The Continuous Rise for Social Networking Privacy and Security

By

Adrian M. Powell

Professor Li Yang

CPSC 5620 Computer Network Security

University of Tennessee at Chattanooga

April 20, 2012

Abstract

This research paper focuses on privacy and security issues that millions of users encounter while using social networks such as Facebook and Google +. Both of these social networking sites are intended to provide means of social interactions and communications, but they also raise large amounts of privacy and security concerns. In this paper I discuss the privacy conflicts that both Facebook and Google+ encountered and also discuss the solution to these problems. The second section of this paper discusses the security conflicts that both sites encounter, and presents how these security conflicts can be avoided or resolved with the proper counter measures.

In today's society, social networking sites have changed the way that we conduct our everyday lifestyles. We now use networking sites such as Facebook, MySpace, Google +, LinkedIn, Twitter, etc. to stay in touch with friends, coworkers, colleagues, and even strangers all over the world, simply by the click of a mouse. Fortune 500 companies to local mom and pop stores have both benefited from the ability to advertise through theses social networking sites as well. Daily users all over the world customize these social networking sites with personal information such as family pictures, personal background information, real-time location status, personal videos, and personal messages. However, many social networking site users fail to understand the risk that he or she takes by placing all of their personal information in the hands of an enormous site such as Facebook or Google + where security and privacy issues have been an ongoing dilemma. Security in the social networking generation has always been an issue over the past years, however, the hype always seems to dwindle, and the world continues to use these beloved social sites limited of knowing that more people other than their friends are able to view and obtain personal information to use in an unethical manner.

One of the most popular social networking sites, Facebook, created by Mark Zurkerburg in 2004 has 600 million current users and generates a confounding 770 billion page views per month (Zang, 2011). With a user base of this size, large amounts of possibly sensitive and private information on users and their interaction are collected on a continuous basis (Zang, 2011). The information that is collected is usually private and intended for the eyes of authorized users only, however due to the popularity of social networking sites it attracts not only faithful users but parties with adverse intentions as well (Zang, 2011). With a user base of this size it creates a wide range of variety, related to the purposes and usage patterns of various social networking sites that unavoidably present privacy infringement risk to all of its users by information exchange and sharing on the Internet (Zang, 2011). This is why one

of the most important concerns currently with social networking sites are the security and privacy of sensitive information, which is any data that an adversary could obtain or use to cause significant harm to other users.

A large majority of social networking sites offer basic features of online communication, interaction, and interest sharing by letting each individual user create online profiles that others can view (Zang, 2011). Staying connected with one another through the web, was the sole objective for many of these social networking sites, however users demand for added features forced social networking sites to add more functionality and now one of the main motivations for users to join is because of the third-party applications that are offered by almost all of the social networking sites, which allow users to share information with selected contacts or the public and facilitate social interactions between users of the social networking site (Zang, 2011). Due to the constant functionality change in social networking sites, many privacy and security vulnerabilities go overlooked (Ieba, 2011).

Facebook and sites like Google + place so much emphasis on impressing their users interface experience that they sometimes fail to spend adequate time on more important areas such as the privacy and security of their user's information. These overlooked areas have cause leakage of personal information such as one's identity; it has invited malicious attacks from the real world, and cyberspace such as stalking, reputation insult, personalized spamming, and phishing (Ieba, 2011). Even with all of these possibilities for attack lingering, many of the privacy access control mechanism of today's social networking sites are purposefully weak to make joining the site and sharing information easy and this is why social network sites like Facebook and the fairly new Google + constantly deal with privacy issues on a monthly basis (Zang, 2011). One of the key issues social networking sites face is the privacy of its user's content. This can vary from personal information, pictures, videos, and messages but the problem is created when many of these sites display items that are meant to be private to the entire social network world without explicit permission from its rightful owner.

For the social networking site Facebook one of these privacy issues were bought to the light in 2007 when Facebook introduced its ad platform Beacon (Martin, nd). The Beacon ad platform was created with intensions of transforming the way advertising was done through the Internet (Martin, nd). Facebook believed the Beacon ad platform would achieve this by allowing Facebook users to share information with their specific Facebook friends after they visited one of Beacon's 44 affiliate websites e.g. Ebay.com, Overstock.com, and Blockbuster etc (Martin, nd). However the idea of creating a new way of advertising slowly formed into a privacy issue for Facebook and its users.

The Beacon ad platform that Facebook introduced would publicly display Facebook's users Internet browsing habits and recent purchases on his or her Facebook news feed without explicit permission (Martin, nd). This sparked numerous amounts of questions and concerns from users regarding Facebook's privacy settings and the purpose of the Beacon platform (Martin, nd). This brought concern from Facebook users because the Beacon platform ran behind the scenes of Facebook and only notified users by a small pop-up message which appeared briefly and only gave users a few seconds to click deny so that their information was not displayed publicly (Martin, nd). If this pop-up message was ignored or just over looked the information was automatically displayed for the entire Facebook world to know. If users did manage to click deny, their information was not posted to their Facebook page, but was still saved in one of Facebook's user's database (Martin, nd). This was an extreme concern because Facebook's users felt that they were not properly informed about the Beacon platform functionality or given a fair choice to opt in or out of the application from the start.

The Facebook social networking site did focus on differentiating its privacy controls from its closest competitors by claiming that users had full control of how their information was searched, shared, and accessed however over time the Beacon platform sparked revolts and many Facebook user's battled to end its use of the Beacon ad platform and stressed that more focus should be spent on Facebook's privacy complications (Martin, nd). Not only did Facebook encounter privacy issues but the social network new comer, Google + did as well.

Since the initial launch of the Google + social-networking project potential problems were spotted concerning its privacy issues. Google had previously encountered social related privacy issues in the past with "Google Buzz", a social networking micro-blogging and messaging tool that was developed into its web based email program Gmail. The Google Buzz privacy issues brought behind with it a class action and Federal Trade Commission settlements. Since then, Google tried to keep their users privacy in mind, but during the creation of Google + a few privacy holes were overlooked.

One of the privacy concerns that Google + had was it's built in "share" option. If a Google + user posted a photo, anyone connected in that users group of friends had the ability to share that photo with anyone in their network simply by a single click of the mouse (Albanesis, 2011). While many users loved the option to share others' posts, many users were not exactly sure how it worked but once users became aware of the privacy vulnerability that this "share" option created they soon looked for better ways to keep their private information (Albanesis, 2011). Facebook and Google + both faced privacy issues within their social networking sites, but to be successful in the social networking industry creating a sense of protection and privacy for its

users was very imperative. This forced both social networking sites to focus on ways to solve any current or future privacy issues that had developed.

Facebook's solution to its Beacon ad platform privacy issue was resolved when the founder and CEO Mark Zurkerburg, announced that users could now completely turn off the Beacon ad platform (Martin, nd). After Facebook users revolts about the Beacon ad platform reached news headlines Facebook's Mark Zurkerburg responded by stating, "We simply did a bad job with the release, and I apologize for it. We've made a lot of mistakes building this feature, but we've made even more with how we've handled them" (Martin, nd). Facebook dug even further for a solution to the Beacon ad platform by letting Facebook users adjust their privacy setting after logging in, or users could click on the "privacy" tab in the upper right hand corner of the profile page and click on "external web sites" which would give users the option to stop Web sites from sending information about their browsing habits back to their Facebook news feed and to the Facebook database (Havenstein, 2011). The final solution for the lightweight system that was made so that users would not have to touch it for it to work resulted in a class action lawsuit on August 12, 2008 (Havenstein, 2011). The Beacon ad platform that was intended to transform the way advertising was done through the Internet resulted in Facebook paying a $9.5 million dollar settlement (Havenstein, 2011). This was a major setback for Facebook's brand name and with hopes of becoming the world's most used social networking site it only made founder and CEO, Mark Zurkerburg more aware of how important privacy is in the world of social networking (Havenstein, 2011). Facebook was not the only social networking site working to find solutions for their privacy issues, Google + also had a few solutions to meet their privacy issues as well.

Google + solution to its users "share" option was by done by creating a pop-up tip that would appear when the user made a photo post, telling them how to disable the sharing option if that was what they preferred (Albanesis, 2011). All post that was designated as private would not be shared publicly. Google + believed that sharing through the Web should not differ from sharing in real life. There is always the risk of telling someone something private, and that person going and possibly telling someone else. This sharing risk could occur even if a user was on Google +, Facebook, or face-to-face. The complete removal of the "share" option would have helped to a certain extent, but what would stop someone from just copying and pasting something from your feed into an email (Albanesis, 2011). The "share" button was solely created to simplify and make sending information very simple, but many of these privacy resolutions caused security holes to go overlooked and security holes in a social networking site was a prime interest for future hackers (Albanesis, 2011).

Security holes within social networking sites can create very serious problems for its users. Both Facebook and Google + have encountered very similar security

issues since their start in the social networking industry. Since their entry into this industry, many social networking sites have had security issues such as, application hijacking, cross-site scripting, hacking through email, phishing, social engineering, cyber-crime, scammers and spammers, and many more.

Application Hijacking was one of the many security exploits; it was used to steal data or spread malware like viruses, worms, and spyware (Ieba, 2011). Hackers used this method to hijack the session of a previously authorized third party Facebook application and invisibly passed it off to a malicious app, which was able to invisibly harvest the user's data as well as "wall" and "messaging" access too (Ieba, 2011). Cross-site scripting in "instant personalization" sites was another issue and Hacker used this method to quietly harvest a user's Facebook friend list, email address, and other personal data (Ieba, 2011). The exploit injected a malicious code into one of the "instant personalization" sites such as Yelp, Pandora, and Microsoft's Docs.com. The instant personalization was a feature that allowed a few selected third party sites to immediately access a user's Facebook information as soon as the user entered the site (Ieba, 2011). The instant personalization feature was much different than the sites Facebook Connect. The instant personalized sites did not have a prompt user to log in or click a 'Connect' button before it shared data. By doing this, if one of the instant personalization sites were compromise, the chance for abuse was much higher than with Facebook's standard sites.

Hacking through email, Phishing, and Social Engineering were the next security exploits that social sites faced (Ieba, 2011). Hacking through a user's email is one of the most common ways to initiate identity theft. The only information the hacker needs to know is your login email for the account and one of the many password-cracking soft wares. Another issue that caused problems was Phishing (Ieba, 2011). Phishing was used to receive the credentials of the social networks members but most hackers went about this by creating a web site that looked similar to Facebook's or Google's +. Hackers would then use these created sites and lead the sites to the malicious web site, which allowed Hackers to steal user's information for later use (Ieba, 2011). Social engineering was another security issue, which was used to hack user's accounts. Hackers would send the user a spoof email claiming to be the true source and by using Facebook chat to obtain users passwords (Ieba, 2011). The next security issues were Cyber Crimes. Do to the large user base it is hard to tell if a user was past or current criminal. Many Cyber Crimes included people being blacked mailed, pictures being misused, information being sold, extortions, spying, and stalking (Ieba, 2011). The last security issue that social networking site users faced was Spamming and Scammers. Spammers were just annoying messages that constantly bombarded the user with unwanted advertisements and messages. Over time many social networking sites have uncovered security issues and solved them

internally, however many users can just customize his or her own privacy setting within the site to help combat with many of the security issues stated above (Ieba, 2011).

To help resolve a majority of the security issues, many simple steps can be done. For users to help protect themselves from Application Hijacking and Cross-site scripting users they should never download anything from a social networking site that you have not prompted, do not let allow applications gain access to your personal information, always remove unused applications, and never download applications whose authenticity is not established (Ieba, 2011). For users to help protect themselves from Hacking through email, Phishing, and Social Engineering threats, users of all social network sites should configure their own privacy settings, keeping them strict and by never sharing you primary email address. Users should also make use of the "https" secure browsing option, which will only allow the users Web page to load up only on a secure connection (Ieba, 2011). Another important feature that many social networking sites offer is a notification message that alerts users when a new computer or mobile device has viewed, or logs into a social network account which would help eliminate a large majority of hackers (Ieba, 2011). For users to help protect themselves from Cyber Crime, users should choose their friends wisely, and not add people you do not know, do not share pictures or videos with everyone, use the block feature to block any suspicious people, be very cautious to what information you put up on your profile page, an never share or provide sensitive, personal, or private information on any type of social network (Ieba, 2011). For users to help protect themselves from Spamming and Scamming, users should never give their email address and phone number for everyone to see, do not use applications or games with your primary email account, un-friend people who forward spam messages, and also leave groups and communities which promote spam advertisement, and report spam links and messages so that they can be removed by the websites management team.

In conclusion, when dealing with others personal information, privacy and security is a big deal for all social networking sites. Social networking sites work diligently to make users feel safe because that is very important for success in the social networking industry and the way that social networking sites and technology are slowly taking over in today's society, makes privacy and security concerns a ongoing demand as time goes on.

References

Ahn, Gail-Joon (2011). Security and Privacy in Social Networks. 10-12. Retrieved from http://ieeexplore.com

Albanesis, Chloe (2011). Google + Privacy: Has Google Learned Its Lesson? Retrieved April 1, 2012, from http:// http://www.pcmag.com/article2/0,2817,2387995,00.asp

Havenstein Heather (2011). Update: Facebook Caces in to Beacon Criticism. Retrieved April 1, 2012, from http:// http://www.computerworld.com/s/article/9051119/Update_Facebook_caves_in_to_Beacon_criticism?taxonomyId=84&pageNumber=1

Ieba, Ian (2011). Social Networks and Security Issues, How to Combat Them. Retrieved April 1, 2012, from http://ianieba.com/social-networks-and-security-issues-how-to-combat-them/

Kee, Edwin (2011). Google + Kindly Meet Privacy Issues. Retrieved April 1, 2010, from http://www.ubergizmo.com/2011/06/google-plus-privacy-issues/

Martin, Kirsten (nd). Facebook (A): Beacon and Privacy. 1-11. Retrieved from http://ieeexplore.com

Pringle, Bill (1999). Facebook Security Issues. Retrieved April 1, 2012, from http://billpringle.com/home/facebook.html

Purvis, Carlton (2011). Facebook Issues Security Tips Guide. Retrieved April 1, 2012, from http://www.securitymanagement.com/news/facebook-issues-security-tips-guide-008912

Shinder, Deb (2009). Social Networking Latest, Greatest Business Tool or Security Nightmare? Retrieved April 1, 2012, from http://www.windowsecurity.com/articles/Social-Networking-Latest-Greatest-Business-Tool-Security-Nightmare.html

Tyson, Joey (2010). Social Hacking. Retrieved April 1, 2012, from http://theharmonyguy.com/oldsite/2010/05/16/more-recent-security-problems-with-the-facebook-platform/

Zang, Chi (2010). Privacy and Security for Online Social Networks: Challenges and Opportunities.13-18. Retrieved April 1, 2012, from http://ieeexplore.com