Saarland University
Information Security & Cryptography Group
Prof. Dr. Michael Backes

Android Security Lab WS 2013/14

References

M.Sc. Sven Bugiel

References

[1] W. Enck, M. Ongtang, and P. Mcdaniel, "Mitigating android software misuse before it happens," Technical Report NAS-TR-0094-2008, Pennsylvania State University, September 2008.

[2] 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.

[3] 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.

[4] 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.

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

[6] L. Davi, A. Dmitrienko, C. Liebchen, and A.-R. Sadeghi, "Over-the-air cross-platform infection for breaking mTAN-based online banking authentication," 2012. BlackHat Abu Dhabi.

[7] 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.

[8] 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.

[9] 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 Mobile Devices (SPSM'11)*, ACM, 2011.

[10] C. Lever, M. Antonakakis, B. Reaves, P. Traynor, and W. Lee, "The core of the matter: Analyzing malicious traffic in cellular carriers," in *Proc. 20th Annual Network & Distributed System Security Symposium (NDSS'13)*, The Internet Society, 2013.

[11] 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)*, Feb. 2012.

[12] 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.

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

[14] L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy, "Privilege escalation attacks on android," in *Proc. 13th Information Security Conference (ISC '10)*, Springer, 2010.

[15] S. Bugiel, L. Davi, A. Dmitrienko, S. Heuser, A.-R. Sadeghi, and B. Shastry, "Practical and lightweight domain isolation on Android," in *Proc. 1st ACM CCS Workshop on Security and Privacy in Mobile Devices (SPSM'11)*, ACM, 2011.

[16] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies," in *Proc. 22nd USENIX Security Symposium (SEC'13)*, USENIX Association, 2013.

[17] 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`.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

[33] 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.

[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] 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.

[36] 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.

[37] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "These aren't the droids you're looking for: Retrofitting Android to protect data from imperious applications," in *Proc. 18th ACM Conference on Computer and Communication Security (CCS '11)*, ACM, 2011.

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