Security Issues of Online Social Networks

M.A. Devmane[1] and N.K. Rana[2]

[1] P.V.P.P. College of Engineering, Mumbai
dmahavir@gmail.com
[2] Theem College of Engineering, Mumbai
ranank@rediffmail.com

Abstract. The number of users of the online social networks like facebook, twitter, google, linkedIn are going on increasing tremendously. Similarly the time spend by each user on such online social networks (OSN) is also increasing. These things clearly indicate that the popularity of these OSN is increasing like a wildfire. These OSN provide a very efficient platform for the user to establish contacts with others. These users are having frequent communication with each other. So the adversaries find the OSN as a soft target to attack easily and spread it to the large number of users in less time. In this paper we consider some of such threats to OSN as well countermeasures to some of these threats so as to make the OSN as well as the user secure in the digital world.

Keywords: Online Social network, cyber security, profile cloning, botnet.

1 Introduction

The OSNs are so popular that the number of users of facebook alone is more than 1000 million around the globe. To become member of the OSN the user has to create his profile by entering information like name ,photo, date of birth , Email ID, place of work , home town and so on [1][2]. Some of these fields are mandatory and remaining are optional and varies from one OSN to the other. To attract more and more friends or to let others to find easily the users try to provide the maximum information in the profile [3]. OSNs are mainly used for keeping in touch with friends, forming new contacts, as well as search for someone else on the OSN and establish contact with him by sending a friend request. Such contacts are used to share some information with each other as well as broadcast the information through a group.

Due to the availability of more number of OSNs some of the users are having their account on more than one OSN so that they can remain in touch with their friends in that OSN also. While creating such profiles or accounts most of the users doesn't go through the privacy policy of each such OSN and provide the information. In such cases there is high risk of leakage of information. As the OSN follow the client-server architecture all the data given by the user in the profile will remain with the server so no one can predict that how secure is the data.

This paper takes into consideration the various threats to the Online Social Networks and provides remedies to some of them in the following sections.

S. Unnikrishnan, S. Surve, and D. Bhoir (Eds.): ICAC3 2013, CCIS 361, pp. 740–746, 2013.

2 Information Leakage

Information leakage means the information stored by the user in his profile is accessed by someone else and use the same for malicious activities [4].Most of the OSN allow the friend of the user to have access to most of the fields from his profile. This must be taken into consideration while either sending friend request or accepting friend request from anybody. Whenever a user accepts friend request it is assumed that he is having trust in that user so such access is provided.

To avoid such malicious access it is necessary to be careful while selecting security settings for various fields in the profile. A field likes contact details can be set as "visible to me only" so that the adversary can't get access to it. Similarly before sending or accepting any friend request just check that the person can be trusted or not otherwise adversary may get direct access to your information and so many other things can happen. Most of the OSN users are careless in this matter which can be supported by the example of automated script which send friend requests to 250000 facebook users and out of that 75000 users accepted the request and him in the friend list without taking due care.

3 Spam in OSN

Spam is abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. Although the most widely recognized form of spam is E-mail spam the term is similarly applied to similar abuses in other media like online social networks [5]. There are two types of spamming.

3.1 Broadcast Spamming

In broadcast spamming the malicious user does not know the exact Email ID of the user so he normally does some combinations of words to generate some probable Email IDs and send Emails. Such spams are not that much effective as the user does not believe in it easily.

3.2 Context Aware Spamming

In the context aware spamming the Email may contain some information of the user which is taken from the profile of the user in one of the OSN. Such information is gathered just by searching the OSN for a name and if it exists find its Email ID and other credentials in the profile and use the same in the spam. As it contains some information about the user he will easily believe in the Email and may reply to it. It is observed that the context aware spams are more successful than the broadcast spam.

4 Profile Cloning

To have account with an OSN the user has to create his profile by providing his details. By using the credentials from this profile a malicious user can create a profile