What Mobile Ads Know About Mobile Users
Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

Most of the apps rely on advertising as their primary revenue, and hence advertising is the key component of mobile app echo-system. They typically use third party AdSDKs, which fetch ads from server and display them, on the running app. AdSDKs use same privileges as their host apps. They track users using device identifiers. Paper focuses threats from malicious advertisers, instead of advertising libraries. Paper demonstrates how the malicious advertisers steal user information by accessing external storage. External storage is essential for media-rich ads containing audio, video, etc. Malicious advertisers first tempt the users to download an HTML page containing malicious payload. Then they load the payload by opening this page within the same WebView as the ad. "After loading the page, javascript present in the payload, can be used to steal any local file that belongs to the same file-scheme origin"[1]. This can be done only if certain conditions get satisfied, for e.g. from version Android 4.4 KitKat, the host app must have READ_EXTERNAL_STORAGE permission, url must be loaded with the scheme other than https, etc. Paper shows that using this technique sensitive user information can be leaked, such as browsing history, location related information, etc.

2 Contribution

"Paper studies ad isolation in four popular android SDKs, AdMob, MoPub, AirPush and AdMarvel"[1]. It demonstrates that the malicious ad can learn about user despite the presence of existing defenses and "the only attack vector available to a malicious advertiser is an ad-supported app that runs on the user's device and displays the attackers' ads in a confined WebView instance"[1]. Paper also proposes some short term and long term defenses.

3 Strengths

I liked that the authors have provided attacker code snippets which are easy to understand. I also like that they provide short term (Though rely on SDK providers) and long term solutions (Though I find them rather speculative).

4 Limitations

I think the short term solutions which are provided require SDK providers to make changes in their code and policies. But, there are tons of SDK providers and you can't expect each and everyone to be aware or careful or legit. Also, paper proposes some long term changes without any demonstration or any discussion about performance and the other implications (For eg. if we treat each ad impression as a separate app with dedicated storage, there may be some performance implications).

5 Future Work

I think more work needed at advertising library providers' side, to not only check for ads that push malware, but also check for ads that collect information from devices. Also, there is a need of concrete os solution, instead of relying on SDK providers (i.e. short term solutions).

References

[1] Sooel Son, Daehyeok Kim and Vitaly Shmatikov *What Mobile Ads Know About Mobile Users*, NDSS (2016)