International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 7, July 2013)

A New Social Media Security Model (SMSM)

Ehinome J. Ikhalia[1]

[1]*University of East London, London, United Kingdom*

***Abstract*— As social media increases in functionality and popularity, it has become more vulnerable. It is no secret that social media vendors exclude security during development, hence leaving it to users' discretion which raises a serious cause for concern. The aim of this research is to study existing vulnerabilities of online social media and propose practical solutions. The importance of studying social media vulnerabilities provides a clear understanding in developing a new security model to prevent social engineering attacks. In this paper; we investigate key security vulnerabilities eroding the trust placed on social media such as profile cloning, single factor authentication, weak password creation, weak account activation systems, privacy vulnerabilities, unethical posts and multiple login sessions. We develop and propose a novel social media security model (SMSM) to reduce the aforementioned vulnerabilities.**

***Keywords*— Single factor authentication, profile cloning, one-time password, phishing, Twitter, Facebook, security vulnerabilities, LinkedIn, Google+, social media**

I. Introduction

Social networking sites otherwise known as 'Web 2.0' such as LinkedIn, Twitter, Facebook and Chinese 'Renren', are growing ceaselessly with huge opportunities providing fast and cheap human interaction as well as vast economic expansions through digital 'word of mouth' (Li et al, 2013).

A huge number of social network users publicly share a large proportion of their private and sensitive information within their online social networking space (Lee, 2010). The information shared consists of**:** personal contact addresses, business addresses, telephone numbers, date of birth, demographic information, images, videos, posts and comments (Gayathri et al. 2012). Most of this information is shared without consideration; therefore social networks have now become a repository of uncontrolled sensitive data (Manos, 2012).

Social networking sites have become targets for various attacks used by cyber-criminals (Lenkart, 2011). Malicious attackers often exploit single-factor authentication mechanism implemented by social networks. (Khonji et al, 2013).

The contributions of this paper are the following:

1. We review key vulnerabilities affecting the current social media platforms.
2. We propose a new social media security model (SMSM) to reduce the vulnerabilities identified.

II. Background

Previous security methods have been proposed to reduce the vulnerabilities encountered by most social networks without altering the usability of the system. These models emphasised user education and policy implementation. However, these have very limited success as users are notoriously non-compliant with such methodology.

Some work has been done to explore the effects of social networks in disseminating information about successful social engineering attacks. Coronges et al, 2012, developed an experiment where phishing emails were created and sent to a controlled user population. Their results showed that local leadership within an organisation appeared to influence security vulnerability but had no influence on security resilience or phishing prevention.

Joshi and Kuo (2011) investigated mathematical formulation and computational models for security and privacy of social networks. In their empirical study, they presented several ways an attacker can take advantage of the security vulnerabilities in an online social network. Some of the vulnerabilities discussed were Social Phishing Attacks, and Neighbourhood Attacks which is a form of privacy attack. This gives the attacker sufficient information about the target. Furthermore, their work presented theories that recent work in programming language techniques demonstrates that it is possible to build online services that have strict privacy policies. Unfortunately, service providers need private data to generate revenue from their 'free' service, limiting the application of strict security and privacy measures. It is important to clearly identify the main vulnerabilities of current social media.

III. Key Vulnerabilities Of Social Media

A. *Single Factor Authentication*

Single factor authentication is the conventional security procedure which requires a username/email and password before a user is granted access to the system (Almuairfi et al, 2011).

As the complexities of Web 2.0 applications increase, this is affected by both the sensitivity and power of the technology. Therefore, it is imperative to implement a more secure authentication system such as a two-factor authentication strategy. This has become evident as the results revealed from LinkedIn hack shows that most users still use terms like ‘password’, ‘password1’, ‘abc123’ as passwords to the sensitive information which form a huge part of their existence in many social networking sites (Altinkemer & Wang, 2011).

The security methods involved in authenticating account owners before gaining access into a system started as a debate in the industry and has now become the greatest cause of concern (Altinkemer, 2011). The sophistication of social engineering tools used by attackers poses a serious threat to the integrity, reputation and lives of users which may result in a sudden decline of social media usage (Parwani et al, 2013).

B. Profile Cloning

The easiest technique used in stealing the identity of a social network's user is called profile cloning. With the current structural outlook of profile pages on Facebook, it is very easy to clone an original user and perform malicious activities with the cloned account before the victim or the platform providers discovers. The profile pages of Facebook have no particular unique separation from one another, and in cases were two users co-incidentally share the same first and surnames as well as the same profile image, the true owner of the account is left for the viewer to identify (Kumar et al, 2013). There are two types of profile cloning, (1) Existing profile cloning, (2) Cross site profile cloning.

- *Existing Profile Cloning:*

This means that attackers can create a replica of an already existing user's profile page using their first and surname, some personal information as well as the same profile image to disguise as the original user. Then the attacker sends 'friend' requests to ‘friends’ of the original user which in most cases are successful, because the 'perceived friend' profile is familiar. With this vulnerability the attacker can interact with the ‘friend’ of the victim and get access to sensitive information about the victim and their ‘friends’ (Khonji et al, 2013). Linkedln is similar to Facebook but Twitter is less vulnerable in this regard.

- *Cross Site Profile Cloning:*

This is the process were an attacker steals a user's profile information from one social networking site and uses it to register in another social networking site which the user has never signed up for (Aggarwal et al, 2012).

The main aim for this attack is to use the 'friends' list of the victim's social network to send friend requests to all the victim's friends in the other social networking site. This method of phishing is more dangerous because the victims or their 'friends' may never be aware of the malicious impersonation for fraudulent purposes (Arachchilage et al, 2013).

C. Phishing Attacks

Phishing could be described as a malicious craft used by social engineers with the aim of exploring the vulnerabilities of a system which are made easy through the ignorance of end-users (Khonji et al, 2013). To launch a phishing attack on a social media user, an attacker would create a replica of a genuine site, for example Facebook, and then lure the victim via an HTTP link sent to the user’s email address or posted on the user’s profile page within the site. The aim of this kind of attack is to (*impersonate*) the user to provide original login details associated with his/her social network account such as username/email and password. If the user falls prey to this attack, the email/username and password supplied in the site, is stored in the database of the attacker, making the victim's account totally vulnerable (He et al, 2011).

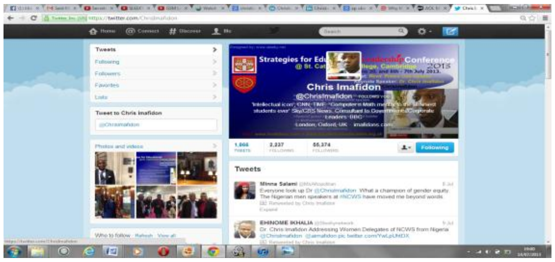
D. Watering Hole Malware Attack

This method of malware attack involves the attacker guessing which websites members of an organisation normally go, and then it infects these websites with malware with the hope that a user’s computer within the target organisation will be infected when an infected site is visited. It was discovered in January 2013, that a watering hole attack was targeted at developers working at Facebook. An online forum which Facebook developers visited regularly was hacked and got infected with MAC Trojan. It was an attempt not to steal personal information or monetary values but simply to damage their systems (Khonji et al, 2013).

E. Multiple Login Sessions

The security vulnerabilities created by allowing multiple login sessions can result in both data theft and economic consequences (Imafidon & Ikhalia, 2013). In websites that make it compulsory that users’ pay before using their service e.g. an online movie store; by allowing the creation of multiple login sessions on one account to run concurrently, the user and other users can share the benefits on one subscription regardless of their remote locations. Hence, it leads to a huge financial consequence for the online service providers (Adebiyi, Arreymbi & Imafidon, 2012).

Moreover, monitoring the sessions that are being created on an account becomes very difficult because the user may have no idea if their account is being compromised or not. Implementing a solution to this problem will also reduce the security issues associated with session hijacking, and data theft in online social networks (Choti et al, 2012).



'Intellectual icon', CNN, TIME 'Computer's Math mentor to the brightest students ever' Sky/CBS News. Consultant to Government/Corporate Leaders. BBC

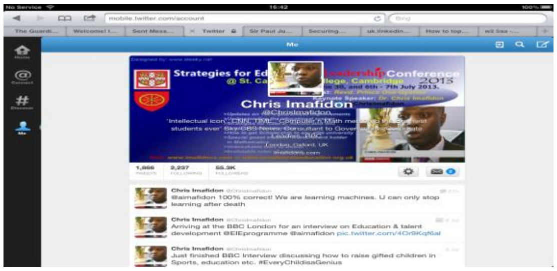
London, Oxford, UK · imafidons.com

Tweets

Minna Salami @MsAfropolitan · 5 Jul
Everyone look up Dr @Chrisimafidon What a champion of gender equity. The Nigerian men speakers at #NCWS have moved me beyond words
Retweeted by Chris Imafidon

EHINOME IKHALIA @Sleekynetwork · 5 Jul
Dr. Chris Imafidon Addressing Women Delegates of NCWS from Nigeria @Chrisimafidon @aimafidon pic.twitter.com/YwLpUhtDX
Retweeted by Chris Imafidon

Figure 1: User login on Twitter as seen via laptop browser



'Intellectual icon', CNN, TIME 'Computer's Math mentor to the brightest students ever' Sky/CBS News. Consultant to Government/Corporate Leaders. BBC

London, Oxford, UK · imafidons.com

Chris Imafidon @Chrisimafidon
@aimafidon 100% correct! We are learning machines. U can only stop learning after death

Chris Imafidon @Chrisimafidon
Arriving at the BBC London for an interview on Education & talent development @EIEprogramme @aimafidon pic.twitter.com/4Or9Kqf6al

Chris Imafidon @Chrisimafidon
Just finished BBC Interview discussing how to raise gifted children in Sports, education etc. #EveryChildisaGenius

Figure 2: User login on Twitter as seen via iPad 2

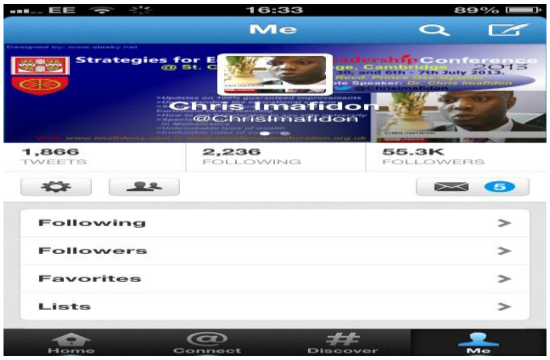


Figure 3:User login on Twitter as seen via iPhone 5

F. *Weak Password Creation*

Password function as the main key to a lock, they can be guessed, cracked, deliberately shared or stolen. Most social networking sites require users to create passwords of no less than 6 characters during account registration. The passwords created are usually hashed or encrypted in the database using MD5 or Sha1l hash functions (Kioon et al, 2013). Unfortunately, users are meant to believe that when the passwords are encrypted in the database, it is impossible to decrypt them if the system is compromised.

The main vulnerability with passwords is that users often choose "easy" to remember passwords; therefore they use a phrase or number such as their birthday, spouse's name or car registration number (Weir et al, 2010). This allows any intruder who knows something about the user to be able to guess the password. Our proposed model shows that the length of a password created does not determine its security strength and if the password strength classification algorithm can be improved, user behaviour when creating passwords will positively change.

IV. THE PROPOSED SOCIAL MEDIA SECURITY MODEL (SMSM)

A. Modification of Password Classification Algorithm:

This model proposes that passwords should be classified according to their various levels of security using more declarative terms such as 'very unsafe', 'unsafe', 'not secure', 'a little secure', 'secure' and 'very secure'. This can be done by ensuring that passwords created by users must consist of combinations of uppercases, lowercases, numbers and at least two special characters. Furthermore, this new security feature will display an instant message to the user using any of the aforementioned declarative terms based on the character combinations selected (Vijaya et al, 2009).

B. Embedding Unique Usernames on Profile Pages:

This security feature is proposed to solve the problem of profile cloning within the site. Many social networking sites only display the first and surnames of users on their profile pages which opens up certain security vulnerabilities when more than one user coincidentally share the same first and surnames. The vulnerabilities involved may allow the malicious user exhort money or commit an online crime under the guise of the victim which could take time to detect. In addition, embedding unique usernames on profile pages within the site will make it very difficult for a malicious user to steal the identity of a genuine user and act on their behalf (Chen et al, 2009).

C. Re-authenticating Registered Users During Activation:

This method will ensure that social media accounts must be activated before full access is granted. The application of this approach is generating a 25 character code for each user and the system sends the code to their email addresses to confirm the ownership of the email used for registration. When the users attempt to activate the account by clicking the activation link sent to their email address, they are redirected to another page, and are required to provide the 25 character code, the username and password before full activation is complete.

This security mechanism will help in preventing web robots from undermining the validation method of the social network. Furthermore, it will increase security consciousness in every user subscribing for the service and protect a user whose email address has been compromised (Fu, 2006).

D. Email Based Two Factor Authentication:

The technique used to implement two factor authentication in this model, is an email based approach. When a user initiates a login session and passes the first stage of authentication (traditional username/email and password), the system sends a randomly generated one time password token to the user's email address and redirects the user to another page within the site which requires the one-time password concurrently (Ikhalia & Imafidon, 2013). The user must navigate to the email address containing the randomly generated password token and supply it before access to the system is granted. This security model is now in huge demand by the industry and implementing an email based two factor authentication method is feasible and cost effective when compared with the SMS approach. Retrospectively, this new security enhancement will reduce security vulnerabilities faced by social media victims of spear phishing, session hijacking, identity and data theft (Yee, 2004).

E. Make Private Message Notification 'Private':

The importance of this security functionality is to protect the confidentiality of a user whose email address is being compromised. This model only allows a message notification sent to a user's email when a private message is sent from the social networking site to the user. In other words, the user must navigate to their private message inbox within the site to read the content of their messages. The necessity of this is to protect users whose emails have been compromised and users who have lost their email accounts (Joshi & Kuo, 2011).

F. Restrict Unauthorised Access To Users' Profile Information:

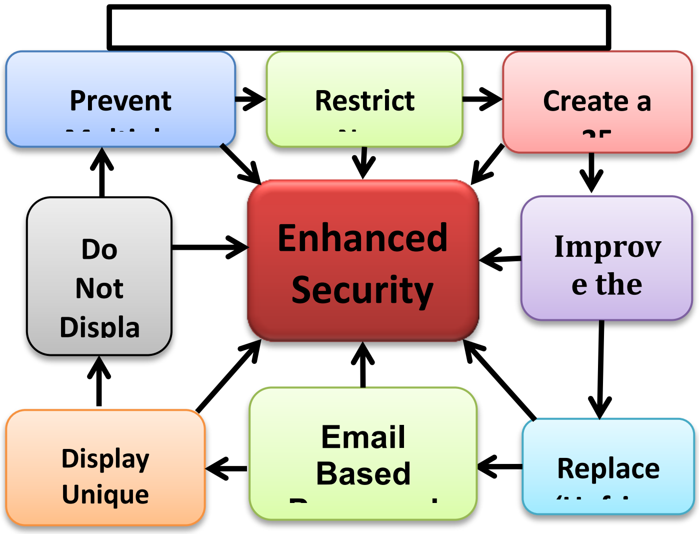
One of the keywords used to define social media by (Dabner, 2012) is "A web-based service that allows individuals to construct a public or semi-public profile within a bounded system"; therefore, only registered users must have access to the information they share within the site. This new security enhancement proposed will prevent external users from viewing profile information of registered users within the site (Ijeh, Preston & Imafidon, 2009).

The major benefit of this security feature prevents the difficulties involved by digital forensic investigators in tracking down malicious attackers hijacking users' information for cross site profile cloning (Ademu & Imafidon, 2012). When this security model is implemented an attacker must register in the system before a malicious activity can be performed, therefore making it easy for the attacker to be traced as most social networks store the IP address of registered users and updates them when they login. (Joshi & Kuo, 2011).

G. Prevent Multiple Login Sessions:

The system prevents users from creating multiple sessions at the same time. The implementation of this security mechanism will ensure that users have control over their accounts. This new enhancement will also make users know when a cyber intruder is accessing their accounts because a message will be shown to the user if a session has been established on the account (Choti et al, 2012).

V. SMSM PROPOSED



VI. CONCLUSION

Social media's lack of security is one of the biggest limitations to the full potential and benefits to the service it provides. Many platform providers are pre-occupied with functionality and ignore serious security loopholes that can be exploited by the exponential growth of social engineering, and other attacks. Hence, platform providers often leave the security of the system to users' discretion, making it vulnerable to the weakest threats.

We have shown that social media can increase in both privacy and security if the new security model proposed in this research work is implemented and tested with the right programming logic.

Further research should include a non-modular implementation of each component of our proposed model (SMSM). It could also point towards evaluating and testing the (*application*) of popular programming languages in order to implement these proposed security solutions to reduce social media vulnerabilities.

REFERENCES

[1] Imafidon, C.O, Ikhalia, E. (2013). “The investigation and implementation of social media security”. Proceedings of the 2nd global conference, London on communication information science and engineering. 24th to 26th June 2013.

[2] Devmane, M. A., Rana, N. K. (2013). “Security Issues of Online Social Networks”. Advances in Computing, Communication, and Control Communications in Computer and Information Science. 361 (1), p740-746.

[3] Ikhalia, E., Imafidon, C.O. (2013). “The need for two factor authentication in social media”. Proceedings of the International Conference on Future Trends in Computing and Communication - FTCC 2013. July 13th-14th, pp1-7.

[4] Adebiyi, A., Arreymbi, J., Imafidon, C. (2012). “Security Assessment of Software Design using Neural Network”. (IJARAI) International Journal of Advanced Research in Artificial Intelligence. Vol. 1 (4), p1-6

[5] Li, J. S., Barnett, T. A., Goodman, E., Wasserman, R. C., & Kemper, A. R. (2013). “Approaches to the Prevention and Management of Childhood Obesity: The Role of Social Networks and the Use of Social Media and Related Electronic Technologies A Scientific Statement from the American Heart Association”. Circulation, 127(2), 260-267.

[6] Manos, T. (2012). “Mining Social Media: Tracking Content and Predicting Behaviour”. Ph.D. Thesis. Geboren Te Athene, Griekenland: Universiteit van Amsterdam.

[7] Lenkart, J. J. (2011). “The Vulnerability of Social Networking Media and the Insider Threat: New Eyes for Bad Guys”. MA Thesis. Monterey, California: naval postgraduate school.

[8] Ijeh, A.C., Preston, D.S., Imafidon, C., Williams, G. (2009). Security Strategy Models (SSM). The School of Computing, Information Technology and Engineering, 4th Annual Conference 2009. pp126-131.

[9] Fu, A.Y, (2006). “Web identity security: advanced phishing attacks and counter measures”. PhD. Hong Kong: City University of Hong Kong

[10] Khonji, M.; Iraqi, Y.; Jones, A. (2013). “Phishing Detection: A Literature Survey”. Communications Surveys & Tutorials, IEEE. 1 (99), p1-31.

[11] Vijaya, M.S., Jamuna, K.S., Karpagavalli, S. (2009). “Password Strength Prediction using Supervised Machine Learning Techniques”. Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09. International Conference. pp401- 405.

[12] Aggarwal, A., Singan, A. R., Kumaraguru, P. (2012). “PhishAri: Automatic Realtime Phishing Detection on Twitters”. IEEE. 1 (1), p1-12.

[13] Yee, K. (2004). “Aligning Security and Usability”. Security & Privacy, IEEE. 2 (5), pp48 - 55.

[14] Joshi, P., Kuo, C.-C.J. (2011). “Security and Privacy in Online Social Networks: A Survey”. Multimedia and Expo (ICME), 2011 IEEE International Conference. pp1- 6.

[15] He, M., Horng, S.J., Fan, P., Khan, M.K., Run, R.S.,, Lai, J.L., Chene, R.J., Sutanto, A. (2011). “An efficient phishing webpage detector”. Expert Systems with Applications (ScienceDirect). 38 (10), pp12018–12027.

[16] Chen, T., Hwang, M., Lee, C., Jan, J. (2009). “Cryptanalysis of a secure dynamic ID based remote user authentication scheme for multi-server environment”. Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference.p725-728.

[17] Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). “Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords”. Proceedings of the 17th ACM conference on Computer and communications security. pp162-175.

[18] Coronges, K., Dodge, R. Mukina, C., Radwick, Z., Shevchik, J., Rovira, E.(2012). “The Influences of Social Networks on Phishing Vulnerability”. 2012 45th Hawaii International Conference on System Sciences. pp2366-2373.

[19] Dabner, N. (2012). “Breaking Ground’ in the use of social media: A case study of a university earthquake response to inform educational design with Facebook”. The Internet and Higher Education. 15 (1), pp69–78.

[20] Lee, P. J. (2010). “A Qualitative Study of the Facebook Social Network: The Desire to Influence, Associate, and Construct a Representative and Ideal Identity”. MA Thesis. Long Beach, CA 90840: California State University.

[21] Altinkemer, K. Wang, T. (2011). “Cost and benefit analysis of authentication systems”. Decision Support Systems (ScienceDirect). 51 (3), p394–404.

[22] Choti, Francis, J., Shaffer, J. A., Sun, C., Soundararajan, E., Willis, S.S., Hochberg, L., and Sean Curtis "Multiple User Login Detection and Response System." U.S. Patent No. 20,120,324,537. 20 Dec. 2012.

[23] Ademu , I. O., Imafidon, C. O. (2012). “Applying Security Mechanism to Digital Forensic Investigation Process”. International Journal of Emerging trends in Engineering and Development. 7 (2), p128-p132.

[24] Almuairf, S., Veeraraghavan, P., Chilamkurti, N. (2011). “IPAS: Implicit Password Authentication System”. 2011 Workshops of International Conference on Advanced Information Networking and Applications. 1 (1), p430 - 435.

[25] Kumar, A., Gupta, S.K., Rai, A. K. ,Sinha, S. (2013). “Social Networking Sites and Their Security Issues”. International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013. 3 (4), p1-5.

[26] Gayathri, K.S., Thomas, T., Jayasudha, J. (2012). Security issues of social media sharing in social cloud. International Conference on Modelling, Optimisation and Computing. 38 (1), pp3806-3815.

[27] Kontaxis, G., Polakis I., Ioannidis S., Markatos, E.P. (2011). Detecting Social Network Profile Cloning. 3rd International Workshop on Security and Social Networking. 1 (1), p295-300.

[28] Kioon, M. C. A., Wang, Z., & Das, S. D. (2013). "Security Analysis of MD5 algorithm in Password Storage". Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation. Pp706-709.

[29] Arachchilage, N. A. G., Love, S. (2013). "A game design framework for avoiding phishing attacks". Computers in Human Behaviour (ScienceDirect). 29 (3), p706-714.

[30] ZDNet. (2013). "Twitter hacked, 250,000 users affected". Available: http://www.zdnet.com/twitter-hacked-250000-users-affected-7000010712/. Last accessed 1st April 2013.

[31] Velazco, C. (2012). LinkedIn Confirms Hack and Leak of "Some" User Passwords. Available: http://techcrunch.com/2012/06/06/linkedin-speaks-some-of-those-compromised-passwords-are-from-linkedin-accounts/. Last accessed 4th May 2013.