Internet Based User Profiling is a Threat to Privacy: Proactive Safe User Profiling Mechanism

Monika Pathak*
Sukhdev Singh**

Abstract

With an exponential growth in internet facilities and its monumental impact on daily lives activities makes an individual dependent. The internet changed our life enormously and influence social as well as business activities. It becomes a social media for communication, Business and entertainment. These social networking sites recognized each and every user through user profiling. The user profiling is an act carried out to gather information about the user. The information of user can be utilized in many ways such as customized the contents and interface of the hosting site, color combination of interface, automatic advertisement, update on issues related to interest of the user. On the counterpart information gather from the user on name of user profile leads to a serious threat to private and confidential information of the user. Most of the frauds originated from the unsafe user profiling. According to the survey conducted by Symantac[7] in the year of 2012, report entitled as "Internet security threats Report" the social networking sites were the softest target of the intruders to hack the personal information so that it can be misused. The present study is aimed to explore the threats to private information of the user due to unsafe profiling. We have also analyzed the survey reports to identify the issues related to safe user profiling. We have proposed a new mechanism to overcome unsafe user profiling problems which is called as "Proactive Safe User Profiling Mechanism". It is a client side application which enforces certain conditions or rules to create user profile over the internet.

Keywords: Proactive safe user profiling, cyber crime, Threats on private Information, Identity theft, Online Intrusion

Introduction

We are living in information age where everybody wants information within a second through internet. The influence of the internet can be observed on our daily life activities. Now it is part and parcel of our life. It provides way to exchange information across many channels such as email and social networks, and it also helps us accomplish tasks like reservation of seat on Railways (Train) flight, online financial tractions like paying bills, money transfer, filing income taxes return, etc. The emergence of technology in the fields of social networking influence every age of people over the world. It provides way to share information and participate in discussion over the globe. The social networking sites are popular due to worthwhile services like to find new contacts, way to find former friends, maintain current relationships, promote a business, share certain topic, or just have fun meeting and interacting with other users. Every social networking site asks new users to create profile during registration process. The user profile is an activity carried out over the internet to fetch user information in aim to provide customized facilities like color combination, user interface, advertisements, alerts on the site. But, when user unintentionally reveals personal or confidential information indirectly through user profile, then it leads to serious problem. The most of the cybercrime are reported through social networking sites where the personal and private information of the users

Monika Pathak*
Multani Mal Modi College, Patiala
Sukhdev Singh**
Multani Mal Modi College, Patiala

are gained and manipulated and misused. In the present study we have gone through survey conducted by

- Javelin Strategy & Research[2], “2010 Identity fraud Survey Report: Consumer Version”
- Javelin Strategy & Research[3] “2013 Identity Fraud Report”
- Symantec Corporation[6], “Internet Security Threat Report, 2011 Trends”
- Websence Security Labs web[9] “2010 Threat Report”
- AV Comparative[1], “IT security Survey 2013”
- McAfee,Center for Strategic and International Studies [5],”The Economic Impact Of Cybercrime and Cyber Espionage”, 2013.

We have also proposed a proactive safe profiling mechanism which enables the user to create safe profile over the internet.

Cyber Crime over Internet

The advancement in internet technology whereas it invites a lot of fruitful services, there is an adverse effect also comes into scene from late decade. As per the survey conducted by Javelin Strategy and Research Reports [2, 3] 2010 and 2013, it is observed that rate of cybercrime is rapidly including by passes of the time.

Cybercrime is a worldwide security concern as it is affecting Banking, utilities, healthcare, communications, government services, emergency services, transportation, etc. The advancement of technology in the field of Internet has provided a new tool of making crime. To make a crime now one may not to go physically somewhere, over the internet from known place crime can be executed such as online identity theft, cyber stalking, and viruses. Internet crime is quickly becoming one of the biggest and most threatening problems for both law enforcement and the public at large.

Online Fraud: Online fraud is an act of breaching of confidence information online in order to gain financial profit. Most common types of such of frauds are: auction fraud, lottery, phishing.

Auction Fraud: The auction is a business activity which is carried out online and different buyers participates to buy product of particular company. To make auction fraud, the seller products or seller name are misrepresented and after payment product never delivered to the buyer.

Lottery Scams: The lottery crime is initiated with an attractive offer which is send to the customer by email. The customer is asked to pay a small amount of fee to get prize in lakhs or millions. After payment,the prize money never delivered to the customer.

Phishing: The phishing is an act in which hosting web site pretend to belong to original whereas in fact it is a fake one. The appearance and working of the fishing site is as similar to the original one. The fishing sites target a bank, credit card Company, or online retailer sites. The victim is asked to provide id, password of credit card or information of bank account. The crime often involves spoofed emails that are designed to fetch personal or bank information.

Online Assault: Online assault is a psychological attack to the user, particularly minor in age. It involves threatening, emotional harassment to the victim by email or by posting unwanted information about the victim. The result of such assault leads victim to feelings of worry or fear**.** The purpose of such attacks is to damage victim’s identity, mental harassment and annoy the victim using of particular service over the internet.

Online Theft: The Online theft is an act carried over the internet and use technology to steal confidential information to gain access to money or business resources without the knowledge of the owner. The Identity theft and piracy are major part of Internet crime.

Identity Theft*:* This type of crime involves the misuse of an individual’s personal information without their consent or knowledge for the purposes

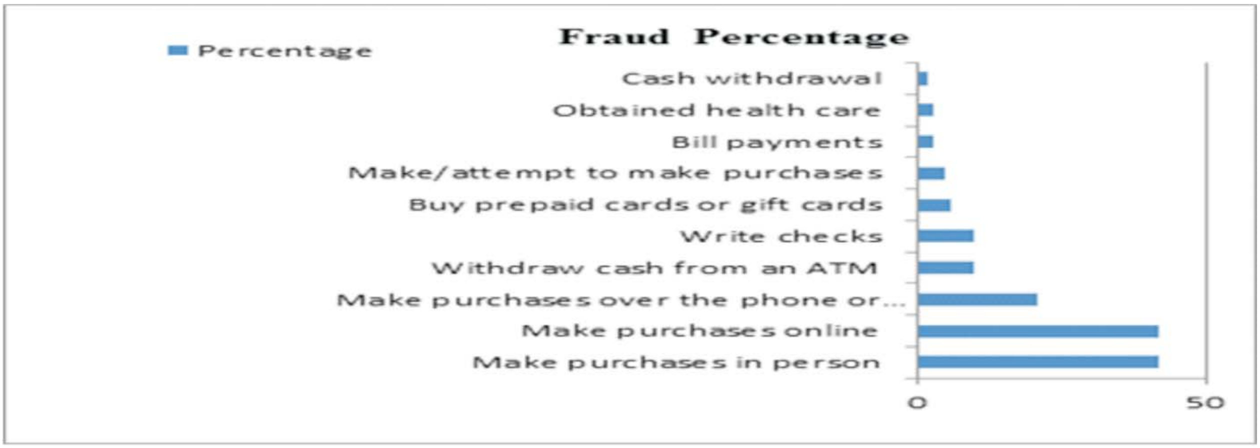

Fig. 1: Fraud Percentage on Different Services

Source: Javelin Strategy & Research, "2010 Identity fraud Survey Report: Consumer Version"

of committing fraud or theft. The victim's personal information can be used for financial purposes. It is basically an act to steal someone identity and use that identity for your own purposes.

Online Piracy: The online piracy is a violation of intellectual property right in which intellectual property steal and used for financial purpose. Commonly entertainment and music industry is targeted.

Online Intrusion: Online intrusion involves the use of the Internet to harm, infect processing power of server, server memory, etc. The goal of such crime is to slow down or hang up the web sites or client-server machines. The most common examples of this type of online crime are hacking and spreading viruses.

Hacking: Hacking is an act in which an individual attempt to surpass a Website, Network, or Computer System's security measures to gain access to protected resources. It has been observed that such acts sometime done to just show off individual technical skills.

Viruses and Worms*:* These are computer programs designed specifically to spread throughout computer networks to slow down the processing of network or harm machines in network. These programs can be added into network or machine through number of methods such as email, attachments, external hard disk, and freeware software.

Threats on private information

As per survey conducted by Javelin strategy and research [3, 6] in February 2010, the most common methods of fraud is reported in survey was identity theft. The identity thieves misused stolen information which is shown above in Figure-1.

It shows that both in person and online purchases account for more than four in 10 cases of fraud. Because online purchases require only a credit or debit card number, this method of fraud is increasingly favored by criminals. Additionally, slightly more than 20% of victims of identity fraud had their information used to make phone or mailorder catalog purchases. According to survey conducted by Symantec Antivirus entitled as Internet Security report, 2010 (Figure-2). The most of the web sites were targeted for malfunctions was social networking sites. In the survey they have categorized 10 categories of websites and out which blogs sites are listed on the top of high risk category.

They have also listed few guidelines [2, 3, 8] to protect personal information which are reproduced here as:

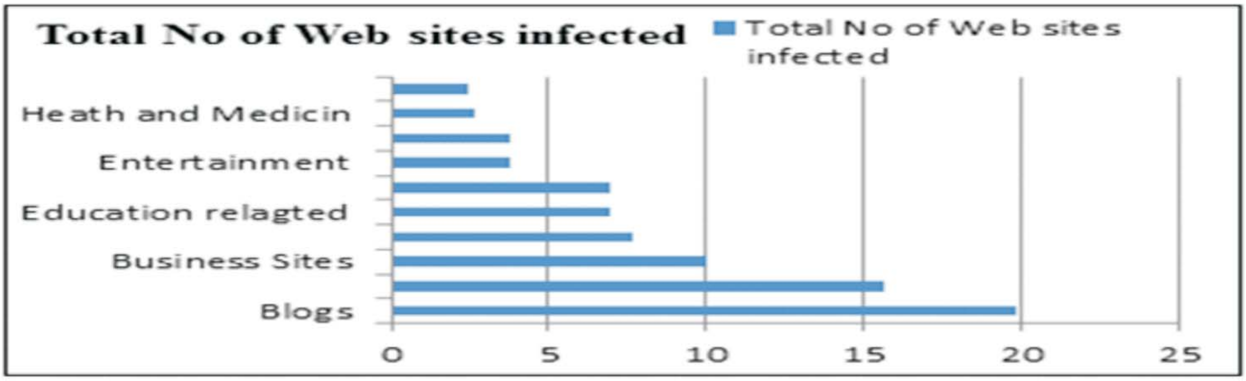

Fig. 2: Web Site Infected by Cyber Attack[2]

- They advised to limit the amount of personal information you make publicly available on the Internet) as it may be misused
- Confirmed the legitimation of the sources only then disclose the personal information. It means before disclosing confidential information double check the web site URL or identification certificate Information.
- While you are using online transaction, keep reviewing your bank, credit card, and credit information. Avoid shopping online from public computers such as libraries, Internet cafes.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing Web sites. Check the settings and preferences of the applications and Web sites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you login or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

There are numbers of technologies available that resolve some of the risks associated with sharing personal information. Encryption technology [4] is the technique in which information in encrypted into unreadable ciphertext by using concept of public key and private key. Another option is Anonymization**.** The technology provides an interface which can blur private information if the user is not authenticated.

Proposed proactive user profiling mechanism (PPUP)

User profiling is the activities which is unavoidable, almost every commercial or social networking site ask for registration and request for personal information. We have proposed proactive safe user profiling model which enable the users to create safe profile. In the proposed mechanism, the user is asked to create profile fields which are personal and confidential. The information is stored into the client machine. Whenever the user is asked to create a profile, say, for social networking site, then fields are scanned for sensitivity according to the database stored into client machine. This way a proactive scanning may be carried out to find the sensitivity of the information and moreover we can avoid the unsafe profiling over the internet. The process will be done on client machine and consider to be safe for Processing and storing personal information.

The complete process to execute the proactive user profiling is given below:

1. The user is asked to create database of fields from his profile and stored the information into the database.
2. When the user is asked to create profile for some site, the profile is consider as unsafe profile.

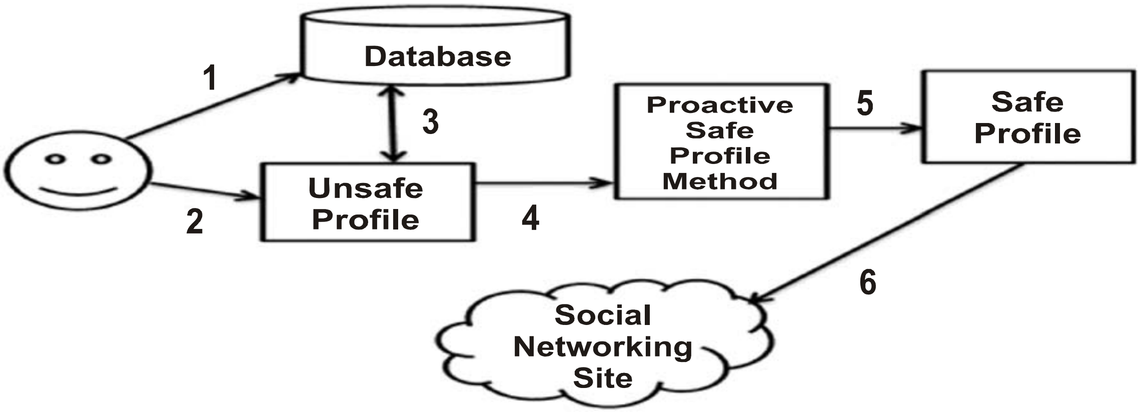

Fig. 3: Working of Proactive User Profiling Method

3. The unsafe profile is evaluated on comparison with database fields.
4. The analysis on the basis of correlation of unsafe profile with fields stored into database, the proactive safe profile is created through proactive safe profile method.
5. The safe profile is created after the filtration.
6. The profile is forwarded to the networking site.
7. The Proactive user profiling mechanism ensures the sensitivity of the profile by comparing the information stored on the client machine. The computational overhead is on client side as no processing power is carried out on server. The proposed mechanism is a strong step to safe user profile and secures your sensitive information.

Conclusion

User profiling is an activity which is carried out to fetch information from user. Sometime users reveal personal information and confidential information that may be misused. The social networking sites are most soft target of intruders as lot of personal information is available over there. We have proposed a proactive user profiling mechanism which may help users to create safe user profile. In the proposed mechanism, user create a personal profile on client machine which may have list of fields which are very confidential and personal and whenever user actually want to create profile for social networking sites then PPUP interface will filter the profile information before sending the information over the internet. In literature, we have not found such system which automatically enforces rules or conditions for safe profiling. Other mechanisms such as encryption, SSL security are used to safeguard the private information. As compared to these systems, proposed system is faster and easy to implement. It is light application running on client machine where as other systems like encryption or SSL consumed processing power of server machine. The proposed system has scope of improvement as confidential or personal data stored on client machine leads to security problem itself. Moreover we have implemented the proposed method using asp and MS access database, where as it can be improve by using advanced programming languages.

References

1. AV Comparative, “IT security Survey 2013”
2. Javelin Strategy & Research, “2010 Identity fraud Survey Report: Consumer Version”
3. Javelin Strategy & Research “2013 Identity Fraud Report”

4. L. Millett, B. Friedman, and E. Felten, “Cookies and Web browser design: toward realizing informed consent online”, In Proceedings of conference on Human factors in computing systems, ACM Press: New York, pp. 46-52, 2001.

5. McAfee, Center for Strategic and International Studies July 2013 , “The Economic Impact Of Cybercrime And Cyber Espionage”

6. Symantec Corporation, “Internet Security Threat Report, 2011 Trends,” Websence Security Labs web “2010 Threat Report” AV Comparative, “IT security Survey 2013.

7. Symantec Corporation, “Internet Security Threat Report, 2011 Trends”

8. The annual Global Fraud survey Report 2013-14 by Kroll.

9. Websence Security Labs web “2010 Threat Report”