Engineering Village™

1. **Lie to Me: Abusing the Mobile Content Sharing Service for Fun and Profit**
Xu, G.; Li, S.; Zhou, H.; Liu, S.; Tang, Y.; Li, L.; Luo, X.; Xiao, X.; Xu, G.; Wang, H. **Source:** *WWW '22: Proceedings of the ACM Web Conference 2022*, 3327-35, 2022; **ISBN-13:** 978-1-4503-9096-5; **DOI:** 10.1145/3485447.3512151; **Conference:** WWW '22: ACM Web Conference 2022, 25-29 April 2022, Virtual Event, France; **Sponsor:** SIGWEB; **Publisher:** ACM, New York, NY, USA

Author affiliation:
Beijing University of Posts and Telecommunications, China
Hong Kong Polytechnic University, China
ShanghaiTech University, China
Monash University, Australia
Case Western Reserve University, United States
Huazhong University of Science and Technology, China

Abstract: Online content sharing is a widely used feature in Android apps. In this paper, we observe a new Fake-Share attack that adversaries can abuse existing content sharing services to manipulate the displayed source of shared content to bypass the content review of targeted Online Social Apps (OSAs) and induce users to click on the shared fraudulent content. We show that seven popular content-sharing services (including WeChat, AliPay, and KakaoTalk) are vulnerable to such an attack. To detect this kind of attack and explore whether adversaries have leveraged it in the wild, we propose DeFash, a multi-granularity detection tool including static analysis and dynamic verification. The extensive in-the-lab and in-the-wild experiments demonstrate that DeFash is effective in detecting such attacks. We have identified 51 real-world apps involved in Fake-Share attacks. We have further harvested over 24K Sharing Identification Information (SIIs) that can be abused by attackers. It is hence urgent for our community to take actions to detect and mitigate this kind of attack. (0 refs.) **Inspec controlled terms:** Internet - mobile computing - program diagnostics - security of data - social networking (online)

Uncontrolled terms: online content sharing - Android apps - shared content - content review - shared fraudulent content - multigranularity detection tool - real-world apps - mobile content sharing service - fake-share attack - sharing identification information - targeted online social apps - DeFash - temperature 24.0 K

Classification Code: C6190V Mobile, ubiquitous and pervasive computing - C6150G Diagnostic, testing, debugging and evaluating systems - C6130S Data security - C7210N Information networks

IPC Code: G06F9/44 - G06F11/36 - G06F21/00

Treatment: Practical (PRA)

Database: Inspec