International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V7I4201703
Volume 7 Issue 4 November 2017

# Secrecy and Safety Concerns in Social Media Site

Dr. Vishal Kumar Goar
Assistant Professor
Govt. Engineering College Bikaner, Rajasthan, India

dr.vishalgoar@gmail.com

## ABSTRACT

Social media sites offer a frank way for people to have a simple common presence through web. They provide a cybernetic milieu for people to share each and every activity, their interests, and their circle of associate with their family, friends, or even the unknown. With so much sharing, hackers and thieves have found very easy ways to steal privatedata through these social media sites. This sounds for advances in safetyconventions to safeguard against hackers which form the basis of this research. In this paper, we will discuss some of the secrecy and safety concerns, attacks and their respective anticipationmethods. 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 approaches will prove the best protection in the warfare against cyber-attacks.

**Keywords** – Social Media; Hacking; Privacy; Security;

## INTRODUCTION

Social media area unit one among the simplest styles of communication recently. They replicate the social image of an individual. they'll keep you affixed to your avatar for hours along and cause you to ditch the entire physical world around you. The network of social relations that build up throughout your way of life is merely translated onto your “profile” and created obtainable for the entire of your friends to ascertain. Then there's a plan of “following” that may flip a roamer into a rockstar. the planet of images you share live has solely created your presence felt a lot of. It all looks therefore amusing that one would rarely consider effort this “world” associated changing into an offline monk. however, the more leisurelyand connected we become with these sites, a lot of casual and careless we have a tendency to area unit to share personal details regarding ourselves. People, many countless them, use a large style of social media sites (SMSs) that appear no but a menu card during a building. Facebook, the world’s leading social networking website, as an example, has a lot of users than the population of the many of the countries combined. there's completely little question that social networks became a region of each web user recently and also the trend is just set to extend. Figures recommend that there have been regarding one billion social network users in 2012, representing a nineteen.2% increase over 2011 figures. even supposing the utilization of social network websites and applications is progressively day by day however users aren't attentive to the risks related to uploading sensitive info. the rationale why cyber-conspirators feed on these networks is as a result of users transfer their personal info that normally embody their interests, social relationships, pictures, counseling and different media content, and share this info to the entire world via SMSs that area unit terribly simply accessible. Employees, too, unwittingly share embarrassment of non-publicinfo on SMS therefore putt their company infrastructure and information at a risk. the amount and simple accessibility of non-public info obtainable on these sites have attracted malicious those who obtain to use this info. owing to the sensitivity of data keep at intervals social networking sites, intensive analysis within the spaceof data security has become a section of overriding importance. Facts reveal that the bulk of social media users post risky info on-line, unaware of the privacy and security issues. Social networking sites area unit meant to urge as several users in one place as potential on one platform and for attackers there is a ton of return-on-investment in going once them. The values at the core of networking sites – openness, connecting, and sharing with others – sadly area unit the terribly aspects which permit cyber criminals to use these sites as a weapon for varied crimes. while not a careful security policy in situ, the amusing face of social networking may simply compromise on the social stature of a private. The dramatic rise in attacks within the last year tell U.S. that social networks and their countless users got to do lots a lot of to shield themselves from organized crime, or risk failing to fraud schemes, scams, and malware attacks. Understanding these risks and challenges ought to be self-addressed to avoid potential loss of personal and private info. Social networking positively must be integrated into the data security policy and user education.

## II. PRIVACY ISSUES

### Security risks

With increasing use of SMSs, the associated security risks also are increasing hugely. a number of the protection risks area unit fraud, phishing, scam, cyber bullying etc. folks use to produce their personal knowledge on SMSs like facebook, twitter etc. This knowledge is hold on in SMS and in lack of correct security techniques enforced in SMSs, it's not secure.

### Fraud

Some of the attacker's attack through the applying within which they raise permission for accessing the data provided within the profile of SMS. once a user permits to try to therefore, they get all data and might misuse that simply while not the user knowledge or permissions.

### Phishing

Phishing in SMS began in 2007[3]. the aim of phishing is to damage economically that's the phishers attempt to retrieve the profile info to grasp regarding the banking or the money info of the users.

### Profiling Risk

Profiling risk is that the risk related to profile biological research. The attackers retrieve the private info of the users and create a a twin of the profile [2]. they are doing therefore to form their social image dangerous or for alternative functions like knowing regarding friends of victims. this can be the foremost widespread security risk related to the SMSs as a result of it's terribly simple to try to to while not the permission of the user. there's nearly no security for profile biological research in SMSs. there's otherwise of profile biological research that's "cross-site profile cloning". during this the assaulter steals info from one social networking web {site} and uses this info to form a profile on another social networking site.

### Fake Product Sale

The assaulter advertises on the SMSs for marketing the merchandise giving large discount and once the user clicks on the merchandise advertising their profile info goes to the attackers. Generally, once user tries to buy and provides their account info for payment, all the account info is retrieved by the attackers and that they misuse this info.

## ATTACKING SCENARIOS

### Conventional offensive situations

### 1. CBIR (Content based Image Retrieval)

during this situation, the assaulter will understand the situation of a user by matching the patterns of the photographs related to the profile of the user [1]. These types of attacks square measure done to understand this location of the user.

### 2. Click jacking

This is another style of attack situation within which assaulter posts some videos or post to the victim and once victim clicks on the page some malicious actions square measure performed. this can be common in Facebook with the name like jacking that's once a user likes a page, an image or a video the user is at bay by the attackers [4]. this kind of attacks square measure done to try and do malicious attack or to form some page widespread.

### 3. Neighborhood Attack

The neighborhood attacks square measure done by the attackers by knowing the victim's neighborhood [4]. It means that the assaulter is aware of the chums of the victim. assaulter uses the link among these friends and supported this relationship tries to spot the victim.

### B. New attack Strategy

### Watering Hole

In Gregorian calendar month 2013, the attackers accustomed a brand-new approach to form SNSs user insecure. The attack was done on Facebook. The attackers hacked a mobile developer forum and once developers visited the forum their system got infected with a raincoat trajon [5]. This attack wasn't done to steal profile info or funds; however, it had been done to infect the system of developers. when attacks on Facebook, identical attack was done on several different company, not solely on SNS, however on their insecure sites similarly.

## IV. Prevention Methods

Limit the "amount" - Limit the quantity of non-public data you post. don't disclose data like your residential address or data concerning your coming schedule or your daily routine. even be kind once posting data, together with photos, videos and different media content. net is often "public" – perpetually bear in mind that something that you simply post on the net is often accessible to the general public. Thus, it's your responsibility to post data that you simply are comfy with anyone seeing. This includes your personal data and photos you post and people during which you're labelled in. Also, once you post data on-line, you cannot delete it. although you take away the data from a website, cached versions stay on the globe wide internet and additionally on different people's computers which will be later retrieved still.

### Watch out for Strangers

The internet makes it very easy for individuals to misrepresent their personal identities and motives. it's perpetually suggested to limit the people that are allowed to contact you on these sites. If you act with unknown persons, use caution concerning the quantity of data you reveal or maybe agreeing to fulfil them nose to nose. good judgment ought to prevail and dominate in such things despite however tempting it's going to seem.

### Be sceptical

Don't believe altogether that you simply scan on-line. individuals build several mistakes and do post false or dishonest data concerning completely different topics, together with their own identity data. this can be not essentially through with a malicious intent since it may well be unintentional, associate degree exaggeration of any topic, or just a joke that one could misinterpret. Take applicable precautions, though, and check that you verify the genuineness of any data before taking any action. As aforesaid before, good judgment ought to matter a lot of.

**Evaluate your settings**
Make sure you keep updated with the site's privacy settings. The default settings could enable anyone to examine your "profile", however you will have associate degree choice to customise your settings to limit access to solely sure individuals. Sites could amendment their options sporadically, thus certain you review your privacy/security settings frequently to form sure that your decisions are still applicable.

**Beware of third-party applications**
Third-party applications could offer diversion or practicality, however use caution and common sense once deciding that applications will access your personal data. Avoid applications that appear suspicious, and check that to change your settings to limit the quantity of data that the applications will access.

**Use sturdy passwords**
Shield your account with passwords that are onerous to be guessed. If your parole is compromised, somebody else could access your account and fake to be you or will do nearly something on your behalf, while not your information. Combining capital and minuscule letters with numbers and symbols creates a safer parole. completely different parole for various accounts perpetually confuses the cyber-criminals.

**Keep package, significantly your applications programme, up to date**
Install the newest package updates so attackers cannot make the most of well-known issues or vulnerabilities. most in operation systems and package supply automatic updates. If this selection is on the market, it's perpetually recommendable to alter it.

**Use associate degree Anti-virus**
Anti-virus package helps shield your laptop against well-known viruses. Since the attackers are frequently making new viruses, it's vital to stay your virus definitions up to now. ensuring you have got the newest security package, applications programme is that the best apply against on-line threats.

**Keep an eye fixed on your kids**
Children are quite prone to the threats in social networking sites. though several of those sites have age restrictions, kids are good enough to misrepresent their ages so they'll be part of. By teaching kids concerning net usage, being attentive to their on-line habits, and guiding them to correct and safe sites, oldsters will check that that the kids become accountable and safe net users.

**Create a web name:** A recent analysis conducted by Microsoft additionally found that recruiters respond completely to a robust, enticing personal whole on-line. thus, show your smartness, thoughtfulness and creative thinking to make an effect on your recruiter.

**Know and manage your friends:**
On-line friends mustn't be thought-about as real friends unless you have got met them in person or have spent it slow along. watch out for what you share with these "pseudo-friends". If you're making an attempt to make a public image like blogger or skilled, produce associate degree open profile or a "fan" page that encourages broad participation and additionally limits personal data. Use a private profile to stay your real friends a lot of synched up together with your lifestyle.

**Be open if you're uncomfortable:**
If an acquaintance links you to a post and it causes you to uncomfortable otherwise you

assume it's inappropriate, raise them to get rid of it straight off. Likewise, keep broad-minded and co-operative if an acquaintance asks you to get rid of one thing you announce that produces him or her uncomfortable. individuals have completely different tolerances and mawkish levels. Respect those variations.

**Know what to try and do:**
If somebody is harassing or threatening you, check that you employ correct measures to get rid of them from your friends list, block them, or report them to the location administrator mistreatment correct channels.

**When unsure, take the safer path:**
Cyber-criminals compromise your laptop by causing links in emails, tweets, posts, and on-line advertising. If it's suspicious, it's best to delete or if applicable, mark as spam and news to others still through correct channels and be an accountable net subject.

Other ways in which to Secure associate degree Account typewriting a username and parole into an internet site is not the solely thanks to establish yourself on the net services you employ.

a) Multi-factor authentication uses over one sort of authentication to verify associate degree identity. Some examples are biometric identification, iris recognition, voice ID, and identity verification.

b) Two-factor authentication uses a username and parole and another sort of identification, usually a security code within the sort of a "Captcha", or likewise.

one among the most reasons why social media has numerous loopholes is that the trust issue. we predict that the individuals we tend to are managing are literally our friends, our colleagues, our favourite sports groups, magazines, or food brands and therefore they cannot be "fake" or "criminals". this can be the purpose wherever the particular criminals make the most of your trust to retrieve your data.

## V. PROPOSED ARCHITECTURE

Secure Request-Response Application design. its associate design developed for the secure exchange of knowledge between SMSs users. This design permits a user to just accept or reject the request of accessing info from his profile. The user will reject the request of friend moreover because the guests. The second practicality of this design is that user will have 2 totally different databases with different info provided. The user could choose knowledge from anyone of the 2 databases to response a selected request. This design improves the degree of customization of the profile of a user. in step with this design the guests or friends request for any info to the appliance between the traveller and therefore the user. the appliance requests to the user for the response then the user will response from anyone of the databases in step with his trust on the one who has requested for the knowledge.

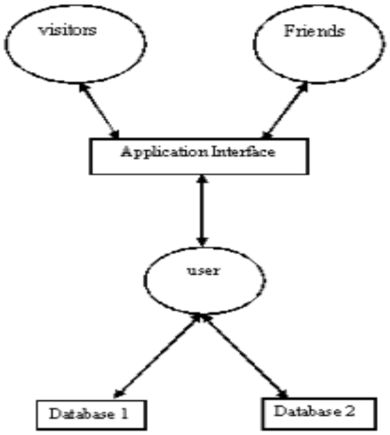

Figure 2 : Secure request response data exchange

**Benefits of architecture**

The planned design improves the customization of user profile and offers the flexibility to user to indicate his profile and data to the others in additional custom-built manner. this may profit the user to cover his profile info from unwanted guests and friends. Limitations

The planned design solely adds price to the customization however it's unable to shield from profile biological research. If anyone gets info once approval of the user then he could use the knowledge to create the image of the profile. during this case it's the responsibility of user to produce the knowledge solely to trustworthy persons.

## VI. CONCLUSION

In the end, the sole resolution to social network privacy and security problems is to own some information of the ways that within which one will get fooled. do not post something you'd wish to cover from an interloper. take care UN agency you add as a "friend" since there is merely no approach of confirming a user's actual identity on-line. we've planned a design for secure communication between the users and a secure request-response design for exchange of knowledge between the users. Keep your system clean and updated. Keep your senses open whereas victimisation the net and ne'er jump to conclusions. Analyse the content completely before doing something. And bear in mind, there are not any free lunches during this world. And, web is not any totally different.

## REFERENCES

[1] http://www.networkworld.com/news/2010/020110-facebook-twitter-socialnetwork attacks.html?source=NWWNLE_nlt_daily_am_2010-02-02

[2] EsmaAimeur, SebastienGambas, Ai Ho “Towards a Privacy-enhanced Social Networking Site” 2010 International Conference On Availability, Reliability and Security.

[3] Markus Huber, Martin Mulazzani, Edgar Weippl “Social Networking Sites Security: Quo Vadis” IEEE International Conference on Privacy, Security, Risk and Trust.

[4] http://www.uscert.gov/sites/default/files/publications/safe_social_networking.pdf

[5] 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.

[6] http://www.us-cert.gov/ncas/tips/st06-003

[7] Dolvara Gunatilaka “A Survey of Privacy and Security Issues in Social Networks”www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.

[8] http://www.fastcompany.com/1030397/privacy-and-security-issues-socialnetworking&

[9] http://blog.tweetsmarter.com/social-media/spring-2012-social-media-userstatistics/

[10] http://abcnews.go.com/Technology/apple-hacked-similar-attack-facebookdata-breached/story?id=18539110

[11] http://my.safaribooksonline.com/book/-/9781597495455/chapter-3dotphishingattacks/phishing_attack_scenarios_agai#X2ludGVybmFsX0J2ZGVwRmxh

c2hSZWFkZXI/eG1saWQ9OTc4MTU5NzQ5NTQ1NS80NQ==

[12] http://www.pcmag.com/encyclopedia_term/0,2542,t=social%2Bnetworking&i=55316,00.asp

[13] http://pewinternet.org/Commentary/2012/March/Pew-Internet-SocialNetworking-full-detail.aspx

[14] http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2012.01580.x/full

[15] http://mobile.scmagazineuk.com/a-lack-of-security-on-social-networkingsites-causes-problems-for-businesses/marticle/173602/

[16] http://searchenginewatch.com/article/2065928/Social-Media-The-Privacyand-Security-Repercussions

[17] http://msisac.cisecurity.org/newsletters/2010-03.cfm

[18] http://www.informit.com/blogs/blog.aspx?uk=Security-Issues-of-SocialNetwork-Sites

[19] http://www.staysafeonline.org/stay-safe-online/protect-your-personalinformation/id-theft-and-fraud