THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

A Literature Survey on Analysis of Social Network Security System

Vivek Kumar Sinha[1], Divya Anand[2], Aman Singh[2]
[1]Research Scholar, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.
[2]Asst. Professor, School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India.

Abstract

Social networking sites are available for customers to interact upon chat-based services (CBS), which is now a days one of the fastest and most popular means of communication taking place between two people around the world. In social networking most of the users are unaware of their friends, they just accept friend requests to achieve popularity. An interaction pattern for social network systems should be based upon the analysis of communication between the community within the group and outside the group. Moreover, users sharing their personal information can be used for bad cause by hackers or mid-man attackers. This information should be confidential and can be used to solve the authentication problem by a) unique password, i.e., one-time password (OTP) for two-phase authentication (2PA) to resolve secret information related problems before providing personal identities to any person b) Question/Answer mechanism for last five activities. These days, social networking applications are not limited to desktop, but it has enhanced upto mobile ones which enable a user to interact anywhere, anytime but the establishment of individual data on SNS has been a dangerous and important topic for social web. We are proposing a new technique to resolve this issue by implementing various mechanisms. Ultimately, we are focusing on privacy protection, preservation on specified parameters. We are more emphasized on identifying, securing, protecting, corroboration and establishment of individual data on SNS which is becoming an important issue for social web these days.

Keywords: Social network security; access control mechanism; preventive, detective and corrective control; high, medium & low, social network sites, privacy protection.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

1. Introduction

These days the use of social networking websites has increased. The customers are utilizing the chat apps for various purposes like to get access to networks and to provide services to their customers. Netnography provides special methods to communicate between various dating applications. People from near or far places can communicate with each other [1]. These days social networking sites are widely being used to relieve stress created from the hectic schedules of most of the people engaged in different activities like study, jobs, and family etc. Firstly, the time frame in today's scenario is quite reduced and we have very less time to connect socially with people. Secondly, most people experience a very limited social circle. The social network platform allows the user to interact and share knowledge with each other over the internet [2]. The social network platform allows a user to perform social activities like send/receive the messages, respond to queries, provide a view, like or dislike activities. In the past, traditional login/password authentication mechanism has been used which is not sufficiently secure for now, as many security-critical applications are developed. The Two-phase authentication system (2PA) is developed which can provide an extended level of protection by enhancing the authentication PA (a Smartphone) [3].

1.1 Mobile Social Networking

The work is conducted on real-time access control mechanisms and networking as per the requirement of social network security. These days, the things like data security and related services are the most significant and sound requirements to any data moving through the internet. According to the review done on this, we can define the information security as a set of processes, procedures, policies, personnel with property to prevent, detect, improve and revival from illegal or adaptation, disclosure or usage of information [4].

1.2 Social Network Architecture

The social network architecture comprises of a mobile user, desktop and other cellular devices. This architecture have a certain geographical area, a centralized server connected to a wireless network or cellular network through the base station and

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

local servers deployed in the local area. Wireless devices like mobile devices, tablets, and other cellular devices are connected to the local server and interact with the global server through a wifi / cellular network or some communicate directly with the nearby users. Otherwise, few link up with chatting based applications through login mechanism and interact with the desired user.

1.3 Characteristics of Social Network

The principal objective of social network is to enhance social circle and to increase the interaction within the large groups. The various characteristics shown by the social network are:

- User mobility
- Resource limitation
- Profile management
- Protection vulnerability
- Centralized control

1.4 Introduction to Netnography

- The word ‘Netnography’ is the combination of ‘Internet’ and ‘ethnography’.
- Netnography allows the persons to reveal or hide their identity, even his/her presence, but it's not possible in the ethnography.
- It is the collection of both the information on groups of involvement as well as the written description of the study of those groups.
- The importance of online communication has grown.
- Netnography may not be necessarily involved in full disclosure in terms of the researcher’s identity or intent [5].
- Some researchers reveal the identity and design of study after the research is finished.
- Correspond with members to validate the interpretation of reflections.

1.5 Location-based Application

- Location-aware networking.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

- Live up to the multiple demands of an advanced society.
- To solve complex technology problems, heterogeneous networking & sophisticated society.
- Increasing the uncertainty, unorder, unsafety by unauthorized users & hackers.

1.6 Challenges on Social Network

The increasing number of networking sites, resources and technologies gives rise to the increase in uncertainty, unorderness, unsafety and unauthorized access in different social networking [6]. The challenges faced in the social network comprises of the following:

- Client Site Security
- Server Site Security
- Security during Transmission

1.7 Suggested Protection Methodology

The trust model improves the reliability of communication and trustworthiness between two users, whether they are in the same group of a network or in different groups at different location. This method also provide the protection against mid man attacks. It is to reward the safe behavior; and block and report bad behavior over time. A general picture arises that how a user is trusted, and it allows to obtain more quality services depending on it. Detecting Sybil user through social network analysis provides a key role in enhancing the safeguard methodology which provides the solutions to current problems.

2. Literature Review

Now a days, there are lots of procedures available for encrypting SMS content which mainly employs discrete factorization and logarithms [6]. To provide a solution to the existing issue of authentication and cryptography based problems, we will employ the post-quantum cryptography technique that provides a priori resistant to the quantum computer. Thus, here we will work on the security of transmitting privilged

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

information such as SMS OTP on the unauthenticated public means of channel. We will then further proceed with an OTP based SMS encryption mechanism with a quasi-cyclic mdpc version of the MC-Ellice system crypto and also an electronic signature of outputs based on elliptic crossovers (ECDSA).

Social Network Architecture

The users have a certain geographical area, a centralized server either connected to a wireless network or cellular network through the base station; and local servers deployed in the that area [7]. Wireless devices like mobile devices, tablets, and other cellular devices which connects to the local server and interacts with the global server through a wifi/cellular network or some communicate directly with nearby users [8]. A social network is an aggregation of three nodes, i.e., one node from one community can communicate with other communities within the group, outside the group and within the group with a connected node from outside the group [9]. One of the scenario is illustrated in figure 1.

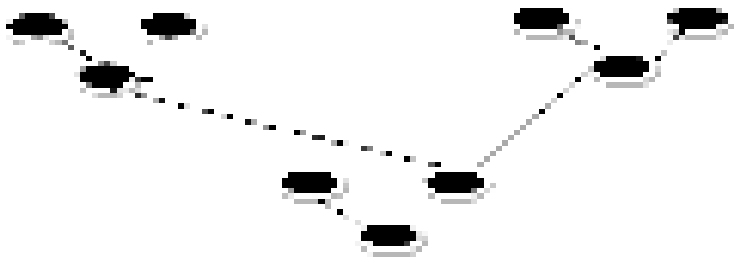

Figure 1 Interaction among communication between Social Group

Attack on Devices in 2PA based on SMS OTP

- An attack can be avoided with two-factor authentication systems and it also affects the Internet by developing browser rootkit which will be able to perform an automated approach to retrieve confidential client data **[10, 11]**.
- Online banking service is an example in which TAN solutions sent via SMS is used. The attack scenario which is presented here is quite simple to eliminate the challenge of cross-platform infection **[12, 13]**.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Security of 2PA based on SMS OTP

- The encipherment of SMS was proposed by employing classical cryptography technique, with the encryption algorithm of César and Vigenere combined [14].
- The encoding of SMS depending upon the chaotic encryption was proposed by using a new cryptography technique [15].
- In the same perspective, others ensures the authenticity of SMS messages by implementing the MNTRU algorithm [16, 17].
- Other SMS security features have been set up to provide a solution to the confidentiality and integrity of SMS information [18].

3. Conclusion

Millions of people are using social networking websites as an important application, the current work provides a new direction to the analysis of networking sites. Starting from the already existing mechanisms, all the fundamental security issues related to the mid man attack between one client and the other client are discovered. The security-related issues in the industries are discovered which requires direct access to those companies that own, publish and develop the apps. The valid mPass for the allotted SMS recovery on the client machine through malicious code is also generated. However, to avoid attacks, we have to improve the existing system security services to optimal. Indeed, we propose a 2PA system which implements the cryptographic technique and it allows us to ensure the confidentiality in chat based services and it completely avoids the authenticate problem by restricting the mid man attacks. Hence, the security analysis of our proposed system demonstrates how we are able to resist attacks with the implementation of the quantum machine today.

References

[1] A. Bengry-Howell, R. Wiles, M. Nind and G. Crow, “A review of the academic impact of three methodological innovations: Netnography, child-led research and creative research methods”, E.S.R.C. Economic and Social Research Council, 2011.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[2] P. Schartner, S. Burger, ”Attacking mTAN-Applications like e-Banking, and mobile Signatures”, University of Klangenfurt, 2011.

[3] E. J. Finkel, P. W. Eastwick, B. R. Karney, H. T. Reis, and S. S. SAGE, “Online Dating: A Critical Analysis From the Perspective of Psychological Science:, Psychological Science in the Public Interest, 2012.

[4] S., Rangarajan, N. S. Ram, N. V. Krishna, “Securing SMS using Cryptography”, International Journal of Computer Science and Information Technologies (IJCSIT), pp. 285-288, 2013.

[5] M. Bart, V. K. Kannan, H. Stockinger, “A review and analysis of literature on netnography research”, Int. J. Technology Marketing, Vol. 11, No. 2, 2016.

[6] Y. Park, “Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks”, Sensors”, Vol. 16, no. 12, 2016.

[7] M., Abo-Zahhad, S. M. Ahmed, and S. N. Abbas, “A new multi-level approach to EEG based human authentication using eye blinking”. Pattern Recognition Letters, Vol. 82, pp. 216–225, 2016.

[8] M. Khamis, R. Hasholzner, A. Bulling and F. Alt, ”GTmoPass: two-PActor authentication on public displays using gaze-touch passwords and personal mobile devices”, Proceedings of the 6th ACM International Symposium on Pervasive Displays, 2017.

[9] Q. Hu, and F. Luo, “Review of Secure Communication Approaches for In-Vehicle Network”, International Journal of Automotive Technology, 2018

[10] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, “How to Attack Two-Factor Authentication Internet Banking”, International Conference on Financial Cryptography and Data Security, pp. 322–328, 2013.

[11] S. Boonkrongs “Internet Banking Login with Multi-Factor Authentication”, KSII Transactions on Internet and Information Systems, 2017.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[12] S. Rangarajan, N. S. Ram, N. V. Krishna, "Securing SMS using Cryptography", 2013.

[13] S. Jha, U. Dutta, "Review on SMS Encryption using MNTRU Algorithms on Android", 2015.

[14] F. Yuan, G.-Y. Wang, & B. Cai, Android SMS encryption system based on chaos, IEEE 16th International Conference on Communication Technology (ICCT), 2015.

[15] S. Jha, U. Dutta, "Review on SMS Encryption using MNTRU Algorithms on Android", International Journal of Computer Science and Information Technologies, Vol. 6, No. 4, pp. 3855-3858, 2015.

[16] V. Verma, R. Kumar, "A Unique Approach to Multimedia Based Dynamic Symmetric Key Cryptography", 2014.

[17] I. Ibekwe, S. Aljareh, "SMS Security: Highlighting Its Vulnerabilities & Techniques Towards Developing a Solution", Proceedings of the 13th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting 2012.

[18] K. Albury and P. Byron, "Queering sexting and sexualisation", SAGE Journals, Vol. 153, No. 1, 138-147, 2014.