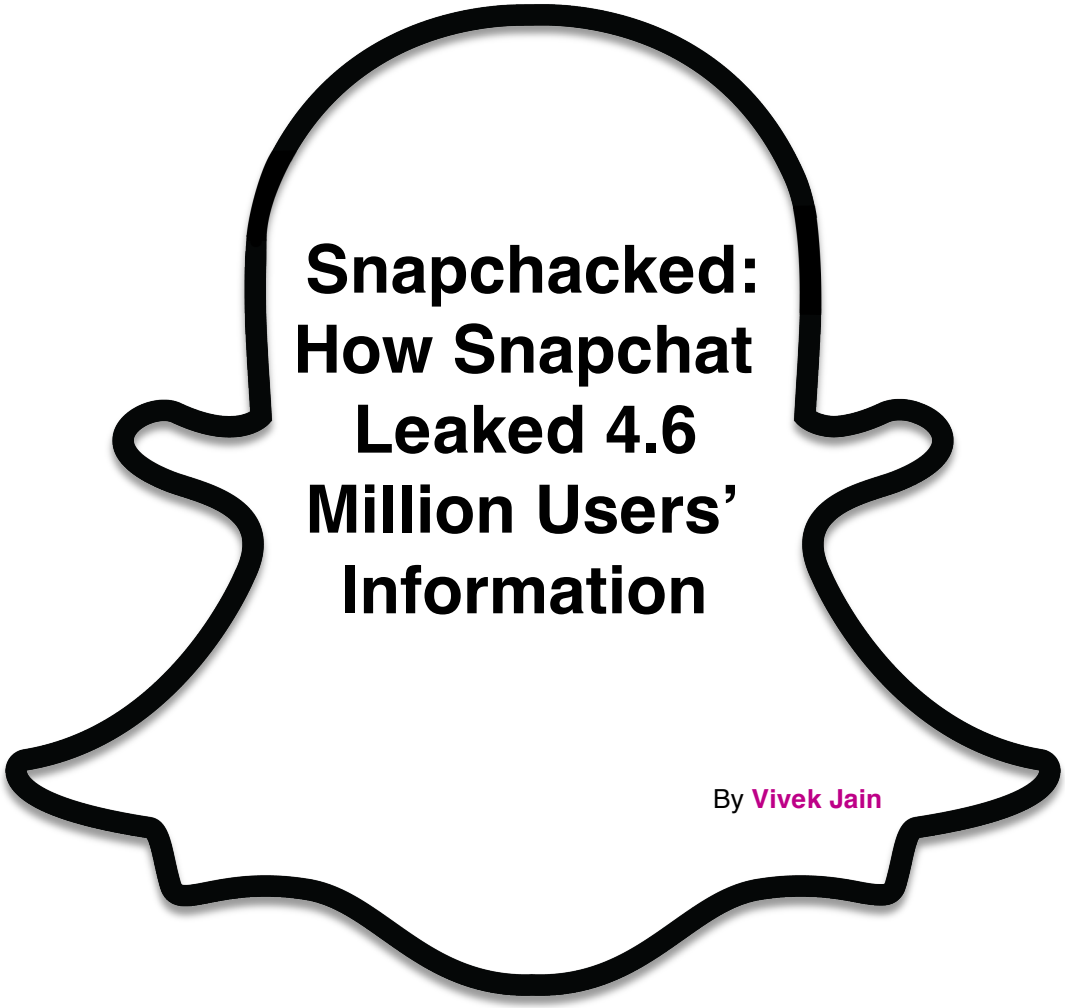

Snapchacked: How Snapchat Leaked 4.6 Million Users' Information

By **Vivek Jain**

If you've been living under a rock for the past year or two and haven't heard of Snapchat, it's the hot new social media app on the block. It is for sending photos and videos, and its claim to fame is that sent items are automatically deleted after a sender-specified number of seconds. In an age where increased sharing over the Internet has led to concerns over our lack of privacy, Snapchat claims to put power back in the hands of users. But can it deliver?

Snapchat's appeal is that you don't have to worry about taking the perfect picture, or think twice about whether posting something will come back to bite you later. While Snapchat can't prevent receivers from simply taking a screenshot on their phone, it does send a notification to the sender if you do so.[1] Snapchat has found a wide variety of use cases, from sexting (sending sexually explicit photographs)[2] to sending potentially embarrassing or incriminating information by Wall Street bankers.[3] In fact, Snapchat is so popular that it refused a $3 billion acquisition offer from Facebook[4] and a $4 billion offer from Google,[5] expecting an even larger valuation in the future.

> **"Snapchat claims to put power back in the hands of users. But can it deliver?"**

However, for a service whose allure is predicated on its (perceived) increased privacy, Snapchat makes no real claims about the security of its system. On January 1, 2013, after a prolonged back and forth between Snapchat and security researchers, an

embarrassing public revelation of the system's weaknesses undermined Snapchat's reputation and raised questions about its valuation. The following is a timeline of events as they unfolded, resulting in the leak of 4.6 million users' usernames and phone numbers.

Prelude

July 27, 2013

Gibson Security, a group of three student security researchers based in Australia,[6] finds several vulnerabilities by reverse-engineering Snapchat's apps. The students "attempted to apply for the Software Developer position [posted on Snapchat's website] saying we would gladly help improve the security and performance of the application, but failed to get a response."[7] It is unclear if, either explicitly or implicitly, their help required Snapchat to hire and pay them.

Exposition

August 27, 2013

After receiving no response, Gibson Security releases details of their exploits to the public.[7] Among other problems, Gibson Security details the weak encryption used by Snapchat and the easy exploitability of Snapchat's Find Friends feature. The Find Friends feature is designed to allow new users to easily find friends who are already using Snapchat. A new user can give Snapchat access to their phone's contacts, and Snapchat uses contacts' phone numbers to find their corresponding Snapchat usernames. Users must also tell Snapchat their own phone numbers, so that others can in turn find them.

"By simply sending every possible mobile number to Snapchat, you can find out the corresponding username for many of its users."

To allow Snapchat's apps to offer this functionality, Snapchat's servers have an API (application programming interface) that specifies how the apps must request the information from the server. In Snapchat's case, that API is not made publicly available, but using tools that are publicly available[8] it is possible to reverse-engineer the API. Snapchat uses *security through obscurity* – Wikipedia defines this as "secrecy of design or implementation to provide security. A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that if the flaws are not known, then attackers will be unlikely to find them." [9] Security through obscurity is frowned upon, since it appears to provide security on the surface, but a determined person may be able to find out how the system works and then easily exploit any vulnerability. This is precisely what Gibson Security did.

For the Find Friends API, you essentially give Snapchat a list of numbers and their corresponding contact names, and Snapchat's servers return to you a list of Snapchat usernames for each phone number that you passed in (full technical details are given in the sidebar on the next page). How can this be exploited? Snapchat places no limits on how many such API requests you can make. By simply sending every possible mobile number to Snapchat, you can find out the corresponding username for many of its users. This is especially pernicious because it doesn't require hacking Snapchat's servers and doesn't require knowing or cracking any user's password.

Furthermore, cross-referencing the Snapchat username with other social media websites (since usernames often reflect someone's real name, and people often use the same username across websites) could be used to build a lot of personal information. This could be used not only for advertising, but also scamming and stalking.

In the conclusion of their release, Gibson Security is somewhat forgiving regarding Snapchat's security (or lack thereof) but at the same time urges Snapchat to fix their problems

Snapchat's Find Friends API:

```
POST https://feelinsonice.appspot.com/ph/find_friends

username=<username>&req_token=<token>&timestamp=<timestamp>&countryCode=US&numbers=%7B%22311-555-4202%22%3A%20%22Kate%20Libby%22%7D
```

feelinsonice.appspot.com is owned by Snapchat. In the body of the request, you specify a username, a token (which is obtained by "lots of voodoo and witchcraft"[7] and was worked out by Gibson Security – but since it is not illustrative, it is left unexplored here), a timestamp (which can actually be arbitrary but must be the same timestamp that was used to create the token), a country code (e.g. "US"), and an encoded JSON dictionary of numbers and their corresponding contact names (the decoded version of the example above is {"311-555-42-2": "Kate Libby"}). In return, Snapchat's servers return to you a list of Snapchat usernames for each phone number that you passed in.

Example response:

```
{
 logged: true,
 results: [{
          type: 0,
          name: "acidburn",
          display: "Kate Libby"
          }]
}
```

and place a greater focus on security. They say that as a startup, Snapchat is likely "to be working under shorter deadlines, which – although it may benefit the business in the short-term – leaves vulnerabilities in the final product to be found (if ever) and exploited by a malicious third party."[7] They recommend future steps for Snapchat, including to "implement internal code guidelines" and "audit your code often, using external services."[7]

"They've had four months, if they can't rewrite ten lines of code in that time they should fire their development team."

Crescendo

December 25, 2013

With Snapchat still not addressing the outlined vulnerabilities, Gibson Security publishes even more details about Snapchat's API and releases code to exploit the Find Friends request. Gibson Security's researchers were able to scan upwards of 10,000 numbers in 7 minutes, and believe that this could easily be improved to 10,000 numbers in 1.5 minutes.[10] Gibson Security also mentions that based on their previous release showing how Snapchat's API works, several public Snapchat clones have been released, some of which allow users to save Snapchat's photos and videos, further undermining Snapchat's supposed privacy and reputation.

In an email exchange with ZDNet, Gibson Security suggests rate limiting (restricting how many requests from a particular user or computer the server responds to) as a basic measure:

> "[Snapchat could have fixed this] by adding rate limiting; Snapchat can limit the speed someone can do this, but until they rewrite the feature, they're vulnerable. They've had four months, if they can't rewrite ten lines of code in that time they should fire their development team. This exploit wouldn't have appeared if they followed best practices and focused on security (which they should be, considering the use cases of the app)."[11]

Development

December 27, 2013

Snapchat publishes a blog post saying that "theoretically" Find Friends is exploitable, but "over the past year we've implemented various safeguards to make it more difficult to do."[12]

Evan Spiegel, CEO of Snapchat. Photo © JD Lasica

SnapchatDB, an anonymous individual or group, a few days later says the exploit "was still functional with very minor modifications."[13]

Climax

January 1, 2014

4.6 million users' usernames and phone numbers are leaked and ma de publicly available by SnapchatDB. They were obtained "through the recently patched Snapchat exploit."[14] Despite Snapchat having patched (fixed) the exploit, SnapchatDB released the information due to dissatisfaction with Snapchat's response.[15] Their site www.snapchatdb.info appears to have since been taken down, as the author had trouble accessing it recently. The last two digits of phone numbers were censored to "minimize spam and abuse."[14]

Diminuendo

January 9, 2014

Snapchat apologizes for the leak and updates its apps to allow opting out of its Find Friends feature.

Denouement

Present

Actual consequences of the leak are unclear. Snapchat is a private company and doesn't release any numbers, so any ramifications, either to Snapchat's users or to Snapchat's reputation and valuation, are just conjecture. With regards to negative consequences to users, none of the Snapchat

users I surveyed said that they had received marketing or suspicious text messages/phone calls since the incident. However, they had noticed an increase in Snapchat spam and friend requests from unknown users. With the combination of usernames released by SnapchatDB and details on Snapchat's API released by Gibson Security, it would be easy to create spam programs that try to add users as friends and then send them advertising. Snapchat itself is aware of the problem, noting in a blog post that they have heard complaints "about an increase in Snap Spam"[16] but believe that it is unrelated to the Find Friends issue.

As for the consequences to the company, Yahoo Finance suggests it could cost the company its life, which was valued by Google at $4 billion. [17] On the other hand, Computerworld suggest consequences are far less dire; teenagers, the primary age group for the app, are "undaunted by security issues like this,"[18] and the cost of the leak to Snapchat is closer to zero. I agree with the latter view. In my survey of Snapchat users, when told about the leak, not a single one said that they would stop using Snapchat as a result. Some respected Snapchat less because of the leak, but that didn't change their usage. The majority of users already knew about the leak. Several believed that usernames and phone numbers weren't something to get "overly concerned about," and others said that they wouldn't use Snapchat to communicate sensitive information. One user compared it to Target's breach (around 100 million users' information, including payment information, was compromised),[19] concluding that such a breach "could happen to anyone." Although Target's breach was far more serious, researchers didn't warn Target four months before the breach occurred.

So it seems reasonable to deduce that the leak didn't have a large impact on existing users of Snapchat. What about future users? Could the leak hamper Snapchat's growth? Again, Snapchat doesn't release growth numbers, so we can't know for sure. Most non-users probably don't even know about the leak, but I set out to find at least anecdotal evidence on this question. I asked people who currently don't use Snapchat whether they would consider using it in the future. I then asked whether the leak of 4.6 million usernames and passwords affected their decision (or made them even more convinced to not use it). Most said the leak wasn't a strong factor in their decision-making. They believed their other reasons (either for or against using Snapchat) were more important, and had a nonchalant attitude towards the leak, similar to the Snapchat users I surveyed.

"Although Target's breach was far more serious, researchers didn't warn Target four months before the breach occurred."

That leaves us with the final question: what should Snapchat and other companies learn from the leak? Not fixing a known, publicly disclosed vulnerability is, in my opinion, inexcusable – they should be more active in dealing with security issues that have been reported to them, and possibly hire security contractors. To assist with this, at the suggestion of Gibson Security, Snapchat has added the security@snapchat.com email address that can be used to contact them about security problems.[20]

But even this simple, small step doesn't seem to be necessary. It seems the leak had little to no negative consequences for Snapchat, and may even have had positive consequences by providing publicity – as the old adage goes, any press is good press. Until and unless users start expecting and demanding greater security, companies have no reason to spend time and money implementing it. We have only ourselves to blame.

Vivek Jain *is a Computer Science student at Stanford University*.

[1] "The Inside Story Of Snapchat: The World's Hottest App Or A $3 Billion Disappearing Act?" 2014. *Forbes*. Accessed January 24. http://www.forbes.com/sites/jjcolao/2014/01/06/the-inside-story-of-snapchat-the-worlds-hottest-app-or-a-3-billion-disappearing-act/.

[2] "Snapchat Breach Exposes Weak Security." 2014. *Bits Blog*. Accessed January 24. http://bits.blogs.nytimes.com/2014/01/02/snapchat-breach-exposes-weak-security/.

[3] Roose, Kevin. 2014. "Wall Street Is Obsessed With Snapchat." *Daily Intelligencer*. Accessed January 24. http://nymag.com/daily/intelligencer/2013/06/wall-street-is-obsessed-with-snapchat.html.

[4] "Snapchat Spurned $3 Billion Acquisition Offer from Facebook - Digits - WSJ." 2014. Accessed January 24. http://blogs.wsj.com/digits/2013/11/13/snapchat-spurned-3-billion-acquisition-offer-from-facebook/.

[5] "Google Reportedly Tried to Outbid Facebook for Snapchat with $4 Billion Offer." 2014. *The Verge*. Accessed January 24. http://www.theverge.com/2013/11/15/5106950/google-snapchat-4-billion-buyout-rumor.

[6] "FAQ - GSFD." 2014. Accessed January 24. http://gibsonsec.org/faq/.

[7] "Snapchat Security Disclosure - Gibson Security." 2014. Accessed January 24. http://gibsonsec.org/snapchat/.

[8] "Neuebits | [WIP] Snapchat API." 2014. Accessed January 24. http://neuebits.com/snapchat/.

[9] "Security through Obscurity." 2013. *Wikipedia, the Free Encyclopedia*. http://en.wikipedia.org/w/index.php?title=Security_through_obscurity&oldid=588125312.

[10] "Snapchat - GSFD." 2014. Accessed January 24. http://gibsonsec.org/snapchat/fulldisclosure/.

[11] 25, Violet Blue for Zero Day | December, and 2013-- 01:13 Gmt. 2014. "Researchers Publish Snapchat Code Allowing Phone Number Matching after Exploit Disclosures Ignored." *ZDNet*. Accessed January 24. http://www.zdnet.com/researchers-publish-snapchat-code-allowing-phone-number-matching-after-exploit-disclosures-ignored-7000024629/.

[12] "Finding Friends with Phone Numbers." 2014. Accessed January 24. http://blog.snapchat.com/post/71353347590/finding-friends-with-phone-numbers.

[13] Jackson, Rusty Foster and Benjamin. 2014. "Anatomy of a Snap Attack." *The New Yorker Blogs*. http://www.newyorker.com/online/blogs/elements/2014/01/the-attack-on-snapchat.html.

[14] "SnapchatDB!" 2014. Accessed January 24. http://www.snapchatdb.info/.

[15] "4.6 Million Snapchat Phone Numbers and Usernames Leaked." 2014. *The Verge*. Accessed January 24. http://www.theverge.com/2014/1/1/5262740/4-6-million-snapchat-phone-numbers-and-usernames-leaked.

[16] "Snap Spam Update." 2014. Accessed January 24. http://blog.snapchat.com/post/73216178814/snap-spam-update.

[17] "Snapchat Hack May Have Just Cost the Company Founder $4 Billion." 2014. *Yahoo Finance*. Accessed January 24. http://finance.yahoo.com/blogs/breakout/snapchat-hack-may-have-just-cost-the-company-founder--4-billion-155733225.html.

[18] "Will Teens Be Scared off by Snapchat Hack? Probably Not." 2014. *Computerworld*. January 2. http://www.computerworld.com/s/article/9245123/Will_teens_be_scared_off_by_Snapchat_hack_Probably_not.

[19] Harris, Elizabeth A., and Nicole Perlroth. 2014. "For Target, the Breach Numbers Grow." *The New York Times*, January 10. http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

[20] "The Hackers Who Revealed Snapchat's Security Flaws Received One Response From The Company...Four Months Later." 2014. *Forbes*. Accessed January 24. http://www.forbes.com/sites/jjcolao/2014/01/02/the-hackers-who-revealed-snapchats-security-flaws-received-one-response-from-the-company-four-months-later/.