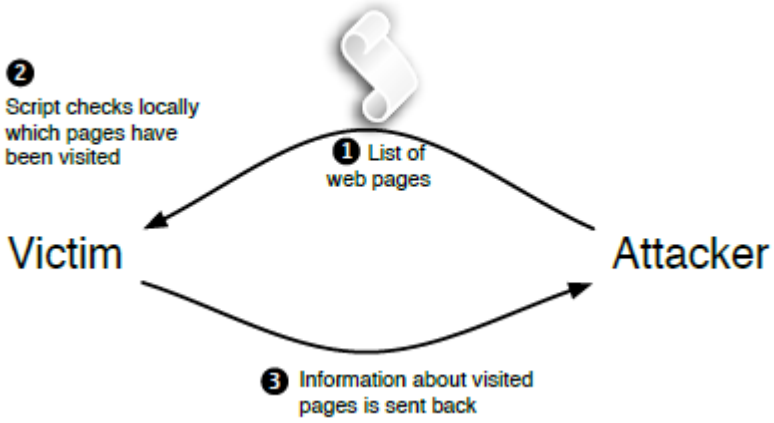
A Practical Attack to De-Anonymize Social Network Users - Summary

Sandeep Reddy Salla

February 8, 2016

De-anonymization attack can be performed on group members of a group on social networking sites like Facebook, twitter, Xing, etc. (they have similar structure) to get the information of group members or about specific users. De-anonymization attack is practically done on Xing social network. The results indicate 42% of users present in this network that use groups can be affected.

1. Two types of **groups** on social network:
   - **Public Group:** Any member of the social network can join into this group. Authorization is not required.
   - **Closed Group:** It requires some authorization before joining into this group.
2. **History stealing** is one of the main techniques an attacker can use. With the help of this technique attacker can keep track of the victims browser history for certain URLs which will reveal the group members on a social network.



3. **Model and Definition:** Social Networks S is represented as a graph G.

$$G = (V, E) \tag{1}$$

where V represents users and E represents friendship between users.

$\Gamma(v) := (\Gamma g(v))_{g \epsilon G}$
$\Gamma g(v) = 1$ If v is a member of group g
$\Gamma g(v) = 0$ If v is not a member of group g

4. **Efficiently Obtaining Group Information:**
   - **Group Directory:** Group directory can be reconstructed if attacker guesses the group IDs.
   - **Group Member Crawling:** To gain information about members of the group, attacker also needs to keep track of the IDs of the members of the group along with the group IDs.
5. **Social Network Crawling Approaches:**
   - **Customer Crawler:** Web crawler has been implemented to follow the hyperlinks of a public page to download HTML source code in order to access the parts of social network (restricted to members).
   - **Commercial Crawling Service:** Attackers with less number of network resources lead to commercial crawling service.
6. **Crawling Experiment Results:**
   - **Xing:** Automated member requests are sent to 1306 closed groups, 108 groups accepted. This allowed an attacker to track the user IDs of total groups.
   - **Facebook:** Using two machines, 43.2 million members of the group are crawled from 31,853 groups in a span of 23 days.
   - **LinkedIn:** Two phase crawling scenario has been implemented. In the first scenario, collected 3 million hyperlinks from the observed group Ids space. In the second phase, additional information like group size, description has been retrieved.
7. **Mitigation Techniques:**
   - **Server-side Mitigation:** To send parameter values in an URL, web application must use HTTP POST instead of HTTP GET.
   - **Client-side Mitigation:** Restrict the properties of cascading style sheet of hyperlinks, disable browsing history.