Syntactic Analysis for Monitoring Personal Information Leakage on Social Network Services: A Case Study on Twitter

Dongjin Choi, Ilsun You, Pankoo Kim

Syntactic Analysis for Monitoring Personal Information Leakage on Social Network Services: A Case Study on Twitter

Dongjin Choi[1] Ilsun You[2], and Pankoo Kim[1*]

[1] Dept. Of Computer Engineering Chosun University,
375 Seoseok-dong, Dong-gu, Gwangju, Republic of Korea
Dongjin.Choi84@gmail.com, pkkim@chosun.ac.kr
[2] Korean Bible University,
16 Danghyun 2-gil, Nowon-gu, Seoul, Republic of Korea
isyou@bible.ac.kr

Abstract. Social network services such as Twitter and Facebook can be considered as a new media different from the typical media group. The information on social media spread much faster than any other traditional news media due to the fact that people can upload information with no constrain to time or location. Because of this reason, people got fascinated by SNS and it sinks into our life. People express their emotional status to let others know what they feel about information or events. However, there is a high possibility that people not only share information with others, but also they expose personal information unintentionally such as place to live, phone number, date of birth, and more. This will be serious problem if someone has impure mind. It is actually happening in cyber-stalking, offline stalking or others. There are also many spam messages in SNS because of the fact that information in SNS spread much faster than any other media and it is easy to send a message to others. In other words, SNS provides vast backbone environment to spammers to hunt normal pure users. In order to prevent information leakage and detect spam messages, many researchers traditionally have been studied for monitoring email systems, web blogs, and so on. In this paper, we dealt with text message data in Twitter which is one of the most popular social network services over the world in order to reveal various hidden patterns. Twitter data is severely dangerous to organizations and more is that anyone who has Twitter account can access to any users by "following" function. The following function does not require permission from the requested person to confirm to ready their timelines. This study will be focused on the user to whom exchange text messages and what types of information they reciprocated with others by monitoring 50 million tweets on November in 2009 which was collected by Stanford University.

Keywords: Information flow, Social network services, Information leakage, Twitter

* Corresponding author

1 Introduction

People are living in the place to find and share information with no constrains to time or location due to the huge enhancements of wireless internet infrastructure and Smartphone devices. We used to have to go back to home or internet cafe to search information or upload photos in very few years ago. However, we no longer have to go back to place to find desktop which has an internet access. We are simply able to obtain and share diverse information using Smartphone via mobile web browser or social network service (SNS) platform. Traditionally, the Web provides convenient and useful services to find information, knowledge, and more. People are willing to upload what they have been experienced during their travel or knowledge from their researches. Despite of this great convenience, there is a high possibility of personal private information leakage. The problem is that this personal information is leaking more seriously due to SNS. SNS is an online web platform to provide social activities among people. They share interests, activities, knowledge, events and more to strengthen their social relation with others in anytime and anywhere. There was a popular event make Twitter[2] got famous after U.S. Air ways jet crashes into the Hudson River on 15th of January 2009. The first photograph of this crash had appeared on Twitter earlier than any even local news media arrived at the accident place. This event brings an aspect that Twitter is not just a social web page but it is one of media. People got fascinated by this event so the popularity of Twitter was increased dramatically and it sinks into our life. The fastest social media is not always positive to people. Because of the fact that information on Twitter spread within a few second to all over the world, this might bring big obstacle to us all. The main reason why Twitter data is severely dangerous to organizations and more is that anyone who has Twitter account can access to any users by "following" function. The following function does not require permission from the requested person to confirm whether he/she will grant authority to read their timeline (or text message with others) or not. If user *A* send a following request to user *B*, user A automatically will be confirmed that he hereby can read timelines of user B based on the Twitter policy.

Let assume that user *C* sends a message to their friends to share information that tomorrow is his/her birthday. Or user *D* sends a message to celebrate his/her friend's birthday. In this case, although the date of birth is highly related to personal information, people normally expose precise date of birth unintentionally. The problem here is that as long as user *E* is following user *C* or *D*, user *E* is able to acquire personal text messages between user *C* and *D*. Moreover, people send a text to others with their real name or place to live. This is the main reason why we want to monitor personal information leakage on Twitter. Many researchers believe that SNS has great potential to reveal unknown personal attitude or sentiments but it still has an information leakage problem. This will be a serious problem if someone who has impure mind track personal information for cyber stalking. In order to prevent this problem on Twitter, we dealt with text message data in Twitter to reveal various hidden patterns related to personal information. This study will be focused on the user to whom reciprocated with by monitoring 50 million tweets on November in 2009

2 http://twitter.com

which was collected by Stanford University. We defined simple syntactic patterns to uncover date of birth in human written text messages.
The reminder of the paper is organized as follows: Section 2 describes related works; Section 3 explains a method for monitoring personal information leakage on Twitter based on syntactic patterns; Section 4 gives example for tracking breaking-events using Twitter; and finally Section 5 presents a conclusion to this work and makes suggestions for the future work.

2 Related Works

Digital personal information or personal identifiable information (PII) is always secured from other users. PII is information to uniquely identify or distinguish a single person identity. Full name, national identification number, driver license number, credit card number, date of birth, and more are commonly used to distinguish individual identity [1]. For example, if there is person who wants to withdraw huge amount of money from his/her bank accounts, he/she will be asked for presenting a valid PII to authenticate his/her identity. Moreover, when people forgot passwords for certain webpage, he/she will be asked for input PII data such as date of birth or email address. This digitized data can be easily duplicated to others and it tends to be exposed to others more readily than traditional physical resources [2]. This can be a serious crime if someone who has impure mind obtains digital PII intentionally or even accidently.
Over the years, many researchers have been studied for prevent personal information leakage not only in Internet web pages but also in SNS. Traditionally, packets which contain encrypted messages considered as an important factor to improve personal information security by monitoring transferring packets in networks [3]. Moreover, there was a research proposed a model to support a supply chain to make understand how confidential information of companies may be leaked using a conceptual model [4]. In order to infer private information in SNS, authors in [5] studied Facebook[3] data based on Naïve Bayes classification to predict privacy sensitive trait information among users. This research analyzed links among users to determine that personal information can be leaked to unknown person. [6] presented a new architecture for protecting personal private information published on Facebook for mitigating the privacy risks. Moreover, there was another research to trace social footprint of user's profile in order to uncover the fact that diverse personal information is leaking on multiple online social networks such as Flickr[4], LiveJournal[5], and MySpace[6] [7]. There is a big issue we have to give great attention that is personal information in SNS is leaking involuntarily [8]. People have been starting to take good care of preventing their personal information leakage when they make web documents. However, the problem is happened in SNS that SNS is full of freedom and enough metadata to infer someone's personal information. Users in SNS are likely to expose

[3] http://facebook.com
[4] http://flickr.com
[5] http://livejournal.com
[6] http://myspace.com

their private information unintentionally. This is why this paper focused on text messages in timeline on Twitter to reveal the fact that people reciprocate their personal information with others without any attention. Even they do beware of it, private information is leaking unintentionally.

3 Monitoring Personal Information Leakage on Social Network Services

This section describes a method for monitoring personal information leakage on Twitter. Twitter is a one of the most popular online SNS and microblogging service to share information by sending text-based messages restricted to 140 characters, known as "tweets" [9, 10]. Twitter users can freely follow others or are followed in contrary to most online SNS, such as Facebook or MySpace. Most of the SNS requires permission when users want to access others social web pages but not in Twitter. According to the Twitter policy, being a follower on Twitter means that users are able to obtain all the tweets from those users are following [9]. This issue guarantees a freedom of information sharing among anyone. However, personal information does not be exposed to everyone. In order to protect user personal information from unknown third parties, we define syntactic patterns to detect date of birth in human written text messages in Twitter. Let us assume that when people celebrate someone's birthday by a text message via Twitter or other SNS, the text message normally includes given keywords "birthday," "b-day." According to this assumption, we can obtain tweets which contain those keywords from huge amount of Twitter data set by simple text matching approach. The Twitter data set (8.27GB) which was collected by Stanford University [11] consists of time, user and tweet message information described in following Table 1.

Table 1. Examples of the Twitter data set

Type	Information
T	2009-11-02 14:49:31
U	*http://twitter.com/jhernandez48*
W	alright well off to cal class, I agree w/ Valentine on mike and mike but its a good things he is not the Philies manager, so oh well
T	2009-11-02 14:49:31
U	*http://twitter.com/kamanax*
W	This is the month of months and the week of weeks... Looking forward to the celebraaa on Friday, satday and Sunday! (cont) http://tl.gd/qkuu
T	2009-11-02 14:49:31
U	*http://twitter.com/koreainsider*
W	freezing waiting for bus, sweating on the bus and freezing again outside...I love that winter is here ?
…	…

T means the time when a given tweet was uploaded on Twitter and U indicates the Twitter user id who wrote the tweet. W represents the tweet at time T by user U.
In order to uncover the pattern hided in human natural language on Twitter, we simply extract tweets only include “birthday” and “b-day” from the data set. The size of extracted tweets was only approximately 30MB consist of around 189 thousand tweets. The following Table 2 shows examples of the extracted tweets.

Table 2. Examples of the extracted tweets from Twitter data set

Type	Information
T	2009-10-31 23:59:58
U	*http://twitter.com/nadiamaxentia*
W	@Anissarachma happy birthday to you, happy birthday to you, i wanna 'traktir' dont forget it, happy birthday to you. Haha
T	2009-11-01 00:01:45
U	*http://twitter.com/1crazy4justinb*
W	@justinbieber today is my b-day and it would mean the world to me if you told me happy birthday i love u!MAKE MY DREAM COME TRUE!<3
T	2009-11-01 00:10:04
U	*http://twitter.com/rgttos*
W	Kyny td udaah yaaa va, hahaha RT @virania: @rgttos happy birthday hhaaaa
…	…

Twitter has several functions such as ‘RT,’ ‘@,’ ‘#,’ and more. ‘RT’ means retweet, ‘@’ indicates specific person (user id) whom user wants to send a tweet message and ‘#’ is a hashtag that represents keywords or topics of tweets. We hereby define patterns to infer personal data of birth from the extracted tweets as described in Table 3. In order to define those patterns, we checked entire 189 thousand tweets by manually.

Table 3. Syntactic patterns for detecting date of birth

Index	Pattern information
1	***someone*** **(name or user ID) happy birthday (b-day) to** ***someone*** **(name, userID, or pronoun)**
ex)	@Anissarachma happy birthday to you
	Frank happy happy birthday from my heart
	happy birthday to my cousin Nathan and @Franklero
2	***someone*** **(name or userID) happy birthday (b-day)** ***someone*** **(name, userID, or pronoun)**
ex)	@LauraThomas34 happy birthday friend
	@kerronclement happy birthday
	Lolo happy birthday
3	***date*** **(such as today or tomorrow) is** ***possessive*** **birthday (b-day)** or **it is** ***possessive*** **birthday**
ex)	@justinbieber today is my b-day
	@JackAllTimeLow today is my birthday looooh
	@Teairra_Monroe Its my birthday and
4	**wish** ***someone*** **(name, user ID, or objective) a birthday**
ex)	@krystyl: On the east coast - its @drew's birthday! Everyone wish him happy bday
	will you please wish me a happy birthday
	@MixMastaMario I wish her a happy birthday

According to patterns described in Table 3, pattern 1 and 2 is for celebrating someone's birthday but pattern 3 is for celebrating his/her own birthday. Pattern 4 is for celebrating not only for themselves but also others. In the case of pattern 1 and 2, the first "*someone*" indicates name of user, user ID, or @user ID. The second "*someone*" represents name of user, user ID, @user ID, or pronouns. In order to detect name of user in text messages, we collect every name lists of boys and girls from the website[7] which contains 10,532 names. Moreover, it is easy to detect user ID due to the fact that users on Twitter are most likely to add "@" function when they send a text message to others. Therefore, if tweet is satisfied with pattern 1 and 2 when user ID comes at first, the date when this tweet was uploaded will be the date for use ID's birthday. In case for pattern 3, the important factors to determine which date is the date of someone's birthday are *date* and *possessive* words. The *date* can be one of words such as today, tomorrow, or specific date and *possessive* represents words e.g. my, his, her, *name*'s, and *user ID*'s. "*Someone*" in pattern 4 can be a name, user ID, or objective word such as "me, her, him, etc." In order to detect personal date of birth on Twitter, we developed simple extraction program based on above patterns using Python.

4 Experiment

In order to protect user personal information such as date of birth on Twitter, we conducted simple experiment using syntactic patterns described in Table 3 based on following Fig 1. The test Twitter data set which only includes "birthday" and "b-day" words contains 189,247 tweets with time, user address, and text message.

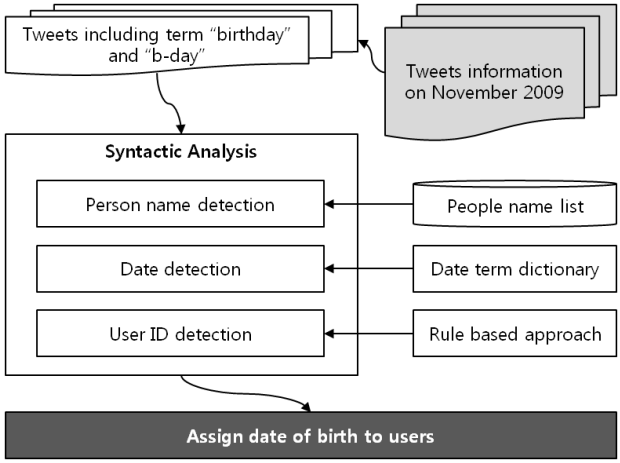

Fig. 1. Personal date of birth detection process

[7] http://www.momswhothink.com

According to the proposed detection process in Fig 1, we can infer the user's date of birth as described in Table 4.

Table 4. Example of experiment results

User	Date of birth	User	Date of birth
JanetRN	1st of November	davematthewsbnd	2nd of November
Larry	1st of November	sethredcast	2nd of November
1crazy4justinb	1st of November	Queen_MuLa_BaBy	2nd of November
dhilaloma	1st of November	ly_dalena	2nd of November
joseph	1st of November	dhardiker	2nd of November
Robert C Pernell	1st of November	glennmc	2nd of November
Brian Walker	1st of November	DJAYBUDDAH	2nd of November
rgttos	1st of November	TwentyFour	2nd of November
twephanie	1st of November	SoleHipHop	2nd of November
…	…	…	…

Let us assume that we have a tweet "RT @rhonda_ Happy birthday @JanetRN" by user apostlethatroks. This given text message indicates that user apostlethatroks send a celebration message which was originally written by user rhonda to user JaneRN. In other words, it was the birthday of user JanetRN. However, there is a problem that it is not guarantee the extracted date of birth is the precise date of user's birthday due to the fact that the proposed syntactic patterns cannot represent various human written text messages. In order to test how the proposed method can detect personal date of birth precisely, we randomly selected a hundred results to compare its accuracy manually. As a result, we can infer 61 percent of date of birthday from test data set with 75 percent of accuracy rate despite of fact that we only defined four kinds of syntactic patterns.

5 Conclusion and Future works

In this paper, we proposed a method for monitoring personal information leakage on Twitter by inferring date of birth using proposed syntactic patterns. People can upload diverse information on social network services with no constrain to time or location. This fact brings great convenience to us all but it is still challenging issue. The serious problem is that people are likely to expose their personal information unintentionally via SNS. Therefore, we proposed simple syntactic patterns to give an idea to protect personal private information. Considering that only four kinds of patterns were applied, we believe that the inference rate from test data set is acceptable. If we can define syntactic patterns in detail, the results will be much better than this work. However, it is difficult to determine users when test tweets have pronouns, possessive, or objective words. In the nearest future, we are planning to apply named entity disambiguation approach to enhance the performance.

Acknowledgments. This research was financially supported by the Ministry of Education, Science Technology (MEST) and National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation

References

1. Krishnamurthy, B.: I know what you will do next summer. ACM SIGCOMM Computer Communication Review, vol. 40, no. 5, pp. 65-70 (2010)
2. Yim, G., Hori,Y.: Guest Editorial: Information Leakage Prevention in Emerging Technologies. Journal of Internet Services and Information Security, vol. 2, no. 3-4, pp. 1-2 (2012)
3. Choi, D., Jin, S., Yoon, H.: A personal Information Leakage Prevention Method on the Internet. IEEE 10th International Symposium on Consumer Electronics, pp. 1-5 (2006)
4. Zhang, D.Y., Zeng, Y., Wang, L., Li, H., Geng, Y.: Modeling and evaluating information leakage caused by inference in supply chains. Computers in Industry, vol. 62, no. 3, pp. 351-363 (2011)
5. Lindamood, J., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: Inferring private information using social network data. Proceedings of the 18th international conference on World wide web, pp. 1145-1146 (2009)
6. Lucas, M.M., Borisov, N.: flyByNight: Mitigating the Privacy Risks of Social Networking. Proceedings of the 7th ACM workshop on Privacy in the electronic society, pp. 1-8 (2008)
7. Irani, D., Wwwwebb, S., Pu, C., Li, K.: Modeling Unintended Personal-Information Leakage from Multiple Online Social Networks. IEEE Internet Computing, vol. 15, no. 3, pp. 13-19 (2011)
8. Lam, I.F., Chen, K.T., Chen, L.J.: Involuntary Information Leakage in Social Network Services. Proceedings of the 3rd International Workshop on Security: Advanced in Information and Computer Security, pp. 167-183 (2008)
9. Kwak, H., Lee, C., Park, H., Moon, S.: What is Twitter, a Social Network or a News Media. 19th International Conference on World Wide Web, pp. 591-600 (2010)
10. Java, A., Song, X., Finin, T., Tseng, B.: Why We Twitter: Understanding Microblogging Usage and Communities. Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis, pp. 56-65 (2007)
11. Yang, J., Leskovec, J.: Patterns of Temporal Variation in Online Media. ACM International Conference on Web Search and Data Mining, pp. 177-186 (2011)