

Scopus

Document details

[< Back to results](#) | 1 of 1[Export](#) [Download](#) [Print](#) [E-mail](#) [Save to PDF](#) [Add to List](#) [More... >](#)[Full Text](#)[View at Publisher](#)

Proceedings - 2013 International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013

2014, Article number 6836615, Pages 406-411

2nd International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2013; Kuching, Sarawak; Malaysia; 23 December 2013 through 24 December 2013; Category numberP5234; Code 106250

Empirical analysis of android apps permissions (Conference Paper)

Bakar, N.S.A.A. [✉](#), Mahmud, I. [✉](#)

Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia

Abstract

[View references \(10\)](#)

Android applications or apps are taking the smart phones industry to a new level. Smart phone users can do most of their everyday tasks using the various types of applications offered in the Android Play Store. Generally, prior to installation of the apps, users need to agree on the permissions requested by the apps, they are not given any other option. Essentially, users may not aware on some security issues that may arise from the permissions. Some apps request the right to manipulate sensitive data, such as GPS location, photos, calendar, contact, email and files. In this paper, we explain the sources of sensitive data, what the malicious apps can do to the data, and apply the empirical software engineering analysis to find the factors that could potentially influence the permissions in Android apps. In addition, we also highlight top ten most implemented permissions in Android apps. © 2013 IEEE.

Author keywords

Android applications empirical analysis permission types sensitive data statistics

Indexed keywords

Engineering controlled terms: Smartphones Software engineering Statistics

Android applications
 Android apps
 Empirical analysis
 Empirical Software Engineering
 GPS location
 permission types
 Security issues
 Sensitive datas

Engineering main heading: Android (operating system)

ISBN: 978-147992758-6

Source Type: Conference Proceeding

Original language: English

DOI: 10.1109/ACSAT.2013.86

Document Type: Conference Paper

Sponsors:

Publisher: IEEE Computer Society

Metrics

0 Citations in Scopus

0 Field-Weighted Citation Impact



PlumX Metrics 

Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)

[Set citation feed >](#)

Related documents

ASPG: Generating android semantic permissions

Wang, J. , Chen, Q. (2015) *Proceedings - 17th IEEE International Conference on Computational Science and Engineering, CSE 2014, Jointly with 13th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2014, 13th International Symposium on Pervasive Systems, Algorithms, and Networks, I-SPAN 2014 and 8th International Conference on Frontier of Computer Science and Technology, FCST 2014*

Evaluating the trust of android applications through an adaptive and distributed multi-criteria approach

Dini, G. , Martinelli, F. , Matteucci, I. (2013) *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in*