Frank Kargl

List of Publications by Year
in descending order

Source: https://exaly.com/author-pdf/9000636/publications.pdf

Version: 2024-02-01

122 papers	4,142 citations	361413 20 h-index	254184 43 g-index
126 all docs	126 docs citations	126 times ranked	2724 citing authors

#	Article	IF	Citations
1	Risk Prediction of IoT Devices Based on Vulnerability Analysis. ACM Transactions on Privacy and Security, 2022, 25, 1-36.	3.0	5
2	Online Privacy Literacy and Online Privacy Behavior â€“ The Role of Crystallized Intelligence and Personality. International Journal of Human-Computer Interaction, 2021, 37, 1455-1466.	4.8	22
3	Ride and Hide: A Study on the Privacy of Ride Hailing Services. , 2019, , .		0
4	Detecting Anomalous Driving Behavior using Neural Networks. , 2019, , .		20
5	Cryptographic Design of PriCloud, a Privacy-preserving Decentralized Storage with Remuneration. IEEE Transactions on Dependable and Secure Computing, 2019, , 1-1.	5.4	3
6	Survey of Protocol Reverse Engineering Algorithms: Decomposition of Tools for Static Traffic Analysis. IEEE Communications Surveys and Tutorials, 2019, 21, 526-561.	39.4	24
7	Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. IEEE Communications Surveys and Tutorials, 2019, 21, 779-811.	39.4	157
8	Privacy in Mobile Sensing. Studies in Neuroscience, Psychology and Behavioral Economics, 2019, , 3-12.	0.3	16
9	An Evaluation of Pseudonym Changes for Vehicular Networks in Large-Scale, Realistic Traffic Scenarios. IEEE Transactions on Intelligent Transportation Systems, 2018, 19, 3400-3405.	8.0	11
10	Applications of Smart-Contracts: Anonymous Decentralized Insurances with IoT Sensors. , 2018, , .		5
11	An SDN-based Approach For Defending Against Reflective DDoS Attacks. , 2018, , .		5
12	iRide: A Privacy-Preserving Architecture for Self-Driving Cabs Service. , 2018, , .		4
13	Identifying Devices of the Internet of Things Using Machine Learning on Clock Characteristics. Lecture Notes in Computer Science, 2018, , 417-427.	1.3	13
14	uMine: A Blockchain Based on Human Miners. Lecture Notes in Computer Science, 2018, , 20-38.	1.3	3
15	Privacy of Connected Vehicles. , 2018, , 229-251.		3
16	Secure Code Execution: A Generic PUF-Driven System Architecture. Lecture Notes in Computer Science, 2018, , 25-46.	1.3	1
17	Retro-Î». , 2018, , .		6
18	Multi-Source Fusion Operations in Subjective Logic. , 2018, , .		8

#	Article	IF	Citations
19	Log Pruning in Distributed Event-sourced Systems. , 2018, , .		2
20	A Flexible Network Approach to Privacy of Blockchain Transactions. , 2018, , .		5
21	Performance Engineering in Distributed Event-sourced Systems. , 2018, , .		0
22	VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 318-337.	0.3	78
23	SDN-Assisted Network-Based Mitigation of Slow DDoS Attacks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2018, , 102-121.	0.3	18
24	A Privacy Engineering Framework for the Internet of Things. Law, Governance and Technology Series, 2017, , 163-202.	0.4	12
25	Consistent retrospective snapshots in distributed event-sourced systems. , 2017, , .		5
26	Security Challenges and Opportunities of Software-Defined Networking. IEEE Security and Privacy, 2017, 15, 96-100.	1.2	69
27	Chronograph. , 2017, , .		10
28	Design of a Privacy-Preserving Decentralized File Storage with Financial Incentives. , 2017, , .		33
29	Analyzing attacks on cooperative adaptive cruise control (CACC). , 2017, , .		63
30	An Extensible Host-Agnostic Framework for SDN-Assisted DDoS-Mitigation. , 2017, , .		8
31	A Testing Framework for High-Speed Network and Security Devices. , 2017, , .		0
32	Formal Analysis of V2X Revocation Protocols. Lecture Notes in Computer Science, 2017, , 147-163.	1.3	15
33	Enhanced Position Verification for VANETs Using Subjective Logic. , 2016, , .		23
34	Exploiting propagation effects for authentication and misbehavior detection in VANETs. , 2016, , .		1
35	POSTER: Anomaly-based misbehaviour detection in connected car backends. , 2016, , .		9
36	Setting Up a High-Speed TCP Benchmarking Environment - Lessons Learned. , 2016, , .		1

#	Article	IF	Citations
37	A Comparison of TCP Congestion Control Algorithms in 10G Networks. , 2016, , .		17
38	KopperCoin â€“ A Distributed File Storage with Financial Incentives. Lecture Notes in Computer Science, 2016, , 79-93.	1.3	24
39	PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. Ad Hoc Networks, 2016, 37, 122-132.	5.5	51
40	A resilient in-network aggregation mechanism for VANETs based on dissemination redundancy. Ad Hoc Networks, 2016, 37, 101-109.	5.5	12
41	Wireless channel-based message authentication. , 2015, , .		5
42	Decentralized enforcement of k-anonymity for location privacy using secret sharing. , 2015, , .		7
43	Context-adaptive detection of insider attacks in VANET information dissemination schemes. , 2015, , .		3
44	A framework for evaluating pseudonym strategies in vehicular ad-hoc networks. , 2015, , .		12
45	Pre-Distribution of Certificates for Pseudonymous Broadcast Authentication in VANET. , 2015, , .		9
46	Secure Cluster-Based In-Network Information Aggregation for Vehicular Networks. , 2015, , .		4
47	Sequence-aware Intrusion Detection in Industrial Control Systems. , 2015, , .		101
48	Terrorist fraud resistance of distance bounding protocols employing physical unclonable functions. , 2015, , .		1
49	Pseudonym Schemes in Vehicular Networks: A Survey. IEEE Communications Surveys and Tutorials, 2015, 17, 228-255.	39.4	327
50	Formal Verification of Privacy Properties in Electric Vehicle Charging. Lecture Notes in Computer Science, 2015, , 17-33.	1.3	9
51	REWIRE â€“ Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks. Lecture Notes in Computer Science, 2015, , 193-208.	1.3	12
52	Modeling Message Sequences for Intrusion Detection in Industrial Control Systems. IFIP Advances in Information and Communication Technology, 2015, , 49-71.	0.7	17
53	Redundancy-based statistical analysis for insider attack detection in VANET aggregation schemes. , 2014, , .		7
54	Insights on the Security and Dependability of Industrial Control Systems. IEEE Security and Privacy, 2014, 12, 75-78.	1.2	30

#	Article	IF	Citations
55	Concurrent programming in web applications. IT - Information Technology, 2014, 56, 119-126.	0.9	0
56	Formal model of certificate omission schemes in VANET. , 2014, , .		4
57	Dynamic packet-filtering in high-speed networks using NetFPGAs. , 2014, , .		0
58	In-Network Aggregation for Vehicular &lt;italic&gt;Ad Hoc&lt;/italic&gt; Networks. IEEE Communications Surveys and Tutorials, 2014, 16, 1909-1932.	39.4	46
59	Revisiting attacker model for smart vehicles. , 2014, , .		15
60	PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET). , 2014, , .		36
61	A flexible, subjective logic-based framework for misbehavior detection in V2V networks. , 2014, , .		27
62	On credibility improvements for automotive navigation systems. Personal and Ubiquitous Computing, 2013, 17, 803-813.	2.8	5
63	SeDyA. , 2013, , .		8
64	Impact of V2X privacy strategies on Intersection Collision Avoidance systems. , 2013, , .		57
65	Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols. IEEE Transactions on Vehicular Technology, 2013, 62, 1505-1518.	6.3	42
66	The impact of security on cooperative awareness in VANET. , 2013, , .		29
67	POPCORN. , 2013, , .		21
68	Efficient and secure storage of private keys for pseudonymous vehicular communication. , 2013, , .		11
69	Short paper: Towards data-similarity-based clustering for inter-vehicle communication. , 2013, , .		3
70	Electronic Decal: A Security Function Based on V2X Communication. , 2013, , .		2
71	On the Feasibility of Device Fingerprinting in Industrial Control Systems. Lecture Notes in Computer Science, 2013, , 155-166.	1.3	15
72	Privacy context model for dynamic privacy adaptation in ubiquitous computing. , 2012, , .		8

#	Article	IF	Citations
73	Evaluation of congestion-based certificate omission in VANETs. , 2012, , .		15
74	CANE: A Controlled Application Environment for privacy protection in ITS. , 2012, , .		2
75	Security in nano communication: Challenges and open research issues. , 2012, , .		11
76	Understanding vehicle related crime to elaborate on countermeasures based on ADAS and V2X communication. , 2012, , .		2
77	On the potential of PUF for pseudonym generation in vehicular networks. , 2012, , .		12
78	Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters. , 2012, , .		45
79	Towards security in nano-communication: Challenges and opportunities. Nano Communication Networks, 2012, 3, 151-160.	2.9	67
80	Privacy-by-design in ITS applications. , 2011, , .		21
81	Spoofed data detection in VANETs using dynamic thresholds. , 2011, , .		18
82	ACM WiSec 2011 poster and demo session. Mobile Computing and Communications Review, 2011, 15, 34-34.	1.7	0
83	Research challenges in intervehicular communication: lessons of the 2010 Dagstuhl Seminar. , 2011, 49, 158-164.		65
84	Modeling in-network aggregation in VANETs. , 2011, 49, 142-148.		34
85	V-Tokens for Conditional Pseudonymity in VANETs. , 2010, , .		47
86	Measuring long-term location privacy in vehicular communication systems. Computer Communications, 2010, 33, 1414-1427.	5.1	25
87	Decentralized position verification in geographic <i>ad hoc</i> routing. Security and Communication Networks, 2010, 3, 289-302.	1.5	37
88	Interaction weaknesses of personal navigation devices. , 2010, , .		14
89	Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. , 2010, , .		145
90	On the efficiency of secure beaconing in VANETs. , 2010, , .		44

#	Article	IF	Citations
91	Resilient secure aggregation for vehicular networks. IEEE Network, 2010, 24, 26-31.	6.9	39
92	Exploration of adaptive beaconing for efficient intervehicle safety communication. IEEE Network, 2010, 24, 14-19.	6.9	163
93	On the potential of generic modeling for VANET data aggregation protocols. , 2010, , .		16
94	Privacy Requirements in Vehicular Communication Systems. , 2009, , .		48
95	A fuzzy logic based approach for structure-free aggregation in vehicular ad-hoc networks. , 2009, , .		53
96	Measuring location privacy in V2X communication systems with accumulated information. , 2009, , .		10
97	Channel switch and quiet attack: New DoS attacks exploiting the 802.11 standard. , 2009, , .		24
98	A location privacy metric for V2X communication systems. , 2009, , .		37
99	On the security of contextâ€adaptive information dissemination. Security and Communication Networks, 2008, 1, 205-218.	1.5	6
100	Secure vehicular communication systems: design and architecture. , 2008, 46, 100-109.		394
101	Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Communications Magazine, 2008, 46, 110-118.	6.1	213
102	Communication patterns in VANETs. , 2008, 46, 119-125.		291
103	Evaluation of Position Based Gossiping for VANETs in an Intersection Scenario. , 2008, , .		4
104	Pseudonym-On-Demand: A New Pseudonym Refill Strategy for Vehicular Communications. , 2008, , .		32
105	Advanced Adaptive Gossiping Using 2-Hop Neighborhood Information. , 2008, , .		20
106	Implementing and Validating an Environmental and Health Monitoring System. , 2008, , .		11
107	Optimized Position Based Gossiping in VANETs. , 2008, , .		16
108	SNMP Proxy for Wireless Sensor Network. , 2008, , .		16

#	Article	IF	Citations
109	Secure and efficient beaconing for vehicular networks. , 2008, , .		28
110	Simulation of Ad Hoc Networks: ns-2 compared to JiST/SWANS. , 2008, , .		21
111	Vulnerabilities of Geocast Message Distribution. , 2007, , .		6
112	Interactive Realistic Simulation of Wireless Networks. , 2007, , .		13
113	The iNAV Indoor Navigation System. , 2007, , 110-117.		16
114	Adaptive Topology Based Gossiping in VANETs Using Position Information. , 2007, , 66-78.		9
115	POSITION VERIFICATION APPROACHES FOR VEHICULAR AD HOC NETWORKS. IEEE Wireless Communications, 2006, 13, 16-21.	9.0	127
116	Location Tracking Attack in Ad hoc Networks based on Topology Information. , 2006, , .		6
117	Improved security in geographic ad hoc routing through autonomous position verification. , 2006, , .		100
118	Re-identifying Anonymous Nodes. Lecture Notes in Computer Science, 2006, , 103-115.	1.3	1
119	Semantic Information Retrieval in the COMPASS Location System. Lecture Notes in Computer Science, 2006, , 129-143.	1.3	5
120	Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks. Lecture Notes in Computer Science, 2005, , 152-165.	1.3	72
121	The COMPASS Location System. Lecture Notes in Computer Science, 2005, , 105-112.	1.3	12
122	Influence of Falsified Position Data on Geographic Ad-Hoc Routing. Lecture Notes in Computer Science, 2005, , 102-112.	1.3	27