46. SANOOP C K

Understanding in-app ads and detecting hidden attacks through the app-web interface

Abstract

Mobile users are increasingly becoming targets of malware infections and scams. In order to curb such attacks it is important to know how these attacks originate. While a significant amount of research effort has been spent analysing the malicious applications themselves, an important, yet unexplored vector of malware propagation is benign, legitimate applications that lead users to websites hosting malicious applications. It's called the app-web interface. In some cases this occurs through web links embedded directly in applications, but in other cases the malicious links are visited via the landing pages of advertisements coming from ad networks. When the user taps on the advertisement, he/she is led to a web page which may further redirect until the user reaches the final destination. Even though the original applications may not be malicious, the Web destinations that the user visits could play an important role in propagating attacks. Since all the sensitive user data is stored in mobile devices, it is important to identify malicious attacks. A systematic static analysis methodology can be used to find ad libraries embedded in applications and dynamic analysis methodology consisting of three components related to triggering web links, detecting malware and scam campaigns, and determining the provenance of such campaigns reaching the user.