Helge Janicke

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/3039450/publications.pdf

Version: 2024-02-01

118 papers	4,228 citations	236612 25 h-index	128067 60 g-index
123 all docs	123 docs citations	123 times ranked	3730 citing authors

#	Article	IF	Citations
1	Blockchain Technologies for the Internet of Things: Research Issues and Challenges. IEEE Internet of Things Journal, 2019, 6, 2188-2204.	5.5	480
2	A Survey of COVID-19 Contact Tracing Apps. IEEE Access, 2020, 8, 134577-134601.	2.6	469
3	Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 2020, 50, 102419.	1.8	421
4	SCADA security in the light of Cyber-Warfare. Computers and Security, 2012, 31, 418-436.	4.0	257
5	Authentication Protocols for Internet of Things: A Comprehensive Survey. Security and Communication Networks, 2017, 2017, 1-41.	1.0	193
6	Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 2018, 101, 55-82.	5.8	190
7	Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access, 2022, 10, 40281-40306.	2.6	168
8	RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks. Future Internet, 2020, 12, 44.	2.4	142
9	A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models. , 2019, , .		140
10	Cyber security of critical infrastructures. ICT Express, 2018, 4, 42-45.	3.3	122
11	Social Internet of Vehicles for Smart Cities. Journal of Sensor and Actuator Networks, 2016, 5, 3.	2.3	114
12	Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis. IEEE Access, 2021, 9, 138509-138542.	2.6	103
13	Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. Computers and Security, 2019, 83, 313-331.	4.0	83
14	Route Optimization of Electric Vehicles Based on Dynamic Wireless Charging. IEEE Access, 2018, 6, 42551-42565.	2.6	82
15	Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 2016, 9, 4667-4679.	1.0	76
16	A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities and Society, 2018, 38, 806-835.	5.1	73
17	Cyber warfare: Issues and challenges. Computers and Security, 2015, 49, 70-94.	4.0	68
18	A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles. Array, 2020, 5, 100013.	2.5	56

#	Article	IF	Citations
19	HEART-IS: A novel technique for evaluating human error-related information security incidents. Computers and Security, 2019, 80, 74-89.	4.0	55
20	Vulnerability Analysis of Network Scanning on SCADA Systems. Security and Communication Networks, 2018, 2018, 1-21.	1.0	53
21	A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access, 2020, 8, 209802-209834.	2.6	50
22	Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. Telecommunication Systems, 2020, 73, 317-348.	1.6	44
23	Semantics-aware detection of targeted attacks: a survey. Journal of Computer Virology and Hacking Techniques, 2017, 13, 47-85.	1.6	43
24	The industrial control system cyber defence triage process. Computers and Security, 2017, 70, 467-481.	4.0	38
25	Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications. , 2020, , .		35
26	Runtime-Monitoring for Industrial Control Systems. Electronics (Switzerland), 2015, 4, 995-1017.	1.8	33
27	A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied Sciences (Switzerland), 2020, 10, 3660.	1.3	30
28	Digital Twins and Cyber Security â€“ solution or challenge?. , 2021, , .		24
29	Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis. , 2019, , .		23
30	Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector. International Journal of Medical Informatics, 2019, 127, 109-119.	1.6	22
31	Verification and enforcement of access control policies. Formal Methods in System Design, 2013, 43, 450-492.	0.9	19
32	Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form. IEEE Access, 2019, 7, 102087-102101.	2.6	18
33	PenQuest: a gamified attacker/defender meta model for cyber security assessment and education. Journal of Computer Virology and Hacking Techniques, 2020, 16, 19-61.	1.6	18
34	Intrusion Detection System for Platooning Connected Autonomous Vehicles. , 2019, , .		17
35	Exploring the role of work identity and work locus of control in information security awareness. Computers and Security, 2019, 81, 41-48.	4.0	17
36	Concurrent Enforcement of Usage Control Policies. , 2008, , .		16

#	Article	IF	Citations
37	Privacy-preserving Schemes for Fog-based IoT Applications: Threat models, Solutions, and Challenges. , 2018, , .		16
38	Critical Theory as an Approach to the Ethics of Information Security. Science and Engineering Ethics, 2014, 20, 675-699.	1.7	15
39	Blockchain and Its Role in the Internet of Things. Springer Proceedings in Business and Economics, 2019, , 1029-1038.	0.3	15
40	Deriving Enforcement Mechanisms from Policies. , 2007, , .		14
41	Attribution of Cyber Attacks on Industrial Control Systems. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 2016, 3, 151158.	1.5	14
42	WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles. Sensors, 2021, 21, 2443.	2.1	13
43	Measuring the Risk of Cyber Attack in Industrial Control Systems. , 0, , .		13
44	An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 2018, 114, 70-87.	5.8	12
45	CYRAN. , 2018, , 622-637.		12
46	A note on the formalisation of UCON. , 2007, , .		11
47	Vulnerability Assessment of Cyber Security for SCADA Systems. Computer Communications and Networks, 2018, , 59-80.	0.8	11
48	User interface design for privacy awareness in eHealth technologies. , 2016, , .		10
49	An assessment of the application of IT security mechanisms to industrial control systems. International Journal of Internet Technology and Secured Transactions, 2017, 7, 144.	0.3	10
50	Developing cyber peacekeeping: Observation, monitoring and reporting. Government Information Quarterly, 2019, 36, 276-293.	4.0	10
51	AIDIS: Detecting and classifying anomalous behavior in ubiquitous kernel processes. Computers and Security, 2019, 84, 120-147.	4.0	9
52	Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique. IEEE Access, 2019, 7, 142147-142175.	2.6	9
53	Quantitative Quality Assurance Approach. , 2009, , .		8
54	Formality, Agility, Security, and Evolution in Software Development. Computer, 2014, 47, 86-89.	1.2	8

#	Article	IF	Citations
55	Cyber Security: From Regulations and Policies to Practice. Springer Proceedings in Business and Economics, 2019, , 763-770.	0.3	8
56	Published incidents and their proportions of human error. Information and Computer Security, 2019, 27, 343-357.	1.5	8
57	Teaching the process of building an Intrusion Detection System using data from a small-scale SCADA testbed. Internet Technology Letters, 2020, 3, e132.	1.4	8
58	Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure. , 0, , .		8
59	Towards IoT Security Automation and Orchestration. , 2020, , .		8
60	Low-Latency Service Data Aggregation Using Policy Obligations. , 2014, , .		7
61	MIMO Techniques for Jamming Threat Suppression in Vehicular Networks. Mobile Information Systems, 2016, 2016, 1-9.	0.4	7
62	Two-stage Security Controls Selection. Procedia Computer Science, 2016, 100, 971-978.	1.2	7
63	Editorial: Industrial Internet of Things (I2oT). Mobile Networks and Applications, 2018, 23, 806-808.	2.2	7
64	Managing incident response in the industrial internet of things. International Journal of Internet Technology and Secured Transactions, 2018, 8, 251.	0.3	7
65	A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. , 2021, , .		7
66	Optimizing Software Quality Assurance. , 2010, , .		6
67	A novel Two-Factor HoneyToken Authentication Mechanism. , 2021, , .		6
68	Autonomous Agents and Multi â€“agent Systems (AAMAS) for the Military â€“ Issues and Challenges. Lecture Notes in Computer Science, 2006, , 1-13.	1.0	6
69	Insecure by Design: Using Human Interface Devices to exploit SCADA systems. , 2015, , .		6
70	Design of an Anomaly-based Threat Detection & Explication System. , 2017, , .		6
71	SmartValidator: A framework for automatic identification and classification of cyber threat data. Journal of Network and Computer Applications, 2022, 202, 103370.	5.8	6
72	New framework for policy support for Mobile Grid Services. , 2011, , .		5

#	Article	IF	Citations
73	An Industrial Control Systems incident response decision framework. , 2015, , .		5
74	A security architectural pattern for risk management of industry control systems within critical national infrastructure. International Journal of Critical Infrastructures, 2017, 13, 113.	0.1	5
75	Electronic medical records and risk management in hospitals of Saudi Arabia. Informatics for Health and Social Care, 2019, 44, 189-203.	1.4	5
76	Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis. Enterprise Information Systems, 2021, 15, 448-473.	3.3	5
77	Novel Intrusion Detection Mechanism with Low Overhead for SCADA Systems. Advances in Information Security, Privacy, and Ethics Book Series, 0, , 160-178.	0.4	5
78	New Framework for Dynamic Policy Management in Grid Environments. Communications in Computer and Information Science, 2011, , 297-304.	0.4	5
79	Decentralized XACML Overlay Network. , 2010, , .		4
80	The mimetic virus: a vector for cyberterrorism. International Journal of Business Continuity and Risk Management, 2016, 6, 259.	0.2	4
81	Improved Security Performance for VANET Simulations. IFAC-PapersOnLine, 2016, 49, 233-238.	0.5	4
82	Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?. Journal of Sensor and Actuator Networks, 2017, 6, 16.	2.3	4
83	SEQUIN: a grammar inference framework for analyzing malicious system behavior. Journal of Computer Virology and Hacking Techniques, 2018, 14, 291-311.	1.6	4
84	A Practical Approach to Protect IoT Devices against Attacks and Compile Security Incident Datasets. Scientific Programming, 2019, 2019, 1-11.	0.5	4
85	The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. Computers and Security, 2021, 109, 102398.	4.0	4
86	On data leakage from non-production systems. Information and Computer Security, 2017, 25, 454-474.	1.5	3
87	Class Balanced Similarity-Based Instance Transfer Learning for Botnet Family Classification. Lecture Notes in Computer Science, 2018, , 99-113.	1.0	3
88	Review of Security in VANETs and MANETs. Advances in Information Security, Privacy, and Ethics Book Series, 2014, , 1-27.	0.4	3
89	A Property Based Framework for Trust and Reputation in Mobile Computing. , 2009, , .		2
90	A Robust Eco-Routing Protocol against Malicious Data in Vehicular Networks. , 2015, , .		2

#	Article	IF	Citations
91	Root cause analysis (RCA) as a preliminary tool into the investigation of identity theft. , 2016, , .		2
92	Taxonomy of Supervised Machine Learning for Intrusion Detection Systems. Springer Proceedings in Business and Economics, 2020, , 619-628.	0.3	2
93	Effect of Network Architecture Changes on OCSVM Based Intrusion Detection System. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 90-100.	0.2	2
94	Cybersecurity of Critical Infrastructures: Challenges and Solutions. Sensors, 2022, 22, 5105.	2.1	2
95	Secure management layer for JXTA-based information sharing systems. , 2010, , .		1
96	Efficient Data Processing for Large-Scale Cloud Services. , 2012, , .		1
97	SMP-based service matching. , 2014, , .		1
98	Towards location-aware access control and data privacy in inter-cloud communications. , 2017, , .		1
99	Towards data privacy in heterogeneous cloud environments: An extension to the SANTA policy language. , 2017, , .		1
100	A Novel Hybrid Cyber Range for Security Exercises on Cyber-Physical Systems. International Journal of Smart Security Technologies, 2021, 8, 16-34.	0.3	1
101	CYRAN. Advances in Information Security, Privacy, and Ethics Book Series, 0, , 226-241.	0.4	1
102	Ensuring Data Confidentiality and Privacy in Mobile Ad Hoc Networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2012, , 490-499.	0.2	1
103	Cyber Warfare. Advances in Digital Crime, Forensics, and Cyber Terrorism, 2015, , 13-36.	0.4	1
104	Novel Intrusion Detection Mechanism with Low Overhead for SCADA Systems. , 2020, , 299-318.		1
105	The Cost Perspective of Password Security. Advances in Information Security, Privacy, and Ethics Book Series, 2020, , 319-330.	0.4	1
106	From Cyber Terrorism to Cyber Peacekeeping: Are we there yet?. , 2020, , .		1
107	Security and Privacy for a Sustainable Internet of Things. , 2020, , .		1
108	Software Certification through Quality Profiling. , 2009, , .		0

#	Article	IF	Citations
109	A Model-Based Approach for RFID Application Testing. , 2013, , .		0
110	Special issue on the Security Track at the ACM Symposium on Applied Computing 2013. International Journal of Information Security, 2015, 14, 101-102.	2.3	0
111	Protecting Civilians from Cyber Warfare with Cyber Buffer Zones. International Journal of Smart Security Technologies, 2019, 6, 31-48.	0.3	0
112	OSNs as Cyberterrorist Weapons against the General Public. Advances in Information Security, Privacy, and Ethics Book Series, 2017, , 179-197.	0.4	0
113	Security Visualization: Detecting Denial of Service. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2017, , 39-49.	0.2	0
114	A Novel Method for Calculating Customer Reviews Ratings. Advances in Computer and Electrical Engineering Book Series, 2018, , 460-478.	0.2	0
115	SCIPS. , 2018, , 1168-1183.		0
116	Developing Cyber Buffer Zones. , 2020, , 287-303.		0
117	Redefining the â€˜arsenal of democracyâ€™. Nature Human Behaviour, 0, , .	6.2	0
118	Development and application of the Information Security Core Human Error Causes (IS-CHEC) technique. , 2022, , 267-295.		0