Global Perspective of Security Breaches in Facebook

Kanwalinderjit Kaur Gagneja
Dept. of Computer Science
Southern Oregon University
Ashland, OR, USA

Abstract— This paper presents, what most people think of when they hear someone's Facebook was hacked? We will present some outdated methods of hacking Facebook that no longer work and how Facebook solved these vulnerabilities. In this paper we also present the current methods of hacking Facebook and how you can protect yourself. When someone says their Facebook had been hacked, what do they usually mean? Nine times out of ten, they left their account logged on around friends who posted a prank status update, or chose a funny picture for the victim's profile picture. This, of course, is not hacking. The other tenth of the time, someone's account has actually been hacked and someone remotely has access to their account.

Keywords—spoofing; keylooger; firesheep; phishing; hackers; evesdroppers;

I. INTRODUCTION

There are a number of social networking sites over the Internet, such as Instagram, InkedIn, Flickr, Facebook, Google+, Twitter, etc. to name a few. Facebook is the largest social networking site in the world. It has over a billion registered users. Actually, we think none of us would know someone who is not already registered. So it concerns all of us.

A researcher from University of Vienna, Stefan Stieger, Ph.D in psychology and some of his fellow researchers took a survey of around 300 Facebook users and almost 300 Facebook quitters to know how these two groups differ in terms of cyber psychology, behavior, and social networking [7].

The responses of the participants were recorded to assess their level of concern over issues such as security and privacy, and users' inclination towards cyber addiction.

The disposition of both groups those who kept on with Facebook and those who had quit the Facebook were looked into. They surveyed them on their behaviors such as outgoingness, neuroticism, amicability, and diligence. From the survey, they found out that about 48.3% of quitters were worried about their security and privacy on Facebook.

The results of above study revealed that the top most reason for the quitter group to quit the Facebook was their concerns over privacy on the social site. So as a user we need to be aware and vigilant about all the possible attacks and how to protect ourselves from them.

The paper is organized as follows. Section II describes about literature review. Section III talks about I was not even logged on! But I have been hacked. Different Facebook hacking techniques are explained in Section IV through section VIII. Finally the paper is concluded.

II. LITERATURE REVIEW

Electronic Frontier Foundation, in 2010 found out that anybody can access information from Facebook profile, although the saved profile is not public [1]. If a user hits 'Like' for some product or service, it creates a "connection" either to product site or on Facebook itself. And such connections or relationships are considered public information on Facebook. Hence, the user's information could be used to be posted on the product or service page hosted on the Facebook [1].

The Facebook is used by Government, federal, state and local agencies to investigate cases to collect evidences to solve some criminal activities. Using Facebook they can find the location, sometimes even could establish the motives, etc…[4]. There are a number of instances when Facebook has readily shared information with government agencies. However, they cannot provide information for private, unopened inboxes those are less than 181 days old, since such accounts need a warrant and a cause by law [6].

May 31, 2010 was observed as Quit Facebook Day. It was an online event. Mainly the users were quitting Facebook because of privacy concerns [5]. It was projected that about 2% of US Facebook users would delete their accounts [10]. Though, only 33,000 users deleted their accounts [3].

Last year it has been identified that Facebook is participating in the PRISM program. Therefore, now Facebook provides information of users from governments all over the world [8].

Data mining over Facebook databases is a real concern. There are number of private companies and individuals unaffiliated with Facebook those are doing data mining over Facebook databases. Lately in 2005, two Massachusetts Institute of Technology (MIT) students downloaded over 70,000 Facebook profiles by running an automated script from four different Universities, that is, Massachusetts Institute of Technology, New York University, University of Oklahoma, and Harvard University. They did it as their research project on Facebook privacy issues [2]. After this incident, Facebook started enhancing security protection for users by building various defense mechanisms to combat phishing and malware [9].

III. I Wasn't Even Logged On!?

When someone says their Facebook had been hacked, what do they usually mean? Nine times out of ten, they left their account logged on around friends who posted a prank status update, or chose a funny picture for the victim's profile picture. This, of course, is not hacking. The other tenth of the time, someone's account has actually been hacked and someone remotely has access to their account. Merriam-Webster's dictionary defines a hacker as "a person who secretly gets access to a computer system in order to get information, cause damage, etc…: a person who hacks into a computer system" [11].

Over Facebook's lifetime, it has had multiple vulnerabilities that have been taken advantage of by hackers to either gain people's information, or even just to wreak havoc. These methods take advantage of anything from weaknesses in Facebook's authentication system, to the Facebook user's naivety of internet scams. While some of the methods we cover are outdated and no longer work on Facebook, it is entirely likely that they still work on other websites that Facebook users visit.

For this paper, we researched as many methods for hacking Facebook as we could find and how to implement them. We then tested each of them on our own account, using multiple browsers, a virtual machine, and Wireshark. If they didn't work, we researched what had been done to prevent them from working. If they did work, we researched what methods could be used to stop these attacks. While we could not find how to implement all of the methods used throughout Facebook's existence, we believe we covered almost all of them. The following table I describes different methods with their minimum requirements to implement it.

Table I: Different methods with their requirements

METHOD	REQUIRES
SMS Spoofing	Phone, SMS messaging service
Session Hijacking	Wireshark, Firefox, and a cookie editing add-on like Cookie Manager+.
Phishing	A fake Facebook HTML and PHP file, and a web host
Keylogging	FTP server, Keylogger software
Trusted Friends	Two browsers and four to five fake Facebook profiles

First, we will begin with the outdated methods that no longer work and continue with the current working methods after.

IV. SMS Spoofing

The first method we tested, which seemed to be the easiest, was SMS Spoofing. SMS spoofing is using a service to send a "spoofed" SMS message, a message that has a falsified sender address. If this method is still possible in the US, it is extremely difficult. We do believe it is possible in other countries. The most common example we saw was India, but most of the information available on the internet lists Australia and New Zealand as the two easiest countries to mask SMS messages.

Fortunately, masking SMS messages is very difficult in the US. Before Facebook solved this issue, it

was still very easy to target victims in the US. What the hacker would do is start by going to the victim's profile page, and check if there was a phone number listed in their 'About Me' section. If there was, it meant they had signed up for and enabled Facebook texting. Next they would go to an SMS spoofing site, enter in the victim's phone number to appear as the sender's number and one of the Facebook numbers for a country that SMS spoofing is easier in. Then the hacker could enter anything into the message text and when Facebook received that message, the text would become the victim's status update.

Facebook solved this issue, at least in the US, quite gracefully. They simply asked you to specify which country your cellular service is in and the provider, making it so you couldn't update with messages sent to another country's Facebook number.

V. SESSION HIJACKING

The next method tested that did not work was session hijacking through packet capturing. This method captures packets from network traffic and uses the information in them to hijack someone's session with a website. It requires Wireshark, Firefox, and a cookie editing add-on like Cookie Manager+. First, the hacker would ping www.facebook.com to get its IP address.

Next, they would start a capture on Wireshark and filter it by the IP address you received from the ping. You would then search for a HTTP GET packet with '/index.php'. You would then open the packet and find the cookies. There would have been around 8-10 cookies with varying key, value pairs. The hacker would then open Firefox and open the cookie editor. Next, they would copy the key, value pairs into the cookie editor and add each of the cookies. They would then navigate to Facebook and be logged in as the victim.

Shortly before this problem was fixed, an add-on for Firefox was released called Firesheep. Firesheep would essentially do all of this within Firefox. You would turn it on, it would listen and whenever someone log on to certain sites, it would capture the packets and give you the option to go the site they logged in to and to log in as them. Firesheep was claimed to have been created to bring to light the vulnerabilities in not using HTTPS for cookies. Shortly after Firesheeps creation, many sites began to use encrypted cookies to prevent attacks like these, including Facebook.

VI. PHISHING

The first method tried that was successful was phishing. Phishing is attempting to retrieve information such as usernames, passwords, etc. by pretending to be a trustworthy entity in electronic communication. This method is quite easy to implement. It is accomplished by creating a fake Facebook log in site that collects usernames and passwords. This method requires a fake Facebook HTML and PHP file for phishing, and a webhost for the files. First the hacker would get the files you need and upload them to the webhost site. The hacker would then send the phishing link to the victim(s).

The more victims targeted, the higher the likelihood of success. Once the victim clicks the link, they are sent to a page that looks exactly like the Facebook log in page and is prompted to sign in. If the victim falls for this ruse, the phishing site will record the log in information from them and place it into a file with a name along the lines of 'passes.txt'. The hacker then gets the txt file from the webhost and uses the entire collected log in information, usually spreading the phishing link. This method can be easily defended by being careful which links you follow and always checking the URL of any site you are entering log in information into.

VII. KEYLOGGING

The next method we were able to use was keylogging. A keylogger is either a piece of hardware or software that records keystrokes input into a system. This method can be used with either a hardware keylogger or a software keylogger, and we used a software keylogger in our test since, they are free and used most commonly.

Using a software keylogger also requires a FTP server. They are very easy to use and easy to find. First, the hacker would download a keylogger generator. Next, they would give the generator the process name the keylogger will run as, typically 'server.exe' or something else inconspicuous. They would then designate a FTP server for the keylogger to send log files to and what to name the log files. Next they would designate what size the log files should be before the keylogger uploads them. They would then run the generator which will output a 'keylogger.exe' file, which the hacker then renames to something that the victim is likely to open.

Once the victim runs the keylogger executable, it will run in the background under the name designated

by the hacker. It then records all the keystrokes the victim enters until the log file reaches the designated size. The file is then uploaded to the FTP server where it can later be accessed by the hacker at their convenience.

It does all of this without the victim ever seeing the keylogger or knowing it was there. This method is also capable of gathering much more information than just Facebook log in information. It can be used to gain log in information to any site the victim logs into, including banks, to track what they've done searches for and many other purposes. While it's easy to create the keyloggers, they are very easily detectable by the vast majority of anti-viruses, making it unlikely it will even reach many of the victims' computers. In order to even download the keylogger generator, we had to disable my antivirus. Even if the keylogger wasn't detected by an anti-virus, the victim would have to be gullible enough to run an untrustworthy executable file.

Although, we would expect that the people who would go without an anti-virus would also be the people naïve enough to open such a file. This form of attack can be defended against by making sure you have an anti-virus with good reviews with an up to date database and by not opening executable files from sources you don't trust.

VIII. TRUSTED FRIENDS

The last method tested was the 'Trusted Friends' method. This method takes advantage of Facebook's password retrieval system and the victim's willingness to accept friend requests from people they don't know. This method only requires two browsers and four to five fake Facebook profiles. If all goes optimally, only three fake accounts will be needed.

The hacker first makes their fake accounts and attempts to get the victim to accept friend requests from at least three of them. Once the hacker has three accounts on the victim's friend list, they go to the victim's Facebook page and copy the victim's user ID from the URL, (It's the part after 'facebook.com/'). Next, the hacker goes to the Facebook log in page and clicks 'Forgot Password?'.

On the page that loads, the hacker then enters the victim's username and searches it. When it brings up the victim's account with different recovery options, they then click the link 'No longer have access to these?'. Facebook then asks for a new email for verification, which the hacker supplies an email account they have access to. Next Facebook will then either give you the option to 'Recover with the help of trusted friends' or ask for the answer to a security question and will have a link to the "Trusted Friends" option. Once the hacker makes it to this page, they select the three accounts they control as the "trusted friends" and Facebook will send three different verification codes to those accounts. The hacker then uses the second browser to collect the verification codes from the three accounts and enter them into the fields on the first browser. Facebook then sends a verification email to the address the hacker specified and once the hacker activates it, they have full access to the victim's account.

This was probably the most difficult method to complete, especially if we were not targeting our own account. This method would also send far more red flags since the victim's log in information would be changed and they would no longer be able to log in. We have seen fake accounts, which we would assume exist for this purpose, on Facebook very often. A tell-tale sign is an account with an attractive girl for the profile picture, with very few other pictures and friends that are mostly random men from all over. An easy way to protect yourself from an attack like this would be to only accept friend requests from people you know and that would almost completely eliminate the possibility of this kind of attack. If you were paranoid about this kind of attack specifically, you could verify with your friends that the request is them.

If we were actually attempting to use any of these methods to target anyone other than ourselves, we believe the phishing method would be most likely to yield results over the others due to the fact that it would be the easiest to distribute amongst enough people for it to be likely that someone would give their information. The keylogger would be the next easiest since it requires less work, you would simply have to upload it to a file server and make it seem like something people would want to download and just wait for someone without an anti-virus to download and run it.

The "trusted friends" method would most likely be the most difficult to target specific victims. It would however be effective in the scenario we listed earlier. All a hacker would have to do is make multiple fake accounts with attractive women in the profile pictures and spam them to men on the internet. We feel like this would by far have the best results with the "trusted friends" method since men on the internet are more likely to accept a friend request from someone they think is an attractive girl over any other friend request scenario.

As for the outdated methods, we remember when session hijacking was a big problem. It was very

common in cafes or any other network that wasn't password protected and had a lot of different users accessing it at any given time. We remember, Firesheep was released in 2010. Everyone was freaking out because they had just found out about Firesheep. The following table II describes the countries affected by the methods and if Facebook solved the problem and if not what we recommend to solve the given method.

Table II

Method	Countries	Resolved by Facebook	Solution by us
SMS Spoofing	India, Australia, New Zealand masking SMS in US difficult	yes	Already solved
Session Hijacking	Anywhere all over world	use encrypted cookies to prevent attacks	use encrypted cookies to prevent attacks
Phishing	worldwide	_	check the URL
Keylogging	worldwide	_	Keep up to date anti-virus
Trusted Friends	worldwide	_	accept friend requests only from people you know

It wasn't long after that most major websites switched to HTTPS for their authentication cookies. We had never heard of the SMS spoofing method though until it was already fixed on Facebook. That being said, this also would have had immense potential for harassing people and, overall, it's good that it has been solved.

IX. CONCLUSION

In conclusion, Facebook has done their best to protect its users from hackers and people who would gain access to their user's information against the user's will. They have done a very good job with it so far, as all the methods we could find that still worked took advantage of the user and not weaknesses in Facebook itself. While Facebook is doing its best to keep you safe, there are many people out there who are creative and talented at tricking people into giving out their information. Even though our Facebook accounts can almost never be completely safe from a hacker, practicing sensible browsing and common sense on the internet will go a very long way to keep hackers out.

X. DISCLAIMER

The information in this presentation is for instructional purposes only and is intended to inform others of how easily their Facebook account can be hacked and how they can protect themselves. We tested all of these on our own account, on our own computer using multiple browsers and a virtual machine. Please don't try this at home.

REFERENCES

1. Esguerra Richard, "A Handy Facebook-to-English Translator | Electronic Frontier Foundation", April, 2010.
2. Harvey Jones, and Hiram Soltren José, "Facebook: Threats to Privacy", Cambridge, MA, Ethics and Law on the Electronic Frontier, Fall 2005.
3. Jemima Kiss, "Facebook: Did anyone really quit?", Guardian, London, June 2010.
4. Lynch John, Ellickson Jenny, "Computer Crime and Intellectual Property Section, Obtaining and Using Evidence from Social Networking Sites: Facebook, MySpace, LinkedIn, and more", U.S. Dept. of Justice, 2013.
5. Paul Ian, "It's Quit Facebook Day, Are You Leaving?", PC World, May 2010.

6. Semitsu Junichi P., “From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance”, 31 Pace L. Rev. 291, 2011.

7. Stieger Stefan, “Quitting Facebook—What's Behind the New Trend to Leave Social Networks?”, Cyberpsychology, Behavior, and Social Networking Journal, September 2013.

8. Stretch Colin, “Rapport over verzoeken tot gegevensverstrekking van internationale overheden Facebook”, August 2013.

9. Wolens Fred, “Facebook Security Response”, TheIndyChannel, Nov. 2010.

10. Woollacott Emma, “Quit Facebook Day set to be a flop”, TG Daily, May 2010.

11. http://www.merriam-webster.com/dictionary/hacker