All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks

Report

Konstantinos Kleftogiorgos
kleftog@csd.uoc.gr
935
June 5, 2016

Social networking sites have millions of registered users who use them in order to share personal information with their contacts. This paper investigates how easy it would be for a potential attacker to launch automated crawling and identity theft attacks against a number of popular social networking sites in order to gain access to this large volume of personal user information.

The first presented attack is the automated identity theft of existing user profiles. The main idea is that they cloned an already existing profile in a social network and they sent friend requests to the contacts of the victim. Hence, they were able to “steal” the contacts of a user by forging his identity and creating a second, identical profile in the same social network. Having access to the contacts of a victim they were able to access the sensitive personal information provided by these contacts.

In the second attack, they show that it is effective and feasible to launch an automated, cross-site profile cloning attack. In this attack, they are able to automatically create a forged profile in a network where the victim is not registered yet and contact the victim's friends who are registered on both networks. Their experimental results with real users show that the automated attacks are effective and feasible in practice.

They implemented the attacks in a prototype system called iCloner (identity Cloner). iCloner consists of several components that are able to crawl popular social networking sites, col-
lect information on users, automatically create profiles, send friend requests and personal messages. Furthermore, iCloner also supports CAPTCHA analysis and breaking capabilities that make the attacks feasible against social networking sites that employ CAPTCHAs to prevent automated access. Figure 1 gives an architectural overview of iCloner and depicts the dependencies between the various components.

![Figure 1: An architectural overview of iCloner](image)

The crawler was tested on StudiVZ, MeinVZ, and XING, using the crawler component of iCloner, with the aim of collecting large volumes of contact lists and public user profile data. For StudiVZ and MeinVZ, they crawled more than 5 million public user profiles with contact information, more than 1.2 million profiles with complete user information and around 118,000 profiles for XING.

iCloner, using the collected public information on user profiles, was able to duplicated the profiles of five users who had given their consent for the experiments. After the profile creation, iCloner sent contact requests to all contacts in the friendship list of each victim. They also created a control set of one fictitious profile for each duplicated profile, in order to measure how effective profile cloning is with respect to requests that the contacted users might receive from people that they do not know. They contacted the same users from these accounts as with the respective duplicated profiles. Figure 2 shows the acceptance rate for the duplicate profiles compared to this of the fake ones.

For the second attack ICloner obtained 5 accounts from XING and imported them into LinkedIn. They identified that 78 out of their 443 XING friend contacts were also registered on LinkedIn and sent contact requests to these accounts. As shown in Figure 3 out of the 78 contact requests that were sent to the users in LinkedIn, 56% were accepted.

To sum up, this paper investigates how easy it would be for a potential attacker to launch automated crawling and identity theft (i.e., cloning) attacks against popular social networking sites. They presented and experimentally evaluated two identity theft attacks, showing that this sort of attacks are quite feasible. Although social networking sites are useful, they believe that it is important to raise awareness among users about the privacy and security risks that are involved.
Figure 2: The fraction of accepted contact requests (D1..D5 are the forged profiles, and F1..F5 are the fictitious profiles)

Figure 3: Percentage of XING profiles found in LinkedIn (LP) and the success rate (SR) of the contact requests

<table>
<thead>
<tr>
<th>Profiles</th>
<th>LP</th>
<th>SR</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>18.2%</td>
<td>50.0%</td>
</tr>
<tr>
<td>X2</td>
<td>14.5%</td>
<td>66.6%</td>
</tr>
<tr>
<td>X3</td>
<td>22.8%</td>
<td>51.6%</td>
</tr>
<tr>
<td>X4</td>
<td>14.5%</td>
<td>100.0%</td>
</tr>
<tr>
<td>X5</td>
<td>15.6%</td>
<td>46.4%</td>
</tr>
<tr>
<td>Total</td>
<td>17.6%</td>
<td>56.4%</td>
</tr>
</tbody>
</table>

Figure 3: Percentage of XING profiles found in LinkedIn (LP) and the success rate (SR) of the contact requests