Abacus (Mathematics Science Series) Vol. 44, No 1, Aug. 2019

TACKLING ONLINE SOCIAL NETWORK THREATS: PROPOSED SECURITY MEASURES

by

Abudu A. O. & Sulaimonh. A.

Dept. of Computer Science Federal College of Education, Zaria Kaduna State, Nigeria & Dept. of Computer Science Federal College of Education, Zaria Kaduna State, Nigeria

Email: abuduabimbola@gmail.com, sulaimonha@gmail.com

Abstract

Social Network sites are platform where people interact freely, sharing and discussing information about each other and their lives, using a multimedia mix of personal words, pictures, videos and audio. Also, the users post their personal details for others to see through this various social network sites. Despite all the benefits of SNS, it is observed that attackers still penetrate the user's information without being authorized. This paper presents the common security threats such as identity theft, information leakage, digital dossier, password theft andidentity cloning faced by the social network users. It proposes how some of these identified threats could be avoided by using stronger authentication techniques like Token and CAPTCHA. It also proposes the means of reducing the rate at which the attackers make use of others information by modifying the default setting of the sites.The proposed authentication technique was evaluated and the result shows that the new technique is stronger.

Keywords: *Authentication Techniques, Social Network Sites, Token, CAPTCHA*

Introduction

Social media are Internet sites where people interact freely, sharing and discussing information about each other and their lives, using a multimedia mix of personal words, pictures, videos and audio. There are hundreds of Social Network Sites (SNSs); some of these SNSs are based on chatting, meeting friends and sharing images like Facebook, Twitter, Google+,Theglobe and Geocities.Geocities was one of the first social media sites created in 1994. It allows users to create their own websites (Walker, 2013).In 2004, Facebook started as a Harvard-only social network, it propagated into other schools, then to high schools, corporate and eventually everyone by 2006. In 2008, Facebook became the most popular social networking site, surpassing some other social sites such as MySpace. Facebook doesn't allow the same kind of customization that MySpace does. Facebook does, however, allow users to post photos, videos and otherwise customize their profile content, if not the design. Its features include instant messaging and apps, private messaging, Wall posts and privacy settings.

In the recent years, online social networking services have gained more popularity in the world, with many Social Network Sites (SNSs) such as Myspace, Facebook, Blogger and Yahoo! Groups, are now among the most visited websites. Furthermore, since such forums are user friendly and easy to access, the users are often not aware of the size and the nature of the audience accessing their profiles; they often reveal more information which is not appropriate to a public forum (Abdullah, 2008). As a result, such commercial and social sites with so much sharing may often generate a number of security related threats for the member's unknowingly. The attackers have found ways to steal personal information through these networking sites. This calls for advances in security protocols to safeguard against attacker which form the basis of this study.Having stated the benefits of social networks, there are issues or threats of online social networks.The users are not security conscious whenever they are on social network; they reveal their information to friends

unknowingly in an unguided way. The careless posting of personal information by the users' unknowingly on Social Network Sites (SNSs) might create problems to the users' by allowing the attacker to use the personal information posted by the user to produce a number of threats to the users. So it encourages some of this security threats like Identity Theft, Identity Cloning, Information Leakage, Digital Dossiers and Password Theft.To be able to checkmate the security threats stated above, there is need to design a stronger authentication and a standard default setting that can be used to reduce the threats.

Robert and Rodney (2011) explained many of the Social Media usage risk that an enterprise can conduct a risk assessment and determine which risk is applicable to the organization.The researchers carry out a survey on some organizations and observed that many organizations that were making use of social media are prone to security risk by losing their important data, intellectual property or increased costs to repair the damage.The researchers did not actually state the solution to the risk and how itcould affect the organizational data or products.

Hak (2012)used Figure 1 to show the service framework of Social Network Site (SNS), which consists of three parts; user applications (e.g. web services, e-mail services, instant messaging services, and other services), social media devices (mobile phones (i.e., iPhone), iPad, laptop computers, and desktop computers), and network infrastructure (e.g. traditional LAN/WAN, mobile-based wireless networks, and cable networks).

Furthermore, he explained the Security Risks and Trust Zones of Social Network Sites where he used the Analytic Hierarchy Process (AHP) approach for assessing SNS's security risks based on each trust zone.The researcher only discusses the risk assessment based on Social Media Application zone and leaves the other two zones which are Social Media Devices and Network Infrastructure zone.

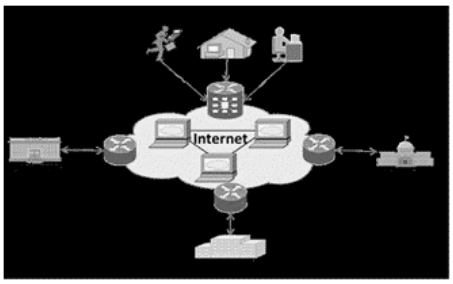

Figure 1: The generic network architecture for online social network services (Hak, 2012).

In the work of Saba (2015), security threats facing Businesses and Organizations were discussed and Two Factor Authentication (2FA) was proposed. Pin and Token were used as 2FA which was developed with the use of RSA encryption algorithm.Saba (2015) only use an RSAencryption algorithm to generate the token.

Security issues in social network sites

Some of the security issues in Social Networks are stated as follows: Identity Cloning (IC), Identity Theft (IT), Password Theft (PT), Information Leakage (IL), Digital Dossier (DD) and Phishing.

(a) **Identity Theft (IT):** It can be seen as when hackers steal the identity of other users like name, picture, and place of work, home address and date of birth and use it to blackmail

or tormenting the right owner. Mali (2014) stated that 12 million people became victims of identity theft and fraud in 2012, and the financial loss of this attack was pegged at $21 billion. Obiniyi*et al*., (2014) stated that Identity theft in social network has become rampant in popular social networks.

(b) **Identity Cloning (IC):** In most social networking sites, users use their real name torepresent their accounts. So, their identity is exposed publicly to other social network users; as well as everyone else in the online world. Identity Cloning occurs when the hackers have gotten vital information pertaining to a user and use this information to create another profile and be pretend as if he or she is the right owner of the account.

(c) **Information Leakage (IL):** Rick (2011) stated that with the advent of "always-on" connectivity, the traditional lines between work and personal life are becoming blurred. Particularly, younger workers use the same technologies in the office as at home. Social network user's profiles mostly contain vital information about users that can be seen by both the user's friend and non-users friend because the information is public, such information are user's full name, contact information, relationship status, date of birth, previous and current work and education background which attract hackers. All this information can be searched mostly on google.com using only the name.

(d) **Digital Dossier (DD):** occur due to the advancement of data mining technology and the reduction of cost of disk storage, this give right to hackers to create a profile due to the sensitive information been disclosed unknowingly. All the sensitive information that is directly accessible by profile browsing can be accessed via search (e.g. a person's name and profile image is accessible via search on MySpace, Facebook and others, unless default privacy settings are changed). The information could be used to embarrass or blackmail the profile holder. For instance people are missing out their employment opportunities since the employer reviews the SNS profiles of the prospective candidates (Flesher, 2006; and Fuller, 2006).

(e) **Phishing:** Obiniyi*et al*., (2014) stated that Phishing is a tricking of online users togive out some details such as password, to an illegitimate website. In phishing attack, hackers create a fake link that will look real and attach to SNSs that require the user's sensitive information such as password, financial information, or identification number to the website. Phishing hack together with personal information from social networks make the attack becomes more successful (Huber*et al*.,2011).

(f) **Password Theft** (PT): is when a user was careless with his or her login details which are email address and password. The password theft can occur in different ways. The user may use some one's system to sign into his or her page and sign out. During the signing in, he or she may carelessly click on the alert message "recognize my password" that always pop out at the left corner top of the webpage. Secondly, it may be through a fake link that look authentic that will require the user to log in with your Facebook details

Benefits and prospects of Social Network Sites (SNS)

We can all see the rate at which SNS are making life easy for the people or users to be able to communicate with friends, family or relatives, even with business associates.

The benefits of SNSs cannot be left without being mentioned, this includes:

a. It reduces costs of advertising. Ability to post message or adverts to SNSsespecially Facebook is more cost effective than printing bills or to post office to mail thousands of products to people.

b. It allows interlink between companies in order to allow other companies to view and see your product without contacting your company to see your goods and products.
c. It allows platforms to communicate. It allows you to view what other company orretailers comments on how they feel pertaining to your products and ask question about what they need to know about your company.
d. It allows users to create own personal profile. Social media is a great way to display your business' personality, as well as behind-the-scenes information about you, your employees, your workspace, and more.
e. It also reduces waste of time. If a user tries to send messages to a friend, instead of using post office that will stay up to a week before getting to destination. So, the use of SNS will get to the destination within shortest minutes.
f. It allows Customers to validate organizational business on SNS.
g. With SNS you can provide value the idea that you can provide a truly valuable service to your target market means you are positioning yourself as an expert in your industry. Whether that's educational and entertaining blogs, posts, or tweets, if you are solving a problem or providing information, you're adding value that customers will appreciate.
h. SNS lets you gain the competitive advantage if used correctly, social media canboost your search rankings, allow you to provide better customer service, build an effective online personality, connect with new business partners, build connections, and validate your professional standing all while providing your consumers with the value they want.

Materials and Method

Google search was used to surf the web sites of various aspects of Social Networks based on the threats and how to reduce them. The tools used to accomplishing this study includes PHP scripting language and Java programming Language, Mysql, Structural Query Language(SQL), Dreamweaver (Integrated Development Environment(IDE)),xampp (configuration of Mysql, php and apache) server and apache as web server.

In order to propose a security measure that can tackle the online social network threats, the paper proposed an authentication algorithm that illustrateda reliable user authentication paradigm. An access-control authentication technique and user privacy setting mechanisms were developed.

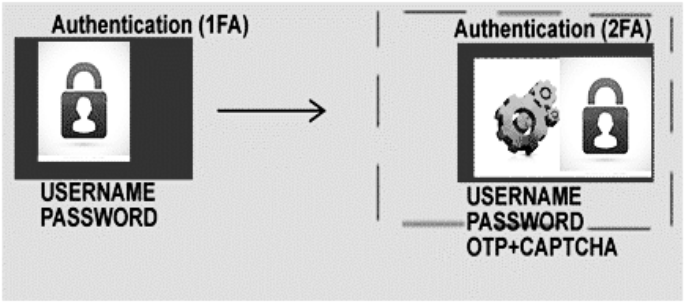

Figure 2:The Access-ControlAuthentication technique.

The Figure 2 shows the proposed Access-Control Authentication techniquewhere the existing authentication techniqueis called the One Factor Authentication (1FA) and it contains e-mail (or username) and password only. The proposed authentication techniqueis called the Two Factor Authentication (2FA) that contains 1FA, Tokens and the Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).

CAPTCHA makes provision for some characters to appear in a box so that the user will be expected to type the same words to show that the person trying to log into the site is not a robot. At the same time a token can be a set of numbers or alphanumeric data that can be sent to the user's phone number to be type back into the box that appear in front of the word "token" and the token will show that the person trying to log in is the right owner. All these are used for authenticating the users log in to the social network site.

The following algorithm 1 is to generate a Token and algorithm 2 is to generate CAPTCHA. Both the Token and CAPTCHA are used to make the security stronger.

//Token generation algorithm.

1. Let time_now = current time
2. Convert time_now to unix timestamp
3. Create unix_step
   Randomly select value range(1,5);
4. Let tc = (time_now – unix timestamp) / unix_step
5. Salt = hexadec(tc and rand(5,9999)
6. Hash=hexdec(salt, encryption_algorithm) //eg sha256
7. Store->DB(hash as token, (time_now+10) as expiry_time)
8. Return token

Algorithm 1: Token Generation

// CAPTCHA generation algorithm.

1. Create empty image for CAPTCHA
2. Create canvas for drawing CAPTCHA
3. Set canvas to background color
4. Generate random dots around canvas
5. Let i=upper(alphabet) U lower(alphabet) Udigits(0-9)
6. Let n = len(i);
7. Set num_digit = number of characters in CAPTCHA
8. Whilenum_digits> 0
   P = randomly select char from i
   CAPTCHA = CAPTCHA + p
   -- num_digits
   end while
9. Draw CAPTCHA
10. Store->DB(CAPTCHA)
11. Return CAPTCHA

Algorithm 2: CAPTCHA Generation

USER PRIVACY SETTINGS MODULE (Major)

// User privacy settings module is used to update users' privacy settings using the information //gathered by the behaviouraldaemon. Behaviouraldaemon is used to get information pertaining to //behavior of the online users.

```
Let t ← isAuth()
if !tthen
        authUser()
else
        startBehaviouralDaemon()
```

```
        dsetting ← DB::getDefaultsettings()
        for each dsetting → i
                dp ← setpage(dsetting_i)
        psetting ← DB::getsetting()
        for each psetting → k
                pp ← setpage (psetting_k)
        showpage(dp,pp)
        while !session_logout
                dstore ← updatedaemon
                deallocatememory[session_daemon]
        endwhile
        Event:OnLogout
        DB::updatepersonalprofile(dstore)
endelse
BEHAVIOUR DAEMON ALGORITHM  (Minor)
        Def:averagekeystroke, Ip, browserAgent,webpage
        Events: keystroke, time=30s, pagechange
        init_time = 0
        foreach keystroke
                session _t ← diff (keystroketime_i, keystroketime_i-1)
        Event:Ontime ||Onpagechange
        session_avg_time ← average (session _t)
        session_daemon [session_avg_time, Ip, browserAgent, webpage].
```

Algorithm 3: User Privacy Setting Mechanism

Results and Discussion

The figure 3 shows the existing authentication module which is called One Factor Authentication (1FA) that contains the user e-mail and password which the SNSs require from the user. The 1FA is not strong enough for authenticating a user if the user login details (user email and password) are compromised.

Figure 3: The One Factor Authentication (1FA).

The existing authentication processes can be compromisedby the carelessness of the user whereby login details are not protected or the user used someone deviceto log into his Social

Network web page. The mistake may occur when the user has logged in his details and unknowingly press "allow" on the alert message that normally appear at the upper left corner of the window. Also, the user's login details could be compromised whenstrange links are sent to the user to click. Once the user clicks on the link, the person will be redirected to a webpage that will ask the user to log on the login details which includes the user name and password that will be stored in their database.

The proposed authentication module

JAVA programming language was used to generating CAPTCHA and Token. The output of the codes that generated both CAPTCHA and Tokenare displayedinthe figure 4 which is the proposed authentication module called 2FA that rely on the existing authentication module called 1FA. When the user filled in the 1FA, the 2FA will appear and it will contain CAPTCHA and Token which will be used to authenticate the user. Even if the user is careless with the email and password or mistakenly click on the alert message that always appear at the left upper part of the system then outsider or any intruder will still find it difficult to get access to the users home page.

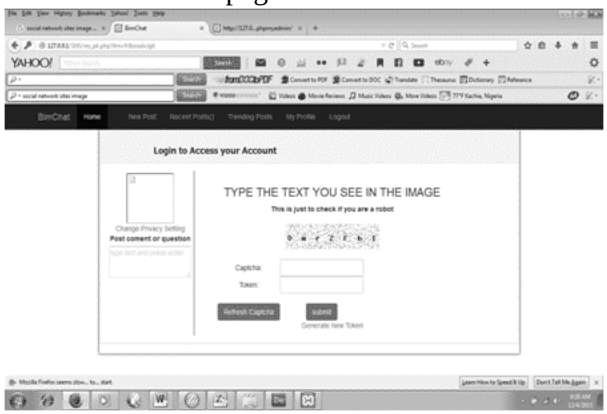

Figure 4: The Two Factor Authentication (2FA).

When the user has finish filling the CAPTCHA and token box, then the user will be allowed to have access to the Social Network Site and figure 5 will appear which shows the user's home page.

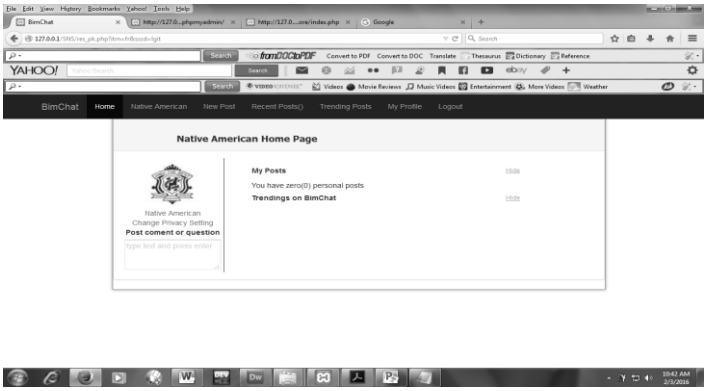

Figure 5: User sign in into the SNS.

The existing default settings

Figure 6shows the existing default setting that will show immediately after the new user sign up or register into the SNS with user's personal or profile information such as names, place of work, institution attended, phone number, sex and date of birth that need to be secured very well by the user. User can hide all theseinformationby mere adjusting the settings.All these adjustment can be easy for users that have time and are used to SNSs. But for those that have no knowledge pertaining to the settings or that have no time for such, they will be at disadvantage.

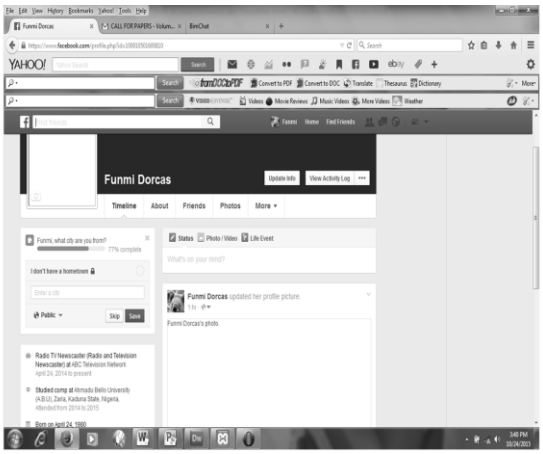

Figure 6: The existing default settings.

To make things right, default settings need to be designed so that when the user finished with registration or signing up and log-in into SNS, what will be visible to others should be the users name and the picture. Any other detailed personal information should be hidden. The default settings should be strict and flexible. So, if any user at all wants other friends to see more that the picture and the name, the user can later go to the settings and make some adjustments. This will be of advantage to both users that are used to SNSs and those that are not. The figure 7shows the proposed default setting that displays the users name and picture after the user has successfully registered and logged in into SNS. This proposal will improve the security challenges facing the users of SNS.

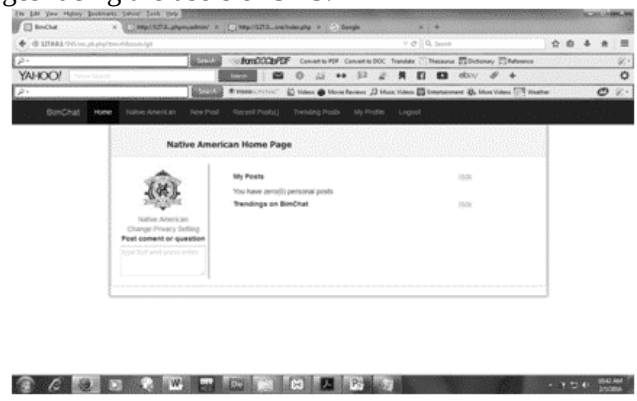

Figure 7: The proposed default settings.

Conclusion

In conclusion,the hackers are Password Theft, Information Leakage, Digital Dossier, Identity Cloning and Identity Theft. The algorithm designed such as behavioral logs, user privacy, Token and CAPTCHA can be used to checkmate the hackers from hacking into user's page.From this study, the researchers observed that 2FA is stronger compare to 1FA and the proposed default setting is more secure and efficient compare to the existing one. Few limitations were observed in this study, the first of which is that if the user lost his phone number, to get the Token through the phone will be impossible. Furthermore, the users will be forced to enter Token and CAPTCHA which may not interest the user andit may appear as a waste of time to users by trying to enter the Token and CAPTCHA again.In addition, the network problem may also be an issue which may lead to delay in Token sent to the user'sphone number.

References

Abdullah, A. H. (2008): Threats of Online Social Networks. *TKK T-110.5190 Seminar on Internetworking*. Retrieved October9,2014 from https://hakin9.org/hacking-social- media-threats-vulnerabilities-threats-anti-threats-strategies-for-social-networking- websites/

Flesher, J.(2006). How to Clean Up Your Digital Dirt Before It Trashes Your Job Search. *In The Internet Engineering Task Force.Retrieved November 21, 2015 from*http://www.careerjournal.com/jobhunting/usingnet/20060112-43766/flesher.html.

Fuller,A.(2006). Employers snoop on Facebook. *In The Stanford Daily*. Retrieved *November 21, 2014 from* http://daily.stanford.edu/article/1/20/employersSnoopOnFacebook

Hak, J.K.(2012). Online Social Media Networking and Assessing Its Security.*International Journal of Security and Its Applications., 6(3).* Retrieved November 25, 2014from http://www.sersc.org/journals/IJSIA/vol6_no3_2012/2.pdf

Huber, M., Mulazzani, M., Weippl, E., Kitzler, G. and Goluch, S.(2011). "Friend-in-the- Middle Attacks: Exploiting Social Networking Sites for Spam," *InternetComputing, IEEE,vol.15, no.3, May-Jun. 2011, pp.28-34*. Retrieved July 2, *2014*fromhttp://www.sbaresearch.org/wpcontent/uploads/publications /FITM_ Internet Computing_preprint.pdf

Mali, J. (2014). How to Avoid Identity Theft on Facebook. Retrieved July 28, 2015from http://www.lifehack.org/articles/technology/identity-theft-through social-networking-lessons-take-now.html

Obiniyi, A. A., Oyelade, O. N. and Obiniyi, P. (2014). Social Network and Security Issues:Mitigating Threat through Reliable Security Model. *International Journal of Computer Applications Volume 103 (9)*

Robert, S. and Rodney, C. (2011). Risk Assessment of Social Media. GIAC (GSEC) Gold Certification. Retrieved October 23, 2015 from https://www.sans.org/reading- room/whitepapers/riskmanagement/risk-assessment-social-media-33940

Saba, H. (2015). Two Factor Authentication. Retrieved January 4, 2016 from www.slideshare.net/mmubashirkhan/slideshelf

Somen, P. (2015). How to Manage Different Social Media Profiles for Your Website Effectively? Retrieved on june29,2015 from http://www.buzzlouder.com/how-to- manage-different-social-media-profiles-for-your-website-effectively

Timm, D. M. and Duven, C. J.(2008). Privacy and Social Networking Sites. A chapter Published online in Wiley InterScience (www.interscience.wiley.com) • DOI: 10.1002/ss.297. New directions for student services, no. 124, Winter 2008 © Wiley Periodicals, Inc.

Walker, M. (2013). "The History of Social Networking". Retrieved November2, 2013 from http://www.webmasterview.com/2011/08/social-networking-history/