 Crypto-Logical Systems -- 2.1 Crude and Overly General Definition -- 2.2 Information Sets and Preorders of States -- 2.3 Refining the Definition of Crypto-Logical Systems -- 2.4 Probability vs. Knowledge -- 2.5 Global Semantics -- 2.6 Knowledge of Probability vs Probability of Knowledge -- 3 Cryptographic Definitions in Crypto-Logic -- 4 Examples of Reasoning in Crypto-Logic -- 4.1 Security of the Vernam Cryptosystem -- 4.2 El-Gamal. 4.3 Towards Protocols for Noisy Muddy Mistrustful Children -- References -- Joshua Guttman: Pioneering Strand Spaces -- 1 Introduction -- 2 Strand Spaces -- 3 Concluding Remarks -- References -- Cryptographic Protocol Analysis and Compilation Using CPSA and Roletran -- 1 Introduction -- 2 Message Algebras -- 3 Strand Spaces with Channels -- 3.1 Unilateral Protocol Example -- 3.2 Channel Assumptions -- 4 Abstract Execution Semantics -- 4.1 Correctness -- 5 A Runtime with Probabilistic Encryption -- 6 Concrete Execution Semantics -- 7 Relating Execution Semantics -- 8 Epilogue -- References -- On Orderings in Security Models -- 1 Introduction -- 2 Preliminaries -- 3 Attack Trees -- 4 Copland -- 5 Attribute Domains -- 6 Copland Trust Ordering -- 7 Cryptographic Protocols -- 8 Conclusion -- References -- Prototyping Formal Methods Tools: A Protocol Analysis Case Study -- 1 Introduction -- 2 End-To-End Language-Oriented Modeling -- 2.1 Protocol Analysts: Custom Visualization and Queries -- 2.2 The Protocol Creator: Translating Domain-Specific Input -- 2.3 Scripting and Extensibility -- 3 Relational Model Finding -- 4 Modeling Protocol Executions -- 5 Processing cpsa Declarations -- 5.1 Deriving Relational Constraints -- 5.2 Queries and Predicates -- 6 Visualizing Strands -- 7 Prototype Performance -- 8 Related Work -- 9 Discussion -- References -- Principles of Remote Sattestation -- 1 Introduction -- 2 Overview of Self-authenticating Traditional Addresses -- 2.1 Third-Party Sattestation -- 2.2 Trust Yourself..., But Verify -- 3 Principles of (S)attestation -- References --

