De-Anonymize Social Network Users

Bhargav Uppalapati

02/06/2015

Privacy of a website does not depend on how secure the website is but rather the amount of sensitive or private data stored on the website. With ever increasing population. The need for people to know and connect with each other, has made big bucks for social networking websites. With 400 million registered user base, Social networking giant Facebook reports growth up to 3% every week. With people connecting and sharing private information, there is always a chance for the attacker to steal private information, like photos and messages. Generally the identity of the user is anonymous to the attacker, but in a ***De-Anonymize*** kind of attack the main goal of the attacker is to find the identity of the user.

A ***De-Anonymize attack*** involves the user and the attacker being a part of a social networking website. Instead of tracking the browsing history of the user on the network, the attacker tracks individual persons. Every user likes to belong to a group and interact with their friends i.e. gaining membership to a group also known as group memberships. The next step for the attacker is to lure the user into a malicious website or attack the user when he visits a malicious website. Through a browser attack the attacker obtains the browsing history of the user. Through the browsing history, user identity can be obtained. The attacker now meticulously searches for the user on the social network and group memberships to gain further access to private information of the user.

All the users in a social networking website may or may not be a part of a group. So, to find the target user the attacker also becomes part of the group, searches if the user exists in the group. If the user is not found or if the group listing is private the attacker moves on to the next group. But a real world situation where, giant social networking websites like Facebook, crawling through all the groups and finding the target user can be very hard. But a disadvantage to the user and an advantage to the attacker is that social networks provide public lists visible to everyone so that users can join others with similar interests. At the end of the day the attacker can use the data provided by the social network itself to find relations between groups and their members and eventually find the victim.

With the consent from the users and several social networking websites a real world. A ***De-Anonymize attack*** was performed. It was found that no countermeasures were put in place. Attacker tried to join and become a member of a group thereby collecting personal data of users with 90% success rate. When 26 volunteers with the Xing social networking website were attacked 15/26 people were De-Anonymized. Showing the success rate of the attack and seriousness of the threat.

Threat to the users can be mitigated by:
1.Using secure non-guessable URLs at the server side among other countermeasures.
2.Users need to be cautious avoiding malicious websites and frequently clearing browsing data.

	Facebook	MySpace	Friendster	LinkedIn	Xing	Kiwibox
Uses Dynamic Links	Yes	Yes	Yes	Yes	Yes	Yes
Group Directory Restrictions	Full	Searchable	Full	Searchable	Searchable	Full
Member Directory Restrictions	Full	Searchable	Full	Full	Searchable	Searchable
Members per Group	$\leq 6,000$	Unlimited	Unlimited	≤ 500	Unlimited	Unlimited
Vulnerable	Yes	Yes	Yes	Yes	Yes	Yes

The table shows vulnerabilities in several social networking websites.