Somesh Jha

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/10685477/publications.pdf

Version: 2024-02-01

38

papers

7,498

citations

623574

14

h-index

677027

22

g-index

41

all docs

41

docs citations

41

times ranked

4303

citing authors

#	Article	IF	Citations
1	The Limitations of Deep Learning in Adversarial Settings. , 2016, , .		1,868
2	Practical Black-Box Attacks against Machine Learning. , 2017, , .		1,665
3	Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. , 2015, , .		1,231
4	Counterexample-guided abstraction refinement for symbolic model checking. Journal of the ACM, 2003, 50, 752-794.	1.8	798
5	Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting. , 2018, , .		336
6	Towards automatic generation of vulnerability-based signatures. , 2006, , .		179
7	Weighted pushdown systems and their application to interprocedural dataflow analysis. Science of Computer Programming, 2005, 58, 206-263.	1.5	144
8	Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors. , 2010, , .		143
9	Testing malware detectors. , 2004, , .		129
10	Composite Constant Propagation: Application to Android Inter-Component Communication Analysis. , 2015, , .		111
11	Towards Formal Verification of Role-Based Access Control Policies. IEEE Transactions on Dependable and Secure Computing, 2008, 5, 242-255.	3.7	94
12	Verification of the Futurebus+ cache coherence protocol. Formal Methods in System Design, 1995, 6, 217-232.	0.9	86
13	A Methodology for Formalizing Model-Inversion Attacks. , 2016, , .		83
14	Retargeting Android applications to Java bytecode. , 2012, , .		76
15	Creating Vulnerability Signatures Using Weakest Preconditions. Computer Security Foundations Workshop (CSFW), Proceedings of the IEEE, 2007, , .	0.0	63
16	Combining static analysis with probabilistic models to enable market-scale Android inter-component analysis. , 2016, , .		56
17	MCI : Modeling-based Causality Inference in Audit Logging for Attack Investigation. , 2018, , .		50
18	Backtracking Algorithmic Complexity Attacks against a NIDS. , 2006, , .		49

#	Article	IF	Citations
19	Randomized Stopping Times and American Option Pricing with Transaction Costs. Mathematical Finance, 2001, 11, 33-77.	0.9	40
20	Speculative Parallel Pattern Matching. IEEE Transactions on Information Forensics and Security, 2011, 6, 438-451.	4.5	27
21	A Refined Binomial Lattice for Pricing American Asian Options. Review of Derivatives Research, 1999, 3, 85-105.	0.6	25
22	Accurate approximations for European-style Asian options. Journal of Computational Finance, 1998, 1, 11-30.	0.3	24
23	Software transformations to improve malware detection. Journal in Computer Virology, 2007, 3, 253-265.	1.9	23
24	NetSpy: Automatic Generation of Spyware Signatures for NIDS. , 2006, , .		21
25	Composite Constant Propagation and its Application to Android Program Analysis. IEEE Transactions on Software Engineering, 2016, 42, 999-1014.	4.3	20
26	Overfitting, robustness, and malicious algorithms: A study of potential causes of privacy risk in machine learning. Journal of Computer Security, 2020, 28, 35-70.	0.5	20
27	TRACE: Enterprise-Wide Provenance Tracking for Real-Time APT Detection. IEEE Transactions on Information Forensics and Security, 2021, 16, 4363-4376.	4.5	20
28	Theory and Techniques for Automatic Generation of Vulnerability-Based Signatures. IEEE Transactions on Dependable and Secure Computing, 2008, 5, 224-241.	3.7	18
29	DIFC programs by automatic instrumentation. , 2010, , .		16
30	Detecting Adversarial Examples Using Data Manifolds. , 2018, , .		12
31	Secure Programming via Visibly Pushdown Safety Games. Lecture Notes in Computer Science, 2012, , 581-598.	1.0	10
32	Declarative, Temporal, and Practical Programming with Capabilities. , 2013, , .		9
33	Neural-augmented static analysis of Android communication. , 2018, , .		8
34	Efficient verification of security protocols using partial-order reductions. International Journal on Software Tools for Technology Transfer, 2003, 4, 173-188.	1.7	5
35	Checking relational specifications with binary decision diagrams. Software Engineering Notes: an Informal Newsletter of the Special Interest Committee on Software Engineering / ACM, 1996, 21, 70-80.	0.5	3
36	An Iterative Framework for Simulation Conformance. Journal of Logic and Computation, 2005, 15, 465-488.	0.5	2

#	Article	IF	Citations
37	Analysis Techniques for Information Security. Synthesis Lectures on Information Security Privacy and Trust, 2010, 2, 1-164.	0.3	2
38	Program synthesis for interactive-security systems. Formal Methods in System Design, 2017, 51, 362-394.	0.9	2