Facebook : User Data Harvest through Mobile Number

Zankruti Desai

March 12, 2017

Abstract

In August 2015 a popular social networking site - Facebook was urged to tighten the privacy setting after a Software Engineer was able to harvest details of thousands of users by only their mobile number.

1 Introduction

Facebook, founded on February 4, 2004 was under the scrutiny of media and security experts again. A software Engineer and technical director, Reza Moaiandin, at salt.agency was able to extract information of Facebook users with their mobile numbers. Prior to this there have been many such small incidents where users were able to find details of random people using their mobile number as a source of key. Blogs like SlashDot have local user incidents pertaining to the issue.

2 Background

2.1 What happened?

In August 2015 a Software Engineer and technical blog editor of salt.agency put up an article describing a flaw in Facebook privacy setting. The "Who can find me?" feature of Facebook is by default set to "Everyone/Public" and hence a user can show up in search if their mobile number has been entered in the search space. The mobile number need not be public, numbers made private on a profile can too pull out the information of the user. Reza constructed a simple algorithm that could make combinations of thousands of mobile number. Next he linked the mobile numbers by sending them to Facebook's application programming interface,a tool that allows developers to build applications linked to the social network. This process can be scripted and automated to work through Facebook's API. He got as output ids of the user profile along with URL links of the data for that users. The URL were the direct links which displayed profile pictures - both current and previous of that user. Hackers can communicate with GraphQL, a data querying language created by Facebook, and extract as many details as possible, by passing the hashed ID

2.2 Actions

Before posting the article on the salt.agency blog, Reza had approached Facebook twice informing them about the bug. First, in April 2015, he briefed Facebook about the issue by using their bug-bounty program. A bug bounty program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities. These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. He again informed them about the loophole on July 28,2015.

2.3 Response

Facebook shelved the incident stating that they have implemented measures to block any suspicious behavior. They did not consider this as a security vulnerability and stated that they have controls in place where they can monitor and alleviate such abuses. Further, they insisted that they have strict rules that limit how developers are able to use its API. They claimed to have industry-leading proprietary network monitoring tools constantly running in order to ensure data security.

2.4 Media Outcry and Opinion

The incident portrayed Faceboook in a negative light. Security researcher and analyst considered such privacy loophole as a medium to invite hackers to get a free access to informations of thousands of users. It was stated that Facebook should make it “as difficult as possible” for third parties to scoop up even the publicly shared information belonging to Facebook’s billion users. Moaiandin compared such an incident to walking in a bank and asking details of few thousand customers by providing account numbers of few thousand customers. Various security researcher claimed that many sophisticated spear phishing attacks are based on public information found on Facebook and other social networks and hence the users should choose whether they want to make their phone numbers publicly accessible, rather than that being a default. Sophisticated hackers and black market sellers can access names and mobile phone numbers in as little as an hour through reverse engineering

3 Conclusion

3.1 Suggested implementation for increased privacy

The potential for hackers and black market sellers to discover how to harvest Facebook user data in bulk is reason why Reza urged Facebook to implement pre-encryption to further secure their APIs. This is a second layer of encryption, something that Apple and Google have already implemented. Reza explained that when the Facebook API communications happen, the user ID can be seen in the JSON content. He is suggesting that Facebook encrypt that JSON so that it cannot be read during the communication, decrypting the JSON later so that it is harder for hackers to sniff out Facebook user IDs. Also he suggested that Facebook could limit how much data a single user can extract through the API. If the limit is implemented then extraction of bulk of data could be extracted.

3.2 Similar Incidents - Facebook

On a blogging website SlashDot in January 2013, one user has dictated an incident of similar issue. The user was able to find the details of the location of the person who was harassing her through text messages by searching for the number on Facebook. Although, the loophole here proved beneficial for the user she stated that this loophole could be used for the reverse scenario as well. All mobile numbers have area code as the preceding three or four digits. The malicious user can try combinations of number and could find profile information of users in the nearby area.

Another such incident was reported on a technical blog where a user has tried contacting Facebook reporting them of the loophole when he was able to traverse through profile of unknown users by just inputing a random number and was able to find more information on that users by searching those names on different open information websites.

3.3 Effect

The primary concern here is not here that the information could be found of different users. Since most of the information was already public and Hackers if wanted could take the information directly. The main concern was how easy it was to link contact information with the users. If looked on to them separately a bunch of mobile numbers and a bunch of random information is useless unless there is a way it could be linked. If these type of information were to be available so easily then it would allow hackers to create large databases of Facebook users to be sold to the black market. Concluding there could be no way an information of a user if he has made public could be hidden, the only way a user information could be fully protected is if the user chooses not to publish the information on internet for the world to see and until then no user or no user information is fully protected.

References

Articles from Websites -

1. Facebook urged to tighten privacy settings after harvest of user data(Aug 2015)
https://www.theguardian.com
2. Wanna harvest a stranger's Facebook data? Get a mobile number and off you go(Aug 2015)
https://www.theregister.co.uk
3. Why you should think twice before putting your mobile phone number on Facebook (Aug 2015)
http://www.smh.com.au
4. Facebook hack: Your personal data can be harvested by cyber criminals using your cellphone number(Aug 2015)
https://www.techworm.net
5. Harvest of Facebook user data prompts calls for tighter privacy settings(Aug 2015)
https://www.rawstory.com
6. Facebook Lets You Harvest Account Phone Numbers(Jan 2013)
https://yro.slashdot.org
7. How to stop hackers harvesting your Facebook data(Aug 2015)
http://www.telegraph.co.uk