1. Characterizing Sensor Leaks in Android Apps

Sun, X. (1); Chen, X. (1); Liu, K. (2); Wen, S. (3); Li, L. (1); Grundy, J. (1)

Source: *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, p 498-509, 2021; **ISBN-13:** 978-1-7281-8595-8; **DOI:** 10.1109/ISSRE52982.2021.00058; **Conference:** 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 6-8 July 2021, Kharagpur, India; **Publisher:** IEEE, Piscataway, NJ, USA

Author affiliation: (1) Monash University, Melbourne, VIC, Australia (2) Nanjing University of Aeronautics and Astronautics, China (3) Swinburne University of Technology, Melbourne, VIC, Australia

Abstract: While extremely valuable to achieve advanced functions, mobile phone sensors can be abused by attackers to implement malicious activities in Android apps, as experimentally demonstrated by many state-of-the-art studies. There is hence a strong need to regulate the usage of mobile sensors so as to keep them from being exploited by malicious attackers. However, despite the fact that various efforts have been put in achieving this, i.e., detecting privacy leaks in Android apps, we have not yet found approaches to automatically detect sensor leaks in Android apps. To fill the gap, we designed and implemented a novel prototype tool, Seeker, that extends the famous FlowDroid tool to detect sensor-based data leaks in Android apps. Seeker conducts sensor-focused static taint analyses directly on the Android apps' bytecode and reports not only sensor-triggered privacy leaks but also the sensor types involved in the leaks. Experimental results using over 40,000 real-world Android apps show that Seeker is effective in detecting sensor leaks in Android apps, and malicious apps are more interested in leaking sensor data than benign apps. (0 refs)

Inspec controlled terms: Android (operating system) - data privacy - invasive software - mobile computing - sensors - smart phones

Uncontrolled terms: characterizing sensor leaks - mobile phone sensors - mobile sensors - privacy leaks - sensor-based data leaks - Seeker conducts sensor-focused static taint analyses - real-world Android apps - malicious apps

Classification Code: B6250F Mobile radio systems - C6130S Data security - C6190V Mobile, ubiquitous and pervasive computing

IPC Code: G06F9/44 - G06F9/46 - G06F21/00 - H04B7/00 - H04B7/26 - H04W - H04M1/725

Treatment: Practical (PRA) - Experimental (EXP)

Database: Inspec

Data Provider: Engineering Village