Markail Bruner

English 231

Research Paper

April 15, 2014

Word Count: 2,419

Social Networking: Friend or Foe?

 Fifty six percent of Americans have a social networking profile which means this is over half of the nation. Every person enjoys their daily dose of social media because it is similar to reading a newspaper in the morning. However, being said this means there is a lot of personal information on the internet to be discovered by unwanted parties. People are unaware and uneducated to the fact that their information is being stolen without them knowing. There are many questions that come into factor when a topic like so is presented. Why do people not know that they are essentially giving their information away? Is it because the companies who create startup applications are too focused on a certain matter such as profits? Is it the consumers’ fault that they are not educated enough to understand what they are signing up for? **There needs to be a certain privacy or security measure which will ensure the safety for users for current and future social networking applications, which leads me to the question that seems to be prominent, are there ways to prevent future information leaks or upgrades to current privacy restrictions to social networking applications?**

 There are a mass amount of social networking applications that currently exist and there are new applications being created every day known as startups (Beach, Gartrell, & Han, 2009). Startups are applications that have been popular in the recent four years because due to more people seeing the success of large social networking companies such as Facebook or Twitter. The popularity draws millions of users but it also brings in the “black hat “hackers which are the people who specifically prey on unknowingly users (Hemey, 2011). Every startup is vulnerable to attacks from the hackers because most of the development is focused on the actually applications’ aspects such as design and content. This obviously leaves the window to security wide open, which allows companies’ new users to be raided and potentially disturb the company is their users are unhappy with the product. This explicitly is the reason privacy and security plays such an important role when creating or modifying a social networking application. There are many ways a hackers obtain information or break into the application’ s system, as well as possible solutions to these problems.

 There are various threats to personal information and tools used to obtain what the person needs in. Threats come in ways that are unimaginable and so undetectable that some people may be amazed (Beach, Gartrell, & Han, 2009). There are some larger topics when referring to strategies for infiltration such as direct anonymity, indirect anonymity, eavesdropping, spoofing, replay, and wormhole attacks (Beach, Gartrell, & Han, 2009). Along with data mining, distributed denial of service, malware, phishing, fraud, and spamming to name a few (Chen, & Michael, 2012). Each of these will be covered with an extensive breakdown with sub topics such as how they are implemented or how commonly they are used.

 Direct anonymity is something that is noticed often in startups due to the vulnerability in the system allowing for easy access because there are only small amounts of protection for the consumers data (Beach, Gartrell, & Han, 2009). The most common occurrence of this along with a prime example is on the popular application Facebook when there is a redirect page that appears asking for the user’s agreement to allow whatever they are agreeing for to allow access to the data. This later can be picked up over Wi-Fi with someone as being near a person with a Bluetooth, which is the direct part of this method because there is a contact like situation (Beach, Gartrell, & Han, 2009). Location and tracking also plays a part in direct anonymity because what a lot of people do not realize is there are applications such as SocialAware that logs data. This means that anywhere a person may travel to or visit can be stored for later by a person therefore intruding privacy of another user’s data. This all is brought together because social networking applications such as WhozThat or SocialAware allow people to share their networking identification (Beach, Gartrell, & Han, 2009). This flaw in the applications system that leads to privacy and security risks which originally seemed harmless. Also, there are times where networking identification may not be directly linked to mobile systems however through logs and tracking which is provided it is possible to still attain the information the hacker wants (Beach, Gartrell, & Han, 2009). Manipulation is key with direct anonymity because these flaws in the system are not something that are necessary a lack of security rather than loopholes to get around the system.

 Where there is direct there must be indirect which leads to indirect anonymity which means that although the exact identification of the user is not given out because there is something related to the user in the system there is risk of stolen information. This could be something simple such as the person’s favorite movies which seems ridiculous but is actually all that it takes (Beach, Gartrell, & Han, 2009). This is not as common as the direct anonymity approach however the reason this occurs is because of another issue regarding hospital and voter information that was released to public. When information becomes public there is more risk for it to be disturbed clearly, so when it comes to social networking applications there are many similarities when exposing data.

 Spoofing and replay go hand to hand because it starts with a spoofing attack, which basically takes an already compromised user, puts a disguise on as the compromised user, and then attacks multiple mobile devices. It is sending the data out also known as replaying the data by using the user’s identification to gain the information (Beach, Gartrell, & Han, 2009). Another type of attack that branches off of replay are wormhole attacks, which focuses on one side of the a wireless broadcast where data is captured then replayed once again off of the other end of the networking. The large picture here is the lack of assurance that certain identification is an actual person; the key is disguise and manipulation with these different attacks especially when on a mobile networking systems (Beach, Gartrell, & Han, 2009). Eavesdropping is another associated method of gaining information although this requires a wireless transmission where the material could be collected by another device. These are some techniques that are used commonly and easily fool people.

 There are more complex methods of getting information from a user such as data mining for example. This is completed by removing the data out by the use of patterns because users’ information is in fragments however it is then conveyed together and decoded (Chen, & Michael, 2012). This is a dangerous tool because information that is leaked from this can be things such as social security numbers and credit card numbers. There are a number of ways that this can completed rather it be from web pages, emails, public documents or even social networking applications because of the friends system anyone is vulnerable (Chen, & Michael, 2012). Data mining is a method that seems to be uncommon because of how unique of a technique it is and the complexity of the scheme.

 There is an acronym passed around in the technology and threats world known as DDoS, which stands for distributed denial of service. This is when packets are sent to a server which then causes a crash in the system which may leave it vulnerable for infiltration; however this is uncommonly used because it takes a lot of power to knock off larger servers on popular applications such as Facebook. With the mention of Facebook this leads to another technique that is commonly used, which is malicious applications within the social networking application or site (Chen, & Michael, 2011). An example of this is “Secret Crush” where a person may receive a message or popup letting them know they have a message from a crush therefore it asks to download a tool. This tool is actually a hidden spyware bot in which is implanted on the account or computer of the individual allowing information to be transferred to whoever’s bot (Kayastha, Niyato, Ping, & Hossain, 2011). There are also phishing mechanisms such as being a trusted company of a person which then an application appears asking for permission which they click accept and a virus may be installed even though it looks harmless. There are many things that look like a simply innocent adventure when in fact these are the most commonly used ways of getting personal information (Shakeel, 2012).

 The amount of techniques and tools available for use of hackers are astonishing, as well as how often people fall for their tricks is also surprising. There are ways to prevent these occurrences from happening and solutions to problems that seem unsolvable. There are certain steps that startups need to apply to their applications before releasing them to the unaware public (Kayastha, Niyato, Ping, & Hossain, 2011). More education towards what people are signing up for should be advertised to prevent information leak crises. People should also take into consideration the risks for joining new social networking applications. There are some strategies for prevention and solution which are possible for the future (Kayastha, Niyato, Ping, & Hossain, 2011).

 Since Wi-Fi makes everything run essentially when it comes to distributing information from one user to another Beach, Gartrell, and Han proposed an idea that when information is being linked there should be some sort of message basically asking permission to allow the user’s data to be transferred (2009). This would basically allow the user to see what device is trying to receive their information and if they did not know the device they could simply decline it thus improving privacy and security for direct anonymity problems. They also suggested an idea of an identity server in which the information is separate from basically breaking apart for example the location of a person and their Facebook preferences making it more difficult for a hacker to obtain a person’s identification (2009). This also contributes to lessening the direct anonymity issues that occur.

 For the indirect anonymity there is more compound strategy involved when finding a solution, however although it is one issue that is an algorithm that will create distinctive paths and certain sets (Beach, Gartrell, & Han, 2009). What this is saying is that there should be a certain algorithm that reroutes information that is being asked for to the identity server which already has broken the information into pieces which should cause difficulty for the hacker. The identity server could be used for direct or indirect anonymity as long as the algorithm is correctly modified for the indirect anonymity.

 Although threats such as eavesdropping, spoofing, replaying, and wormhole attacks sound dangerous they are actually easily defended against. Most protocols that are implemented in most websites such as HTTPS simply make sure that none of that gets through. Not all of it is blocked out and that is where the anonymous identifier comes into play, which when information is being transmitted between people there are checks that occur and messages about information being sent is popping up to the users allowing them to confirm that they want their information shared (Beach, Gartrell, & Han 2009).

 There is another approach that could be offered solution wise which is an application called Safebook in which would require multiple outside help to ensure success in the application. However, the application would provide numerous privacy, security, and data collection protection. Based around “… decentralization and exploiting real-life trust …” this would allow social media applications to bounce their users’ information off of the Safebook’s servers and protect the data that it retrieves which is where the trust is introduced (Cutillo, Molva, & Strufe, 2009). The idea is solid on paper however it requires a lot of real life trust and independent parties to help keep it running, this is another solution that would allow anyone who is attempting to steal information to run into trouble (Cutillo, Molva, & Strufe, 2009).

Prevention is one of the strongest solutions and there is a way everyone can contribute to this way, which is the abundant amount of carelessness that people possess. If everyone would be more cautious to what they click on and come to realization that everything they download may not be safe even if it is something that looks meaningless. Education of certain common spyware or malware for example is also a key factor because people should know what to do in case that occurs. The more aware a person is allows the hackers to have room for error which could lead to decreased attacks on social networking applications.

 Social networking applications are some of the most popular visited places daily and have a conflict which needs resolving. Although the problems are vast and may seem unstoppable, that is a false statement because there is a solution. Not only is there a solution there are also many ways to prevent occurrences with the use of strategic methods and use of common sense. Whether it is a startup application or an application that has been successful, any company has been and will be attacked. Being said that should not stop companies from pursuing the steps to finding ways to prevent and creating solutions to the problems that transpire.

References Page

Beach, A., Gartrell, M., & Han, R. (2009). Solutions to Security and Privacy Issues in Mobile Social Networking. *IEEE Technology and Society Magazine*. 4. Retrieved from: http://ieeexplore.ieee.org/xpls/abs\_all.jsp?arnumber=5283078

Chen, X., & Michael, K. (2012). Dr. Katina Michael. Privacy Issues and Solutions in Social Network Sites. *IEEE Technology and Society Magazine.* *31*(4). Retrieved from: http://works.bepress.com/kmichael/309/

Cutillo, L., Molva, R., & Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Technology and Society Magazine*. *47*(7). Retrieved from: http://ieeexplore.ieee.org/xpls/abs\_all.jsp?arnumber=5350374&tag=1

Hemey, C. (2011.). 5 top social media security threats. *Network World*. Retrieved from: http://www.networkworld.com/news/2011/053111-social-media-security.html

Kayastha, N., Niyato, D., Ping, W., & Hossain, E. (2011). Applications, Architectures, and Protocol Design Issues for Mobile Social Networks: A Survey. *IEEE Technology and Society Magazine*. *99*(12). Retrieved from: http://ieeexplore.ieee.org/xpls/abs\_all.jsp?arnumber=6070945

Reading, D. (2012). Security Startups Focusing On Threats, Not Malware. *Dark Reading*. Retrieved from: http://www.darkreading.com/analytics/threat-intelligence/security- startups-focusing-on-threats-not-malware/d/d-id/1137873

Shakeel, I. (2012). Social Media & Security Risk - InfoSec Institute. *InfoSec Institute*. Retrieved from: http://resources.infosecinstitute.com/social-media-security-risk/