Online social networks threats

Hamza Ahmed

Abstract: (SNSs) Social Networking Sites or online social networks are the most outstanding technological phenomena in the twenty first century. These are the most visited sites globally with an informal but comprehensive management tools. SRNs are also used for commercial purposes for instance, MySpace, LinkedIn, Facebook and Twitter. In this study, various aspects of network, social and physical security associated with online social networks sites have been discussed beginning with the introduction of the mechanisms related to each threat and the summaries of relevant solutions that can be adopted to solve these issues amicably (Wang et al., 2009). Each mode of online threat comes with different risks, therefore, relevant measures can be taken to prevent or solve issues related to them. These measures have been discussed into details with examples mentioned at each end. However, it is recognized that individuals and organizations have a legitimate personal and financial uses for online social network, at the same time it's recommended that certain measures should be taken to reinforce stronger users' awareness with more secure network and software designs (Novak et al., 2013).

Keywords: Facebook, social network security, twitter, LinkedIn, firewall, identity hijacking, phishing, sniffers, keyloggers, DoS attack, Virus dissemination, worms, Spoofing, Net extortion, malware and cooperate security

Research Questions: In this study, several research questions were obtained as follows: what are the threats that affect online network sites? How do they interrupt normal user conversations? Who are the most affected when it comes to online social network threats? How can one identify online network threats? How many individuals or companies can be affected at the same time or at intervals, who can pose such threats? What are the objectives of online social network threats? When one is involved in posing threat? What are the penalties? What are the possible solutions that can be implored in case and individual or a company is affected? Who are vulnerable? In the normal operation of social network, is it possible to prevent any attack or possible threats from taking place (Johnson, 2014)? These research questions helps in understanding the objective of this research and the details entailed in this paper.

However, this study does not stop at research questions; it elaborates the intention of the whole research paper with recommendations and conclusions. The research questions have been obtained from online literature reviews with references made from different writers having similar or different opinions in order to find the facts and compile the same for study purposes.

———————————— ◆ ————————————

Introduction

Having noted that online social network have become so popular across the world, many users with different intentions use it to pass information from one end to another. Users may include; financial institutions such as banks, pharmaceutical companies, government and defense agencies, multinational corporations, contractors of government agencies, internet service providers, students, teachers, researchers, bloggers and media (Minchev et al., 2013). All those who have been mentioned above are also vulnerable to social network threats that are experienced through the internet. These threats include (Fossi, 2010); phishing, spoofing, worm, child pornography, net extortion, virus dissemination, computer vandalism, DoS attack and malware. These threats are passed through the internet from one server to the other provided an individual or company is connected to the internet (Hasib, 2008).

Hackers use different tools to aid their intentions of hijacking network communications. These tools include but not limited to keyloggers and sniffers (Fewer et al., 2008). These tools can be used to send spam mails, install viruses, send messages and retrieve data from any given website (Novak et al., 2013). Currently, Many employers hire their employees following their behaviour on social network since much information is relayed on their profiles such as photos, gender, sexual orientation, phone numbers, games, interests, favorite music, languages, types of friends and associates are all checked before employment letter is sent to them (Fewer et al., 2008). With the information at their reach, it is very possible to breach into someone's profile without his/her knowledge. Privacy and information security is at risk if in case such kinds of activities are carried by un-authorized persons or group for any benefit or interest.

Security Threats

Phishing

Under this attack, the hacker masquerades as a reliable entity in order to get someone's credentials or private information over the internet for personal benefit. It is easy to copy someone's legitimate website or profile for malicious reasons. it is a fact that phishing is the second most effective threat after spam when it comes to compromising systems and PCs where hackers are able to index someone's credentials based on different dimensions (Enisa, 2007). To stop phishing, password encapsulation or in simple words, changing one's password with complex letters frequently would help to prevent phishing. Also, using many defaults IP addresses for a single PC.

Malware

Currently, about 60,000 to 80,000 number of malwares is reported monthly (Rand, 2007). Malwares are sent by a hacker in order to collapse the system or damage files of the intended recipient. The often come in terms of adds that cannot be easily detected by many users. The most prominent solution is to train users not to trust every link or site or photos that look attractive and downloading un-licensed software from the internet (Enisa, 2007).

Attack Sophistication

Most companies have placed resources online in their websites for marketing purposes and winning more customers. Most attackers come from the back end where many transactions are taking place. DNS servers and DoS vectors abuse are common over the internet. Worms can compromise over 2 million PCs or systems at the same time for instance worms such as Conficker always attack websites that are not protected with a company firewall or internal server settings (Becker et al., 2009). To prevent such an attack, companies should adopt sophisticated firewalls that cannot be broken often by attackers.

Conclusion

With several online social network attacks being report, many users are at high risk of being victims of the same. Privacy and security of data and information is important to the development of new systems that facilitate these ambitions. With current technologies such as; cloud, mobile devices, network perimeter and system level are used to prevent any possible attacks and provide solutions to these threats. Attacks such as spoofing can be controlled when network IP are set to defaults in order to hide user identity from possible hackers since it takes the form of man-in-the-middle attack. Users are also advised not to put all their vital information on social media where it can be easily compromised without their prior knowledge. Proper authentication and access control is very vital for companies and individuals who use social networks for marketing, social and communication purposes. Users should also ensure their anti-virus programs are up to date in order to scan the entire system frequently. They should also avoid opening attachments any how or sites that look attractive with un-necessary pop-ups that may end up being traps set by hackers. Moreover, users should change their passwords frequently to avoid being trapped by hackers (Rand, 2007). At time, they can use sophisticated passwords that they are able to remember.

References

Beach, A., Gartrell, M., Han, R. (2009). Solutions to Security and Privacy Issues in Mobile Social Networking. Available at: < http://www.cs.colorado.edu/~rhan/Papers/smw09_solutions_security_privacy.pdf>

Becker, J., Chen, H. (2009). Measuring Privacy Risk in Online Social Networks. Available at: < http://web.cs.ucdavis.edu/~hchen/paper/w2sp2009.pdf >

Enisa, G.H. (2007). Security Issues and Recommendations for Online Social Networks. Available at: < http://fredstutzman.com/papers/ENISA2007.pdf>

Fewer, D., Lawson, P., Gosselin, M (2008). Online Privacy Threats: A review and analysis of current threats. Available at: < https://cippic.ca/sites/default/files/publications/CIPPIC-Online_Privacy_Threats-Final.pdf >

Fossi, M. (2010). Online Threats: What Government needs to know? Available at: < http://www.summitconnects.com/Articles_Columns/PDF_Documents/201011/Nov10_vol13_i7_05.pdf>

Hasib, A.A. (2008). Threats of Online Social Networks. Available at: <

http://www.cse.hut.fi/en/publications/B/1/papers/Hasib_final.pdf>

Johnson, M. (2014). Cybercrime: Threats and Solutions. Available at: < http://www.ark-group.com/Downloads/Cybercrime-Threats-and-Solutions-Sample1.pdf>

Minchev, Z., Petkova, M. (2013). Information Processes and threats in social networks. A case study. Available at: < http://www.syssec-project.eu/m/page-media/3/minchev-social-threats.pdf>

Novak, E., Li, Q. (2013). A Survey of Security and Privacy in Online Social Networks. Available at: < http://www.cs.wm.edu/~liqun/paper/tr12-2.pdf>

Rand, D. (2007). CSIS Security Research and Intelligence: Threats when using Online Social Networks. Available at: < http://www.csis.dk/downloads/LinkedIn.pdf>

Wang, E., Jain, R. (2009). Social Network Security: A Brief Overview of Risks and Solutions. Available at: < http://www.cse.wustl.edu/~jain/cse571-09/ftp/social.pdf>