1. Record Nr. UNINA9910725087503321

Autore	Kallel Slim
Titolo	Risks and Security of Internet and Systems : 17th International Conference, CRiSIS 2022, Sousse, Tunisia, December 7-9, 2022, Revised Selected Papers / / edited by Slim Kallel, Mohamed Jmaiel, Mohammad Zulkernine, Ahmed Hadj Kacem, Frédéric Cuppens, Nora Cuppens
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031311086 9783031311079
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (268 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13857
Altri autori (Persone)	JmaielMohamed ZulkernineMohammad Hadj KacemAhmed Cuppensédéric CuppensNora
Disciplina	005.8
Soggetti	Data protection Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Context Correlation for Automated Dynamic Android App Analysis to Improve Impact Rating of Privacy and Security Flaws -- 1 Introduction -- 2 Related Work -- 2.1 Contribution -- 3 Dynamic Analysis Environment -- 4 Context Correlation and Issue Generation -- 4.1 Privacy Sensitive Data Sources -- 4.2 Data Sinks -- 4.3 Graph Generation -- 4.4 Example Graph -- 4.5 Graph Analysis: Issue Creation -- 4.6 Issue Correlation Pass -- 5 Evaluation -- 5.1 Overview and Statistics -- 5.2 Deep Manual Issue Inspection -- 5.3 Damn Vulnerable App -- 6 Conclusion and Future Work -- References -- Errors in the CICIDS2017 Dataset and the Significant Differences in Detection Performances It Makes -- 1 Introduction -- 2 Related Works -- 2.1 Datasets -- 2.2 Machine Learning Use on CICDS2017 -- 2.3 Previous Criticism on CICIDS2017 -- 3 Errors in the CICIDS2017 Dataset and the CICFlowMeter Tool, and

Their Fixes -- 3.1 CICFlowMeter Issue with Misordered Packets -- 3.2 Incoherent Timestamps -- 3.3 Dealing with Data Duplication -- 3.4 Attack Omission: Labelling Issues and Correction -- 4 Assessment of the Consequences on Intrusion Detection Models Performances -- 4.1 Experimental Evaluation Protocol -- 4.2 Experiments Results -- 5 Conclusion -- References -- A Comparative Study of Attribute Selection Algorithms on Intrusion Detection System in UAVs: A Case Study of UKM-IDS20 Dataset -- 1 Introduction -- 2 Literature Review -- 3 Dataset and Methods -- 3.1 Dataset -- 3.2 Attribute Selection Algorithms -- 3.3 Creating MLP Model -- 4 Modeling -- 5 Performance Evaluation -- 5.1 Scenario 1: 15 Feature -- 5.2 Scenario 2: 20 Feature -- 6 Conclusion -- References -- PRIAH: Private Alerts in Healthcare -- 1 Introduction -- 2 Background -- 2.1 Smart Hospital Ecosystem -- 2.2 Privacy-preserving Strategies.
2.3 Alert Detection and Edge Computing Paradigm -- 2.4 Big Data and Streaming Processing -- 3 Related Work -- 3.1 Alert Identification and Dissemination -- 3.2 Privacy Preservation -- 3.3 Real-Time Processing of Alerts -- 4 PRIAH Approach -- 4.1 PRIAH Components at the Edge -- 4.2 PRIAH Components at the Server Side -- 4.3 System Administrator -- 4.4 End-Users -- 5 Implementation and Results -- 5.1 Implementation -- 5.2 Evaluation -- 6 Conclusion -- References -- Tool Paper - SEMA: Symbolic Execution Toolchain for Malware Analysis -- 1 Context -- 2 The SEMA Toolset in a Nutshell -- 3 The Architecture of SEMA -- 4 SEMA in Action -- 5 Conclusion -- References -- Blockchain Survey for Security and Privacy in the e-Health Ecosystem -- 1 Introduction -- 2 Research Strategy -- 3 State of the Art -- 4 Background -- 4.1 Blockchain Technology Overview -- 4.2 e-Health Applications -- 5 Security and Privacy Requirements for e-Health Applications -- 6 Blockchain Platforms and Their Security Solutions -- 6.1 Hyperledger Fabric -- 6.2 Hyperledger Besu -- 6.3 Quorum -- 6.4 Corda R3 -- 6.5 Cosmos -- 7 A Security Framework for Blockchain-Based e-Health Applications -- 7.1 When Blockchain Can be Used in e-Health Applications ? -- 7.2 Which Blockchain Solution to Use? -- 8 Conclusions and Future Work -- References -- Towards a Dynamic Testing Approach for Checking the Correctness of Ethereum Smart Contracts -- 1 Introduction -- 2 Background Materials -- 2.1 Blockchain -- 2.2 Smart Contracts -- 2.3 Common Vulnerabilities -- 2.4 Blockchain Testing Techniques -- 3 Related Work -- 4 Proposed Approach -- 4.1 Modelling the Smart Contract and Its Blockchain Environment -- 4.2 Test Case Generation -- 4.3 Test Case Execution -- 4.4 Test Result Analysis and Test Report Generation -- 5 Illustration -- 5.1 Case Study Description -- 5.2 Modelling the E-voting System.
5.3 Test Case Generation -- 5.4 Test Tool Implementation -- 6 Conclusion -- References -- Blockchain Olive Oil Supply Chain -- 1 Introduction -- 2 Related Work -- 3 Proposed Approach -- 4 Obtained Results -- 4.1 Implemented Blockchain on Raspberry Pi -- 4.2 Web Application -- 5 Conclusion -- References -- Impact of EIP-1559 on Transactions in the Ethereum Blockchain and Its Rollups -- 1 Introduction -- 2 Background -- 2.1 Layers 1 and 2 in Ethereum -- 2.2 Eip-1559 -- 3 Testing Approach -- 3.1 Smart Contract -- 3.2 Interaction with the Smart Contract -- 4 Experimentation -- 4.1 Testing Results -- 4.2 Discussion -- 5 Conclusion -- References -- Towards a Secure Cross-Blockchain Smart Contract Architecture -- 1 Introduction -- 2 Background and Related Work -- 3 Bifröst Extension Proposal -- 3.1 Smart Contracts Invocation -- 3.2 Fault Tolerance -- 3.3 Security -- 4 Discussion and Challenges -- 5 Conclusion and Future Work -- References -- Security Analysis: From Model to System Analysis -- 1 Introduction -- 2 Background -- 2.1 Previous MBSE

Approach -- 2.2 Property Specification Patterns -- 2.3 OBP Model Checker -- 3 Motivating Example -- 3.1 System Presentation -- 3.2 General Approach -- 4 Detailed Approach -- 4.1 Environment Modeling -- 4.2 System State and Behavior -- 4.3 The OBP Model Checker -- 5 Security Property Modelling -- 5.1 Raising Abstraction Level of Formal Security Properties -- 5.2 From Attacker Interests to Formal Security Properties -- 6 Property Verification Results Analysis -- 6.1 Model Checking Embedded System Code -- 6.2 Security Property Verification -- 7 Related Works -- 8 Conclusion -- References -- Modeling Train Systems: From High-Level Architecture Graphical Models to Formal Specifications -- 1 Introduction -- 2 Background -- 2.1 Model-Driven Engineering -- 2.2 SysML -- 2.3 Event-B -- 2.4 ATO over ERTMS Case Study Excerpt.
3 Related Work -- 4 The Proposed Approach -- 4.1 High-level Architecture Graphical Modeling -- 4.2 Model Transformation and Event-B Generation -- 4.3 Formal Verification -- 5 Conclusion -- References -- How IT Infrastructures Break: Better Modeling for Better Risk Management -- 1 Introduction -- 2 Related Work -- 2.1 Risk Analysis -- 2.2 Infrastructure Modeling -- 3 Guided Risk Management for IT Infrastructures -- 3.1 Side-Effect Analysis -- 3.2 Part Analysis -- 3.3 Assembly Analysis -- 4 Case Study: A Cloud Infrastructure -- 4.1 Requirements -- 4.2 Infrastructure Model -- 4.3 Constraints -- 4.4 Risk -- 4.5 Lessons Learned -- 5 Conclusion and Future Work -- References -- IoT Security Within Small and Medium-Sized Manufacturing Companies -- 1 Introduction -- 2 Research Methodology -- 3 Data and Findings -- 3.1 Screening -- 3.2 Experience -- 3.3 Awareness -- 3.4 Activities -- 3.5 Knowledge -- 4 Conclusion and Further Research -- References -- An Incentive Mechanism for Managing Obligation Delegation -- 1 Introduction -- 2 Background -- 2.1 The Beta Distribution -- 2.2 Defining Obligations -- 3 An Incentive Scheme for One Hop Delegation -- 3.1 Obligation Trust -- 3.2 Delegating Obligations -- 4 Incentivising Schemes -- 4.1 Updating Obligation Trust -- 4.2 Earning Reward Credits -- 4.3 Eligibility of Delegatees -- 5 Cascaded Delegation of Obligations -- 6 Evaluation -- 6.1 Experimental Setup -- 6.2 Results -- 7 Related Work -- 8 Concluding Remarks -- References -- Virtual Private Network Blockchain-based Dynamic Access Control Solution for Inter-organisational Large Scale IoT Networks -- 1 Introduction -- 2 Background -- 2.1 Blockchain -- 2.2 Virtual Private Networks (VPN) -- 3 Related Work -- 3.1 Basic Access Control Model in IoTs -- 3.2 Inter-organisational Access Control Solution Overview -- 4 VPNBDAC for Large Scale IoT Network -- 4.1 Actors.
4.2 Smart Contract and Transactions -- 5 Implementation of the Prototype -- 6 Performance Evaluation -- 7 Conclusions -- References -- Pseudonym Swapping with Secure Accumulators and Double Diffie-Hellman Rounds in Cooperative Intelligent Transport Systems -- 1 Introduction -- 1.1 Pseudonyms in Cooperative Intelligent Transport Systems -- 1.2 Problem Statement -- 1.3 Contribution -- 2 Related Work -- 3 Preliminaries -- 4 System Model and Architecture -- 4.1 C-ITS Trust Model and Architecture -- 4.2 Threat Model -- 4.3 Pseudonym Swapping System Model -- 5 Pseudonym Swapping with Accumulator-Based Storage -- 5.1 Proposed Alignment to ETSI Standard -- 5.2 Proposed Security Architecture -- 5.3 Protocol Definition and Algorithms -- 6 Security Analysis -- 7 Proof of Concept Implementation -- 8 Conclusion -- References -- Benchmark Performance of the Multivariate Polynomial Public Key Encapsulation Mechanism -- 1 Introduction -- 2 Related Work -- 3 Summary of MPPK KEM -- 3.1 Key Generation -- 3.2 Encryption -- 3.3 Decryption -- 4

	Benchmarking MPPK -- 4.1 NIST Level I -- 4.2 NIST Level III -- 4.3 NIST Level V -- 5 Conclusion -- References -- Author Index.
Sommario/riassunto	This book constitutes the proceedings of the 17th International Conference on Risks and Security of Internet and Systems, CRiSIS 2022, which took place in Sousse, Tunesia, during December 7-9, 2022. The 14full papers and 4 short papers included in this volume were carefully reviewed and selected from 39 submissions. The papers detail security issues in internet-related applications, networks and systems.