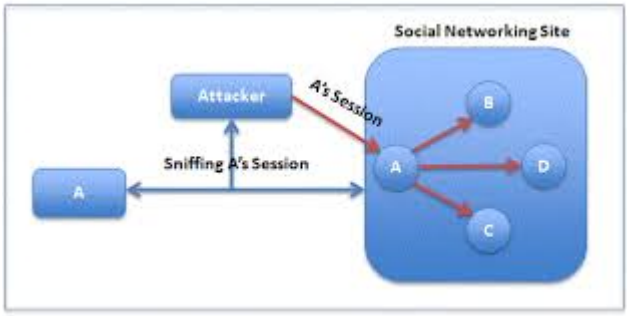
Summary of A Practical Attack to De-Anonymize Social Network Users

Saranya Radhakrishnani

02/08/2015

Social networks have provisioned the feature of creating groups of users with an idea of connecting users with similar interests . The amount of private and sensitive information stored in social networking sites is greater compared to other sites , thus making the social networking sites vulnerable to attacks. The most common way of attacking these sites to steal personal information is by garnering user information from group memberships which uniquely identifies the user.



The authors of the paper , A Practical Attack to De-Anonymize Social Network Users have leveraged on stealing group membership of users from well known web browser history stealing attacks. This implies that whenever a user visits a malicious website,it would initiate the de-anonymization attack and pick up visitors identity.
The authors have further detailed their attacks based primarily on stealing history as of two types namely Basic attack - steals user information Improved attack - relies on groups instead of individual users
The paper further explains crawling experiments that were used to fetch the information about groups based on experiments performed on three social networks Xing, Facebook and LinkedIn. The findings of the experiment are elaborated below.

1. Xing: The authors have demonstrated the feasibility of attacks on users of Xing social network successfully. Attacking Xing , a moderate sized

social networking medium , with approximately 8 million users (at the time of writing this paper) , resulted in extensive collection of data of the groups as well as the users of Xing. The analysis of the attack led to the findings that attacker checked 6,277 groups , implying it needed to check only 6,277 urls only instead of 8 million urls.

2. Facebook:

   Due to the enormity of facebook data the authors decided to use a commercial crawling service to download requite user information .They extracted the group IDs and then supplied that as input to their own custom crawler to extract information about group members. The findings were as follows The authors crawled more than 43.2 million group members from 31,853 groups in a span of 23 days using only two machines.

3. LinkedIn:

   The authors applied a two-phase crawling method , In the first pass .they generated 3 million hyperlinks for the observed group ID space, and then these links were supplied as input to a commercial crawling service. The authors had to perform another crawling pass to extract information such as group size and group description.

   After a studying other social networking sites, the authors tabulated their findings as shown below

	Facebook	LinkedIn	Xing
Uses dynamic links	YES	YES	YES
Group Directory	FULL	SEARCHABLE	SEARCHABLE
Member Directory	FULL	FULL	SEARCHABLE
Group member enumeration	less than or equals 6,000	less than or equals 500	UNLIMITED
Public member profiles	YES	YES	YES
Vulnerable	YES	YES	YES

Further the authors proposed mitigation techniques to counter the attacks as stated below

1. Server side mitigation technique

   - Usage of dynamic hyperlinks that would contain HTTP GET parameters with randomized tokens
   - Pass parameters through HTTP POST instead of HTTP GET in order to prevent creation of browser history.

2. Client side mitigation technique

- Prohibit the browsers from disclosing private information through CSS by restricting the access of client-side scripts.
- The users can prevent information leakage by deleting browser history periodically.