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

**ABSTRACT:**

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.

**EXISTING SYSTEM:**

* Some researchers propose attack methods to steal browsing history using user interactions and side-channels.
* Weinberg et al. exploit CAPTCHA to deceive users and to induce user’s interaction. They also use a webcam to detect the light of the screen reflected at the user’s face, which can be used to distinguish the colors of visited from those of unvisited links.
* He et al. and Lindamood et al. build a Bayesian network to predict undisclosed personal attributes.
* Zheleva and Getoor show how an attacker can exploit a mixture of private and public data to predict private attributes of a target user.
* Similarly, Mnislove et al. infer the attributes of a target user by using a combination of attributes of the user’s friends and other users who are loosely (not directly) connected to the target user.
* Calandrino et al. propose algorithms inferring customer’s transactions in the recommender systems, such as Amazon and Hunch.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Previous studies have considered attack techniques that cause privacy leaks in social networks, such as inferring private attributes and de-anonymizing users.
* Most of them combine public information from several different data sets to infer hidden information.
* Need complicated techniques or assumptions

**PROPOSED SYSTEM:**

* In this paper, we propose novel attack methods for inferring whether a specific user clicked on certain shortened URLs on Twitter.
* Our attacks rely on the combination of publicly available information: click analytics from URL shortening services and metadata from Twitter.
* The goal of the attacks is to know which URLs are clicked on by target users. We introduce two different attack methods: (i) an attack to know who click on the URLs updated by target users and (ii) an attack to know which URLs are clicked on by target users.
* To perform the first attack, we find a number of Twitter users who frequently distribute shortened URLs, and investigate the click analytics of the distributed shortened URLs and the metadata of the followers of the Twitter users.
* To perform the second attack, we create monitoring accounts that monitor messages from all followings of target users to collect all shortened URLs that the target users may click on. We then monitor the click analytics of those shortened URLs and compare them with the metadata of the target user.
* Furthermore, we propose an advanced attack method to reduce attack overhead while increasing inference accuracy using the time model of target users, representing when the target users frequently use Twitter.

**ADVANTAGES OF PROPOSED SYSTEM:**

* Evaluation results show that our attacks can successfully infer the click information with high accuracy and low overhead.
* We propose novel attack techniques to determine whether a specific user clicks on certain shortened URLs on Twitter.
* To the best of our knowledge, this is the first study that infers URL visiting history on Twitter.
* We only use public information provided by URL shortening services and Twitter (i.e., click analytics and Twitter metadata).
* We determine whether a target user visits a shortened URL by correlating the publicly available information.
* Our approach does not need complicated techniques or assumptions such as script injection, phishing, malware intrusion, or DNS monitoring. All we need is publicly available information.
* We further decrease attack overhead while increasing accuracy by considering target users’ time models. It can increase the practicality of our attacks so that we demand immediate countermeasures.

**SYSTEM ARCHITECTURE:**



**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium Dual Core.
* Hard Disk : 120 GB.
* Monitor : 15’’ LED
* Input Devices : Keyboard, Mouse
* Ram : 1GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows 7.
* Coding Language : JAVA/J2EE
* Tool : Eclipse
* Database : MYSQL

**REFERENCE:**

Jonghyuk Song, Nonmember, IEEE, Sangho Lee, Member, IEEE, and Jong Kim, Member, IEEE, “Inference Attack on Browsing History of Twitter Users using Public Click Analytics and Twitter Metadata”, **IEEE Transactions on Dependable and Secure Computing, 2016.**