Miguel P Correia

List of Publications by Year in Descending Order

113 papers	1,839 citations	22 h-index	38 g-index
149 ext. papers	2,365 ext. citations	2.6 avg, IF	4.98 L-index

#	Paper	IF	Citations
113	Sanare: Pluggable Intrusion Recovery for Web Applications. *IEEE Transactions on Dependable and Secure Computing*, **2022**, 1-1	3.9	
112	Statically Detecting Vulnerabilities by Processing Programming Languages as Natural Languages. *IEEE Transactions on Reliability*, **2022**, 1-24	4.6	
111	Hermes: Fault-tolerant middleware for blockchain interoperability. *Future Generation Computer Systems*, **2022**, 129, 236-251	7.5	4
110	SRX Secure Data Backup and Recovery for SGX Applications. *IEEE Access*, **2022**, 10, 35901-35918	3.5	0
109	Secure cloud-of-clouds storage with space-efficient secret sharing. *Journal of Information Security and Applications*, **2021**, 59, 102826	3.5	1
108	Omega: a Secure Event Ordering Servicefor for the Edge. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 1-1	3.9	
107	Fireplug: Efficient and Robust Geo-Replication of Graph Databases. *IEEE Transactions on Parallel and Distributed Systems*, **2020**, 31, 1942-1953	3.7	1
106	CryingJackpot: Network Flows and Performance Counters against Cryptojacking **2020**,		1
105	Multi-Language Web Vulnerability Detection **2020**,		2
104	Big Data Analytics for Intrusion Detection. *Advances in Information Security, Privacy, and Ethics Book Series*, **2020**, 292-316	0.3	3
103	MultiTLS: Secure Communication Channels with Cipher Suite Diversity. *IFIP Advances in Information and Communication Technology*, **2020**, 64-77	0.5	
102	Genet: A Quickly Scalable Fat-Tree Overlay for Personal Volunteer Computing using WebRTC **2019**,		3
101	SEPTIC: Detecting Injection Attacks and Vulnerabilities Inside the DBMS. *IEEE Transactions on Reliability*, **2019**, 68, 1168-1188	4.6	9
100	OutGene: Detecting Undefined Network Attacks with Time Stretching and Genetic Zooms. *Lecture Notes in Computer Science*, **2019**, 199-220	0.9	0
99	BlockSim: Blockchain Simulator **2019**,		17
98	An empirical study on combining diverse static analysis tools for web security vulnerabilities based on development scenarios. *Computing (Vienna/New York)*, **2019**, 101, 161-185	2.2	5
97	Fireplug: Flexible and robust N-version geo-replication of graph databases **2018**,		1

96	REPSYS: A Robust and Distributed Incentive Scheme for Collaborative Caching and Dissemination in Content-Centric Cellular-Based Vehicular Delay-Tolerant Networks. *IEEE Wireless Communications*, **2018**, 25, 65-71	13.4	12
95	Securing Electronic Health Records in the Cloud **2018**,		4
94	RockFS **2018**,		7
93	Koordinator: A Service Approach for Replicating Docker Containers in Kubernetes **2018**,		7
92	FlowHacker: Detecting Unknown Network Attacks in Big Traffic Data Using Network Flows **2018**,		7
91	ePRIVO: An Enhanced PRIvacy-preserVing Opportunistic Routing Protocol for Vehicular Delay-Tolerant Networks. *IEEE Transactions on Vehicular Technology*, **2018**, 67, 11154-11168	6.8	13
90	S-Audit: Efficient Data Integrity Verification for Cloud Storage **2018**,		6
89	. *IEEE Transactions on Reliability*, **2018**, 67, 1159-1175	4.6	22
88	State machine replication in containers managed by Kubernetes. *Journal of Systems Architecture*, **2017**, 73, 53-59	5.5	40
87	On the Design of Resilient Multicloud MapReduce. *IEEE Cloud Computing*, **2017**, 4, 74-82		3
86	Chrysaor: Fine-Grained, Fault-Tolerant Cloud-of-Clouds MapReduce **2017**,		4
85	TruApp: A TrustZone-based authenticity detection service for mobile apps **2017**,		3
84	Demonstrating a Tool for Injection Attack Prevention in MySQL **2017**,		2
83	PRIVO: A privacy-preserving opportunistic routing protocol for delay tolerant networks **2017**,		9
82	Rectify **2017**,		3
81	On Combining Diverse Static Analysis Tools for Web Security: An Empirical Study **2017**,		9
80	REPSYS **2017**,		8
79	T2Droid: A TrustZone-Based Dynamic Analyser for Android Applications **2017**,		8

78	A Systematic Approach for the Application of Restricted Boltzmann Machines in Network Intrusion Detection. *Lecture Notes in Computer Science*, **2017**, 432-446	0.9	6
77	Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining. *IEEE Transactions on Reliability*, **2016**, 65, 54-69	4.6	52
76	Medusa: An Efficient Cloud Fault-Tolerant MapReduce **2016**,		15
75	DEKANT: a static analysis tool that learns to detect web application vulnerabilities **2016**,		26
74	Light-SPD **2016**,		3
73	Feature set tuning in statistical learning network intrusion detection **2016**,		6
72	**2016**,		6
71	DARSHANA: Detecting route hijacking for communication confidentiality **2016**,		3
70	JITeR: Just-in-time application-layer routing. *Computer Networks*, **2016**, 104, 122-136	5.4	5
69	Hacking the DBMS to Prevent Injection Attacks **2016**,		3
68	Equipping WAP with WEAPONS to Detect Vulnerabilities: Practical Experience Report **2016**,		2
67	Betweenness centrality in Delay Tolerant Networks: A survey. *Ad Hoc Networks*, **2015**, 33, 284-305	4.8	22
66	Greft: Arbitrary Fault-Tolerant Distributed Graph Processing **2015**,		4
65	Shuttle: Intrusion Recovery for PaaS **2015**,		3
64	Big Data Analytics for Detecting Host Misbehavior in Large Logs **2015**,		10
63	A multi-objective routing algorithm for Wireless Multimedia Sensor Networks. *Applied Soft Computing Journal*, **2015**, 30, 104-112	7.5	39
62	Anticipating Requests to Improve Performance and Reduce Costs in Cloud Storage. *Performance Evaluation Review*, **2015**, 43, 21-24	0.4	
61	Automatic detection and correction of web application vulnerabilities using data mining to predict false positives **2014**,		33

60	Cloud Computing Dependability. *Operating Systems Review (ACM)*, **2014**, 48, 1-2	0.8	
59	Clouds-of-Clouds for Dependability and Security: Geo-replication Meets the Cloud. *Lecture Notes in Computer Science*, **2014**, 95-104	0.9	
58	MITRA. *SIGMOD Record*, **2014**, 43, 32-38	1.1	3
57	NodesUmisbehavior in Vehicular Delay-Tolerant Networks **2013**,		2
56	Securing energy metering software with automatic source code correction **2013**,		2
55	. *IEEE Transactions on Mobile Computing*, **2013**, 12, 2441-2454	4.6	15
54	Efficient Byzantine Fault-Tolerance. *IEEE Transactions on Computers*, **2013**, 62, 16-30	2.5	118
53	On the Performance of Byzantine Fault-Tolerant MapReduce. *IEEE Transactions on Dependable and Secure Computing*, **2013**, 10, 301-313	3.9	8
52	DepSky. *ACM Transactions on Storage*, **2013**, 9, 1-33	1	153
51	Byzantine fault-tolerant state machine replication with twin virtual machines **2013**,		5
50	BFT-TO: Intrusion Tolerance with Less Replicas. *Computer Journal*, **2013**, 56, 693-715	1.3	7
49	On the Feasibility of Byzantine Fault-Tolerant MapReduce in Clouds-of-Clouds **2012**,		6
48	Lucy in the sky without diamonds: Stealing confidential data in the cloud **2011**,		83
47	Byzantine Fault-Tolerant MapReduce: Faults are Not Just Crashes **2011**,		18
46	DepSky **2011**,		164
45	Byzantine consensus in asynchronous message-passing systems: a survey. *International Journal of Critical Computer-Based Systems*, **2011**, 2, 141	0.4	22
44	The Final Frontier: Confidentiality and Privacy in the Cloud. *Computer*, **2011**, 44, 44-50	1.6	30
43	Randomization can be a healer: consensus with dynamic omission failures. *Distributed Computing*, **2011**, 24, 165-175	1.2	

42	Byzantine Fault-Tolerant Transaction Processing for Replicated Databases **2011**,		2
41	Anomaly-based intrusion detection in software as a service **2011**,		17
40	RITAS: Services for Randomized Intrusion Tolerance. *IEEE Transactions on Dependable and Secure Computing*, **2011**, 8, 122-136	3.9	17
39	N-party BAR Transfer. *Lecture Notes in Computer Science*, **2011**, 392-408	0.9	3
38	**2010**,		7
37	Asynchronous Byzantine consensus with 2f+1 processes **2010**,		14
36	Vulnerability Discovery with Attack Injection. *IEEE Transactions on Software Engineering*, **2010**, 36, 357-370	3.5	30
35	Highly Available Intrusion-Tolerant Services with Proactive-Reactive Recovery. *IEEE Transactions on Parallel and Distributed Systems*, **2010**, 21, 452-465	3.7	70
34	EBAWA: Efficient Byzantine Agreement for Wide-Area Networks **2010**,		34
33	Intrusion Tolerant Services Through Virtualization: A Shared Memory Approach **2010**,		8
32	A Distributed Systems Approach to Airborne Self-Separation **2010**, 215-236		
31	Intrusion-tolerant self-healing devices for critical infrastructure protection **2009**,		7
30	Spin One's Wheels? Byzantine Fault Tolerance with a Spinning Primary **2009**,		43
29	Sharing Memory between Byzantine Processes Using Policy-Enforced Tuple Spaces. *IEEE Transactions on Parallel and Distributed Systems*, **2009**, 20, 419-432	3.7	5
28	An Efficient Byzantine-Resilient Tuple Space. *IEEE Transactions on Computers*, **2009**, 58, 1080-1094	2.5	5
27	Randomization Can Be a Healer: Consensus with Dynamic Omission Failures. *Lecture Notes in Computer Science*, **2009**, 63-77	0.9	2
26	The CRUTIAL reference critical information infrastructure architecture: a blueprint. *International Journal of System of Systems Engineering*, **2008**, 1, 78	0.3	15
25	The CRUTIAL Architecture for Critical Information Infrastructures. *Lecture Notes in Computer Science*, **2008**, 1-27	0.9	14

24	DepSpace. *Operating Systems Review (ACM)*, **2008**, 42, 163-176	0.8	11
23	On Byzantine generals with alternative plans. *Journal of Parallel and Distributed Computing*, **2008**, 68, 1291-1296	4.4	9
22	. *IEEE Security and Privacy*, **2008**, 6, 44-51	2	46
21	DepSpace **2008**,		36
20	Automated Rule-Based Diagnosis Through a Distributed Monitor System. *IEEE Transactions on Dependable and Secure Computing*, **2007**, 4, 266-279	3.9	23
19	GRIDTS: A New Approach for Fault-Tolerant Scheduling in Grid Computing **2007**,		12
18	Exploiting Tuple Spaces to Provide Fault-Tolerant Scheduling on Computational Grids **2007**,		5
17	Intrusion Tolerance in Wireless Environments: An Experimental Evaluation **2007**,		3
16	Decoupled Quorum-Based Byzantine-Resilient Coordination in Open Distributed Systems **2007**,		2
15	Worm-IT □A wormhole-based intrusion-tolerant group communication system. *Journal of Systems and Software*, **2007**, 80, 178-197	3.3	15
14	Resilient Intrusion Tolerance through Proactive and Reactive Recovery **2007**,		32
13	Evaluating Byzantine Quorum Systems **2007**,		2
12	From Consensus to Atomic Broadcast: Time-Free Byzantine-Resistant Protocols without Signatures. *Computer Journal*, **2006**, 49, 82-96	1.3	53
11	Experimental Comparison of Local and Shared Coin Randomized Consensus Protocols. *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, **2006**,		10
10	Brief Announcement: Decoupled Quorum-Based Byzantine-Resilient Coordination in Open Distributed Systems. *Lecture Notes in Computer Science*, **2006**, 554-556	0.9	
9	CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture. *Lecture Notes in Computer Science*, **2006**, 1-14	0.9	9
8	Solving vector consensus with a wormhole. *IEEE Transactions on Parallel and Distributed Systems*, **2005**, 16, 1120-1131	3.7	19
7	Low complexity Byzantine-resilient consensus. *Distributed Computing*, **2005**, 17, 237-249	1.2	27

6	Intrusion-Tolerant Architectures: Concepts and Design. *Lecture Notes in Computer Science*, **2003**, 3-36	0.9	65
5	The Design of a COTS Real-Time Distributed Security Kernel. *Lecture Notes in Computer Science*, **2002**, 234-252	0.9	20
4	Randomized Intrusion-Tolerant Asynchronous Services		10
3	Using Attack Injection to Discover New Vulnerabilities		24
2	Efficient Byzantine-resilient reliable multicast on a hybrid failure model		17
1	HERMES: Fault-Tolerant Middleware for Blockchain Interoperability		2