De-Anonymization Attacks on Social Networking sites

-by Vikram Patil

Tuesday, February 9, 2016

This paper introduces de-anonymization attack on social networking sites like Xing, Facebook, LinkedIn etc. As we know these social networking sites have grown enormously in past few years. In fact Facebook claims 3

- Introducing a novel de-anonymization attack to show how same can be applied to such social networking to get information about specific users.
- Showing several techniques to attack these sites.
- Providing theoretical analysis and empirical measurements to show the feasibility of attacks.

Background:-

A)Model and definitions: In this section, paper explains model and definitions of social networks, browser history and attacker model.

- **Social Networks:** A social network S is a graph G = (V;E) where nodes V = users, edges E = the friendship relation between two users.
- **Browser history:** It is used as a building block in attack on browsing history B. Visited page URL is added to B.

B)Structure of networking sites:

This section gives overview on structuring of sites regarding Group formation, types and web applications.

C)History stealing:

A malicious website is used by attacker to retrieve users browsing history. In this technique attacker creates a HTML page with links to target specific web pages and uses background image tags. This way, attacker can also use client-side scripting to generate and move over a list of target links and check for visited pages.

De-Anonymization attacks:-

In this section attacks are explained in detail.

A) Basic attack:

In this approach, attacker may join a group in the social networking sites and look for a person by in built search function. This is not feasible attacker has to check a link for every user and the user base is huge on such networking sites. Still this is a valuable tool for the attacker to identify a user if the user belongs to a small group of members.

B) Improved attack:

The special features provided by networking sites such as forums and mailing lists can be used for history stealing technique. In this attack, attacker first gathers information about the group and the uses history stealing technique to identify a specific user by checking the page visited history if he/she is a group member or not.

C) Effectively obtaining group information:

Number of groups compared to number of users is small but obtaining group and group member information is also tough. This can be done effectively in following two techniques.

- **Group Directories:** Social networking give search functionality to serch for groups. This give most of the group names in a list. This is group directory.

- **Group member crawling:** Obtaining user information which is public and searching the user in the groups.

Following table demonstrates vulnerability comparison of social networks.

	Facebook	LinkedIn	Xing
Uses dynamic links	Yes	Yes	Yes
Group directory	Full	Searchable	Searchable
Member directory	Full	Full	Searchable
Group member search count	<=6000	<=500	Unlimited
Public member profiles	Yes	Yes	Yes
Vulnerable?	Yes	Yes	Yes

My github repository link: `https : //github.com/vikrampatil1/vikramlatex.git`