Account Creation Security of Social Network Sites

Joanne Kuzma
University of Worcester
United Kingdom
E-mail: j.kuzma@worc.ac.uk

Abstract

The growth of Online Social Networking (OSN) sites has created opportunities for consumers to communicate with others as well as partake in many new services. To use OSN features, consumers must create accounts using security technology and processes established by individual OSNs. These protective measures are not consistent among various networks and there is wide variation on how OSNs use various security methods: password strength, verification, password reset requirements and verification. This study analyzed 30 global networking sites to determine the level of account creation and authentication protection. The results showed significant gaps among security methods, which could lead to vulnerabilities and unauthorized access to personal data, and should raise serious concerns to OSN users and firms. The paper suggests some technical and procedural options for mitigating risks.

Key Words: Online social networks, login security, passwords

Introduction

The rise of Online Social Networking (OSN) sites has brought a multitude of new services and methods allowing consumers to communicate globally. The business success of OSNs depends on attracting a large number of users. Traditionally, business growth has ranked highest in priority than security, and design and development has lagged (Hogben, 2007). The author explains that due to the specific nature of their business, OSNs may have certain threats and vulnerabilities that can especially affect their sites and cause dangers to users. Some if these specific risks include: user profiles and personal information downloaded by third parties (secondary data collection), digital dossier aggregation, face recognition, content-based image retrieval, identification (ID) theft, social aggregators, spam and phishing (Hogben, 2007). The author states that although a myriad of technical and procedural methods exist to address each problem, OSNs should first start with stronger authentication and access control during account creation to protect both the firm's systems as well as individual private data.

Users must establish an individual account before using OSN services. Part of the setup process includes establishing a secure account ID and password, which will be used to access specific site services. Some vulnerability problems, such weak passwords control, could open up users to risks such as social aggregators breaking passwords and entering the site to mine personal data. In addition, hackers could steal member's passwords to enter the site and promote offers on other's profiles (Hogben, 2007). Thus, account creation security and authentication is a powerful first-step in risk mitigation for OSNs and their users.

There were two major aims addressed in this study:

1. Document common security schemes that OSNs use for account creation
2. Determine if various OSNs consistently apply the common security methods.

The study starts with a literature review of account creation and security, followed by a methodology and results discussion. Finally, this study highlights security implications and suggests alternatives for OSNs to consider when strengthening account security.

2. Literature Review

2.1 Account Creation Safety

Logging in with usernames and passwords is the most common way to access modern computer systems (Bardram, 2005). However, the author argues that if authentication is too difficult, users will find ways to circumvent the system. In Adams and Sasse's study (as cited in Bardram, 2005), increasing the level of account security can have the opposite intended effect. Passwords with too many digits may make them difficult to remember. Thus, users may write them down and place their accounts at risk. Although users may be motivated to support high levels of security, actual practice might be different (Bardram, 2005).Bradley (2010) suggests firms require strong passwords to protect systems, as more characters take longer to crack. It is also advisable to have a combination of letters and numbers, or special characters. Although a dedicated hackers can crack most passwords with enough time, having a minimal level of protection will mitigate many attacks.

The idiom CAPTCHA stands for 'Completely Automated Public Turing test to tell Computers and Humans Apart" (Schlaikjer, 2007). These are computer-generated checks that attempt to tell humans and computers apart by presenting specific checks that humans should be able to pass, but computers could not. This technology came into being because problems Web owners encountered with automated spam-bots gaining access to Web services that they should not have (Schlaikjer, 2007). CAPTCHA is now almost a standard security mechanism for defending against undesirable or malicious Internet bot programs (El Ahmad, et al, 2010). CAPTCHA technologies can be used as part of the account creation or modification process. The process requires users to complete a task, such as typing in a specific combination of letters or numbers. Once the task is successfully completed, the system allows the user to continue the process. Site managers implement CAPTCHAs to prevent programmatic access and account creation by automated programs (Heymann, et al 2007). Heymann (et al, 2007) completed research on using security countermeasures on OSNs. They concluded that methods, such as CAPTCHAs, could be effective in preventing spam and automated account creation by computers. They suggest that different methods might be better suited for specific OSN communities.

Automated password-reset is common for Web mail (Keizer, 2008). This authentication method allows locked-out users to reset their passwords by clicking on a 'forgot password' link. The system then asks a challenge, or 'personal verification' question, such as a mother's maiden name (Rabkin, 2008). Ideally, the most secure security scheme would allow users to write their own question, providing a measure of control to the user. However, a study by Rabkin (2008) found that only one in 20 banking sites allowed this option.

There are vulnerabilities with automated resets and challenge questions. Keizer (2008) indicates that personal information contained in the challenge questions can often be found by searching OSNs and other Web sites. In addition, OSNs often email passwords to primary email addresses, but few bother to email new passwords to alternate addresses for another level of verification. Falk (et al, 2008) indicates there are risks of using email addresses for user names, as they are easy to collect and guess. User acceptance with security is also an issue site administrators need to consider. Users may find some methods bothersome and time-consuming, such as waiting for verification emails to reset passwords (Shirali-Shahrez, et al., 2007).

2.2 Security Practice Studies

Furnell (2007) assessed the password practices for 10 popular Web sites, including guidance selection, restrictions on password choices and policies for resetting forgotten passwords. The findings revealed a variable situation among sites, but none performed ideal safe security. A study of 34,000 legitimate MySpace passwords found that almost 1% had 'password' as part of the text, and many contained easily guessed common words such as colors, years, names and sports (Grimes, 2006). Falk (et al, 2008) performed a study on 214 financial sites, and found 28% had inadequate policies for user IDs and passwords, such as permitting short passwords or email addresses for user IDs.

A study by Rabkin (2008) found that 12% of answers to challenge questions could be found on a social networking site. Another study by Griffith and Jakobsson (cited by Rabkin, 2008) found that mother's maiden names could often be discerned from online public record sites. Although these sites did perform a variety of different Web sites, no OSN site study has performed research on the various security factors contained in this study.

3. Methodology

The research was accomplished through analyzing 30 OSNs and determining the levels of account creation safety. The project consisted of three phases:

1. Choosing a sampling of sites to test
2. Determining which types of security factors should be included in the study
3. Compiling and analyzing the results.

3.1 Choosing a sampling of sites

The first phase of this project was dividing 30 OSNs into categories using stratified random sampling methodology. comScore, a global marketing intelligence firm, provides demographic information about OSNs located throughout the world (www.somscore.org). A random sampling of 30 different OSNs was chosen from a list of 100 most popular OSNs.

3.2 Determining security factors

Although a plethora of security factors exist for online application security, this research concentrates on seven popular methods most appropriate for account creation. The types included:

1. The minimum number of characters or digits required for a password (including the range of digits).
2. Does the OSN ask a challenge question if the user needs to reset a password?

3. Does the user have the ability to reset their password?
4. Does the OSN have a stated policy that indicates that they automatically prompt for a password change at a specific time interval?
5. Does the user need to use a CAPTCHA method to verify their account?
6. Does the OSN require email validation for account setup?
7. Does the OSN use a user name instead of an email address as the login ID?

3.3 Compiling and analyzing factors

For each of the 30 OSNs, the researcher followed the account lifecycle in creating an account. This started with accessing the home page URL and clicked on the 'create new account' link. For different OSNs, different account information was required to complete the account creation. For example, MySpace requires a user to provide an email address, password, full name, date of birth and gender (MySpace, 2010). Each OSN had slightly different requirements, but all did mandate an ID/email and a password. For all passwords, the researcher first attempted to bypass this required field and clicked on 'submit' to continue. In all cases, the system responded with a request to enter a valid password and gave the required number of characters to enter. All OSNs required the user to enter a minimum of one digit to complete the account creation process.

The next stage in account creation was usually a verification step. Some OSNs then sent an email to the user to click on a link to verify the account setup. One issue with email verification is that emails were not always quickly received. In a few cases, several minutes passed before the OSN verification email was received and when the account could be created. Other OSNs had a CAPTCHA method requiring the user to enter a series of text to continue to account creation process. The only problem encountered with filling out the CAPTCHA was usability, as sometimes the CAPTCHA characters were difficult to decipher.

4. Results

The tables in this section show results for security account creation testing. The first column is the list of 30 OSN sites tested. Column two shows the number of password digits required. Column three indicates whether the OSN asks a challenge question in order to reset a password or if the user has forgotten a password. The answers are either yes (y) or no (n). Column four designates if the user has the ability to reset their password. Column five shows if the OSN automatically prompts for a change in password after the initial creation. Column six shows if the OSN has a CAPTCHA requirement during account creation. Column seven lists if the OSN requires the user verify the account setup via email verification. The final column indicates whether the user can create their own account user name instead of their email serving as the ID.

The average minimum requirement for password digits is five characters. Two sites only require a one-digit password and three OSNs require a minimum of three. The largest minimum requirement is eight digits (two OSNs). Results in column four show that 27 sites (97%) do allow the user to request a password reset. If a user forgets their password and requests it to be reset, only two sites require that the users answer a predefined challenge question in order to reset their password (column three). Results from column five show that no OSN has a policy that automatically prompts users for a change in password. Eighteen sites (60%) do have a CAPTCHA requirement during account creation and 20 (67%) send an email verification during account creation setup. The final column shows that 18 OSNs (60%) do require the users to create a valid user ID as their account name instead of merely using an email address for the ID.

Table 1: OSN Account Setup Results

Site	Digits	Challenge question if forget	Reset	Change	Captcha	Verify Via email	User Name
bebo	5+	n	y	n	y	y	y
bharatstud	6-12	n	y	n	n	n	y
bigadda	6-15	n	y	n	y	y	y
blackplanet	6+	n	n	n	y	y	y
blurty	3+	n	y	n	n	y	y
classmates	6-12	y	y	n	n	n	n
couchsurf	5+	n	n	n	y	y	y
facebook	6+	y	y	n	y	y	n
fanpop	3+	n	y	n	n	n	y
friendster	5-10	n	y	n	n	y	n
graduates	4+	n	y	n	n	y	n
habbo	6+	n	y	n	y	y	y
hi5	6-20	n	y	n	n	y	n
hyves.nl	4+	n	y	n	y	y	y
ibibo	6-32	n	y	n	y	n	y
inviteshare	1+	n	y	n	n	n	y
linkedin	6+	n	y	n	n	y	y
migente	6+	n	y	n	y	y	y
mog	6+	n	y	n	y	y	y
myspace	6+	n	y	n	y	n	n
myyearbook	3-12	n	y	n	y	n	n
ning	1+	n	y	n	y	y	n
orkut	8+	n	y	n	y	y	n
perfspot	6-20	n	n	n	n	n	n
skyrock	6-16	n	y	n	y	y	y
sofamous	5+	n	y	n	n	n	y
tagged	6+	n	y	n	y	y	n
twitter	6+	n	y	n	y	y	y
xing	4+	n	y	n	n	y	n
youtube	8+	n	y	n	y	n	y
Total (y)		2	27	0	18	20	18
Percent		0.06	0.90	0.00	0.60	0.67	0.60

5. Implications and Discussion

The major aims of this study were to document which security mechanisms most sites use for account creation and to determine which methods are consistently applied. Seven security methods were identified and analyzed. Positive results in this study show that at least 60% of OSNs do require email verification, use CAPTCHAs and require user accounts instead of emails for account IDs. In addition, 90% of sites do allow users to reset passwords. However, overall usage of various methods was inconsistent among OSNs, with some security types not being used by any sites. One of the major issues discovered is that no OSN had an automatic password change policy where passwords are periodically changed. Buechler (2007) recommends that systems are set up to prompt users to modify passwords every 30-90 days.

Most security experts recommend that six or seven characters to be the minimum number required for a strong password (Wood, 2007). Yet, this research has shown that the average minimum for OSNs is five characters, with 12 sites (40%) requiring five or less characters. This could put the sites and user account at risk of automated password hacking software, which can use brute force attacks or dictionary attacks to break passwords. OSN site administrators may consider other technical and procedural account creation options to provide higher protection levels or better risk mitigation. For example, instead of relying on users to create passwords, a system could automatically generate passwords. However, most firms have abandoned this approach because it was not user-friendly and was an administrative burden (Wood, 2007). However, the author explains that if site administrators allow users to create their own passwords, the firm should ensure that users are acquainted with rules to constructing strong passwords and the reasons strong security is important to keeping their information secure.

Another development is the quest for an industry standard, such as OpenID, which would allow users to sign on to multiple social sites with one ID. This would provide safety by having the process managed by an authentication provider (Recordon & Fitzpatrick, 2006).

In some cases, OSN site administrators need more specific access control over their sites, such as the ability to determine whether the client attempting to access the page is a member of a certain group. Yardi (et al 2008) proposed a photo-based Web site authentication framework for OSNs such as Facebook. Their proposed system is especially useful for the social networking industry, and presents photos to a user and asks them to identify the names of subjects in those photos, which can help verify a client's membership in a certain group. It restricted access to content to a specific social network group without requiring individual site-specific access control. This study raises some serious concerns of security that could have potential harmful effects on millions of OSN users. Sarel & Marmorstein (2006) quote studies that show security issues often are the main reason for barriers to adoption of online use by consumers. Not only are users adversely affected by lack of security, but online service providers could potentially suffer from poor security. Goel & Shawky (2009) state that security problems and breaches can damage a firm's reputation, and they estimated that an announcement of a breach had a negative impact of about 1% of the market value of the firm during the days surrounding the event. Thus, lack of secure account creation could be problematic for both consumers as well as firms.

A good deal more research is needed to fully assess the overall security of OSNs. One limitation of this study is that it reviewed seven techniques, but further research may analyze other methods. For example, a review on how many OSNs deploy a method of locking users out of the system after a number of failed login attempts may be beneficial to understand. This technique would prevent brute-force attacks from discovering passwords, but may cause inconvenience to users. The study could also be to other types of security criteria.

4. Conclusion

This paper had two goals: document current account creation methods most OSNs use and determine the level of use among popular sites. The research found a wide range of methods does exist that can ensure more robust security. However, various OSNs inconsistently used available security options. In one case, prompting for periodic password changes, no OSN used this practice. This lack of consistency and weak security design may leave both the firm and individual at risk for a variety of vulnerabilities. This paper clearly shows a potential serious impact of user security, and consumers who utilize OSN sites should be concerned about their data protection. If accounts are breached, individuals could suffer identification theft. OSNs themselves could lose the goodwill of their consumers and suffer loss of service as well as inconvenience of fixing hacked systems.

Personal account creation is the first step in actively securing an online system. A variety of authentication methods and procedures do exist to mitigate vulnerabilities, and it is imperative that OSNs actively deploy safe authentication schemes to protect their firm and customers.

References

Bardram, E. (2005). The trouble with login: on usability and computer security in ubiquitous computing. Personal and Ubiquitous Computing, 9(6), 357-367.

Bradley, T. (2010). How to Stop 11 Hidden Security Threats. PCWorld, March 2010, 68-78.

Buechler, C. (2007). Six steps to developing secure passwords. Managing Information, 14(3), 6-8.

El Ahmad, A, Yan, J, & Marshall, L. (2010). The robustness of a new CAPTCHA. In Proceedings of the Third European Workshop on System Security, pp. 36-41. Paris, France. European Conference on Computer Systems.

Falk, L, Prakash, A, & Borders, K. (2008). Analyzing websites for user-visible security design flaws. In Proceedings of the 4th symposium on Usable privacy and security (SOUPS), pp. 117-126. Pittsburgh, PA, July 2008. ACM International Conference Proceeding Series.

Furnell, S. (2007). An assessment of website password practices. Computers & Security, 26(7-8), 445-451.

Goel, S, & Shawky, H. (2009). Estimating the market impact of security breach announcements on firm values. Information and Management. 46(7), 404-410.

Grimes, R. (2006). MySpace password exploit: Crunching the numbers (and letters). InfoWorld. [Online] Available: http://www.infoworld.com/d/security-central/myspace-password-exploit-crunching-numbers-and-letters-983 (October 29, 2010)

Heymann, P, Koutrika, G, & Garcia-Molina, H. (2007). Fighting Spam on Social Web Sites: A Survey of Approaches and Future Challenges. IEEE Internet Computing, 11(6), 36-45.

Hogben, G. (2007). Security Issues and Recommendations for Online Social Networks, Technical Report ENISA. [Online] Available: http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (October 30, 2010)

Keizer, G. (2008). Web Mail Rivals at Risk of Password-Reset Hacks. Computerworld. [Online} Available: http://www.computerworld.com/s/article/327018/Web_Mail_Rivals_at_Risk_of_Password_Reset_Hacks (November 5, 2010)

Rabkin, A. (2008). Personal knowledge questions for fallback authentication: Security questions in the era of Facebook. In Proceedings of the 4th symposium on Usable Privacy and Security (SOUPS), pp.13-23. Pittsburgh, PA, July 2008. ACM International Conference Proceeding Series.

Recordon, D. & Fitzpatrick, B. (2006). OpenID authentication 1.1. [Online} Available: http://openid.net/specs/openid-authentication-1_1.html (December 20, 2010)

Sarel, D & Marmorstein, H. (2006). Addressing consumers' concerns about online security: A conceptual and empirical analysis of banks'actions. Journal of Financial Services Marketing, 11(2), 99-115,

Schlaikjer, A., (2007, November). A Dual-Use Speech CAPTCHA: Aiding Visually Impaired Web Users while Providing Transcriptions of Audio Streams. [Online] Available: http://www.cs.cmu.edu/~vunit/participants/Andy_Schlaikjer.html (November 23, 2010)

Shirali-Shahrez, S, Shirali-Shahreza,M, & Manzuri-Shalmani, M. (2007). Easy and Secure Login by CAPTCHA. International Review on Computers and Software. 2(4), 393-400.

Wood, C. (1996). Constructing difficult-to-guess passwords. Information Management & Computer Security. 4(1), 43-44.

Yardi, S, Feamster, N, & Bruckman, A. (2008). Photo-based authentication using social networks. In Proceedings of the first workshop on Online social networks, pp. 55-60, Seattle, WA, August, 2008.