Joaquin Garcia-Alfaro

List of Publications by Year in Descending Order

Source: https://exaly.com/author-pdf/5962428/joaquin-garcia-alfaro-publications-by-year.pdf
Version: 2024-04-20

This document has been generated based on the publications and citations recorded by exaly.com. For the latest version of this publication list, visit the link given above.
The third column is the impact factor (IF) of the journal, and the fourth column is the number of citations of the article.

144 papers	912 citations	15 h-index	22 g-index
184 ext. papers	1,108 ext. citations	1.8 avg, IF	4.47 L-index

#	Paper	IF	Citations
144	Cyber-physical defense in the quantum Era.. *Scientific Reports*, **2022**, 12, 1905	4.9	1
143	Resilience Estimation of Cyber-Physical Systems via Quantitative Metrics. *IEEE Access*, **2021**, 9, 46462-46475	3.5	1
142	1. Quantum Applications - Fachbeitrag: The Quantum What? Advantage, Utopia or Threat?. *Digitale Welt*, **2021**, 5, 34-39	0.5	1
141	DECA: A Dynamic Energy Cost and Carbon Emission-Efficient Application Placement Method for Edge Clouds. *IEEE Access*, **2021**, 9, 70192-70213	3.5	3
140	Capacity Requirements in Networks of Quantum Repeaters and Terminals **2020**,		3
139	A Real-Time Query Log Protection Method for Web Search Engines. *IEEE Access*, **2020**, 8, 87393-87413	3.5	3
138	Cyber-Resilience Evaluation of Cyber-Physical Systems **2020**,		2
137	Geocaching-Inspired Navigation for Micro Aerial Vehicles with Fallible Place Recognition. *Lecture Notes in Computer Science*, **2020**, 55-70	0.9	
136	Reflective Attenuation of Cyber-Physical Attacks. *Lecture Notes in Computer Science*, **2020**, 19-34	0.9	1
135	Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things **2020**,		3
134	LockDown: Balance Availability Attack Against Lightning Network Channels. *Lecture Notes in Computer Science*, **2020**, 245-263	0.9	7
133	Stateful RORI-based countermeasure selection using hypergraphs. *Journal of Information Security and Applications*, **2020**, 54, 102562	3.5	0
132	Stateful RORI-based countermeasure selection using hypergraphs. *Journal of Information Security and Applications*, **2020**, 54, 102541	3.5	0
131	Switched-Based Resilient Control of Cyber-Physical Systems. *IEEE Access*, **2020**, 8, 212194-212208	3.5	3
130	Security and Privacy in the TeSLA Architecture. *Lecture Notes on Data Engineering and Communications Technologies*, **2020**, 85-108	0.4	0
129	On the Difficulty of Hiding the Balance of Lightning Network Channels **2019**,		20
128	Geocaching-inspired Resilient Path Planning for Drone Swarms **2019**,		3

127	The Influence of Conception Paradigms on Data Protection in E-Learning Platforms: A Case Study. *IEEE Access*, **2019**, 7, 64110-64119	3.5	5
126	A Study on Mitigation Techniques for SCADA-Driven Cyber-Physical Systems (Position Paper). *Lecture Notes in Computer Science*, **2019**, 257-264	0.9	1
125	Foundations and Practice of Security. *Lecture Notes in Computer Science*, **2019**,	0.9	1
124	Anonymous certification for E-assessment opinion polls. *Journal of Ambient Intelligence and Humanized Computing*, **2019**, 1	3.7	
123	Tuning the demodulation frequency based on a normalized trajectory model for mobile underwater acoustic communications. *Transactions on Emerging Telecommunications Technologies*, **2019**, 30, e3712	1.9	6
122	Towards an Adaptive Defuzzification: Using Numerical Choquet Integral. *Lecture Notes in Computer Science*, **2019**, 113-125	0.9	1
121	Quality Amplification of Error Prone Navigation for Swarms of Micro Aerial Vehicles **2019**,		1
120	Attack Graph-Based Countermeasure Selection Using a Stateful Return on Investment Metric. *Lecture Notes in Computer Science*, **2018**, 293-302	0.9	1
119	Risks and Security of Internet and Systems. *Lecture Notes in Computer Science*, **2018**,	0.9	2
118	Doppler Effect in the Acoustic Ultra Low Frequency Band for Wireless Underwater Networks. *Mobile Networks and Applications*, **2018**, 23, 1282-1292	2.9	7
117	Cyber-physical architecture assisted by programmable networking. *Internet Technology Letters*, **2018**, 1, e44	1.3	4
116	Using an Event Data Taxonomy to Represent the Impact of Cyber Events as Geometrical Instances. *IEEE Access*, **2018**, 6, 8810-8828	3.5	2
115	The Sound of Communication in Underwater Acoustic Sensor Networks. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2018**, 13-23	0.2	5
114	Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems*, **2018**, 83, 535-552	7.5	17
113	Integration of an adaptive trust-based e-assessment system into virtual learning environments The TeSLA project experience. *Internet Technology Letters*, **2018**, 1, e56	1.3	4
112	Hypergraph-driven mitigation of cyberattacks. *Internet Technology Letters*, **2018**, 1, e38	1.3	0
111	Low Frequency Mobile Communications in Underwater Networks. *Lecture Notes in Computer Science*, **2018**, 239-251	0.9	3
110	Doppler Effect in the Underwater Acoustic Ultra Low Frequency Band. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2018**, 3-12	0.2	5

109	Adaptive control-theoretic detection of integrity attacks against cyber-physical industrial systems. *Transactions on Emerging Telecommunications Technologies*, **2018**, 29, e3209	1.9	9
108	Lifelogging Protection Scheme for Internet-Based Personal Assistants. *Lecture Notes in Computer Science*, **2018**, 431-440	0.9	1
107	Towards a Security Event Data Taxonomy. *Lecture Notes in Computer Science*, **2018**, 29-45	0.9	1
106	A polytope-based approach to measure the impact of events against critical infrastructures. *Journal of Computer and System Sciences*, **2017**, 83, 3-21	1	8
105	Selection of Pareto-efficient response plans based on financial and operational assessments. *Eurasip Journal on Information Security*, **2017**, 2017,	3.8	4
104	(mathcal {PCS}), A Privacy-Preserving Certification Scheme. *Lecture Notes in Computer Science*, **2017** , 239-256	0.9	7
103	Learning to Communicate Underwater **2017**,		1
102	Anonymous Certification for an e-Assessment Framework. *Lecture Notes in Computer Science*, **2017**, 70-85	0.9	5
101	On the use of watermark-based schemes to detect cyber-physical attacks. *Eurasip Journal on Information Security*, **2017**, 2017,	3.8	19
100	Security Challenges in e-Assessment and Technical Solutions **2017**,		10
99	Secure Localization in the Presence of Colluders in WSNs. *Sensors*, **2017**, 17,	3.8	3
98	An n-Sided Polygonal Model to Calculate the Impact of Cyber Security Events. *Lecture Notes in Computer Science*, **2017**, 87-102	0.9	2
97	Data Privacy Management, Cryptocurrencies and Blockchain Technology. *Lecture Notes in Computer Science*, **2017**,	0.9	7
96	Security of Cyber-Physical Systems. *Lecture Notes in Computer Science*, **2017**, 3-18	0.9	2
95	Reputation trust mechanism under the organizational-based access control model. *Security and Communication Networks*, **2016**, 9, 5295-5310	1.9	
94	CACEV: A Cost and Carbon Emission-Efficient Virtual Machine Placement Method for Green Distributed Clouds **2016**,		17
93	Data Privacy Management, and Security Assurance. *Lecture Notes in Computer Science*, **2016**,	0.9	1
92	Channel selection using a multiple radio model. *Journal of Network and Computer Applications*, **2016**, 64, 113-123	7.9	1

91	Event-Triggered Watermarking Control to Handle Cyber-Physical Integrity Attacks. *Lecture Notes in Computer Science*, **2016**, 3-19	0.9	8
90	Towards an Automated and Dynamic Risk Management Response System. *Lecture Notes in Computer Science*, **2016**, 37-53	0.9	3
89	Considering Internal Vulnerabilities and the Attacker's Knowledge to Model the Impact of Cyber Events as Geometrical Prisms **2016**,		2
88	Revisiting a Watermark-Based Detection Scheme to Handle Cyber-Physical Attacks **2016**,		11
87	Selection of Mitigation Actions Based on Financial and Operational Impact Assessments **2016**,		3
86	Research in Attacks, Intrusions, and Defenses. *Lecture Notes in Computer Science*, **2016**,	0.9	2
85	Remarks on Peinado et al.'s Analysis of J3Gen. *Sensors*, **2015**, 15, 6217-20	3.8	2
84	Simulation of underwater communications with a colored noise approximation and mobility **2015**,		6
83	Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index. *Computers and Electrical Engineering*, **2015**, 47, 13-34	4.3	23
82	Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. *Computers and Electrical Engineering*, **2015**, 41, 52-63	4.3	35
81	Advanced Research in Data Privacy. *Studies in Computational Intelligence*, **2015**,	0.8	2
80	NACER: A Network-Aware Cost-Efficient Resource Allocation Method for Processing-Intensive Tasks in Distributed Clouds **2015**,		8
79	On the Isofunctionality of Network Access Control Lists **2015**,		1
78	Automated Classification of C&C Connections Through Malware URL Clustering. *IFIP Advances in Information and Communication Technology*, **2015**, 252-266	0.5	7
77	Location-free link state routing for underwater acoustic sensor networks **2015**,		13
76	Security and Privacy Concerns About the RFID Layer of EPC Gen2 Networks. *Studies in Computational Intelligence*, **2015**, 303-324	0.8	7
75	Model-Driven Integration and Analysis of Access-control Policies in Multi-layer Information Systems. *IFIP Advances in Information and Communication Technology*, **2015**, 218-233	0.5	1
74	Using a 3D Geometrical Model to Improve Accuracy in the Evaluation and Selection of Countermeasures Against Complex Cyber Attacks. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2015**, 538-555	0.2	8

73	Searching for a black hole in interconnected networks using mobile agents and tokens. *Journal of Parallel and Distributed Computing*, **2014**, 74, 1945-1958	4.4	8
72	KEDGEN2: A key establishment and derivation protocol for EPC Gen2 RFID systems. *Journal of Network and Computer Applications*, **2014**, 39, 152-166	7.9	7
71	On the similarity of commercial EPC Gen2 pseudorandom number generators. *Transactions on Emerging Telecommunications Technologies*, **2014**, 25, 151-154	1.9	3
70	Classification of SSL Servers based on their SSL Handshake for Automated Security Assessment **2014**,		6
69	A new analysis of the cognitive radio jump-stay algorithm under the asymmetric model **2014**,		4
68	The Bidirectional Algorithm for Channel Selection Using a Two-Radio Model **2014**,		1
67	Revisiting the Performance of the Modular Clock Algorithm for Distributed Blind Rendezvous in Cognitive Radio Networks. *Lecture Notes in Computer Science*, **2014**, 197-208	0.9	
66	Leveraging Ontologies upon a Holistic Privacy-Aware Access Control Model. *Lecture Notes in Computer Science*, **2014**, 209-226	0.9	4
65	Management of stateful firewall misconfiguration. *Computers and Security*, **2013**, 39, 64-85	4.9	15
64	A privacy-aware access control model for distributed network monitoring. *Computers and Electrical Engineering*, **2013**, 39, 2263-2281	4.3	11
63	QoS and security in Link State Routing protocols for MANETs **2013**,		1
62	A new analytic model for the cognitive radio jump-stay algorithm **2013**,		2
61	Privacy-enhanced filtering and collection middleware in EPCglobal networks **2013**,		3
60	Semantic analysis of role mining results and shadowed roles detection. *Information Security Technical Report*, **2013**, 17, 131-147		5
59	Onion routing circuit construction via latency graphs. *Computers and Security*, **2013**, 37, 197-214	4.9	8
58	A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs. *Journal of Network and Computer Applications*, **2013**, 36, 744-755	7.9	26
57	Fine-grained privacy control for the RFID middleware of EPCglobal networks **2013**,		4
56	J3Gen: a PRNG for low-cost passive RFID. *Sensors*, **2013**, 13, 3816-30	3.8	35

55	Real-time malicious fast-flux detection using DNS and bot related features **2013**,		11
54	Towards an Access-Control Metamodel for Web Content Management Systems. *Lecture Notes in Computer Science*, **2013**, 148-155	0.9	11
53	Model-Driven Extraction and Analysis of Network Security Policies. *Lecture Notes in Computer Science*, **2013**, 52-68	0.9	4
52	An Adaptive Mitigation Framework for Handling Suspicious Network Flows via MPLS Policies. *Lecture Notes in Computer Science*, **2013**, 297-312	0.9	
51	Towards Automated Assistance for Mined Roles Analysis in Role Mining Applications **2012**,		4
50	HADEGA: A novel MPLS-based mitigation solution to handle network attacks **2012**,		5
49	Transaction-based authentication and key agreement protocol for inter-domain VoIP. *Journal of Network and Computer Applications*, **2012**, 35, 1579-1597	7.9	2
48	Data and Applications Security and Privacy XXVI. *Lecture Notes in Computer Science*, **2012**,	0.9	4
47	A model-driven approach for the extraction of network access-control policies **2012**,		7
46	Foundations and Practice of Security. *Lecture Notes in Computer Science*, **2012**,	0.9	3
45	Formal Verification of a Key Establishment Protocol for EPC Gen2 RFID Systems: Work in Progress. *Lecture Notes in Computer Science*, **2012**, 242-251	0.9	1
44	Handling Stateful Firewall Anomalies. *International Federation for Information Processing*, **2012**, 174-186		14
43	Security Issues in Link State Routing Protocols for MANETs. *Mathematics in Industry*, **2012**, 117-148	0.2	1
42	A Contextual Privacy-Aware Access Control Model for Network Monitoring Workflows: Work in Progress. *Lecture Notes in Computer Science*, **2012**, 208-217	0.9	2
41	Preventing the Cluster Formation Attack against the Hierarchical OLSR Protocol. *Lecture Notes in Computer Science*, **2012**, 118-131	0.9	
40	Data Privacy Management and Autonomous Spontaneous Security. *Lecture Notes in Computer Science*, **2011**,	0.9	2
39	Dynamic deployment of context-aware access control policies for constrained security devices. *Journal of Systems and Software*, **2011**, 84, 1144-1159	3.3	22
38	A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags. *Wireless Personal Communications*, **2011**, 59, 27-42	1.9	18

37	Improved flooding of broadcast messages using extended multipoint relaying. *Journal of Network and Computer Applications*, **2011**, 34, 542-550	7.9	3
36	Secure geolocalization of wireless sensor nodes in the presence of misbehaving anchor nodes. *Annales Des Telecommunications/Annals of Telecommunications*, **2011**, 66, 535-552	2	9
35	Mitigation of Flooding Disruption Attacks in Hierarchical OLSR Networks **2011**,		2
34	Multiple-polynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags **2011**,		9
33	MIRAGE: A Management Tool for the Analysis and Deployment of Network Security Policies. *Lecture Notes in Computer Science*, **2011**, 203-215	0.9	15
32	Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags. *Lecture Notes in Computer Science*, **2010**, 34-46	0.9	27
31	Data Privacy Management and Autonomous Spontaneous Security. *Lecture Notes in Computer Science*, **2010**,	0.9	3
30	Mitigation of topology control traffic attacks in OLSR networks **2010**,		7
29	Securing the Communications of Home Health Care Systems Based on RFID Sensor Networks **2010**,		6
28	Model-Driven Security Policy Deployment: Property Oriented Approach. *Lecture Notes in Computer Science*, **2010**, 123-139	0.9	9
27	Security Threat Mitigation Trends in Low-Cost RFID Systems. *Lecture Notes in Computer Science*, **2010**, 193-207	0.9	3
26	Handling Security Threats to the RFID System of EPC Networks **2010**, 45-64		2
25	Evaluation of Two Privacy-Preserving Protocols for the DNS **2009**,		13
24	Spyware-Based Menaces Against Web Applications **2009**,		1
23	Semantic context aware security policy deployment **2009**,		10
22	Secure Localization of Nodes in Wireless Sensor Networks with Limited Number of Truth Tellers **2009**,		12
21	A Policy Based Approach for the Management of Web Browser Resources to Prevent Anonymity Attacks in Tor. *IFIP Advances in Information and Communication Technology*, **2009**, 164-175	0.5	
20	Analysis of Threats to the Security of EPC Networks **2008**,		6

19	Distributed Exchange of Alerts for the Detection of Coordinated Attacks **2008**,		1
18	Security Threats on EPC Based RFID Systems **2008**,		6
17	Complete analysis of configuration rules to guarantee reliable network security policies. *International Journal of Information Security*, **2008**, 7, 103-122	2.8	61
16	Anonymous Resolution of DNS Queries. *Lecture Notes in Computer Science*, **2008**, 987-1000	0.9	8
15	A Survey on Detection Techniques to Prevent Cross-Site Scripting Attacks on Current Web Applications. *Lecture Notes in Computer Science*, **2008**, 287-298	0.9	1
14	Aggregating and Deploying Network Access Control Policies **2007**,		6
13	Prevention of Cross-Site Scripting Attacks on Current Web Applications **2007**, 1770-1784		8
12	Management of Exceptions on Access Control Policies. *International Federation for Information Processing*, **2007**, 97-108		6
11	Anti-correlation as a criterion to select appropriate counter-measures in an intrusion detection framework. *Annales Des Telecommunications/Annals of Telecommunications*, **2006**, 61, 197-217	2	19
10	Analysis of Policy Anomalies on Distributed Network Security Setups. *Lecture Notes in Computer Science*, **2006**, 496-511	0.9	14
9	Protection of Components Based on a Smart-Card Enhanced Security Module. *Lecture Notes in Computer Science*, **2006**, 128-139	0.9	0
8	Towards Filtering and Alerting Rule Rewriting on Single-Component Policies. *Lecture Notes in Computer Science*, **2006**, 182-194	0.9	7
7	SMARTCOP A Smart Card Based Access Control for the Protection of Network Security Components. *Lecture Notes in Computer Science*, **2006**, 415-424	0.9	0
6	Protecting on-line casinos against fraudulent player drop-out **2005**,		1
5	Digital chips for an on-line casino **2005**,		1
4	Mechanisms for attack protection on a prevention framework **2005**,		1
3	Amapola: A Simple Infrastructure for Ubiquitous Computing **2005**, 77-86		
2	Decoupling Components of an Attack Prevention System Using Publish/Subscribe **2005**, 87-97		0

1 Decentralized Publish-Subscribe System to Prevent Coordinated Attacks via Alert Correlation. *Lecture Notes in Computer Science*, **2004**, 223-235 0.9 16