传感器进行访问控制是一种可行的侧信道防御方案.Conti 等人[16]提出了一种基于上下文的访问控制机制,该机制可以将用户从人工设置访问权限中释放出来,但是他们所实现的机制需要对已有的操作系统进行复杂的修改,而本文提出的方法只需要在框架层中嵌入少量程序.此外,限制访问控制机制实际应用的最大问题在于无法防御来自具有合法权限的 APP 所进行的侧信道攻击,相比之下,本文方法对应用层程序实现无差别防御.文献[14]和文献[15]提出,通过强制降低传感器采样频率或禁止传感器运行的方式防御传感器侧信道攻击.然而,这种行为对于非恶意应用的影响非常严重,许多 APP,例如射击游戏等,需要较高的采样频率以达到用户满意的运行效果.我们的防御方案能够在进行有效防御的同时,保证合法应用的正常运行.

Shrestha 等人[18]在用户输入敏感信息的过程中向传感器读数中注入强烈噪声的方式完全破坏传感器读数,然而该方案不但可能造成正常应用程序的失效,还可能由于突破 Android 的沙盒机制而被判定为恶意行为.此外,该方案容易被攻击者利用注入有利于构建侧信道的信息[23,24].由于无法准确判断用户何时进行敏感信息输入,该方案仍然依赖于安全意识普遍较低的用户决策.与之相比,我们的防御过程实施于系统框架层,不会被恶意攻击者绕过或利用,此外,由于完全透明于应用,防御将不会有用户行为的干扰.

输入侧信道的基本假设是攻击者知道目标用户使用的键盘尺寸和布局,Young 等人[17]首次提出随机改变目标键盘的布局是针对输入侧信道攻击的有效保护策略.在此基础上,Maiti 等人[48]对默认布局中的按键大小、排序等采取不同程度随机化,一定程度上平衡了随机键盘策略的易用性和安全性.通过改变键盘布局的防御方法具有明显的局限性:首先,改变广泛使用且用户已经非常熟悉的默认键盘对于绝大部分用户而言是不友好的,而且除了系统的默认键盘外,很多 APP(微信,支付宝等)自带键盘,难以将键盘布局随机化策略应用到所有 APP 中;其次,布局随机化策略无法防御同样利用运动传感器的追踪侧信道攻击.

已有的工作在以下两个方面存在缺陷:首先,已有研究无法有效平衡用户体验与防御能力,要么牺牲用户体验来提高防御效果,要么保证了用户体验而防御能力较差;其次,已有的研究无法做到对各种类型侧信道的普适防御.本文提出的防御方法有效地解决了上述问题:通过在系统框架层进行信号混淆,能够对各种类型侧信道的构建过程进行干扰,实现了该防御方案的有效性和灵活性.此外,我们在先前的工作[21]中分析了合法应用程序与侧信道对于传感器数据精度的差异,讨论了各种类型运动传感器相关功能的噪声承受上界,提出了各类合法功能的建议混淆范围,进而保证防御方法的可用性.与其他研究相比,该防御方案实现了防御能力与用户体验的平衡,具有优异的应用价值.

7 总 结

本文针对移动设备运动传感器侧信道攻击,提出了基于 Laplace 机制的传感器信号混淆防御方案,并对防御原理进行了详细和全面的理论分析.本文的防御方案中,通过平移混淆方式向传感器读数中无差别地注入服从 Laplace 分布的少量随机噪声,在保证 APP 正常运行的前提下,有效降低各种类型的运动传感器侧信道攻击成功率.该防御方案部署在系统框架层,对于攻击者和用户完全透明,不会破坏系统原有安全机制,具有良好的可用性、普适性和灵活性.首先,对运动传感器侧信道的构建过程进行了分析,讨论运动传感器侧信道通用模型;然后,从理论层面分析了信号混淆干扰运动传感器侧信道学习阶段的原理,进而证明本文提出的信号混淆方案对于符合模型的传感器侧信道均有效;最后,对 8 种典型的输入侧信道以及 3 种追踪侧信道进行防御测试,验证防御方案在应对实际攻击时的有效性,其中,混淆程度ε=10 时,平移混淆降低输入侧信道单次预测准确率平均约 19 个百分点,降低追踪侧信道单次设备识别准确率平均约 13 个百分点.本文的研究不仅能够在侧信道防御的实际应用中发挥积极作用,对后续运动传感器侧信道相关工作也具有重要的参考价值.

References:

[1] Spreitzer R, Moonsamy V, Korak T, Mangard S. Systematic classification of side-channel attacks: A case study for mobile devices. IEEE Communications Surveys & Tutorials, 2018,20(1):465−488. [doi: 10.1109/COMST.2017.2779824]

[2] Nahapetian A. Side-Channel attacks on mobile and wearable systems. In: Proc. of the Consumer Communications & Networking Conf. Piscataway: IEEE, 2016. 243−247. [doi: 10.1109/CCNC.2016.7444763]

[3] Cai L, Chen H. On the practicality of motion based keystroke inference attack. In: Katzenbeisser S, ed. Proc. of the 5th Int'l Conf. on Trust and Trustworthy Computing. Berlin: Springer-Verlag, 2012. 273–290. [doi: 10.1007/978-3-642-30921-2_16]

[4] Lee YJ. Detection of movement and shake information using android sensor. Advanced Science and Technology Letters, 2015,90: 52–56. [doi: 10.14257/astl.2015.90.12]

[5] Shala U, Rodriguez A. Indoor positioning using sensor-fusion in android devices [MS. Thesis]. Kristianstad: Kristianstad University, 2011.

[6] Das A, Borisov N, Caesar M. Tracking mobile Web users through motion sensors: Attacks and defenses. In: Proc. of the Network and Distributed System Security Symp. Rosten: Internet Society, 2016. [doi: 10.14722/ndss.2016.23390]

[7] Das A, Borisov N, Chou E. Every move you make: Exploring practical issues in smartphone motion sensor fingerprinting and countermeasures. Proc. on Privacy Enhancing Technologies, 2018,2018(1):88–108. [doi: 10.1515/popets-2018-0005]

[8] Dey S, Roy N, Xu W, Choudhury RR, Nelakuditi S. AccelPrint: Imperfections of accelerometers make smartphones trackable. In: Proc. of the Network and Distributed System Security Symp. Rosten: Internet Society, 2014. [doi: 10.14722/ndss.2014.23059]

[9] Tang BX, Wang ZB, Wang R, Zhao L, Wang LN. Niffler: A context-aware and user-independent side-channel attack system for password inference. Wireless Communications and Mobile Computing, 2018,2018:Article ID 4627108. [doi: 10.1155/2018/4627108]

[10] Zhang W, He H, Zhang QZ, Kim T. PhoneProtector: Protecting user privacy on the android-based mobile platform. Int'l Journal of Distributed Sensor Networks, 2014,10(2):1–10. [doi: 10.1155/2014/282417]

[11] Mehrnezhad M, Toreini E, Shahandashti SF, Hao F. Stealing pins via mobile sensors: Actual risk versus user perception. Int'l Journal of Information Security, 2018,17(3):291–313. [doi: 10.1007/s10207-017-0369-x]

[12] Mohamed M, Shrestha B, Saxena N. SMAshed: Sniffing and manipulating android sensor data for offensive purposes. IEEE Trans. on Information Forensics and Security, 2017,12(4):901–913. [doi: 10.1109/TIFS.2016.2620278]

[13] Cai L, Machiraju S, Chen H. Defending against sensor-sniffing attacks on mobile phones. In: Proc. of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds. New York: ACM Press, 2009. 31–36. [doi: 10.1145/1592606.1592614]

[14] Maiti A, Jadliwala M, He J, Bilogrevic I. (Smart) watch your taps: Side-channel keystroke inference attacks using smartwatches. In: Proc. of the ACM Int'l Symp. on Wearable Computers. New York: ACM Press, 2015. 27–30. [doi: 10.1145/2802083.2808397]

[15] Owusu E, Han J, Das S, Perrig A, Zhang J. ACCessory: Password inference using accelerometers on smartphones. In: Proc. of the 12th Workshop on Mobile Computing Systems & Applications. New York: ACM Press, 2012. 1–6. [doi: 10.1145/2162081.2162095]

[16] Conti M, Nguyen VTN, Crispo B. CRePE: Context-related policy enforcement for Android. In: Burmester M, ed. Proc. of the 13th Int'l Conf. on Information Security. Berlin: Springer-Verlag, 2010. 331–345.

[17] Ryu YS, Koh DH, Aday BL, Gutierrez XA, Platt JD. Usability evaluation of randomized keypad. Journal of Usability Studies, 2012, 5(2):65–75.

[18] Shrestha P, Mohamed M, Saxena N. Slogger: Smashing motion-based touchstroke logging with transparent system noise. In: Proc. of the 9th ACM Conf. on Security & Privacy in Wireless and Mobile Networks. New York: ACM Press, 2016. 67–77. [doi: 10.1145/2939918.2939924]

[19] Qing SH. Research progress on Android security. Ruan Jian Xue Bao/Journal of Software, 2016,27(1):45–71 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[20] Dwork C, Mcsherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. In: Halevi S, ed. Proc. of the Theory of Cryptography Conf. Berlin: Springer-Verlag, 2006. 265–284.

[21] Tang BX, Wang LN, Wang R, Zhao L, Wang DL. A defensive method against android physical sensor-based side-channel attack based on differential privacy. Joural of Computer Research and Development, 2018,55(7):1371–1392 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2018.20170982]

[22] Wang YJ, Wu JZ, Zeng HT, Ding LP, Liao XF. Covert channel research. Ruan Jian Xue Bao/Journal of Software, 2010,21(9): 2262–2288 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]

[23] Laskov P, Lippmann R. Machine learning in adversarial environments. Machine Learning, 2010,81(2):115−119. [doi: 10.1007/s10994-010-5207-6]

[24] Auer P, Cesa-Bianchi N. On-Line learning with malicious noise and the closure algorithm. Annals of Mathematics & Artificial Intelligence, 1998,23(1-2):83−99.

[25] Malkin N, Harbach M, De Luca A, Egelman S. The anatomy of smartphone unlocking: Why and how Android users around the world lock their phones. GetMobile: Mobile Computing and Communications, 2016,20(3):42−46. [doi: 10.1145/3036699.3036712]

[26] Mehrnezhad M, Toreini E, Shahandashti SF, Hao F. Touchsignatures: Identification of user touch actions and pins based on mobile sensor data via javascript. Journal of Information Security and Application, 2016,26:23−38. [doi: 10.1016/j.jisa.2015.11.007]

[27] Mehrnezhad M, Toreini E, Shahandashti SF, Hao F. Stealing pins via mobile sensors: Actual risk versus user perception. Int'l Journal of Information Security, 2018,17(3):291−313. [doi: 10.1007/s10207-017-0369-x]

[28] Ping D, Sun X, Mao B. Textlogger: Inferring longer inputs on touch screen using motion sensors. In: Proc. of the 8th ACM Conf. on Security & Privacy in Wireless and Mobile Networks. New York: ACM Press, 2015. No.24. [doi: 10.1145/2766498.2766511]

[29] Miluzzo E, Varshavsky A, Balakrishnan S, Choudhury RR. Tapprints: Your finger taps have fingerprints. In: Proc. of the 10th Int'l Conf. on Mobile Systems, Applications, and Services. New York: ACM Press, 2012. 323−336. [doi: 10.1145/2307636.2307666]

[30] Xu Z, Bai K, Zhu SC. TapLogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In: Proc. of the 15th ACM Conf. on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2012. 113−124. [doi: 10.1145/2185448.2185465]

[31] Shen C, Pei SC, Yang ZY, Guan XH. Input extraction via motion sensor behavior analysis on smartphones. Computers & Security, 2015,53:143−155. [doi: 10.1016/j.cose.2015.06.013]

[32] Aviv AJ, Sapp B, Blaze M, Smith JM. Practicality of accelerometer side channels on smartphones. In: Proc. of the 28th Annual Computer Security Applications Conf. New York: ACM Press, 2012. 41−50. [doi: 10.1145/2420950.2420957]

[33] Zheng N, Bai K, Huang H, Wang H. You are how you touch: User verification on smartphones via tapping behaviors. In: Proc. of the IEEE 22nd Int'l Conf. on Network Protocols. Piscataway: IEEE, 2014. 221−232. [doi: 10.1109/ICNP.2014.43]

[34] Peng HC, Long FH, Ding C. Feature selection based on mutual information: Criteria of max-dependency, max-relevance, and min-redundancy. IEEE Trans. on Pattern Analysis & Machine Intelligence, 2005,27(8):1226−1238. [doi: 10.1109/TPAMI.2005.159]

[35] Liu XH, Li S. An optimized algorithm of decision tree. Ruan Jian Xue Bao/Journal of Software, 1998,9(10):797−800 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/9/797.htm

[36] Maaten L, Hinton G. Visualizing data using *t*-SNE. Journal of Machine Learning Research, 2008,9(2008):2579−2605.

[37] Maaten L. Accelerating *t*-SNE using tree-based algorithms. Journal of Machine Learning Research, 2014,15(1):3221−3245.

[38] Bojinov H, Boneh D, Michalevsky Y, Nakibly G. Mobile device identification via sensor fingerprinting. arXiv preprint arXiv: 1408.1416, 2014.

[39] Shen C, Yu T, Yuan S, Guan XH. Performance analysis of motion-sensor behavior for user authentication on smartphones. Sensors, 2016,16(3):345−365. [doi: 10.3390/s16030345]

[40] Cai L, Chen H. TouchLogger: Inferring keystrokes on touch screen from smartphone motion. In: Proc. of the 6th USENIX Workshop on HotSec. New York: ACM Press, 2011. 9−15.

[41] Noor MFM, Ramsay A, Hughes S, Ogers S, Williamson J, Smith RM. 28 frames later: Predicting screen touches from back-of-device grip changes. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. New York: ACM Press, 2014. 2005−2008. [doi: 10.1145/2556288.2557148]

[42] Negulescu M, Mcgrenere J. Grip change as an information side channel for mobile touch interaction. In: Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems. New York: ACM Press, 2015. 1519−1522. [doi: 10.1145/2702123.2702185]

[43] Marquardt P, Verma A, Carter H, Traynor P. (sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In: Proc. of the 18th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2011. 551−562. [doi: 10.1145/2046707.2046771]

[44] Luca AD, Hang A, Brudy F, Lindner C, Hussmann H. Touch me once and i know it's you! Implicit authentication based on touch screen patterns. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. New York: ACM Press, 2012. 987−996. [doi: 10.1145/2207676.2208544]

[45] Shahzad M, Liu AX, Samuel A. Behavior based human authentication on touch screen devices using gestures and signatures. IEEE Trans. on Mobile Computing, 2017,16(10):2726−2741. [doi: 10.1109/TMC.2016.2635643]

[46] Liu JY, Zhong L, Wickramasuriya J, Vasudevan V. uWave: Accelerometer-based personalized gesture recognition and its applications. Pervasive and Mobile Computing, 2009,5(6):657−675. [doi: 10.1016/j.pmcj.2009.07.007]

[47] Andriotis P, Tryfonas T, Oikonomou G, Yildiz C. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: Proc. of the 6th ACM Conf. on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2013. 1−6. [doi: 10.1145/2462096.2462098]

[48] Maiti A, Crager K, Jadliwala M, He J, Kwiat K, Kamhoua C. Randompad: Usability of randomized mobile keypads for defeating inference attacks. In: Proc. of the IEEE Euro S&P Workshop on Innovations in Mobile Privacy & Security (IMPS). Piscataway: IEEE, 2016.

附中文参考文献:

[19] 卿斯汉.Android 安全研究进展.软件学报,2016,27(1):45−71. http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[21] 唐奔宵,王丽娜,汪润,赵磊,王丹磊.基于差分隐私的 Android 物理传感器侧信道防御方法.计算机研究与发展,2018,55(7):1371−1392. [doi: 10.7544/issn1000-1239.2018.20170982]

[22] 王永吉,吴敬征,曾海涛,丁丽萍,廖晓锋.隐蔽信道研究.软件学报,2010,21(9):2262−2288. http://www.jos.org.cn/1000-9825/3880.htm [doi: 10.3724/SP.J.1001.2010.03880]

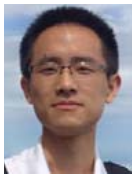
[35] 刘小虎,李生.决策树的优化算法.软件学报,1998,9(10):797−800. http://www.jos.org.cn/1000-9825/9/797.htm

唐奔宵(1991－),男,湖北黄石人,博士,CCF 学生会员,主要研究领域为 Android 隐私保护,机器学习.

赵磊(1985－),男,博士,副教授,博士生导师,CCF 专业会员,主要研究领域为系统安全,软件分析.

王丽娜(1964－),女,博士,教授,博士生导师,主要研究领域为系统安全,信息隐藏.

陈青松(1995－),男,学士,主要研究领域为移动隐私保护.



汪润(1991－),男,博士,主要研究领域为移动设备隐私保护,机器学习.