1. Record Nr. UNISA996490357303316

Titolo	Science of cyber security : 4th international conference, SciSec 2022, Matsue, Japan, August 10-12, 2022, revised selected papers / / edited by Chunhua Su, Kouichi Sakurai, and Feng Liu
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-17551-4
Descrizione fisica	1 online resource (575 pages)
Collana	Lecture Notes in Computer Science ; ; v.13580
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Blockchain and Applications -- ChainSCAN: A Blockchain-Based Supply Chain Alerting Framework for Food Safety -- 1 Introduction -- 2 Related Work -- 3 Threat Model -- 4 ChainSCAN Framework -- 4.1 Data Layer -- 4.2 BC Layer -- 4.3 APP Layer -- 5 ChainSCAN Prototype Evaluation -- 5.1 Prototype Implementation -- 5.2 Performance Evaluation -- 5.3 Security Analysis of ChainSCAN -- 6 Conclusion -- References -- BlockRAT: An Enhanced Remote Access Trojan Framework via Blockchain -- 1 Introduction -- 2 Background and Related Work -- 2.1 RAT, Botnets and C2 Channel -- 2.2 Blockchain Technology in RAT -- 2.3 Related Work -- 3 Our Approach -- 3.1 System Design -- 3.2 Attack Characteristics -- 4 Implementation Detail -- 4.1 Challenge and Solution 1: Blockchain Selection -- 4.2 Challenge and Solution 2: Obvious Traffic Characteristics -- 4.3 Challenge and Solution 3: Backdoor Persistence -- 5 Evaluation -- 5.1 Comparison with Common RATs -- 5.2 Effectiveness Evaluation -- 5.3 Comparison with Existing Blockchain-based RATs/botnets -- 5.4 Limitation and Discussion -- 6 Conclusions -- References -- Adapted PBFT Consensus Protocol for Sharded Blockchain -- 1 Introduction -- 2 Related Work -- 2.1 Sharded Blockchain -- 2.2 PBFT Algorithms -- 3 Background and Preliminaries -- 3.1 Blockchain Sharding -- 3.2 BFT Consensus Algorithms -- 4 Solution: A New Cross-shard BFT Consensus -- 4.1 Committee-wise

Monitoring -- 4.2 How Does It Work? -- 4.3 Performance Guarantee Analysis -- 5 Performance Evaluation -- 5.1 Settings -- 5.2 Baseline Algorithms -- 5.3 Performance Discussion -- 6 Conclusion -- References -- A Practical Blockchain-Based Maintenance Record System for Better Aircraft Security -- 1 Introduction -- 2 Background and Related Work -- 2.1 Background on Blockchain -- 2.2 Blockchain in Aircraft Maintenance.
3 Our Proposed System - AirChain -- 3.1 Blockchain Platform Analysis and Selection -- 3.2 System Overview -- 3.3 Front-End Design and Implementation -- 4 Evaluation -- 4.1 Storage Growth -- 4.2 Processing Time -- 5 Limitations and Discussion -- 5.1 Scalability: Adding Smart Contracts -- 5.2 Security -- 6 Conclusion -- References -- Redactable Blockchain with Fine-Grained Autonomy and Transaction Rollback -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Gap Diffie-Hellman (GDH) Group -- 2.3 Double Trapdoor Chameleon Hash Function -- 2.4 The Chameleon Hashing Without Key Exposure -- 2.5 A Discrete Log-Based Double Trapdoor Commitment Scheme -- 2.6 Blocks and Chain -- 2.7 Publicly Verifiable Secret Sharing (PVSS) -- 3 Double Trapdoor Key-exposure Free Chameleon Hash Function -- 3.1 Our Double Trapdoor Key-Exposure Free Chameleon Hash Function -- 4 Blockchain Redacting Protocol -- 4.1 Redactable Blockchain System -- 4.2 Technique Overview -- 4.3 Block Information Revision -- 4.4 Transaction Rollback -- 5 Conclusion -- References -- Cryptography and Applications -- Pitch in: A Secure Extension Signature Based on SM9 -- 1 Introduction -- 1.1 Related Work -- 1.2 Our Contribution -- 1.3 Organization -- 2 Preliminaries -- 2.1 Definitions -- 2.2 The SM9-IBS -- 2.3 q-Strong Diffie-Hellman Problem -- 3 Our Scheme -- 3.1 Notation -- 3.2 Construction -- 4 Analysis -- 4.1 Correctness -- 4.2 Security Results -- 5 Efficiency Discussions -- 6 Conclusion -- References -- Verifiable DOPE from Somewhat Homomorphic Encryption, and the Extension to DOT -- 1 Introduction -- 1.1 Background -- 1.2 Our Contribution -- 2 Preliminaries -- 2.1 Model -- 2.2 Shamir's Secret Sharing -- 2.3 The Paillier Cryptosystem -- 2.4 Message Authentication Code -- 2.5 Security -- 3 Our Protocol -- 3.1 Setup Phase -- 3.2 Computation Phase -- 4 Security Evaluation -- 5 Extension to DOT.
6 Conclusion -- References -- Scalable M+1st-Price Auction with Infinite Bidding Price -- 1 Introduction -- 2 Related Works -- 3 Preliminaries -- 4 Our Protocol -- 4.1 Auction Protocol -- 4.2 Features and Security -- 5 Implementation and Optimization -- 6 Comparison -- 7 Conclusion -- References -- The Shared Memory Based Cryptographic Card Virtualization -- 1 Introduction -- 2 Related Work -- 2.1 Software Virtualization -- 2.2 Hardware-Assisted Virtualization -- 3 Framework -- 4 Implementation -- 4.1 Shared Memory -- 4.2 Frontend Service -- 4.3 Backend Service -- 5 Performance Evaluation -- 5.1 Experiment Environment -- 5.2 Data Transfer Performance Test -- 5.3 Encryption Algorithm Performance Test -- 5.4 Performance Test After Optimization -- 6 Summary and Outlook -- References -- Network Security -- Feature Transfer Based Network Anomaly Detection -- 1 Introduction -- 1.1 Motivation -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Transformer -- 2.2 Experimental Data Set -- 2.3 Evaluation Indicators -- 3 Feature Transfer Based Anomaly Detection Model -- 3.1 Framework -- 3.2 Data Pre-processing -- 3.3 Model Training -- 4 Experimental Results and Analysis -- 4.1 Identification of Various Types of Known Attacks -- 4.2 Identification of Various Types of Unknown Attacks -- 5 Conclusion -- References -- Hybrid Routing for Efficient Fine-Grained Management of Specific Services in SDN -- 1 Introduction -- 2 Related Work -- 3 Motivation and Our

Intuition -- 4 Network Mode and Hybrid Routing for Efficient Fine-grained Management -- 4.1 Network Model -- 4.2 Heterogeneous Rule Installment for Case A -- 4.3 Heterogeneous Rule Installment for Case B -- 4.4 Heterogeneous Rule Installment for Case C -- 5 Performance Evaluation -- 5.1 Testbed Evaluation -- 5.2 Simulation Evaluation -- 6 Conclusion -- References.
AtNet: A Novel Anti-tracking Network with Multi-Party Judgement Capability Based on Cross-Domain Small-World Topology -- 1 Introduction -- 2 Related Work -- 3 Designing AtNet -- 3.1 The Overview of AtNet -- 3.2 The Construction of AtNet -- 3.3 The Maintenance of AtNet -- 3.4 Multi-party Judgement Mechanism on AtNet -- 4 Experiment and Evaluation -- 4.1 Evaluation of Network Robustness -- 4.2 Evaluation of Maintenance Effect -- 4.3 Evaluation of Multi-party Judgement Capability -- 5 Conclusion and Future Work -- References -- A Two-Stage Method for Fine-Grained DNS Covert Tunnel Behavior Detection -- 1 Introduction -- 2 Background and Related Work -- 2.1 DNS Covert Tunnel -- 2.2 Related Work -- 3 Method -- 3.1 DNS Covert Tunnel Behavior Detection Framework -- 3.2 DNS Covert Tunnel Traffic Detection -- 3.3 DNS Covert Tunnel Behavior Detection -- 4 Evaluation -- 4.1 Dataset -- 4.2 Performance Metrics -- 4.3 DNS Covert Tunnel Traffic Detection Evaluation -- 4.4 DNS Covert Tunnel Behavior Detection Evaluation -- 5 Conclusion -- References -- Analysis and Detection Against Overlapping Phenomenon of Behavioral Attribute in Network Attacks -- 1 Introduction -- 2 Background and Related Work -- 2.1 UNSW-NB15 -- 2.2 CIC-AndMal-2020 -- 3 Analysis of Overlapping Phenomenon -- 3.1 Overview -- 3.2 Definition of Overlapping Phenomenon -- 3.3 Case Analysis of Overlapping Phenomenon -- 3.4 Cause Analysis of Overlapping Phenomenon -- 3.5 Experimental Statistics of Overlapping Phenomenon -- 3.6 Data Re-labeling -- 4 Multi-label Attack Detection and Evaluation -- 4.1 Definition of Multi-label Attack Detection Problem -- 4.2 Multi-label Detection Methods -- 4.3 Experiment and Evaluation -- 5 Discussion -- 5.1 Performance of Multi-label Detection Methods -- 5.2 Application Scenarios for Overlapping Phenomenon Analysis -- 6 Conclusion -- References.
Integration of Cybersecurity Related Development Processes by Using a Quantification Method -- 1 Introduction -- 1.1 Measurement of Cybersecurity Relevant Development Processes According to ISO 21434 -- 1.2 Classification of the Security Relevant Processes in the V-Model -- 2 Quantification of the Cybersecurity Relevant Processes -- 2.1 Determination of the Supporting Processes for the Evaluation of the Preconditions -- 2.2 Preconditional Coefficient (PCC) for the Quantification of the Maturity -- 3 Application Example on an Automotive Project for an ADAS System -- 3.1 Derivation of a Measure Based on the Result of the Preconditional Coefficient -- 4 Summary and Discussion -- References -- Cyber-Physical System -- ZoomPass: A Zoom-Based Android Unlock Scheme on Smart Devices -- 1 Introduction -- 2 Related Work -- 2.1 Authentication Based on Graphical Password -- 2.2 Touch Behavioral Authentication -- 3 ZoomPass Design -- 4 User Study -- 5 Discussion -- 6 Conclusion -- References -- Metasploit for Cyber-Physical Security Testing with Real-Time Constraints -- 1 Introduction -- 2 Related Work -- 3 Background: Cyber-Attack as a Real-Time Process -- 4 Methodology -- 4.1 Program Configuration -- 4.2 Experimental Setup -- 4.3 Experiments -- 5 Results and Discussion -- 6 Case Study -- 7 Conclusion -- References -- Passive User Authentication Utilizing Consecutive Touch Action Features for IIoT Systems -- 1 Introduction -- 2 Consecutive Touch Actions Based Passive Authentication -- 2.1 User Identity

Characterization Based on Time-Varying Touch Action Sequence -- 2.2 User Identity Characterization Based on Cumulative Touch Screen Action Trajectories -- 2.3 User Authentication Based on both HMM and PatternNet -- 3 Experiment and Analysis -- 3.1 Influence of the Number of Touch Screen Actions -- 3.2 Performance of Resisting Impersonation Attacks -- 4 Conclusion.
References.