Hello, Facebook! Here Is the Stalkers' Paradise!: Design and Analysis of Enumeration Attack Using Phone Numbers on Facebook

Jinwoo Kim[1], Kuyju Kim[1], Junsung Cho[1], Hyoungshick Kim[1(✉)], and Sebastian Schrittwieser[2]

[1] Sungkyunkwan University, Seoul, Republic of Korea
{jinwookim,kuyjukim,js.cho,hyoung}@skku.edu
[2] Josef Ressel Center for Unified Threat Intelligence on Targeted Attacks, St. Pölten University of Applied Sciences, Sankt Pölten, Austria
sebastian.schrittwieser@fhstp.ac.at

Abstract. We introduce a new privacy issue on Facebook. We were motivated by the Facebook's search option, which exposes a user profile with his or her phone number. Based on this search option, we developed a method to automatically collect Facebook users' personal data (e.g., phone number, location and birthday) by enumerating the possibly almost entire phone number range for the target area. To show the feasibility, we launched attacks for targeting the users who live in two specific regions (United States and South Korea) by mimicking real users' search activities with three sybil accounts. Despite Facebook's best efforts to stop such attempts from crawling users' data with several security practices, 214,705 phone numbers were successfully tested and 25,518 actual users' personal data were obtained within 15 days in California, United States; 215,679 phone numbers were also tested and 56,564 actual users' personal data were obtained in South Korea. To prevent such attacks, we recommend several practical defense mechanisms.

Keywords: Enumeration attack · Information leakage
User profile · Privacy · Facebook

1 Introduction

Facebook (https://www.facebook.com/) is one of the most popular online social networking service and reported more than 1.94 billion monthly active users for March 2017 [1]. Due to its popularity, Facebook has also become an attractive target of cyber criminals (spam, phishing, and misuse of personal data). For example, spammers have often used tools and bots for harvesting people's contact information (e.g., phone numbers and email addresses) in the past [8].

In this paper, we particularly focus on security concerns raised by the friend search option with phone numbers in Facebook. Facebook offers various options for searching registered users. An option is to use a user's phone number. At first

J. K. Liu and P. Samarati (Eds.): ISPEC 2017, LNCS 10701, pp. 663–677, 2017.
https://doi.org/10.1007/978-3-319-72359-4_41

glance, this search option seems to be a proper compromise between privacy and utility, revealing a user's profile for his or her friends or acquaintances who only know the user's phone number. In this paper, however, we will show that this feature could potentially be misused by attackers who want to harvest Facebook users' data such as their names, phone numbers, locations, education and even photos at large scale; those stolen data can be exploited for conducting additional cyber criminal activities such as sending spam/phishing messages or creating sybil accounts. To show the security risk of the search option, we developed a method to automatically collect Facebook users' personal data (phone number, friends, current city, home town, education, family, work and relationship) by enumerating the (possibly) entire phone number range of a target area. Our main contributions are summarized as follows:

- We present a novel *enumeration* attack using the search option to enumerate entire phone number ranges to harvest Facebook users' profile information in an automatic manner at large scale (see Sect. 3).
- We describe how to bypass the defense mechanisms such as anomaly detection and CAPTCHAs provided by Facebook. We implemented an automated crawling process with a few sybil accounts to mimic normal users' activities (see Sect. 4).
- We provide a thorough evaluation of the practicality of the enumeration attack. Our evaluation is based on experiments on the actual Facebook service. In our experiments, we collected 25,518 Facebook user profiles from 214,705 phone numbers within 15 days in California, United States. Also, we collected 56,564 Facebook user profiles from 215,679 phone numbers in South Korea (see Sect. 5).
- We suggest possible defense mechanisms to mitigate such enumeration attacks and discuss their advantages and disadvantages (see Sect. 6).

While our evaluation is Facebook-specific, it could also offer important lessons for other websites which use the people search feature by phone number or email address.

2 Facebook's Profile Search

To encourage users to find their friends and acquaintances (i.e., promotional purposes), Facebook provides several options to search for people on Facebook (e.g., by name, email address, or phone number). For example, when a phone number is typed into the Facebook search bar, the results from people who registered that phone number will be displayed if the default privacy setting for the search option was not changed. We found that for a Facebook profile the default setting for the option to search for users their phone numbers is "`Everyone`", which means that anyone could use this feature to find that specific profile (see Fig. 1). Interestingly, even if users hide their phone numbers in profile page, they can still be searched with their phone numbers if this option is not disabled manually.

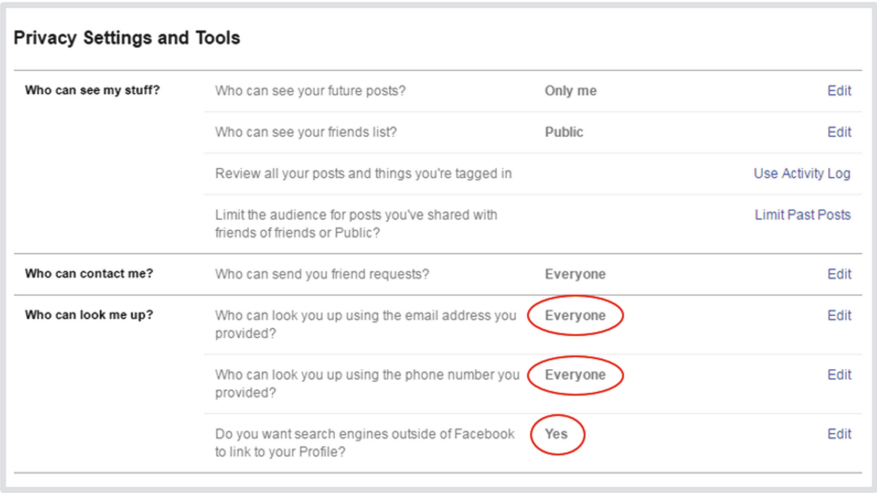
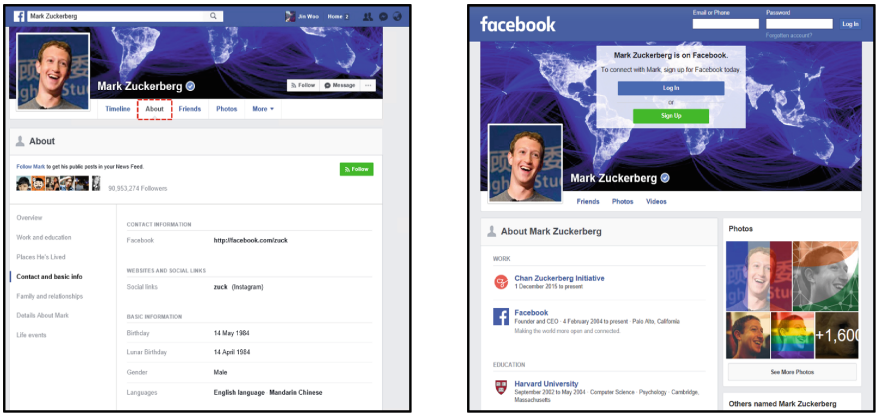


Fig. 1. Privacy setting options in Facebook.



(a) Logged in (b) Not logged in

Fig. 2. People search results ("Logged in" vs. "Not logged in").

We will exploit this feature to develop a method for performing enumeration attacks on Facebook.

We also found that the user profile information (e.g., work, education, and location) significantly changes depending on whether we are logged in or not. Figure 2 shows the differences between logged in and not logged in. When we are logged in and then try to search for a user, the search results for the user include the section called `About` which displays the detailed information about the user (e.g., the link to other services such as `Instagram`, birthday, gender, relationship

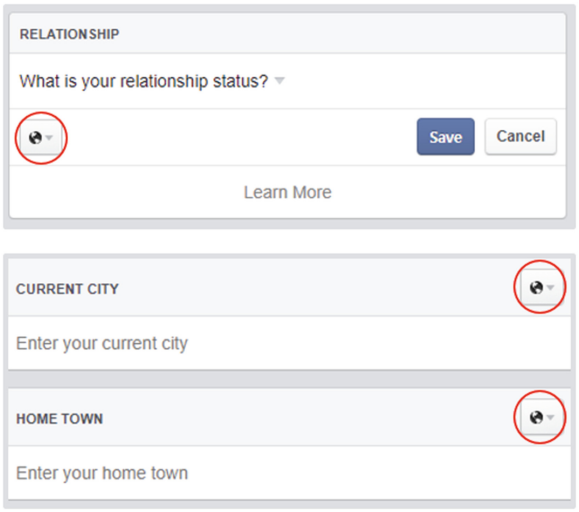


Fig. 3. Privacy settings for relationship, current city and home town in Facebook.

with the user's partner, family members, life events, etc.) (see Fig. 2(a)). To make matters worse, such personal information can be exposed to the public eye by default (see Fig. 3). In this figure, the globe icon denotes `public`. However, this section is disappeared when we are not logged in (see Fig. 2(b)). Therefore, we would perform enumeration attacks under logged in Facebook user. Each step is described in detail in the following sections.

3 Overview of Enumeration Attack Using the People Search with Phone Numbers

In this section, we present the overview of an enumeration attack to *automatically* harvest user profile data using the search feature provided by Facebook. The proposed enumeration attack involves the following three steps: (i) enumerating target phone numbers in a random or sequential order; (ii) checking whether the search results (including the user profile) are successfully returned; (iii) extracting the interesting user data from the crawled user profile web page if valid search results were returned.

To conduct the enumeration attack using the people search with phone numbers, an attacker first generates a range of phone numbers in a valid format and tries to search for people with that number. The phone numbers used for the enumeration attack can be generated for a specific target area. For example, the country code is 1 for United States; and the area codes are {209, 213, 279, 310, 323 $\cdots$} for California. If the attacker wants to collect the information about Californian users, the generated phone number format would look like `+1209XXXXXXX`.

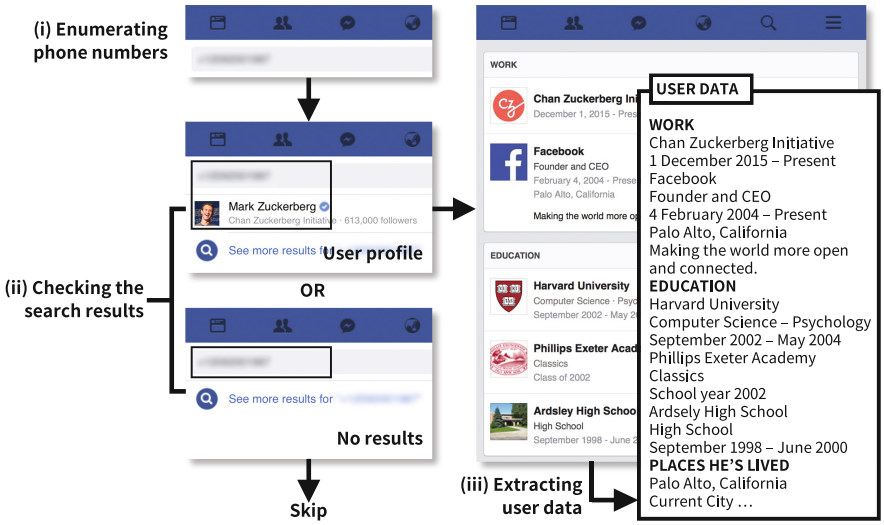


Fig. 4. Overview of the enumeration attack using the people search with phone numbers.

As described in Sect. 2, Facebook allows users to search for people with his or her phone number. Our method performs the following procedure repeatedly (see Fig. 4):

1. An attacker signs into Facebook using a sybil account. We note that a sybil account for Facebook can simply be created by a temporary email service in an automatic manner.
2. The attacker generates a phone number from a range of phone numbers in a valid format (e.g., `010XXXXXXXX`, `+1209XXXXXXX`) and tries to search for people with that phone number on Facebook.
3. If the search results are successfully returned, the web page for user profile is crawled; otherwise, this step is skipped.
4. After the crawled web page is parsed appropriately, the user data extracted from that web page and the phone number used are stored as the output of the attack.

As a result of this attack, an attacker can harvest victims' personal data (such as phone number, name, education level, the place user are living, etc.).

Facebook is already using several defense mechanisms to protect user data from web crawling attempts. As an example, if an unusual or suspicious activity is detected, Facebook displays the "Security Check" error message, and asks the user to solve a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) [3] problem as shown in Fig. 5.

This policy seems effective against such enumeration attacks or web crawling. However, we found that this anomaly detection can be bypassed by using a few

Fig. 5. Example of CAPTCHA used in Facebook.

sybil accounts and performing attack attempts with an intentional delay. In the next section, we will explain how defense mechanisms can effectively be bypassed.

4 Evading Anomaly Detection by Mimicking Normal User Activities

In practice, a naive approach for the enumeration attack is not working. Our simple attempt failed to continuously operate the attack procedure described in Sect. 3 even when we signed in to our *normal* Facebook account. When the attack procedure was repeated around 300 times, a CAPTCHA challenge was displayed.

Unsurprisingly, the best strategy is to mimic normal user behavior by sending only a small number of search requests to evade the anomaly detection solution used by Facebook. In this case, however, the attack efficiency can be degraded significantly. To overcome this drawback, our key idea is to use multiple independent sessions to mimic multiple users' search activities rather than a single user alone.

To do this, we need to generate k temporary accounts before performing the attack procedure. We launch the attack with the first account. After repeating the user search procedure t times with the first account for as long as possible, we switch to the second account and continue this process. We note that the first account is used again after the kth account was used. Figure 6 illustrates this process visually. As shown in this figure, the attacker tries to search t consecutive phone numbers with an account (e.g., phone numbers $i, i+1, \cdots, i+(t-1)$ with account 1) and switches to another account.

It is important to use appropriate k and t for efficiently evading the anomaly detection used by Facebook. For example, if t is too large, the attack attempt can still be detected; if t is too small, switching cost will be higher. Those parameter values were determined experimentally with a small number of test samples. In Sect. 5, we will discuss how to choose proper k and t.

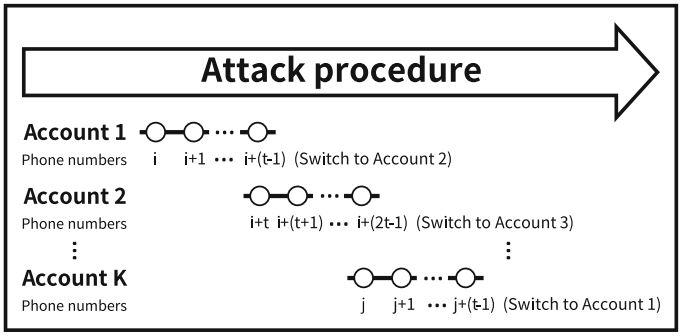


Fig. 6. Enumeration attack with k sybil accounts.

5 Experiments

We implemented a tool for performing enumeration attacks described in Sect. 3 to show the feasibility against Facebook and evaluate its attack performance in a real-world environment.

5.1 Implementation

For the enumeration attack via phone number search in Facebook, we used a virtual machine (VMware Workstation 12.0.0) installed on an Ubuntu 16.04 LTS desktop computer (with two 2.7 GHz CPU and 2.4 GB RAM) and equipped with a non-congested 100 MB WiFi connection to a LAN that was connected to the Internet. In addition, we used the software-testing framework `Selenium` (http://www.seleniumhq.org/) to automate our enumeration attack attempts.

It is important to choose optimal parameter values for k and t that maximize the attack performance without incurring significant costs for creating k sybil accounts and maintaining them. To practically determine the optimal threshold for the enumeration attack, we used 50 Facebook accounts as the training dataset. For each account, we counted the number of friend search requests until a CAPTCHA challenge was displayed.

Figure 7 shows the number of requests, and the mean, median and minimum values, which were 392.4 (with the standard deviation of 102.44), 366 and 300, respectively. Based on this evaluation, we selected $t = 300$ as a more conservative threshold value because 300 was the worst case in our test samples.

To minimize the cost of managing sybil accounts, it will be preferred to find the smallest k that can evade the anomaly detection mechanism. To do this, we simply tested possible k until CAPTCHA challenges were not displayed. We found that the proposed enumeration attack can be successfully performed without any delay when $k = 3$. To use fewer accounts for attack, additional delays are required between the enumeration attacks of each account. But, this delay can slow down the crawling speed.

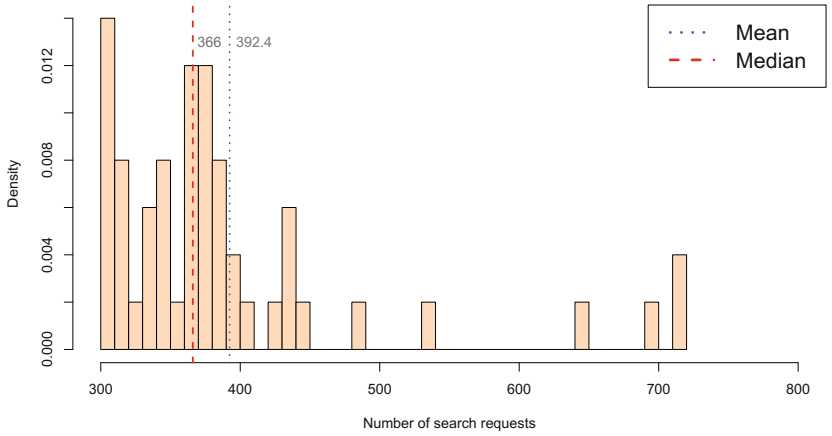


Fig. 7. Number of search requests until a CAPTCHA challenge is displayed.

We note that 300 people search operations took about 35 min on average. Thus, each account would be reused every 70 min on average. In fact, we surmise that Facebook might count the number of search operations within a specific time interval (e.g., 70 min) and then try to block additional requests if the counted number is greater than a pre-determined threshold (e.g., 300).

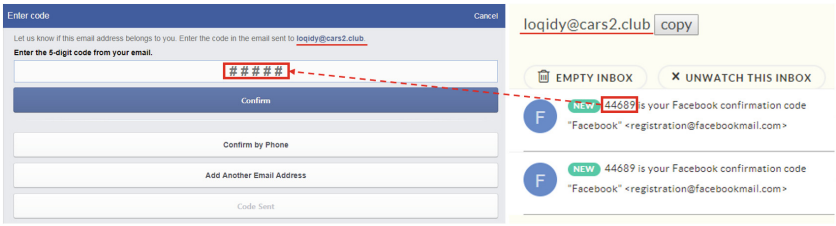


Fig. 8. Example of using a temporary email address for creating a sybil account on Facebook.

In Facebook, either email verification or phone verification is required for creating user accounts as a defense against bulk account creation. However, we figured out that this verification process does not pose a real challenge to attackers because account registration can be fully automated. Attackers can use a temporary email service such as `nada` (https://getnada.com/). Figure 8 shows an example of using a temporary email address for creating a sybil account on Facebook.

Even though Facebook does not allow users to create multiple accounts by checking their operating system and network environment and asking them to complete a security check if the same environment is used more than twice for

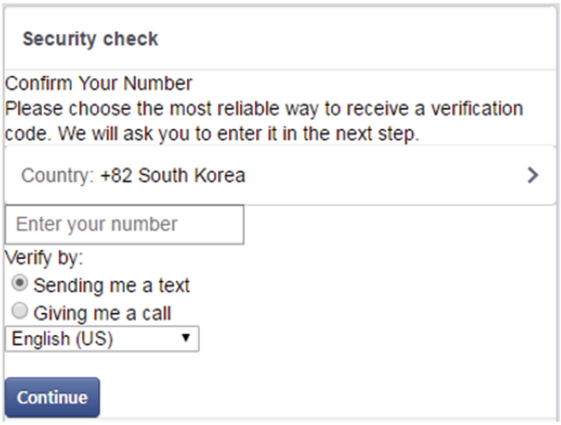


Fig. 9. Security check alert for multiple user accounts at a single machine.

creating user accounts (see Fig. 9) this restriction can also be evaded using a *rooted* Android mobile phone and a VPN connection. Whenever creating an account on Facebook, attackers can simulate a new target device by changing Android ID, International Mobile Equipment Identity (IMEI) and IP address in order to disable the security Facebook's check feature.

With this implementation, we successfully performed automated enumeration attacks without any challenges from Facebook. The experiment results are presented in the next section.

5.2 Attack Results

To show the feasibility of the enumeration attack on Facebook, we performed enumeration attacks to collect user profile data in California, United States and South Korea, respectively. The mean time required for extracting a user profile was 4.78 s if the search results were successfully returned; otherwise, the mean time to process "`no search results`" was 6.49 s on average. For California, we particularly tested 214,705 phone numbers for 15 days and confirmed 25,518 (11.89%) valid user profiles from those phone numbers. For South Korea, we also tested 215,679 phone numbers for the same time period and confirmed 56,564 (26.23%) valid user profiles from those numbers. Those results demonstrate that the enumeration attack using phone numbers was significantly more effective in South Korea than California, United States. We surmise that Korean users' phone numbers were likely to be denser than California users' phone numbers in Facebook. Table 1 shows the statistics for the collected user profiles. We found that several types of personal information (phone number, friends, current city, home town, education, family, work and relationship) can be accessed easily through user profiles collected by the enumeration attack developed here. From the collected user profiles using phone numbers (25,518 and 56,564 user profiles for California and South Korea, respectively), most users did not protect

Table 1. Summary of the collected users' personal data.

Region	Phone number	Friends	Current city	Home town	Education	Family	Work	Relationship
California	25,518	18,080	12,205	11,470	9,703	7,849	7,354	7,279
South Korea	56,564	42,379	25,555	22,594	20,126	3,952	13,580	8,940

their friend list information (70.9% of the California users and 74.9% of the Korean users, respectively). The location information (current city and home town) was the second most publicly accessible information; 44.9%–47.8% of the users revealed their current location and/or home town information. The users' education history was also frequently included in the collected user profiles (38.0% of the California users and 35.6% of the Korean users, respectively). Users' work information was often revealed via their user profiles (28.8% of the California users and 24.0% of the Korean users, respectively). Interestingly, California users' profiles quite frequently include the family and relationship information (30.8% of the California users for family and 28.5% of the California users for relationship, respectively) while this information was included less frequently in the Korean user profiles (only 7.0% of the Korean users for family and 15.8% of the Korean users for relationship, respectively). This implies that Korean users are expected to be more concerned about their family members and partners compared with California users. In a targeted attack scenario, such private data might be used to design sophisticated spam, spear phishing [10], or profile cloning attacks [5].

6 Countermeasures

In this section, we describe several defense mechanisms for preventing enumeration attacks on online social networking services.

6.1 Detecting Sequential Patterns of Queried Phone Numbers

An enumeration attack tries to automatically collect user information by enumerating the target phone numbers. Since the proposed enumeration attacks are performed with multiple user accounts, it might not be easy to detect suspicious patterns from a user account during a session. Our strategy is to uncover sequential patterns from enumerated phone numbers instead of focusing on user activities because phone numbers are sequentially queried from the target phone number range even with multiple user accounts.

However, attackers may effectively avoid this detection method without incurring significant additional costs by using a random permutation list (with some delay) instead of a sequential phone number order.

6.2 Deploying Honey Phone Numbers

"Honey" is the traditional term used to indicate a "decoy" or "bait" for attackers in the field of security. For example, a honeypot is a security resource, which is intended to be attacked and compromised to gain more information about an attacker [22]. Also, the technique called "honeyword" was proposed by Juels et al. [12] to detect password theft against hashed password databases.

To mitigate enumeration attacks, we suggest a novel technique called "honey phone numbers" to detect attacks against the people search with phone numbers. The system generates a large set of fake users having nonexistent phone numbers which cannot be distinguishable from real phone numbers to deceive attackers that automatically perform enumeration attacks on those phone numbers. Probably, a normal user would not try to use such nonexistent phone numbers to search for his or her friends while an attacker might try to enumerate phone numbers including honey phone numbers. Therefore, if a significant number of search requests arrive within a short period of time, this might be an unusual event for normal users and could be an evidence of enumeration attack against the friend search feature in Facebook.

6.3 Using Advanced Device Fingerprinting Techniques

Facebook already deployed security techniques that can make it difficult for attackers to create sybil accounts and use them to crawl data. However, current techniques are not sufficient to detect abusive activities used for enumeration attacks. As discussed in Sect. 5.1, email verification can be bypassed by using temporary email accounts; IP address can easily be changed by using VPN services; and device identities (e.g., UUID, IMEI or MAC address) can also be changed.

One way to overcome this limitation of existing device identification is to use some inherent characteristics of a device or web browser, which are usually hard to change. For example, web browsing history [20], network measurements [14], canvas fingerprinting [2], acoustic fingerprinting [24], plugins and fonts [17]. With some of those techniques, service providers could monitor a suspicious user (or browser) and track his or her activities. Using such advanced device (or browser) fingerprinting techniques would lead to significant cost increases of attackers.

However, those fingerprinting techniques may also raise privacy concerns because all Facebook users' activities can be tracked.

6.4 Changing the Default Privacy Settings

Even though Facebook allows users to opt-out of making their profile *searchable* using phone numbers or email addresses (see Fig. 1), users rarely change their privacy settings from the default [16]. Probably, this is an interesting feature to increase the number of users and/or friend relationships on Facebook. However, as we described in this paper, this feature now can be used for enumeration attacks. Therefore, Facebook should consider making the default privacy settings more restrictive.

6.5 Blacklisting Service Providers for Temporary Email Services

To perform the enumeration attack described in this paper, several sybil accounts must be created. In Sect. 5, we show that temporary email addresses are allowed to create these sybil accounts.

To protect the service against the described attacks using sybil accounts, Facebook needs to set more strict security policies (i.e., disallowing users to use temporary email addresses for user account creation).

However, it is likely to degrade the usability of the user account creation process because it allows email addresses from specific domains only. To make matters worse, there exist professional account generators for trustworthy email addresses (e.g., Gmail). Hence, Facebook needs to carefully blacklist email servers to effectively block sybil accounts while minimizing negative effects on normal users.

7 Ethical Issues

The main motivation of our experiments is not to obtain personal information data or to use collected data for commercial or illegal purposes. Instead, we developed a method to show the risk of enumeration attacks on Facebook and introduced reasonable countermeasures to mitigate such attacks. Therefore, we only checked Facebook's responses for our enumeration attack attempts; however, actual user data were not stored.

Finally, we reported the discovered design flaws to Facebook, which acknowledged them.

8 Related Work

Since a huge amount of user data is shared on social network services such as Facebook, Twitter, Google+ and YouTube, user privacy is becoming ever more important in using those services. Naturally, privacy concerns about user data on social network services were often discussed. Gross et al. [9] showed that user profiles in social network services could be misused to violate people's privacy if proper measures are not taken. They observed that 77.7% of users were stalked because of the disclosure of their profiles. Zheleva and Getoor [23] showed the risk of inferring social network users' private information from their user profiles in four social network services (Facebook, Flickr, Dogster and BibSonomy). Mahmood et al. [18] demonstrated several privacy leaks on Facebook and Twitter. For example, they showed that users' email addresses can be mapped to their real names using the Facebook's user password recovery service in Facebook. Backstrom et al. [4] introduced deanonymization attacks against an anonymized graph using the social graph mining where true node identities are replaced with pseudonyms. Mislove et al. [19] also showed that certain user profile attributes can be inferred with a high accuracy using the social network community structure. To prevent such inference attacks, Heatherly et al. [11] proposed three

possible defense techniques and evaluated their effectiveness. Bonneau et al. [6] demonstrated that an approximation of a social graph can be used to infer users' several sensitive properties on Facebook. Kim et al. [15] explored several sampling techniques to hide the structure of original social graph against such inference attacks.

The strategy of this attack is not new. There were several studies to design enumeration attacks. For instant messenger applications such as WhatsApp, Viber and Tango, Schrittwieser et al. [21] introduced an enumeration attack to collect active phone numbers. They showed the feasibility of the attack by collecting 21,095 valid phone numbers that are using the WhatsApp application within less than 2.5 h. Kim et al. [13] performed an enumeration attack against Kakaotalk by collecting 50,567 users' personal information (e.g., users' phone numbers, display names and profile pictures). They also proposed three possible defense strategies to mitigate enumeration attacks.

A similar problem related to enumeration attack was already reported in social network services. Balduzzi et al. [5] showed the feasibility of an enumeration attack that automatically queries about e-mail addresses to collect a list of valid e-mail addresses by uploading them to the friend-finder feature of Facebook. Based on the return value of Facebook, they were able to determine the status of an email address. They tested about 10.4 million e-mail addresses and identified more than 1.2 million user profiles associated with these addresses. After they reported the discovered design flaw, Facebook fixed this problem by limiting the number of search requests that a single user can perform. This seems a reasonable security practice because there is no normal user who submitted a million search queries within a short time interval. In this paper, however, we show that enumeration attacks can still be performed on Facebook by mimicking multiple users' search activities with a few sybil accounts.

Bonneau et al. [7] already showed that user accounts can be created anonymously by using temporary email accounts and an anonymous networking technique such as Tor (https://www.torproject.org/). To prevent such user account creation, Facebook already tried to check not only the network identity (e.g., IP address) but also the device identity (e.g., IMEI). In this paper, however, we demonstrate that this procedure can be evaded easily with a rooted Android mobile phone.

9 Conclusion

This paper analyzed a security issue in the people search functionality provided by Facebook, which is the most popular social networking service worldwide. The people search functionality with phone numbers could potentially be misused to leak user's sensitive personal data on a large scale. Based on this feature, we developed a method to automatically collect Facebook users' personal data by enumerating all the valid phone numbers for a target area. To show its feasibility, we implemented an attack for targeting users from in two specific regions (United States and South Korea) by mimicking a real users' search activities with three

sybil accounts. Our implementation can evade the Facebook's defense mechanisms; 215,679 South Korean phone numbers were tested and data from 56,564 user profiles was collected in within 15 days; during the same time period 214,705 US phone numbers were tested and data from 25,518 user profiles was collected.

To mitigate such automated enumeration attacks, we suggest five possible defense mechanisms: (1) detecting sequential patterns of queried phone numbers; (2) identifying enumeration attacks with faked phone numbers; (3) using advanced device fingerprinting techniques; (4) changing the default privacy settings and (5) blacklisting service providers for temporary email services. As part of future work, we plan to implement those mechanisms and evaluate their performance against our attacks.

Acknowledgments. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03030627), and the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Promotion). The financial support by the Austrian Federal Ministry of Science, Research and Economy and the National Foundation for Research, Technology and Development is gratefully acknowledged. The authors would like to thank all the anonymous reviewers for their valuable feedback.

References

1. Number of monthly active Facebook users worldwide as of 1st quarter 2017 (The Statistics Portal, statista). https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
2. Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., Diaz, C.: The Web never forgets: persistent tracking mechanisms in the wild. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (2014)
3. von Ahn, L., Blum, M., Hopper, N.J., Langford, J.: CAPTCHA: using hard AI problems for security. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 294–311. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_18
4. Backstrom, L., Dwork, C., Kleinberg, J.: Wherefore art Thou R3579x?: anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of the 16th International Conference on World Wide Web (2007)
5. Balduzzi, M., Platzer, C., Holz, T., Kirda, E., Balzarotti, D., Kruegel, C.: Abusing social networks for automated user profiling. In: Jha, S., Sommer, R., Kreibich, C. (eds.) RAID 2010. LNCS, vol. 6307, pp. 422–441. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15512-3_22
6. Bonneau, J., Anderson, J., Anderson, R., Stajano, F.: Eight friends are enough: social graph approximation via public listings. In: Proceedings of the 2nd ACM EuroSys Workshop on Social Network Systems (2009)
7. Bonneau, J., Anderson, J., Danezis, G.: Prying data out of a social network. In: Proceedings of the International Conference on Advances in Social Network Analysis and Mining (2009)

8. Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., Zhao, B.Y.: Detecting and characterizing social spam campaigns. In: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement (2010)
9. Gross, R., Acquisti, A.: Information revelation and privacy in online social networks. In: Proceedings of the ACM Workshop on Privacy in the Electronic Society (2005)
10. Halevi, T., Lewis, J., Memon, N.D.: Phishing, personality traits and Facebook. Social Science Research Network (2015)
11. Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: Preventing private information inference attacks on social networks. IEEE Trans. Knowl. Data Eng. **25**(8), 1849–1862 (2013)
12. Juels, A., Rivest, R.L.: Honeywords: making password-cracking detectable. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (2013)
13. Kim, E., Park, K., Kim, H., Song, J.: Design and analysis of enumeration attacks on finding friends with phone numbers: a case study with KakaoTalk. Comput. Secur. **52**, 267–275 (2015)
14. Kim, H., Huh, J.H.: Detecting DNS-poisoning-based phishing attacks from their network performance characteristics. Electron. Lett. **47**(11), 656–658 (2011)
15. Kim, H., Bonneau, J.: Privacy-enhanced public view for social graphs. In: Proceedings of the 2nd ACM Workshop on Social Web Search and Mining (2009)
16. Krishnamurthy, B., Wills, C.E.: Characterizing privacy in online social networks. In: Proceedings of the First Workshop on Online Social Networks (2008)
17. Laperdrix, P., Rudametkin, W., Baudry, B.: Beauty and the beast: diverting modern web browsers to build unique browser fingerprints. In: Proceedings of IEEE Symposium on Security and Privacy (2016)
18. Mahmood, S.: New privacy threats for Facebook and Twitter users. In: Proceedings of the 7th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (2012)
19. Mislove, A., Viswanath, B., Gummadi, K.P., Druschel, P.: You are who you know: inferring user profiles in online social networks. In: Proceedings of the 3rd ACM International Conference on Web Search and Data Mining (2010)
20. Olejnik, L., Castelluccia, C., Janc, A.: Why Johnny can't browse in peace: on the uniqueness of web browsing history patterns. In: Proceedings of the 5th Workshop on Hot Topics in Privacy Enhancing Technologies (2012)
21. Schrittwieser, S., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M.: Guess who's texting you? Evaluating the security of smartphone messaging applications. In: Proceedings of the 19th Annual Symposium on Network and Distributed System Security (2012)
22. Spitzner, L.: Honeypots: Tracking Hackers. Addison-Wesley Longman Publishing Co., Inc., Boston (2002)
23. Zheleva, E., Getoor, L.: To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In: Proceedings of the 18th International Conference on World Wide Web (2009)
24. Zhou, Z., Diao, W., Liu, X., Zhang, K.: Acoustic fingerprinting revisited: generate stable device ID stealthily with inaudible sound. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (2014)