International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 4 : Issue 1 *[ISSN 2250 – 3757]*
Publication Date : 09 January 2014

The Need for Two Factor Authentication in Social Media

[Ehinome J. Ikhalia, Dr. Chris O. Imafidon]

Abstract— **Social networks are unequivocally the most used application for communication and information sharing in the 21st century. As growth of this technology increases, there is a need to implement a more secure authentication mechanism to protect users as well as the platform providers from various social engineering attacks. A recent study from LinkedIn and Twitter hacks shows that weak passwords and single factor authentication are still prevalent shortcomings facing most social networking sites. This end-user security lapse often paves way for phishing and malware attacks and undermines the overall integrity of the system. In this study, we review the rise of social networks and the underlying concepts of two factor authentication. Furthermore, we propose a novel, feasible, cost effective and secure technique of applying an email based password tokenization as a second factor authentication in social networking sites.**

Keywords— Authentication, Social Media Security, Tokenization, Renren, Sina Weibo

I. Introduction

In the last few years the evolution of the Web has gained additional technologies commonly referred to as 'social media', examples are social networks, video-sharing, and blogs (Asur et al, 2010). These technologies allow dynamic user-generated contents, the publishing of consumer feedbacks forming global online communities at real time (Saw et al. 2013).

Social media is defined simply as the means of sharing or transmitting information with an audience (Guadagno et al, 2008). With social media, users are the creators and distributors of information using Internet connections.

Authors : Ehinome J. Ikhalia
line 1: University of East London
line 2: United Kingdom
line 4: ehinomeikhalia@gmail.com

Authors: Dr. Chris O. Imafidon

line 1: University of East London, United Kingdom/ Director, EIE
line 2: Formerly, Head, Management of Technology, Queen Mary Univ.
line 4: coimafidon@gmail.com

Moreover, Social networking sites can be described as internet driven platforms that allow users to interact and share information about common interests with one another. Within these platforms, users can articulate a list of other users such as 'Friends' on Facebook or 'Followers' on twitter (Anderson et al, 2012).

On the other hand, Social networking is the process of engaging audiences, such as groups of people with common personal or professional interests who build virtual relationships forming online communities via a social networking website (Li et al, 2013).

After review of existing literature and studies, we propose a two factor authentication model. Based on our proposed two factor authentication model, this paper defines social networks, as an internet based distributed system that involves the processes of identification, authentication, re-authentication and authorization before limited access to its resources is granted the user (Cranor et al, 2008).
Social media can be classified according to the quality, quantity and content of the information being shared in that particular platform (WonKim et al, 2010). Some may appear as macro-blogs, microblogs, forums, wikis, social bookmarking, tagging, digital storytelling, scrapbooking video sharing and podcasts portals.

II. A Review of the Usage of Social Networks

Facebook: Facebook is still the number one most visited social networking platform in the world. With over 1.11 billion registered users worldwide. Studies show that 51 percent of all internet users visit the site at least once a month (GlobalWebIndex, 2013).

Google+: A report by GlobalWebIndex in January 2013 confirms the data in **figure 1.1** that Google+ has moved up the ladder of social network adoption with approximately 343 million registered users.

YouTube: YouTube, which is now widely considered as a social network, trails behind Google+ with 25 percent giving social media giants 'Facebook' a 'head hunt' competition with its exponential growth and massive popularity (GlobalWebIndex, 2013).

S**Twitter:** Between the second quarter of 2012 and the first quarter of 2013, the active users of Twitter increased by 42 percent globally. This indicates that Twitter's growing pace may be tied to the business to business opportunities of the effective usage of the site which is globally accepted and solves the trauma of the global financial meltdown facing so many businesses (GlobalWebIndex, 2013).

III. China's Social Media Evolution

Sina Weibo: Chinese twitter-like micro-blogging site, Sina Weibo, is worth more than 3 billion dollars with over 46 million daily logged in users. The site grew financially in 2012 with a profit of 50 million dollars at the end of the fourth quarter which was generated from advertising (Cutler, 2013). The site surpasses Twitter in areas of functionalities and it currently has more than 100 million registered users. Experts predict that that the rapid growth of the site may exceed Twitter anytime soon (Grumbachm, 2013).

Renren: A Facebook replica 'Renren' is China's leading real-name social networking site and planning for an Initial public offering anytime soon. When Facebook releases a new functionality 'Renren' copies it immediately, it is a social networking site that is seriously business oriented. When it comes to financial returns 'Renren' is the strongest, unlike Facebook's free fan pages, theirs is sold from a starting price of 600, 000 Yuan, which is about 90,000 US dollars (Saw et al. 2013).

Qzone: Qzone currently has about 492 million registered users and most users use a nickname as compared to real names used in 'Reren' which poses a huge limitation to the monetary benefits of the site. Qzone's active users are not clearly known and most of its users are younger people from the rural communities of China (Lukoff, 2013).

From the brief overview of trending social networking sites, it is evident that this technology is not about to fade anytime soon, section 2 explores the concept of Two factor authentication which has not being adopted by these money spinning social networks and is highly expedient because social media has evolved into a new level of social commerce as seen from the trends in section 1.

IV. The Concept of Two Factor Authentication

Two factor authentication is an extra layer of authentication added to the conventional single factor authentication to an account login, which requires users to have additional information before access to a system is granted (Gonzalez, 2008). The traditional method of authentication requires the user to enter only a username and password before being granted access to a closed software or application, whereas two factor authentication requires the user to have additional information known only to the user before access to the system is granted. (Al-Fairuz, 2011).

The information required to authenticate users includes one of the following methods listed below.

- **Knowledge based** i.e. a piece of information the user knows such as a Personal Identification Number (PIN) or password.
- **Biometric** i.e. the biological components of the user such as fingerprints or face recognition.
- **Something within the possession of the user**, such as a hardware or software token.

1.1 **Knowledge based authentication:** This is the commonly used method for decades (Dinne & Mandava, 2010). This requires users to remember lengthy passwords to ensure the 'security' of their accounts. However, it becomes a bane in information security for users to maintain multiple accounts with different passwords, and this results to the creation of 'easy' to remember passwords which becomes a vulnerability exploited by 'attackers' to gain unauthorised access to user accounts (Al-Fairuz, 2011).

Knowledge based authentication method involves the use of secret and open knowledge. Secret knowledge is the information that only the user knows, this includes passwords, password hints, memorable words and PINS. On the other hand, open or shared knowledge is the information which the user uses to interact with the people around him, such as email address, date of birth social security number, name of pets et al (Margot, 2011).

1.2 Something within the possession of the user: With this method, the user may need to carry a token or smart card always in order to have authorised access into the system. The card is first taken by the system and then the password, the user will only be granted access if the details in the card and information of the card matches the corresponding information to the user's id in the database. A study by Hasan & Nur (2012), published through IEEE, discussed that traditional tokenization methods is unusable for accessing emails or social networking sites, which leads an hypothesis that textual based authentication which relies on 'what the user knows' is largely depended on as the most feasible and usable (Devmane et al, 2013).

Contrary to this hypothesis, Argles, Pease & Walters (2007) presented an IEEE publication which combined the use of an electronic token and a biometric based system to authenticate users which proved to be a better authentication mechanism than single based authentication. Furthermore, research findings by Alsulaiman and Saddik (2008), supported (Argles et al 2007), stating that to build secure

information systems such as a social media, it is necessary to use keys which cannot easily be committed to memory by users. The emphasis was that users who use lengthy passwords, store their information in a file directory which can be easily accessed later by them or hacked by attackers. Thus, it defeats the effectiveness and objectives of password secrecy and presents a weak point for attackers to exploit.

Based on the aforementioned studies, we propose a new method in applying tokenization as a second factor authentication in social networking sites. The proposed model is an email based one-time password sent to users after initiating a login session on their social network accounts at the first layer of authentication. When the user successfully passes the second authentication, the onetime password becomes invalid and a new one is sent to his/her email address if the current session is terminated by the user and another session is initiated.

.

v. Vulnerabilities of Single Factor Authentication

Over the last few years, Social media, otherwise known as 'Web 2.0' has grown indelibly to become the greatest technological evolution in history. The impact of this technology has positively changed the way of doing business, accessing information and negatively ruining the political and professional careers of many (Posetti, 2010). Ironically, increase in usability is now proportionate to the increase in vulnerabilities of social media (Ademu & Imafidon, 2012). Single factor authentication is the use of static passwords and is still the only requirement in accessing today's dynamic Web 2.0 applications by most platform providers. The major advantage of this type of authentication is the 'convenience' experienced by users because most static passwords are very 'easy' to remember. This becomes a serious vulnerability issue as such passwords are easy to guess by humans and computers.

A. *Dependent on one line of defence:*

In addition to the open or shared knowledge used by majority of the knowledge based authentication methods of social networks discussed in section 2.1 A static password acts as the first and last line of defence to restrict unauthorised access. This system requires a user to enter a username or email which is followed by a 'secure' password. Then the system queries the database to check if there is a matching record with the details entered. If the system gets a matching record, the 'secure' password of the user is compared against the password stored in the database, and then if there is a match the user will be granted access into the system. In most social networks, user passwords are encrypted in the database, therefore the comparison is done after the entered password is also encrypted with the same algorithm used to encrypt the stored password (Piper et al, 2004).

Single factor password authentication methods are user defined, and most users use weak passwords they can remember (Chen et al, 2011). On worst scenarios, users tend to write the passwords down and store the soft copy in a 'safe' location, thereby totally degrading the secrecy of passwords (Adebiyi et al, 2012).

. Studies have shown that the growth of dynamically diverse Internet application services and mobile smart phones compels users to manage multiple social network accounts (Freund & Weinhold, 2002). Therefore, the number of passwords required to secure multiple accounts has also increased proportionately, however, the common unsecure practice for users is to reuse one passwords across all accounts which increases the security lapse because it easily permits an attacker to explore all other accounts when one has been compromised.

B. *Susceptibility to Phishing Attacks*

Phishing is a social engineering attack initiated by cyber-criminals through sending disguised emails or posting URLs on social networks to lure potential victims to access fake websites and induce them to expose sensitive and private information (Coronges et al, 2012). Phishing attacks are aimed at spoofing users visually and semantically by making the appearance of the fake website look almost the same as the real ones as well as their Universal Resource Locators (URL).

To describe the financial losses accrued by individuals and organisations due to this crime as 'alarming' is an understatement. In fact this 'online tornado' has the capacity of causing a more severe global economic meltdown or worse still an 'economic evaporation' (Fu, 2006). In 2012 the number of phishing attacks initiated was 59% higher than 2011 with a record breaking loss of $1.5 billion US dollars, which represents an approximate increase of 22% from 2011 (RSA, 2013).

C. *How Single Factor Authentication Is Vulnerable To Phishing*

In addition to the facts presented in section 3.2, this study posits that the degree of sensitivity or vulnerability of information determines the level of security needed to protect such information. For example, the medical records of patients are both sensitive and vulnerable. It is sensitive because unauthorised access could result to The Health Insurance Portability and Accountability Act of 1996 violations and also lead to the loss of medical institution's integrity (HIPAA, 2013). On the other hand, it is vulnerable if the computing device is shared by many users and connected to the Internet. Considering the amount of information shared on social networking sites, an attacker can easily aggregate and link such information with the medical records of a user, or launch

a targeted phishing attack. However, since most authentication procedures of Web 2.0 sites require only a username/email and password to verify users, it becomes easy to harvest the victim's information. Therefore, these kinds of situations require two-factor authentication.

VI. Benefits of Two Factor Authentication

The following are the benefits of two factor authentication in any closed application system.

Enhanced security: Many users store their passwords unsafely since 'secure' passwords can easily be forgotten. The use of two factor authentication will prevent such security vulnerability. Even when the password of a user is guessed or discovered using any social engineering technique by an 'attacker', the attacker will not be able to provide the second information necessary at the second layer of authentication such as a smart card, finger print or a onetime password token. Therefore the implementation of these second authentication factors will deny unauthorised access to any system by potential attackers (Mohammed, 2004).

Reduced Risk: The implementation of two factor authentication reduces the probability that an unscrupulous action will be performed. With two factor authentication social engineering techniques such as dictionary attack, brute force attacks, phishing, is reduced to the lowest minimum. The use of single factor authentication brings extreme risks because the technology is very easy to implement and as well very easy to break by potential attackers (Almuairfi et al, 2011).

Prevents Monetary Loss: One of the most significant benefits of two factor authentication is the prevention of illegal access to the bank accounts of potential victims. With the description of what two factor authentication is as highlighted in section 2, an attacker will find it very difficult or impossible to steal money from the bank account of a potential victim. Nevertheless, in areas were legal policies are applied to prosecute 'attackers' when caught; tax payers money is also wasted on circumstances that can be prevented if two factor authentication is in place. Therefore, two factor authentication prevents not only the financial loss of the victim but also the government (Ijeh, 2010).

Reduces Identity Theft: The challenge of identity theft has been in existence for a long time. The application of identity theft is also intertwined with the issue of profile cloning. Identity theft is the process of an attacker gaining unauthorised access to the online account of a victim (e.g. a social network), and then generates posts or sends messages through the account of the victim, that such victim would not normally post or send. The negative implication of identity theft could lead to a totally damaged reputation of the targeted victim or in worse cases loss of employment and life. Two factor authentication mitigates this problem, because at the second layer of authentication the password token automatically generated is a onetime password and it is difficult for someone else to intercept or guess. Even if the token is intercepted it can't be usable the next time it is needed, therefore two factor authentication helps to prevent the vulnerability of identity theft (Barral, 2010) and (Imafidon & Ikhalia, 2013)

Reduced Data Theft: Unauthorised access to sensitive information of an individual or an organisation often leads to the theft of valuable data. The result of this problem leads to issues such as loosing credibility and loss of business which affects victims of this vulnerability. Fortunately, two factor authentication has the capacity to reduce this security challenge to a minimal extent (Reddy, 2011).

Increased Flexibility: With implementation of two factor authentication, organisations and individuals will worry less about the security of online applications they use for personal or business purposes because the security and privacy of their data will be too hard to breach by prospective attackers. Hence, there will be free remote access to applications (such as social networking sites) within the organisation which will enhance greater working flexibility practices (Mohammed, 2004).

VII. Drawbacks of Two Factor Authentication

Cost: The major issue with setting up a two factor authentication procedure is the financial implications it involves. The software implementation may not be very expensive but the maintenance which includes training people to use and enforce the system. For example the RSA securID system uses a keychain device that automatically generates one-time ciphers regularly. The devices are developed to last a certain amount of years and new ones will need more money to be implemented (Dinne & Mandava, 2010).

Inconvenience: This particular disadvantage of two factor authentication depends on the methodology of the authentication used. For example if the second layer of authentication used by a system requires a user to slot in a hardware token such as a smart card before being authenticated, it becomes very inconvenient and unfeasible if the smart card is damaged or stolen, which may require the user to purchase a new one. Secondly, if the password token is sent via SMS to the mobile phone of the user, the user will be compromised if the phone is stolen or lost. Therefore this buttresses the point emphasised in sub section 5.1 above (Dinne & Mandava, 2010).

VIII. The application of the proposed email based two factor authentication.

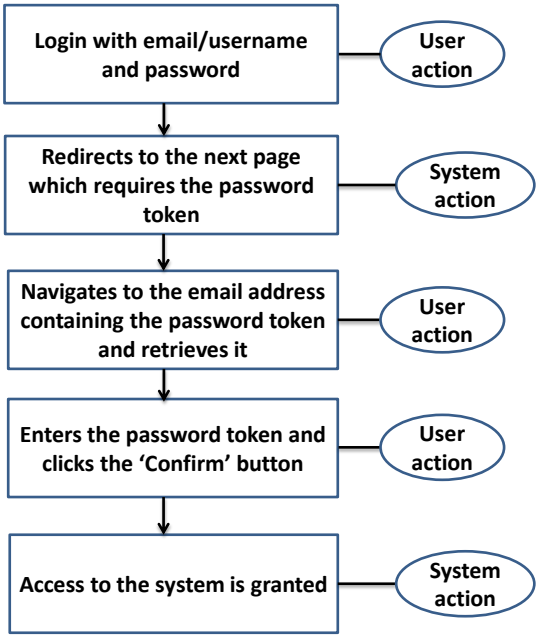

Figure 1: Showing the proposed two factor authentication solution to enhance the security of social networking sites.

From figure 1 above, the following steps below explains the new proposed model.

Step 1: Common with many existing social networks, an email or username and password is required for users to login to their account. The user enters the correct details of the email and password then clicks the 'login 'or 'sign up' button.

Step 2: Instead of being granted access to the profile page or home page of his/her account, the system redirects the user to the second stage of authentication (re-authentication), which requires the one time password token sent to the email address of the user when the login process was initiated at the first authentication stage.

Step 3: The user navigates to the email address which contains the password token needed to pass the re-authentication procedure and then retrieves it.

Step 4: The user enters the onetime password token in the required input field and then clicks the 'confirm' button.

Step 5: Now the user is securely allowed access to the system and must go through this 5steps if another login session is initiated.

IX. Evaluation and conclusion.

We have discussed the concepts of two factor authentication, and explained the reasons why it is a necessity in social networking sites and not only banks, health sector and the RSA. From this work, we also reviewed the two major drawbacks of two factor authentication, which are the cost of implementation and inconvenience to usage. However, these problems could be dealt with depending on the methodology of the second factor authentication implemented. Our proposed model is inexpensive as well as convenient as against the hypothesis proposed by Hasan & Nur (2012).

This study has shown that two factor authentication is an important security measure that should be implemented in social networks as seen in banks and governmental institutions such as the RSA. Some of the reasons are due to the fact that social networking has redefined the way millions of people are living their lives and also the way many business operate. Therefore the sensitive data that is being shared via social networks and the identities of the users that shares them needs adequate security to be able to withstand advancements in social engineering techniques by cyber-criminals.

Furthermore, this study evaluated the benefits of two factor authentication and proved that the benefits outweigh the drawbacks if the methodology used is taking into consideration.

Finally, we conclude by proposing a more feasible, cost effective and secure solution on the applicability of two factor authentication which involves only five steps, thus keeping the integrity of the system intact and reducing the intractability between security and usability.

X. Further Research

Although two factor authentication helps in reducing the problems associated with identity theft, data theft and phishing, there are vulnerabilities were this technology becomes totally defenceless. For instance, the watering hole malware attack was targeted at software developers working at Facebook in January 2013. This successfully executed attack infected websites the developers normally visit with a malware called 'MAC Trojan', thereby infecting their personal PCs. When an attacker gets Trojan installed on a victim's computer, if the victim logs into his/her bank account's Website the attacker piggybacks on the session trough the Trojan to make any fraudulent transaction he wants. Therefore, there is a need to investigate and develop a filtering system to mitigate the distribution of malware and viruses on social networks. Also

Multiple logins generate a new set of threat that should be investigated and mitigated.

Acknowledgments

The University of Cambridge (Computer Science security seminar series) and William H Gates computer laboratory. Research Division of The Excellence in Education Programme, London (www.ExcellenceinEducation.org.uk). Anne-Marie Imafidon M. Math & Comp Sci (Oxon) Formerly, Keble College, University of Oxford, Oxford, England, UK

References

[1] Al-Fairuz, M. A. S. (2011). "An investigation into the usability and acceptability of multi-channel authentication to online banking users in Oman." (Doctoral dissertation, University of Glasgow

[2] Argles, D., Pease, A., Walters, R.J. (2007). "An Improved Approach to Secure Authentication and Signing". *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*. 1 (1), p119-123 .

[3] Hasan, M., Nur, K. (2012). "A novel 3-Layer user authentication system for remote accessibility". *Computer and Information Technology (ICCIT), 2012 15th International Conference* . 1 (1), p44-445.

[4] Ijeh, A.C, (2010). "Geofencing as a Security Strategy Model". Ph.D. *University of East London*: East London. (Director of studies: Dr Chris Imafidon)

[5] Barral, C., (2010). *Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography*. Ph.D. École Polytechnique Fédérale De Lausanne: Suisse.

[6] Gonzalez, E.P. (2008). Content Authentication and Access Control in Pure Peer-to-Peer Networks. *Universidad Carlos Iii De Madrid* Ph.D. Thesis 1 (1), p1-240.

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

[8] 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.

[9] Yoo, S. G., Lee, H., & Kim, J. (2013). "A Performance and Usability Aware Secure Two-Factor User Authentication Scheme for Wireless Sensor Networks." *International Journal of Distributed Sensor Networks, 2013*.

[10] Grumbach, S. (2013). "The stakes of Big Data in the IT industry China as the next global challenger"? The 18th International Euro-Asia Research Conference, The Globalisation of Asian Markets: implications for Multinational Investors, Venezia, January 31 and February 1st, 2013. 1 (1), p1-15.

[11] Shi, Z., & Whinston, A. (2013). "Network Structure and Observational Learning: Evidence from a Location-Based Social Network" 2013. 1(1), p1-31

[12] Saw, G., Abbott, W., Donaghey J. (2013). Social media for international students – it's not all about Facebook. *Library Management*. Vol. 34 (3), p156 - 174.

[13] Mohammed, H.C, (2004). "Authentication as a tool of Web Security". M.Sc. *University of East London*: East London. (Supervisor: Dr. Chris Imafidon)

[14] Reddy, M.A., (2010). "Security Issues in Clinical Informatics". M.Sc. *University of East London*: East London.(Supervisor: Dr Chris Imafidon)

[15] Dinne, H., Mandava, K., (2010). "Two Way Mobile Authentication System". M.A. *Blekinge Institute of Technology: Karlskrona, Sweden*.

[16] Freund, C., & Weinhold, D. (2002). The Internet and international trade in services. *The American Economic Review, 92*(2), 236-240

[17] 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.

[18] Almuairfi, 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.

[19] WonKim A., Ok-RanJeong A., Sang-WonLee (2010). "On Social Websites". *Information Systems (ScienceDirect)*. 2 (35), p215–236.

[20] Chen. X., Bose, I., Leung, A.C.M., Guo, C. (2011). "Assessing the severity of phishing attacks: A hybrid data mining approach". *Decision Support Systems (ScienceDirect)*. 50 (4), p662-672.

[21] 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.

[22] Anderson, J and Stajano, F. (2012). "Not That Kind of Friend: Misleading Divergences between Online Social Networks and Real-World Social Protocols". *University of Cambridge Computer Laboratory*. 1 (1), p1-6.

[23] Coronges, K.,Dodge, R.,Mukina, C.,Radwick, Z., Shevchik, J., Rovira, E .(2012). "The Influences of Social Networks on Phishing Vulnerability". *System Science (HICSS), 2012 45th Hawaii International Conference*. 1 (1), p2366 - 2373.

[24] RSA. (2013). "The year in phishing". *RSA fraud report*. 1 (1), p1-7.

[25] HIPAA. (2013). "Welcome to the HIPAA, Privacy & Security Training Module". *The University of North Carolina at Chapel hill*. 1 (1), p1-61.

[26] 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

[27] Asur, S., Huberman, B. A. (2010). "Predicting the Future with Social Media". *2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*. Vol.4 (10), p492-499.

[28] Guadagno, R.E., Okdie, B.M., Eno, C.A. (2008). "Who blogs? Personality predictors of blogging". *Computers in Human Behaviour(ScienceDirect)*. Vol.24 (5), p1993-2004.

[29] Helkala, K. (2012). "Disabilities and Authentication Methods: Usability and Security". *2012 Seventh International Conference on Availability, Reliability and Security*. 1 (1), p328-344.

[30] Posetti, J. (2010). "The #Spill Effect: Twitter hashtag upends Australian political journalism". *Mediashift* (Available on: http://www.pbs.org/mediashift/2010/03/the-spill-effect-twitter-hashtag-upends-australian-political-journalism061.html Last accessed: 4th March 2013)

[31] Hartshorn, S. (2010). "5 Differences between Social Media and Social Networking". *Available: http://socialmediatoday.com/index.php?q=SMC/194754. Last accessed* 20th May 2013

[32] Cutler, K., M. (2013). "*Sina Weibo, China's Equivalent of Facebook and Twitter, Gets $586M Investment from Alibaba"*. Available: http://techcrunch.com/2013/04/29/sina-weibo/. Last accessed 29th April 2012.

[33] Lukoff, K. (2013). "What Makes China's Top 4 Social Networks Tick"? Available: http://mashable.com/2011/03/18/china-top-social-network/. Last accessed 29th April 2012.

[34] eMarketer. (2013). *Which Social Networks Are Growing Fastest Worldwide? Read more at http://www.emarketer.com/Article/Which-Social-Networks-Growing-Fastest-Worldwide/1009884#lQeiTIAboGvAhGgv.9.* Available: http://www.emarketer.com/Article/Which-Social-Networks-Growing-Fastest-Worldwide/1009884. Last accessed 14th May 2013.

[35] GlobalWebIndex. (2013). *Stream Social Q1 2013: Facebook Active Usage Booms.* Available: http://www.globalwebindex.net/Stream-Social. Last accessed 14th May 2013.

[36] 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.

About Author (s):

Ehinome J. Ikhalia has recently completed his Masters degree in Information Technology and shown interest in Social Media and computer security. He was one of the students nominated to attend the computer security seminars at the University of Cambridge, UK. His research has been accepted for publication in The Institution of Engineering & Technology (IET) sponsored conference (CCSIE) in London

Chris O. Imafidon is consulted by Presidents, Monarchs, Governments and Corporate leaders. He is Director of Research (Hon) for the Excellence in Education program (UK). Chris Imafidon has been guest professor at Harvard, Cornell, and Columbia Universities. He has been invited to lecture at Cambridge and Oxford. He has been featured by the BBC; CNN; TIME Magazine; The Times; USA-Today; Wall Street Journal; New York Times and other leading media outlets.