Summary on *A Practical Attack to De − anonymize Social Network Users*

Sourav Bhowmik

Saturday, February 6, 2016

A Practical attack to De-anonymize social network users

In the IEEE paper, "*A Practical attack to De−anonymize social network users*", the authors launch a de-anonymization attack on various social networking sites such as Xing, facebook and LinkedIn. These social networks make use of groups for better connectivity amongst it's users. The authors try to exploit this feature and launch attacks on the users(and not mere browsers) to de-anonimize (or uniquely identify) them and extract personal information such as full name, profile, photos, resume and more. They claim these kinds of attacks require a fairly low level of effort and expertise in spite of the fact that most of these social networks have millions of users.

Using tracking information is not very sufficient to identify a user, so the authors have used a technique called *history stealing* to successfully de-anonimize a user. The attacker runs a malicious website. He examines the URLs in the user's history to extract group information of a social network. This way he can identify the user whenever the latter visits the malicious website. Their research on structure of social networking sites reveals information about groups such as closed and open groups and roles of group administrators.The web applications of these sites use *dynamic hyperlinks* which makes it easy to extract $groupIDs$ and $userIDs$ from the URLs itself.

The study provides further details on de-anonymization attacks by categorizing them into:

1. *Basic attack*
2. *Advanced attack*

Both of them combine history stealing and social network information in order to trick the user to visit the attacker's website.

The basic attack is said to be less practical and looks good only on paper (especially for facebook that has 100s of millions of users). This is because the candidate set or the search space for the attack would become too large to be of any practical use.

In order to reduce the candidate set and make the attack more feasible, the advanced version makes use of group information and tries to create a intersection of multiple user sets of groups. This reduces the size of the search space and takes less time.

The authors next explain about their *crawling* experiments to obtain group information in more detail. They used their own customized *web crawler* and also online crawler services to expose weaknesses in anti-crawler techniques used by social networks for group directories. The practical feasibility of these attacks was found to be very high. They successfully downloaded data from 1.8 million unique members from over 6500 groups in Xing. While in Facebook they could crawl over 40 million users in a small time of 3 weeks. Similar were the results for other networks such as LinkedIn, MySpace, etc. All of the crawling services used were merely worth 10s of dollars. The table below is representative of their exact findings.

Table 1: Vulnerability Comparison of Social Netwoks.

	Xing	Facebook	MySpace	LinkedIn
Uses dynamic links	Yes	Yes	Yes	Yes
Group Directory	Searchable	Full access	Searchable	Searchable
Member directory	Searchable	Full access	Searchable	Full
Public member profiles	Yes	Yes	Yes	Yes
Vulnerability	High	High	High	High

Some mitigation strategies that could be used to counter these attacks have also been suggested such as use of $HTTP\ POST$ on the server-side or a mechanism that makes it tough to predict $HTTP\ GET$. Disabling browser history on client side is another measure.

In conclusion, the authors demonstrated the ease and feasibility of launching attacks on social networks and their associations that can impact millions of users.

GitHub repository link 'https://github.com/souravbhowmikmarist/SecurityAlgo/blob/master/Finalsummary.pdf"