Protecting Online Social Networks Against Threats

Mahmood K. Ibrahem, Wael A. Abbas

Abstract— Online social network platforms comprise several issues related to the privacy and security of user. This paper aims to develop a security framework which comprises methods to shield Online Social Networks (OSN) against social network threats and preserving the privacy of the user while maintaining balance between security and system performance. This was achieved by using SSL protocol, Captcha implementation in the server, bcrypt password hashing algorithm and account auto-locking mechanism. In addition, various methods have been used to countermeasure web application vulnerabilities. The proposed system has been tested and evaluated under various scenarios including automated program attacks and human based attacks. The evaluation showed that the proposed system is efficient in creating a secure environment for online social networks.

Index Terms— OSN, Privacy, Security, Authentication, Encryption, Web application vulnerabilities.

1 Introduction

THE popularity of OSN is rising. The online societies produced by OSNs considered a rapid growing phenomenon on the web enabled by new modes of social interactions among users from different places around the world. Some OSNs are friendship-focused which basically used for communication, entertainment, and photo/video sharing such as Orkut [1], Facebook [2], and MySpace [3]. On the other hand, OSNs such as XING [4] and LinkedIn [5] are used for professional contacts, where the user discovers business connections [6].

The social networks growth poses a significant threats to users. Attackers can obtain the personal information of the user easily depending on social networks. It is difficult to protect the information by utilizing conventional techniques as the internet is connecting the whole world over this digital network. It is necessary to know the purpose behind the attacks and information theft of the social network sites in order to provide the optimum techniques for protection the information of the user. Attackers might attack to show that they are able to penetrate a secure system, others might attack to obtain control over systems to arrange devices into a Botnet in order to perform Denial of service (DOS) attacks. However, the most popular purpose is the financial profit obtained by collecting important personal information of the user such as passwords, social security number, and bank account. By doing so, attacker commits identity theft crime and generates profit [7].

2 Online Social Networks Issues

2.1 Privacy Issues

Sensitive information such as full name of the user, date of birth, contact information, previous and current work, education background and relationship status attracts attackers. Subsequently, the major issue of a user's profile is the leak of personal information through poor privacy setting or third party application [8].

2.2 Identity Theft Issues

Identity theft refers to stealing user's sensitive information or identity and pretending to be that user or using these information in a malicious way. Profile cloning is a technique of identity theft. In this technique, the attacker takes advantage of trust among friends because users aren't careful when they confirm a friend request. Social phishing is another technique which is used for stealing the identity of the user [8].

2.3 Social Networks Spam

The massive growth in social networks has inspired the spammers to generate unwanted messages which is called SN spam in order to create high traffic load inside SNs. Spammers generally use automated programs (bots) to get access to SNs. Spamming can cause malware spreading, trust loss, traffic overload or difficulties in the web application usage [9].

2.4 Malware Attacks

Malware refers to a malicious software that designed to get access to a computer system without the awareness of the owner. The increased use of OSNs has become the main repository for malicious attacks to spread malware [10]. Malware in OSNs uses the structure of OSN to distribute itself between the user and his friends in OSNs [11]. This software can include viruses, worms and Trojans that can cause undesirable activities on a users computers system i.e. destroying data [10].

2.5 Web Application Vulnerabilities

The lack of proper programming of websites may leads to serious threats like, Cross Site Request Forgery (CSRF), Cross Site Scripting (XSS) and Structured Query Language (SQL) injection attacks that used in stealing sensitive information and the propagation of malware attacks [8].

There are diverse precautions must be taken into account along with the technical solutions. These include increasing the awareness of the users in order to help them differentiate between public and sensitive information. Furthermore, OSN sites must play a major role to protect user's personal information [7].

3 Proposed System Architecture

In order to protect the online social network against the men-

tioned attacks, the system architecture will be divided into multiple components, each component may contain modules or services responsible for different functions provided by the system as shown in Fig. 1. The key components are the privacy component and the security component which contains: Authentication module, encryption module, spamming attack module, phishing attack module, brute force attack module, SQL injection attack module, XSS attack module and CSRF attack module.

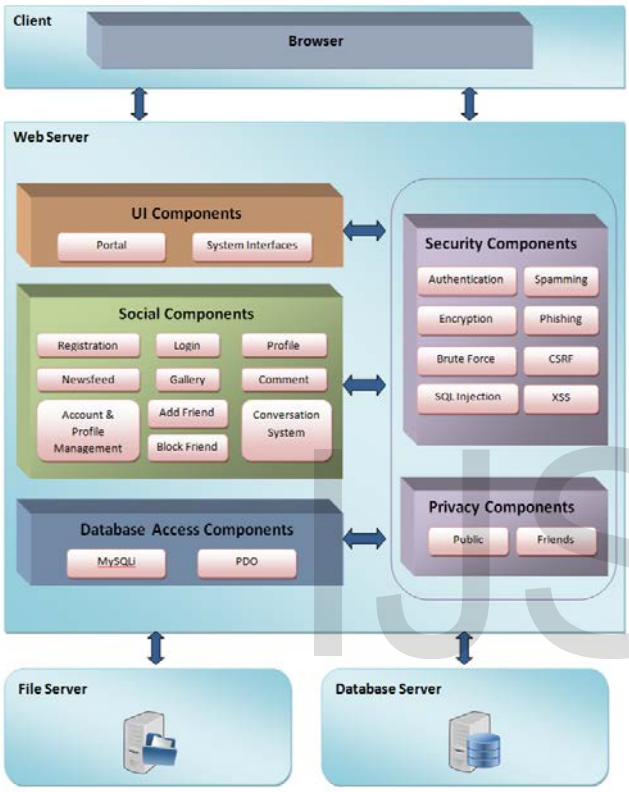

Figure 1: System Model Architecture

3.1 Privacy Module

The privacy of user's information is an important factor in social networks due to the fact that the user may not want to share his/her personal information to the public. To enable users themselves to play a critical role in helping to safeguard their own information, privacy mechanisms are built into the OSN platform. Privacy settings are adjusted and customized according to how users want to share their information. The system provides two levels of privacy for users:

a) Public: with this level user's personal information , gallery ,wall posts and friends list can be viewed by anyone.
b) Friends only: with this level user's personal information , gallery ,wall posts and friends list can only be viewed by the user's friends.

3.2 Authentication Module

The responsibility of this module is to authenticate OSN users before giving them the accessibility to the social network. Password authentication method has been used in the system which is the most commonly used method within OSNs. In order to protect the confidential/sensitive data stored in the database including passwords and security questions answers, a hashing module will be used. This module uses password_hash and password_verify PHP hashing functions that has the following parameters:

- **Hashing algorithm:** determine the type of the hashing algorithm to be used. Bcrypt algorithm has been used to create the hash which is based on blowfish algorithm. The produced hash will always be 60 character string length .
- **Salt:** a random generated data has been used to be concatenated with the password in order to prevent rainbow table attacks and dictionary attacks .
- **Cost factor:** The cost parameter is represented by an integer value between 4 to 31 specifies the iteration count of the algorithm as a power of two. The used cost factor for our system is 10 .

The security of bcrypt algorithm is related to the speed of the algorithm. Bcrypt is very slow, it can take even seconds to generate hash value. That means a brute force attack is hard to be executed, due to the amount of time that it needs. The structure of Bcrypt hash is shown below:

$2a$(2 chars cost)$(22 chars salt)(31 chars hash)

The reason why this algorithm can be expensive and complex is because it runs 2cost times. However, the important part is to maintain a balance between performance and security. Using high cost factor will make it harder for the attacker to launch a brute force attack, but it also can add unnecessary overhead on the server.

3.3 Encryption Module

The responsibility of this module is to encrypt the data streams between clients and the web server in order to protect the confidentiality of information against eavesdropping and forging the contents of the communication. For this case HTTPS protocol has been used and established on the web server. Data sent using HTTPS is secured by (TLS) protocol, that provides three protection layers [12]:

a) Encryption: protect the data from eavesdroppers by encrypting the data exchanged between clients and server. So, nobody can track and listen to users activities or steal the important information like cookies and passwords.
b) Data integrity: ensures the data are not corrupted or altered in any way during transmission.
c) Authentication: proves the identity of the OSN to the users. It protects users against man in the middle attacks (MITM) and provide an indication whether the website is legitimate or not, Hence protect users against phishing attacks.

3.4 Phishing Defense Module

Phishing attacks is a dangerous type of attack used as identity theft attack to steal social network's users credentials and impersonate their identities. This module is responsible for minimizing the risk of phishing attack by identifying the identity of the legitimate website to the user using SSL certificate signed via trusted certificates authority. However, phishing prevention is highly depends on user's awareness by giving him/her an indication whether the visited website is safe or not. The indication is represented by a green padlock icon near the URL with the use of HTTPS protocol. Further precautions should be taken by the user such as not clicking on links supplied by untrusted people and being aware when important credential information is required.

3.5 Spamming Defense Module

Two types of security techniques are proposed as anti-spam registration security level.

a) Email activation strategy for a new user account: this feature helps to prevent spammers from signing up to the system. After a user submits the registration form, an account activation module sends an activation link to that user's email. After the user successfully activated his account, he will be able to login.
b) A robust text based Captcha: Captcha are currently used by a lot of social networks during registration to make sure that users are humans. In order to enhance the strength of the Captcha image against various breaking attacks against the captcha, a text based Captcha algorithm was proposed in which every challenge will associate with basic features all of them dramatically increase the Captcha security. New features such as code length, font type and font size will be produced randomly at every challenge to narrow the chances of predicting the next challenge and that will make the automated techniques for breaking Captcha useless.

3.6 Brute Force Defense Module

Usually when a website requires user authentication it will be a target of brute force attack. Hackers use this attack to gain unauthorized access to the user's profile. So this attack can still be a dangerous threat to the online social network unless proper precautions are taken. Three strategies have been proposed as follows:

a) Enforcement of a strong password policy: this strategy used to defense against targeted attack based on the fact that an attacker will use an automated tool that tries all possible combinations of letters , numbers and special characters. The length of the password must be at least 6 characters (the longer password, the more difficult to be broken by brute force). The password must include letters (uppercase and lowercase) and numbers .
b) Delay strategy: The success rate of the brute force attack highly depends on time. So adding a reasonable delay can greatly slow down the attack. The delay strategy was provided by the password hashing process .The applied hashing algorithm is based on a cost factor (delay factor) which is used to make the hashing process slower and it may take even seconds to produce the hash.
c) Account Lockout after 3 failed attempts: if the server detects that a user has provided an incorrect password attempt three times since his last login for the same email, the server will temporary lock the account and then gives the user another chance to prove his/her identity by displaying a new form acquiring the user to answer his/her security question in order to unlock the account and back again to the login process. However, if a user failed to enter a correct answer for the security question three times, the server will decide that the account is under brute force attack and will lock it for one day.

3.7 SQL Injection Prevention Module

SQL injection attack is considered one of the web vulnerabilities threats directed to data based applications. To protect against SQL injection, the input data must not directly be embedded in SQL statements especially when the data comes from a user. That problem is avoided entirely with prepared statements by making sure that the embedded query doesn't execute at the time of inserting the data and also validating and escaping the user's input data before sending it to the database.

3.8 XSS Prevention Module

XSS, or Cross Site Scripting is another dangerous attack allows the attacker to run malicious script on the vulnerable website from the victim's browser. This attack may leads to compromising user's data, stealing cookies or launching phishing attacks. This module is responsible for preventing XSS vulnerability by sanitizing and validating all user's input data at the client side and the server side. After the sanitization and validation process, the special characters that may present in the user's data will be encoded. Thus, the browser will display these characters as text and doesn't execute it.

3.9 CSRF Prevention Module

CSRF attacks is an exploitation of a particular web site in which the user sends vicious requests that the vulnerable web site will trust without user's knowledge. For OSNs this attack can be used to publish posts, changing user's personal information including profile picture, uploading pictures or any other action that result in dishonoring user's reputation without the user's knowledge. This module is responsible for preventing this attack by using a secure random token (e.g CSRF token). CSRF token is a long random generated value which is difficult to guess. this value will be generated at the beginning of a user session and it will be correlated with this specific user's session. The token will be embedded in every request associated with sensitive server-side operations as a hidden field or inserted directly in Ajax requests. Then, the server will use that token to verify the validity of the user's request.

4 Penetration Testing

In order to test the proposed system security in terms of web application vulnerabilities attacks and proves the effectiveness of the prevention techniques, automated based attacks and human based attacks were conducted to test the security of the system. Different scenarios were performed locally to test the system against SQL injection, XSS and CSRF attacks. For SQL injection attack, sqlmap open source penetration testing tool was used to check the efficiency of the used prevention technique by trying to get access to the database and hack it. While for XSS and CSRF attacks, tests were performed manually by setting up specific testing environments. The testing of the security framework shows that the proposed framework is effective in providing a secure OSN environment against web vulnerabilities threats.

5 System Performance

As mention earlier, Bcrypt is an expensive hashing algorithm which uses a cost factor (n) that defines the algorithm complexity by making the algorithm run 2n rounds. Because password hashing generally associates with frequent tasks such as logging the user into the social network, it's very important to achieve a suitable balance between system's performance and security. Using high cost factor will make it harder for the attacker to launch a brute force attack, but it also can add unnecessary overhead on the server. In order to find the highest cost factor value that system computational power can stand without sacrificing performance, the OSN web server was tested with various cost factors to determine the time it takes to verify a hashed password in the authentication module.

The tested web server has the following specifications in terms of hardware and software : 2 cores CPU, 1GB of RAM and operates on Linux OS . To get more accurate results , the database was filled with 1 thousand random users data to simulate a large number of users and adding extra overhead on the system. Fig. 2 showed that when the cost factor values increases by 1, the time consumed during password verification process will double. The consumed time were ranged from few milliseconds to several seconds. There must be compromises between cost factor value and execution time of the algorithm, so in that case the appropriate consumed time that will add a reasonable unnoticed overhead on the system will be 111.29 ms . That means the correct cost factor that will be used in the system is 10 which provides a good balance between security and performance.

Another test was performed to show the difference between MD5 and Bcrypt hashing algorithms in terms of execution time. Fig. 3 showed that MD5 has execution time of 0.37 ms .That means Bcrypt with the used cost factor 10 is about 300 times slower than MD5.

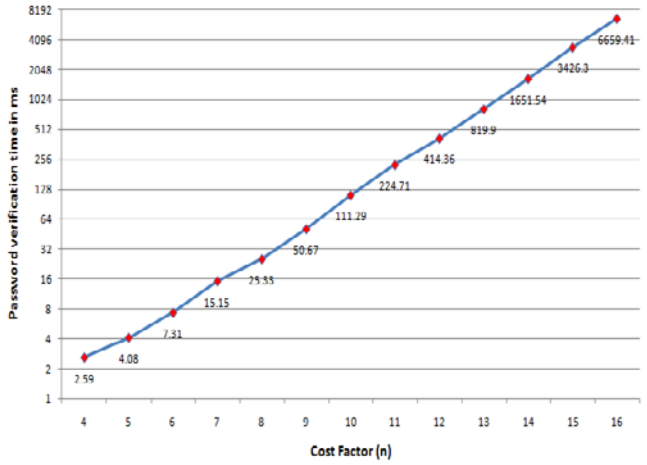

Figure 2: Bcrypt Impact On System Performance

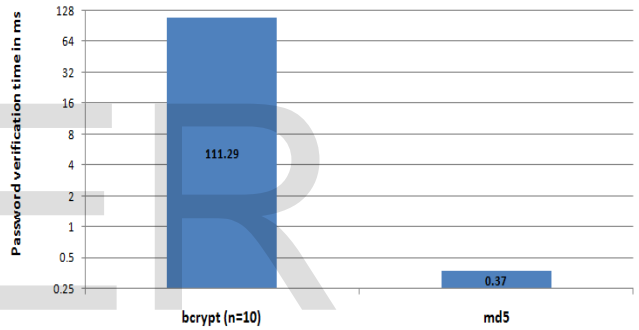

Figure 3: Difference Between Bcrypt and MD5 in Terms of Execution Time

6 Conclusions

Security and privacy are important aspects in online social networks and they became more important as social networks grow. The proposed system enables users to play a critical role in protecting their personal information from unauthorized access by giving them the right to determine what type of information needed to be shared with others and who can view it.
The following conclusions were obtained:

- HTTPS protocol has been implemented in the system to provide the authentication, confidentiality and integrity. The SSL certificate verifies the server's identity and thus minimizes the threat of phishing attacks. However, phishing prevention highly depends on user's precautions like verifying the legitimacy of the certificate and checking any warnings displayed by the browser before proceeding .
- Limiting the number of failed login attempts and providing strong password policy which have been implemented in the proposed system play an important role in preventing attackers from brute forcing

and accessing the system in unauthorized way.

- Using Bcrypt instead of MD5 for hashing user's passwords and security answers makes the system more secure against brute force attack because the computation time of Bcrypt is longer compared to MD5, and hence it is more difficult to break with brute force than MD5.
- Increasing the complexity (cost factor) of Bcrypt hashing algorithm results in more secure hash but it will also increase the computation time of the algorithm exponentially and add extra overhead on the server. Thus, choosing the right complexity (cost factor) value for Bcrypt is essential in making balance between security and performance and providing smooth experience for the user.

REFERENCES

[1] Orkut [offline]. http://www.orkut.com
[2] Facebook [online]. Available: http://www.facebook.com
[3] MySpace [online]. Available: http://www.myspace.com
[4] XING [online]. Available: http://www.xing.com
[5] LinkedIn [online]. Available: http://www.linkedin.com
[6] A. Makridakis, E. Athanasopoulos, S. Antonatos, D. Antoniades, S. Ioannidis, and E. P. Markatos, "Understanding the behavior of malicious applications in social networks", IEEE Network, Vol. 24 , No. 5, pp: 14 - 19, 2010.
[7] R. Ajami, N. Ramadan, N. Mohamed, and J. Al Jaroodi, "Security Challenges and Approaches in Online Social Networks: A Survey", International Journal of Computer Science and Network Security (IJCSNS), Vol. 11, No .8, 2011.
[8] D. Gunatilaka, "A Survey of Privacy and Security Issues in Social Networks", Student Survey Paper, Washington University, Department of Computer Science & Engineering, 2011.
[9] A. Al Hasib, "Threats of Online Social Networks", International Journal of Computer Science and Network Security (IJCSNS), Vol. 9, No. 11, 2009.
[10] V. Vanheuangdy, "Security Threats of Web 2.0 and Social Networking Sites", Research Report for ACC 626, 2010.
[11] M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions", IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, 2014.
[12] W. Stallings, "Cryptography And Network Security Principles And Practice", Fifth Edition, Prentice Hall, 2011.

Author's Details:

Mahmood K. Ibrahem and Wael A. Abbas
College of Information Engineering/ Department of Networks Engineering and Internet Technology
Al-Nahrain University/ Baghdad-Iraq
mahmoodkhalel@coie.nahrainuniv.edu.iq
waelnumb2012@gmail.com