1.

Record Nr.	UNISA996464409203316
Titolo	Silicon valley cybersecurity conference : first conference, svcc 2020, san jose, ca, usa, december 17-19, 2020, revised selected papers / / edited by Younghee Park, Divyesh Jadav, Thomas Austin
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-72725-4
Descrizione fisica	1 online resource (232 pages) : illustrations
Collana	Communications in Computer and Information Science ; ; v.1383
Disciplina	005.8
Soggetti	Artificial intelligence
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 -- Application and Network Security -- Dynamic Security Analysis of Zoom, Google Meet and Microsoft Teams -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Materials -- 3.2 Experimental Setup -- 3.3 Data Collected -- 4 Results -- 4.1 Analysis -- 4.2 End to End Encryption -- 4.3 Call Setup and Cipher Suites -- 4.4 Encrypted in Transit -- 4.5 Encrypted at Rest -- 4.6 Past Communications Secure -- 4.7 Verifiable Contacts -- 4.8 Open Source Code -- 4.9 Properly Documented Security Design -- 4.10 Metadata -- 4.11 Additional Findings -- 5 Evaluation -- 6 Limitations and Future Work -- 7 Conclusion -- References -- A Secure Encapsulation Schemes Based on Key Recovery System -- 1 Introduction -- 2 Related Work -- 2.1 Encapsulation Key Recovery System -- 2.2 Multi-agent Key Recovery -- 2.3 Signcryption -- 2.4 Proxy Re-Encryption -- 3 System Models -- 3.1 Key Recovery System Using Signcryption -- 3.2 Key Recovery System Using Proxy Re-Encryption -- 4 Proposed Schemes -- 4.1 Key Recovery System Using Signcryption -- 4.2 Key Recovery System Using Proxy Re-Encryption -- 5 Analysis of the Proposed Schemes -- 5.1 Key Recovery System Using Signcryption (Proposed Scheme1) -- 5.2 Key Recovery System Using Proxy Re-Encryption (Proposed Scheme2) -- 6 Conclusions -- References -- Path Authentication Protocol: Based on a Lightweight MAC and a Nonlinear Filter Generator -- 1 Introduction -- 2

Preliminaries -- 2.1 Message Authentication Code -- 2.2 Chaskey -- 2.3 Controller Area Network -- 2.4 Pseudorandom Number Generator -- 3 A New Protocol -- 3.1 Conditions of NLFG -- 3.2 The Flow of Protocol -- 3.3 Security Analysis -- 4 Experiment and Result -- 4.1 Assumption and Experimental Enviroments -- 4.2 Experimental Result and Consideration -- 5 Conclusion -- References.

STRISA: A New Regulation Architecture to Enforce Travel Rule -- 1 Introduction -- 2 TRISA Introduction -- 2.1 VASP Certificate -- 2.2 Authentication Between VASPs -- 3 STRISA Framework -- 3.1 STRISA Network -- 3.2 BDL System -- 3.3 Blockchain-Based AML Regulation System -- 4 Related Work -- 4.1 CFTC -- 4.2 Blockchain Databases -- 4.3 ABC/TBC Architecture -- 5 Conclusion -- References -- System Security -- Post-quantum Hash-Based Signatures for Secure Boot -- 1 Introduction -- 2 Related Work -- 3 HBS for Secure Boot -- 3.1 Intro to HBS -- 3.2 Hierarchy -- 3.3 Parameters -- 4 Experiments -- 4.1 RSA vs. LMS vs. SPHINCS+ -- 4.2 FPGA-Based Signature Verification -- 5 Conclusion -- References -- Exploring the Coverage of Existing Hardware Vulnerabilities in Community Standards -- 1 Introduction and Motivations -- 2 Survey of Hardware Security Categorizations -- 2.1 Trusted and Assured MicroElectronics Forum -- 2.2 Common Attack Pattern Enumeration and Classification (CAPEC) -- 2.3 SAE G-32 Cyber Physical Systems Security Committee -- 2.4 Trust-Hub -- 2.5 CVE and CWE -- 3 CWE 4.x Hardware Categories -- 4 Conclusion -- References -- MurQRI: Encrypted Multi-layer QR Codes for Electronic Identity Management -- 1 Introduction -- 2 Background -- 2.1 Multi-layer QR Code -- 2.2 Attribute-Based Encryption -- 3 Proposed Scheme -- 4 Real-World Applications -- 4.1 MurQRI for Electronic Identification in Airports -- 4.2 MurQRI for Patient Data in Hospitals -- 5 Discussion -- 5.1 Utilizing Biometric Authentications -- 5.2 Utilizing Secret Hiding -- 6 Related Work -- 7 Conclusion and Further Work -- References -- An Attack on Quantum Circuits Based on the Error Rates of NISQ Systems and a Countermeasure -- 1 Introduction -- 2 Attack -- 3 Countermeasure -- 4 Validation -- 5 Conclusion -- References -- Blockchain and Security.

SpartanGold: A Blockchain for Education, Experimentation, and Rapid Prototyping -- 1 Introduction -- 2 Popular Cryptocurrency Code Bases -- 3 Choice of JavaScript -- 4 SpartanGold Design -- 4.1 Classes -- 4.2 Single-Threaded Mode -- 4.3 Multi-process Mode -- 5 Use Cases -- 5.1 Mining Pools -- 5.2 Unspent Transaction Output Model -- 6 Conclusion and Future Work -- References -- BIOT: A Blockchain-Based IoT Platform for Distributed Energy Resource Management -- 1 Introduction -- 2 Research Baseline -- 3 BIoT Distributed Platform -- 4 Evaluation -- 4.1 Cybersecurity -- 4.2 Performance -- 5 Related Works -- 6 Conclusions and Future Work -- References -- A Privacy Preserving E-Voting System Based on Blockchain -- 1 Introduction -- 2 Background -- 2.1 Problem of E-Voting Systems -- 2.2 Blockchain Technology -- 3 Our Approach -- 3.1 System Overview -- 3.2 System Components in Detail -- 4 Evaluation -- 4.1 Experiment Setup -- 4.2 Experimental Results -- 5 Related Work -- 6 Conclusion -- References -- BioBlockchain: Useful Proof-of-Work with Multiple Sequence Alignment -- 1 Introduction -- 2 Multiple Sequence Alignment in Bioinformatics -- 2.1 Common Tool for MSA -- 2.2 Multiple Sequence Alignment Using Genetic Algorithms -- 3 Mining Process -- 4 Essential Properties of Proof-of-Work -- 4.1 Difficulty Adjustability -- 4.2 Efficient Verification -- 4.3 Precomputation Resistance -- 4.4 Non-reusability -- 5 BioBlockchain Architecture -- 6 Conclusion -- References -- Machine Learning for Security -- Reconstructing Classification to Enhance Machine-Learning Based Network Intrusion

Detection by Embracing Ambiguity -- 1 Introduction -- 2 Reconstructing Classification by Embracing Ambiguity -- 2.1 Classify into Three Classes -- 2.2 Ambiguous Dataset -- 3 Model Build -- 3.1 Classification Algorithms -- 3.2 Confidence of Decision -- 4 Evaluation -- 4.1 Feature Sets.

4.2 Preprocessing -- 4.3 Results: Performance of Base Classifiers -- 4.4 Results: Performance of Ensemble Classifier -- 4.5 Results: Misclassified Dataset -- 4.6 Results: Unknown Datasets -- 4.7 Results: Re-evaluation of Ambiguous Dataset -- 5 Related Works -- 6 Conclusion -- References -- A Systematic Approach to Building Autoencoders for Intrusion Detection -- 1 Introduction -- 2 Related Work -- 2.1 Autoencoders for Feature Reduction -- 2.2 Autoencoders for Anomaly Detection -- 3 Our Approach -- 3.1 An Overview -- 3.2 Model Design -- 3.3 Threshold Selection -- 4 Dataset -- 4.1 CIC-IDS 2017 Data -- 4.2 NSL-KDD Data -- 5 Evaluation -- 5.1 PCA Analysis -- 5.2 Experiment 1: CIC-IDS 2017 Data -- 5.3 Experiment: NSL-KDD Data -- 5.4 Discussions -- 6 Conclusion -- References -- ConTheModel: Can We Modify Tweets to Confuse Classifier Models? -- 1 Introduction -- 2 Related Work -- 3 ConTheModel Overview -- 3.1 Dataset -- 3.2 System Methodology and Algorithm -- 4 Evaluation -- 4.1 Evaluation Setup -- 4.2 Evaluation Metrics -- 4.3 Classifiers -- 5 Classification Results -- 6 Human Evaluation -- 7 Conclusion -- References -- IoT Checker Using Timing Side-Channel and Machine Learning -- 1 Introduction -- 2 Literature Review -- 3 Project Architecture -- 4 Methodology -- 4.1 Experimental Setup -- 4.2 Implementation of Attacks -- 4.3 Machine Learning Implementation -- 5 Result -- 6 Conclusion -- References -- Author Index.