Role of Security in Social Networking

David Hiatt
College of Arts & Sciences
Regent University
Virginia Beach, Virginia, U.S.A.

Young B. Choi
College of Arts & Sciences
Regent University
Virginia Beach, Virginia, U.S.A.

***Abstract*—In this paper, the concept of security and privacy in social media, or social networking will be discussed. First, 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. Our research will help the readers to understand the security and privacy issues for the social network users, and some steps which can be taken by both users and social network organizations to help improve security and privacy.**

Keywords—Security; Information Security; Social Networking: CIA; Confidentiality; Integrity; Availability; PII; Social Networking Service; SNS

I. Introduction

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. [1] states that information security is necessary because of the risk generated when technology is used to process information because information may be disclosed in the wrong way or to the wrong person. Information security is broken up into three major areas, which are called the CIA of information security. These areas are confidentiality, integrity, and availability. 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. This is about protecting information in storage, transmission, and processing, using policy, education, and technology, according to the McCumber Cube model of information security. 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, honeypots, and appropriate training and policy enacted by their security managers.

It's a different ball game when talking about social networks though. Social networking service (SNS) 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. According to [2], the staggering popularity of these social networks, which are often used by teenagers and people who do not have privacy or security on their minds, leads to a huge amount of potentially private information being placed on the Internet where others can have access to it. She goes on to say that interacting with people is not new, but this medium for doing it is relatively new. She says, "Social networking sites have become popular sites for youth culture to explore themselves, relationships, and share cultural artifacts. These sites centralize and help coordinate the interpersonal exchanges between American teens and global brands [2]." According to [3], it is very easy to communicate with others using a social network construct. He also 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 combatted with education. [3] states that Facebook and other sites have become such a part of many of our lives and Internet usage. So compounding the huge repository of personal data online is the careless and over-trusting nature in which people, especially teenagers, share personal information online. This information may not contain actual PII (Personally Identifiable Information), but it does contain many parts that can be aggregated into a whole by an attacker. This information can also be contained in pictures that are posted; for example a picture taken in front of your house may contain the house number. It is easy to see how this can happen when people are not very attentive to their security and the security of their information. It is essential to be careful what we put online in this way; being careless can lead to information being posted that should not be available to others.

II. History and Development of Social Networking

Sharing information and communicating with people has been around for as long as people have been around. But when computers and the Internet became much more common, we saw the use of email systems and short text messages as the first popular means of communication between people [4]. This was not so dangerous because it involved the sending of one message at a time between two people only, and it was no riskier than sending other information across the web to only one person. [4] goes on to point out that more technologies like chat rooms and online games came to be, and then social media where users could share information, talk, discuss interests and likes, post pictures and video, etc. One of the first social networking sites like this was MySpace [2]. Its original audience was teenagers and the music and art scene. She points out that its popularity dropped like a rock when Facebook came online and then it became the most popular social network. Some sites, such as LinkedIn or Flickr, have a specific purpose, and some are more general. There is almost no limit to what people can post online these days, and this is a potentially scary thing. According to [5], social media "spread quickly and widely and contain large-scale information of a broad audience. However, the unstructured massive data transaction may overwhelm users with information overflow" leading to a form of chaos. [2] states that social media sites and chat rooms are basically just "organizational and software procedures that control the exchange of interpersonal information in social networking sites, text messaging, instant messenger programs, bulletin boards, online role-playing games, computer-supported collaborative work (CSCW), and online education." As mentioned in [4], sites that provide these types of services to users at little to no cost provide a lot of enticement for people and have become very popular.

[6] tells us in his article that there is a rich history for social media, which has always been a promising idea that drew many users, especially young people. The use of social media today among teens is almost universal. The success of a social platform is largely dependent on its architecture, which dictates the nature of the interactions that can occur. It is interesting to note, he says, that when conversations can be overheard by others, it gives rise to potentially much more interesting interaction among users. It is starting to become clear where the risks are in this, with the combination of social networking being so easy to access by teens and people who are not security/privacy conscious.

III. Security and Privacy Risks in Social Networking

Needless to say, social networking is not without its security risks. A great majority of social networking deals with privacy. [6] 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 [2] 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. This is a huge part of the problem, and a possible solution that should help to combat this will be suggested later. Sometimes this is in the name of being popular. Sometimes this is just pure carelessness. [2] says the "private versus public boundaries of social media spaces are unclear." He goes on to note that parents are often very unaware, or not caring about, what their teens are putting online.

Another main risk with the privacy and security of information in social networks is the centralized architecture. As stated previously, social media servers are a gold mine of personally identifiable information, which is freely given up, by teenagers and adult users alike. [4] says that this gives rise to grave privacy concerns and can give rise to things like identity theft and selling of user data to third parties. Users have a false sense of trust in their social network provider to protect their information, when it is often being sold to third parties or hacked by identity thieves. He goes on to point out that while Facebook added privacy settings that the user can control, their default setting is public when an account is first created. Thus, a brand new user that does not changes these settings to make them more strict is actually posting information that can be viewed by the public and non-friends. [4] continues to show that the amount of information that trusting users put in their profiles on popular social media sites can be pieced together to form a picture of the user, if you will, that contains enough information to trick their friends into thinking it's really them. An identity thief can then create a false profile of that person, re-friend all of their friends, and then trick their friends into revealing more personal information about the user. [3] calls this practice "profile cloning." He states that some thieves steal information about users from one site to create a fake profile on another. He states that information can also be tricked out of users through the use of phishing attacks, where information is gleaned from users via setting up fake Websites that ask for personal information or even passwords and social security numbers.

Various other attacks, according to [3], are engineered to either take personal information from users, or infect their system with viruses. They include click jacking in which an attacker posts a video to a user and when the user plays it, malicious code is introduced into their system, and watering hole attacks, where a developer's forum is hacked and everyone that visits the forum gets their system infected by a Trojan horse virus. Other risks include scams and cyber bullying, too. The risk any user takes on will be proportional to the amount of personal information they choose to post, and how they set their security/privacy settings.

The biggest problem here, according to [3], is that many users are not aware of the privacy settings and how to use them. They are also "not aware of the risks associated with uploading sensitive information." Studies have shown that social media sites are designed to get as many users together into one place, and many of these users are unaware of how to use the privacy settings. These sites value "openness, connecting, and sharing with others – unfortunately the very aspects which allow cyber criminals to use these sites as a weapon for various crimes [3]." He goes on to say that employees often post company information on social networks, introducing risk to the organization they work for. When you see how naïve and trusting some people are, and how much private information is stored in a central repository like a social media service, it is easy to see that this is a very big reason why attackers go after social networks.

So it is plain to see, according to [4], that even though technology and policy may be used at the social networking sites the same as any other organization, the centralized structure and the huge repository of private information gives rise to huge security gaps. These can be addressed with more policy, some common sense by users, and some architectural changes.

IV. Some Possible Solutions

The rising tide of attacks on social networks, according to [3], tell us that "social networks and their millions of users have to do a lot more to protect themselves from organized cybercrime, or risk failing to identity theft schemes, scams, and malware attacks. Understanding these risks and challenges should be addressed to avoid potential loss of private and personal information." Also, as [7] says, "The area of internet information security is well developed and evolves continuously in response to new threats" and so it must evolve with social media too."

[3] gives some important tips for social network users to follow to help protect themselves online. The amount of personal information posted should be limited, and not post home addresses or private contact information. This, and information about your likes and daily routine can all be pieced together by a cybercriminal. Also, think of the Internet as public. Even if privacy settings are in place, information posted can still get out there, through friends reposting, and it is stored on servers that can be hacked. Be comfortable with the public seeing whatever you are posting on social network sites. Also be skeptical and beware of strangers. Not everyone is who he or she claims to be, and they could have stolen someone's identity to commit cybercrime. Do not use the third party applications that are often making their way around Facebook. They often install malware that tracks your online activities. Use strong passwords, use anti-virus software, and keep your software up to date to help protect against the latest security threats. For those with kids, they need to be monitored very closely because they often do not know the wise techniques of online security or don't care to keep themselves safe. Remember that once you post something, it never goes away even if you delete it, and know what to do to report someone that you suspect may be a security threat.

This goes into some other ideas that [2] brings up in her article, which are still applicable today. One thing she says is that parents need to be much more involved in the online activity of their children, since they are not experienced or wise enough to watch out for themselves or make the best decisions. Schools are also taking some actions in this regard, with policy and supervision, but not all schools are on the same page with this. Some are just letting kids suffer the natural consequences, and warning them that college and potential employers check their social networking pages and the posting of certain content is frowned upon and could result in non-admission or non-hiring.

This problem can also be combatted with changes to architecture and policy. One such architectural change was proposed by [3] in the form of a Secure Request-Response Application Architecture. This scheme involves the ability for a user to accept or reject another user's request for information, whether they are a friend or not. The user can also set up two different databases for information depending on how much they trust the requestor. He can then protect his most sensitive information. [2] points out that some sites are implementing better and more customizable privacy settings. Facebook has overhauled their privacy system several times to make it more user-friendly to customize settings and give users the power over who can see individual posts. While this is not a completely safe solution, it does help, as long as people are aware of the features and use them wisely. But this is no substitute for being smart about what you post online. She goes on to say that many schools are making more of an effort to teach students about the importance of online privacy in the name of greater security. [4] gives us an idea that a decentralized architecture would help keep information safer. In this type of setup, any user's information would never be all on the same server or even at the same facility. This would do a great deal to help prevent a full retrieval of a user's profile by an attacker. An example of a social network that employs this approach is Diaspora. And according to [8], it is essential that a good amount of risk management be done. This will help solidify the security policy in place at the organization in question.

A very extensive paper was written by [9] that details an extremely complex study outlining the effects of unfriending people in your social profile. The main idea of this approach was that every friend someone has in their profile has a certain risk factor assigned to them by an algorithm, and this is based on the habits of how they interact with the user online, and how they pass on information, or repost things, to their friends. Due to this effect, even if you post online to just your friends, there is no guarantee they will not repost it to their friends, thus allowing the post to get outside your friend circle. So once the most vulnerable friends are identified using this algorithm, they can be defriended and have the effect of making your online experience more secure and private. The math formulas that went into this calculation were extremely complicated and likely nothing that would be comprehended by the average user, but the upshot of all of this is clear; unfriend people that are leaking your information, and your time online will be safer

V. A New Proposed Solution

The biggest problem here is carelessness in what is posted online, and this is one of the easiest to solve conceptually. A possible solution is certainly not complete, but will help put a dent in the problem and reduce the amount of carelessness on the Internet, and fits in with the idea of using education as one of the three ways to secure information systems. A proposal that all social networks, including Facebook, Twitter, Flickr, LinkedIn, as well as all portable applications that serve a similar purpose is suggested to require all new users, when signing up for an account, to view a short video that discusses the topic of Internet safety, personally identifiable information, and instructs users on that network's privacy settings. The button to submit for an account should not appear until the video has played. This way it cannot be bypassed like the legal disclaimers that people just accept blindly. Also, any current users would have to watch the video on the day it goes online in order to continue using their accounts. To expand on the idea of yearly training often used in the military, the video could be required to be viewed once a year to remind users of its importance. Such an idea is rather easy to implement with the technology of today. With much better education, we can help combat this problem, especially if we also decentralize the information storage on these social networks.

VI. 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. There is also a large risk because many people, especially teenagers, are extremely trusting of other people and what type of information about themselves they reveal online.

This can only be combatted in a limited way by technological means, or even by policy. [10] tells us that we should consider any information sent through social media not secure, and therefore not transmit any sensitive information through social networks. The burden falls mainly on users to be smart about what they are doing online. The best thing we can do is to be smart when online.

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.

Lastly, it is important that research continue in the area of how to make social networks more secure even though trusting users are placing a plethora of personally identifiable information online.

References

[1] Hekkala, R., Väyrynen, K., & Wiander, T. (2012, June). Information Security Challenges of Social Media for Companies. In *ECIS* (p. 56).

[2] Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). doi:10.5210/fm.v11i9.1394

[3] Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. *International Journal of Scientific and Research Publications*, *3*(4), 3.

[4] Verma, A., Kshirsagar, D., & Khan, S. (2013). Privacy and Security: Online Social Networking. *International Journal of Advanced Computer Research*, *3*(8), 310-315.

[5] Deng, X., Bispo, C. B., & Zeng, Y. (2014). A Reference Model for Privacy Protection in Social Networking Service. *Journal Of Integrated Design & Process Science*, *18*(2), 23-44. doi:10.3233/jid-2014-0007

[6] Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. *Government Information Quarterly*, *29*(1), 30-40.

[7] Vladlena, B., Saridakis, G., Tennakoon, H., & Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal Of Human - Computer Studies*, *80*36-44. doi:10.1016/j.ijhcs.2015.03.004

[8] Kim, H. J. (2012). Online Social Media Networking and Assessing Its Security Risks. *International Journal Of Security & Its Applications*, *6*(3), 11-18.

[9] GUNDECHA, P., BARBIER, G., JILIANG, T., & HUAN, L. (2014). User Vulnerability and Its Reduction on a Social Networking Site. *ACM Transactions On Knowledge Discovery From Data*, *9*(2), 12:1-12:25. doi:10.1145/2630421

[10] Thompson, A. F., Otasowie, I., & Famose, O. A. (2014). Evaluation of Security Issues in Social Networks. *Computing & Information Systems*, *18*(1), 6-20.