

Seyit A Camtepe

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/647752/publications.pdf>

Version: 2024-02-01

79
papers

2,976
citations

279701

23
h-index

254106

43
g-index

85
all docs

85
docs citations

85
times ranked

2187
citing authors

#	ARTICLE	IF	CITATIONS
1	A Survey on Cyber Situation-awareness Systems: Framework, Techniques, and Insights. ACM Computing Surveys, 2023, 55, 1-37.	16.1	14
2	Vulnerability Detection in IoT Applications: A Fuzzing Method on their Binaries. IEEE Transactions on Network Science and Engineering, 2022, 9, 970-979.	4.1	2
3	Backdoor Attack on Machine Learning Based Android Malware Detectors. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 3357-3370.	3.7	13
4	Evaluation and Optimization of Distributed Machine Learning Techniques for Internet of Things. IEEE Transactions on Computers, 2022, 71, 2538-2552.	2.4	23
5	Physical publicly verifiable randomness from pulsars. Astronomy and Computing, 2022, 38, 100549.	0.8	3
6	Fuzzing: A Survey for Roadmap. ACM Computing Surveys, 2022, 54, 1-36.	16.1	61
7	A few-shot meta-learning based siamese neural network using entropy features for ransomware classification. Computers and Security, 2022, 117, 102691.	4.0	28
8	A channel perceiving attack and the countermeasure on long-range IoT physical layer key generation. Computer Communications, 2022, 191, 108-118.	3.1	3
9	ANS-based compression and encryption with 128-bit security. International Journal of Information Security, 2022, 21, 1051-1067.	2.3	2
10	Performance and Information Leakage in Splitfed Learning and Multi-Head Split Learning in Healthcare Data and Beyond. Methods and Protocols, 2022, 5, 60.	0.9	3
11	Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey. IEEE Internet of Things Journal, 2021, 8, 4132-4156.	5.5	48
12	Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in Biology and Medicine, 2021, 129, 104130.	3.9	80
13	Using Process Mining to Identify File System Metrics Impacted by Ransomware Execution. Lecture Notes in Computer Science, 2021, , 57-71.	1.0	0
14	Compcryptâ€“Lightweight ANS-Based Compression and Encryption. IEEE Transactions on Information Forensics and Security, 2021, 16, 3859-3873.	4.5	11
15	Privacy preserving distributed machine learning with federated learning. Computer Communications, 2021, 171, 112-125.	3.1	60
16	PPaaS: Privacy Preservation as a Service. Computer Communications, 2021, 173, 192-205.	3.1	6
17	DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks. Future Generation Computer Systems, 2021, 118, 240-251.	4.9	24
18	Synthesized Corpora to Evaluate Fuzzing for Green Internet of Things Programs. IEEE Transactions on Green Communications and Networking, 2021, 5, 1041-1050.	3.5	1

#	ARTICLE	IF	CITATIONS
19	Advancements of Federated Learning Towards Privacy Preservation: From Federated Learning to Split Learning. <i>Studies in Computational Intelligence</i> , 2021, , 79-109.	0.7	20
20	AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification. <i>IEEE Access</i> , 2021, 9, 146810-146821.	2.6	56
21	FedDICE: A Ransomware Spread Detection in a Distributed Integrated Clinical Environment Using Federated Learning and SDN Based Mitigation. <i>Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering</i> , 2021, , 3-24.	0.2	3
22	A Secure Access and Accountability Framework for Provisioning Services in Named Data Networks. , 2021, , .		4
23	Evaluating the Security of Machine Learning Based IoT Device Identification Systems Against Adversarial Examples. <i>Lecture Notes in Computer Science</i> , 2021, , 800-810.	1.0	2
24	Local Differential Privacy for Deep Learning. <i>IEEE Internet of Things Journal</i> , 2020, 7, 5827-5842.	5.5	116
25	CSI-Fuzz: Full-speed Edge Tracing Using Coverage Sensitive Instrumentation. <i>IEEE Transactions on Dependable and Secure Computing</i> , 2020, , 1-1.	3.7	6
26	Continuous authentication for VANET. <i>Vehicular Communications</i> , 2020, 25, 100255.	2.7	17
27	Privacy Preserving Face Recognition Utilizing Differential Privacy. <i>Computers and Security</i> , 2020, 97, 101951.	4.0	60
28	A Trustworthy Privacy Preserving Framework for Machine Learning in Industrial IoT Systems. <i>IEEE Transactions on Industrial Informatics</i> , 2020, 16, 6092-6102.	7.2	138
29	An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network. <i>IEEE Transactions on Information Forensics and Security</i> , 2020, 15, 3107-3122.	4.5	34
30	Can We Use Split Learning on 1D CNN Models for Privacy Preserving Training?. , 2020, , .		51
31	Stochastic Modeling of IoT Botnet Spread: A Short Survey on Mobile Malware Spread Modeling. <i>IEEE Access</i> , 2020, 8, 228818-228830.	2.6	19
32	An Accountable Access Control Scheme for Hierarchical Content in Named Data Networks with Revocation. <i>Lecture Notes in Computer Science</i> , 2020, , 569-590.	1.0	6
33	Identity-Based Broadcast Encryption with Outsourced Partial Decryption for Hybrid Security Models in Edge Computing. , 2019, , .		9
34	An efficient and scalable privacy preserving algorithm for big data and data streams. <i>Computers and Security</i> , 2019, 87, 101570.	4.0	50
35	A Feature-Oriented Corpus for Understanding, Evaluating and Improving Fuzz Testing. , 2019, , .		8
36	Outlier Dirichlet Mixture Mechanism: Adversarial Statistical Learning for Anomaly Detection in the Fog. <i>IEEE Transactions on Information Forensics and Security</i> , 2019, 14, 1975-1987.	4.5	80

#	ARTICLE	IF	CITATIONS
37	Reducing USB Attack Surface: A Lightweight Authentication and Delegation Protocol. , 2018, , .		2
38	Efficient data perturbation for privacy preserving and accurate data stream mining. Pervasive and Mobile Computing, 2018, 48, 1-19.	2.1	51
39	Efficient Route Update and Maintenance for Reliable Routing in Large-Scale Sensor Networks. IEEE Transactions on Industrial Informatics, 2017, 13, 144-156.	7.2	23
40	A Study on Formal Methods to Generalize Heterogeneous Mobile Malware Propagation and Their Impacts. IEEE Access, 2017, 5, 27740-27756.	2.6	17
41	Reed Solomon Codes for the Reconciliation of Wireless PHY Layer Based Secret Keys. , 2017, , .		2
42	Revocation and update of trust in autonomous delay tolerant networks. Computers and Security, 2016, 60, 15-36.	4.0	9
43	A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. ACM Computing Surveys, 2016, 48, 1-31.	16.1	129
44	Nash Equilibrium-Based Semantic Cache in Mobile Sensor Grid Database Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016, , 1-12.	5.9	12
45	Securing DNP3 Broadcast Communications in SCADA Systems. IEEE Transactions on Industrial Informatics, 2016, 12, 1474-1485.	7.2	46
46	A Deadline-Constrained 802.11 MAC Protocol With QoS Differentiation for Soft Real-Time Control. IEEE Transactions on Industrial Informatics, 2016, 12, 544-554.	7.2	36
47	Formal modelling and analysis of DNP3 secure authentication. Journal of Network and Computer Applications, 2016, 59, 345-360.	5.8	30
48	Understanding data flow and security requirements in wireless Body Area Networks for healthcare. , 2015, , .		8
49	Security analysis of the non-aggressive challenge response of the DNP3 protocol using a CPN model. , 2014, , .		7
50	An efficient proactive route maintenance process for reliable data transmissions in sensor networks. , 2013, , .		1
51	Complexity of Increasing the Secure Connectivity in Wireless Ad Hoc Networks. Lecture Notes in Computer Science, 2013, , 363-378.	1.0	2
52	A Framework for Automated Identification of Attack Scenarios on IT Infrastructures. PIK - Praxis Der Informationsverarbeitung Und Kommunikation, 2012, 35, 25-31.	0.2	0
53	A trusted ecosystem for Android applications based on context-aware access control. , 2012, , .		1
54	Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. , 2011, , .		80

#	ARTICLE	IF	CITATIONS
55	A simulation framework for smart meter security evaluation. , 2011, , .		17
56	Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within Android applications. , 2011, , .		101
57	Behavioral biometrics for persistent single sign-on. , 2011, , .		14
58	Multi-device Key Management Using Visual Side Channels in Pervasive Computing Environments. , 2011, , .		0
59	Context-aware device self-configuration using self-organizing maps. , 2011, , .		3
60	Application-level Simulation for Network Security. Simulation, 2010, 86, 311-330.	1.1	18
61	An Android Application Sandbox system for suspicious software detection. , 2010, , .		273
62	A generic framework and runtime environment for development and evaluation of behavioral biometrics solutions. , 2010, , .		6
63	Teamworking for Security. , 2010, , 1466-1487.		0
64	Design and modeling of collaboration architecture for security. , 2009, , .		1
65	Monitoring Smartphones for Anomaly Detection. Mobile Networks and Applications, 2009, 14, 92-106.	2.2	78
66	Developing and Benchmarking Native Linux Applications on Android. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2009, , 381-392.	0.2	22
67	Static Analysis of Executables for Collaborative Malware Detection on Android. , 2009, , .		162
68	Identity theft, computers and behavioral biometrics. , 2009, , .		48
69	Detecting Symbian OS malware through static function call analysis. , 2009, , .		43
70	Smartphone malware evolution revisited: Android next target?. , 2009, , .		65
71	Key Management in Wireless Sensor Networks. Computer Communications and Networks, 2009, , 513-531.	0.8	1
72	A lightweight biometric signature scheme for user authentication over networks. , 2008, , .		6

#	ARTICLE	IF	CITATIONS
73	Modeling and detection of complex attacks. , 2007, , .		35
74	Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 2007, 15, 346-358.	2.6	252
75	Decentralized Detector Generation in Cooperative Intrusion Detection Systems. , 2007, , 37-51.		5
76	Expander Graph based Key Distribution Mechanisms in Wireless Sensor Networks. , 2006, , .		86
77	Modeling and Multiway Analysis of Chatroom Tensors. Lecture Notes in Computer Science, 2005, , 256-268.	1.0	75
78	Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. Lecture Notes in Computer Science, 2004, , 293-308.	1.0	110
79	A Tool for Internet Chatroom Surveillance. Lecture Notes in Computer Science, 2004, , 252-265.	1.0	7