Roberto Di Pietro

List of Publications by Year in Descending Order

Source: https://exaly.com/author-pdf/8095216/roberto-di-pietro-publications-by-year.pdf
Version: 2024-04-19

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.

192 papers	3,688 citations	30 h-index	54 g-index
218 ext. papers	4,641 ext. citations	3.8 avg, IF	5.95 L-index

#	Paper	IF	Citations
192	Privacy-Preserving and Sustainable Contact Tracing Using Batteryless Bluetooth Low-Energy Beacons. *IEEE Security and Privacy*, **2021**, 2-11	2	0
191	Critical Infrastructure. *Advances in Information Security*, **2021**, 157-196	0.7	0
190	Cryptocurrencies. *Advances in Information Security*, **2021**, 69-97	0.7	
189	Information Disorder. *Advances in Information Security*, **2021**, 7-64	0.7	2
188	PPRQ: Privacy-Preserving MAX/MIN Range Queries in IoT Networks. *IEEE Internet of Things Journal*, **2021**, 8, 5075-5092	10.7	2
187	Cryptomining makes noise: Detecting cryptojacking via Machine Learning. *Computer Communications*, **2021**, 171, 126-139	5.1	6
186	Cyber security research in the Arab region. *Communications of the ACM*, **2021**, 64, 96-101	2.5	0
185	. *IEEE Communications Magazine*, **2021**, 59, 82-88	9.1	8
184	Short-Range Audio Channels Security: Survey of Mechanisms, Applications, and Research Challenges. *IEEE Communications Surveys and Tutorials*, **2021**, 23, 311-340	37.1	4
183	New Dimensions of Information Warfare. *Advances in Information Security*, **2021**,	0.7	6
182	Receivers location privacy in avionic crowdsourced networks: Issues and countermeasures. *Journal of Network and Computer Applications*, **2021**, 174, 102892	7.9	0
181	New Dimensions of Information Warfare: The Economic Pillar Fintech and Cryptocurrencies. *Lecture Notes in Computer Science*, **2021**, 3-27	0.9	
180	DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, **2021**, 122, 149-171	7.5	9
179	Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	3
178	Road Traffic Poisoning of Navigation Apps: Threats and Countermeasures. *IEEE Security and Privacy*, **2021**, 2-11	2	0
177	Metaverse: Security and Privacy Issues **2021**,		11
176	. *IEEE Access*, **2020**, 8, 52075-52090	3.5	3

175	Next Generation Information Warfare: Rationales, Scenarios, Threats, and Open Issues. *Communications in Computer and Information Science*, **2020**, 24-47	0.3	1
174	. *IEEE Access*, **2020**, 8, 5049-5064	3.5	8
173	GNSS spoofing detection via opportunistic IRIDIUM signals **2020**,		7
172	Foundations, Properties, and Security Applications of Puzzles. *ACM Computing Surveys*, **2020**, 53, 1-38	13.4	8
171	Emergent properties, models, and laws of behavioral similarities within groups of twitter users. *Computer Communications*, **2020**, 150, 47-61	5.1	13
170	. *IEEE Internet of Things Journal*, **2020**, 7, 621-638	10.7	27
169	PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis. *Computer Networks*, **2020**, 168, 107044	5.4	11
168	. *IEEE Access*, **2020**, 8, 173481-173490	3.5	6
167	Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Communications Magazine*, **2020**, 58, 90-96	9.1	17
166	SecureAIS - Securing Pairwise Vessels Communications **2020**,		6
165	Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges. *IEEE Communications Surveys and Tutorials*, **2020**, 22, 2658-2693	37.1	12
164	Increasing Renewable Generation Feed-In Capacity Leveraging Smart Meters **2020**,		1
163	. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 17, 2-21	3.9	12
162	Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues **2019**,		48
161	**2019**,		3
160	Detecting Drones Status via Encrypted Traffic Analysis **2019**,		12
159	Intrusion Detection at the Network Edge: Solutions, Limitations, and Future Directions. *Lecture Notes in Computer Science*, **2019**, 59-75	0.9	6
158	Drive me not: GPS spoofing detection via cellular network **2019**,		10

157	Key is in the Air: Hacking Remote Keyless Entry Systems. *Lecture Notes in Computer Science*, **2019**, 125-132	0.29	0
156	FORTRESS: An Efficient and Distributed Firewall for Stateful Data Plane SDN. *Security and Communication Networks*, **2019**, 2019, 1-16	1.9	11
155	SOS: Standard-Compliant and Packet Loss Tolerant Security Framework for ADS-B Communications. *IEEE Transactions on Dependable and Secure Computing*, **2019**, 1-1	3.9	9
154	Bittransfer: Mitigating Reactive Jamming in Electronic Warfare Scenarios. *IEEE Access*, **2019**, 7, 156175-156190	3.9	3
153	Reliability of ADS-B communications **2019**,		10
152	Location Privacy Issues in the OpenSky Network Crowdsourcing Platform. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2019**, 549-568	0.2	1
151	EXCHANge: Securing IoT via channel anonymity. *Computer Communications*, **2019**, 134, 14-29	5.1	8
150	Docker ecosystem Vulnerability Analysis. *Computer Communications*, **2018**, 122, 30-43	5.1	56
149	A blockchain-based Trust System for the Internet of Things **2018**,		39
148	Virtualization Technologies and Cloud Security: Advantages, Issues, and Perspectives. *Lecture Notes in Computer Science*, **2018**, 166-185	0.9	2
147	A Spark Is Enough in a Straw World: A Study of Websites Password Management in the Wild. *Lecture Notes in Computer Science*, **2018**, 37-53	0.9	1
146	Strength of Crowd (SOC)-Defeating a Reactive Jammer in IoT with Decoy Messages. *Sensors*, **2018**, 18,	3.8	14
145	ADvISE: Anomaly Detection tool for blockchaIn SystEms **2018**,		9
144	SOS - Securing Open Skies. *Lecture Notes in Computer Science*, **2018**, 15-32	0.9	4
143	GopJam: Key-less jamming mitigation via gossiping. *Journal of Network and Computer Applications*, **2018**, 123, 57-68	7.9	1
142	Shooting to the Stars: Secure Location Verification via Meteor Burst Communications **2018**,		2
141	Enabling broadcast communications in presence of jamming via probabilistic pairing. *Computer Networks*, **2017**, 116, 33-46	5.4	4
140	HyBIS: Advanced Introspection for Effective Windows Guest Protection. *IFIP Advances in Information and Communication Technology*, **2017**, 189-204	0.5	1

139	Social Fingerprinting: Detection of Spambot Groups Through DNA-Inspired Behavioral Modeling. *IEEE Transactions on Dependable and Secure Computing*, **2017**, 1-1	3.9	26
138	Epidemic data survivability in Unattended Wireless Sensor Networks: New models and results. *Journal of Network and Computer Applications*, **2017**, 99, 146-165	7.9	5
137	CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT **2017**,		26
136	The Paradigm-Shift of Social Spambots **2017**,		140
135	CoLLIDE: CLoud Latency-based IDEntification. *Procedia Computer Science*, **2017**, 113, 81-88	1.6	
134	Exploiting Digital DNA for the Analysis of Similarities in Twitter Behaviours **2017**,		7
133	Trusted, Heterogeneous, and Autonomic Mobile Cloud **2016**, 439-455		
132	. *IEEE Transactions on Dependable and Secure Computing*, **2016**, 13, 296-311	3.9	4
131	To Docker or Not to Docker: A Security Perspective. *IEEE Cloud Computing*, **2016**, 3, 54-62		95
130	Secure Management of Virtualized Resources **2016**, 193-217		3
129	CUDA Leaks. *Transactions on Embedded Computing Systems*, **2016**, 15, 1-25	1.8	26
128	Proof of ownership for deduplication systems: A secure, scalable, and efficient solution. *Computer Communications*, **2016**, 82, 71-82	5.1	16
127	Heterogeneous Architectures: Malware and Countermeasures **2016**, 421-438		1
126	Reliable and perfectly secret communication over the generalized Ozarow-Wyner wire-tap channel. *Computer Networks*, **2016**, 109, 21-30	5.4	3
125	DNA-Inspired Online Behavioral Modeling and Its Application to Spambot Detection. *IEEE Intelligent Systems*, **2016**, 31, 58-64	4.2	66
124	CURE owards enforcing a reliable timeline for cloud forensics: Model, architecture, and experiments. *Computer Communications*, **2016**, 91-92, 29-43	5.1	10
123	Logical key hierarchy for groups management in Distributed Online Social Network **2016**,		3
122	EXPEDITE: EXPress closED ITemset Enumeration. *Expert Systems With Applications*, **2015**, 42, 3933-3944	7.8	3

121	Freedom of speech: thwarting jammers via a probabilistic approach **2015**,		4
120	Alterdroid: Differential Fault Analysis of Obfuscated Smartphone Malware. *IEEE Transactions on Mobile Computing*, **2015**, 1-1	4.6	9
119	Fame for sale: Efficient detection of fake Twitter followers. *Decision Support Systems*, **2015**, 80, 56-71	5.6	166
118	Silence is Golden. *ACM Transactions on Information and System Security*, **2015**, 17, 1-24		13
117	Visual detection of singularities in review platforms **2015**,		1
116	VISIO: A Visual Approach for Singularity Detection in Recommendation Systems. *Lecture Notes in Computer Science*, **2015**, 33-47	0.9	1
115	The impact of GPU-assisted malware on memory forensics: A case study. *Digital Investigation*, **2015**, 14, S16-S24	3.3	4
114	SOLDI: Secure Off-Line Disposable CredIts to Secure Mobile Micro Payments. *Communications in Computer and Information Science*, **2015**, 340-362	0.3	
113	AntiCheetah: Trustworthy computing in an outsourced (cheating) environment. *Future Generation Computer Systems*, **2015**, 48, 28-38	7.5	2
112	ESC: An efficient, scalable, and crypto-less solution to secure wireless networks. *Computer Networks*, **2015**, 84, 46-63	5.4	8
111	Provable Storage Medium for Data Storage Outsourcing. *IEEE Transactions on Services Computing*, **2015**, 8, 985-997	4.8	3
110	A Criticism to Society (As Seen by Twitter Analytics) **2014**,		10
109	Thwarting Obfuscated Malware via Differential Fault Analysis. *Computer*, **2014**, 47, 24-31	1.6	39
108	Security in wireless ad-hoc networks A survey. *Computer Communications*, **2014**, 51, 1-20	5.1	91
107	Clone wars: Distributed detection of clone attacks in mobile WSNs. *Journal of Computer and System Sciences*, **2014**, 80, 654-669	1	29
106	CloRExPa: Cloud resilience via execution path analysis. *Future Generation Computer Systems*, **2014**, 32, 168-179	7.5	15
105	A tunable proof of ownership scheme for deduplication using Bloom filters **2014**,		24
104	FORCE - Fully Off-line secuRe CrEdits for Mobile Micro Payments **2014**,		5

103	Virtualization and Cloud Security: Benefits, Caveats, and Future Developments. *Computer Communications and Networks*, **2014**, 237-255	0.5	3
102	Towards a GPU Cloud: Benefits and Security Issues. *Computer Communications and Networks*, **2014**, 3-22	0.5	3
101	COKE Crypto-Less Over-the-Air Key Establishment. *IEEE Transactions on Information Forensics and Security*, **2013**, 8, 163-173	8	17
100	Preserving privacy against external and internal threats in WSN data aggregation. *Telecommunication Systems*, **2013**, 52, 2163-2176	2.3	21
99	Titans revenge: Detecting Zeus via its own flaws. *Computer Networks*, **2013**, 57, 422-435	5.4	12
98	Data confidentiality and availability via secret sharing and node mobility in UWSN **2013**,		8
97	Track me if you can: Transparent obfuscation for Location based Services **2013**,		3
96	CREPUSCOLO: A collusion resistant privacy preserving location verification system **2013**,		4
95	Confidentiality and availability issues in Mobile Unattended Wireless Sensor Networks **2013**,		4
94	United We Stand: Intrusion Resilience in Mobile Unattended WSNs. *IEEE Transactions on Mobile Computing*, **2013**, 12, 1456-1468	4.6	11
93	AntiCheetah: An Autonomic Multi-round Approach for Reliable Computing **2013**,		2
92	Windows Mobile LiveSD Forensics. *Journal of Network and Computer Applications*, **2013**, 36, 677-684	7.9	12
91	Epidemic theory and data survivability in unattended wireless sensor networks: Models and gaps. *Pervasive and Mobile Computing*, **2013**, 9, 588-597	3.5	6
90	Security in Wireless Ad Hoc Networks **2013**, 106-153		
89	. *IEEE Network*, **2013**, 27, 10-15	11.4	37
88	Adversaries and Countermeasures in Privacy-Enhanced Urban Sensing Systems. *IEEE Systems Journal*, **2013**, 7, 311-322	4.3	9
87	Visual Role Mining: A Picture Is Worth a Thousand Roles. *IEEE Transactions on Knowledge and Data Engineering*, **2012**, 24, 1120-1133	4.2	20
86	Wireless Sensor Replica Detection in Mobile Environments. *Lecture Notes in Computer Science*, **2012**, 249-264	0.9	4

85	A business-driven decomposition methodology for role mining. *Computers and Security*, **2012**, 31, 844-855	1.9	17
84	Sense-And-Trace: A Privacy Preserving Distributed Geolocation Tracking System. *Lecture Notes in Computer Science*, **2012**, 199-213	0.9	1
83	Self-healing in unattended wireless sensor networks. *ACM Transactions on Sensor Networks*, **2012**, 9, 1-21	2.9	5
82	Boosting efficiency and security in proof of ownership for deduplication **2012**,		58
81	PRISM Privacy-Preserving Search in MapReduce. *Lecture Notes in Computer Science*, **2012**, 180-200	0.9	31
80	Preserving Query Privacy in Urban Sensing Systems. *Lecture Notes in Computer Science*, **2012**, 218-233	0.9	4
79	. *IEEE Transactions on Dependable and Secure Computing*, **2011**, 8, 685-698	3.9	85
78	Intrusion-resilient integrity in data-centric unattended WSNs. *Pervasive and Mobile Computing*, **2011**, 7, 495-508	3.5	4
77	"Who Counterfeited My Viagra?" Probabilistic Item Removal Detection via RFID Tag Cooperation. *Eurasip Journal on Wireless Communications and Networking*, **2011**, 2011,	3.2	1
76	Cross-border co-operation and education in digital investigations: A European perspective. *Digital Investigation*, **2011**, 8, 106-113	3.3	1
75	A new role mining framework to elicit business roles and to mitigate enterprise risk. *Decision Support Systems*, **2011**, 50, 715-731	5.6	27
74	CASSANDRA: a probabilistic, efficient, and privacy-preserving solution to compute set intersection. *International Journal of Information Security*, **2011**, 10, 301-319	2.8	1
73	Secure topology maintenance and events collection in WSNs. *Security and Communication Networks*, **2011**, 4, 744-762	1.9	6
72	Events privacy in WSNs: A new model and its application **2011**,		9
71	**2011**,		7
70	Introducing epidemic models for data survivability in Unattended Wireless Sensor Networks **2011**,		10
69	Location privacy and resilience in wireless sensor networks querying. *Computer Communications*, **2011**, 34, 515-523	5.1	27
68	An optimal probabilistic solution for information confinement, privacy, and security in RFID systems. *Journal of Network and Computer Applications*, **2011**, 34, 853-863	7.9	11

67	Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, **2011**, 34, 1113-1122	7.9	186
66	Epidemic data survivability in unattended wireless sensor networks **2011**,		9
65	Robust and efficient authentication of video stream broadcasting. *ACM Transactions on Information and System Security*, **2011**, 14, 1-25		3
64	Time in Privacy Preserving LBSs: An Overlooked Dimension. *International Journal of Vehicular Technology*, **2011**, 2011, 1-12		0
63	Event Handoff Unobservability in WSN. *Lecture Notes in Computer Science*, **2011**, 20-28	0.9	4
62	Hierarchies of keys in secure multicast communications. *Journal of Computer Security*, **2010**, 18, 839-860	0.8	
61	ABBA **2010**,		11
60	**2010**,		4
59	Intrusion-Resilience in Mobile Unattended WSNs **2010**,		15
58	CReW: Cloud Resilience for Windows Guests through Monitored Virtualization **2010**,		5
57	Time Warp: How Time Affects Privacy in LBSs. *Lecture Notes in Computer Science*, **2010**, 325-339	0.9	5
56	Securing Mobile Unattended WSNs against a Mobile Adversary **2010**,		13
55	**2010**,		1
54	The smallville effect **2010**,		9
53	Transparent security for cloud **2010**,		22
52	Concise: Compressed □□Composable Integer Set. *Information Processing Letters*, **2010**, 110, 644-650	0.8	53
51	Taming role mining complexity in RBAC. *Computers and Security*, **2010**, 29, 548-564	4.9	27
50	eRIPP-FS: Enforcing privacy and security in RFID. *Security and Communication Networks*, **2010**, 3, 58-70	1.9	5

49	Evaluating the Risk of Adopting RBAC Roles. *Lecture Notes in Computer Science*, **2010**, 303-310	0.9	1
48	Mining Business-Relevant RBAC States through Decomposition. *IFIP Advances in Information and Communication Technology*, **2010**, 19-30	0.5	4
47	CUDACS: Securing the Cloud with CUDA-Enabled Secure Virtualization. *Lecture Notes in Computer Science*, **2010**, 92-106	0.9	5
46	CED2: Communication Efficient Disjointness Decision. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2010**, 290-306	0.2	1
45	Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks. *Ad Hoc Networks*, **2009**, 7, 1463-1475	4.8	29
44	Distributed data source verification in wireless sensor networks. *Information Fusion*, **2009**, 10, 342-353	16.7	8
43	Confidentiality and integrity for data aggregation in WSN using peer monitoring. *Security and Communication Networks*, **2009**, 2, 181-194	1.9	23
42	Privacy-preserving robust data aggregation in wireless sensor networks. *Security and Communication Networks*, **2009**, 2, 195-213	1.9	42
41	KvmSec **2009**,		19
40	Collaborative authentication in unattended WSNs **2009**,		23
39	The Quest for Mobility Models to Analyse Security in Mobile Ad Hoc Networks. *Lecture Notes in Computer Science*, **2009**, 85-96	0.9	5
38	. *IEEE Transactions on Computers*, **2009**, 58, 1500-1511	2.5	47
37	A formal framework to elicit roles with business meaning in RBAC systems **2009**,		34
36	Mobility and Cooperation to Thwart Node Capture Attacks in MANETs. *Eurasip Journal on Wireless Communications and Networking*, **2009**, 2009,	3.2	25
35	Mining Stable Roles in RBAC. *IFIP Advances in Information and Communication Technology*, **2009**, 259-269	0.5	10
34	A Probabilistic Bound on the Basic Role Mining Problem and Its Applications. *IFIP Advances in Information and Communication Technology*, **2009**, 376-386	0.5	11
33	Sec-TMP: A Secure Topology Maintenance Protocol for Event Delivery Enforcement in WSN. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2009**, 265-284	0.2	1
32	POSH: Proactive co-Operative Self-Healing in Unattended Wireless Sensor Networks **2008**,		39

31	Scalable and efficient provable data possession **2008**,		460
30	Catch Me (If You Can): Data Survival in Unattended Sensor Networks **2008**,		66
29	Emergent properties **2008**,		51
28	A cost-driven approach to role engineering **2008**,		43
27	Redoubtable Sensor Networks. *ACM Transactions on Information and System Security*, **2008**, 11, 1-22		64
26	Gossip-based aggregate computation **2008**,		2
25	A mechanism to enforce privacy in vehicle-to-infrastructure communication. *Computer Communications*, **2008**, 31, 2790-2802	5.1	17
24	Maximizing service availability for secure satellite broadcasting. *International Journal of Satellite Communications and Networking*, **2008**, 26, 269-289	1.7	1
23	A Live Digital Forensic system for Windows networks. *International Federation for Information Processing*, **2008**, 653-667		3
22	Leveraging Lattices to Improve Role Mining. *International Federation for Information Processing*, **2008**, 333-347		14
21	. *IEEE Vehicular Technology Conference*, **2007**,	0.1	6
20	Robust RSA distributed signatures for large-scale long-lived ad hoc networks. *Journal of Computer Security*, **2007**, 15, 171-196	0.8	1
19	ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks. *Ad Hoc Networks*, **2007**, 5, 49-62	4.8	23
18	Efficient and Adaptive Threshold Signatures for Ad hoc networks. *Electronic Notes in Theoretical Computer Science*, **2007**, 171, 93-105	0.7	4
17	VIPER: A vehicle-to-infrastructure communication privacy enforcement protocol **2007**,		5
16	Secure k-Connectivity Properties of Wireless Sensor Networks **2007**,		7
15	A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks **2007**,		80
14	FastRIPP: RFID Privacy Preserving protocol with Forward Secrecy and Fast Resynchronisation **2007**,		4

13	**2007**,		23
12	Information Confinement, Privacy, and Security in RFID Systems. *Lecture Notes in Computer Science*, **2007**, 187-202	0.9	16
11	Addressing the shortcomings of one-way chains **2006**,		6
10	**2006**,		12
9	Sensor Networks that Are Provably Resilient **2006**,		17
8	Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks. *Wireless Networks*, **2006**, 12, 709-721	2.5	58
7	Key management for high bandwidth secure multicast*. *Journal of Computer Security*, **2004**, 12, 693-709	0.8	5
6	Connectivity properties of secure wireless sensor networks **2004**,		34
5	Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, **2003**, 46, 74-79	2.5	34
4	Providing secrecy in key management protocols for large wireless sensors networks. *Ad Hoc Networks*, **2003**, 1, 455-468	4.8	31
3	Random key-assignment for secure Wireless Sensor Networks **2003**,		116
2	Formal Specification for Fast Automatic IDS Training. *Lecture Notes in Computer Science*, **2003**, 191-204	0.9	2
1	Network Security509-585		0