

# CITATION REPORT

List of articles citing

## The science of cyber security experimentation

DOI: 10.1145/2076732.2076752  
, 2011, , .

**Source:** <https://exaly.com/paper-pdf/50189752/citation-report.pdf>

**Version:** 2024-04-23

This report has been generated based on the citations recorded by exaly.com for the above article. 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.

#	Paper	IF	Citations
67	NCS security experimentation using DETER. <b>2012,</b>		4
66	Reducing allocation errors in network testbeds. <b>2012,</b>		2
65	The DETER Project: Towards Structural Advances in Experimental Cybersecurity Research and Evaluation. <i>Journal of Information Processing</i> , <b>2012</b> , 20, 824-834	0.2	3
64	One year of SSL internet measurement. <b>2012,</b>		14
63	A dual-process cognitive model for testing resilient control systems. <b>2012,</b>		6
62	In quest of benchmarking security risks to cyber-physical systems. <i>IEEE Network</i> , <b>2013</b> , 27, 19-24	11.4	64
61	First steps toward scientific cyber-security experimentation in wide-area cyber-physical systems. <b>2013,</b>		3
60	Replay of malicious traffic in network testbeds. <b>2013,</b>		3
59	Enabling Collaborative Research for Security and Resiliency of Energy Cyber Physical Systems. <b>2014</b>		1
58	Semi-synthetic data set generation for security software evaluation. <b>2014,</b>		13
57	Towards a science of trust. <b>2015,</b>		2
56	. <i>IEEE Transactions on Smart Grid</i> , <b>2015</b> , 6, 2444-2453	10.7	107
55	Tor Experimentation Tools. <b>2015,</b>		7
54	Dispersing Asymmetric DDoS Attacks with SplitStack. <b>2016,</b>		7
53	Cost sensitive moving target consensus. <b>2016,</b>		1
52	Platoon. <b>2016,</b>		2
51	Complex log file synthesis for rapid sandbox-benchmarking of security- and computer network analysis tools. <i>Information Systems</i> , <b>2016</b> , 60, 13-33	2.7	9

50	Application of HAZOP to the Design of Cyber Security Experiments. <b>2016,</b>		0
49	Experimentation Support for Cyber Security Evaluations. <b>2016,</b>		1
48	Authorization and Access Control: ABAC. <b>2016,</b> 203-234		3
47	A security analysis and revised security extension for the precision time protocol. <b>2016,</b>		13
46	VirTUAL remoTe labORatories Management System (TUTORES): Using Cloud Computing to Acquire University Practical Skills. <i>IEEE Transactions on Learning Technologies</i> , <b>2016,</b> 9, 133-145	4	18
45	EZSetup. <b>2017,</b>		1
44	Secure Double-Layered Defense against HTTP-DDoS Attacks. <b>2017,</b>		2
43	SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit. <b>2017,</b>		31
42	Secure Causal Atomic Broadcast, Revisited. <b>2017,</b>		10
41	Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. <b>2017,</b>		11
40	Lessons learned from complex hands-on defence exercises in a cyber range. <b>2017,</b>		20
39	A conceptual framework to federate testbeds for cybersecurity. <b>2017,</b>		1
38	A Flexible Approach Towards Security Validation. <b>2017,</b>		
37	Trustworthy DDoS Defense: Design, Proof of Concept Implementation and Testing. <i>IEICE Transactions on Information and Systems</i> , <b>2017,</b> E100.D, 1738-1750	0.6	2
36	LDplayer. <b>2018,</b>		
35	A Formal Treatment of Efficient Byzantine Routing Against Fully Byzantine Adversary. <b>2018,</b>		
34	Building a Cybersecurity Research and Experimentation Testbed. <b>2018,</b>		
33	Tsumiki: A Meta-Platform for Building Your Own Testbed. <i>IEEE Transactions on Parallel and Distributed Systems</i> , <b>2018,</b> 29, 2863-2881	3.7	1

32	Virtually the Same: Comparing Physical and Virtual Testbeds. <b>2019</b> ,			1
31	. <b>2019</b> ,			2
30	. <b>2019</b> ,			
29	Powering Hands-on Cybersecurity Practices with Cloud Computing. <b>2019</b> ,			0
28	TestREx: a framework for repeatable exploits. <i>International Journal on Software Tools for Technology Transfer</i> , <b>2019</b> , 21, 105-119	1.3		1
27	A Security Analysis and Revised Security Extension for the Precision Time Protocol. <i>IEEE Transactions on Dependable and Secure Computing</i> , <b>2020</b> , 17, 22-34	3.9		11
26	Blockchain Performance Analysis for Supporting Cross-Border E-Government Services. <i>IEEE Transactions on Engineering Management</i> , <b>2020</b> , 67, 1310-1322	2.6		13
25	Cyber Range for Research-Inspired Learning of Attack Defense by Pretense Principle and Practice. <i>IEEE Transactions on Learning Technologies</i> , <b>2021</b> , 14, 322-337	4		3
24	Sharing Pandemic Vaccination Certificates through Blockchain: Case Study and Performance Evaluation. <i>Wireless Communications and Mobile Computing</i> , <b>2021</b> , 2021, 1-12	1.9		6
23	Case Studies in Experiment Design on a minimega Based Network Emulation Testbed. <b>2021</b> ,			0
22	AI-assisted Computer Network Operations testbed for Nature-Inspired Cyber Security based adaptive defense simulation and analysis. <i>Future Generation Computer Systems</i> , <b>2022</b> , 127, 297-308	7.5		3
21	Pandora: A Cyber Range Environment for the Safe Testing and Deployment of Autonomous Cyber Attack Tools. <i>Communications in Computer and Information Science</i> , <b>2021</b> , 1-20	0.3		1
20	BChain: Byzantine Replication with High Throughput and Embedded Reconfiguration. <i>Lecture Notes in Computer Science</i> , <b>2014</b> , 91-106	0.9		20
19	A Survey of Industrial Control System Testbeds. <i>Lecture Notes in Computer Science</i> , <b>2015</b> , 11-26	0.9		39
18	DETERLab and the DETER Project. <b>2016</b> , 35-62			4
17	Using Terminal Histories to Monitor Student Progress on Hands-on Exercises. <b>2020</b> ,			4
16	CYRAN. <i>Advances in Information Security, Privacy, and Ethics Book Series</i> , 226-241	0.3		1
15	CYRAN. <b>2018</b> , 622-637			9

14	KYPO: A Tool for Collaborative Study of Cyberattacks in Safe Cloud Environment. <i>Lecture Notes in Computer Science</i> , <b>2015</b> , 190-199	0.9	
13	Towards a Self-Adaptive Middleware for Building Reliable Publish/Subscribe Systems. <i>Lecture Notes in Computer Science</i> , <b>2015</b> , 157-168	0.9	
12	Achieving Reproducible Network Environments with INSALATA. <i>Lecture Notes in Computer Science</i> , <b>2017</b> , 30-44	0.9	1
11	Cyber threat modeling and validation. <b>2020</b> ,		0
10	An Experimental Approach for Estimating Cyber Risk: a Proposal Building upon Cyber Ranges and Capture the Flags. <b>2020</b> ,		1
9	Toolset for Collecting Shell Commands and Its Application in Hands-on Cybersecurity Training. <b>2021</b> ,		1
8	Novel Network Testbed of Adaptive Cyber Defense System Design for Web Data security. <i>International Journal of Advanced Research in Science, Communication and Technology</i> , 333-340	0.5	
7	Blockchain for Transport (BC4 T), Performance Simulations of Blockchain Network for Emission Monitoring. <b>2022</b> ,		
6	A game model design using test bed for Malware analysis training. <i>Information and Computer Security</i> ,	1.4	
5	Reproducible and Adaptable Log Data Generation for Sound Cybersecurity Experiments. <b>2021</b> ,		1
4	Towards an Operations-Aware Experimentation Methodology. <b>2022</b> ,		0
3	Toward Findable, Accessible, Interoperable, and Reusable Cybersecurity Artifacts. <b>2022</b> ,		0
2	Measuring and Analyzing DoS Flooding Experiments. <b>2022</b> ,		
1	The Semantic Processing Pipeline: Quantifying the Network-Wide Impact of Security Tools. <b>2020</b> ,		0