

# Security breaches in Social Networking

Lovi Gupta

*M.tech Student, KITE, Jaipur*

**Abstract - Social networking sites offer a straightforward way for people to have a simple social presence through web. They provide a virtual environment for people to share each and every activity, their interests, and their circle of acquaintance with their family, friends, or even the unknown. With so much sharing, hackers and thieves have found very easy ways to steal personal information through these networking sites. This calls for advances in security protocols to safeguard against hackers which form the basis of this research. In this paper, we will discuss some of the privacy and security concerns, attacks and their respective prevention techniques. In this paper we propose an architecture for secure request response exchange of data between users. This architecture improves the customization of profiles. Our research suggests that only a proper knowledge of the hacking strategies will prove the best defence in the war against cyber-attacks.**






**Keywords: Social Networking sites, security, privacy, secure request-response data exchange , prevention strategies, survey.**

## I. INTRODUCTION

Social networks are one of the easiest forms of communication these days. They reflect the social image of a person. They can keep you glued to your *avatar* for hours together and make you forget about the whole physical world around you. The network of social relations that build up during your everyday life can be simply translated onto your “*profile*” and made available for the whole of your friends to see. Then there is a concept of “*following*” that can turn a nomad into a rockstar. The world of pictures you share *live* has only made your presence felt more. It all seems so entertaining that one would seldom think of leaving this “world” and becoming an offline monk. But the more comfortable and attached we become with these sites, the more casual and careless we are to share personal details about ourselves.

People, hundreds of millions of them, use a wide variety of social networking sites (SNSs) that seem no less than a menu card in a restaurant. Facebook, the world’s leading social networking site, for example, has more users than the population of many of the countries combined. There is absolutely no doubt that social networks have become a part of every internet user these days and the trend is only set to increase. Figures suggest that there were about 1 billion social network users in 2012, representing a 19.2% increase over 2011 figures.

Table 1  
Five biggest social networking sites as of May 2014

Rank	Network	Number of Users (in millions)	Monthly Visits (in millions)
1		901	7012.9
2		555	182.1
3		170	61
4		150	85.7
5		11.7	104.4

Even though the use of social network web sites and applications is increasingly day by day but users are not aware of the risks associated with uploading sensitive information. The reason why cyber-conspirators prey on these networks is because users upload their personal information that commonly include their interests, social relationships, pictures, confidential information and other media content, and share this information to the whole world via SNSs which are very easily accessible. Employees, too, unknowingly share plethora of personal information on SNS thus putting their corporate infrastructure and data at a risk. The volume and ease of accessibility of personal information available on these sites have attracted malicious people who seek to exploit

this information. Due to the sensitivity of information stored within social networking sites, intensive research in the area of information security has become an area of paramount importance.

Facts reveal that the majority of social media users post risky information online, unaware of the privacy and security concerns. Social networking sites are meant to get as many users in one place as possible on one platform and for attackers there's a lot of return-on-investment in going after them. The values at the core of networking sites – openness, connecting, and sharing with others - unfortunately are the very aspects which allow cyber criminals to use these sites as a weapon for various crimes. Without a careful security policy in place, the entertaining face of social networking could easily compromise on the social stature of an individual. The dramatic rise in attacks in the last year tell us that social networks and their millions of users have to do a lot more to protect themselves from organized cybercrime, or risk failing to identity theft schemes, scams, and malware attacks. Understanding these risks and challenges should be addressed to avoid potential loss of private and personal information. Social networking definitely needs to be integrated into the information security policy and user education.

## II. PRIVACY ISSUES

### *2.1 Security risks*

With increasing use of SNSs, the associated security risks are also increasing tremendously. Some of the security risks are identity theft, phishing, scam, cyber bullying etc. People use to provide their personal data on SNSs like facebook, twitter etc. This data is stored in SNS and in lack of proper security techniques implemented in SNSs, It is not secure.

### *2.2 Identity Theft*

Some of the attackers attack through the application in which they ask permission for accessing the information provided in the profile of SNS. When a user allows to do so, they get all the information and can misuse that easily without the user knowledge or permissions.

### *2.3 Phishing*

Phishing in SNS began in 2007[3]. The purpose of phishing is to harm economically that is the phishers try to retrieve the profile information to know about the banking or the financial information of the users.

### *2.4 Profiling Risk*

Profiling risk is the risk associated with profile cloning. The attackers retrieve the personal information of the users and make a clone of the profile [2]. They do so to make their social image bad or for other purposes like knowing about friends of victims. This is the most popular security risk associated with the SNSs because it is very easy to do without the permission of the user. There is nearly no security for profile cloning in SNSs. There is another way of profile cloning that is “cross-site profile cloning”. In this the attacker steals information from one social networking site and uses this information to make a profile on another social networking site.

### *2.5 Fake Product Sale*

The attacker advertise on the SNSs for selling the products offering huge discount and when the user clicks on the products advertisement their profile information goes to the attackers. Sometimes when user tries to purchase and give their account information for payment, all the account information is retrieved by the attackers and they misuse this information.

## III. ATTACKING SCENARIOS

### *3.1 Conventional Attacking Scenarios*

#### *3.1.1 CBIR ( Content based Image Retrieval)*

In this scenario, the attacker can know the location of a user by matching the patterns of the images associated with the profile of the user [1]. These type of attacks are done to know the current location of the user.

### 3.1.2 *Click jacking*

This is another type of attack scenario in which attacker posts some videos or post to the victim and when victim clicks on the page some malicious actions are performed. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers[4]. This type of attacks are done to do malicious attack or to make some page popular.

### 3.1.3 *Neighbourhood Attack*

The neighbourhood attacks are done by the attackers by knowing the victim's neighbourhood[4]. It means the attacker knows the friends of the victim. Attacker uses the relationship among these friends and based on this relationship tries to identify the victim.

## 3.2 *New attack Strategy*

### 3.2.1 *Watering Hole*

In January 2013, the attackers used to a new approach to make SNSs user insecure. The attack was done on Facebook. The attackers hacked a mobile developer forum and when developers visited the forum their system got infected with a MAC trojan [5]. This attack was not done to steal profile information or funds, but it was done to infect the system of developers. After attacks on facebook, the same attack was done on many other company, not only on SNS, but on their insecure sites as well.

## IV. PREVENTION STRATEGIES

4.1 *Limit the "amount"* - Limit the amount of personal information you post. Do not disclose information such as your residential address or information about your upcoming schedule or your daily routine. Also be considerate when posting information, including photos, videos and other media content.

4.2 *Internet is always "public"* – Always remember that anything that you post on the internet is always available to the public. Thus, it is your responsibility to post information that you are comfortable with anyone seeing. This includes your personal information and photos you post and those in which you are tagged in. Also, once you post information online, you can't delete it. Even if you remove the information from a site, cached versions remain on the world wide web and also on other people's computers that may be later retrieved as well.

4.3 *Beware of strangers* - The internet makes it really easy for people to misrepresent their personal identities and motives. It is always recommended to limit the people who are allowed to contact you on these sites. If you interact with unknown persons, be cautious about the amount of information you reveal or even agreeing to meet them in person. Common sense should prevail and dominate in such situations no matter how alluring it may appear.

4.4 *Be sceptical* - Don't believe in all that you read online. People make many mistakes and do post false or misleading information about different topics, including their own identity information. This is not necessarily done with a malicious intent since it could be unintentional, an exaggeration of any topic, or simply a joke that one may misinterpret. Take appropriate precautions, though, and make sure you verify the authenticity of any information before taking any action. As said before, common sense should matter more.

4.5 *Evaluate your settings* – Make sure you stay updated with the site's privacy settings. The default settings may allow anyone to see your "profile", but you may have an option to customize your settings to restrict access to only certain people. Sites may change their features periodically, so make sure you review your privacy/security settings regularly to make sure that your choices are still appropriate.

*4.6 Beware of third-party applications* - Third-party applications may provide entertainment or functionality, but use caution and common-sense when deciding which applications can access your personal information. Avoid applications that seem suspicious, and make sure to modify your settings to limit the amount of information which the applications can access.

*4.7 Use strong passwords* - Protect your account with passwords that are hard to be guessed. If your password is compromised, someone else may access your account and pretend to be you or can do virtually anything on your behalf, without your knowledge. Combining capital and lowercase letters with numbers and symbols creates a more secure password. Different password for different accounts always confuses the cyber-criminals.

*4.8 Keep software, particularly your web browser, up to date* - Install the latest software updates so that attackers cannot take advantage of known problems or vulnerabilities. Almost all operating systems and software offer automatic updates. If this option is available, it is always recommendable to enable it.

*4.9 Use an Anti-virus* - Anti-virus software helps protect your computer against known viruses. Since the attackers are continually creating new viruses, it is important to keep your virus definitions up to date. Making sure you have the latest security software, web browser is the best practice against online threats.

*4.10 Keep an eye on your children* - Children are quite susceptible to the threats in social networking sites. Although many of these sites have age restrictions, children are smart enough to misrepresent their ages so that they can join. By teaching children about internet usage, being aware of their online habits, and guiding them to proper and safe sites, parents can make sure that the children become responsible and safe internet users.

*4.11 Once posted, it cannot be removed:* Protect your social reputation on these networks. What you post anything online, it stays online even if you are not able to see it. It is always advisable to think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.

*4.12 Create an online reputation :* A recent research conducted by Microsoft also found that recruiters respond positively to a strong, attractive personal brand online. So show your smartness, thoughtfulness and creativeness to create an impression on your recruiter.

*4.13 Know and manage your friends :* Online friends should not be considered as real friends unless you have met them personally or have spent some time together. Beware of what you share with these "pseudo-friends". If you're trying to create a public image like blogger or expert, create an open profile or a "fan" page that encourages broad participation and also limits personal information. Use a personal profile to keep your real friends more synched up with your daily life.

*4.14 Be open if you're uncomfortable:* If a friend links you to a post and it makes you uncomfortable or you think it is inappropriate, ask them to remove it immediately. Likewise, stay broad-minded and co-operative if a friend asks you to remove something you posted that makes him or her uncomfortable. People have different tolerances and sentimental levels. Respect those differences.

*4.15 Know what to do :* If someone is harassing or threatening you, make sure you use proper measures to remove them from your friends list, block them, or report them to the site administrator using proper channels.

*4.16 When in doubt, take the safer path :* Cyber-criminals compromise your computer by sending links in emails, tweets, posts, and online advertising. If it looks suspicious, it's best to delete or if appropriate, mark as spam and reporting to others as well through proper channels and be a responsible internet citizen.

4.17 *Other Ways to Secure an Account* Typing a username and password into a website isn't the only way to identify yourself on the web services you use.

4.17.1 *Multi-factor authentication* uses more than one form of authentication to verify an identity. Some examples are facial recognition, iris recognition, voice ID, and finger scanning.

4.17.2 *Two-factor authentication* uses a username and password and another form of identification, often a security code in the form of a “*Captcha*”, or likewise.

One of the main reasons why social media has so many loopholes is the trust factor. We think that the people we are dealing with are actually our friends, our colleagues, our favourite sports teams, magazines, or food brands and thus they cannot be “fake” or “criminals”. This is the point where the actual criminals take advantage of your trust to retrieve your information.

## V. PROPOSED ARCHITECTURE

Secure Request-Response Application Architecture. It is an architecture developed for the secure exchange of data between SNSs users. This architecture allows a user to accept or reject the request of accessing information from his profile. The user can reject the request of friend as well as the visitors. The second functionality of this architecture is that user can have two different databases with different information provided. The user may select data from any one of the two databases to response a particular request. This architecture improves the degree of customization of the profile of a user.

According to this architecture the visitors or friends request for any information to the application between the visitor and the user. The application requests to the user for the response then the user can response from any one of the databases according to his trust on the person who has requested for the information.

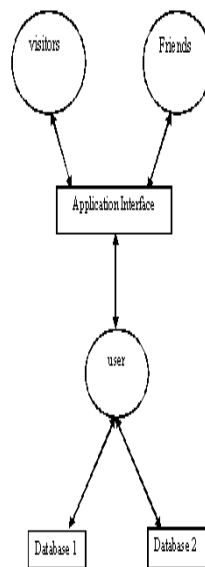


Figure 2 : Secure request response data

### 5.1 Benefits of architecture

The proposed architecture improves the customization of user profile and gives the ability to user to show his profile and information to the others in more customized manner. This will benefit the user to hide his profile information from unwanted visitors and friends.

### 5.2 Limitations

The proposed architecture only adds value to the customization but it is unable to protect from profile cloning. If anyone gets information after approval of the user then he may use the information to make a clone of the profile. In this case it is the responsibility of user to provide the information only to trustworthy persons.

## VI. CONCLUSION

In the end, the only solution to social network privacy and security issues is to have some knowledge of the ways in which one can get fooled. Don't post anything you would want to hide from a stranger. Be careful who you add as a "friend" since there's simply no way of verifying a user's actual identity online. We have proposed a architecture for secure communication between the users and a secure request-response architecture for exchange of information between the users. Keep your system clean and updated. Keep your senses open while using the internet and never jump to conclusions. Analyse the content thoroughly before doing anything. And remember, there are no free lunches in this world. And, internet is no different.

## REFERENCES

- [1] Markus Huber, Martin Mulazzani, Edgar Weippl "Social Networking Sites Security: Quo Vadis" IEEE International Conference on Privacy, Security, Risk and Trust.
- [2] Michael Lang, Jonathan Devitt, Sean Kelly, Andrew Kinneen, John O'Malley, Darren Prunty "Social Networking and personal Data Security: A Study of Attitudes and Public Awareness in Ireland" 2009 International Conference on Management of e-Commerce and e-Government.
- [3] EsmaAimeur, SebastienGambas, Ai Ho "Towards a Privacy-enhanced Social Networking Site" 2010 International Conference On Availability, Reliability and Security.
- [4] Dolvara Gunatilaka "A Survey of Privacy and Security Issues in Social Networks" www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.
- [5] <http://abcnews.go.com/Technology/apple-hacked-similar-attack-facebook-data-breached/story?id=18539110>
- [6] <http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx>
- [7] <http://blog.tweetsmarter.com/social-media/spring-2012-social-media-user-statistics/>
- [8] <http://msisac.cisecurity.org/newsletters/2010-03.cfm>
- [9] [http://www.pcmag.com/encyclopedia\\_term/0,2542,t=social%2Bnetworking&i=55316,00.asp](http://www.pcmag.com/encyclopedia_term/0,2542,t=social%2Bnetworking&i=55316,00.asp)
- [10] [http://www.networkworld.com/news/2010/020110-facebook-twitter-social-network-attacks.html?source=NWWNLE\\_nlt\\_daily\\_am\\_2010-02-02](http://www.networkworld.com/news/2010/020110-facebook-twitter-social-network-attacks.html?source=NWWNLE_nlt_daily_am_2010-02-02)
- [11] <http://www.informit.com/blogs/blog.aspx?uk=Security-Issues-of-Social-Network-Sites>
- [12] <http://www.fastcompany.com/1030397/privacy-and-security-issues-social-networking&>
- [13] <http://www.us-cert.gov/ncas/tips/st06-003>
- [14] [http://www.us-cert.gov/sites/default/files/publications/safe\\_social\\_networking.pdf](http://www.us-cert.gov/sites/default/files/publications/safe_social_networking.pdf)
- [15] <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2012.01580.x/full>