

Tools and Techniques to Prevent Misuse of Personal Information in Social Networking

J.SathyaPriya

Department of Information Technology, Velammal Engineering College, Chennai.

C.M.Nalayini

Department of Information Technology, Velammal Engineering College, Chennai.

S.Priyadharshini

Assistant Professor, Department of Information Technology, Velammal Engineering College, Chennai.

ABSTRACT

Social Network sites are used by many people in recent years. There are a lot of security issues in using social networks nowadays. The success of any social network is based on the total number of users who use the social network. So the providers of the social network are forced to design a system, which will help to increase the numbers of users who use the social network and at the same time, the connections also. In any social network sites, security will not take the major role, because the main concept of the social network is to share the knowledge and ideas among all the people who involved in the social network site. This will cause social security risks. It would be good if the social network users are provided with security tool like any other tools. With the help of social security tool, the social network user can retrieve the information about another online user through chat or website. This paper will address about the tools for social network, that will help to reduce the security risks and also to determine the non personal information such as IP address and MAC address of the user.

Keywords - Social Security Risks, MAC Address, IP address.

I. INTRODUCTION

In this paper, we have described the forensic security software tools that will protect the users of social network site from the various security threats that are existing in the current situation. Initially, we have found the various issues that exist in social network sites. As a result, we found there are numerous security threats in social network sites. So we concentrate on developing tools that will help in tracking down the criminals. The developed tools will focus on identifying the non personal information such as IP address, MAC address of the social network site user.[3] Identifying such information is based on the non real(virtual) contact, such as browsing the personal page, contacting the person through a virtual meeting, that is chatting. In this paper, the procedures used, results of tests and the future enhancement are covered.

The various social network site issues are listed as, viruses and worms, cross-site scripting, corporate espionage.[6] The aggregators of social network site are infiltration of networks that leads to data leakage, phishing that is specific to the social network, spear phishing vulnerabilities of digital dossier aggregation, vulnerabilities of data collection and face recognition.

1.1 Case Study

We have been motivated to do this work from the following criminal case.

Using a social network, two persons become friends, one of them say, Alex, wanted to meet the other person. But the other person is really a robber, whose main intention is to rob Alex. While trying to escape from the other person, Alex ran through a narrow lane and met with an accident by a vehicle, which leads to a homicide case.[7]

In the next case, a woman was involved in creating a phony account to trick a teenager. That teenage person committed suicide later.[7]

As mentioned earlier, there are so many cases and such cases are growing as the social network sites are used in an expanded fashion. In this paper, some tools are used, which will help to track the criminals and will also help to prevent crimes which are related to social network sites.

II. METHODOLOGY

To design the procedure for storage and tools to retrieve the data, Java, Java applets, PHP, SQL, MSDOS scripting, Java web application, database access concepts are used.[4]

III. FETCHING OF USER'S INFORMATION

3.1 Outline

The information about the users, who have visited your profile on the social network site such as facebook, twitter shall be identified and fetched. In some social network sites, we will have some inbuilt application which will help us to know the list of users who have visited our profile. There is a concept called store log transcripts which will track the chat session data like, MAC address and IP address.[1]

A concept called click tracking is used to store the users information who visits the website of the social network. The Click tracking system collects the domain name, referring URL, pages visited, IP address, web browser type.[5] There is service in Facebook which will track all the activities of the users in third party sites, which includes the people will not have signed up with Facebook

or the people who have invalidated the account with facebook. This will tempt the intruders misuse the social network sites.

A mechanism called Beacon will capture the data details about the tasks done by the users on the other partner sites.[8] Such data is sent to the Facebook server, which will include the IP address of the web pages that are visited and the users IP address. It is also possible for some users of social network sites to add some scripts and objects, by which they can understand the information of another user who visits the social network sites. In Myspace, the users are allowed to track the other users who visit their profile, with the help of a third party service called "whovisited".[7]

3.2 Fetching of Data in social network site using PHP

The task of fetching the data of users can be performed within the website, by using the incorporation of PHP code or Java. For the above-mentioned reason, some of the social network sites, have provided a system, which will automatically make the PHP and Java code in an inactive mode, whenever a user attempts to incorporate into the social network site. For example, the social network site called Myspace will not permit Java scripting code to be used in their network site.[7]

In this paper, we have included various procedures that will help us to find out the nonpersonal information about the users who visit the social network site and also about the users who communicate with the social network site in the virtual world. The process of fetching the users information is done using scripts or commands in this paper.

Using online environments, virtual meetings, various chat sessions and electronic mail, it becomes possible to perform the process of users data retrieval. Based on users data fetching method, we have focused mainly on retrieving the nonpersonal user information, which is said to be "IP address". With the help of IP address we can track the location of users which is also called as ISP location of users.

Once the process of fetching the IP address is completed, the geographical location of the user can be found out with the help of PHP scripting language. Using the PHP scripting language, there are certain links we can make use of, to identify the geographical location. Some of the links are,

<http://www.virtualforensics.net/track.php>[7]

<http://www.virtualforensics.net/>[7]

Once the information about the user is found, they are added to the list which is called as users list; that is already maintained in the database of the social network site. From the database log, all the visitors information will be easily fetched and viewed.

Figure1 PHP code for fetching of users

```
GATEWAY INTERFACE=CGI/1.1
SADDR=192.181.2.4
SNAME=73.121.8.111
SSOFTWARE=APACHE/2.2.10
SPROTOCOL=HTTP
```

```
REQMETHOD=GET()
REQTIME=122228215
DOCROOT=C:/ProgramFiles/Apache
HTTPACCEPTENCODING=ZIP
SADMIN=ja.yahoo.com
Sport=8081
Scriptname=/php/files/all.php
Requiri=php/files/all.php
```

Figure 2: Code written in PHP for IR

```
http-user-agent=<?php echo
```

```
$ server['http-host'];?><br>
```

```
Remote-addr=<?php echo
```

```
$ server['server admin'];?><br>
```

```
Server_port=<?php echo
```

```
Request_uri=<?php echo
```

```
$server['serverport'];?><br>
```

3.3 Fetching the device type in social network site

The type of the device can be identified using the PHP scripting code. Using the link given below, we can understand whether the social network site visitor is accessing the social network site through a personal computer or through a mobile phone or through another device.

<http://www.virtualforensics.net/mobiledetect/detect.php>[7]

It is also possible to find out what mobile phone model is used by the social network site user to access the social network site using the link given below,

<http://www.virtualforensics.net/mobiledetect/detectmobile.php>[7]

3.4 Fetching of User information through IM chat session

A tool named NetStat which is called as Network Statistics is used to find the other person Internet Protocol address during the IM chat session which is said to be virtual meeting.[6] The information such as incoming network connection, outgoing network connection, routing tables, network interface statistics. One example is shown, which will guide us to understand the use of netstat command for fetching the Internet Protocol address and MAC protocol address.[3]

```
NetStat -n 3
```

Sample output will be,

```
TCP110.000.0000.00.2222 33.3.33.33:6666 established
```

```
TCP 000.00.000.00:5555 77.7.777:6666 established
```

The Internet Protocol address which is displayed on the left side will refer the Internet Protocol address of the current machine in which we are working. The Internet Protocol address on the right side will refer the Internet protocol address of the foreign machine. The digits that

are following the Internet Protocol address will represent the port number to which the machine is connected.

The following command is used to connect to the Internet Protocol address of the foreign machine,

```
C:/>nbstat-A 77.7.77.777
```

Here 77.7.77.777 is the Internet Protocol address of the foreign machine. The above-mentioned command will give the value of the node, NetBIOS remote machine table, and the MAC address.

3.5 Fetching user data through email

It is possible to extract the IP address of a particular person from whom we receive email. For example, using a Gmail email account, perform the following.[7]

Go to the inbox of your email account

Perform right click on the mail sender

Click the option to select the source code

Now the sender's IP address will be appearing on the screen

4.1 Fetching users data from website

3.6.1. Through Java-fetching the data

It is possible to get the list of nonpersonal identifiable information for the website which is coded using Java.

Context path of the website is found using the method, req.getContextPath(), here req is the object of the HttpServletRequest class.

LocalAddress gives the address of the datagram socket, the method used is, req.getLocalAddr(), here req is the object of the class HttpServletRequest.[4]

LocalName gives the local name of the system, the method used is req.getLocalName(), here req is the object of the class HttpServletRequest.

LocalPort gives the port number of the local host and the method used is req.getLocalPort(), here req is the object of the class HttpServletRequest.[4]

Locale gives the users locale from the HTTP Accept Header. The method used is req.getLocale(), here req is the object of the class HttpServletRequest.

Protocol which gives the type of protocol used. The method used in req.getProtocol(), here req is the object of the class HttpServletRequest.

Remote Address which gives the clients Internet Protocol address. The method used is req.getRemoteAddr(), here req is the object of the class HttpServletRequest.[4]

RemoteHost which indicated the domain name in a fully qualified manner. The method used is req.getRemoteHost(), here req is the object of the class HttpServletRequest

RequestSessionID –when the first request is submitted to the client, a session shall not be requested. So there will be no session id. In order to receive the session id from the server we go for the method, req.getRequestSessionId(), here req is the object of the class HttpServletRequest.

RequestURI, gives the path from the name of the protocol to the query string. The method used is req.getRequestURI(), here req is the object of the class HttpServletRequest.

RequestURL will give the Uniform Resource Locator of the browser, that we are using. The method is req.getRequestURL(), here req is the object of the class HttpServletRequest.

3.6.2 MAC address extraction using Java applets

Most of the network adapters and network interface cards will possess media control address which is called as MAC address, Ethernet hardware address which is called as EHA, hardware address, adapter address, physical address. These addresses are provided by the manufacturer for the purpose of identification. These addresses will have manufacture's registered identification number.

The following concepts of Java applet code is used to access the above mentioned information,[7]

```
macAdd = windowsRunIpConfigCommand();
```

```
intlen = macAdd.length();
```

```
intAddressDet = macAdd.indexOf("Ethernet adapter Local Area Connection:");
```

```
macA=windowsRunIpConfCommd();
```

the above inbuilt function is to find the configuration of the system.

```
MacAdd.indexof();
```

This function is to find the index of the local area connection.

IV. COMPUTER LOGS

4.1 Monitoring computer using software

There is a powerful tool called spytechnetvizor, that will monitor all the activities that are done by the users on our computer. The agent provides required features that will monitor the computer and also performs the website and application content filtering, chat client blocking and remote delivery of logs through email or file transfer protocol.

Network Gazer will give us a real-time overview of current network configuration. There is a network named as lookup network which will give the details about the people who accessed the network. It is also possible to identify the level of access of the people who use the social network site. We can retrieve the internet history, cookies, web page history etc.,[7]

Universal IM History Decoder is a component, which will decode the message history files which belongs to the popular instant messengers. With the help of this component we can look at not only our data but also the information about other people's conversation without using the password of the user. Such decoded messages are saved in a text file for future use.[7]

IM History is the component which acts as the first service in the world; that will perform the process of saving the chat history. This is used by all the people in the world, to maintain the history of all the instant messenger. This component performs various services such as, onlinestorage, easy surfing over the messages and contacts. This makes possible to retrieve the history from all our messengers in a safer mode with highly reliable storage. Further our own messages are placed and

protected in a server which is highly secured and so that no one else except we can view them.

4.2 Forensics tools

Encase Forensics is the most famous tool that will undergo forensics related investigations. This is a single tool which can perform complex and large-scale investigations from the initial stage to final stage. This tool used the concepts such as intuitive GUI, very powerful scripting engine and enriched email and internet support. The beneficiaries of such tool are corporate investigators, government officers and IT consultant around the globe.[8]

UTK, which is named as, Ultimate Toolkit, consists of all that is needed to analyze and investigate digital data. This particular tool kit has got forensic toolkit, password recovery toolkit, NTaccess, FTK imager, technical phone support etc.,

Mareware, which gives us a set of tools for securing the private information and for investigating the records of the computer. It also satisfies all the requirements of the investigators across law enforcement, corporate security professionals and private, public intelligence agency.

V. CONCLUSION

In social networks, security becomes an important issue. Hence, the problem of finding the appropriate solutions and facing various security issues becomes a major concern. The tools used in this paper must be used at their fullest usage in the current communication world. The concepts and tools described here will help in investigating crimes in social network sites and also provides help to protect the users from committing crime at the start of the interaction with the social network site. We can also use the various websites that will track all the activities of the visitors on the website. The outcome of this research is to implement the tools that are described in this paper in order to provide security in social network sites.

VI. FUTURE ENHANCEMENTS

The future scope will be identifying Mac address of the client using the applet, fetching the name of the user of some other monitored social network page.

REFERENCES

- [1] Roman Schlegel; Duncan S. Wong, Private friends on a social networking site operated by an overly curious SNP, nt. J. of Computational Science and Engineering, 2015 Vol.10, No.3, pp.281 – 292.
- [2] DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo, "Secure Data Sharing in the Cloud", Security Privacy and Trust in Cloud Systems, 45 DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014.
- [3] EmanM.Mohamed, HatemSAbdelkader and Sherif El-Etriby, "Enhanced Data Security Model for Cloud Computing", The 8th International Conference on INFOrmatcs and Systems (INFOS2012) - 14-16

- [4] BhawanaRudra; A.P. Manu; O.P. VyasService-oriented network architecture: significant issues and principles of communication, Int. J. of Computational Science and Engineering, 2015 Vol.10, No.3, pp.306 - 314
- [5] <http://publishing2.com/2007/10/31/facebooksvulnerabilities/>, accessed December 2008
- [6] <http://thehackers.freesevers.com>, accessed December 2008
- [7] Marilyn Silva, Rajeswari Ian, AnuNagpal, Anthony Glover, Steve Kim.Virtual Forensics: Social Network Security Solutions, Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 8th, 2009
- [8] <http://java.sun.com/products/servlet/2.1/api/javax.servlet.http.HttpServletRequest.html>, accessed December 2008.