Yu-An Tan

List of Publications by Year
in descending order

51 papers	1,284 citations	331538 21 h-index	360920 35 g-index
52 all docs	52 docs citations	52 times ranked	829 citing authors

#	Article	IF	Citations
1	A fineâ€grained and traceable multidomain secure dataâ€sharing model for intelligent terminals in edgeâ€cloud collaboration scenarios. International Journal of Intelligent Systems, 2022, 37, 2543-2566.	3.3	12
2	Boosting crossâ€task adversarial attack with random blur. International Journal of Intelligent Systems, 2022, 37, 8139-8154.	3.3	4
3	Identity-based Multi-Recipient Public Key Encryption Scheme and Its Application in IoT. Mobile Networks and Applications, 2021, 26, 1543-1550.	2.2	9
4	Hybrid sequenceâ€based Android malware detection using natural language processing. International Journal of Intelligent Systems, 2021, 36, 5770-5784.	3.3	45
5	On-line Firmware Updating and Fingerprint Generating for Solid State Disks. Communications in Computer and Information Science, 2021, , 28-36.	0.4	0
6	Building Covert Timing Channel of the IoT-Enabled MTS Based on Multi-Stage Verification. IEEE Transactions on Intelligent Transportation Systems, 2021, , 1-18.	4.7	7
7	Determining the Image Base of ARM Firmware by Matching Function Addresses. Wireless Communications and Mobile Computing, 2021, 2021, 1-10.	0.8	2
8	Software Misconfiguration Troubleshooting Based on State Analysis. , 2021, , .		0
9	Code Decoupling Execution Isolating Based on TF Card Firmware Extension. , 2021, , .		0
10	An Android Inline Hooking Framework for the Securing Transmitted Data. Sensors, 2020, 20, 4201.	2.1	4
11	A feature-vector generative adversarial network for evading PDF malware classifiers. Information Sciences, 2020, 523, 38-48.	4.0	20
12	An Evolutionary-Based Black-Box Attack to Deep Neural Network Classifiers. Mobile Networks and Applications, 2020, , 1.	2.2	3
13	Determining the Image Base of Smart Device Firmware for Security Analysis. Wireless Communications and Mobile Computing, 2020, 2020, 1-12.	0.8	4
14	Boosting Targeted Black-Box Attacks via Ensemble Substitute Training and Linear Augmentation. Applied Sciences (Switzerland), 2019, 9, 2286.	1.3	19
15	A High-Imperceptibility and Histogram-Shifting Data Hiding Scheme for JPEG Images. IEEE Access, 2019, 7, 73573-73582.	2.6	43
16	Detecting adversarial examples via prediction difference for deep neural networks. Information Sciences, 2019, 501, 182-192.	4.0	33
17	Optimizing the restoration performance of deduplication systems through an energy-saving data layout. Annales Des Telecommunications/Annals of Telecommunications, 2019, 74, 461-471.	1.6	2
18	The security of machine learning in an adversarial setting: A survey. Journal of Parallel and Distributed Computing, 2019, 130, 12-23.	2.7	127

#	Article	IF	Citations
19	Tracing Android Kernel Codes at Early Stage without Extra Hardware Components. , 2019, , .		0
20	A sensitive network jitter measurement for covert timing channels over interactive traffic. Multimedia Tools and Applications, 2019, 78, 3493-3509.	2.6	35
21	A packet-reordering covert channel over VoLTE voice and video traffics. Journal of Network and Computer Applications, 2019, 126, 29-38.	5.8	37
22	Secure Multi-Party Computation: Theory, practice and applications. Information Sciences, 2019, 476, 357-372.	4.0	197
23	A fault-tolerant and energy-efficient continuous data protection system. Journal of Ambient Intelligence and Humanized Computing, 2019, 10, 2945-2954.	3.3	14
24	DPPDL: A Dynamic Partial-Parallel Data Layout for Green Video Surveillance Storage. IEEE Transactions on Circuits and Systems for Video Technology, 2018, 28, 193-205.	5.6	42
25	A Covert Channel Over VoLTE via Adjusting Silence Periods. IEEE Access, 2018, 6, 9292-9302.	2.6	93
26	RootAgency: A digital signature-based root privilege management agency for cloud terminal devices. Information Sciences, 2018, 444, 36-50.	4.0	44
27	A root privilege management scheme with revocable authorization for Android devices. Journal of Network and Computer Applications, 2018, 107, 69-82.	5.8	63
28	A code protection scheme by process memory relocation for android devices. Multimedia Tools and Applications, 2018, 77, 11137-11157.	2.6	17
29	Building covert timing channels by packet rearrangement over mobile networks. Information Sciences, 2018, 445-446, 66-78.	4.0	48
30	Cross-cluster asymmetric group key agreement for wireless sensor networks. Science China Information Sciences, 2018, 61, 1.	2.7	23
31	An optimized data hiding scheme for Deflate codes. Soft Computing, 2018, 22, 4445-4455.	2.1	13
32	Covert Timing Channels for IoT over Mobile Networks. IEEE Wireless Communications, 2018, 25, 38-44.	6.6	33
33	An Efficient Identity-Based Proxy Blind Signature for Semioffline Services. Wireless Communications and Mobile Computing, 2018, 2018, 1-9.	0.8	13
34	Building packet length covert channel over mobile VoIP traffics. Journal of Network and Computer Applications, 2018, 118, 144-153.	5.8	31
35	A payload-dependent packet rearranging covert channel for mobile VoIP traffic. Information Sciences, 2018, 465, 162-173.	4.0	39
36	An Identity-Based Anti-Quantum Privacy-Preserving Blind Authentication in Wireless Sensor Networks. Sensors, 2018, 18, 1663.	2.1	24

#	Article	IF	Citations
37	An end-to-end covert channel via packet dropout for mobile networks. International Journal of Distributed Sensor Networks, 2018, 14, 155014771877956.	1.3	21
38	Cryptographic key protection against FROST for mobile devices. Cluster Computing, 2017, 20, 2393-2402.	3.5	25
39	A round-optimal lattice-based blind signature scheme for cloud services. Future Generation Computer Systems, 2017, 73, 106-114.	4.9	41
40	A methodology for determining the image base of ARM-based industrial control system firmware. International Journal of Critical Infrastructure Protection, 2017, 16, 26-35.	2.9	32
41	Determining Image Base of Firmware Files for ARM Devices. IEICE Transactions on Information and Systems, 2016, E99.D, 351-359.	0.4	18
42	Determining image base of firmware for ARM devices by matching literal pools. Digital Investigation, 2016, 16, 19-28.	3.2	24
43	Descrambling data on solid-state disks by reverse-engineering the firmware. Digital Investigation, 2015, 12, 77-87.	3.2	10
44	Scalable protocol for cross-domain group password-based authenticated key exchange. Frontiers of Computer Science, 2015, 9, 157-169.	1.6	6
45	Buffer Overflow Attacks Defending Using A Segment-based Approach. , 2006, , .		2
46	A High-Throughput Fibre Channel Data Communication Service. , 2005, , .		0
47	A WBEM based disk array management provider. , 2005, , .		2
48	A Segment-based Approach of Defending Against Buffer Overflow Attacks. , 2005, , .		1
49	Design and Implementation of a WBEM Disk Array Provider. , 2005, , .		0
50	Buffer overflow protection based on adjusting code segment limit. , 0, , .		0
51	A blockchain-based access control protocol for secure resource sharing with mobile edge-cloud collaboration. Journal of Ambient Intelligence and Humanized Computing, 0, , .	3.3	1