Privacy Threats and Techniques to Secure Personal Data on Social Networks

**Dr. Barkha Bahl, **Mr. Rahul Aggarwal*

Abstract

Social Networking sites have become the most efficient and effective means of communication and information sharing. Social networks provide an online space for people to share their personal information. As a result of such increased usage and sharing of information through these sites, negative entities such as hackers have found an easy way to steal the users' personal information and exploit them. To keep personal information private is the challenge and has been a matter of concern for every user. The reason behind this is the increased number of attacks and difficulties faced while protecting the personal data against attacks and threats. This paper aims to discuss various data privacy threats which persist for the people on social media platforms, various prevention techniques and also to discuss the proposed technique to avoid and possibly prevent such attacks on privacy.

Keywords: Social Networking, Privacy, Threats, Risk factors

*** Professor, Delhi Institute of Advanced Studies, Delhi, India**
****Associate Software Developer, Softin System Private Limited, Delhi**

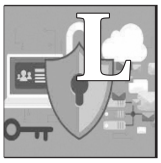
INTRODUCTION

In the modern society, internet is the hub of information, social networks being at the heart of it. Social media provides a common platform for like-minded people and friends form a group, discuss ideas, share a mutual interest and also exchange information through various services with like-minded people.

There are various Social networking sites that are popular based on geographic location. Orkut is popular in Brazil, V Kontakte in Russia and Mixi in Japan. Facebook and Twitter have maximum usage worldwide. A Business-Oriented focus is provided through Linkedin and Xing to enable sharing of business contacts and job offerings among the people who are using it.

The main purpose of such platforms is to communicate with others and provide different criteria for searching friends based on local areas, company name or based on common interest. Some search engines like yasni or 123people will search the keywords in multiple networks and return all possible results centrally. With the growth of the enterprises it has become more popular. It has been observed in a survey conducted by Symantec that 95% of the companies who were enquired do not block access to social network sites as they use social media for marketing purpose and also to keep their employees happy. 32% of people surveyed would not want to work for a company that prevents them from accessing a social network at work. On the other hand, the main worry of IT department which includes 84% of CIOs and 77% of system administrators, is security of personal data on social networks at work place. It is very difficult for administrators to prevent users from visiting social networks from work laptops while at home or when using company smart phones.

Social networking sites are used by millions of people to communicate, share their posts and login to access other services of different websites. To secure the personal data, awareness about its security, privacy and defending techniques against attacks are important for the users to understand. Social networking privacy issues have risen among users. The challenge today for every user is to keep computers and social networking more secure and more private. This is primarily due to the number of attacks and difficulties faced in defending against these attacks and threats (Kumar A., et. al. 2013). Next section will discuss data privacy threats, problems, risks and existing applications & widgets to secure the personal data on social networks.



LITERATURE REVIEW

As highlighted in the above section, social networks have become incredible tool in all age groups of the people especially among the youth and has become widely popular worldwide. It is mainly used for communication, self-expression, and for sharing information such as likes, dislikes, photos, interests, job details, relationship status, political views, current town details, religious views etc. Unfortunately, most of the users are not aware of the privacy risks associated with their shared sensitive information on the internet. The privacy concern is raised among the users of social network when the personal information has been accessed by other users on the network. B2B International together with Kaspersky conducted a survey in 2015, which shows that although social networking is being used worldwide, but there are very few users who understand the risks of using social networking especially when using mobile device to access the sites. According to study (Gangopadhyay, S., et. al., 2014) 78% of the users are not concerned about the cyber-crime or cyber-attacks associated with their information.

The literature (Go-Gulf., 2014) shows some principle privacy problems in social networks. In Facebook, the real information of the user is used to create an account profile for the rest of Facebook users. The default privacy settings provided in Facebook are not enough, consequently the users are exposed to too much information of other users. The online social network default privacy settings are not changed by the users and sometime it is unavailable to adjust the privacy setting which are offered by Facebook such as the users can see the whole his or her shared information whenever users add his or her to be in friend list.

Literature (Kumar, A.et. al., 2013) reveals that the dissemination of private content on social networking platforms has increased the risk of identity crime and it also promotes establishment of a separate industry based on the trade of personal identification information. Another mode by which some of the attackers steal information is by requesting permission to access personal information through falsely projected pages. When the targeted user grants the permission, the attackers can easily access information and can misuse the same without the knowledge or permission of the users Research conducted at Carnegie Melon University suggests that biggest bunch of social networking users who are victimized by identity criminals are between the age group of 15 to 25 years. It can also be looked up in the literature that young users are unaware but are still not bothered about the privacy settings offered by the social networking sites. Posting updates is the favorite pastime for the youngsters. It has been found by Staista, 2014 that the account of the users can be hacked and someone else can post updates on their behalf which can be different and peculiar, leading to problems for the users.

Protecting the personal content from malicious attacks is one of the major challenges being faced by the developers of website, especially social network providers. Social Network Privacy issue has been discussed by Several researchers (Gangopadhyay, S. et. al.,2014). According to researchers, in the year 2009, the information given by a user became 'more and more' public by default. This has happened not only because of information or updates given, but also providing the access to one's profiles like seeing photos as well as the list of friends which one might wish to keep private. These changes have made the personal data public for others without the knowledge of the users. In 2011, facebook has introduced some more setting changes, which even allowed the users, who are not even in the friends list to access the personal information.

According to Jo Pierson and Rob Heyman, 2011, the Internet

Cookie is considered to be the most powerful tool for collecting personal identifiable information. In 1994 Cookies were basically developed to give websites a memory or state, a configuration last used by a user and is known as Fisrt party http cookie. It is automatically sent to the user's browser, when the user interacts with the website. Another type of cookie is placed through advertisements, images or scripts hosted on a first party website by a third party server and are known as third party cookies.

Social media, needs third party cookies to get state information through different websites so as to ensure an optimal working service. Facebook, Google Buzz plugin and Twitter's tweet button gather's user's data in this way and hence can track the users. This is problematic as users have not accepted to be tracked via the plugins, which are not even used by them.

Unitied Virtualities have implemented "Zombie Cookies" as 30 percent of the internet user's were deleting http cookies. These cookies are tagged to the user's browser . These can not be deleted by any commercially available adware, spyware or malware removal program.

The challenges of user's disempowerment and online privacy can be dealt at user level, technology level and on policy level. At the user level, the communication between the consumers and consumer groups has to be controlled and this is to be supported at technological level by introducing new techniques for tracking and exposing online consumer behavior. To control the misuse of the personal data, policy needs to be enforced to address transparency and awareness, by which users can know about the exchange taking place, which is further required to be addressed by the researchers. E.g with the social network site Buzz by Google. At the launch on 9 February 2010 Google Buzz automatically, without asking, published openly all personal networks of users based on the people they interact with via Gmail. However, e-mail contact lists can hold very private information, like names of personal physicians, romantic relationships or the identities of anti-government activists. They wrongfully assumed that information in one context (of e-mail correspondence like Gmail) could be disclosed without any problem in another setting (of social network relationships like Buzz).

In order to achieve a high level of privacy, literature discusses online privacy setting techniques to prevent the identity crime. The users should be authorized to govern their privacy settings whenever they receive or requests a service related to their personal details. Online privacy protection settings, that allow the user to control the profile view and distribution of personal data, vary across social networking websites, and there is no privacy standard for controlling the user 's personal information settings. Although privacy settings should be chosen carefully, most online social network providers have complex privacy settings. These complex privacy settings may cause confusion among users. There is the 'Help' option too that provide help to the users to clarify their concerns (Gangopadhyay, S. et. al.,2014), but it was found that very less number of people use it. As a result, the major problems being faced by the young users of social networking site are identifying theft, hacking and commenting on controversies. Young users between the age group of 15 to 25 years are usually unaware about the privacy Settings offered by the social networking sites. Also, they do not hesitate in sharing their personal details and photographs and they believe that their close friends are the only one who are sharing their updates and as a result their accounts can be hacked and they may receive disgraceful posts.

To avoid the hacking of personal data and its misuse. It suggests that the users should be more careful about adding friends while using social networking sites. Further, the public access to the private information should be restrained, also frequent changing of passwords is advisable to keep the accounts safe One potential way to mitigate privacy risk is to use different settings with targeted disclosure - that is, using different privacy settings for different posts. For example, It has been observed by Fiesler, C. . et. al., 2017, that the users were controlling the use of emotional or self expressive content Ad-hoc strategies are also adopted by the Facebook to prevent privacy threats. Overall, on social networking, privacy management are complex and encompassing a range of strategies.

In addition to above following data protection techniques are also suggested by researchers:

1.Stronger authentication methods: Server side authentication should always be adopted so that the server should know the identity of the user. Client side authentication is to be performed so that the request for the information can be processed by the server being requested. Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints. Client side authentication usually involves the server giving a certificate to the client in which a trusted third party, that the server belongs to the entity that the client expects it to connect can be verified. Social networking accounts should be protected with the usage of strong password and using different passwords on different social networking sites.

2.Usage of HTTPS to secure the user's connection to the site is recommended as it introduces encryption to provide security.

3.One should be Cautious while replying to emails sent through social networking sites to avoid spoofed attacks sent by cyber criminals.

4.Suspected Malicious Links/scams should not be clicked to avoid any attempt to infect the system. Apps like games should not be installed as these apps may have full access to the user's account and their private information.

Limitations of using social networking sites as revealed in literature talks about data privacy threats and other threats being encountered by the users of social networking sites. These are decreased productivity, more resource utilization, Viruses and Malware attacks, Access to personal web log or different social networking website account by Cyber criminals. The productivity of employees in an organization has been affected as they will be involved in changing their profile information or accessing the sites throughout the day. The users will be accessing the video links which will increase the price of web browsing. Attackers use social networks as a channel to spread viruses and malware. Since the associated risks as discussed above are more corresponding to profile data hacking, therefore, the motivation of the research is to secure private data of the social networking users. Next section will explain the data privacy attacks caused due to limitations of existing applications and widgets in social networking site.

LIMITATIONS OF EXISTING APPLICATIONS & WIDGETS IN SOCIAL NETWORKS

Some social networks allow active content to be embedded in the form of applications or widgets. These applications can then interact with the user and his group of friends. A simple example would be a daily joke application, which posts a new humorous joke to the user's profile site every day for the user and the user's friend's amusement. More complex applications are also possible, like multiplayer games or photo rotation albums.

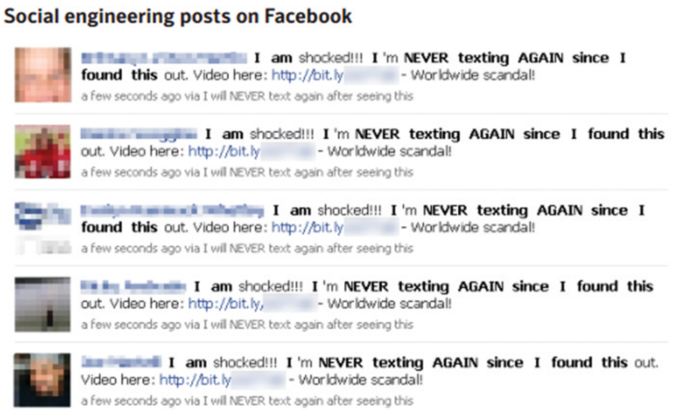
Wuest, C., Symantec found that each social network has its own way of implementing applications and embedding active content. Some allow remote code to be included in their application, which poses a great risk as it is hard to control the data which will be loaded on the site. Larger networks have created their own APIs, which allows developers to access specific information from the user's accounts. Unfortunately, that sometimes allows them to covertly access some information or even attack users or other applications.

The following section shows some examples of attacks. In first example, researchers observed that how a video shared by Facebook user's messages through malware (Wuest, C., Symantec) and in second example, we found that how other websites take user's information without any permission.

Personal Data Attacks Due to Sharing of Video on Social Network

In July 2010 around 300,000 people fell for a shady application in Facebook. Suddenly more and more personal profiles started showing a message with the following text:

I am shocked!!! I'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly/[REMOVED] - Worldwide scandal!



Social engineering posts on Facebook

[redacted] I am shocked!!! I 'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly[redacted] - Worldwide scandal!
a few seconds ago via I will NEVER text again after seeing this

[redacted] I am shocked!!! I 'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly[redacted] - Worldwide scandal!
a few seconds ago via I will NEVER text again after seeing this

[redacted] I am shocked!!! I 'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly[redacted] - Worldwide scandal!
a few seconds ago via I will NEVER text again after seeing this

[redacted] I am shocked!!! I 'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly/[redacted] - Worldwide scandal!
a few seconds ago via I will NEVER text again after seeing this

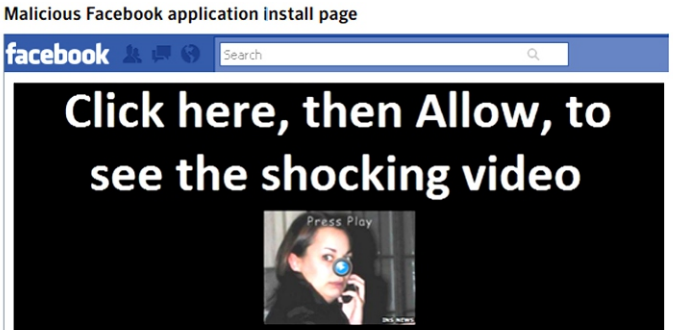
[redacted] I am shocked!!! I 'm NEVER texting AGAIN since I found this out. Video here: http://bit.ly[redacted] - Worldwide scandal!
a few seconds ago via I will NEVER text again after seeing this

Analyzing the click statistics for this specific short URL revealed nearly 300,000 clicks. If an inquisitive user clicks on the shortened link he or she is redirected to a Facebook application. The names and URLs of the application vary. For example:

http://apps.facebook.com/wonttextagain/

http://apps.facebook.com/nevertxtingagain/

The list of application names grows and grows. This is because Facebook bans such applications as soon as they are discovered, but the malware author re-registers them under a new name in order to keep the attack working(Wuest, C., Symantec). The Malicious Facebook application's Installation page is shown in Figure 1 below:

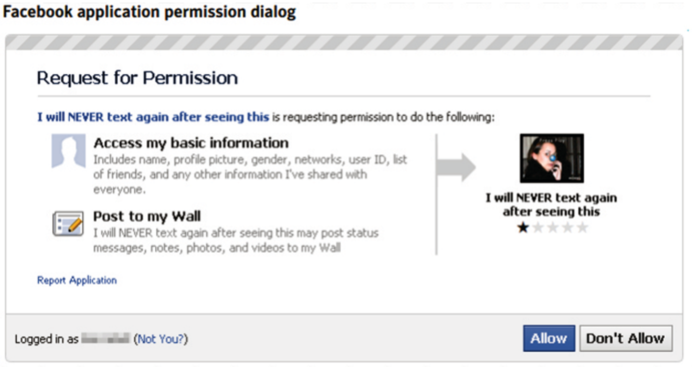


Malicious Facebook application install page

Click here, then Allow, to see the shocking video

Figure 1: Malicious Facebook Application's Installation Page

Clicking on the Facebook application starts the application installation process. In order to fulfill its shady business the application requests some elevated privileges from the user, as seen in Figure 2:



Facebook application permission dialog

Request for Permission

I will NEVER text again after seeing this is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Post to my Wall
I will NEVER text again after seeing this may post status messages, notes, photos, and videos to my Wall

I will NEVER text again after seeing this
★☆☆☆☆

Report Application

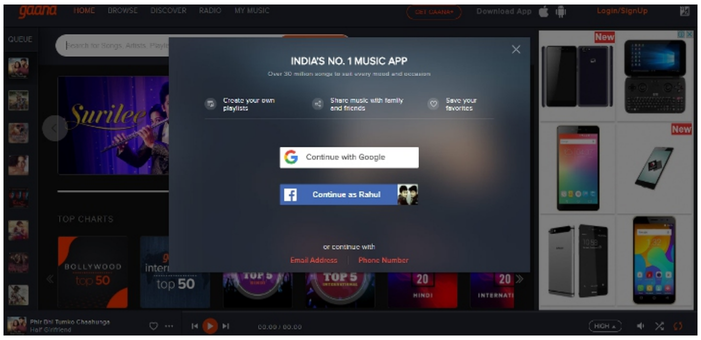
Logged in as [redacted] (Not You?)

Figure 2: Facebook Applications's Permission Dialog Box

Personal Data Attacks Due to Usage of Music Application Ganna.com

While visiting some websites, we observed that there is only server side authentication through Facebook or google and mostly users easily ignore this and share their information for using website services.

Figure 3 below shows India's most famous music app gaana.com, which plays song online for users, but If user login through Facebook, it will ask for sharing information for using the services of the application.



INDIA'S NO. 1 MUSIC APP

Over 30 million songs to suit every mood and occasion

Create your own playlists

Share music with family and friends

Save your favorites

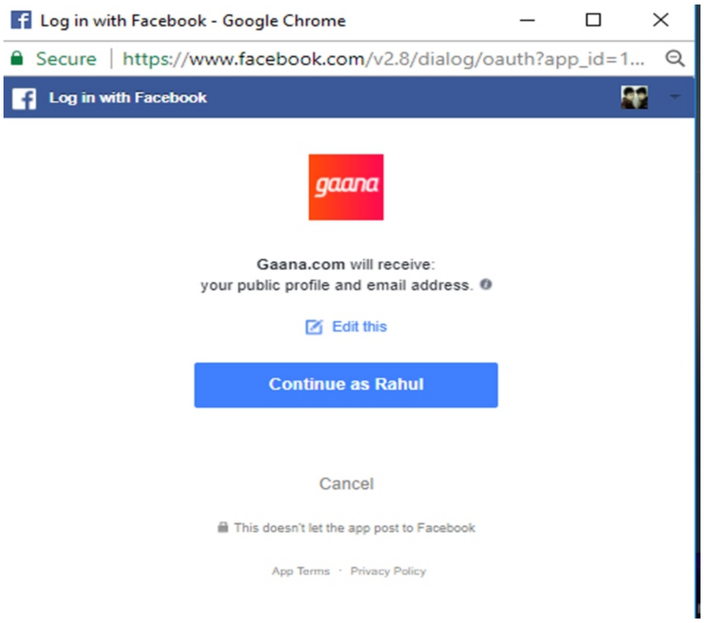
Continue with Google

Continue as Rahul

or continue with

Email Address | Phone Number

Figure 3: Gaana.com


Log in with Facebook - Google Chrome

Secure | https://www.facebook.com/v2.8/dialog/oauth?app_id=1...

Log in with Facebook

Gaana.com will receive:
your public profile and email address.

Edit this

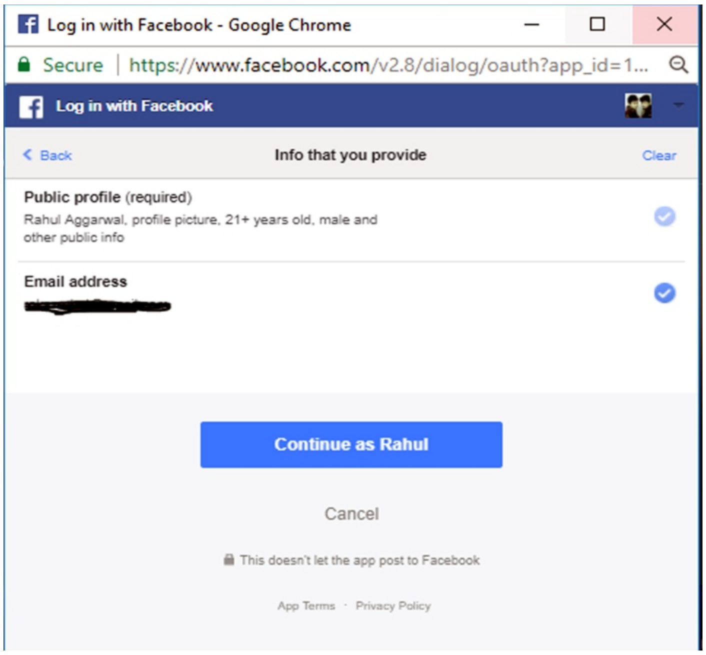
Continue as Rahul

Cancel

This doesn't let the app post to Facebook

App Terms · Privacy Policy

Figure 3: Ganna.com asks for sharing information


Log in with Facebook - Google Chrome

Secure | https://www.facebook.com/v2.8/dialog/oauth?app_id=1...

Log in with Facebook

< Back | Info that you provide | Clear

Public profile (required)
Rahul Aggarwal, profile picture, 21+ years old, male and other public info ✓

Email address ✓
[redacted]

Continue as Rahul

Cancel

This doesn't let the app post to Facebook

App Terms · Privacy Policy

Figure 4: Editing page for sharing information

In Figure 3, Gaana.com asks for sharing user's public profile. If user clicks on “Edit this”, another dialog box will open (Figure 4 : right side figure) which will show what information the user is going to share. With one click, the whole user's datasets will be shared. These datasets may be in the form of API's which carry every user's information which is submitted by the user at the time of signup. Working of these applications has been explained below:

Working of Existing Applications

Most social networks allow applications to have a wide variety of access to user's data through different interfaces. Some provide documented Application Programming Interfaces(APIs) that allow specific access to pieces of information. Depending on its type, the application can be anchored deep within the social network and melded within the user interface. Alternatively, it could just interact on a loose level, displaying some partial information on a different website(Go-Gulf., 2014)

As an example, Facebook has two basic application types. First, there are social plugins, which allow the integration of basic Facebook features onto any website. Canvas applications, which do interact with the profile, can send update messages or open a new page, which in turn can contain nearly anything. Since 2010, Facebook requires any new developer to confirm their identity either by the help of a working mobile phone number or a credit card number.

This is done in order to combat anonymous developers registering dummy accounts for malicious applications.Unfortunately, this does not make it impossible to registeranonymous accounts with anonymous phone numbers which are still available in some countries. It has been suggested by the researchers (Wuest C., Symantec) that following list of some of the information an application can get permission for:

- Access the public information— this includes the user's name, profile picture, list of friends, and all other public parts of the profile.

- Access the profile information— this includes any additional information, such as birthday, favorite movies and books, etc.

- Send email— this means sending direct emails to the registered email address.

- Access posts in the News feed— this allows the application to read the posted messages.

- Access family and relationships information

- Access photos and videos

- Access friends' information— this includes their details, birthdays, etc.

- Access the data at any time— this means the application can access the data even if the user is logged out and not using the application at that moment.

- Post to the wall— add new message posts on the user's behalf.

There is server side authentication through Facebook which take these permissions from user for sharing information. If User allows these permissions whole API will be shared to that unsecure page and that page can save the data into database. This data can be shared to big companies for promotion and other purposes.

Research Gaps in the Existing Applications

Above reviews state that an application could get access to nearly all information that a user has entered in their profile, given that the user grants the permission to do so. Since the applications are allowed to load remote scripts, it is not possible to conclusively say what does happen to the user information and how it is processed. An application could easily store all the accessible information on an offsite database and use it later.

There is no client side authentication to stop sharing of the user information to the other users of the application. The users should be made aware of the data, which will be shared to other users through the warning box. In the current research the client side authentication technique has been proposed and is being explained in the next section.

RESEARCH METHODOLOGY

As a research methodology, a comprehensive approach has been followed which in turn is a two-fold process. During first process, research gaps have been identified based on the existing literature resulting to which, Privacy Ensurer Extension has been designed by dint of top-down approach. Adhering to the procedure of top-down approach, firstly problem is being identified and then solution is find out by splitting up the problem under study at various levels. According to literature survey as explained above, it has been realized that there is a requisite to develop a technique which is proficient of warning the users whenever malicious attack occurs during web browsing. As a solution to this problem, we proposed a Google Chrome extension which is developed and added. Subsequently, as a part of second process of our research methodology, the proposed technique is tested against the third party-attacks during web browsing. For this, data survey was conducted by eighty trained users for analyzing the successful and satisfactory execution of the extension on various social networks. The below mentioned section explains the proposed personal data privacy technique, its design and, algorithm.

PROPOSED PERSONAL DATA PRIVACY TECHNIQUE

Privacy Ensurer, a browser extension application has been proposed to provide client side authentication. The application will work when user clicks on link of unauthorized page on Facebook or on other social networking sites. This extension application works through OAUTH keyword in the URL which is used to provide the authentication of transferring the user data like name, profile picture, gender, friend's information to other pages. If user wants to continue for redirection, then he can click on -Ok button on alert box. If not, then he can click on cancel button. Details of the Privacy Ensurer, its design and implementation has been explained below:

DESIGN METHODOLOGY OF PRIVACY ENSURER (Extension for browser)

A Browser Extension is a plug-in that extends or adds to the functionality of a web browser. Also web technologies like HTML, Javascript, CSS are used to develop web extensions. Others are developed using machine code and application programming interfaces (APIs) provided by web browsers, such as Netscape Plugin Application Programming Interface (NPAPI) and PPAPI. Browser extensions can even make changes in the user created interface.

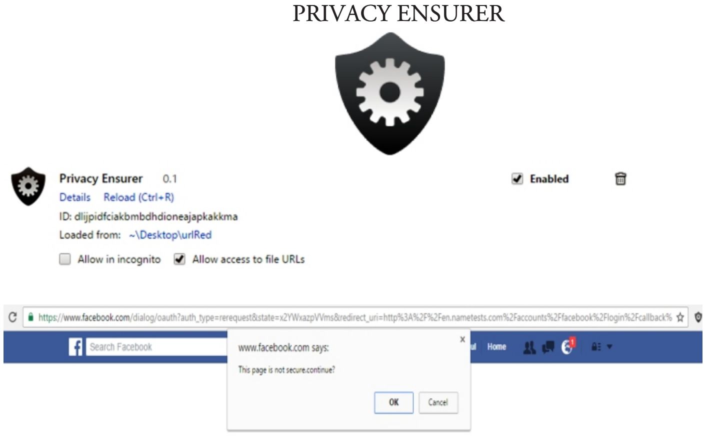
Privacy Ensurer is a browser extension which is used to warn user whenever his personal information transfers from social network to other web pages.

The word “oauth” is very common in URLs where authentication is required, as shown by a study of URLs of various networking sites.

OAuth 2 is a framework for authorization, in which the applications are enabled to access to user accounts on an HTTP service, such as GitHub, Facebook, Linkedin and DigitalOcean. The working of OAuth 2 is based on delegation of user authentication to the service that hosts the user account, and third-party applications are authorized to access the user account. OAuth 2 provides authorization flows not only for desktop and web applications but also for mobile devices. When there is call for users datasets or API's then Oauth token is sent to servers for giving permission for sharing the information in the form of API's to other sites. OAuth2 works through passing access and refresh tokens between the apps. OAuth defines four roles:

- Resource Owner
- Client
- Resource Server
- Authorization Server

Whenever this “oauth” word is encountered while using these applications, privacy ensurer will warn the user with an alert box as shown in Figure 5.



Privacy Ensurer 0.1
Details Reload (Ctrl+R)
ID: dlijpidfciakbmbdhdioneajapkakkma
Loaded from: ~\Desktop\urlRed
☐ Allow in incognito ☑ Allow access to file URLs
☑ Enabled

https://www.facebook.com/dialog/oauth?auth_type=rerequest&state=x2YWxazpVVms&redirect_uri=http%3A%2F%2Fen.nametests.com%2Faccounts%2Ffacebook%2Flogin%2Fcallback%

www.facebook.com says:
This page is not secure.continue?
OK Cancel

Figure 5: Privacy Ensurer Alert Box

Design of Privacy Ensurer Algorithm: The proposed algorithm to implement a privacy ensurer browser extension has been designed using top down approach. Once the user has logged in and tries to click the unsecure page link, it will confirm from the owner's page whether the data can be shared or not.

Once found ok it will continue otherwise the message will be redirected to the Facebook page of user.

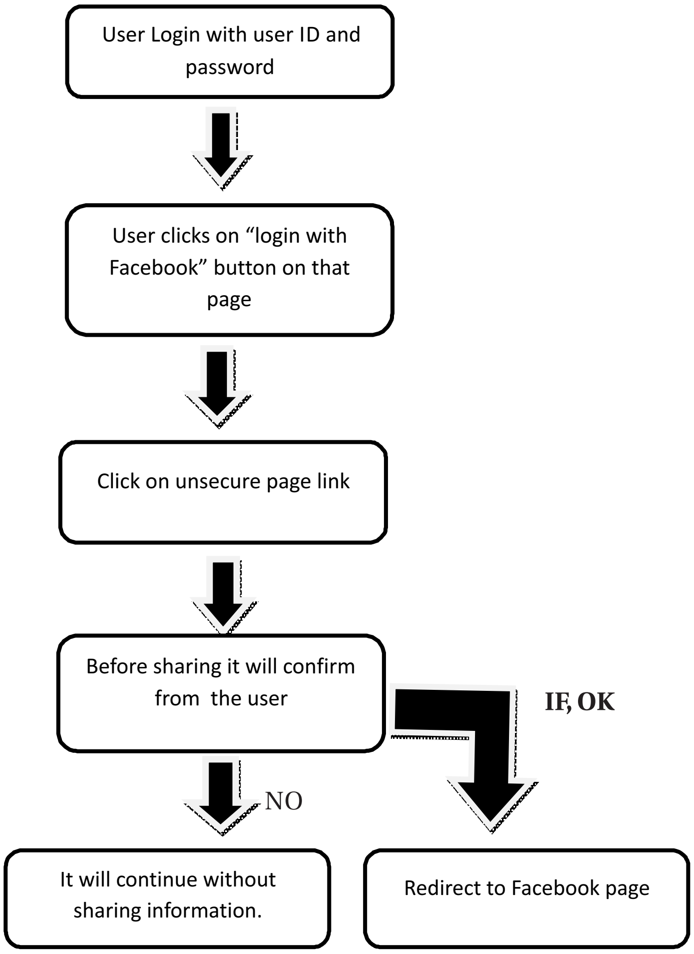

User Login with user ID and password
User clicks on “login with Facebook” button on that page
Click on unsecure page link
Before sharing it will confirm from the user
IF, OK
NO
It will continue without sharing information.
Redirect to Facebook page

Figure 6: Flow Chart- Showing Steps for Privacy Ensurer

Implementation of Algorithm

We have developed a packed extension and then loaded it into Chrome browser.

The program has been developed using JavaScript and JSON. Back.js implements backend JavaScript code. It will search “OAUTH” keyword from URL and confirm user with a warning box.

Back.js

```
var page_url = location.href;          // variable 'page_url' is used to store page url

if (page_url.search("oauth") >= 0) { //page_url.search function is used to check ouath Keyword in the page url

if(confirm("This page is not secure.continue?") != true) //Confirm function is used to confirm from the user to continue further or not after displaying the message that “this page is not secure”

{

        window.location.replace("http:/facebook.com"); //redirect back to facebook

}

}
```

Every extension has a JSON-formatted manifest file, named manifest.json that provides important information. This manifest file describes all important information about our extension.

Manifest.json

```
{

"manifest_version": 2,        //The version of the manifest file format is specified, that our extension package requires.

"name": "Privacy Ensurer",        //The name  manifest properties are short, plain text used to identify the name of extension.

"version": "0.1",        //One to four dot-separated integers are used to identify the version of the extension.

"default_locale": "en",        //Specifies the subdirectory of _locales that contains the default language for this extension.

"description": "For securing your data from social network sites",        //A plain text  that describes the extension. It specifies task performed by extension.

"browser_action": {

"default_icon": "icon.png”

},  //set icon. png as default icon and put in the main google Chrome toolbar, to the right of the address bar.

"content_security_policy": "defined",        //To mitigate a large class of potential cross-site scripting issues, Chrome's extension system is working on the general concept of content security policy.

"devtools_page":"devtools.html",        //A DevTools file extension adds functionality to the Chrome DevTools for the extension.

"permissions":["tabs"],        //To use most chrome APIs, this extension  must declare its intent in the "permissions" field of the manifest. It gives permission to access any tab.

"content_scripts": [

{
```

```
"matches": [
 "<all_urls>" //here it is used to apply script on all urls
  ],
"js": ["back.js"]
   }
]      //This property has JavaScript files that run in the context of all the web pages. By using the standard Document object model (DOM), we can easily read details of the web pages the browser visits, or working on it accordingly.
}
```

Steps for adding Privacy Ensurer Extension in Google Chrome-

Privacy Ensurer extension can be added by following the steps mentioned below :

Google Chrome is to be opened

Three dots on the upper left corner to be clicked

Settings option to be chosen

Extension Option to be selected

Figure 7 shows the illustrative representation of all the steps to be followed to add Privacy Ensurer Extension in Google Chrome.

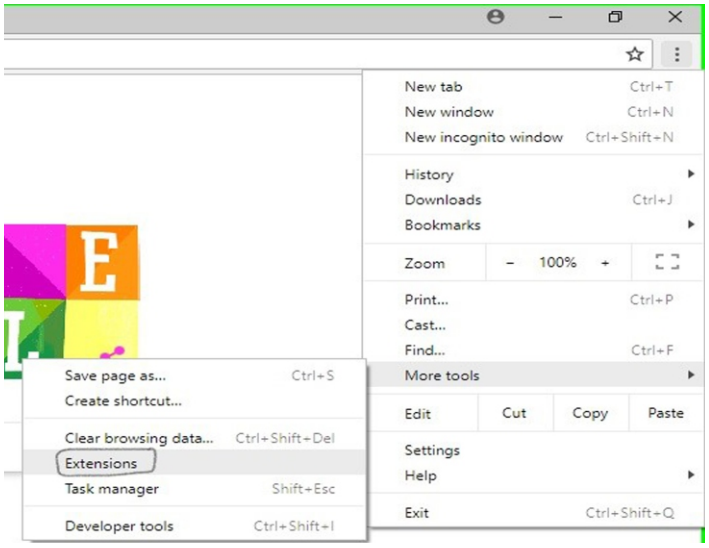
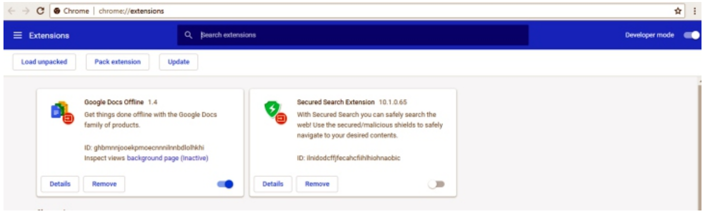


Figure 7: Adding Privacy Ensurer to Google Chrome

Once the pack extension is loaded, extension icon will be visible with other extensions as shown in Figure 8.After activating the extension icon, users will receive the warning alert whenever there are malicious web-browsing attacks.



Google Docs Offline 1.4

Get things done offline with the Google Docs family of products.

ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi

Inspect views background page (Inactive)

Secured Search Extension 10.1.0.65

With Secured Search you can safely search the web! Use the secured/malicious shields to safely navigate to your desired contents.

ID: ilnidodcffjfecahcfihlhiohnaobic

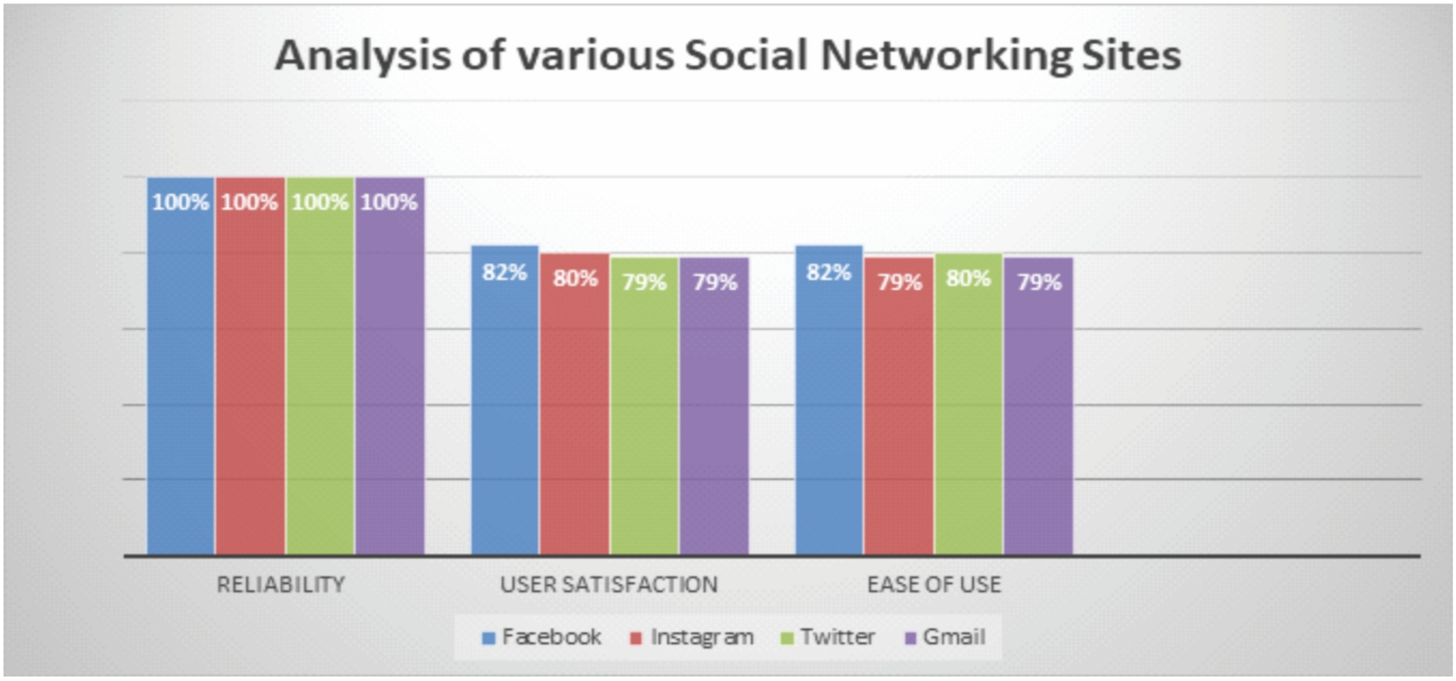
Figure 8: Extension ICON

Data Survey on Various Social Networks

As conferred earlier in research methodology, survey has been conducted on 80 trained users. By trained users, here we meant that users have been given the prior knowledge of installing and activating the Privacy Ensurer extension in their respective web browsers. Succeeding to this, proposed extension has been analysed based on the four parameters Reliability of the Extension, User Satisfaction for the raised Alert box and Ease of access for the user on various Social Networking sites i.e Facebook, Instagram, Twitter and Gmail. Statistics of the same has been shown below in Table 1. An average of 100%, 80% and 80% has been achieved against reliability, user satisfaction and ease of use corresponding to the four social networking sites under survey.

Table 1 : Analysis of the Data Survey on Various Social Networks

Parameters	**Facebook**	**Instagram**	**Twitter**	**Gmail**	**Average**
Reliability	100 %	100 %	100 %	100 %	100 %
User satisfaction	82%	80%	79%	79%	80%
Ease of use	82%	79%	80%	79%	80%



Graph 1: Parameter wise analysis of various Social Networking Sites

The statistics show that 100 percentage of the users are getting access to the extension, 80 percent users are satisfied for the alert being sent as warning and 80 percent user's can easily access the extension.

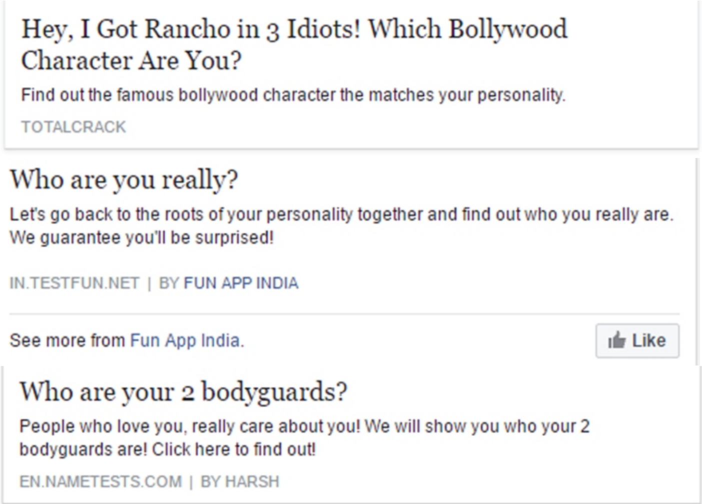
IMPLICATIONS FOR SOCIAL NETWORK USERS

Our paper has practical implications for the social network users. By installing the extension on Google Chrome personal data security has been provided to the users by sending an alert to the users seeking his permission to made the data available for other users or not. The existing privacy extensions on the Google Chrome uses Virtual Private Network and are encrypting the data so that third party can not steal the data. But in literature, there have been several attacks recorded against Virtual Private Nertwork secured traffic through Cookie Syncronization being used widely by third parties for advertisement and tracking purposes. Therefore, as per the statistical analysis , since 80 or 100 percentage of the users are satisfied on the individual parameters the extension developed can be adopted for the social network users.

TESTING AND RESULT OBTAINED

The proposed algorithm was implemented and tested on a extension application as discussed above. The extension was primarily developed using JavaScript and supported by multiple users. While testing, the extension was installed using Chrome browser. Around eighty users have executed the application and clicks are performed on many links and it has been observed that on every click, a notification pop up is shown on web browser asking for permissions for sharing data of social network sites. Example below shows how clicking on some links will lead to data leakage for the attackers and the same can be avoided by asking for the permission to share the data and continue through Alert Box as shown in Figure 10.

Some links are given below that are examples of applications through which user's personal data can be accessed. Clicking on these links will take the user to a new and attractive page as shown in Figure 9.



Hey, I Got Rancho in 3 Idiots! Which Bollywood Character Are You?

Find out the famous bollywood character the matches your personality.

TOTALCRACK

Who are you really?

Let's go back to the roots of your personality together and find out who you really are. We guarantee you'll be surprised!

IN.TESTFUN.NET | BY FUN APP INDIA

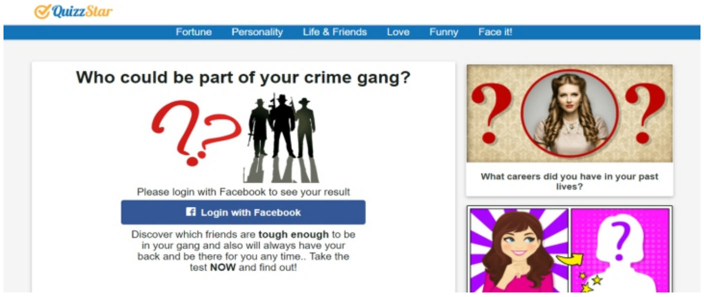
See more from Fun App India.

Who are your 2 bodyguards?

People who love you, really care about you! We will show you who your 2 bodyguards are! Click here to find out!

EN.NAMETESTS.COM | BY HARSH

Pages that look fun actually take the user's information. After clicking on the above link it will redirect the page that looks like following:



Who could be part of your crime gang?

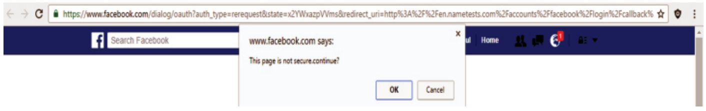
Please login with Facebook to see your result

Discover which friends are **tough enough** to be in your gang and also will always have your back and be there for you any time.. Take the test **NOW** and find out!

What careers did you have in your past lives?

Figure 9: Unauthorized page

Whenever the word “oauth” is encountered in the URL an alert box will pop up as shown in Figure 8. Alert box will ask for the users interest to continue with the personal information being shared to other webpage as shown in Figure 8 or to go back to the home page.



https://www.facebook.com/dialog/oauth?auth_type=rerequest&state=x2YWxazpVVms&redirect_uri=http%3A%2F%2Fen.nametests.com%2Faccounts%2Ffacebook%2Flogin%2Fcallback%

www.facebook.com says:

This page is not secure.continue?

Figure 10: Asking for Permission for Sharing the Personal Data

CONCLUSION

Technology and social networks have made interaction and communication much easier than in the early decade. As social networking has become too popular, people are more concerned about their data privacy issues. In this paper, we have briefly explained the privacy threats, limitations of the existing social network techniques and the associated data privacy risks. It has been observed that personal data is not safe on social networks, as almost everything being posted or shared on social media platforms can be accessed by others, even those who are not in the friend list of the user. We have proposed a technique to avoid data privacy threats to the user through privacy ensurer, an extension of browser. Privacy Ensurer is a client side awareness that can be downloaded as a plug in to warn the users every time about the information leakage threat. The adoption of the privacy ensurer extension by the social networking sites will be beneficial for the users to provide data privacy on social networks.

REFERENCES

I. B2BInternationalInConjunction and KasperskyLab, "CONSUMER SECURITY RISKS SURVEY 2014: MULTI-DEVICE THREATS IN A MULTI-DEVICE WORLD," Kaspersky Lab, 2014.

ii Binden W., Jormae, M., Zain, Z.,and Ibrahim, J., "Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks," International Journal of Scientific and Research Publications, vol. 4, no. 1, pp. 1-6, 2014.

iii Chen, X. and Shi, S., "A Literature Review of Privacy Research on Social Network Sites," International Conference on Multimedia Information Networking and Security, pp. 93-97, 2009.

iv Chewae, M.,Hayikader, S., “How Much Privacy We Still Have on Social Network “ International Journal of scientific and research Publications, Volumn 5, Issue 1, January 2015. ISSN 2250-3153

v Debatin, Bernhard, Lovejoy, Jennette P., Horn, ANNkathrin, And Hughes, Brittany N.(2009). “Facebook and Online privacy: Attitutdes, Behaviors, and Unintended Consequences”, Journal of Computer- Mediated Communication, 15(1), 83-108

vi Dhami A., Agarwal, N., Chakraborty, T. K., Singh B. P., and Minj, J. "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook," 3rd IEEE International Advance Computing Conference (IACC), pp. 465-469, 2013.

vii Dwyer, Catherine, Hiltz, S., and Passerini, K., "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace." AMCIS 2007 Proceedings (2007): 339.

viii Dwyer, Catherine, Hiltz, S., and Passerini, K., "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and Myspace." AMCIS 2007 Proceedings (2007): 339.

ix Fiesler, C., Dye, M., ”Privacy Settings and Social Media Content Sharing”, ACM978-1-4503-4335-0/17/03DOI: http://dx.doi.org/10.1145/2998181.2998223.

x Gangopadhyay, S., Dhar, D. “Social Networking Sites and Privacy Issues Concerning Youths” Global Media Journal-Indian Edition Sponsored by the University of Calcutta/www.caluniv.ac.in ISSN 2249 - 5835 Summer Issue/June 2014/Vol. 5/No. 1.

xi Ge, J., Peng, J., and Chen,Z.,"Your Privacy Information are Leaking When You Surfing on the Social Networks: A Survey of the degree of online selfdisclosure (DOSD)," IEEE 13th Int'l Conf. on Cognitive Informatics & Cognitive Computing (ICCI*CC'14), pp. 329-336, 2014.

xii "GO-Gulf," GO Gulf Web Design Dubai Company, [Online]. Available:http://www.go-gulf.ae/blog/what-people-share-on-socialnetworks/. October 2014.

xiii Holm, E. (2014). “Social networking and identity theft in the digital society”. The International Journal on Advances in Life Sciences, 6(3&4), 157-166.

xiv Jagatic,T.,Johnson, N. Jakobsson, M., & Menczer, F. (2007) “Social phishing”, Communications of the ACM, 5(10), 94-100.

xv Jain, P., Paridhi Jain and Kumaraguru, P.” Call Me MayBe: Understanding Nature and Risks of Sharing Mobile Numbers on Online Social Networks”

xvi Jo Pierson and Rob Heyman. "Social media and cookies: challenges for online privacy", Info, Volume 13 Number 6, 2011.

xvii Kumar, A., Gupta,K.S., Rai, K. A., Sinha, S., “Social Networking Sites and Their Security Issues” International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153.

xviii Lucas, Matthew M., and Borisov, N., "Flybynight: mitigating the privacy risks of social networking." Proceedings of the 7th ACM workshop on Privacy in the electronic society. ACM, 2008.

xix Lucas, Matthew M., and Borisov, N., "Flybynight: Mitigating The Privacy Risks Of Social Networking.", Proceedings of the 7th ACM workshop on Privacy in the electronic society. ACM, 2008.

xx P.Krubhala, P.Niranjana, G.Sindhu Priya, “Online Social Network A Threat to Privacy and Security of Human Society” International Journal of Scientific and Research Publications, Volume 5, Issue 4, April 2015 1 ISSN 2250-3153.

xxi P. Panagiotis, K. Nicolas and M.P.Evangelos, “Exclusive : How the (synced) Cookie Monster breached my encrypted VPN session”, ACM ISBN 978-1-4503-5652-7/18/04, 2018

xxii Raji, F.,Miri, A.and Jazi, M. D., "Preserving Privacy in Online Social Networks," Springer-Verlag Berlin Heidelberg 2012, pp. 1-13, 2012.

xxiii "Social Networks: Global Sites Ranked by Users 2014 | Statistic." Statista. Web. 7 Nov. 2014.

xxiv Srivastava, A. and Geethakumari G., "A Framework to Customize Privacy Settings of Online Social Network Users," IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 187-192, 2013.

xxv Srivastava, A. and Geethakumari, G., "Measuring Privacy Leaks in Online Social Networks," International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2095-2100, 2013.

xxvi Statista, "Statista," October 2014. http://www.statista.com/statistics/272014/global-social-networks-rankedbynumber-of-users/.

xxvii “Suit over sale of MySpace dismissed". seattlepi.com. October 9, 2006. Retrieved October 23, 2011.

xxviii Wüest, C., “The Risks of Social Networking” Symantec.

xxix “Understanding Authentication, Authorization, and encryption”,http://www.bu.edu/tech/about/security-resources/bestpractice/auth/