One Click Privacy for Online Social Networks

Philipp Hehnle[1], Pascal Keilbach[1], Hyun-Jin Lee[1], Sabrina Lejn[1], Daniel Steidinger[1], Marina Weinbrenner[1], Hanno Langweg[1,2]

[1]Department of Computer Science, HTWG Konstanz University of Applied Sciences, Konstanz, Germany
{philipp.hehnle,pascal.keilbach,hyun-jin.lee,
sabrina.lejn,daniel.steidinger,marina.weinbrenner,
hanno.langweg}@htwg-konstanz.de

[2]Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU, Norwegian University of Science and Technology, Gjøvik, Norway

Abstract. We present an approach to reduce the complexity of adjusting privacy preferences for multiple online social networks. To achieve this, we quantify the effect on privacy for choices that users make, and simplify configuration by introducing privacy configuration as a service. We present an algorithm that effectively measures privacy and adjusts privacy settings across social networks. The aim is to configure privacy with one click.

Keywords: Privacy, Social Networks, Metrics for Privacy, Configuration

1 Introduction

Nowadays, social networks are an integral part of everyday life. Recently, the number of users has dramatically increased and the trend continues [1]. Social networking sites allow an easy distribution of information but it is not always easy to delimit the recipients of the information and what kind of information they receive. Moreover, many users are not aware of the consequences that the revelation of personal data could have. The disclosure of private information can be critical and to some extent could be a threat, since "Likes" and other sympathy notices, pictures and location statements reveal a lot more information about a person than it seems at the first sight. In addition, social networks often provide confusing terms of use or make it difficult for users to keep track of their privacy settings.

For this reason, users of social networks should be aware of the consequences that come with privacy disclosure. The aim of our approach is to simplify the configuration of social networks. The main task is to quantify privacy of social networks and provide a tool to support the user to protect his privacy adequately.

2 Related Work

The basic requirement for such a tool to work is to be able to somehow measure privacy. If a privacy level can be measured, values can be compared and conclusions about improvement or worsening of the privacy level can be drawn, even across multiple social networks. The challenging aspect is, that so far, no general method for measuring privacy has been established or approved by an institution.

2.1 Configuration as a Service

People tend to use managed IT services instead of managing everything by themselves. The concept is called "everything as a service" and the most popular example is "software as a service". Cloud storage services or music streaming services are common services which people use every day. Since privacy is a complex topic and managing privacy settings can be challenging, the idea is to provide users a privacy configuration as a service. We analysed some tools that follow a similar approach.

MyPermissions (`https://mypermissions.com/de/`) is an app that allows users to monitor their applications that have access to their social networking sites. As the name says, it is only about permissions and does not change any privacy settings.

Reclaim Privacy scans the user's privacy settings on Facebook and indicates with colours if privacy settings are considered good or bad. Furthermore, the user could adjust the relevant settings. A similar approach is followed by Facebook Privacy Watcher (`http://www.daniel-puscher.de/fpw/`) by TU Darmstadt. While using Facebook, the tool indicates with a colour scheme the privacy level for each published item, such as posts, pictures, comments, etc. When users want to change the visibility e.g. of a post, a colour wheel opens and instead of adjusting the setting, the user picks a colour according to the desired privacy level. Unfortunately, these tools have been discontinued due to different reasons. Most projects were leisure projects. Since maintaining the tools took too much time, developers were compelled to stop their projects.

The most advanced approach is done by Trend Micro. They provide two possibilties for a fee for checking the privacy settings: a anti-virus software and an app. For the paper, the app "Trend Micro Mobile Security - Web Protection" was examined. With the app, it is possible to change settings in Facebook and Twitter. The user has to authenticate through the Trend Micro app with its credentials. However, the user cannot choose a desired privacy level. Instead, he has to follow privacy recommendations by Trend Micro.

None of the tools provides a way to effectively measure and change privacy settings across social networks. Reasons for failure of these tools may be explained through the complexity of privacy, social networks continuously changing their settings and a lack of measure privacy efficiently.

2.2 Privacy Measurement Index

To measure privacy, Wang and Nepali introduce a privacy index (PIDX) in [4]. The basic concept of the model uses actors, that represent a social entity (e.g. people or organisations) in a social network, and attributes to describe an actor. Each attribute has an impact on the user's privacy level, which is called the sensitivity of an attribute. Depending on the settings of the user, each attribute is to some extendt visible. Therefore, the value of visibility is used. Within the simplified scope of the paper, we define the following values according to [4]:

- **Sensitivity** describes the impact of an attribute on a user's privacy level. Sensitivity is described by $S = \{s_1, s_2, s_3, ..., s_\mathrm{n}\}$ and has a value between 0 and 1, where 1 indicates that the attribute describes highly sensitive information.
- **Visibility** describes the disclosure of an attribute. It is described by $V = \{v_1, v_2, v_3, ..., v_\mathrm{n}\}$ and has a value between 0 and 1, where 1 indicates a publicly known attribute.

S and V represent the sensitivities and visibilities of all attributes of an actor in a social network. Wang and Nepali propose three different Privacy Indexes: $wPIDX$, $mPIDX$ and $cPIDX$.

To get the weighted privacy measurement index $wPIDX$, the first step is to multiply the sensitivity and visibility of each known attribute. Then, those values are accumulated. Finally, the $wPIDX$ is calculated by putting the accumulated result in relation to all available attribute's sensitivities and multiplying by 100. Thus, $wPDIX$ results in a value between 0 and 100, with 100 being the highest possible privacy disclosure level [4]. This leads to equation (1).

$$wPIDX == \frac{\sum_{j=1}^{m} v'_\mathrm{j} s'_\mathrm{j}}{\sum_{j=1}^{n} s_\mathrm{j}} * 100 \tag{1}$$

Wang and Nepali also introduce the Maximum Privacy Index $mPIDX$ and the Composite Privacy Index $cPIDX$. $mPIDX$ returns the attribute that has the maximum privacy impact. $cPIDX$ combines both $wPIDX$ and $mPIDX$, giving $mPIDX$ most impact but also considers all other disclosed attributes.

For the current prototype implementation, it was decided to use $wPIDX$, because the handling with easy-structured $wPIDX$ reduces testing effort, but still considers all attributes and thus leads to insightful results. However, the question remains which one of the PIDXes leads to optimum results for our purposes.

Furthermore, if certain attributes are combined, it is possible that they further disclose privacy. For example, knowing any single component of an address (street name, house number and city) does not disclose a lot of personal data. However, knowing all of them has a higher impact on the privacy level. For this reason, Wang and Nepali introduce the concept of virtual attributes [4]. It has to be evaluated if this is applicable for our purposes.

Since the described model uses entities and instances that are valid across multiple social networks, the approach of Wang and Nepali [4] seems very promising for the project and was used to measure the privacy level.

3 One Click Privacy Concept

The concept shall provide a method that enables the user to choose a privacy level. Once the user sets a privacy level, the algorithm must guarantee the adherence to the desired privacy level. If the algorithm optimises the settings in the way that there is a better privacy level than required, this will be accepted. Nevertheless, the optimised privacy level shall be as close as possible to the desired privacy level. If, for instance, the desired privacy level was 40 and the algorithm's result was a privacy level of zero, the requirements would be fulfilled. However, the algorithm's goal to get close to the desired privacy level would not be achieved. Note that our project does not aim to achieve maximum privacy, but to enable the user to retain control of who can see his shared data. This implies the user's free choice on the degree of his privacy.

A further requirement is that personal information with high sensitivity shall not exceed the privacy level and be offset by personal information with low sensitivity that is below the privacy level limit. It is acceptable that personal information with low sensitivity exceeds the privacy level limit. This is even mandatory when complying with the previous requirements. Since it is not possible to set each preference in a way that the actual privacy level equals the desired privacy level, the desired privacy level for personal data with high sensitivity must be below the desired privacy level. If each information was below the limit, the entire privacy level would vary widely from the desired limit. For this reason, personal information with low sensitivity may exceed the limit under certain conditions which are explained in the following.

The algorithm's first step is to define the desired privacy level P_{d}. Afterwards, the algorithm needs to compute the limit for each personal piece of information. When using $wPIDX$, the limit for each information can be calculated like this:

$$z = \frac{P_d * \sum_{i=0}^{N} s_i}{N * 100} \tag{2}$$

Consequently, z is the limit for each personal data item, whereas N is the amount of settings and s_{i} is the sensitivity for the setting i. A simple approach is to check for each setting if the visibility multiplied with the given sensitivity is equal to or below z. If this is not the case, the setting must be adapted. The consequences would be that the actual privacy level would deviate substantially from the desired privacy level. Therefore, each time there is a remainder $R = z - v * s > 0$ for an item with high sensitivity, an item with low sensitivity can exceed the limit by the remainder. This leads to the algorithm displayed in figure 1.

First, the desired privacy level P_d for the entire profile is defined. Then, the limit z is calculated. Now, there are two loops. Before the first loop starts, the

settings are sorted by their sensitivities descending. The first loop runs until each setting in the set has been considered, beginning with the setting that has the highest sensitivity. In each loop run, the setting's visibility is adapted. The visibility is chosen in such a way that $v * s <= z$. Afterwards, the remainder R is calculated with $R = R + z - v * s$. In the next run, the algorithm chooses the next setting and the procedure repeats. This guarantees that those settings with the highest sensitivities are below z. The second loop starts with the last element of the set. This means that the setting with the lowest sensitivity is chosen. The algorithm checks whether the setting can be changed, since the former limit z can be shifted by the remainder. So, there is a new limit for the settings now. As a consequence, the algorithm can adapt the setting so that $v * s <= z + R$. This means, it is checked whether it is possible to worsen this setting concerning privacy. Actually, $v * s$ with the visibility that was chosen in the first loop for this setting should be added to $z + R$, too. For the sake of clarity, this has been omitted in the figure. Since the second loop starts with those settings that have the lowest sensitivities, there is no serious privacy impact if those personal data items exceed the privacy limit. After having adapted the setting, the algorithm calculates the new remainder $R = R + z - v * s$. The next setting is chosen from the set and the procedure repeats. When the remainder R is not greater than zero, z is the limit again.

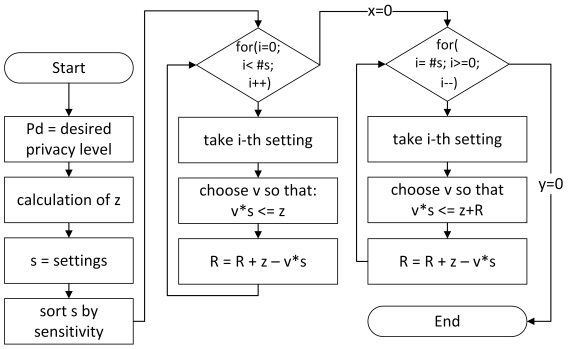

Fig. 1. Settings Optimisation Algorithm

4 Prerequisites for the Implementation

This section describes the necessary steps that need to be done to prepare the implementation. Since we want to provide a tool that manages privacy across multiple social networks, it has to be decided which networks will be considered. Social networks are chosen by number of users and region [3] [2]. For global networks, our focus is on Facebook, Twitter, Google+ and LinkedIn. For national networks, XING for Germany, QZone for China and vKontakte for Russia were chosen.

Since the tool should be able to change settings in the relevant social networks, it is necessary to analyse the relevant settings and which attributes they will affect. Therefore, the settings of each network were summarised in a single file and clustered into ten different topics: my profile, messages, posts, detectability, location, account, announcement, blocking and hiding, security as well as specific topics that only apply to the respective social network. Nearly all settings are described differently in all social networks and have a different meaning. Furthermore, the social networks have different functions and possibilities. For example, Facebook is primary used for personal life, it serves for connecting and communicating between private persons, and LinkedIn for business. Thus, every social network has its own features. For example, QZone has the possibility to specify a security question. With the right answer a user can see certain information of the other user. QZone has a restriction, because it is the only social network which is not available in English, only in Chinese.

After clustering and managing all the settings, the sensitivity of the affected attributes was added. Here the problem arises that each person perceives the sensitivity of each attribute individually. However, tendencies can be recognised. For example, the full address is generally perceived more sensitive than the gender. Therefore, the sensitivity of the attributes is determined through an online survey throughout the project. Since the evaluation of the survey (132 students aged 18-29 years) is ongoing, we use "high", "medium" and "low" as values for sensitivity, to indicate our first results.

5 Implementation

For the first prototype we chose Twitter because the settings options are not as complex as the options on Facebook, which is suitable for testing purposes. We decided to develop a browser extension because it has the advantage that we can use the current session while the user is logged on to Twitter. Since many users remain logged on on their personal computer, users will not need to authenticate themselves again which benefits the usability of the tool. Credentials are not saved or forwarded to any back-end server.

Currently, the user has to visit www.twitter.com and log on. The extension calculates the current PIDX and prints the number in the icon in the top right corner. For a detailed view, the user can click on the extension button. There is a view for the user as shown in figure 2. With a click on the "Adapt Settings" button, the plugin will change the settings so that the new PIDX is better than the desired one.

The extension is completely running on client side and is only using HTML, CSS and JavaScript. For the PIDX calculation, the extension is sending an AJAX GET request to Twitter's settings page. Therefore, the user does not have to visit any particular page and is not being redirected. After parsing the settings to a JavaScript object, we calculate the visibility and change the settings, based on the algorithm developed in section 3. To finally change the settings, we send

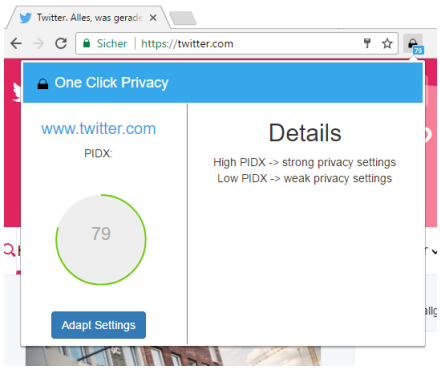

Fig. 2. Prototype 1 - Chrome extension, Twitter

an AJAX POST request to Twitter. A specialty for Twitter is that Twitter is requesting a second user verification when changing the settings.

After some tests on Twitter we faced a problem as Twitter might change the settings page. This already happened once since we started testing. The issue here is to somehow notice that a social network changed its settings page, because this will eventually affect the functionality of the tool.

In the current state of the project, we are developing a second, more detailed prototype which is extended to the social network Xing. With this prototype, we will recheck and optimise our theoretical approach.

6 Discussion and Future Work

Since the project is still going on, there are some issues that have to be considered and will be discussed in this section.

In section 2.2, it was mentioned to use $wPIDX$ for practical reasons of the prototype. Until now, $wPIDX$ leads to promising results. However, it has to be evaluated if $cPIDX$ leads to more accurate results. Wang and Nepali claim $cPIDX$ to be the most accurate since it weighs the attribute with the maximum privacy impact most [4].We plan to verify in several test cases if this statement is true for the desired purposes and if it leads to more accurate results regarding the desired privacy level.

Furthermore, a current task of the project is to evaluate if the concept of virtual attributes described in section 2.2 can be applied for our purposes. A valid alternative could be to group similar attributes from the very beginning. The reduced complexity of the latter approach could lead to a better comparison of attributes across multiple social networks.

The optimisation algorithm introduced in chapter 3 meets exactly the project's requirements and works reliably. First test cases with the prototype implementation prove that. Currently, the test cases only run on Twitter for practical reasons. However, deeper testing needs to be done, especially borderline test

cases. In order to check if the results are equivalent regarding the privacy level, the extended prototype, which includes Twitter and Xing, will be used.

As described in section 4, a survey was conducted to determine the values for sensitivity of each attributes. Meanwhile, the survey has around 150 participants. Therefore, representative values for the sensitivity of the attributes can be specified. We are currently evaluating the results of the survey.

7 Conclusion

One Click Privacy for online social networks aims to provide users a service to easily manage their privacy settings across social networks. The paper concludes with three contributions. Firstly, we developed an algorithm that uses $wPIDX$ which was introduced by Wang and Nepali in [4]. The algorithm is capable of adjusting privacy settings and not exceeding a desired privacy level. With this approach, it is possible to compare privacy settings across multiple social networks. Secondly, we conducted a survey which determines the values for sensitivity. In addition, we have grouped all relevant privacy settings of the chosen social networks in a single file. Last, but not least, the third contribution is the development of a prototype that proves that our approach is working and leads to promising results.

We hope to raise the user's awareness of his privacy, as privacy is not only a question of proper settings, it is also a matter of handling personal data properly.

References

1. Statista: Global social network users growth 2020 — statistic (2014), https://www.statista.com/statistics/270919/worldwide-social-network-user-growth/
2. Statista: Anteil der internetnutzer, die in den letzten drei monaten an sozialen netzwerken im internet teilgenommen haben, nach altersgruppen in deutschland im jahr 2016 (2016), https://de.statista.com/statistik/daten/studie/509345/umfrage/anteil-der-nutzer-von-sozialen-netzwerken-nach-altersgruppen-in-deutschland/
3. Statista: Anteil der nutzer von social networks nach altersgruppen in den usa in den jahren 2005 bis 2016 (2016), https://de.statista.com/statistik/daten/studie/500829/umfrage/anteil-der-nutzer-von-sozialen-netzwerken-nach-altersgruppen-in-den-usa/
4. Wang, Y., Nepali, R.K.: Privacy measurement for social network actor model. In: International Conference on Social Computing (SocialCom), 2013. pp. 659–664. IEEE, Piscataway, NJ (2013)