1.

Record Nr.	UNISA996594166403316
Autore	Kim Dan Dongseong
Titolo	Machine Learning for Cyber Security : 5th International Conference, ML4CS 2023, Yanuca Island, Fiji, December 4-6, 2023, Proceedings
Pubbl/distr/stampa	Singapore : , : Springer Singapore Pte. Limited, , 2024 ©2024
ISBN	981-9724-58-9
Edizione	[1st ed.]
Descrizione fisica	1 online resource (186 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14541
Altri autori (Persone)	ChenChao
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Keystroke Transcription from Acoustic Emanations Using Continuous Wavelet Transform -- 1 Introduction -- 2 Related Work -- 3 Dataset -- 4 Keystroke Transcription -- 4.1 Continuous Wavelet Transform -- 4.2 Keystroke Detection and Segmentation -- 4.3 Normalization and Feature Extraction -- 4.4 Keystroke Classification -- 5 Results -- 5.1 Segmentation -- 5.2 Feature Extraction -- 5.3 Classification -- 6 Discussion -- 7 Conclusions -- References -- Strengthening Cyber Security Education: Designing Robust Assessments for ChatGPT-Generated Answers -- 1 Introduction -- 2 Related Work -- 3 Research Methodology -- 4 Results and Analysis -- 5 Recommendations -- 6 Conclusion -- References -- PassFile: Graphical Password Authentication Based on File Browsing Records -- 1 Introduction -- 2 Related Work -- 2.1 Graphical Password -- 2.2 Smart Unlock Mechanism -- 3 Our Proposed Scheme -- 4 User Study -- 4.1 Steps and Results -- 4.2 User Feedback -- 5 Discussion on Limitations and Enhancement -- 6 Conclusion -- References -- On the Role of Similarity in Detecting Masquerading Files -- 1 Introduction -- 2 A Taxonomy of Masquerading Files -- 3 Collecting Masquerading Files -- 3.1 Step 1: Building Clustering Model -- 3.2 Step 2: Processing Malware Bazaar -- 3.3 Masquerading Results -- 3.4 The No Signature Case -- 3.5 The Not Verified Case -- 3.6 The Contains a X509 Certificate Case -- 3.7 The Certificate Revoked Case -- 3.8 The Certificate Used for

Signing Malware Case -- 3.9 The No Trusted Root Authority Case -- 4 Finding Masquerading Files in Clusters -- 5 Clusters Related to Supply Chain Attacks -- 6 Conclusion and Future Work -- References -- A Password-Based Mutual Authenticated Key Exchange Scheme by Blockchain for WBAN -- 1 Introduction -- 2 Related Works -- 3 Preliminaries -- 3.1 Complexity Problems.

3.2 OPAQUE -- 4 System Model and Security Requirements -- 4.1 System Model -- 4.2 Security Requirements -- 5 The Proposed Scheme -- 5.1 Registration of Remote Medical Server -- 5.2 Broadcasting of Service Messages -- 5.3 Registration of User -- 5.4 Authentication and Key Agreement -- 6 Security Analyses -- 7 Performance Evaluation -- 7.1 Some Comparison -- 7.2 Computation Performance -- 7.3 Communication Performance -- 8 Conclusion -- References -- Traffic Signal Timing Optimization Based on Intersection Importance in Vehicle-Road Collaboration -- 1 Introduction -- 2 Related Work -- 2.1 Graph Neural Network in Traffic -- 2.2 Reinforcement Learning in Traffic Signal Timing Optimization -- 3 Methods -- 3.1 Framework Overview -- 3.2 Constructing Traffic Light Directed Adjacency Graph -- 3.3 Calculating the Importance of Adjacent Nodes -- 3.4 Modeling Reinforcement Learning Method -- 4 Experiments -- 4.1 Experimental Setup -- 4.2 Datasets -- 4.3 Evaluation Metrics -- 4.4 Experimental Results -- 5 Conclusion -- References -- A Client-Side Watermarking with Private-Class in Federated Learning -- 1 Introduction -- 2 Related Works -- 2.1 Deep Learning Watermark -- 2.2 Federated Learning Watermark -- 3 Application Scenario and Watermark Requirements -- 3.1 Application Scenario -- 3.2 Watermark Requirements in Federated Learning -- 4 Proposed Method -- 4.1 Watermark Dataset Generation -- 4.2 Watermark Embedding -- 4.3 Watermark Verification -- 5 Experimental Evaluation -- 5.1 Experiment Settings -- 5.2 Performance Analysis -- 6 Conclusion -- References -- Research on Evasion and Detection of Malicious JavaScript Code -- 1 Introduction -- 2 Relative Work -- 2.1 Techniques for Detecting Malicious Code -- 2.2 Taint Analysis Techniques -- 3 Analysis of Features of Malicious JavaScript Code -- 4 Taint Propagation Methods -- 4.1 Forward Taint Propagation.

4.2 Tracking the Initialization Process of Suspicious Objects -- 4.3 Backward Taint Propagation -- 4.4 Propagation Policies -- 4.5 Discussion on Overtainting and Undertainting Issues -- 5 Theoretical Analysis of the Feasibility of Obfuscation Resistance -- 6 Feature Extraction and Vectorization -- 6.1 Feature Extraction -- 6.2 Vectorization -- 7 Experiments -- 7.1 Dataset and Detection Models -- 7.2 Analysis of Pollution in the Samples -- 7.3 Test Results and Analysis -- 7.4 Comparison with VirusTotal Results -- 8 Conclusion -- References -- Tackling Non-IID for Federated Learning with Components Alignment -- 1 Introduction -- 2 Related Work -- 2.1 Federated Learning -- 2.2 IID Data Construction -- 2.3 Local Models Assimilation -- 3 FCA: Federated Components Alignment -- 3.1 System -- 3.2 Motivation -- 3.3 Method -- 4 Experimental Evaluation -- 4.1 Experimental Setup -- 4.2 Experimental Results -- 4.3 Parameter Configuration -- 5 Summary and Future Work -- References -- Security on Top of Security: Detecting Malicious Firewall Policy Changes via K-Means Clustering -- 1 Introduction -- 2 Our Approach -- 2.1 Goals and Requirements -- 2.2 Design Architecture and Clustering Method -- 2.3 Implementation Details -- 3 Evaluation -- 3.1 Dataset and Pre-processing -- 3.2 Number of Features -- 3.3 Evaluation Results -- 4 Related Work and Discussion -- 4.1 State-of-the-Art -- 4.2 Discussion -- 5 Conclusion -- References -- Penetrating Machine Learning Servers via Exploiting BMC Vulnerability -- 1 Introduction -- 2 Method -- 2.1

Patch the Firmware -- 2.2 Inject the Shellcode to Kernel -- 2.3 Bypass KASLR -- 3 Experiment -- 4 Related Work -- 4.1 Attack on Firmware -- 4.2 Bypass KASLR -- 5 Conclusion -- References -- Author Index.