Huy Kang Kim

List of Publications by Year
in descending order

118 papers	2,868 citations	331259 21 h-index	301761 39 g-index
120 all docs	120 docs citations	120 times ranked	1587 citing authors

#	Article	IF	Citations
1	Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. , 2016, , .		275
2	GIDS: GAN based Intrusion Detection System for In-Vehicle Network. , 2018, , .		218
3	OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame. , 2017, , .		200
4	In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications, 2020, 21, 100198.	2.7	199
5	Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers and Security, 2021, 103, 102150.	4.0	162
6	A Novel Approach to Detect Malware Based on API Call Sequence Analysis. International Journal of Distributed Sensor Networks, 2015, 11, 659101.	1.3	149
7	Know your master: Driver profiling-based anti-theft method. , 2016, , .		100
8	Detecting and Classifying Android Malware Using Static Analysis along with Creator Information. International Journal of Distributed Sensor Networks, 2015, 11, 479174.	1.3	88
9	Online game bot detection based on party-play log analysis. Computers and Mathematics With Applications, 2013, 65, 1384-1395.	1.4	81
10	Anomaly intrusion detection method for vehicular networks based on survival analysis. Vehicular Communications, 2018, 14, 52-63.	2.7	74
11	A hybrid approach of neural network and memory-based learning to data mining. IEEE Transactions on Neural Networks, 2000, 11, 637-646.	4.8	67
12	CAN-ADF: The controller area network attack detection framework. Computers and Security, 2020, 94, 101857.	4.0	41
13	DSS for computer security incident response applying CBR and collaborative response. Expert Systems With Applications, 2010, 37, 852-870.	4.4	40
14	You are a Game Bot!: Uncovering Game Bots in MMORPGs via Self-similarity in the Wild. , 2016, , .		39
15	Self-Supervised Anomaly Detection for In-Vehicle Network Using Noised Pseudo Normal Data. IEEE Transactions on Vehicular Technology, 2021, 70, 1098-1108.	3.9	39
16	GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. , 2018, , .		39
17	Andro-AutoPsy: Anti-malware system based on similarity matching of malware and malware creator-centric information. Digital Investigation, 2015, 14, 17-35.	3.2	38
18	Andro-Dumpsys: Anti-malware system based on the similarity of malware creator and malware centric information. Computers and Security, 2016, 58, 125-138.	4.0	38

#	Article	IF	Citations
19	A behavior-based intrusion detection technique for smart grid infrastructure. , 2015, , .		34
20	Self-similarity Based Lightweight Intrusion Detection Method for Cloud Computing. Lecture Notes in Computer Science, 2011, , 353-362.	1.0	30
21	Analysis of Context Dependence in Social Interaction Networks of a Massively Multiplayer Online Role-Playing Game. PLoS ONE, 2012, 7, e33918.	1.1	28
22	A Novel Biometric Identification Based on a User's Input Pattern Analysis for Intelligent Mobile Devices. International Journal of Advanced Robotic Systems, 2012, 9, 46.	1.3	27
23	Driver Identification Based on Wavelet Transform Using Driving Patterns. IEEE Transactions on Industrial Informatics, 2021, 17, 2400-2410.	7.2	27
24	Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks. Vehicular Communications, 2021, 29, 100338.	2.7	27
25	Multimodal game bot detection using user behavioral characteristics. SpringerPlus, 2016, 5, 523.	1.2	26
26	Cosine similarity based anomaly detection methodology for the CAN bus. Expert Systems With Applications, 2021, 166, 114066.	4.4	23
27	Event-Triggered Interval-Based Anomaly Detection and Attack Identification Methods for an In-Vehicle Network. IEEE Transactions on Information Forensics and Security, 2021, 16, 2941-2956.	4.5	23
28	Survey and research direction on online game security. , 2012, , .		22
29	Security Modelling and Analysis of Dynamic Enterprise Networks. , 2016, , .		22
30	Behavior Analysis and Anomaly Detection for a Digital Substation on Cyber-Physical System. Electronics (Switzerland), 2019, 8, 326.	1.8	22
31	Profit Optimizing Churn Prediction for Long-Term Loyal Customers in Online Games. IEEE Transactions on Games, 2020, 12, 41-53.	1.2	22
32	Detecting and classifying method based on similarity matching of Android malware behavior with profile. SpringerPlus, 2016, 5, 273.	1.2	21
33	Ransomware protection using the moving target defense perspective. Computers and Electrical Engineering, 2019, 78, 288-299.	3.0	21
34	Key Value Drivers of Startup Companies in the New Media Industryâ€"The Case of Online Games in Korea. Journal of Media Economics, 2012, 25, 244-260.	0.8	20
35	Unsupervised Fault Detection on Unmanned Aerial Vehicles: Encoding and Thresholding Approach. Sensors, 2021, 21, 2208.	2.1	20
36	Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimedia Tools and Applications, 2015, 74, 3289-3303.	2.6	19

#	ARTICLE	IF	CITATIONS
37	Crime Scene Reconstruction: Online Gold Farming Network Analysis. IEEE Transactions on Information Forensics and Security, 2016, , 1-1.	4.5	19
38	AutoVAS: An automated vulnerability analysis system with a deep learning approach. Computers and Security, 2021, 106, 102308.	4.0	19
39	A Statistical-Based Anomaly Detection Method for Connected Cars in Internet of Things Environment. Lecture Notes in Computer Science, 2015, , 89-97.	1.0	18
40	What can free money tell us on the virtual black market?. Computer Communication Review, 2011, 41, 392-393.	1.5	17
41	Andro-Simnet: Android Malware Family Classification using Social Network Analysis. , 2018, , .		17
42	Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework. Applied Sciences (Switzerland), 2021, 11, 7738.	1.3	17
43	Andro-profiler. , 2014, , .		16
44	Automated Reverse Engineering and Attack for CAN Using OBD-II. , 2018, , .		16
45	In-Game Action Sequence Analysis for Game BOT Detection on the Big Data Analysis Platform. Proceedings in Adaptation, Learning and Optimization, 2015, , 403-414.	1.5	15
46	Firewall ruleset visualization analysis tool based on segmentation. , 2017, , .		14
47	No Silk Road for Online Gamers!. , 2018, , .		14
48	What can free money tell us on the virtual black market?. , 2011, , .		13
49	Mal-Netminer: Malware Classification Approach Based on Social Network Analysis of System Call Graph. Mathematical Problems in Engineering, 2015, 2015, 1-20.	0.6	13
50	Modeling of bot usage diffusion across social networks in MMORPGs. , 2012, , .		12
51	The contagion of malicious behaviors in online games. , 2013, , .		12
52	Automated Dataset Generation System for Collaborative Research of Cyber Threat Analysis. Security and Communication Networks, 2019, 2019, 1-10.	1.0	12
53	Discovering CAN Specification Using On-Board Diagnostics. IEEE Design and Test, 2021, 38, 93-103.	1.1	12
54	Mal-netminer. , 2014, , .		11

#	Article	IF	Citations
55	Hurst Parameter Based Anomaly Detection for Intrusion Detection System. , 2016, , .		11
56	Contagion of Cheating Behaviors in Online Social Networks. IEEE Access, 2018, 6, 29098-29108.	2.6	11
57	What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol. Pervasive and Mobile Computing, 2020, 66, 101211.	2.1	11
58	Unveiling group characteristics in online social games. , 2014, , .		10
59	The contagion of malicious behaviors in online games. Computer Communication Review, 2013, 43, 543-544.	1.5	10
60	Surgical strike: A novel approach to minimize collateral damage to game BOT detection. , 2013, , .		9
61	De-Wipimization: Detection of data wiping traces for investigating NTFS file system. Computers and Security, 2020, 99, 102034.	4.0	8
62	Do Many Models Make Light Work? Evaluating Ensemble Solutions for Improved Rumor Detection. IEEE Access, 2020, 8, 150709-150724.	2.6	8
63	Cyber Attack and Defense Emulation Agents. Applied Sciences (Switzerland), 2020, 10, 2140.	1.3	8
64	Identifying spreaders of malicious behaviors in online games. , 2014, , .		7
65	Crime scene re-investigation: a postmortem analysis of game account stealers' behaviors. , 2017, , .		7
66	Unveiling a Socio-Economic System in a Virtual World. , 2018, , .		7
67	ADSaS: Comprehensive Real-Time Anomaly Detection System. Lecture Notes in Computer Science, 2019, , 29-41.	1.0	7
68	CBR-Based Decision Support Methodology for Cybercrime Investigation: Focused on the Data-Driven Website Defacement Analysis. Security and Communication Networks, 2019, 2019, 1-21.	1.0	7
69	PF-TL: Payload Feature-Based Transfer Learning for Dealing with the Lack of Training Data. Electronics (Switzerland), 2021, 10, 1148.	1.8	7
70	Network Forensic Evidence Acquisition (NFEA) with Packet Marking. , 2011, , .		6
71	Detection of botnets before activation: an enhanced honeypot system for intentional infection and behavioral observation of malware. Security and Communication Networks, 2012, 5, 1094-1101.	1.0	6
72	Network Forensic Evidence Generation and Verification Scheme (NFEGVS). Telecommunication Systems, 2015, 60, 261-273.	1.6	6

#	Article	IF	Citations
73	Detecting In-vehicle CAN Message Attacks Using Heuristics and RNNs. Lecture Notes in Computer Science, 2019, , 39-45.	1.0	6
74	PhantomFS-v2: Dare You to Avoid This Trap. IEEE Access, 2020, 8, 198285-198300.	2.6	6
75	Unsupervised malicious domain detection with less labeling effort. Computers and Security, 2022, 116, 102662.	4.0	6
76	User Input Pattern-Based Authentication Method to Prevent Mobile E-Financial Incidents. , 2011, , .		5
77	I know what the BOTs did yesterday: Full action sequence analysis using Na&#x00EF;ve Bayesian algorithm. , 2013, , .		5
78	Rise and Fall of Online Game Groups. , 2015, , .		5
79	Function-Oriented Mobile Malware Analysis as First Aid. Mobile Information Systems, 2016, 2016, 1-11.	0.4	5
80	Hybrid Attack Path Enumeration System Based on Reputation Scores. , 2016, , .		5
81	Evaluating Security and Availability of Multiple Redundancy Designs when Applying Security Patches. , 2017, , .		5
82	Altruism in games: Helping others help themselves. , 2014, , .		4
83	â€œI know what you did beforeâ€ General framework for correlation analysis of cyber threat incidents. , 2016, , .		4
84	Automated vulnerability analysis technique for smart grid infrastructure. , 2017, , .		4
85	I Would Not Plant Apple Trees If the World Will Be Wiped. , 2017, , .		4
86	Trading Behind-the-Scene: Analysis of Online Gold Farming Network in the Auction House System. IEEE Transactions on Games, 2022, 14, 423-434.	1.2	4
87	HSViz: Hierarchy Simplified Visualizations for Firewall Policy Analysis. IEEE Access, 2021, 9, 71737-71753.	2.6	4
88	TZMon: Improving mobile game security with ARM trustzone. Computers and Security, 2021, 109, 102391.	4.0	4
89	Applying CBR algorithm for cyber infringement profiling system. Journal of the Korea Institute of Information Security and Cryptology, 2013, 23, 1069-1086.	0.1	4
90	Analysis of Game Bot's Behavioral Characteristics in Social Interaction Networks of MMORPG. Computer Communication Review, 2015, 45, 99-100.	1.5	4

#	Article	IF	Citations
91	Cheating and Detection Method in Massively Multiplayer Online Role-Playing Game: Systematic Literature Review. IEEE Access, 2022, 10, 49050-49063.	2.6	4
92	Multi-relational social networks in a large-scale MMORPG. , 2011, , .		3
93	WHAP: Web-hacking profiling using Case-Based Reasoning. , 2016, , .		3
94	Analysis of Game Bot's Behavioral Characteristics in Social Interaction Networks of MMORPG. , 2015, , .		3
95	Oldie is Goodie: Effective User Retention by In-game Promotion Event Analysis. , 2019, , .		3
96	A Study of Cheater Detection in FPS Game by using User Log Analysis. Journal of Korea Game Society, 2015, 15, 177-188.	0.1	3
97	Game-bot detection based on Clustering of asset-varied location coordinates. Journal of the Korea Institute of Information Security and Cryptology, 2015, 25, 1131-1141.	0.1	3
98	Show Me Your Account: Detecting MMORPG Game Bot Leveraging Financial Analysis with LSTM. Lecture Notes in Computer Science, 2020, , 3-13.	1.0	3
99	Multi-relational social networks in a large-scale MMORPG. Computer Communication Review, 2011, 41, 414-415.	1.5	2
100	Loyalty or profit? Early evolutionary dynamics of online game groups. , 2013, , .		2
101	A Longitudinal Analysis of .i2p Leakage in the Public DNS Infrastructure. , 2016, , .		2
102	Beyond PS-LTE: Security Model Design Framework for PPDR Operational Environment. Security and Communication Networks, 2020, 2020, 1-13.	1.0	2
103	Generosity as Social Contagion in Virtual Community. Lecture Notes in Computer Science, 2015, , 191-199.	1.0	2
104	A survey and categorization of anomaly detection in online games. Journal of the Korea Institute of Information Security and Cryptology, 2015, 25, 1097-1114.	0.1	2
105	A Study on Mobile Game Security Threats by Analyzing Malicious Behavior of Auto Program of Clash of Clans. Journal of the Korea Institute of Information Security and Cryptology, 2015, 25, 1361-1376.	0.1	2
106	Detection of Zombie PCs Based on Email Spam Analysis. KSII Transactions on Internet and Information Systems, 0, , .	0.7	2
107	Online Game Bot Detection in FPS Game. Proceedings in Adaptation, Learning and Optimization, 2015, , 479-491.	1.5	2
108	ADAM: Automated Detection and Attribution of Malicious Webpages. Lecture Notes in Computer Science, 2015, , 3-16.	1.0	2

#	ARTICLE	IF	CITATIONS
109	SECURITY REQUIREMENT REPRESENTATION METHOD FOR CONFIDENCE OF SYSTEMS AND NETWORKS. International Journal of Software Engineering and Knowledge Engineering, 2010, 20, 49-71.	0.6	1
110	Hard-core user and bot user classification using game character's growth types. , 2015, , .		1
111	A Hybrid Defense Technique for ISP Against the Distributed Denial of Service Attacks. Applied Mathematics and Information Sciences, 2014, 8, 2347-2359.	0.7	1
112	Proactive Detection of Botnets with Intended Forceful Infections from Multiple Malware Collecting Channels. Communications in Computer and Information Science, 2011, , 29-36.	0.4	1
113	A study on hard-core users and bots detection using classification of game character's growth type in online games. Journal of the Korea Institute of Information Security and Cryptology, 2015, 25, 1077-1084.	0.1	1
114	Who Is Sending a Spam Email: Clustering and Characterizing Spamming Hosts. Lecture Notes in Computer Science, 2014, , 469-482.	1.0	0
115	Identification of the Use of Unauthorized Apps in the O2O Service by Combining Online Events and Offline Conditions. Electronics (Switzerland), 2020, 9, 1977.	1.8	0
116	Panop: Mimicry-Resistant ANN-Based Distributed NIDS for IoT Networks. IEEE Access, 2021, 9, 111853-111864.	2.6	0
117	Detecting and Preventing Online Game Bots in MMORPGs. , 2015, , 1-8.		0
118	A research on improving client based detection feature by using server log analysis in FPS games. Journal of the Korea Institute of Information Security and Cryptology, 2015, 25, 1465-1475.	0.1	0