How to Hack into Facebook without being a Hacker

Tarun Parwani
Rutgers University
tarun.parwani@rutgers.edu

Ramin Kholoussi
Rutgers University
rk496@rutgers.edu

Panagiotis Karras
Rutgers University
karras@business.rutgers.edu

ABSTRACT

The proliferation of online social networking services has aroused privacy concerns among the general public. The focus of such concerns has typically revolved around providing explicit privacy guarantees to users and letting users take control of the privacy-threatening aspects of their online behavior, so as to ensure that private personal information and materials are not made available to other parties and not used for unintended purposes without the user's consent. As such protective features are usually opt-in, users have to explicitly opt-in for them in order to avoid compromising their privacy. Besides, third-party applications may acquire a user's personal information, but only after they have been granted consent by the user. If we also consider potential network security attacks that intercept or misdirect a user's online communication, it would appear that the discussion of user vulnerability has accurately delimited the ways in which a user may be exposed to privacy threats.

In this paper, we expose and discuss a previously unconsidered avenue by which a user's privacy can be gravely exposed. Using this exploit, we were able to gain complete access to some popular online social network accounts without using any conventional method like phishing, brute force, or trojans. Our attack merely involves a legitimate exploitation of the vulnerability created by the existence of obsolete web-based email addresses. We present the results of an experimental study on the spread that such an attack can reach, and the ethical dilemmas we faced in the process. Last, we outline our suggestions for defense mechanisms that can be employed to enhance online security and thwart the kind of attacks that we expose.

Categories and Subject Descriptors

K.4.0 [**COMPUTERS AND SOCIETY**]: General; K.4.1 [**COMPUTERS AND SOCIETY**]: Public Policy Issues—*Privacy*

Keywords

Online social networking; Facebook; Phishing; Brute Force; Identity; Media

WWW 2013 Companion, May 13–17, 2013, Rio de Janeiro, Brazil.
ACM 978-1-4503-2038-2/13/05.

1. INTRODUCTION

Online social networks such as Orkut, Facebook, MySpace, etc. have gained immense popularity over the recent years. While facilitating communication and interaction among their users, these networking platforms have also raised increasing security and privacy concerns, as malicious users, attackers, or hackers have been attempting to compromise the confidentiality of users' private information and to gain access to other people's accounts in an illegitimate fashion.

For instance, LinkedIn, a popular social networking site for professionals, recently came under attack by Russia-based hackers who publicized the passwords of more than 6.5 million users' accounts [2]. Another related incident occurred in February 2013 when Twitter, a popular micro blogging service, was attacked, compromising the personal information of more than 250,000 users [4] and exposing the vulnerability of all its users.

As of December 2012, there are more than 1 billion monthly active Facebook users [1], which roughly equals one-seventh of the entire human population on our planet. Along with the growth in the number of active users, which has been following an exponential pattern, the size of personal data stored on remote servers is also growing. The immense popularity of such services arises from the fact that it offers an convenient, easy, and reliable manner to maintain contact with friends, relatives, and co-workers, and even reestablish contact with long-lost former classmates, neighbors, and other associates. People who sign up for these services trust the system with their personal information. While public awareness of privacy concerns and vulnerability has been recently growing, many users remain incognizant of the potential for their personal information to be used or compromised by malicious attackers, and, in some cases, the service providers themselves. Academic research has devoted significant efforts in delineating the ways in which users' information can be shared, published, and used in a privacy-preserving manner [7, 6] and to what extent an attacker can exploit bogus accounts in order to gain information [5, 8]. Nevertheless, there has not been a sufficient investigation of the several ways by which malicious adversaries may gain access to other people's accounts.

Online social networking platforms such as Facebook have vulnerabilities, which users should be protected against without compromising the usability of the system. Due to such vulnerabilities, there have been numerous hacking attempts in the past on the website itself, and more such attempts are expected to occur in the future; social networking services constitute a target of malicious users and hackers who are sometimes merely attracted by the mere existence of such vulnerabilities itself. Motivated by this state of affairs, in this paper we study the weaknesses of prevalent social networking services and assess the extent to which they are vulnerable to such online attacks. We decided to focus on the security aspects of Facebook, due to the overwhelming popularity of this particular platform. In the course of our study, we eventually identified a security exploit, which, surprisingly, allows an adversary to gain complete control over a user's Facebook account even *without* entering into hacking activities per se. This identified threat is not limited to Facebook only; the same concept can be applied to any online web service which fulfills certain criteria.

Our exploit is not designed with the intention to target any specific user. Instead, we search for, and exploit the vulnerability of, users who used to possess a web-based email account, which they used in order to sign up when creating their personal account on Facebook in the first place, yet those email accounts have in the meantime expired according to the expiration rules of the web-based service that provided them. This expiration is due to the fact that certain web-based email providers configure the accounts they provide to expire after a certain period of inactivity. Besides, some users may decide to delete their own email accounts without realizing the security threats that this action entails. Such threats arise from the fact that the same web-based email services allow any other willing user to *reactivate* and use the *same* email address which had previously expired, when they sign up. In our study, we found ourselves able to reactivate, and thereby gain control of, such email address accounts; thereafter, using the default password recovery mechanism provided by Facebook, we were also able, in consequence, to gain complete control over Facebook users' private accounts. In effect, the exploit we have identified carries the potential to affect many users with complete loss of control over the personal information.

2. THE ATTACK EXPERIMENT

We started out our study of the Facebook system's security using conventional hacking mechanisms like brute force. We also tried certain social engineering methods such as phishing, so as to see whether people may still fall into these traps. Nevertheless, in the process, we realized the possibility for a remarkably simple exploit which can give us access to a user's complete account and deny access to the same account to that user herself. The potential victims of this exploit are users who have originally created their Facebook accounts using an email address which in the meantime expired due to inactivity.

The exploit arises from the fact that, in order to set up a Facebook account, users are required to provide an email address. While some people opt to use their primary email address to open up an account, others use their least used or rarely used email address. In the case of the latter, the email provider can apply a policy by which email accounts expire after a period of inactivity; examples of such service providers are web-based email services such as Hotmail; in such cases, the user's expired email, and, thereby, their Facebook account as well, are up for grabs. In particular, once an email account has expired due to inactivity, the inactivated email address returns to the pool of *available* addresses; anyone can then legitimately claim such an address when they set up their own web-based email account. As a result, by means of a very simple process of email account reactivation, an email address that has previously belonged to another person can be rendered ours.

The process we have outlined raises a question: How can we detect email accounts that have expired. To facilitate and automate this process, we developed a shell script which checks the MX records on the mail server of any email provider and sends a test email so as to check whether the email is received or not. A failure to deliver the test mail suggests that the email account does not exist on the mail server. The only downside to this approach is that the email address of an individual has to be known and tested manually by the script. Several email providers, such as, in our case, Hotmail, provide an even easier option to find not only one, but a group of expired email accounts. Windows Live Messenger, an instant messaging service provided by Microsoft, allows anyone to import their friends list from Facebook. The records in this imported list are categorized into two groups:

1. People who are currently on Windows Live.
2. People who are not currently on Windows Live.

Membership in the first category signifies that the person in question has already signed up for the Windows Live service; besides, people having a Hotmail accounts are automatically signed up for Windows live. On the other hand, membership in the second category denotes that the person in question does not currently hold an active Windows Live account. Then, in case that person's email is Hotmail email address, we can safely conclude that this email address has expired. We can then proceed to reactivate it ourselves.

Once we have acquired control of a previously expired email address, which had once been used to open up a Facebook account, we can visit Facebook on the web and claim to be the user in question and have forgotten our password. Facebook then promptly sends an email to our reactivated Hotmail email address, which contains a code that allows us to reset the password for the Facebook account in question. All we need to do us copy the submitted code to a designated field on the Facebook site. Once we have done so, we are asked to set a new password. Then the Facebook account in question is all ours, as we are now acting as the legitimate owners of that account. Besides, this process can go on; we can repeat it for every new account that can fall prey to our attack method. Besides, by gaining access to more Facebook accounts, we can automatize the process even further. We can get the friends list of the account that we enter into and figure out which of those friends have expired Hotmail accounts of their turn. Thus, they fall prey to our attack as well. This process can go on in a chain-reaction, branching-out manner, accumulating more and more accounts that we gain access to and deprive the original holders thereof from access to them in the process. The process resembles building a tree iteratively; at each iteration, the tree leaves are the friends of users compromised in the previous iteration; those leaves that can fall prey to our attack are "opened up" and generate children-nodes in the next iteration. This process would only encounter a dead-end when it reaches a point where there are no more vulnerable leaf nodes. We originally speculated that such a state of affairs might be encountered in practice, as users using Facebook accounts with an expired email address might be limited in number and sparsely distributed. However, as we found out in our experiment, such a state of affairs was never reached: We could always detect new accounts that could be compromised at each iteration. We only stopped when we decided to do so on ethical grounds. We found this result to be quite alarming.

3. RESULTS

We visualize the results of our attack experiment by a tree; the internal nodes of the tree correspond to compromised accounts that we have entered into, starting out from an account of ours we originally had access to as the root; the leaves correspond to accounts that were reached as friends and were not compromised, either because they were not vulnerable or because we decided not to pursue the exploit further. We follow a depth-first approach in building the tree, in order to illustrate the fact that out attack can proceed unimpeded across multiple levels at several iterations. Our experiment began with a user having around 760 friends out of which 4 were susceptible to this exploit. In this manner, we were able to gain access to a total of fifteen accounts across six tree levels; the corresponding tree is visualized in Figure 1. While we gained full access to the compromised accounts, we did not manipulate any of their contents. Thereafter, we decided to terminate our exploit as we had already achieved our illustrative proof-of-concept purpose. Pursuing the attack further would merely create problems to more compromised users and raise ethical dilemmas and concerns for us, not to mention potential legal problems. Still, the last node in out attack had more than 2000 friends, 23 of which were vulnerable to our attack. Thus, we saw a significant potential for our attack to be carried along across more iterations.

In Figure 1, $a_{ij}|_k$ denotes the node on the i^{th} level of the tree, j refers to the numbering of nodes on that level, and k refers to the number of vulnerable children nodes which are friends for the parent node. We further use the following notations: NSU denotes a Non-Susceptible User, DNP indicates a path that we Did Not Pursue any further, while CN indicates the Current Node with 23 susceptible friends, at which we decided to discontinue the attack.

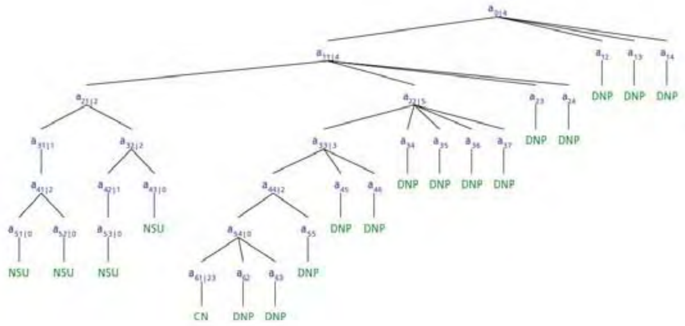

Figure 1: Tree depicting compromised accounts

Overall, we found that up to 2% of a user's friends were generally susceptible to our exploit, with the average value being close to 1%. Thus, for a user with 300 friends, the chances are that 3 of those friends are vulnerable to our exploit. Figure 2 shows the declared locations of the 15 users who accounts we compromised on a world map, using drawing pins. Remarkably, just with a small set of 15 compromised accounts are attack was able to reach world scale.

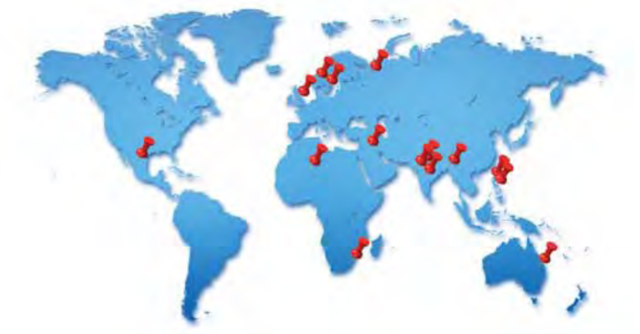

Figure 2: World map with users location

4. DEFENSE MECHANISM

Arguably, Facebook is not the only party to be blamed for the possibility of this exploit. A big portion of the fault lies within Hotmail and its policies. Hotmail is free to set its own rules and policies regarding the expiration of its users' email accounts after a certain period of inactivity. However, such expiration should not lead to a privacy threat for the people concerned by rendering a profile they have created on a social networking website vulnerable to an attack. In short, the problem arises from the fact that the privacy of a user's online social network account rests on the privacy of one's email account. Once the user loses the one, they can lose the other as well.

Facebook can protect users from this exploit. The best method, in our view, would be to eradicate the dependency between Facebook and other service providers, in this case email providers. It is true that resetting a password by means of an activation code sent to the user's email is an old and widespread password resetting method. However, the policies of certain email providers render this method problematic. Facebook can easily generate its own self-contained procedure for password reset that would not rely on third-party dependencies. For example, a method similar to the one used for determining who is tagged in an image could be used. By this procedure, Facebook could present the users with images of different friends they have and ask them to name those present. Yet this method would have its own limitations as some people have thousands of friends out of which they might forget some. Another possibility would be to use an SMS service in combination with the email address procedure. Besides, like several other web-based services do, there could be a security question that would be asked of users who claim to have forgotten their passwords.

Last, as the information stored and shared on Facebook is personal, users themselves should pay more attention to which email addresses they use for identification purposes when they create an account, and maintain those email accounts carefully thereafter. In particular, a user should pay special attention when using an email address provided by an organization having a policy of email account expiration.

5. LIMITATIONS

While our exploit can potentially be quite dangerous, it has its own limitations as well. By our method, an attacker cannot target any specific user. As discussed earlier, only certain users who are vulnerable to this attack can have their accounts compromised. This limitation withholds the choice of whom to pursue from the attacker. Besides, an attack has to be initiated from the attacker's friend list. The attacker has to import her Facebook friend list in her Hotmail account. Once imported, she can follow the leads and repeat this process for the people who are vulnerable to this attack. Thus, only Hotmail and Windows Live users are currently susceptible to this type of attack. Once their Hotmail account becomes inactive, it expires and allows others to claim the email address. To our knowledge, no other popular email account provider currently lets an account expire if not accessed regularly.

The attack we have carried out raises legal and ethical questions. As our intention was only to prove the potential of this exploit rather than maliciously use other people‘s private information, we stopped our pursuit once we attested that we had accumulated sufficient evidence of its practicability. Certainly, techniques such as IP spoofing, using a proxy server, or using a public workstation could significantly reduce the risk of tracing the attack back to its origin. Yet our focus was on illustrating the process rather than taking protective measures and launching a large-scale attack as a hacker would do.

6. LEGAL AND ETHICAL ISSUES

In our exploit, we have been gaining access into accounts and thereby to the friends lists therein. Those friends would later become our next target nodes. Initially, we were thrilled to find out how conveniently we could gain access to other people's accounts. We speculated following the footsteps of Ron Bowes, an information security consultant who collected and published the public data of 100 million Facebook users in 2010. If we had done something similar, it would have shown that very little privacy to talk about is afforded to Facebook users.

Nevertheless, after some careful consideration of the ethical dimensions involved, we decided to settle with only showcasing the possibility of this attack in this paper. Therefore, we stopped our exploration after successfully gaining access to 15 accounts, which we thought sufficed to prove our point. We neither collected nor published any of the personal data we could access. Furthermore we did not change any other recovery settings. Thus, the compromised users could regain access to the account by using their cellphone number or answering their security question. These settings were not modified in any way or form. Indeed, we found out that, after a few days, some of the exploited users had gained back their accounts using these recovery mechanisms. We could have gathered private data hiding behind multiple proxies or secure sockets; we did not do so as we considered how we would have felt if somebody had publicized our private lives to a wide audience, and decided to follow the ethical maxim that we should treat others as we would like to be treated ourselves.

7. CONCLUSION

The growing popularity of Facebook has made it a common target for hackers and attackers. Although such attempts are usually hindered by the high security features of the Facebook system, those that do make their way through can pose a substantial threat to users' online privacy. For research purposes, we attempted to determine the possibility of a quite simple exploit that requires no special hacker skills and credentials. Our results have proven our speculations to be true. We were able to gain total and unlimited control of a user's account merely relying on an expired email account. The underlying reason for the potential of this attack is Hotmail's email account expiration policy in combination with Facebook's policy of allowing a password to by reset by relying merely on a user's given email address. Even though Facebook should not by fully blamed for the possibility of this attack, it could easily prevent it. All they have to do is change their password resetting techniques at least for users having a Hotmail email address. In other words, the password of a Facebook user registered by a Hotmail email address should only be reset by a combination of other techniques, calling for the users to prove their identify via proving the knowledge of the friends they have already connected to, answering one or more security questions, or via a combination of those techniques. Eventually, we conclude that a majority of users who trust social networking websites with their personal information have very little or no control on how this information can be manipulated. Such users need to be more aware of privacy and security threats, as any potential leak may lead to grave consequences. Experience has shown that malicious users who try to crack other people's accounts are quite persistent and usually do end up compromising the users' privacy [3].

8. REFERENCES

[1] 1 billion facebook users on earth: Are we there yet? Online at: http://www.forbes.com/sites/limyunghui/2012/09/30/1-billion-facebook-users-on-earth-are-we-there-yet/.

[2] 2012 LinkedIn hack. Online at: http://en.wikipedia.org/wiki/2012_LinkedIn_hack.

[3] Hackers attempting to crack 600,000 facebook accounts every day. Online at: http://www.dailymail.co.uk/sciencetech/article-2054994/Facebook-hackers-attempting-crack-600-000-accounts-day.html.

[4] Twitter says hackers may have compromised 250,000 accounts. Online at: http://www.forbes.com/sites/andygreenberg/2013/02/01/twitter-says-hackers-may-have-compromised-250000-accounts/.

[5] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In *WWW*, 2007.

[6] Yi Song, Panagiotis Karras, Sadegh Nobari, Giorgos Cheliotis, Mingqiang Xue, and Stéphane Bressan. Discretionary social network data revelation with a user-centric utility guarantee. In *CIKM*, 2012.

[7] Yi Song, Panagiotis Karras, Qian Xiao, and Stéphane Bressan. Sensitive label privacy protection on social network data. In *SSDBM*, 2012.

[8] Mingqiang Xue, Panagiotis Karras, Raissi Chedy, Panos Kalnis, and Hung Keng Pung. Delineating social network data anonymization via random edge perturbation. In *CIKM*, 2012.