Helge Janicke

List of Publications by Citations

110 papers	2,273 citations	21 h-index	45 g-index
123 ext. papers	3,170 ext. citations	2.7 avg, IF	5.76 L-index

#	Paper	IF	Citations
110	Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet of Things Journal*, **2019**, 6, 2188-2204	10.7	289
109	A Survey of COVID-19 Contact Tracing Apps. *IEEE Access*, **2020**, 8, 134577-134601	3.5	233
108	SCADA security in the light of Cyber-Warfare. *Computers and Security*, **2012**, 31, 418-436	4.9	203
107	Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, **2020**, 50, 102419	3.5	194
106	Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks*, **2017**, 2017, 1-41	1.9	137
105	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	7.9	126
104	Social Internet of Vehicles for Smart Cities. *Journal of Sensor and Actuator Networks*, **2016**, 5, 3	3.8	75
103	Cyber security of critical infrastructures. *ICT Express*, **2018**, 4, 42-45	4.9	71
102	A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models **2019**,		57
101	Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, **2016**, 9, 4667-4679	1.9	53
100	Route Optimization of Electric Vehicles Based on Dynamic Wireless Charging. *IEEE Access*, **2018**, 6, 42551-42565	3.9	52
99	A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustainable Cities and Society*, **2018**, 38, 806-835	10.1	51
98	RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks. *Future Internet*, **2020**, 12, 44	3.3	49
97	Cyber warfare: Issues and challenges. *Computers and Security*, **2015**, 49, 70-94	4.9	46
96	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	4.9	41
95	Vulnerability Analysis of Network Scanning on SCADA Systems. *Security and Communication Networks*, **2018**, 2018, 1-21	1.9	34
94	Semantics-aware detection of targeted attacks: a survey. *Journal of Computer Virology and Hacking Techniques*, **2017**, 13, 47-85	3	29

93	A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles. *Array*, **2020**, 5, 100013	4.7	28
92	HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers and Security*, **2019**, 80, 74-89	4.9	28
91	Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues. *Telecommunication Systems*, **2020**, 73, 317-348	2.3	28
90	The industrial control system cyber defence triage process. *Computers and Security*, **2017**, 70, 467-481	4.9	25
89	Runtime-Monitoring for Industrial Control Systems. *Electronics (Switzerland)*, **2015**, 4, 995-1017	2.6	19
88	A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. *Applied Sciences (Switzerland)*, **2020**, 10, 3660	2.6	14
87	Verification and enforcement of access control policies. *Formal Methods in System Design*, **2013**, 43, 450-492	1.4	13
86	Blockchain and Its Role in the Internet of Things. *Springer Proceedings in Business and Economics*, **2019**, 1029-1038	0.2	12
85	Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Analysis		12
84	. *IEEE Access*, **2021**, 9, 138509-138542	3.5	12
83	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	5.3	11
82	Critical theory as an approach to the ethics of information security. *Science and Engineering Ethics*, **2014**, 20, 675-99	3.1	11
81	Concurrent Enforcement of Usage Control Policies **2008**,		11
80	A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access*, **2020**, 8, 209802-209834	3.5	11
79	Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form. *IEEE Access*, **2019**, 7, 102087-102101	3.5	10
78	Measuring the Risk of Cyber Attack in Industrial Control Systems		10
77	Attribution of Cyber Attacks on Industrial Control Systems. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, **2016**, 3, 151158	1.5	10
76	Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. *IEEE Access*, **2022**, 1-1	3.5	10

75	An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, **2018**, 114, 70-87	7.9	9
74	A note on the formalisation of UCON **2007**,		9
73	Deriving Enforcement Mechanisms from Policies **2007**,		9
72	CYRAN **2018**, 622-637		9
71	Exploring the role of work identity and work locus of control in information security awareness. *Computers and Security*, **2019**, 81, 41-48	4.9	9
70	An assessment of the application of IT security mechanisms to industrial control systems. *International Journal of Internet Technology and Secured Transactions*, **2017**, 7, 144	0.6	8
69	Intrusion Detection System for Platooning Connected Autonomous Vehicles **2019**,		8
68	PenQuest: a gamified attacker/defender meta model for cyber security assessment and education. *Journal of Computer Virology and Hacking Techniques*, **2020**, 16, 19-61	3	7
67	MIMO Techniques for Jamming Threat Suppression in Vehicular Networks. *Mobile Information Systems*, **2016**, 2016, 1-9	1.4	7
66	Two-stage Security Controls Selection. *Procedia Computer Science*, **2016**, 100, 971-978	1.6	7
65	Developing cyber peacekeeping: Observation, monitoring and reporting. *Government Information Quarterly*, **2019**, 36, 276-293	7.6	7
64	Cyber Security: From Regulations and Policies to Practice. *Springer Proceedings in Business and Economics*, **2019**, 763-770	0.2	6
63	Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure		6
62	Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique. *IEEE Access*, **2019**, 7, 142147-142175	3.5	6
61	Privacy-preserving Schemes for Fog-based IoT Applications: Threat models, Solutions, and Challenges **2018**,		6
60	Published incidents and their proportions of human error. *Information and Computer Security*, **2019**, 27, 343-357	1.4	5
59	User interface design for privacy awareness in eHealth technologies **2016**,		5
58	A security architectural pattern for risk management of industry control systems within critical national infrastructure. *International Journal of Critical Infrastructures*, **2017**, 13, 113	1	5

57	Formality, Agility, Security, and Evolution in Software Development. *Computer*, **2014**, 47, 86-89	1.6	5
56	Quantitative Quality Assurance Approach **2009**,		5
55	Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications **2020**,		5
54	Teaching the process of building an Intrusion Detection System using data from a small-scale SCADA testbed. *Internet Technology Letters*, **2020**, 3, e132	1.3	5
53	Can a Network Attack Be Simulated in an Emulated Environment for Network Security Training?. *Journal of Sensor and Actuator Networks*, **2017**, 6, 16	3.8	4
52	An Industrial Control Systems incident response decision framework **2015**,		4
51	Decentralized XACML Overlay Network **2010**,		4
50	Optimizing Software Quality Assurance **2010**,		4
49	Design of an Anomaly-based Threat Detection & Explication System **2017**,		4
48	Digital Twins and Cyber Security solution or challenge? **2021**,		4
47	Electronic medical records and risk management in hospitals of Saudi Arabia. *Informatics for Health and Social Care*, **2019**, 44, 189-203	2.7	4
46	AIDIS: Detecting and classifying anomalous behavior in ubiquitous kernel processes. *Computers and Security*, **2019**, 84, 120-147	4.9	3
45	The mimetic virus: a vector for cyberterrorism. *International Journal of Business Continuity and Risk Management*, **2016**, 6, 259	0.2	3
44	Low-Latency Service Data Aggregation Using Policy Obligations **2014**,		3
43	New framework for policy support for Mobile Grid Services **2011**,		3
42	Analysis and Run-Time Verification of Dynamic Security Policies. *Lecture Notes in Computer Science*, **2006**, 92-103	0.9	3
41	Insecure by Design: Using Human Interface Devices to exploit SCADA systems		3
40	Novel Intrusion Detection Mechanism with Low Overhead for SCADA Systems. *Advances in Information Security, Privacy, and Ethics Book Series*,160-178	0.3	3

39	Controlling Data Dissemination. *Lecture Notes in Computer Science*, **2012**, 303-309	0.9	3
38	New Framework for Dynamic Policy Management in Grid Environments. *Communications in Computer and Information Science*, **2011**, 297-304	0.3	3
37	Review of Security in VANETs and MANETs. *Advances in Information Security, Privacy, and Ethics Book Series*, **2014**, 1-27	0.3	3
36	WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles. *Sensors*, **2021**, 21,	3.8	3
35	Improved Security Performance for VANET Simulations. *IFAC-PapersOnLine*, **2016**, 49, 233-238	0.7	3
34	Managing incident response in the industrial internet of things. *International Journal of Internet Technology and Secured Transactions*, **2018**, 8, 251	0.6	3
33	Vulnerability Assessment of Cyber Security for SCADA Systems. *Computer Communications and Networks*, **2018**, 59-80	0.5	3
32	Autonomous Agents and Multi Agent Systems (AAMAS) for the Military Issues and Challenges. *Lecture Notes in Computer Science*, **2006**, 1-13	0.9	3
31	A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments **2021**,		3
30	SEQUIN: a grammar inference framework for analyzing malicious system behavior. *Journal of Computer Virology and Hacking Techniques*, **2018**, 14, 291-311	3	2
29	A Practical Approach to Protect IoT Devices against Attacks and Compile Security Incident Datasets. *Scientific Programming*, **2019**, 2019, 1-11	1.4	2
28	A Robust Eco-Routing Protocol against Malicious Data in Vehicular Networks **2015**,		2
27	A Property Based Framework for Trust and Reputation in Mobile Computing **2009**,		2
26	Towards IoT Security Automation and Orchestration **2020**,		2
25	Taxonomy of Supervised Machine Learning for Intrusion Detection Systems. *Springer Proceedings in Business and Economics*, **2020**, 619-628	0.2	2
24	Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis. *Enterprise Information Systems*, **2021**, 15, 448-473	3.5	2
23	Formality, Agility, Security, and Evolution in Software Engineering **2018**, 282-292		2
22	Towards data privacy in heterogeneous cloud environments: An extension to the SANTA policy language **2017**,		1

21	On data leakage from non-production systems. *Information and Computer Security*, **2017**, 25, 454-474	1.4	1
20	SMP-based service matching **2014**,		1
19	Efficient Data Processing for Large-Scale Cloud Services **2012**,		1
18	CYRAN. *Advances in Information Security, Privacy, and Ethics Book Series*,226-241	0.3	1
17	Novel Intrusion Detection Mechanism with Low Overhead for SCADA Systems **2020**, 299-318		1
16	The Cost Perspective of Password Security. *Advances in Information Security, Privacy, and Ethics Book Series*, **2020**, 319-330	0.3	1
15	Class Balanced Similarity-Based Instance Transfer Learning for Botnet Family Classification. *Lecture Notes in Computer Science*, **2018**, 99-113	0.9	1
14	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
13	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
12	The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. *Computers and Security*, **2021**, 109, 102398	4.9	1
11	Cyber Warfare. *Advances in Digital Crime, Forensics, and Cyber Terrorism*, **2015**, 13-36	0.2	0
10	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	0
9	SmartValidator: A framework for automatic identification and classification of cyber threat data. *Journal of Network and Computer Applications*, **2022**, 202, 103370	7.9	0
8	Developing Cyber Buffer Zones **2020**, 287-303		
7	A Novel Method for Calculating Customer Reviews Ratings. *Advances in Computer and Electrical Engineering Book Series*, **2018**, 460-478	0.3	
6	SCIPS **2018**, 1168-1183		
5	OSNs as Cyberterrorist Weapons against the General Public. *Advances in Information Security, Privacy, and Ethics Book Series*, **2017**, 179-197	0.3	
4	Security Visualization: Detecting Denial of Service. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2017**, 39-49	0.2	

3	Protecting Civilians from Cyber Warfare with Cyber Buffer Zones. *International Journal of Smart Security Technologies*, **2019**, 6, 31-48	0.3
2	Redefining the rsenal of democracy *Nature Human Behaviour*,	12.8
1	Development and application of the Information Security Core Human Error Causes (IS-CHEC) technique **2022**, 267-295	