Sushil Jajodia

List of Publications by Year in Descending Order

265 papers	8,078 citations	48 h-index	83 g-index
289 ext. papers	9,625 ext. citations	2.4 avg, IF	6.16 L-index

#	Paper	IF	Citations
265	PCAM: A Data-driven Probabilistic Cyber-alert Management Framework. *ACM Transactions on Internet Technology*, **2022**, 22, 1-24	3.8	0
264	. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 18, 310-324	3.9	6
263	A Fake Online Repository Generation Engine for Cyber Deception. *IEEE Transactions on Dependable and Secure Computing*, **2021**, 18, 518-533	3.9	21
262	Fake Document Generation for Cyber Deception by Manipulating Text Comprehensibility. *IEEE Systems Journal*, **2021**, 15, 835-845	4.3	4
261	Distributed Query Evaluation over Encrypted Data. *Lecture Notes in Computer Science*, **2021**, 96-114	0.9	
260	Understanding Account Recovery in the Wild and Its Security Implications. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	
259	Disclose or Exploit? A Game-Theoretic Approach to Strategic Decision Making in Cyber-Warfare. *IEEE Systems Journal*, **2020**, 14, 3779-3790	4.3	4
258	Capture the Bot: Using Adversarial Examples to Improve CAPTCHA Robustness to Bot Attacks. *IEEE Intelligent Systems*, **2020**, 1-1	4.2	3
257	Modeling and Mitigating Security Threats in Network Functions Virtualization (NFV). *Lecture Notes in Computer Science*, **2020**, 3-23	0.9	1
256	An Outsourcing Model for Alert Analysis in a Cybersecurity Operations Center. *ACM Transactions on the Web*, **2020**, 14, 1-22	3.2	2
255	Two Can Play That Game. *ACM Transactions on Intelligent Systems and Technology*, **2020**, 11, 1-20	8	0
254	Generating Realistic Fake Equations in Order to Reduce Intellectual Property Theft. *IEEE Transactions on Dependable and Secure Computing*, **2020**, 1-1	3.9	
253	. *IEEE Transactions on Parallel and Distributed Systems*, **2020**, 31, 16-33	3.7	1
252	Understanding the Manipulation on Recommender Systems through Web Injection. *IEEE Transactions on Information Forensics and Security*, **2020**, 15, 3807-3818	8	3
251	Optimizing the network diversity to improve the resilience of networks against unknown attacks. *Computer Communications*, **2019**, 145, 96-112	5.1	9
250	A methodology for ensuring fair allocation of CSOC effort for alert investigation. *International Journal of Information Security*, **2019**, 18, 199-218	2.8	8
249	Mitigating the insider threat of remote administrators in clouds through maintenance task assignments. *Journal of Computer Security*, **2019**, 27, 427-458	0.8	1

248	CASFinder: Detecting Common Attack Surface. *Lecture Notes in Computer Science*, **2019**, 338-358	0.9	0
247	FakeTables: Using GANs to Generate Functional Dependency Preserving Tables with Bounded Real Data **2019**,		4
246	Adaptive Cyber Defenses for Botnet Detection and Mitigation. *Lecture Notes in Computer Science*, **2019**, 156-205	0.9	2
245	Optimizing Alert Data Management Processes at a Cyber Security Operations Center. *Lecture Notes in Computer Science*, **2019**, 206-231	0.9	3
244	Proactive Defense Through Deception. *Advances in Information Security*, **2019**, 169-202	0.7	1
243	. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 1857-1870	8	3
242	Towards Intelligent Cyber Deception Systems **2019**, 21-33		4
241	. *IEEE Transactions on Information Forensics and Security*, **2019**, 14, 1155-1170	8	6
240	. *IEEE Systems Journal*, **2019**, 13, 1060-1071	4.3	6
239	SHARE. *ACM Transactions on Internet Technology*, **2018**, 18, 1-41	3.8	9
238	Defending from Stealthy Botnets Using Moving Target Defenses. *IEEE Security and Privacy*, **2018**, 16, 92-97	2	16
237	Memory Forensic Challenges Under Misused Architectural Features. *IEEE Transactions on Information Forensics and Security*, **2018**, 13, 2345-2358	8	8
236	A methodology to measure and monitor level of operational effectiveness of a CSOC. *International Journal of Information Security*, **2018**, 17, 121-134	2.8	13
235	A Graphical Model to Assess the Impact of Multi-Step Attacks. *Journal of Defense Modeling and Simulation*, **2018**, 15, 79-93	0.4	11
234	Surviving unpatchable vulnerabilities through heterogeneous network hardening options. *Journal of Computer Security*, **2018**, 26, 761-789	0.8	5
233	Adaptive reallocation of cybersecurity analysts to sensors for balancing risk between sensors. *Service Oriented Computing and Applications*, **2018**, 12, 123-135	1.6	5
232	Hybrid adversarial defense: Merging honeypots and traditional security methods1. *Journal of Computer Security*, **2018**, 26, 615-645	0.8	1
231	VULCON. *ACM Transactions on Privacy and Security*, **2018**, 21, 1-28	2.9	28

230	Data synthesis based on generative adversarial networks. *Proceedings of the VLDB Endowment*, **2018**, 11, 1071-1083	3.1	78
229	Modeling and Mitigating the Insider Threat of Remote Administrators in Clouds. *Lecture Notes in Computer Science*, **2018**, 3-20	0.9	1
228	Generating Hard to Comprehend Fake Documents for Defensive Cyber Deception. *IEEE Intelligent Systems*, **2018**, 33, 16-25	4.2	9
227	Dynamic Optimization of the Level of Operational Effectiveness of a CSOC Under Adverse Conditions. *ACM Transactions on Intelligent Systems and Technology*, **2018**, 9, 1-20	8	7
226	Optimal Scheduling of Cybersecurity Analysts for Minimizing Risk. *ACM Transactions on Intelligent Systems and Technology*, **2017**, 8, 1-32	8	26
225	A Probabilistic Logic of Cyber Deception. *IEEE Transactions on Information Forensics and Security*, **2017**, 12, 2532-2544	8	23
224	Threat Modeling for Cloud Data Center Infrastructures. *Lecture Notes in Computer Science*, **2017**, 302-319	0.9	4
223	Computer-Aided Human Centric Cyber Situation Awareness. *Lecture Notes in Computer Science*, **2017**, 3-25	0.9	5
222	Detecting Stealthy Botnets in a Resource-Constrained Environment using Reinforcement Learning **2017**,		14
221	An Integrated Framework for Cyber Situation Awareness. *Lecture Notes in Computer Science*, **2017**, 29-46	0.9	7
220	An authorization model for multi provider queries. *Proceedings of the VLDB Endowment*, **2017**, 11, 256-268	3.1	6
219	Securing Networks Against Unpatchable and Unknown Vulnerabilities Using Heterogeneous Hardening Options. *Lecture Notes in Computer Science*, **2017**, 509-528	0.9	6
218	Network Security Metrics **2017**,		7
217	Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks **2017**, 1-23		11
216	Refining CVSS-Based Network Security Metrics by Examining the Base Scores **2017**, 25-52		5
215	k-Zero Day Safety: Evaluating the Resilience of Networks Against Unknown Attacks **2017**, 75-93		1
214	A Suite of Metrics for Network Attack Graph Analytics **2017**, 141-176		8
213	A Novel Metric for Measuring Operational Effectiveness of a Cybersecurity Operations Center **2017**, 177-207		

212	Evaluating the Network Diversity of Networks Against Zero-Day Attacks **2017**, 117-140		1
211	Profiling Online Social Behaviors for Compromised Account Detection. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 176-187	8	63
210	Minimum cost rule enforcement for cooperative database access. *Journal of Computer Security*, **2016**, 24, 379-403	0.8	3
209	AHEAD **2016**,		13
208	Diversifying Network Services Under Cost Constraints for Better Resilience Against Unknown Attacks. *Lecture Notes in Computer Science*, **2016**, 295-312	0.9	10
207	Deceiving Attackers by Creating a Virtual Attack Surface **2016**, 167-199		15
206	A Moving Target Defense Approach to Disrupting Stealthy Botnets **2016**,		27
205	Using temporal probabilistic logic for optimal monitoring of security events with limited resources. *Journal of Computer Security*, **2016**, 24, 735-791	0.8	3
204	Network Diversity: A Security Metric for Evaluating the Resilience of Networks Against Zero-Day Attacks. *IEEE Transactions on Information Forensics and Security*, **2016**, 11, 1071-1086	8	62
203	Efficient integrity checks for join queries in the cloud1. *Journal of Computer Security*, **2016**, 24, 347-378	0.8	12
202	A moving target defense approach to mitigate DDoS attacks against proxy-based architectures **2016**,		26
201	Dynamic Scheduling of Cybersecurity Analysts for Minimizing Risk Using Reinforcement Learning. *ACM Transactions on Intelligent Systems and Technology*, **2016**, 8, 1-21	8	30
200	Loose associations to increase utility in data publishing1. *Journal of Computer Security*, **2015**, 23, 59-88	0.8	11
199	Pareto-Optimal Adversarial Defense of Enterprise Systems. *ACM Transactions on Information and System Security*, **2015**, 17, 1-39		32
198	Now You See Me **2015**,		5
197	Keeping Intruders at Bay: A Graph-theoretic Approach to Reducing the Probability of Successful Network Intrusions. *Communications in Computer and Information Science*, **2015**, 191-211	0.3	
196	Disrupting stealthy botnets through strategic placement of detectors **2015**,		5
195	A deception based approach for defeating OS and service fingerprinting **2015**,		11

194	Integrity for Approximate Joins on Untrusted Computational Servers. *IFIP Advances in Information and Communication Technology*, **2015**, 446-459	0.5	1
193	Numerical SQL Value Expressions Over Encrypted Cloud Databases. *Lecture Notes in Computer Science*, **2015**, 455-478	0.9	0
192	Security and Privacy of Data in a Cloud. *Lecture Notes in Computer Science*, **2014**, 18-22	0.9	0
191	Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. *IEEE Transactions on Information Forensics and Security*, **2014**, 9, 681-694	8	71
190	Encryption and Fragmentation for Data Confidentiality in the Cloud. *Lecture Notes in Computer Science*, **2014**, 212-243	0.9	17
189	. *IEEE Transactions on Dependable and Secure Computing*, **2014**, 11, 30-44	3.9	87
188	Fragmentation in Presence of Data Dependencies. *IEEE Transactions on Dependable and Secure Computing*, **2014**, 11, 510-523	3.9	33
187	Consistency and enforcement of access rules in cooperative data sharing environment. *Computers and Security*, **2014**, 41, 3-18	4.9	5
186	Integrity for distributed queries **2014**,		11
185	Self-healing wireless networks under insider jamming attacks **2014**,		4
184	MTD 2014 **2014**,		2
183	Metrics suite for network attack graph analytics **2014**,		32
182	Protecting Enterprise Networks through Attack Surface Expansion **2014**,		7
181	An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities. *Communications in Computer and Information Science*, **2014**, 322-340	0.3	2
180	Network Hardening. *SpringerBriefs in Computer Science*, **2014**,	0.4	5
179	**2014**,		15
178	A probabilistic framework for jammer identification in MANETs. *Ad Hoc Networks*, **2014**, 14, 84-94	4.8	7
177	Attack Graph and Network Hardening. *SpringerBriefs in Computer Science*, **2014**, 15-22	0.4	3

176	Minimum-Cost Network Hardening. *SpringerBriefs in Computer Science*, **2014**, 23-38	0.4	2
175	Linear-Time Network Hardening. *SpringerBriefs in Computer Science*, **2014**, 39-58	0.4	2
174	Automated Cyber Situation Awareness Tools and Models for Improving Analyst Performance. *Advances in Information Security*, **2014**, 47-60	0.7	8
173	TrustDump: Reliable Memory Acquisition on Smartphones. *Lecture Notes in Computer Science*, **2014**, 202-218	0.9	18
172	Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks. *Lecture Notes in Computer Science*, **2014**, 494-511	0.9	24
171	Formation of Awareness. *Advances in Information Security*, **2014**, 47-62	0.7	3
170	Consistent Query Plan Generation in Secure Cooperative Data Access. *Lecture Notes in Computer Science*, **2014**, 227-242	0.9	4
169	Optimizing Integrity Checks for Join Queries in the Cloud. *Lecture Notes in Computer Science*, **2014**, 33-48	0.9	4
168	Database Security and Privacy **2014**, 53-1-53-21		
167	Enabling Collaborative Data Authorization Between Enterprise Clouds **2014**, 149-169		
166	Recognizing Unexplained Behavior in Network Traffic. *Advances in Information Security*, **2014**, 39-62	0.7	9
165	Securing Mission-Centric Operations in the Cloud **2014**, 239-259		2
164	Proof of Isolation for Cloud Storage **2014**, 95-121		1
163	Verification of data redundancy in cloud storage **2013**,		7
162	Enforcing dynamic write privileges in data outsourcing. *Computers and Security*, **2013**, 39, 47-63	4.9	24
161	Preserving privacy against external and internal threats in WSN data aggregation. *Telecommunication Systems*, **2013**, 52, 2163-2176	2.3	21
160	Integrity for join queries in the cloud. *IEEE Transactions on Cloud Computing*, **2013**, 1, 187-200	3.3	19
159	**2013**,		23

158	A Unified Framework for Measuring a Network's Mean Time-to-Compromise **2013**,		13
157	Blog or block: Detecting blog bots through behavioral biometrics. *Computer Networks*, **2013**, 57, 634-646	5.4	24
156	Quantitative survivability evaluation of three virtual machine-based server architectures. *Journal of Network and Computer Applications*, **2013**, 36, 781-790	7.9	6
155	Providing Users Anonymity in Mobile Hybrid Networks. *ACM Transactions on Internet Technology*, **2013**, 12, 1-33	3.8	12
154	Reliable mission deployment in vulnerable distributed systems **2013**,		4
153	A Logic Framework for Flexible and Security-Aware Service Composition **2013**,		3
152	On information leakage by indexes over data fragments **2013**,		8
151	Switchwall: Automated Topology Fingerprinting and Behavior Deviation Identification. *Lecture Notes in Computer Science*, **2013**, 161-176	0.9	1
150	Extending Loose Associations to Multiple Fragments. *Lecture Notes in Computer Science*, **2013**, 1-16	0.9	8
149	Rule Enforcement with Third Parties in Secure Cooperative Data Access. *Lecture Notes in Computer Science*, **2013**, 282-288	0.9	5
148	Recoverable Encryption through a Noised Secret over a Large Cloud. *Lecture Notes in Computer Science*, **2013**, 42-64	0.9	1
147	Rule Configuration Checking in Secure Cooperative Data Access **2013**, 135-149		2
146	TerraCheck: Verification of Dedicated Cloud Storage. *Lecture Notes in Computer Science*, **2013**, 113-127	0.9	
145	Secure Data Aggregation in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*, **2012**, 7, 1040-1052	8	69
144	Time-efficient and cost-effective network hardening using attack graphs **2012**,		47
143	Aggregating CVSS Base Scores for Semantics-Rich Network Security Metrics **2012**,		27
142	A Probabilistic Framework for Localization of Attackers in MANETs. *Lecture Notes in Computer Science*, **2012**, 145-162	0.9	2
141	. *IEEE Transactions on Dependable and Secure Computing*, **2012**, 9, 811-824	3.9	320

140	Trading Elephants for Ants: Efficient Post-attack Reconstitution. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, **2012**, 460-469	0.2	
139	Integrating trust management and access control in data-intensive Web applications. *ACM Transactions on the Web*, **2012**, 6, 1-43	3.2	12
138	**2012**,		33
137	Access Rule Consistency in Cooperative Data Access Environment **2012**,		5
136	Support for Write Privileges on Outsourced Data. *International Federation for Information Processing*, **2012**, 199-210		5
135	Enforcing Subscription-Based Authorization Policies in Cloud Scenarios. *Lecture Notes in Computer Science*, **2012**, 314-329	0.9	11
134	Recoverable Encryption through Noised Secret over a Large Cloud. *Lecture Notes in Computer Science*, **2012**, 13-24	0.9	1
133	Cauldron mission-centric cyber situational awareness with defense in depth **2011**,		61
132	Automatic security analysis using security metrics **2011**,		6
131	Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies. *VLDB Journal*, **2011**, 20, 541-566	3.9	94
130	Security considerations in data center configuration management **2011**,		1
129	Private data indexes for selective access to outsourced data **2011**,		10
128	Privacy of data outsourced to a cloud for selected readers through client-side encryption **2011**,		7
127	Securing Topology Maintenance Protocols for Sensor Networks. *IEEE Transactions on Dependable and Secure Computing*, **2011**, 8, 450-465	3.9	12
126	The ephemeral legion. *Communications of the ACM*, **2011**, 54, 129-131	2.5	10
125	Authorization enforcement in distributed query evaluation*. *Journal of Computer Security*, **2011**, 19, 751-794	0.8	17
124	Selective data outsourcing for enforcing privacy*. *Journal of Computer Security*, **2011**, 19, 531-566	0.8	24
123	Scalable Analysis of Attack Scenarios. *Lecture Notes in Computer Science*, **2011**, 416-433	0.9	24

122	Cooperative Data Access in Multi-cloud Environments. *Lecture Notes in Computer Science*, **2011**, 14-28	0.9	1
121	Scalable Detection of Cyber Attacks. *Communications in Computer and Information Science*, **2011**, 9-18	0.3	4
120	Combining fragmentation and encryption to protect privacy in data storage. *ACM Transactions on Information and System Security*, **2010**, 13, 1-33		116
119	Scalable Group Key Management for Secure Multicast: A Taxonomy and New Directions **2010**, 57-75		11
118	Fragments and loose associations. *Proceedings of the VLDB Endowment*, **2010**, 3, 1370-1381	3.1	28
117	Who is tweeting on Twitter **2010**,		250
116	k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks. *Lecture Notes in Computer Science*, **2010**, 573-587	0.9	40
115	Encryption policies for regulating access to outsourced data. *ACM Transactions on Database Systems*, **2010**, 35, 1-46	1.6	65
114	Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks. *IEEE Transactions on Mobile Computing*, **2010**, 9, 913-926	4.6	50
113	An Application-Level Data Transparent Authentication Scheme without Communication Overhead. *IEEE Transactions on Computers*, **2010**, 59, 943-954	2.5	3
112	Cyber SA: Situational Awareness for Cyber Defense. *Advances in Information Security*, **2010**, 3-13	0.7	58
111	Topological Vulnerability Analysis. *Advances in Information Security*, **2010**, 139-154	0.7	37
110	Tracking Skype VoIP Calls Over The Internet **2010**,		7
109	LH*RE: A Scalable Distributed Data Structure with Recoverable Encryption **2010**,		6
108	QoP and QoS Policy Cognizant Module Composition **2010**,		1
107	Providing Witness Anonymity Under Peer-to-Peer Settings. *IEEE Transactions on Information Forensics and Security*, **2010**, 5, 324-336	8	4
106	Access control for smarter healthcare using policy spaces. *Computers and Security*, **2010**, 29, 848-858	4.9	42
105	Providing Mobile Users Anonymity in Hybrid Networks. *Lecture Notes in Computer Science*, **2010**, 540-557	0.9	5

104	**2009**,		8
103	Evaluating privacy threats in released database views by symmetric indistinguishability. *Journal of Computer Security*, **2009**, 17, 5-42	0.8	1
102	Privacy-preserving robust data aggregation in wireless sensor networks. *Security and Communication Networks*, **2009**, 2, 195-213	1.9	42
101	Secure median computation in wireless sensor networks. *Ad Hoc Networks*, **2009**, 7, 1448-1462	4.8	4
100	Preserving Anonymity of Recurrent Location-Based Queries **2009**,		16
99	Privacy-Aware Proximity Based Services **2009**,		45
98	ProvidentHider: An Algorithm to Preserve Historical k-Anonymity in LBS **2009**,		13
97	Advances in Topological Vulnerability Analysis **2009**,		31
96	**2009**,		34
95	Enforcing Confidentiality Constraints on Sensitive Databases with Lightweight Trusted Clients. *Lecture Notes in Computer Science*, **2009**, 225-239	0.9	14
94	Anonymity and Historical-Anonymity in Location-Based Services. *Lecture Notes in Computer Science*, **2009**, 1-30	0.9	25
93	Privacy Preservation over Untrusted Mobile Networks. *Lecture Notes in Computer Science*, **2009**, 84-105	0.9	11
92	L-Cover: Preserving Diversity by Anonymity. *Lecture Notes in Computer Science*, **2009**, 158-171	0.9	3
91	Keep a Few: Outsourcing Data While Maintaining Confidentiality. *Lecture Notes in Computer Science* , **2009**, 440-455	0.9	48
90	Measuring network security using dynamic bayesian network **2008**,		114
89	Detecting VoIP Floods Using the Hellinger Distance. *IEEE Transactions on Parallel and Distributed Systems*, **2008**, 19, 794-805	3.7	92
88	Controlled Information Sharing in Collaborative Distributed Query Processing **2008**,		13
87	Implementing interactive analysis of attack graphs using relational databases. *Journal of Computer Security*, **2008**, 16, 419-437	0.8	15

86	Assessing query privileges via safe and efficient permission composition **2008**,		7
85	Topological Vulnerability Analysis: A Powerful New Approach For Network Attack Prevention, Detection, and Response. *Statistical Science and Interdisciplinary Research*, **2008**, 285-305		17
84	Securely computing an approximate median in wireless sensor networks **2008**,		12
83	Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs. *Journal of Network and Systems Management*, **2008**, 16, 259-275	2.1	61
82	Preserving confidentiality of security policies in data outsourcing **2008**,		21
81	Damage Quarantine and Recovery in Data Processing Systems **2008**, 383-407		
80	How Anonymous Is k-Anonymous? Look at Your Quasi-ID. *Lecture Notes in Computer Science*, **2008**, 1-15	0.9	3
79	Vulnerability-Centric Alert Correlation **2008**, 279-304		
78	Regulating Exceptions in Healthcare Using Policy Spaces. *Lecture Notes in Computer Science*, **2008**, 254-267	0.9	11
77	An Attack Graph-Based Probabilistic Security Metric. *Lecture Notes in Computer Science*, **2008**, 283-296	0.9	127
76	Fragmentation and Encryption to Enforce Privacy in Data Storage. *Lecture Notes in Computer Science*, **2007**, 171-186	0.9	48
75	Information disclosure under realistic assumptions **2007**,		37
74	Chaining watermarks for detecting malicious modifications to streaming data. *Information Sciences*, **2007**, 177, 281-298	7.7	49
73	Anonymity and Diversity in LBS: A Preliminary Investigation **2007**,		6
72	A data outsourcing architecture combining cryptography and access control **2007**,		57
71	Trust management services in relational databases **2007**,		6
70	Trusted Recovery. *Advances in Information Security*, **2007**, 59-94	0.7	3
69	Efficient Distributed Detection of Node Replication Attacks in Sensor Networks **2007**,		42

68	Toward measuring network security using attack graphs **2007**,		68
67	Can-Follow Concurrency Control. *IEEE Transactions on Computers*, **2007**, 56, 1425-1430	2.5	2
66	Measuring the Overall Security of Network Configurations Using Attack Graphs. *Lecture Notes in Computer Science*, **2007**, 98-112	0.9	58
65	Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts. *Computer Communications*, **2006**, 29, 2917-2933	5.1	120
64	A weakest-adversary security metric for network configuration security analysis **2006**,		80
63	Attack-resilient hierarchical data aggregation in sensor networks **2006**,		27
62	Redirection policies for mission-based information sharing **2006**,		3
61	LEAP+. *ACM Transactions on Sensor Networks*, **2006**, 2, 500-528	2.9	327
60	V-COPS: A Vulnerability-Based Cooperative Alert Distribution System. *Proceedings of the Computer Security Applications Conference*, **2006**,		1
59	Fast Detection of Denial-of-Service Attacks on IP Telephony. *IEEE International Workshop on Quality of Service*, **2006**,		27
58	Looking into the seeds of time: Discovering temporal patterns in large transaction sets. *Information Sciences*, **2006**, 176, 1003-1031	7.7	17
57	A fragile watermarking scheme for detecting malicious modifications of database relations. *Information Sciences*, **2006**, 176, 1350-1378	7.7	60
56	Unauthorized inferences in semistructured databases. *Information Sciences*, **2006**, 176, 3269-3299	7.7	6
55	Minimum-cost network hardening using attack graphs. *Computer Communications*, **2006**, 29, 3812-3824	5.1	156
54	Data warehousing and data mining techniques for intrusion detection systems. *Distributed and Parallel Databases*, **2006**, 20, 149-166	0.9	18
53	Modeling and assessing inference exposure in encrypted databases. *ACM Transactions on Information and System Security*, **2005**, 8, 119-152		90
52	Topological Analysis of Network Attack Vulnerability **2005**, 247-266		105
51	Policies, Models, and Languages for Access Control. *Lecture Notes in Computer Science*, **2005**, 225-237	0.9	23

50	Key management for multi-user encrypted databases **2005**,		48
49	A Hierarchical Release Control Policy Framework **2005**, 121-137		
48	Protecting Privacy Against Location-Based Personal Identification. *Lecture Notes in Computer Science*, **2005**, 185-199	0.9	160
47	An Efficient and Unified Approach to Correlating, Hypothesizing, and Predicting Intrusion Alerts. *Lecture Notes in Computer Science*, **2005**, 247-266	0.9	18
46	Cardinality-based inference control in data cubes*. *Journal of Computer Security*, **2004**, 12, 655-692	0.8	28
45	Managing attack graph complexity through visual hierarchical aggregation **2004**,		131
44	Reasoning with advanced policy rules and its application to access control. *International Journal on Digital Libraries*, **2004**, 4, 156-170	1.4	1
43	A logic-based framework for attribute based access control **2004**,		145
42	Enabling the sharing of neuroimaging data through well-defined intermediate levels of visibility. *NeuroImage*, **2004**, 22, 1646-56	7.9	12
41	A Flexible Authorization Framework for E-Commerce. *Lecture Notes in Computer Science*, **2004**, 336-345	0.9	
40	Balancing confidentiality and efficiency in untrusted relational DBMSs **2003**,		129
39	A checksum-based corruption detection technique1. *Journal of Computer Security*, **2003**, 11, 315-329	0.8	1
38	Provisions and Obligations in Policy Rule Management. *Journal of Network and Systems Management*, **2003**, 11, 351-372	2.1	38
37	Discovering calendar-based temporal association rules. *Data and Knowledge Engineering*, **2003**, 44, 193-218	1.3	87
36	Design and implementation of a decentralized prototype system for detecting distributed attacks. *Computer Communications*, **2002**, 25, 1374-1391	5.1	8
35	Solving multi-granularity temporal constraint networks. *Artificial Intelligence*, **2002**, 140, 107-152	3.6	32
34	Temporal Reasoning in Workflow Systems. *Distributed and Parallel Databases*, **2002**, 11, 269-306	0.9	64
33	An Algebraic Representation of Calendars. *Annals of Mathematics and Artificial Intelligence*, **2002**, 36, 5-38	0.8	38

32	The inference problem. *SIGKDD Explorations: Newsletter of the Special Interest Group (SIG) on Knowledge Discovery & Data Mining*, **2002**, 4, 6-11	4.6	155
31	Provisions and Obligations in Policy Management and Security Applications **2002**, 502-513		52
30	An Architecture for Anomaly Detection. *Advances in Information Security*, **2002**, 63-76	0.7	6
29	ADAM. *SIGMOD Record*, **2001**, 30, 15-24	1.1	140
28	Detecting Novel Network Intrusions Using Bayes Estimators **2001**,		127
27	Flexible support for multiple access control policies. *ACM Transactions on Database Systems*, **2001**, 26, 214-260	1.6	382
26	Abstraction-based intrusion detection in distributed environments. *ACM Transactions on Information and System Security*, **2001**, 4, 407-452		38
25	Multilevel secure transaction processing1. *Journal of Computer Security*, **2001**, 9, 165-195	0.8	2
24	Provisional Authorizations. *Advances in Information Security*, **2001**, 133-159	0.7	36
23	Rewriting Histories: Recovering from Malicious Transactions. *Distributed and Parallel Databases*, **2000**, 8, 7-40	0.9	55
22	Flexible Transaction Dependencies in Database Systems. *Distributed and Parallel Databases*, **2000**, 8, 399-446	0.9	2
21	Intrusion confinement by isolation in information systems. *Journal of Computer Security*, **2000**, 8, 243-279	0.8	14
20	Time Granularities in Databases, Data Mining, and Temporal Reasoning **2000**,		111
19	A general framework for time granularity and its application to temporal reasoning. *Annals of Mathematics and Artificial Intelligence*, **1998**, 22, 29-58	0.8	43
18	Exploring steganography: Seeing the unseen. *Computer*, **1998**, 31, 26-34	1.6	537
17	TEMPORAL MEDIATORS: SUPPORTING UNIFORM ACCESSES TO HETEROGENEOUS TEMPORAL INFORMATION. *International Journal on Artificial Intelligence Tools*, **1998**, 07, 319-339	0.9	1
16	A semantic-based transaction processing model for multilevel transactions1. *Journal of Computer Security*, **1998**, 6, 181-217	0.8	3
15	Logical design for temporal databases with multiple granularities. *ACM Transactions on Database Systems*, **1997**, 22, 115-170	1.6	68

14	A unified framework for enforcing multiple access control policies. *SIGMOD Record*, **1997**, 26, 474-485	1.1	26
13	A unified framework for enforcing multiple access control policies **1997**,		122
12	Database security and privacy. *ACM Computing Surveys*, **1996**, 28, 129-131	13.4	14
11	Managing security and privacy of information. *ACM Computing Surveys*, **1996**, 28, 79	13.4	3
10	Semantic assumptions and query evaluation in temporal databases. *SIGMOD Record*, **1995**, 24, 257-268	1.1	
9	Achieving Stricter Correctness Requirements in Multilevel Secure Database Management Systems*. *Journal of Computer Security*, **1993**, 2, 311-351	0.8	1
8	Toward a multilevel secure relational data model. *SIGMOD Record*, **1991**, 20, 50-59	1.1	21
7	Multiple coordinated views for network attack graphs		15
6	Efficient minimum-cost network hardening via exploit dependency graphs		70
5	Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach		7
4	Efficient Distributed Detection of Node Replication Attacks in Sensor Networks		6
3	An authorization model for query execution in the cloud. *VLDB Journal*,1	3.9	0
2	Maintaining the level of operational effectiveness of a CSOC under adverse conditions. *International Journal of Information Security*,1	2.8	
1	Intrusion-Detection Systems403-420		