CISPA
Center for IT-Security, Privacy and Accountability

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Saarland University
Trusted Systems Group
Dr.-Ing. Sven Bugiel

Android Security SS 2016

References

Dr.-Ing. Sven Bugiel

References

[1] B. Lau, Y. Jang, C. Song, T. Wang, P. H. Chung, and P. Royal, "Mactans: Injecting malware into iOS devices via malicious chargers." `https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf`, 2013. BlackHat US.

[2] D. Perez and J. Pico, "A pracitcal attack against gprs/edge/umts/hspa mobile data communications." `https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf`. BlackHat DC.

[3] R.-P. Weinmann, "Baseband attacks: Remote exploitation of memory corruptions in cellular protocol stacks," in *Proc. 6th USENIX Workshop on Offensive Technologies (WOOT 2012)*, 2012.

[4] C. Mulliner, N. Golde, and J.-P. Seifert, "Sms of death: From analyzing to attacking mobile phones on a large scale," in *Proc. 20th USENIX Security Symposium (SEC'11)*, USENIX Association, 2011.

[5] A. Porter Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proc. 1st ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'11)*, ACM, 2011.

[6] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in *Proc. 33rd IEEE Symposium on Security and Privacy (SP'12)*, 2012.

[7] Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. McDaniel, and M. Smith, "SoK: Lessons Learned From Android Security Research For Appified Software Platforms," in *37th IEEE Symposium on Security and Privacy (SP '16)*, IEEE, 2016.

[8] B. W. Lampson, "Protection," *ACM SIGOPS Operating Systems Review*, vol. 8, pp. 18–24, Jan. 1974.

[9] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, you, get off of my market: Detecting malicious apps in official and alternative Android markets," in *Proc. 19th Annual Network & Distributed System Security Symposium (NDSS'12)*, The Internet Society, 2012.

[10] W. Zhou, Y. Zhou, M. Grace, X. Jiang, and S. Zou, "Fast, scalable detection of "piggybacked" mobile applications," in *3rd ACM conference on Data and application security and privacy (CODASPY'13)*, pp. 185–196, ACM, 2013.

[11] C. Gibler, R. Stevens, J. Crussell, H. Chen, H. Zang, and H. Choi, "Adrob: Examining the landscape and impact of android application plagiarism," in *Proc. 11th International Conference on Mobile Systems, Applications, and Services (MobiSys'13)*, ACM, 2013.

[12] W. Zhou, Y. Zhou, X. Jiang, and P. Ning, "Detecting repackaged smartphone applications in third-party android marketplaces," in *Proc. 2nd ACM Conference on Data and Application Security and Privacy (CODASPY'12)*, ACM, 2012.

[13] J. Crussell, C. Gibler, and H. Chen, "Attack of the clones: Detecting cloned applications on android markets," in *Proc. 17th European Symposium on Research in Computer Security (ESORICS '12)*, Springer, 2012.

[14] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proc. 8th Symposium on Usable Privacy and Security (SOUPS'12)*, ACM, 2012.

[15] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android permissions remystified: A field study on contextual integrity," in *Proc. 24th USENIX Security Symposium (SEC'15)*, USENIX Association, 2015.

[16] A. Porter Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proc. 18th ACM Conference on Computer and Communication Security (CCS '11)*, ACM, 2011.

[17] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, "Pscout: analyzing the android permission specification," in *Proc. 19th ACM Conference on Computer and Communication Security (CCS '12)*, ACM, 2012.

[18] M. Backes, S. Bugiel, E. Derr, P. McDaniel, D. Octeau, and S. Weisgerber, "On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis," in *Proc. 25th USENIX Security Symposium (SEC'16)*, USENIX Association, 2016.

[19] E. Chin, A. Porter Felt, K. Greenwood, and D. Wagner, "Analyzing inter-application communication in Android," in *MobiSys'11*, ACM, 2011.

[20] M. Backes, S. Bugiel, and S. Gerling, "Scippa: System-centric ipc provenance on android," in *Proc. 30th Annual Computer Security Applications Conference (ACSAC'14)*, ACM, 2014.

[21] Y. Aafer, X. Zhang, and W. Du, "Harvesting inconsistent security configurations in custom android roms via differential analysis," in *Proc. 25th USENIX Security Symposium (SEC'16)*, USENIX Association, 2016.

[22] H. Bagheri, E. Kang, S. Malek, and D. Jackson, "Detection of design flaws in the android permission protocol through bounded verification," in *20th International Symposium on Formal Methods (FM'15)*, Springer, 2015.

[23] Y. Shao, J. Ott, Q. A. Chen, Z. Qian, and Z. M. Mao, "Kratos: Discovering inconsistent security policy enforcement in the android framework," in *Proc. 23rd Annual Network & Distributed System Security Symposium (NDSS '16)*, The Internet Society, 2016.

[24] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," in *Proc. 16th ACM Conference on Computer and Communication Security (CCS '09)*, ACM, 2009.

[25] A. Porter Felt, H. J. Wang, A. Moshchuk, S. Hanna, and E. Chin, "Permission re-delegation: Attacks and defenses," in *Proc. 20th USENIX Security Symposium (SEC'11)*, USENIX Association, 2011.

[26] A. Lineberry, D. L. Richardson, and T. Wyatt, "These aren't the permissions you're looking for." `http://dtors.files.wordpress.com/2010/08/blackhat-2010-slides.pdf`, 2010. DefCon 18.

[27] Y. Zhou and X. Jiang, "Detecting passive content leaks and pollution in Android applications," in *Proc. 20th Annual Network & Distributed System Security Symposium (NDSS'13)*, The Internet Society, 2013.

[28] L. Wu, M. Grace, Y. Zhou, C. Wu, and X. Jiang, "The impact of vendor customizations on android security," in *Proc. 20th ACM Conference on Computer and Communication Security (CCS '13)*, ACM, 2013.

[29] X. Zhou, Y. Lee, N. Zhang, M. Naveed, and X. Wang, "The peril of fragmentation: Security hazards in android device driver customizations," in *Proc. 35th IEEE Symposium on Security and Privacy (SP'14)*, IEEE Computer Society, 2014.

[30] A. Moulo, "Android OEM's applications (in)security and backdoors without permission." `http://www.quarkslab.com/dl/Android-OEM-applications-insecurity-and-backdoors-without-permission.pdf`.

[31] S. Fahl, M. Harbach, M. Oltrogge, T. Muders, and M. Smith, "Hey, you, get off of my clipboard - on how usability trumps security in android password managers," in *Financial Cryptography (FC)*, 2013.

[32] R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A stealthy and context-aware sound trojan for smartphones," in *Proc. 18th Annual Network and Distributed System Security Symposium (NDSS '11)*, The Internet Society, 2011.

[33] S. Poeplau, Y. Fratantonio, A. Bianchi, C. Kruegel, and G. Vigna, "Execute this! analyzing unsafe and malicious dynamic code loading in android applications," in *Proc. 21st Annual Network and Distributed System Security Symposium (NDSS'14)*, The Internet Society, 2014.

[34] L. Xing, X. Pan, R. Wang, K. Yuan, and X. Wang, "Upgrading your android, elevating my malware: Privilege escalation through mobile os updating," in *Proc. 35th IEEE Symposium on Security and Privacy (SP'14)*, IEEE Computer Society, 2014.

[35] M. Niemietz and J. Schwenk, "Ui redressing attacks on android devices," 2012. BlackHat Asia.

[36] R. Templeman, Z. Rahman, D. Crandall, and A. Kapadia, "Placeraider: Virtual theft in physical spaces with smartphones," in *Proc. 20th Annual Network & Distributed System Security Symposium (NDSS'13)*, The Internet Society, 2013.

[37] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp)iphone: decoding vibrations from nearby keyboards using mobile phone accelerometers," in *Proc. 18th ACM Conference on Computer and Communication Security (CCS '11)*, ACM, 2011.

[38] Z. Wang and A. Stavrou, "Exploiting smart-phone usb connectivity for fun and profit," in *26th Annual Computer Security Applications Conference (ACSAC'10)*, ACM, 2010.

[39] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 4th USENIX Workshop on Offensive Technologies (WOOT 2010)*, USENIX Association, 2010.

[40] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of android unlock patterns," in *ACM Conference on Computer & Communications Security (CCS'13)*, ACM, 2013.

[41] Q. A. Chen, Z. Qian, and Z. M. Mao, "Peeking into your app without actually seeing it: Ui state inference and novel android attacks," in *Proc. 23rd USENIX Security Symposium (SEC'14)*, USENIX Association, 2014.

[42] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing speech from gyroscope signals," in *Proc. 23rd USENIX Security Symposium (SEC'14)*, USENIX Association, 2014.

[43] Z. Xu, K. Bai, and S. Zhu, "Taplogger: inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proc. 5th ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC'12)*, ACM, 2012.

[44] L. Cai and H. Chen, "Touchlogger: inferring keystrokes on touch screen from smartphone motion," in *6th USENIX conference on Hot topics in security (HotSec'11)*, USENIX Association, 2011.

[45] S. Fahl, M. Harbach, T. Muders, L. Baumgärtner, B. Freisleben, and M. Smith, "Why eve and mallory love android: an analysis of android ssl (in)security," in *Proc. 19th ACM Conference on Computer and Communication Security (CCS '12)*, ACM, 2012.

[46] S. Fahl, M. Harbach, H. Perl, M. Koetter, and M. Smith, "Rethinking SSL development in an appified world," in *Proc. 20th ACM Conference on Computer and Communication Security (CCS '13)*, ACM, 2013.

[47] T. Luo, H. Hao, W. Du, Y. Wang, and H. Yin, "Attacks on WebView in the Android system," in *Proc. 27th Annual Computer Security Applications Conference (ACSAC'11)*, ACM, 2011.

[48] V. S. Martin Georgiev, Suman Jana, "Breaking and fixing origin-based access control in hybrid web/mobile application frameworks," in *Proc. 21st Annual Network and Distributed System Security Symposium (NDSS'14)*, The Internet Society, 2014.

[49] P. Mutchler, A. Doupé, J. Mitchell, C. Kruegel, and G. Vigna, "A Large-Scale Study of Mobile Web App Security," in *Proc. 2015 Mobile Security Technologies Workshop (MoST'15)*, IEEE Computer Society, 2015.

[50] R. Wang, L. Xing, X. Wang, and S. Chen, "Unauthorized origin crossing on mobile platforms: Threats and mitigation," in *Proc. 20th ACM Conference on Computer and Communication Security (CCS '13)*, ACM, 2013.

[51] E. Y. Chen, Y. Pei, S. Chen, Y. Tian, R. Kotcher, and P. Tague, "Oauth demystified for mobile application developers," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[52] X. Jin, X. Hu, K. Ying, W. Du, H. Yin, and G. N. Peri, "Code injection attacks on html5-based mobile apps: Characterization, detection and mitigation," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[53] J. Chen, H. Chen, E. Bauman, Z. Lin, B. Zang, and H. Guan, "You shouldn't collect my secrets: Thwarting sensitive keystroke leakage in mobile ime apps," in *Proc. 24th USENIX Security Symposium (SEC'15)*, USENIX Association, 2015.

[54] D. Sounthiraraj, J. Sahs, G. Greenwood, Z. Lin, and L. Khan, "Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps," in *Proc. 21st Annual Network and Distributed System Security Symposium (NDSS'14)*, The Internet Society, 2014.

[55] V. Rastogi, Y. Chen, and X. Jiang, "DroidChameleon: evaluating Android anti-malware against transformation attacks," in *Proc. 8th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '13)*, ACM, 2013.

[56] C. Marforio, H. Ritzdorf, A. Francillon, and S. Capkun, "Analysis of the communication between colluding applications on modern smartphones," in *Proc. 28th Annual Computer Security Applications Conference (ACSAC'12)*, ACM, 2012.

[57] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, "A conundrum of permissions: Installing applications on an android smartphone," in *Proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC'12)*, Springer, 2012.

[58] M. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi, "Unsafe exposure analysis of mobile in-app advertisements," in *Proc. 5th ACM conference on Security and Privacy in Wireless and Mobile Networks (WISEC'12)*, ACM, 2012.

[59] R. Stevens, C. Gibler, J. Crussell, J. Erickson, and H. Chen, "Investigating user privacy in android ad libraries," in *Proc. 2012 Mobile Security Technologies Workshop (MoST'12)*, IEEE Computer Society, 2012.

[60] S. Demetriou, W. Merrill, W. Yang, A. Zhang, and C. A. Gunter, "Free for all! assessing user data exposure to advertising libraries on android," in *Proc. 23rd Annual Network & Distributed System Security Symposium (NDSS '16)*, The Internet Society, 2016.

[61] S. Son, G. Daehyeok, K. Kaist, and V. Shmatikov, "What mobile ads know about mobile users," in *Proc. 23rd Annual Network & Distributed System Security Symposium (NDSS '16)*, The Internet Society, 2016.

[62] M. Backes, S. Bugiel, and E. Derr, "Reliable third-party library detection in android and its security applications," in *Proc. 23rd ACM Conference on Computer and Communication Security (CCS'16)*, ACM, 2016.

[63] V. Rastogi, R. Shao, Y. Chen, X. Pan, S. Zou, and R. Riley, "Are these ads safe: Detecting hidden attacks through the mobile app-web interfaces," in *Proc. 23rd Annual Network & Distributed System Security Symposium (NDSS '16)*, The Internet Society, 2016.

[64] Y. Jang, C. Song, S. P. Chung, T. Wang, and W. Lee, "A11y attacks: Exploiting accessibility in operating systems," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[65] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V. Shmatikov, "The most dangerous code in the world: validating SSL certificates in non-browser software," in *Proc. 19th ACM Conference on Computer and Communication Security (CCS '12)*, ACM, 2012.

[66] M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel, "An empirical study of cryptographic misuse in android applications," in *Proc. 20th ACM Conference on Computer and Communication Security (CCS '13)*, ACM, 2013.

[67] Y. Song and U. Hengartner, "Privacyguard: A vpn-based platform to detect information leakage on android devices," in *Proc. 5th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'15)*, ACM, 2015.

[68] K. Chen, P. Wang, Y. Lee, X. Wang, N. Zhang, H. Huang, W. Zou, and P. Liu, "Finding unknown malice in 10 seconds: Mass vetting for new threats at the google-play scale," in *Proc. 24th USENIX Security Symposium (SEC'15)*, USENIX Association, 2015.

[69] Google, "Android Security: 2015 Year in review," Apr. 2015.

[70] D. Arp, M. Spreitzenbarth, M. H. H. Gascon, and K. Rieck, "Drebin: Effective and explainable detection of android malware in your pocket," in *Proc. 21st Annual Network and Distributed System Security Symposium (NDSS'14)*, The Internet Society, 2014.

[71] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, "Riskranker: scalable and accurate zero-day android malware detection," in *Proc. 10th International Conference on Mobile systems, Applications, and Services (MobiSys'12)*, ACM, 2012.

[72] S. Chakradeo, B. Reaves, P. Traynor, and W. Enck, "Mast: Triage for market-scale mobile malware analysis," in *Proc. 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'13)*, ACM, 2013.

[73] A. Gorla, I. Tavecchia, F. Gross, and A. Zeller, "Checking app behavior against app descriptions," in *Proc. 36th IEEE International Conference on Software Engineering (ICSE'14)*, ACM, 2014.

[74] R. Pandita, X. Xiao, W. Yang, W. Enck, and T. Xie, "WHYPER: towards automating risk assessment of mobile applications," in *Proc. 22nd USENIX Security Symposium (SEC '13)*, 2013.

[75] Z. Qu, V. Rastogi, X. Zhang, Y. Chen, T. Zhu, and Z. Chen, "Autocog: Measuring the description-to-permission fidelity in android applications," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[76] M. Zhang, Y. Duan, Q. Feng, and H. Yin, "Towards automatic generation of security-centric descriptions for android apps," in *Proc. 22nd ACM Conference on Computer and Communication Security (CCS'15)*, ACM, 2015.

[77] M. D. Ernst, R. Just, S. Millstein, W. Dietl, S. Pernsteiner, F. Roesner, K. Koscher, P. B. Barros, R. Bhoraskar, S. Han, P. Vines, and E. X. Wu, "Collaborative verification of information flow for a high-assurance app store," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[78] L. Lu, Z. Li, Z. Wu, W. Lee, and G. Jiang, "Chex: statically vetting android apps for component hijacking vulnerabilities," in *Proc. 19th ACM Conference on Computer and Communication Security (CCS '12)*, ACM, 2012.

[79] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. le Traon, D. Octeau, and P. McDaniel, "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for Android apps," in *Proc. ACM SIGPLAN 2014 Conference on Programming Language Design and Implementation (PLDI'14)*, ACM, 2014.

[80] D. Octeau, P. McDaniel, S. Jha, A. Bartel, E. Bodden, J. Klein, and Y. L. Traon, "Effective inter-component communication mapping in android: An essential step towards holistic security analysis," in *Proc. 22nd USENIX Security Symposium (SEC '13)*, USENIX Association, 2013.

[81] F. Wei, S. Roy, X. Ou, and Robby, "Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[82] L. Li, A. Bartel, T. Bissyande, J. Klein, Y. Le Traon, S. Arzt, S. Rasthofer, E. Bodden, D. Octeau, and P. McDaniel, "Iccta: Detecting inter-component privacy leaks in android apps," in *Proc. 37th IEEE International Conference on Software Engineering (ICSE'15)*, IEEE Computer Society, 2015.

[83] Y. Caox, Y. Fratantonioy, A. Bianchiy, M. E. andChristopher Kruegely, G. Vigna, and Y. Chen, "EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework," in *Proc. 22nd Annual Network and Distributed System Security Symposium (NDSS'15)*, The Internet Society, 2015.

[84] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in *OSDI'10*, USENIX Association, 2010.

[85] Y. Zhang, M. Yang, B. Xu, Z. Yang, G. Gu, P. Ning, X. S. Wang, and B. Zang, "Vetting undesirable behaviors in android apps with permission use analysis," in *Proc. 20th ACM Conference on Computer and Communication Security (CCS '13)*, ACM, 2013.

[86] L. K. Yan and H. Yin, "Droidscope: Seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis," in *Proc. 21st USENIX Security Symposium (SEC'12)*, USENIX Association, 2012.

[87] C. Zheng, S. Zhu, S. Dai, G. Gu, X. Gong, X. Han, and W. Zou, "Smartdroid: An automatic system for revealing ui-based trigger conditions in android applications," in *Proc. 2nd ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'12)*, ACM, 2012.

[88] V. Rastogi, Y. Chen, and W. Enck, "Appsplayground: Automatic security analysis of smartphone applications," in *Proc. 3rd ACM Conference on Data and Application Security and Privacy (CODASPY'13)*, ACM, 2013.

[89] K. Tam, S. J. Khan, A. Fattoriy, and L. Cavallaro, "CopperDroid: Automatic Reconstruction of Android Malware Behaviors," in *Proc. 22nd Annual Network and Distributed System Security Symposium (NDSS'15)*, The Internet Society, 2015.

[90] K. Jamrozik and A. Zeller, "Droidmate: A robust and extensible test generator for android," in *Pro. International Conference on Mobile Software Engineering and Systems (MOBILESoft '16)*, ACM, 2016.

[91] K. Jamrozik, P. von Styp-Rekowsky, and A. Zeller, "Mining sandboxes," in *Proc. 38th IEEE International Conference on Software Engineering (ICSE'16)*, ACM, 2016.

[92] R. Bhoraskar, S. Han, J. Jeon, T. Azim, S. Chen, J. Jung, S. Nath, R. Wang, and D. Wetherall, "Brahmastra: Driving apps to test the security of third-party components," in *Proc. 23rd USENIX Security Symposium (SEC'14)*, USENIX Association, 2014.

[93] M. Xia, L. Gong, Y. Lyu, Z. Qi, and X. Liu, "Effective real-time android application auditing," in *Proc. 36th IEEE Symposium on Security and Privacy (SP'15)*, IEEE Computer Society, 2015.

[94] W. Yang, X. Xiao, B. Andow, S. Li, T. Xie, and W. Enck, "Appcontext: Differentiating malicious and benign mobile app behaviors using context," in *Proc. 37th IEEE International Conference on Software Engineering (ICSE'15)*, IEEE Computer Society, 2015.

[95] S. Rasthofer, S. Arzt, M. Miltenberger, and E. Bodden, "Harvesting runtime values in android applications that feature anti-analysis techniques," in *Proc. 23rd Annual Network & Distributed System Security Symposium (NDSS '16)*, The Internet Society, 2016.

[96] Y. Fratantonio, A. Bianchi, W. Robertson, E. Kirda, C. Kruegel, and G. Vigna, "TriggerScope: Towards Detecting Logic Bombs in Android Apps," in *Proc. 37th IEEE Symposium on Security and Privacy (SP'16)*, May 2016.

[97] D. Barrera, W. Enck, and P. C. V. Oorschot, "Meteor: Seeding a security-enhancing infrastructure for multi-market application ecosystems," in *Proc. 2012 Mobile Security Technologies Workshop (MoST'12)*, IEEE Computer Society, 2012.

[98] S. Fahl, S. Dechand, H. Perl, F. Fischer, J. Smrcek, and M. Smith, "Hey, NSA: Stay Away from my Market! Future Proofing App Markets against Powerful Attackers," in *Proc. 21st ACM Conference on Computer and Communication Security (CCS'14)*, ACM, 2014.

[99] M. Backes, S. Gerling, C. Hammer, M. Maffei, and P. von Styp-Rekowsky, "Appguard - enforcing user requirements on Android apps," in *TACAS'13*, 2013.

[100] R. Xu, H. Saïdi, and R. Anderson, "Aurasium: Practical policy enforcement for Android applications," in *Proc. 21st USENIX Security Symposium (SEC'12)*, USENIX Association, 2012.

[101] B. Davis, B. Sanders, A. Khodaverdian, and H. Chen, "I-arm-droid: A rewriting framework for in-app reference monitors for android applications," in *Proc. 2012 Mobile Security Technologies Workshop (MoST'12)*, IEEE, 2012.

[102] B. Davis and H. Chen, "Retroskeleton: Retrofitting android apps," in *Proc. 11th International Conference on Mobile Systems, Applications, and Services (MobiSys'13)*, ACM, 2013.

[103] S. Rasthofer, S. Arzt, E. Lovat, and E. Bodden, "Droidforce: Enforcing complex, data-centric, system-wide policies in android," in *Proc. 9th International Conference on Availability, Reliability and Security (ARES'14)*, IEEE Computer Society, 2014.

[104] M. Zhang and H. Yin, "Appsealer: Automatic generation of vulnerability-specific patches for preventing component hijacking attacks in android applications," in *Proc. 21st Annual Network and Distributed System Security Symposium (NDSS'14)*, The Internet Society, 2014.

[105] M. Zhang and H. Yin, "Efficient, context-aware privacy leakage confinement for android applications without firmware modding," in *Proc. 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS '14')*, ACM, 2014.

[106] X. Wangy, K. Sun, Y. Wang, and J. Jing, "DeepDroid: Dynamically Enforcing Enterprise Policy on Android Devices," in *Proc. 22nd Annual Network and Distributed System Security Symposium (NDSS'15)*, The Internet Society, 2015.

[107] C. Mulliner, J. Oberheide, W. Robertson, and E. Kirda, "Patchdroid: Scalable third-party security patches for android devices," in *Proc. 29th Annual Computer Security Applications Conference (ACSAC'13)*, ACM, 2013.

[108] M. Backes, S. Bugiel, C. Hammer, O. Schranz, and P. von Styp-Rekowsky, "Boxify: Full-fledged app sandboxing for stock android," in *Proc. 24th USENIX Security Symposium (SEC'15)*, USENIX Association, 2015.

[109] A. Bianchi, Y. Fratantonio, C. Kruegel, and G. Vigna, "Njas: Sandboxing unmodified applications in non-rooted devices running stock android," in *Proc. 5th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'15)*, ACM, 2015.