

Mauro Conti

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4125270/publications.pdf>

Version: 2024-02-01

418
papers

14,116
citations

38742

50
h-index

40979

93
g-index

434
all docs

434
docs citations

434
times ranked

10079
citing authors

#	ARTICLE	IF	CITATIONS
1	Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain. IEEE Transactions on Dependable and Secure Computing, 2023, 20, 225-241.	5.4	19
2	Comparing the Impact of Social Media Regulations on News Consumption. IEEE Transactions on Computational Social Systems, 2023, 10, 1252-1262.	4.4	6
3	Adaptive Intrusion Detection in Edge Computing Using Cerebellar Model Articulation Controller and Spline Fit. IEEE Transactions on Services Computing, 2023, 16, 900-912.	4.6	2
4	Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. ACM Computing Surveys, 2023, 55, 1-36.	23.0	19
5	SEnD: A Social Network Friendship Enhanced Decentralized System to Circumvent Censorships. IEEE Transactions on Services Computing, 2022, 15, 346-360.	4.6	1
6	Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things. IEEE Internet of Things Journal, 2022, 9, 14203-14215.	8.7	28
7	Covert Channel-Based Transmitter Authentication in Controller Area Networks. IEEE Transactions on Dependable and Secure Computing, 2022, 19, 2665-2679.	5.4	4
8	DHACS: Smart Contract-Based Decentralized Hybrid Access Control for Industrial Internet-of-Things. IEEE Transactions on Industrial Informatics, 2022, 18, 3452-3461.	11.3	16
9	Invoice #31415 attached: Automated analysis of malicious Microsoft Office documents. Computers and Security, 2022, 114, 102582.	6.0	9
10	AutoSec: Secure Automotive Data Transmission Scheme for In-Vehicle Networks. , 2022, , .		4
11	Quantifying Location Privacy for Navigation Services in Sustainable Vehicular Networks. IEEE Transactions on Green Communications and Networking, 2022, 6, 1267-1275.	5.5	6
12	Modern Authentication Schemes in Smartphones and IoT Devices: An Empirical Survey. IEEE Internet of Things Journal, 2022, 9, 7639-7663.	8.7	4
13	The Rise of ICS Malware: A Comparative Analysis. Lecture Notes in Computer Science, 2022, , 496-511.	1.3	0
14	A machine learning-based approach to detect threats in bio-cyber DNA storage systems. Computer Communications, 2022, 187, 59-70.	5.1	2
15	SETCAP: Service-Based Energy-Efficient Temporal Credential Authentication Protocol for Internet of Drones. Computer Networks, 2022, 206, 108804.	5.1	7
16	Effect of DIS Attack on 6TiSCH Network Formation. IEEE Communications Letters, 2022, 26, 1190-1193.	4.1	11
17	Demystifying the Transferability of Adversarial Attacks in Computer Networks. IEEE Transactions on Network and Service Management, 2022, 19, 3387-3400.	4.9	15
18	Misinformation Detection on Social Media: Challenges and the Road Ahead. IT Professional, 2022, 24, 34-40.	1.5	5

#	ARTICLE	IF	CITATIONS
19	User-Defined Privacy-Preserving Traffic Monitoring Against n-by-1 Jamming Attack. IEEE/ACM Transactions on Networking, 2022, 30, 2060-2073.	3.8	10
20	Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. IEEE Access, 2022, 10, 25464-25493.	4.2	36
21	Formal model for inter-component communication and its security in android. Computing (Vienna/New York), 2022, 104, 1839-1865.	4.8	3
22	A survey on security challenges and solutions in the IOTA. Journal of Network and Computer Applications, 2022, 203, 103383.	9.1	31
23	Should I Mine or Should I Break: On the Worthiness of Brute-Forcing Cryptocurrency Addresses. , 2022, , .		0
24	Privacy-Friendly De-authentication with BLUFADE: Blurred Face Detection. , 2022, , .		2
25	What you see is not what you get. , 2022, , .		0
26	A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. Journal of Network and Computer Applications, 2022, 204, 103414.	9.1	17
27	A survey and taxonomy of consensus protocols for blockchains. Journal of Systems Architecture, 2022, 127, 102503.	4.3	24
28	Software defined network-based HTTP flooding attack defender. Computers and Electrical Engineering, 2022, 101, 108019.	4.8	4
29	COVID-19 infodemic on Facebook and containment measures in Italy, United Kingdom and New Zealand. PLoS ONE, 2022, 17, e0267022.	2.5	7
30	SENECAN: Secure KEy Distribution OvEr CAN Through Watermarking and Jamming. IEEE Transactions on Dependable and Secure Computing, 2022, , 1-1.	5.4	1
31	A PLS-HECC-based device authentication and key agreement scheme for smart home networks. Computer Networks, 2022, 216, 109077.	5.1	6
32	Do not let Next-Intent Vulnerability be your next nightmare: type system-based approach to detect it in Android apps. International Journal of Information Security, 2021, 20, 39-58.	3.4	8
33	ChoKIFA+: an early detection and mitigation approach against interest flooding attacks in NDN. International Journal of Information Security, 2021, 20, 269-285.	3.4	10
34	Defeating Lattice-Based Data Hiding Code Via Decoding Security Hole. IEEE Transactions on Circuits and Systems for Video Technology, 2021, 31, 76-87.	8.3	7
35	Truck platoon security: State-of-the-art and road ahead. Computer Networks, 2021, 185, 107658.	5.1	22
36	LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Generation Computer Systems, 2021, 115, 406-420.	7.5	68

#	ARTICLE	IF	CITATIONS
37	SPO: A Secure and Performance-aware Optimization for MapReduce Scheduling. Journal of Network and Computer Applications, 2021, 176, 102944.	9.1	11
38	AEGIS: Detection and Mitigation of TCP SYN Flood on SDN Controller. IEEE Transactions on Network and Service Management, 2021, 18, 745-759.	4.9	18
39	Editorial: Special issue on trusted Cloud-Edges computations. Future Generation Computer Systems, 2021, 114, 661-664.	7.5	0
40	Privacy for 5G-Supported Vehicular Networks. IEEE Open Journal of the Communications Society, 2021, 2, 1935-1956.	6.9	4
41	Introduction to the Special Issue on Security and Privacy for Connected Cyber-physical Systems. ACM Transactions on Cyber-Physical Systems, 2021, 5, 1-2.	2.5	1
42	Cyber Forensics for CPS. , 2021, , 1-3.		1
43	TEL: Low-Latency Failover Traffic Engineering in Data Plane. IEEE Transactions on Network and Service Management, 2021, 18, 4697-4710.	4.9	9
44	A Survey on Industrial Control System Testbeds and Datasets for Security Research. IEEE Communications Surveys and Tutorials, 2021, 23, 2248-2294.	39.4	70
45	Anonymous and Verifiable Reputation System for E-Commerce Platforms Based on Blockchain. IEEE Transactions on Network and Service Management, 2021, 18, 4434-4449.	4.9	26
46	Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review, 2021, 39, 100332.	15.3	34
47	Editorial for the Special Issue on Sustainable Cyber Forensics and Threat Intelligence. IEEE Transactions on Sustainable Computing, 2021, 6, 182-183.	3.1	0
48	Contact Tracing Made Un-relay-able. , 2021, , .		8
49	Improving Password Guessing via Representation Learning. , 2021, , .		23
50	A threat model method for ICS malware. , 2021, , .		10
51	An SDN-based framework for QoS routing in internet of underwater things. Telecommunication Systems, 2021, 78, 253-266.	2.5	14
52	Looking Through Walls: Inferring Scenes from Video-Surveillance Encrypted Traffic. , 2021, , .		0
53	FADIA. , 2021, , .		5
54	USB powered devices: A survey of side-channel threats and countermeasures. High-Confidence Computing, 2021, 1, 100007.	3.7	9

#	ARTICLE	IF	CITATIONS
55	A holistic approach to power efficiency in a clock offset based Intrusion Detection Systems for Controller Area Networks. Pervasive and Mobile Computing, 2021, 73, 101385.	3.3	7
56	DETONAR: Detection of Routing Attacks in RPL-Based IoT. IEEE Transactions on Network and Service Management, 2021, 18, 1178-1190.	4.9	50
57	It's a Matter of Style: Detecting Social Bots through Writing Style Consistency. , 2021, , .		2
58	Vulnerabilities in Android webview objects: Still not the end!. Computers and Security, 2021, 109, 102395.	6.0	5
59	Assessing the Use of Insecure ICS Protocols via IXP Network Traffic Analysis. , 2021, , .		7
60	Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Generation Computer Systems, 2021, 120, 13-25.	7.5	53
61	ICN PATTA: ICN Privacy Attack Through Traffic Analysis. , 2021, , .		1
62	BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. Computer Communications, 2021, 180, 31-47.	5.1	57
63	5G Security Challenges and Solutions: A Review by OSI Layers. IEEE Access, 2021, 9, 116294-116314.	4.2	28
64	Online Advertising Security: Issues, Taxonomy, and Future Directions. IEEE Communications Surveys and Tutorials, 2021, 23, 2494-2524.	39.4	9
65	Practical Exchange for Unique Digital Goods. , 2021, , .		1
66	COTS Drone Detection using Video Streaming Characteristics. , 2021, , .		6
67	Fall of Giants: How popular text-based MLaaS fall against a simple evasion attack. , 2021, , .		7
68	On the feasibility of crawling-based attacks against recommender systems. Journal of Computer Security, 2021, , 1-23.	0.8	0
69	Where to Meet a Driver Privately: Recommending Pick-Up Locations for Ride-Hailing Services. Lecture Notes in Computer Science, 2021, , 43-61.	1.3	1
70	Repack Me If You Can: An Anti-Repackaging Solution Based on Android Virtualization. , 2021, , .		2
71	Towards An Enhanced Reputation System for IOTA's Coordicide. , 2021, , .		2
72	A Novel Stealthy Attack to Gather SDN Configuration-Information. IEEE Transactions on Emerging Topics in Computing, 2020, 8, 328-340.	4.6	10

#	ARTICLE	IF	CITATIONS
73	Privacy Aware Data Deduplication for Side Channel in Cloud Storage. IEEE Transactions on Cloud Computing, 2020, 8, 597-609.	4.4	17
74	A Realistic Model for Failure Propagation in Interdependent Cyber-Physical Systems. IEEE Transactions on Network Science and Engineering, 2020, 7, 817-831.	6.4	34
75	TARE: Topology Adaptive Re-keying scheme for secure group communication in IoT networks. Wireless Networks, 2020, 26, 2449-2463.	3.0	13
76	Context-based Co-presence detection techniques: A survey. Computers and Security, 2020, 88, 101652.	6.0	8
77	A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions. ACM Computing Surveys, 2020, 52, 1-38.	23.0	41
78	BAS-VAS: A Novel Secure Protocol for Value Added Service Delivery to Mobile Devices. IEEE Transactions on Information Forensics and Security, 2020, 15, 1470-1485.	6.9	4
79	<i>PermPair</i>: Android Malware Detection Using Permission Pairs. IEEE Transactions on Information Forensics and Security, 2020, 15, 1968-1982.	6.9	97
80	Cryptomining Cannot Change Its Spots: Detecting Covert Cryptomining Using Magnetic Side-Channel. IEEE Transactions on Information Forensics and Security, 2020, 15, 1630-1639.	6.9	11
81	Security and design requirements for software-defined VANETs. Computer Networks, 2020, 169, 107099.	5.1	35
82	Deep and broad URL feature mining for android malware detection. Information Sciences, 2020, 513, 600-613.	6.9	40
83	Attestation-enabled secure and scalable routing protocol for IoT networks. Ad Hoc Networks, 2020, 98, 102054.	5.5	28
84	Similarity-based Android malware detection using Hamming distance of static binary features. Future Generation Computer Systems, 2020, 105, 230-247.	7.5	120
85	Security issues and challenges in V2X: A Survey. Computer Networks, 2020, 169, 107093.	5.1	117
86	STRIDE: Scalable and Secure Over-The-Air Software Update Scheme for Autonomous Vehicles. , 2020, , .		11
87	SHeFU: Secure Hardware-Enabled Protocol for Firmware Updates. , 2020, , .		3
88	TAMBUS: A novel authentication method through covert channels for securing industrial networks. Computer Networks, 2020, 183, 107583.	5.1	8
89	Collective Remote Attestation at the Internet of Things Scale: State-of-the-Art and Future Challenges. IEEE Communications Surveys and Tutorials, 2020, 22, 2447-2461.	39.4	35
90	Eathentication: A Chewing-based Authentication Method. , 2020, , .		1

#	ARTICLE	IF	CITATIONS
91	TMaR: a two-stage MapReduce scheduler for heterogeneous environments. Human-centric Computing and Information Sciences, 2020, 10, .	6.1	4
92	Private Blockchain in Industrial IoT. IEEE Network, 2020, 34, 76-77.	6.9	13
93	Privacy-preserving Navigation Supporting Similar Queries in Vehicular Networks. IEEE Transactions on Dependable and Secure Computing, 2020, , 1-1.	5.4	17
94	UAVs Path Deviation Attacks: Survey and Research Challenges. , 2020, , .		7
95	Proof of Evolution: leveraging blockchain mining for a cooperative execution of Genetic Algorithms. , 2020, , .		10
96	Detection of algorithmically-generated domains: An adversarial machine learning approach. Computer Communications, 2020, 160, 661-673.	5.1	17
97	Secure over-the-air software updates in connected vehicles: A survey. Computer Networks, 2020, 178, 107343.	5.1	64
98	A Proactive Cache Privacy Attack on NDN. , 2020, , .		6
99	The Road Ahead for Networking: A Survey on ICN-IP Coexistence Solutions. IEEE Communications Surveys and Tutorials, 2020, 22, 2104-2129.	39.4	20
100	BitProb: Probabilistic Bit Signatures for Accurate Application Identification. IEEE Transactions on Network and Service Management, 2020, 17, 1730-1741.	4.9	13
101	On defending against label flipping attacks on malware detection systems. Neural Computing and Applications, 2020, 32, 14781-14800.	5.6	37
102	Can machine learning model with static features be fooled: an adversarial machine learning approach. Cluster Computing, 2020, 23, 3233-3253.	5.0	19
103	SPARK: Secure Pseudorandom Key-based Encryption for Deduplicated Storage. Computer Communications, 2020, 154, 148-159.	5.1	1
104	Blockchain-Enabled Secure Energy Trading With Verifiable Fairness in Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2020, 16, 6564-6574.	11.3	115
105	DISPERSE: A Decentralized Architecture for Content Replication Resilient to Node Failures. IEEE Transactions on Network and Service Management, 2020, 17, 201-212.	4.9	0
106	Machine Learning for Web Vulnerability Detection: The Case of Cross-Site Request Forgery. IEEE Security and Privacy, 2020, 18, 8-16.	1.2	14
107	LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks. Computers and Security, 2020, 94, 101849.	6.0	49
108	SARA: Secure Asynchronous Remote Attestation for IoT Systems. IEEE Transactions on Information Forensics and Security, 2020, 15, 3123-3136.	6.9	41

#	ARTICLE	IF	CITATIONS
109	NC based DAS-NDN: Network Coding for robust Dynamic Adaptive Streaming over NDN. Computer Networks, 2020, 174, 107222.	5.1	2
110	One-Time, Oblivious, and Unlinkable Query Processing Over Encrypted Data on Cloud. Lecture Notes in Computer Science, 2020, , 350-365.	1.3	8
111	Effectiveness of state-of-the-art dynamic analysis techniques in identifying diverse Android malware and future enhancements. Advances in Computers, 2020, , 73-120.	1.6	10
112	A robust multicast communication protocol for Low power and Lossy networks. Journal of Network and Computer Applications, 2020, 164, 102675.	9.1	8
113	A Multilabel Fuzzy Relevance Clustering System for Malware Attack Attribution in the Edge Layer of Cyber-Physical Networks. ACM Transactions on Cyber-Physical Systems, 2020, 4, 1-22.	2.5	22
114	Peek-a-boo. , 2020, , .		118
115	Big Enough to Care Not Enough to Scare! Crawling to Attack Recommender Systems. Lecture Notes in Computer Science, 2020, , 165-184.	1.3	1
116	ALISI. , 2020, , .		0
117	PvP: Profiling Versus Player! Exploiting Gaming Data for Player Recognition. Lecture Notes in Computer Science, 2020, , 393-408.	1.3	3
118	Reputation-based Trust: A robust mechanism for Dynamic Adaptive Streaming over Named Data Networking. , 2020, , .		0
119	Predicting Twitter Users' Political Orientation: An Application to the Italian Political Scenario. , 2020, , .		1
120	Detecting Covert Cryptomining Using HPC. Lecture Notes in Computer Science, 2020, , 344-364.	1.3	11
121	COIDS. , 2020, , .		13
122	Your PIN Sounds Good! Augmentation of PIN Guessing Strategies via Audio Leakage. Lecture Notes in Computer Science, 2020, , 720-735.	1.3	2
123	DE-auth of the Blue! Transparent De-authentication Using Bluetooth Low Energy Beacon. Lecture Notes in Computer Science, 2020, , 277-294.	1.3	3
124	Crypto-Wills: Transferring Digital Assets by Maintaining Wills on the Blockchain. Lecture Notes in Networks and Systems, 2020, , 407-416.	0.7	3
125	Spatial bloom filter in named data networking. , 2020, , .		4
126	ASAIN. , 2020, , .		7

#	ARTICLE	IF	CITATIONS
127	A Statistical Analysis Framework for ICS Process Datasets. , 2020, , .		7
128	A Survey on Homomorphic Encryption Schemes. ACM Computing Surveys, 2019, 51, 1-35.	23.0	544
129	Fast multi-hop broadcast of alert messages in VANETs: An analytical model. Ad Hoc Networks, 2019, 82, 126-133.	5.5	19
130	FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments. Journal of Parallel and Distributed Computing, 2019, 132, 274-283.	4.1	160
131	LiMCA: an optimal clustering algorithm for lifetime maximization of internet of things. Wireless Networks, 2019, 25, 4459-4477.	3.0	22
132	Guest Editorial Special Issue on Security and Forensics of Internet of Things: Problems and Solutions. IEEE Internet of Things Journal, 2019, 6, 6363-6367.	8.7	0
133	A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. Journal of Computer Virology and Hacking Techniques, 2019, 15, 277-305.	2.2	64
134	Evaluation of Machine Learning Algorithms for Anomaly Detection in Industrial Networks. , 2019, , .		23
135	DNA Molecular Storage System: Transferring Digitally Encoded Information through Bacterial Nanonetworks. IEEE Transactions on Emerging Topics in Computing, 2019, , 1-1.	4.6	12
136	SYNâ€Guard: An effective counter for SYN flooding attack in softwareâ€defined networking. International Journal of Communication Systems, 2019, 32, e4061.	2.5	14
137	PILOT: Password and PIN information leakage from obfuscated typing videos1. Journal of Computer Security, 2019, 27, 405-425.	0.8	7
138	ECCAuth: A Secure Authentication Protocol for Demand Response Management in a Smart Grid System. IEEE Transactions on Industrial Informatics, 2019, 15, 6572-6582.	11.3	79
139	SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. Future Generation Computer Systems, 2019, 101, 621-634.	7.5	67
140	A New Secure Data Dissemination Model in Internet of Drones. , 2019, , .		45
141	Joint failure recovery, fault prevention, and energy-efficient resource management for real-time SFC in fog-supported SDN. Computer Networks, 2019, 162, 106850.	5.1	32
142	On the Exploitation of Online SMS Receiving Services to Forge ID Verification. , 2019, , .		3
143	KingFisher. , 2019, , .		4
144	On the Resilience of Network-based Moving Target Defense Techniques Against Host Profiling Attacks. , 2019, , .		2

#	ARTICLE	IF	CITATIONS
145	PAKIT: Proactive Authentication and Key Agreement Protocol for Internet of Things. , 2019, , .		6
146	RADIS: Remote Attestation of Distributed IoT Services. , 2019, , .		16
147	SHeLA: Scalable Heterogeneous Layered Attestation. IEEE Internet of Things Journal, 2019, 6, 10240-10250.	8.7	19
148	AMON. , 2019, , .		3
149	Detecting ADS-B Spoofing Attacks Using Deep Neural Networks. , 2019, , .		33
150	Mitch: A Machine Learning Approach to the Black-Box Detection of CSRF Vulnerabilities. , 2019, , .		18
151	BlockAuth: Blockchain based distributed producer authentication in ICN. Computer Networks, 2019, 164, 106888.	5.1	23
152	Threat is in the Air. , 2019, , .		9
153	MapReduce: an infrastructure review and research insights. Journal of Supercomputing, 2019, 75, 6934-7002.	3.6	18
154	TACAN. , 2019, , .		33
155	Mind your wallet's privacy. , 2019, , .		22
156	Identification of Android malware using refined system calls. Concurrency Computation Practice and Experience, 2019, 31, e5311.	2.2	7
157	Lightweight solutions to counter DDoS attacks in software defined networking. Wireless Networks, 2019, 25, 2751-2768.	3.0	35
158	Don't hesitate to share!. , 2019, , .		0
159	Efficient physical intrusion detection in Internet of Things: A Node deployment approach. Computer Networks, 2019, 154, 28-46.	5.1	15
160	Efficient privacy preserving device authentication in WBANs for industrial e-health applications. Computers and Security, 2019, 83, 300-312.	6.0	30
161	Towards privacy preserving unstructured big data publishing. Journal of Intelligent and Fuzzy Systems, 2019, 36, 3471-3482.	1.4	11
162	Key Management Systems for Smart Grid Advanced Metering Infrastructure: A Survey. IEEE Communications Surveys and Tutorials, 2019, 21, 2831-2848.	39.4	171

#	ARTICLE	IF	CITATIONS
163	Analysis and classification of context-based malware behavior. Computer Communications, 2019, 136, 76-90.	5.1	44
164	Remote Attestation as a Service for IoT. , 2019, , .		3
165	SACHa: Self-Attestation of Configurable Hardware. , 2019, , .		11
166	An In-depth Look Into SDN Topology Discovery Mechanisms. , 2019, , .		26
167	Special Issue on Big Data Applications in Cyber Security and Threat Intelligence “ Part 2. IEEE Transactions on Big Data, 2019, 5, 423-424.	6.1	1
168	Special Issue on Big Data Applications in Cyber Security and Threat Intelligence “ Part 1. IEEE Transactions on Big Data, 2019, 5, 279-281.	6.1	4
169	SoFA: A Spark-oriented Fog Architecture. , 2019, , .		11
170	DISC: A Novel Distributed On-Demand Clustering Protocol for Internet of Multimedia Things. , 2019, , .		2
171	MimePot: a Model-based Honeypot for Industrial Control Networks. , 2019, , .		14
172	LISA: Lightweight context-aware IoT service architecture. Journal of Cleaner Production, 2019, 212, 1345-1356.	9.3	41
173	SAND: Social-aware, network-failure resilient, and decentralized microblogging system. Future Generation Computer Systems, 2019, 93, 637-650.	7.5	4
174	Intelligent conditional collaborative private data sharing. Future Generation Computer Systems, 2019, 96, 1-10.	7.5	2
175	AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones. Journal of Information Security and Applications, 2019, 44, 89-103.	2.5	42
176	You click, I steal: analyzing and detecting click hijacking attacks in web pages. International Journal of Information Security, 2019, 18, 481-504.	3.4	6
177	A machine learning based approach to detect malicious android apps using discriminant system calls. Future Generation Computer Systems, 2019, 94, 333-350.	7.5	50
178	CENSOR: Cloud-enabled secure IoT architecture over SDN paradigm. Concurrency Computation Practice and Experience, 2019, 31, e4978.	2.2	22
179	Mobility-aware cross-layer routing for peer-to-peer networks. Computers and Electrical Engineering, 2019, 73, 209-226.	4.8	7
180	Wide-Scale Internet Disconnection: Impact and Recovery on Social-Based P2P Overlays. IEEE Transactions on Network Science and Engineering, 2019, 6, 734-747.	6.4	2

#	ARTICLE	IF	CITATIONS
181	Software defined service function chaining with failure consideration for fog computing. Concurrency Computation Practice and Experience, 2019, 31, e4953.	2.2	8
182	Privacy-Aware Caching in Information-Centric Networking. IEEE Transactions on Dependable and Secure Computing, 2019, 16, 313-328.	5.4	25
183	The Online Identity Detection via Keyboard Dynamics. Advances in Intelligent Systems and Computing, 2019, , 342-357.	0.6	5
184	ChoKIFA: A New Detection and Mitigation Approach Against Interest Flooding Attacks in NDN. Lecture Notes in Computer Science, 2019, , 53-65.	1.3	9
185	Blockchain Trilemma Solver Algorand has Dilemma over Undecidable Messages. , 2019, , .		15
186	Skype & Type. ACM Transactions on Privacy and Security, 2019, 22, 1-34.	3.0	10
187	CoMon-DAS: A Framework for Efficient and Robust Dynamic Adaptive Streaming over NDN. , 2019, , .		2
188	IoT-enabled smart lighting systems for smart cities. , 2018, , .		57
189	Advertising in the IoT Era: Vision and Challenges. IEEE Communications Magazine, 2018, 56, 138-144.	6.1	75
190	Detecting Android Malware Leveraging Text Semantics of Network Flows. IEEE Transactions on Information Forensics and Security, 2018, 13, 1096-1109.	6.9	106
191	Security and Privacy Analysis of National Science Foundation Future Internet Architectures. IEEE Communications Surveys and Tutorials, 2018, 20, 1418-1442.	39.4	24
192	Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks. IEEE Transactions on Dependable and Secure Computing, 2018, 15, 959-973.	5.4	49
193	MDSClone: Multidimensional Scaling Aided Clone Detection in Internet of Things. IEEE Transactions on Information Forensics and Security, 2018, 13, 2031-2046.	6.9	16
194	DELTA: Data Extraction and Logging Tool for Android. IEEE Transactions on Mobile Computing, 2018, 17, 1289-1302.	5.8	13
195	Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. IEEE Internet of Things Journal, 2018, 5, 269-282.	8.7	298
196	Whac-A-Mole: Smart node positioning in clone attack in wireless sensor networks. Computer Communications, 2018, 119, 66-82.	5.1	10
197	Covert lie detection using keyboard dynamics. Scientific Reports, 2018, 8, 1976.	3.3	31
198	The insider on the outside: a novel system for the detection of information leakers in social networks. European Journal of Information Systems, 2018, 27, 470-485.	9.2	3

#	ARTICLE	IF	CITATIONS
199	Unraveling Reflection Induced Sensitive Leaks in Android Apps. Lecture Notes in Computer Science, 2018, , 49-65.	1.3	0
200	The position cheating attack on inter-vehicular online gaming. , 2018, , .		2
201	Enhancing QoE for video streaming in MANETs via multi-constraint routing. Wireless Networks, 2018, 24, 235-256.	3.0	15
202	A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment. IEEE Journal of Biomedical and Health Informatics, 2018, 22, 1299-1309.	6.3	119
203	A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future Generation Computer Systems, 2018, 84, 200-215.	7.5	114
204	Detecting crypto-ransomware in IoT networks based on energy consumption footprint. Journal of Ambient Intelligence and Humanized Computing, 2018, 9, 1141-1152.	4.9	190
205	You Are How You Play: Authenticating Mobile Users via Game Playing. Lecture Notes in Electrical Engineering, 2018, , 79-96.	0.4	1
206	An efficient routing protocol for the QoS support of large-scale MANETs. International Journal of Communication Systems, 2018, 31, e3384.	2.5	31
207	Robust Smartphone App Identification via Encrypted Network Traffic Analysis. IEEE Transactions on Information Forensics and Security, 2018, 13, 63-78.	6.9	227
208	Deep and Broad Learning Based Detection of Android Malware via Network Traffic. , 2018, , .		16
209	IaaS-Aided Access Control for Information-Centric IoT. , 2018, , .		1
210	GATE and FENCE: Geo-Blocking Protocols for Named Data Networking. , 2018, , .		0
211	AppHunter: Mobile Application Traffic Classification. , 2018, , .		2
212	Optimizing Message Ferry Scheduling in a DTN. , 2018, , .		6
213	SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things. , 2018, , .		24
214	Distributed Services Attestation in IoT. Lecture Notes in Computer Science, 2018, , 261-273.	1.3	6
215	A Novel Architecture for Cyber-Physical Security in Industrial Control Networks. , 2018, , .		5
216	All You Need is "Love". , 2018, , .		108

#	ARTICLE	IF	CITATIONS
217	QoE Degradation Attack in Dynamic Adaptive Streaming Over ICN. , 2018, , .		4
218	On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. Computers and Security, 2018, 79, 162-189.	6.0	78
219	PADS: Practical Attestation for Highly Dynamic Swarm Topologies. , 2018, , .		29
220	OSSINT - Open Source Social Network Intelligence. Online Social Networks and Media, 2018, 6, 58-68.	3.6	4
221	Leaky CPS. , 2018, , .		1
222	RARE: Defeating side channels based on data-deduplication in cloud storage. , 2018, , .		35
223	SAFETY: Early Detection and Mitigation of TCP SYN Flood Utilizing Entropy in SDN. IEEE Transactions on Network and Service Management, 2018, 15, 1545-1559.	4.9	127
224	Fair-RTT-DAS: A robust and efficient dynamic adaptive streaming over ICN. Computer Communications, 2018, 129, 209-225.	5.1	7
225	Scheduling Distributed Energy Resource Operation and Daily Power Consumption for a Smart Building to Optimize Economic and Environmental Parameters. Energies, 2018, 11, 1348.	3.1	39
226	Computational Intelligence Approaches for Energy Load Forecasting in Smart Energy Management Grids: State of the Art, Future Challenges, and Research Directions. Energies, 2018, 11, 596.	3.1	178
227	Cyber Threat Intelligence: Challenges and Opportunities. Advances in Information Security, 2018, , 1-6.	1.2	57
228	SCloT: A Secure and sCalable End-to-End Management Framework for IoT Devices. Lecture Notes in Computer Science, 2018, , 595-617.	1.3	4
229	A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys and Tutorials, 2018, 20, 3416-3452.	39.4	615
230	The Dark Side(-Channel) of Mobile Devices: A Survey on Network Traffic Analysis. IEEE Communications Surveys and Tutorials, 2018, 20, 2658-2713.	39.4	62
231	Secure Comparison Under Ideal/Real Simulation Paradigm. IEEE Access, 2018, 6, 31236-31248.	4.2	0
232	An ICN-Based Authentication Protocol for a Simplified LTE Architecture. Lecture Notes in Electrical Engineering, 2018, , 125-140.	0.4	4
233	SILK-TV: Secret Information Leakage from Keystroke Timing Videos. Lecture Notes in Computer Science, 2018, , 263-280.	1.3	6
234	Back To The Epilogue: Evading Control Flow Guard via Unaligned Targets. , 2018, , .		18

#	ARTICLE	IF	CITATIONS
235	Don't Skype & Type!., 2017, , .		23
236	You Surf so Strange Today: Anomaly Detection in Web Services via HMM and CTMC. Lecture Notes in Computer Science, 2017, , 426-440.	1.3	2
237	SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks. IEEE Transactions on Network and Service Management, 2017, 14, 487-497.	4.9	119
238	Do we need a holistic approach for the design of secure IoT systems?., 2017, , .		1
239	A Survey on the Security of Stateful SDN Data Planes. IEEE Communications Surveys and Tutorials, 2017, 19, 1701-1725.	39.4	133
240	Obfuscation and Diversification for Securing Cloud Computing. Lecture Notes in Computer Science, 2017, , 179-202.	1.3	1
241	Detection of Information Leaks via Reflection in Android Apps. , 2017, , .		4
242	DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 2017, 107, 30-48.	5.1	192
243	Plndroid: A novel Android malware detection system using ensemble learning methods. Computers and Security, 2017, 68, 36-46.	6.0	157
244	Combating DDoS Attacks in the Cloud: Requirements, Trends, and Future Directions. IEEE Cloud Computing, 2017, 4, 22-32.	3.9	33
245	Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study. Journal of Forensic Sciences, 2017, 62, 641-654.	1.6	19
246	LineSwitch: Tackling Control Plane Saturation Attacks in Software-Defined Networking. IEEE/ACM Transactions on Networking, 2017, 25, 1206-1219.	3.8	89
247	DDoS victim service containment to minimize the internal collateral damages in cloud computing. Computers and Electrical Engineering, 2017, 59, 165-179.	4.8	16
248	EnergIoT: A solution to improve network lifetime of IoT devices. Pervasive and Mobile Computing, 2017, 42, 124-133.	3.3	32
249	Toward secure and efficient attestation for highly dynamic swarms. , 2017, , .		7
250	Fitness Trackers: Fit for Health but Unfit for Security and Privacy. , 2017, , .		34
251	REMI. , 2017, , .		26
252	Mirage: Toward a Stealthier and Modular Malware Analysis Sandbox for Android. Lecture Notes in Computer Science, 2017, , 278-296.	1.3	9

#	ARTICLE	IF	CITATIONS
253	FADEWICH: Fast Deauthentication Over the Wireless Channel. , 2017, , .		8
254	sPECTRA: A precise framEwork for analyzing CrypTographic vulneRabilities in Android apps. , 2017, , .		3
255	Android inter-app communication threats and detection techniques. Computers and Security, 2017, 70, 392-421.	6.0	29
256	No Free Charge Theorem: A Covert Channel viaÂUSB Charging Cable on Mobile Devices. Lecture Notes in Computer Science, 2017, , 83-102.	1.3	23
257	Panorama: Real-time bird's eye view of an OpenFlow network. , 2017, , .		4
258	Forensics Analysis of Android Mobile VoIP Apps. , 2017, , 7-20.		14
259	A roaming-based denial of service attack on LTE networks. , 2017, , .		5
260	A Novel Distributed Fog-Based Networked Architecture to Preserve Energy in Fog Data Centers. , 2017, , .		28
261	On the Influence of Emotional Valence Shifts on the Spread of Information in Social Networks. , 2017, , .		14
262	ODIN. ACM Transactions on Internet Technology, 2017, 18, 1-22.	4.4	12
263	TextDroid: Semantics-based detection of mobile malware using network flows. , 2017, , .		13
264	Breaking Fitness Records Without Moving: Reverse Engineering and Spoofing Fitbit. Lecture Notes in Computer Science, 2017, , 48-69.	1.3	21
265	AndroTaint: An efficient android malware detection framework using dynamic taint analysis. , 2017, , .		18
266	Toward the Development of Secure Underwater Acoustic Networks. IEEE Journal of Oceanic Engineering, 2017, 42, 1075-1087.	3.8	51
267	Drone Path Planning for Secure Positioning and Secure Position Verification. IEEE Transactions on Mobile Computing, 2017, 16, 2478-2493.	5.8	50
268	Anonymous end-to-end communications in adversarial mobile clouds. Pervasive and Mobile Computing, 2017, 36, 57-67.	3.3	5
269	Service resizing for quick DDoS mitigation in cloud computing environment. Annales Des Telecommunications/Annals of Telecommunications, 2017, 72, 237-252.	2.5	28
270	SNIFFO: Security of networks and intelligence for field operations. , 2017, , .		0

#	ARTICLE	IF	CITATIONS
271	Identifying Emotions in Social Media: Comparison of Word-Emotion Lexicons. , 2017, , .		22
272	A comprehensive and effective mechanism for DDoS detection in SDN. , 2017, , .		20
273	GolfEngine: Network management system for software defined networking. , 2017, , .		2
274	Blocking intrusions at border using software defined-internet exchange point (SD-IXP). , 2017, , .		5
275	Practical extensions to countermeasure DoS attacks in software defined networking. , 2017, , .		7
276	Applications of Trusted Computing in Cloud Context. , 2017, , 449-465.		1
277	Ensuring information security by using Haskell's advanced type system. , 2017, , .		1
278	Evaluating the High Frequency Behavior of the Modified Grounding Scheme in Wind Farms. Applied Sciences (Switzerland), 2017, 7, 1323.	2.5	14
279	Fog over Virtualized IoT: New Opportunity for Context-Aware Networked Applications and a Case Study. Applied Sciences (Switzerland), 2017, 7, 1325.	2.5	25
280	Investigating Storage as a Service Cloud Platform. , 2017, , 185-204.		10
281	Adapting the System to Users Based on Implicit Data: Ethical Risks and Possible Solutions. Lecture Notes in Computer Science, 2017, , 5-22.	1.3	3
282	Type Me the Truth!. , 2017, , .		6
283	Why Snoopy Loves Online Services: An Analysis of (Lack of) Privacy in Online Services. , 2017, , .		1
284	Know Your Enemy: Stealth Configuration-Information Gathering in SDN. Lecture Notes in Computer Science, 2017, , 386-401.	1.3	6
285	Despicable me(ter): Anonymous and fine-grained metering data reporting with dishonest meters. , 2016, , .		13
286	Amplified Distributed Denial of Service Attack in Software Defined Networking. , 2016, , .		9
287	ANASTASIA: ANdroid mAlware detection using STatic analySis of Applications. , 2016, , .		70
288	SANA. , 2016, , .		82

#	ARTICLE	IF	CITATIONS
289	On the Feasibility of Attribute-Based Encryption on Internet of Things Devices. IEEE Micro, 2016, 36, 25-35.	1.8	100
290	RPiDS: Raspberry Pi IDS " A Fruitful Intrusion Detection System for IoT. , 2016, , .		64
291	FlowMine: Android app analysis via data flow. , 2016, , .		10
292	A Survey of Man In The Middle Attacks. IEEE Communications Surveys and Tutorials, 2016, 18, 2027-2051.	39.4	374
293	A Host and Network Based Intrusion Detection for Android Smartphones. , 2016, , .		5
294	Hand Drawn Optical Circuit Recognition. Procedia Computer Science, 2016, 84, 41-48.	2.0	17
295	AppScanner: Automatic Fingerprinting of Smartphone Apps from Encrypted Network Traffic. , 2016, , .		183
296	ABAKA: A novel attribute-based k-anonymous collaborative solution for LBSs. Computer Communications, 2016, 85, 1-13.	5.1	23
297	DDoS attacks in cloud computing: Collateral damage to non-targets. Computer Networks, 2016, 109, 157-171.	5.1	62
298	Modeling Enlargement Attacks Against UWB Distance Bounding Protocols. IEEE Transactions on Information Forensics and Security, 2016, 11, 1565-1577.	6.9	11
299	On the Effectiveness of Sensor-enhanced Keystroke Dynamics Against Statistical Attacks. , 2016, , .		29
300	Mind The Plug! Laptop-User Recognition Through Power Consumption. , 2016, , .		19
301	Provably Secure Authenticated Key Agreement Scheme for Smart Grid. IEEE Transactions on Smart Grid, 2016, , 1-1.	9.0	158
302	OnboardICNg. , 2016, , .		19
303	Secure underwater acoustic networks: Current and future research directions. , 2016, , .		30
304	A smart health application and its related privacy issues. , 2016, , .		37
305	The impact of malicious nodes positioning on vehicular alert messaging system. Ad Hoc Networks, 2016, 52, 3-16.	5.5	18
306	Colluding browser extension attack on user privacy and its implication for web browsers. Computers and Security, 2016, 63, 14-28.	6.0	9

#	ARTICLE	IF	CITATIONS
307	ELBA: Efficient Layer Based Routing Algorithm in SDN. , 2016, , .		15
308	Anonymity in an Electronic Society: A Survey. , 2016, , 283-312.		1
309	MimeoDroid: Large Scale Dynamic App Analysis on Cloned Devices via Machine Learning Classifiers. , 2016, , .		5
310	Towards a realistic model for failure propagation in interdependent networks. , 2016, , .		13
311	Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks. IEEE Transactions on Information Forensics and Security, 2016, 11, 665-676.	6.9	40
312	DroidAnalyst: Synergic App Framework for Static and Dynamic App Analysis. Studies in Computational Intelligence, 2016, , 519-552.	0.9	10
313	Analyzing Android Encrypted Network Traffic to Identify User Actions. IEEE Transactions on Information Forensics and Security, 2016, 11, 114-125.	6.9	197
314	CAPTCHaStar! A Novel CAPTCHA Based on Interactive Shape Discovery. Lecture Notes in Computer Science, 2016, , 611-628.	1.3	12
315	Brain-Computer Interface applications: Security and privacy challenges. , 2015, , .		16
316	Provable Storage Medium for Data Storage Outsourcing. IEEE Transactions on Services Computing, 2015, 8, 985-997.	4.6	4
317	CaT: Evaluating cloud-aided TLS for smartphone energy efficiency. , 2015, , .		1
318	Losing Control. , 2015, , .		85
319	You are AIRing too Much: Assessing the Privacy of Users in Crowdsourcing Environmental Data. , 2015, , .		12
320	Revealing Censored Information Through Comments and Commenters in Online Social Networks. , 2015, , .		6
321	Security and Privacy in Cloud Computing via Obfuscation and Diversification: A Survey. , 2015, , .		8
322	To NACK or Not to NACK? Negative Acknowledgments in Information-Centric Networking. , 2015, , .		24
323	TRAP: Using Targeted ads to unveil Google personal profiles. , 2015, , .		5
324	Boten ELISA: A novel approach for botnet C&C in Online Social Networks. , 2015, , .		9

#	ARTICLE	IF	CITATIONS
325	Verifiable and privacy-preserving fine-grained data-collection for smart metering. , 2015, , .		4
326	Toward an Anonymous Process Mining. , 2015, , .		17
327	EyeCloud: A BotCloud Detection System. , 2015, , .		7
328	Impact of country-scale Internet disconnection on structured and social P2P overlays. , 2015, , .		3
329	Android Security: A Survey of Issues, Malware Penetration, and Defenses. IEEE Communications Surveys and Tutorials, 2015, 17, 998-1022.	39.4	402
330	Robust access control framework for mobile cloud computing network. Computer Communications, 2015, 68, 61-72.	5.1	29
331	Environmentâ€“Reactive Malware Behavior: Detection and Categorization. Lecture Notes in Computer Science, 2015, , 167-182.	1.3	4
332	A robust dynamic analysis system preventing SandBox detection by Android malware. , 2015, , .		19
333	Can't You Hear Me Knocking. , 2015, , .		64
334	LineSwitch. , 2015, , .		41
335	Impact of security threats in vehicular alert messaging systems. , 2015, , .		4
336	On the Feasibility of Attribute-Based Encryption on Smartphone Devices. , 2015, , .		48
337	Leveraging Parallel Communications for Minimizing Energy Consumption on Smartphones. IEEE Transactions on Parallel and Distributed Systems, 2015, 26, 2778-2790.	5.6	6
338	Employing Program Semantics for Malware Detection. IEEE Transactions on Information Forensics and Security, 2015, 10, 2591-2604.	6.9	81
339	The verifier bee: A path planner for drone-based secure location verification. , 2015, , .		9
340	SocialSpy: Browsing (Supposedly) Hidden Information in Online Social Networks. Lecture Notes in Computer Science, 2015, , 83-99.	1.3	2
341	Secure Wireless Sensor Networks. Advances in Information Security, 2015, , .	1.2	12
342	Violating Consumer Anonymity: Geo-Locating Nodes in Named Data Networking. Lecture Notes in Computer Science, 2015, , 243-262.	1.3	19

#	ARTICLE	IF	CITATIONS
343	Evaluation of Android Anti-malware Techniques against Dalvik Bytecode Obfuscation. , 2014, , .		20
344	OASIS. , 2014, , .		7
345	Attack Resilient Underwater Networks Through Software Defined Networking. , 2014, , .		7
346	VirtualFriendship: Hiding interactions on Online Social Networks. , 2014, , .		5
347	Covert ephemeral communication in named data networking. , 2014, , .		12
348	A secure alert messaging system for safe driving. Computer Communications, 2014, 46, 29-42.	5.1	17
349	An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments. IEEE Transactions on Services Computing, 2014, 7, 373-386.	4.6	33
350	MOSES: Supporting and Enforcing Security Profiles on Smartphones. IEEE Transactions on Dependable and Secure Computing, 2014, 11, 211-223.	5.4	37
351	Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact. IEEE Transactions on Information Forensics and Security, 2014, 9, 681-694.	6.9	88
352	Updicator: Updating Billions of Devices by an Efficient, Scalable and Secure Software Update Distribution over Untrusted Cache-enabled Networks. Lecture Notes in Computer Science, 2014, , 76-93.	1.3	18
353	Smart health: A context-aware health paradigm within smart cities. , 2014, 52, 74-81.		463
354	Fast and Secure Multihop Broadcast Solutions for Intervehicular Communication. IEEE Transactions on Intelligent Transportation Systems, 2014, 15, 433-450.	8.0	49
355	Clone wars: Distributed detection of clone attacks in mobile WSNs. Journal of Computer and System Sciences, 2014, 80, 654-669.	1.2	38
356	I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics. Lecture Notes in Computer Science, 2014, , 92-111.	1.3	53
357	Detecting Targeted Smartphone Malware with Behavior-Triggering Stochastic Models. Lecture Notes in Computer Science, 2014, , 183-201.	1.3	16
358	Secure Message Delivery Games for Device-to-Device Communications. Lecture Notes in Computer Science, 2014, , 195-215.	1.3	10
359	Censorship-Resilient Communications through Information Scattering. Lecture Notes in Computer Science, 2014, , 82-89.	1.3	0
360	Preserving privacy against external and internal threats in WSN data aggregation. Telecommunication Systems, 2013, 52, 2163-2176.	2.5	26

#	ARTICLE	IF	CITATIONS
361	FM 99.9, Radio Virus: Exploiting FM Radio Broadcasts for Malware Deployment. IEEE Transactions on Information Forensics and Security, 2013, 8, 1027-1037.	6.9	28
362	Cache Privacy in Named-Data Networking. , 2013, , .		69
363	A lightweight mechanism for detection of cache pollution attacks in Named Data Networking. Computer Networks, 2013, 57, 3178-3191.	5.1	114
364	Hybrid Static-Runtime Information Flow and Declassification Enforcement. IEEE Transactions on Information Forensics and Security, 2013, 8, 1294-1305.	6.9	25
365	MASS: An efficient and secure broadcast authentication scheme for resource constrained devices. , 2013, , .		1
366	Secure Verification of Location Claims on a Vehicular Safety Application. , 2013, , .		6
367	Poseidon: Mitigating interest flooding DDoS attacks in Named Data Networking. , 2013, , .		156
368	Smartphone and Laptop Frameworks for vehicular networking experimentation. , 2013, , .		2
369	Preserving Smartphone Users' Anonymity in Cloudy Days. , 2013, , .		3
370	CREPUSCOLO: A collusion resistant privacy preserving location verification system. , 2013, , .		11
371	The role of the RPL routing protocol for smart grid communications. , 2013, 51, 75-83.		125
372	Windows Mobile LiveSD Forensics. Journal of Network and Computer Applications, 2013, 36, 677-684.	9.1	19
373	Providing Source Location Privacy in Wireless Sensor Networks: A Survey. IEEE Communications Surveys and Tutorials, 2013, 15, 1238-1280.	39.4	137
374	Virtual private social networks and a facebook implementation. ACM Transactions on the Web, 2013, 7, 1-31.	2.5	16
375	ContextOS: A Context Aware Operating System for Mobile Devices. , 2013, , .		5
376	Friend in the Middle (FiM): Tackling de-anonymization in social networks. , 2013, , .		13
377	MITHYS: Mind The Hand You Shake - Protecting Mobile Devices from SSL Usage Vulnerabilities. Lecture Notes in Computer Science, 2013, , 65-81.	1.3	18
378	Demonstrating the effectiveness of MOSES for separation of execution modes. , 2012, , .		4

#	ARTICLE	IF	CITATIONS
379	MOSES. , 2012, , .		45
380	CRÃPE: A System for Enforcing Fine-Grained Context-Related Policies on Android. IEEE Transactions on Information Forensics and Security, 2012, 7, 1426-1438.	6.9	63
381	Wireless Sensor Replica Detection in Mobile Environments. Lecture Notes in Computer Science, 2012, , 249-264.	1.3	6
382	FakeBook: Detecting Fake Profiles in On-Line Social Networks. , 2012, , .		68
383	Sense-And-Trace: A Privacy Preserving Distributed Geolocation Tracking System. Lecture Notes in Computer Science, 2012, , 199-213.	1.3	1
384	Optimal Solutions for Pairing Services on Smartphones: A Strategy to Minimize Energy Consumption. , 2012, , .		3
385	Secure Data Aggregation in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 2012, 7, 1040-1052.	6.9	96
386	Sense-And-Trace: A Privacy Preserving Distributed Geolocation Tracking System (Transcript of) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50 462	1.3	0
387	Events privacy in WSNs: A new model and its application. , 2011, , .		10
388	Distributed Detection of Clone Attacks in Wireless Sensor Networks. IEEE Transactions on Dependable and Secure Computing, 2011, 8, 685-698.	5.4	130
389	"Who Counterfeited My Viagra?" Probabilistic Item Removal Detection via RFID Tag Cooperation. Eurasip Journal on Wireless Communications and Networking, 2011, 2011, .	2.4	2
390	CRePE: Context-Related Policy Enforcement for Android. Lecture Notes in Computer Science, 2011, , 331-345.	1.3	110
391	CASSANDRA: a probabilistic, efficient, and privacy-preserving solution to compute set intersection. International Journal of Information Security, 2011, 10, 301-319.	3.4	1
392	Secure topology maintenance and events collection in WSNs. Security and Communication Networks, 2011, 4, 744-762.	1.5	6
393	Virtual private social networks. , 2011, , .		30
394	Mind how you answer me!. , 2011, , .		68
395	Time in Privacy Preserving LBSs: An Overlooked Dimension. International Journal of Vehicular Technology, 2011, 2011, 1-12.	1.1	1
396	Event Handoff Unobservability in WSN. Lecture Notes in Computer Science, 2011, , 20-28.	1.3	5

#	ARTICLE	IF	CITATIONS
397	The smallville effect. , 2010, , .		12
398	Context- and social-aware middleware for opportunistic networks. Journal of Network and Computer Applications, 2010, 33, 525-541.	9.1	76
399	eRIPP-FS: Enforcing privacy and security in RFID. Security and Communication Networks, 2010, 3, 58-70.	1.5	6
400	Time Warp: How Time Affects Privacy in LBSs. Lecture Notes in Computer Science, 2010, , 325-339.	1.3	10
401	Reverse Tree-based Key Routing: Robust Data Aggregation in Wireless Sensor Networks. , 2010, , .		1
402	Security in Outsourced Storage: Efficiently Checking Integrity and Service Level Agreement Compliance. , 2010, , .		1
403	CED2: Communication Efficient Disjointness Decision. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2010, , 290-306.	0.3	1
404	Distributed data source verification in wireless sensor networks. Information Fusion, 2009, 10, 342-353.	19.1	24
405	Privacyâ€preserving robust data aggregation in wireless sensor networks. Security and Communication Networks, 2009, 2, 195-213.	1.5	51
406	Secure median computation in wireless sensor networks. Ad Hoc Networks, 2009, 7, 1448-1462.	5.5	8
407	The Quest for Mobility Models to Analyse Security in Mobile Ad Hoc Networks. Lecture Notes in Computer Science, 2009, , 85-96.	1.3	6
408	Mobility and Cooperation to Thwart Node Capture Attacks in MANETs. Eurasip Journal on Wireless Communications and Networking, 2009, 2009, .	2.4	27
409	Sec-TMP: A Secure Topology Maintenance Protocol for Event Delivery Enforcement in WSN. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2009, , 265-284.	0.3	3
410	Emergent properties. , 2008, , .		69
411	Securely computing an approximate median in wireless sensor networks. , 2008, , .		16
412	A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. , 2007, , .		131
413	FastRIPP: RFID Privacy Preserving protocol with Forward Secrecy and Fast Resynchronisation. , 2007, , .		5
414	RIPP-FS: An RFID Identification, Privacy Preserving Protocol with Forward Secrecy.. , 2007, , .		32

#	ARTICLE	IF	CITATIONS
415	ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks. <i>Ad Hoc Networks</i> , 2007, 5, 49-62.	5.5	25
416	Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN. , 2006, , .		17
417	Secure Cooperative Channel Establishment in Wireless Sensor Networks. , 0, , .		8
418	Correction to: On defending against label flipping attacks on malware detection systems. <i>Neural Computing and Applications</i> , 0, , .	5.6	5