Limin Liu

List of Publications by Year
in descending order

27	814	840776 11	677142 22
papers	citations	h-index	g-index

27	27	27	795
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	S-Blocks: Lightweight and Trusted Virtual Security Function With SGX. IEEE Transactions on Cloud Computing, 2022, 10, 1082-1099.	4.4	2
2	Semi-Synchronized Non-Blocking Concurrent Kernel Cruising. IEEE Transactions on Cloud Computing, 2022, 10, 1428-1444.	4.4	0
3	ARGAN: Adversarially Robust Generative Adversarial Networks for Deep Neural Networks Against Adversarial Examples. IEEE Access, 2022, 10, 33602-33615.	4.2	4
4	Using honeypots to model botnet attacks on the internet of medical things. Computers and Electrical Engineering, 2022, 102, 108212.	4.8	7
5	A Large-Scale Study of Android Malware Development Phenomenon on Public Malware Submission and Scanning Platform. IEEE Transactions on Big Data, 2021, 7, 255-270.	6.1	10
6	Exploiting Security Dependence for Conditional Speculation Against Spectre Attacks. IEEE Transactions on Computers, 2021, 70, 963-978.	3.4	1
7	EEJE: Two-Step Input Transformation for Robust DNN Against Adversarial Examples. IEEE Transactions on Network Science and Engineering, 2021, 8, 908-920.	6.4	5
8	A Co-Design Adaptive Defense Scheme With Bounded Security Damages Against Heartbleed-Like Attacks. IEEE Transactions on Information Forensics and Security, 2021, 16, 4691-4704.	6.9	4
9	Commercial hypervisor-based task sandboxing mechanisms are unsecured? But we can fix it!. Journal of Systems Architecture, 2021, 116, 102114.	4.3	2
10	Reviewing IoT Security via Logic Bugs in IoT Platforms and Systems. IEEE Internet of Things Journal, 2021, 8, 11621-11639.	8.7	13
11	An Evolutionary Study of IoT Malware. IEEE Internet of Things Journal, 2021, 8, 15422-15440.	8.7	16
12	Tainting-Assisted and Context-Migrated Symbolic Execution of Android Framework for Vulnerability Discovery and Exploit Generation. IEEE Transactions on Mobile Computing, 2020, 19, 2946-2964.	5.8	11
13	DAMBA: Detecting Android Malware by ORGB Analysis. IEEE Transactions on Reliability, 2020, 69, 55-69.	4.6	33
14	The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal, 2019, 6, 1606-1616.	8.7	302
15	Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 438-453.	5.4	8
16	Learning From Expertsâ€™ Experience: Toward Automated Cyber Security Data Triage. IEEE Systems Journal, 2019, 13, 603-614.	4.6	14
17	POMP++: Facilitating Postmortem Program Diagnosis with Value-set Analysis. IEEE Transactions on Software Engineering, 2019, , 1-1.	5.6	4
18	Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution. Lecture Notes in Computer Science, 2019, , 638-657.	1.3	15

#	Article	IF	Citations
19	Online and Scalable Adaptive Cyber Defense. Lecture Notes in Computer Science, 2019, , 232-261.	1.3	1
20	Leveraging Information Asymmetry to Transform Android Apps into Self-Defending Code Against Repackaging Attacks. IEEE Transactions on Mobile Computing, 2018, 17, 1879-1893.	5.8	17
21	Using Bayesian Networks for Probabilistic Identification of Zero-Day Attack Paths. IEEE Transactions on Information Forensics and Security, 2018, 13, 2506-2521.	6.9	92
22	Towards probabilistic identification of zero-day attack paths. , 2016, , .		18
23	HeapTherapy: An Efficient End-to-End Solution against Heap Buffer Overflows. , 2015, , .		16
24	ViewDroid. , 2014, , .		127
25	Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies. Lecture Notes in Computer Science, 2013, , 536-555.	1.3	15
26	A Framework for Evaluating Mobile App Repackaging Detection Algorithms. Lecture Notes in Computer Science, 2013, , 169-186.	1.3	60
27	SHELF: Preserving Business Continuity and Availability in an Intrusion Recovery System. , 2009, , .		17