Inference Attack on Browsing History of Twitter Users Using Public Click Analytics and Twitter Metadata

Twitter is a popular online social network service for sharing short messages (tweets) among friends. Its users frequently use URL shortening services that provide (i) a short alias of a long URL for sharing it via tweets and (ii) public click analytics of shortened URLs. The public click analytics is provided in an aggregated form to preserve the privacy of individual users. In this paper, we propose practical attack techniques inferring who clicks which shortened URLs on Twitter using the combination of public information: Twitter metadata and public click analytics. Unlike the conventional browser history stealing attacks, our attacks only demand publicly available information provided by Twitter and URL shortening services. Evaluation results show that our attack can compromise Twitter users' privacy with high accuracy.