Securing Android

ACM Computing Surveys 47, 1-45 DOI: 10.1145/2733306

Citation Report

Ст	DΤ

#	Article	IF	CITATIONS
1	Survey on Privacy Protection of Android Devices. , 2015, , .		14
2	Privacy and security constraints for code contributions. , 2015, , .		0
3	Accurate mobile malware detection and classification in the cloud. SpringerPlus, 2015, 4, 583.	1.2	27
4	Accurate Specification for Robust Detection of Malicious Behavior in Mobile Environments. Lecture Notes in Computer Science, 2015, , 355-375.	1.3	1
5	Detection and Visualization of Android Malware Behavior. Journal of Electrical and Computer Engineering, 2016, 2016, 1-17.	0.9	25
6	Reviving Android Malware with DroidRide: And How Not To. , 2016, , .		0
7	A Cloud-Assisted Malware Detection Framework for Mobile Devices. , 2016, , .		5
8	Exploring the Usage of Topic Modeling for Android Malware Static Analysis. , 2016, , .		9
9	HybriDroid: static analysis framework for Android hybrid applications. , 2016, , .		48
10	Fingerprinting Android packaging: Generating DNAs for malware detection. Digital Investigation, 2016, 18, S33-S45.	3.2	28
11	Mystique. , 2016, , .		42
12	*droid. ACM Computing Surveys, 2017, 49, 1-30.	23.0	51
13	The Evolution of Android Malware and Android Analysis Techniques. ACM Computing Surveys, 2017, 49, 1-41.	23.0	251
14	Security and Privacy in Device-to-Device (D2D) Communication: A Review. IEEE Communications Surveys and Tutorials, 2017, 19, 1054-1079.	39.4	237
15	Cryptographic key protection against FROST for mobile devices. Cluster Computing, 2017, 20, 2393-2402.	5.0	25
16	A survey on ultra-dense network and emerging technologies: Security challenges and possible solutions. Journal of Network and Computer Applications, 2017, 95, 54-78.	9.1	47
17	Android inter-app communication threats and detection techniques. Computers and Security, 2017, 70, 392-421.	6.0	29
18	Understanding Android Application Programming and Security: A Dynamic Study. , 2017, , .		18

ARTICLE IF CITATIONS # Exception beyond Exception: Crashing Android System by Trapping in "Uncaught Exception"., 2017,,. 10 19 DroidFax: A Toolkit for Systematic Characterization of Android Applications., 2017, , . RootAgency: A digital signature-based root privilege management agency for cloud terminal devices. 22 6.9 44 Information Sciences, 2018, 444, 36-50. Forensic analysis and security assessment of Android m-banking apps. Australian Journal of Forensic Sciences, 2018, 50, 3-19. Circumventing iOS security mechanisms for APT forensic investigations: A security taxonomy for 24 7.5 29 cloud apps. Future Generation Computer Systems, 2018, 79, 247-261. A survey on dynamic mobile malware detection. Software Quality Journal, 2018, 26, 891-919. 2.2 94 Machine-Learning-Based Android Malware Detection Techniquesâ€"A Comparative Analysis. Lecture 26 0.7 5 Notes in Networks and Systems, 2018, , 181-190. Analyzing the analyzers: FlowDroid/IccTA, AmanDroid, and DroidSafe., 2018, , . 28 A Context-Perceptual Privacy Protection Approach on Android Devices., 2018,,. 1 Understanding Android Financial MalwareAttacks:Taxonomy, Characterization, and Challenges. 29 Journal of Cyber Security and Mobility, 2018, 7, 1-52. An Insight into Android Side-Channel Attacks., 2018,,. 30 1 Systematically Understanding the Cyber Attack Business. ACM Computing Surveys, 2019, 51, 1-36. 59 Idea: Benchmarking Android Data Leak Detection Tools. Lecture Notes in Computer Science, 2018, 32 1.3 6 116-123. Protecting contacts against privacy leaks in smartphones. PLoS ONE, 2018, 13, e0191502. 2.5 34 A temporal permission analysis and enforcement framework for Android., 2018,,. 23 NDroid: Toward Tracking Information Flows Across Multiple Android Contexts. IEEE Transactions on 6.9 Information Forensics and Security, 2019, 14, 814-828. BridgeTaint: A Bi-Directional Dynamic Taint Tracking Method for JavaScript Bridges in Android Hybrid 36 6.9 9 Applications. IEEE Transactions on Information Forensics and Security, 2019, 14, 677-692. On the Deterioration of Learning-Based Malware Detectors for Android., 2019,,.

CITATION REPORT

		CITATION REPORT		
#	Article	IF		CITATIONS
38	A Characterization of Digital Native Approaches To Mobile Privacy and Security. , 2019, , .			2
39	An Empirical Study of Cross-Platform Mobile Development in Industry. Wireless Communications Mobile Computing, 2019, 2019, 1-12.	and 1.2	2	22
40	The Android OS stack and its vulnerabilities: an empirical study. Empirical Software Engineering, 2 24, 2056-2101.	019, 3.9	¢	16
41	SeMA: A Design Methodology for Building Secure Android Apps. , 2019, , .			1
42	Android Malware Similarity Clustering using Method based Opcode Sequence and Jaccard Index. , , , ,	2019,		3
43	A scalable and extensible framework for android malware detection and family attribution. Computers and Security, 2019, 80, 120-133.	6.0	0	40
44	A formal framework for software faults and permissions based on unified theory of programming. Cluster Computing, 2019, 22, 14049-14059.	5.0	0	1
45	Android data storage security: A review. Journal of King Saud University - Computer and Informatic Sciences, 2020, 32, 543-552.	on 3.9	Ð	21
46	Are free Android app security analysis tools effective in detecting known vulnerabilities?. Empirica Software Engineering, 2020, 25, 178-219.	3.9	9	22
47	A Taxonomy for Security Flaws in Event-Based Systems. Applied Sciences (Switzerland), 2020, 10,	7338. 2.8	5	2
48	DroidXP: A Benchmark for Supporting the Research on Mining Android Sandboxes. , 2020, , .			1
49	Code analysis for intelligent cyber systems: A data-driven approach. Information Sciences, 2020, 5 46-58.	24, 6.9	9	25
50	A Longitudinal Study of Application Structure and Behaviors in Android. IEEE Transactions on Software Engineering, 2021, 47, 2934-2955.	5.0	6	28
51	A study of run-time behavioral evolution of benign versus malicious apps in android. Information a Software Technology, 2020, 122, 106291.	nd 4.4	4	37
52	Android security assessment: A review, taxonomy and research gap study. Computers and Securit 2021, 100, 102087.	y, 6.0	0	13
53	Research on Third-Party Libraries in Android Apps: A Taxonomy and Systematic Literature Review. Transactions on Software Engineering, 2022, 48, 4181-4213.	EEE 5.0	5	11
55	Analyzing Android Taint Analysis Tools: FlowDroid, Amandroid, and DroidSafe. IEEE Transactions o Software Engineering, 2022, 48, 4014-4040.	n 5.6	5	3
57	A survey on analysis and detection of Android ransomware. Concurrency Computation Practice ar Experience, 2021, 33, e6272.	d 2.2	2	21

#	Article	IF	CITATIONS
58	Malicious application detection in android — A systematic literature review. Computer Science Review, 2021, 40, 100373.	15.3	31
59	On the Interplay Between Static and Dynamic Analysis for Mining Sandboxes. , 2021, , .		Ο

CITATION REPORT

Malware detection using static analysis in Android: a review of FeCO (features, classification, and) Tj ETQq0 0 0 rgBT /Overlock 10 Tf 50 $\frac{4.5}{15}$

61	Exploring the use of static and dynamic analysis to improve the performance of the mining sandbox approach for android malware identification. Journal of Systems and Software, 2022, 183, 111092.	4.5	5
62	Position Paper on Recent Cybersecurity Trends: Legal Issues, Al and IoT. Lecture Notes in Computer Science, 2018, , 484-490.	1.3	1
63	Assessing and Improving Malware Detection Sustainability through App Evolution Studies. ACM Transactions on Software Engineering and Methodology, 2020, 29, 1-28.	6.0	72
64	DroidMark: A Lightweight Android Text and Space Watermark Scheme Based on Semantics of XML and DEX. Lecture Notes on Data Engineering and Communications Technologies, 2018, , 756-766.	0.7	0
65	Information Disclosure Detection in Cyber-Physical Systems. Communications in Computer and Information Science, 2019, , 85-94.	0.5	1
66	Where Are We Looking for Security Concerns? Understanding Android Security Static Analysis. Advances in Intelligent Systems and Computing, 2020, , 467-483.	0.6	0
67	Dynamic Taint Tracking Simulation. Communications in Computer and Information Science, 2020, , 203-227.	0.5	0
68	Feature Point Detection for Repacked Android Apps. Intelligent Automation and Soft Computing, 2020, 26, 1359-1373.	2.1	11
69	Embracing mobile app evolution via continuous ecosystem mining and characterization. , 2020, , .		17
70	The Effect of Context on Small Screen and Wearable Device Users' Performance - A Systematic Review. ACM Computing Surveys, 2021, 53, 1-44.	23.0	7
71	CryptoTutor. , 2020, , .		8
72	Learning Latent Correlation of Heterogeneous Sensors Using Attention based Temporal Convolutional Network. , 2020, , .		0
73	Taxonomy of security weaknesses in Java and Kotlin Android apps. Journal of Systems and Software, 2022, 187, 111233.	4.5	9
74	The rise of obfuscated Android malware and impacts on detection methods. PeerJ Computer Science, 2022, 8, e907.	4.5	9
75	A Comprehensive Review of Android Security: Threats, Vulnerabilities, Malware Detection, and Analysis. Security and Communication Networks, 2022, 2022, 1-34.	1.5	7

#	Article	IF	CITATIONS
76	FSAFlow: Lightweight and Fast Dynamic Path Tracking and Control for Privacy Protection on Android Using Hybrid Analysis with State-Reduction Strategy. , 2022, , .		1
77	ADAM: Automatic Detection ofÂAndroid Malware. Lecture Notes in Computer Science, 2022, , 18-31.	1.3	0
78	Towards a fair comparison and realistic evaluation framework of android malware detectors based on static analysis and machine learning. Computers and Security, 2023, 124, 102996.	6.0	10
79	Large-scale analysis of non-termination bugs in real-world OSS projects. , 2022, , .		3
80	Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. Technologies, 2023, 11, 76.	5.1	4
81	A Survey and Evaluation of Android-Based Malware Evasion Techniques and Detection Frameworks. Information (Switzerland), 2023, 14, 374.	2.9	2
82	Android Malware Detection Based onÂStatic Analysis andÂData Mining Techniques: A Systematic Literature Review. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2023, , 51-71.	0.3	0
83	A Small Leak Will Sink Many Ships: Vulnerabilities Related to mini-programs Permissions. , 2023, , .		1
84	Detection approaches for android malware: Taxonomy and review analysis. Expert Systems With Applications, 2024, 238, 122255.	7.6	2
85	Artificial Neural Network-Based Malware Detection Model Among Shopping Apps to Increase the App Security. Smart Innovation, Systems and Technologies, 2023, , 267-275.	0.6	0
86	Exploring the Effectiveness of Machine and Deep Learning Techniques for Android Malware Detection. , 2024, , 1-10.		0
87	On Running Disabled Networking Features: A Taxonomy with Security Implications. , 2024, , .		0

CITATION REPORT