International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Secure Authentication and Cyber Crime Mitigation for Social Networking Sites

Anjitha T[1], Harsha V[2]

[1, 2]Cochin University, College of Engineering Kallooppara, Kerala, India

Abstract: ***With the advent of online social networking sites, its usage has grown dramatically, now rivaling search engines as the most visited Internet sites. Even though these OSNs offer attractive means for digital social interactions and data sharing, they raise a number of cyber issues on security and privacy. Usually OSNs allow users to restrict access shared data but there had not been any mechanism to enforce security and privacy concerns over data associated with multiple users. One of the main issues in today's OSNs is to give users the ability with which they can control the messages posted on their private space to avoid displaying of unwanted contents. The proposed framework creates firewall in network security. It gives close wall security while accessing the Social Network sites. It also enables the protection of shared data with multi users virtual environment in OSNs. And it also allows OSN users to have a direct control on the messages posted on their walls and a secured login method is provided to avoid cyber attacks like hacking, Phishing and Social Engineering. These are achieved by using RSA Algorithm.***

Keywords: Social Networking Sites, Hacking, Phishing, Security and Privacy risks, RSA algorithm

1. Introduction

A social networking service (also social networking site or SNS) is a platform to initiate social relations among people who share similar interests, activities, backgrounds or real-life connections. Existence of large number of compromise machines on the internet is a real threat for these sites. Such machines are used to launch various security attacks including spamming and spreading malware, DDoS, and identity theft.

A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, plus web pages, where users and friends can post content and send messages. A user profile usually includes information regarding the user's birthday, gender, interests, education and employment history, and contact information. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in user's spaces, they do not have control over data residing outside their spaces. In the case of Facebook, it allows users to state who is allowed to insert messages in their walls. Here no content based preferences are supported and therefore it is not possible to prevent unwanted messages, no matter of the user who posts those.

The reason why cyber-conspirators prey on these networks is because users upload their personal information that commonly include their interests, social relationships, pictures, confidential information and other media content, and share this information to the whole world through SNSs which are very easily accessible. The platform openness feature that users use to share same applications, results in installing the application which is malicious and infected. Attackers use this characteristic to manipulate that user to act as antisocial against all the internet users which are connected to the victim user. They often lure users into clicking on specific malicious links. As a result of the larger user base and large amount of information available in social networks, it has become a potential channel for attackers and criminals to exploit.

The posted content can be re-distributed by the viewers, and eventually the content can be shared with unintended users who were not explicitly allowed to view that content. Such open sharing availability of social networking sites exposes the users to a number of privacy risks. Thus OSNs are suffered by various security and privacy attack. In this paper, I propose an idea to overcome the issues with content preference and security policies.

2. Literature Survey

A design which authenticates and uniquely identifies each internet user especially users on social networks is proposed by Adu Michael K. A system that enables internet users' activities to be monitored in order to control threats to online social networks in Nigeria is offered. If users suspect any of their associate, they can send a request on social networks to get confirmation on genuine identity of the individual. Mitigating Cyber crime and online social Networks Threats in Nigeria written by Adu Michael K.

A framework called Secure Social Aware (SSA) by Aaron Beach allows for the interaction of social network information with real-world location-based services without compromising user privacy and security. Secure Social Aware: A Security Framework for Mobile Social Networking Applications by Aaron Beach.

Regarding cyber attacks through social networking platforms Sarah Ackerman focuses on: Process (steps and methods used to carry out cyber attacks), Effect (Possible consequences of a cyber attack to a company), Safeguard (Includes methods used to limit cyber attacks and identify possible threats). Social Media as a vectorfor cyber crime by Sarah AckermanWajeb Gharibi investigates and studies the cyber threats in social networking websites. The author goes through the amassing history of online social websites,

classify their types and also discuss cyber threats, suggest anti-threats mechanisms and visualize the future trends of such hoppy popular websites. Cyber Threats in Social Networking Websites by Wajeb Gharibi and Maha Shaabi": Wajeb Gharibi Dharmendra Singh has listed which all vulnerabilities were exploited for executing these attacks and their effects on these systems and social networks. The focus is mainly on the vulnerabilities that are used in OSNs as the convertors which convert the social network into antisocial network creating a consecutive chain of attacks on increasing number of social networking users by inducing further network attacks on the users associated with the victim user. Vulnerabilities and Attacks Targeting Social Networks and Industrial Control Systems by Dharmendra Singh, Rakhi Sinha, Pawan Songara and Dr. Rakesh Rathi.

3. Attempts to Solve Cyber Attacks

Online social network users are facing prevalent and varied security and privacy threats. There are many software solutions and techniques today which have been put in place to assist OSN users in defending themselves against these threats. Many cybercrime attacks can be avoided in a cost-effective manner when armed with a little technical advice and common sense. Basic ways that cybercrime can be prevented are as follows [1]:

- Keep computer system up-to-date
- Secure configuration of the system
- Choose a strong password and protect it
- Keep firewall turned on
- Install or update antivirus software
- Protect personal information
- Read the fine print on website privacy policies
- Remove unnecessary personal information:
- Adjust privacy and Security Setting
- Do not Accept Friend Requests from Strangers.
- Do Not Trust Your OSN Friends

4. Proposed Method

In the proposed method, whenever users login to their account, it verifies the login id and performs graphical image authentication. It provides a unique key to users when they need to access features like chat, post, comment and video chat. Thus it provides secure login and secure access to different features in proposed application.

4.1 Registration Module

In this phase, the client requester is authenticated by registering oneself in the authentication server. At the time of registration, the user provides his personal data such as name, email, address, gender, birth date, login etc. Also user needs to arrange a set of random images in an order. After completing the registration, the user will be able to login to the website by entering login id and Graphical image authentication. Then the user will be able to login to their profile page. Thus secure registration is provided using this phase.

4.2 Key Generation Module

In this phase, a Graphical User Key is generated during the registration phase which needs to be arranged by the user in any order. Once the registration is completed a unique key is generated for each user. And whenever the user tries to login to the website the key generator provides the Graphical image authentication in random order every time and the user needs to arrange the images in the same order which they arranged during registration. If the answers are correct, key generator generates the unique key immediately to access the features in the application.

4.3 Authentication Module

In this phase, the Authentication Server authenticates the user during the registration phase. Two factor authentication is followed such as graphical image authentication and security authentication. Once the registration is successful and if the user try to login to the website, user needs to provide the correct login and Graphical image authentication.

5. System Components

5.1 Client Requester

The client (i.e, student, staff, others) makes request to Authentication Server (AS) for registration over the internet. Once the registration process is completed, the AS generates a unique key for the client and save all the client details in the database manager. The client is expected to provide correct answers for the security authentication during login in order to get the unique key to access any features in the server.

5.2 Communication Manager

Between the client and server the Communication Manager (CM) acts as a communication medium. It transfers the client request to the server and server response to the client. Public Key Infrastructure mechanisms are used to secure the requester interfaces.

5.3 Authentication Server

All registered clients are recorded in the Authentication Server (AS). The authentication of the client is done by the authentication server by matching the images in proper order with the order of the images stored in the Data Base. AS establishes connection with Data Base Manager after authentication for retrieving user's details. The information flow on the network is secured by encrypting and decrypting the message. The Authentication Server setup consists of a Key Generator, Image Matcher and Data Base Manager.

5.4 Key Generator

The Key Generator (KG) generates a unique key for every client once the authentication is given to the user. It stores the unique key in the Data Base Manager inside the server. The key is encrypted using RSA algorithm for security reasons.

5.5 Database Manager

The Data Base Manager (DBM) stores all the client details along with their security unique key. The profile information of every user is stored in the database. It contains Image Matcher (a set of images) for verification of Graphical image authentication. All data inside the Data Base Manager is in encrypted form.

5.6 Image Matcher

The Image Matcher (IM) verifies the Graphical image authentication. It matches the image order selected by the client to the image order stored in the Data Base. If the order matches, it indicates to the server to give authentication to the client else server displays an error message to the client. The images inside the Image Matcher are stored in encrypted form.

6. Result

In this paper, the proposed framework for social networking applications will be able to provide more security and privacy for OSN users from major cyber attacks. This is achieved with secure authentication by the generation of the unique key for securing login process and another step of Graphical Image Authentication

7. Conclusions

The emerging cyber attacks are becoming more sophisticated and technically advanced that their prevention and detection occurs at a slower phase than that needed. Phishing sites that elicit users into clicking on malicious links thereby stealing login credentials and financial data, adwares that outsource private information from users system, Spams, Malwares which are escalating in social networking sites need to be controlled in a well manner. It is noticed that average OSN users find it difficult in understanding the simple privacy settings provided by today OSNs. Given the emerging threats of social networking usage I hence explored mitigation strategies for these attacks.

In this paper, I have presented a new method to provide a unique key to each users in order to make the login process more secured. Also data are encrypted using the RSA algorithm. And a secure authentication is provided to the users by generating a unique key and a Graphical image authentication. The proposed application provides more security and privacy to the OSNs users. Two level authentication is done to provide secure login to the users in encrypted form.

References

[1] Adu Michael K, Alese Boniface K and Adewale Olumide S," Mitigating Cybercrime and online social Networks Threats in Nigeria" Proceedings of the World Congress on Engineering and Computer Science 2014 Vol I.

[2] Aaron Beach, Mike Gartrell, Baishakhi Ray, Richard Han," Secure Social Aware: A Security Framework for Mobile Social Networking Applications," in Proc. IEEE International Conf. on 2012, pp. 439-446.

[3] Sarah Ackerman, Kyle Schutt, "Social Media as a vector for cyber crime"in Proc of Clark Schaefer Consulting, 2015.

[4] Wajeb Gharibi, Maha Shabi, "Cyber Threats in Social Networking Websites",in Proc of International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[5] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D.Starin," Persona: An online social network with user-defined privacy," in Proc. of ACM SIGCOMM Computer Communication Review, 2009, pp. 135–146.

[6] K. Strater and H. Richter, "Examining Privacy and Disclosure in a Social Networking Community," in Proc. 3rd Symp. Usable Privacy and Security (SOUPS "07), 2007, pp. 157-158.

[7] Dharmendra Singh, Rakhi Sinha, Pawan Songara, Dr. Rakesh Rathi, "Vulnerabilities and Attacks Targeting Social Networks and Industrial Control Systems" in Proc of International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

Author Profile

Anjitha T obtained the Degree of Bachelor of Technology in Computer Science and Engineering from College of Engineering, Chengannur in 2014. She is now pursuing her master degree in Computer Science with specialization in Cyber Forensics and Information Security at College of Engineering, Kallooppara under Cochin University of Science and Technology.

Harsha V obtained B.Tech in Computer Science and Engineering from SHM College of Engineering and M.Tech in Computer and Information Science from Cochin University. She is currently working as Assistant Professor in College of Engineering, Kallooppara.