

1. A First Look at Security Risks of Android TV Apps (Open Access)

Liu, Yonghui (1); Li, Li (1); Kong, Pingfan (2); Sun, Xiaoyu (1); Bissyande, Tegawende F. (2)

Source: *Proceedings - 2021 36th IEEE/ACM International Conference on Automated Software Engineering*

Workshops, ASEW 2021, p 59-64, 2021, *Proceedings - 2021 36th IEEE/ACM International Conference on Automated Software Engineering Workshops, ASEW 2021*; **ISBN-13:** 9781665435833; **DOI:** 10.1109/ASEW52652.2021.00023;

Conference: 36th IEEE/ACM International Conference on Automated Software Engineering Workshops, ASEW 2021, November 15, 2021 - November 19, 2021; **Sponsor:** Amazon Web Services; et al.; Facebook; Huawei; Monash University; NASA Ames Research Centre; **Publisher:** Institute of Electrical and Electronics Engineers Inc.

Author affiliation: (1) Monash University, Melbourne, Australia (2) University of Luxembourg, Luxembourg

Abstract: In this paper, we present to the community the first preliminary study on the security risks of Android TV apps. To the best of our knowledge, despite the fact that various efforts have been put into analyzing Android apps, our community has not explored TV versions of Android apps. There is hence no publicly available dataset containing Android TV apps. To this end, We start by collecting a large set of Android TV apps from the official Google Play store. We then experimentally look at those apps from four security aspects: VirusTotal scans, requested permissions, security flaws, and privacy leaks. Our experimental results reveal that, similar to that of Android smartphone apps, Android TV apps can also come with different security issues. We hence argue that our community should pay more attention to analyze Android TV apps. © 2021 IEEE. (33 refs)

Main heading: Android (operating system)

Controlled terms: Mobile security

Uncontrolled terms: Android apps - First look - Google plays - Privacy - Security - Security aspects - Security flaws - Security risks - Security/privacy - Smart-TV

Classification Code: 723 Computer Software, Data Handling and Applications - 723.2 Data Processing and Image Processing

Funding Details: Number: DE200100016, DP200100020, Acronym: ARC, Sponsor: Australian Research Council;

Funding text: ACKNOWLEDGEMENTS This work was supported by the Australian Research Council (ARC) under a Discovery Early Career Researcher Award (DECRA) project DE200100016, and a Discovery project DP200100020.

Open Access type(s): All Open Access, Green

Database: Compendex

Data Provider: Engineering Village

Compilation and indexing terms, Copyright 2022 Elsevier Inc.