Social and security influence of social networks

Utkarsh Kaushik

Student, Computer Engineering Department

Poornima College of Engineering, Jaipur.

2020pcecsutkarsh191@poornima.org

Prachi Khandelwal

Student, Computer Engineering Department

Poornima College of Engineering, Jaipur.

2020pcecsprachi119@poornima.org

Siddharth Kothari Sanya Gupta

Student, Computer Engineering Department Student, Computer Engineering Department

Poornima College of Engineering, Jaipur. Poornima College of Engineering, Jaipur.

[2020pcecssiddharth181@poornima.org](mailto:2020pcecstushar181@poornima.org) 2020pcecssanya120@poornima.org

**ABSTRACT**

Cyber Security plays an important role in the field of information technology. A brief history and the concept of social networking will be introduced. Many of the security risks associated with using social media are presented. Also, the issue of privacy and how it relates to security are described. Based on these discussions, some solutions to improve a user’s privacy and security on social networks will be suggested.

**INTRODUCTION**

Social networks have caused a revolution in the way how users e particularly teenagers e share information about themselves and others. Information security is very important these days to anyone using a computer or to any organization that employs computers and networking in their day to day operations. That is nearly everyone. Information security should be at the forefront of everyone’s mind since so much of our personal information is out there on the Internet. Confidentiality deals with making sure only authorized people have access to the information. Integrity deals with making sure that the information is not tampered with or corrupted in any way. And finally, availability is just making sure the information can be accessed and where it is supposed to be. social networks as modern communication medium that can be misused by techniques of social engineering.

**LITERATURE REVIEW**

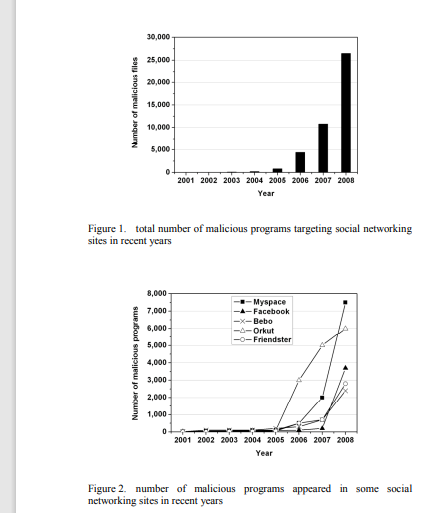
Social networks, as virtual communication medium, serve for communication among users, sharing multimedia data, keeping in touch or fun. Once logged into one of these networks, participants are asked to create a profile to represent themselves digitally. The aim of socio-technical attacks is usually to steal or misuse information, which are not supposed to be public, namely for the purpose of financial profit or to discredit person, company or institution. In recent times these information are highly valued, therefore we expect that market with such private information will grow up. Many companies and organizations that are just working with day to day data are taking all precautions to prevent hackers from causing attacks and data breaches, using firewalls, intrusion detection and prevention systems, honey pots, and appropriate training and policy enacted by their security managers. While social networks offer tools to protect information, these tools are generally not sufficiently understood by the average social network user. Their default configuration also tends to be set on

making information public, and is seldom changed by the users. Because social networks are a recent phenomenon, there are no existing, clear social conventions about their use d for example, whether it is considered acceptable to ignore friend requests on a social network? Many users will automatically accept such, so that even information that is marked as private on their profile, becomes accessible to an unwieldy number of other users. Other users consider the number of friends as a status symbol, effectively causing the boundaries between private life and professional life to become increasingly blurred. Enabling social interactions among individuals is a critical requirement for many network applications. Boosted by the availability of ubiquitous connectivity, the internet is even more an internet of people (IOP), rather than a simple internetwork of hosts (Zhang et al., 2011). This paradigm has also accounted for the huge success of Web 2.0, which enables to create and share contents with an increased degree of social connectivity. Although, such features were already present in the original web vision. Specifically, the Social Web Incubator Group within the World Wide Web Consortium (W3C) put effort in the definition of a social web, where “people can create networks of relationships overlapped with the entire web, while controlling their own privacy and data” . Unfortunately, as today, social services are not based on standardised architectures. Rather, they are implemented by ad hoc frameworks that are becoming real cultural phenomena. The fact, we find very interesting, is that people are willing to provide their information via social networks to anyone rather effortlessly. In case of using the other kinds of communication (i.e. personal, via email or phone) it is proved that much more effort to obtain the same information is needed.

**ATTACKS ON SOCIAL NETWORKS**

In 2005 Sammy worm attacked MySpace and this represented the danger in social networks. Sammy utilized the loopholes in MySpace and spread very fast. Though Sammy did not filch users 'information, it still had seriously affected the normal operation of MySpace. In April 2009 Mikeyy worm attacked Twitter and modified the users’ pages with some useless message. Mikeyy did not filth the personal information just like Sammy. Unfortunately in May 2009 Koobface worm spread in Facebook and filched the important personal information such as password. Later Koobface began to spread in other social networking sites and a greater harm was brought. Obviously attackers have found that social networks are a better way to commit network crimes.

Malware is not the only threat. Due to the unlimited access to the profiles of users, attackers can further gain the information of corporation and commercial secrets. In the survey conducted by Sophos it indicates that, the concern of 62.8 percent companies is that the employees provide too much information in social networks and 66 percent companies think that using social networks will pose a great threat to corporations. Gostev points out: ”The growing popularity of social networking sites has not gone unnoticed by cybercriminals; in 2008, such sites became a hotbed of malware and spam and yet another source of illegal earnings on the Internet. By the end of 2008, the Kaspersky Lab collection contained more than 43 000 malicious files relating to social networking sites. As to cybercriminals social networking sites are an increasingly popular target.” The number of programs received by the Kaspersky Virus Lab which target social networking sites demonstrates that such sites are an increasingly popular target.



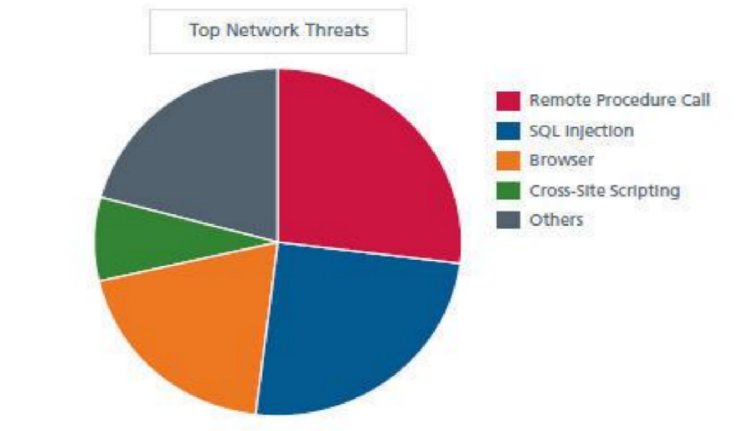
**SOCIAL NETWORKS AND PRIVACY PROTECTION**

The Internet lacks walls. Conversations spread and contexts collapse. Technical solutions are unlikely to provide reprieve from this because every digital wall built has been destroyed by new technologies. The inherent explicability of bits and the power of search make most walls temporary at best. This is why most participants in networked publics live by security by obscurity where they assume that as long as no one cares about them, no one will come knocking . In future we expect increased misusing of information published on social networks sites. This is due to the fact that half of teenagers in USA have an account on some of the social networks where they reveal all kinds of personal information from their life. It’s a different ball game when talking about social networks though. Social networking service like Facebook are not as secure, despite the technologies implemented at their facilities or the policies put in place by their security personnel. The main reason for this is because of the information that users put on these social networks.

These sites centralize and help coordinate the interpersonal exchanges between American teens and global brand. It is very easy to communicate with others using a social network construct. It is also said that says that all the information you post on these sites over the years builds up into a collection of information that becomes known as your profile and nearly anyone online is able to see it, especially your friends. So with the continued prevalence of social networking there is a continued risk to the security of information, but not mainly from hackers or thieves, but from the false trust that many people have when placing private information about themselves online. This is a huge risk but it can be combated with education.

**ROLE OF SOCIAL NETWORKS IN CYBER SECURITY**

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.



**SECURITY AND PRIVACY RISKS IN SOCIAL  NETWORKING**

It tells us that there are many information management issues with social media services, mainly in the area of privacy and personally identifiable information and how to properly store and protect it. This often makes the information available to government agencies. This is because, as puts it, «social networking sites create a central repository of personal information» which continues to grow as users keep adding to it. What makes this worse is teenagers, who are less worried about privacy and security, continue giving up information about themselves willingly.

**CONCLUSION**

It is fairly clear from all of this research that social networks are big security and privacy risks. They have this risk because of their centralized architecture, their huge repository of all the personally identifiable information a hacker could ever want, and the general ignorance of the populace to how to properly use privacy settings to improve their online safety. This can only be combated in a limited way by technological means, or even by policy. tells us that we should consider any information sent through social media not secure, and therefore not transmit any sensitive information through social networks. But with better education and some architectural changes, social networks can be used more safely. Education is the biggest part. People fall into complacency and need to be reminded of things sometimes. Users are not afraid of setting up their personal information such as date of birth; however they don’t want to publish public information such as their career. On the other hand all users we have probed published their education. We have expected this fact because Facebook has its origin in university environment; its purpose was to provide communication medium among university students and graduates.

**REFERNCES**

1. Bilge, L., Strufe, T., Balzarotti, D. and Kirda, E. (2009) ‘All your contacts are belong to us: automated identity theft attacks on social networks’, Proceedings of the 18th International Conference on World Wide Web, 24–29 April, Madrid, Spain, pp.551–560.
2. Bodorik, P. and Jutla, D. (2008) ‘Privacy with web services: intelligence gathering and enforcement’, Proceedings of the International Conference on Web Intelligence and Intelligent Agent Technology, 9–12 December, Sydney, Australia, Vol. 3, pp.546–549.
3. Brentham, J. (2002) TCP/IP Lean (Web Servers for Embedded Systems), CMPBooks, Lawrence, Kansas.
4. Hekkala, R., Väyrynen, K., & Wiander, T. (2012, June). Information  Security Challenges of Social Media for Companies. In *ECIS* (p. 56).
5. Barnes, S. (2006). A privacy paradox: Social networking in the United  States. First Monday, 11(9). doi:10.5210/fm.v11i9.1394
6. Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013).
7. Social Networking Sites and Their Security Issues. International Journal of  Scientific and Research Publications, 3(4), 3.
8. Globally,BusinessWeek,2008. http://www.businessweek.com/technology/content/aug2008/ tc20080812 853725.htm. Cited 29 Oct 2008
9. Larkin: Threat Alert: Spear Phishing. PC World, 2005. http://www.pcworld.com/article/122497/threat alert spear phishing.html. Cited 29 Oct 2008
10. Adusumalli SK, Vatsavayi VK, Vadisala J (2014) A study of privacy attacks on social network data. J Glob Res Computer Sci
11. Alqatawna J (2015) An adaptive multimodal biometric framework for intrusion detection in online social networks. IJCSNS Int J Computer Science Network Security
12. Backstrom L, Dwork C, Kleinberg J (2007) Wherefore art thou r3579x?: anonymized social net- works, hidden patterns, and structural steganography. In: Proceedings of the 16th international conference on World Wide Web.