Self-disclosure in Social Media: An opportunity for Self-Adaptive Systems

Nicolás Emilio Díaz Ferreyra and Johanna Schäwel

University of Duisburg Essen, Germany
{nicolas.diaz-ferreyra,johanna.schaewel}@uni-due.de
https://www.ucsm.info/

Abstract. Users of Social Network Sites (SNSs) spend considerable amounts of hours per day exchanging (consuming or sharing) information and using services provided by such platforms. However, nothing comes for free. SNSs survive at the expense of the information that users' upload to their profiles, and the knowledge derived from their on-line behavior. Discovering hidden knowledge in social networks is a centerpiece in many personalized on-line services and ad-targeting techniques, and helps to make a SNS profitable. However, users seem not to be aware of this common practice and keep sharing content compulsively. Nevertheless, self-disclosure and over-exposition can have severe consequences and can put users' integrity into risk. In order to develop better information control and awareness systems, we believe that it is important to take into account the users' on-line habits and behavior. In this work we introduce an initial assessment of the different factors that contribute to self-disclosure in Social Media, and discuss the elements that a self-adaptive solution should consider to address this issue.

Keywords: social-media, self-disclosure, awareness, self-adaptive systems

1 Introduction

Social Media has set new standards for our interpersonal relations, and has accelerated the dynamics of our lives. Many users are bridged through SNSs, and new sub-communities are built everyday based on common interests, likes or even mottos. The inhabitants of these virtual communities are spending considerable amounts of time exchanging (consuming or sharing) information, and using services provided by the SNSs. However, none of this is for free. SNSs survive at the expense of the information that users' place in their profiles, and the behavior they exhibit while using the different services provided by these platforms.

Discovering hidden knowledge in social networks is a centerpiece in many personalized on-line services and ad-targeting techniques, and is basically what makes a SNS profitable [18]. However, many of the content that is uploaded to social platforms (text, image, video, location) contain a high level of private and

sensitive information. The reality is that Social Media users compulsively share content without caring about the consequences. Moreover, their behavior off-line (in the real world) differs highly from their on-line behavior (inside a SNS) [3][14]. If we add to this that users are careless when adding new contacts to their network, there is a high chance of having potentially dangerous individuals accessing this information.

Although existing privacy-preserving mechanisms have been developed and improved over the years, they are still not helping users in distinguishing a self-exposition behavior that might put them into risk. It is very hard for a regular user to keep track of everything that he or she has shared through its "on-line life". Moreover, once the content has been shifted to the Internet, the user has no control over it anymore. This situation demands new mechanisms for tracking the sensitive information that a user has already shared, and the degree of sensitiveness that new information might have. Thus, users of SNSs can make a wiser decision before sharing content, and have a better vision of what they have shared (and would like to un-share) in the past.

In this work we present an analysis of the "self-disclosure" problem in Social Media and provide insights towards a self-adaptive solution. Different dimensions of the problem like the users' behavior and information sensitiveness are studied from an inter-disciplinary perspective. Furthermore, initial guidelines for a self-adaptive approach based on the MAPE-K model by IBM [9] are here introduced.

In the following section the fundamental bases and concepts involved in our proposal are initially introduced (Section 2). Section 3 covers the different aspects of the self-disclosure issue including: the diversity of information in SNSs, the so-called "privacy paradox", information sensitiveness, and an adapted version of the MAPE-K model. Next, Section 4 discusses alternative existing solutions, and finally Section 5 presents our conclusions and related future work.

2 Theoretical Background

This section introduces the fundamental concepts that form the bases of our proposal. Here, Autonomic Systems and run-time self-adaptation concepts are presented and analyzed for further application in a Social Media scenario.

In order to raise awareness of self-disclosure among the users of SNSs we propose to develop an Autonomic Computing vision of this issue. The goal of Autonomic Computing is to design and develop distributed and service-oriented systems that can easily adapt to changes that affect the system administration and service delivery, while reducing some of the complexities associated with the management of such systems [10]. Considering the user's content-sharing behavior in SNSs as the managed element of our autonomic system, will allow us to apply the concepts of Autonomic Computing into a Social Media domain. MAPE-K (Monitor, Analyze, Plan, Execute, and Knowledge) is a reference model for control loops used in Autonomic Computing with the objective of supporting the concepts of self-management, specifically: self-configuration, self-optimization, self-healing, and self-protection [9][10]. Fig. 1 shows the ele-

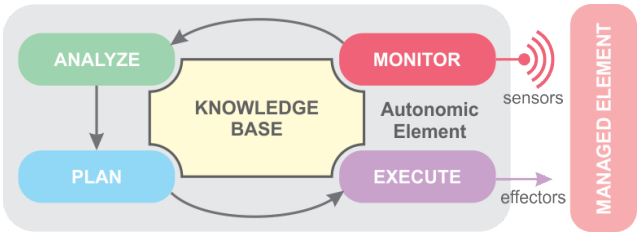

Fig. 1. Autonomic Computing and MAPE-K Loop [9]

ments of an Autonomic System: the control loop activities, sensor and effector interfaces, and the managed system.

The *Monitor* component provides the mechanisms to observe through *Sensors* different events or changes that take place in the *System* (managed element). It also filters and aggregates the data, and reports details or metrics [9]. The *Analyze* component provides the means to correlate and model the reported attributes or measurements. It is able to interpret the environment, to handle complex situations, and predict future scenarios. *Plan* provides the means to construct the set of actions required to achieve a certain goal or objective in response to certain events. On the other hand, *Execute* offers the elements to release the actions involved in a particular plan (e.g. to control the system by means of *Effectors* that modify the managed element)[10]. Additionally, a common *Knowledge Base* acts as the central part of the control loop, and is shared by the activities to store and access collected and analyzed data.

The MAPE-K model is used as an architectural reference in cases where a feedback loop is a distinctive characteristic of the system being built. Such is the case of [7], where a MAPE-K loop is used for run-time monitoring of trustworthiness properties in a socio-technical system in order to achieve trust goals. In a Social Media context like ours, the users' accounts are the elements we want to monitor since they contain the resources and services consumed by them. In line with this, the actions executed over the accounts (managed elements) are directed to aware the users about an over-exposition behavior.

3 A self-adaptive approach for addressing Self-disclosure

It is necessary to conduct an analysis of several factors that contribute to the problem and the solution of self-disclosure in SNSs. In this section we will go through the different types of information that can be found in a SNS (particularly on Facebook), and we will provide some insights for further sensitiveness classification. We will also discuss the influence of users' on-line behavior and risk aversion. At the end of this section, an approach for addressing this issue based on the MAPE-K model will be introduced.

3.1 Diversity of information in SNSs

SNSs are a rich source of the most varied kinds of information. However, users do not realize the importance that this information they "voluntarily" deposit in these sites has. From a high level inspection, normally one can find in a Facebook profile the following information: list of friends, personal information (e.g. first name, surname and profession), wall posts (public messages from other users), messages, photos, and notes [11].

However, if one takes a closer look to the now improved "Facebook Security Centre", it is now possible for users to download a copy of the information that Facebook stores about them. Surprisingly, the list is way bigger than the one mentioned before, and includes (among other information)[1]:

- *Ads Clicked:* Dates, times and titles of ads clicked by the user.
- *Ad Topics:* A list of topics that the user is targeted against based on its likes, interests and other data included in its Timeline.
- *Check-ins:* Places where the user has checked-in to.
- *Facial recognition data:* A unique number based on a comparison of the photos the user has been targeted in.
- *IP Address.*
- *Log-ins and Log-outs.*
- *Deleted friends.*

Clearly, users do not submit many of this information voluntarily to Facebook. For someone familiar within SNSs and their privacy practices, it is not surprising that Facebook (like many other SNSs) keeps all these records in their servers. However, for many users (newcomers or advanced) this situation remains unclear, even when the privacy settings of their Facebook accounts are public by default [16].

3.2 Self-disclosure and the Privacy Paradox

Exposing personal information to other persons is referred as individuals' self-disclosure. Self-disclosure in on-line contexts like Social Media is, at least to a certain extent, the precondition for a functional social network [12]. In other words, users' contributions are necessary for the survival of SNSs. Without the users' shared content (such as posted information and tagged photos), SNSs would lack of diversity and fail on being interesting enough for the users to engage with.

Self-disclosure is frequent among the users of SNSs. Furthermore, users seem careless when providing sensitive information through SNSs. However, they consider privacy protection an important issue that must be addressed. This phenomenon of contradiction has been referred as the "privacy paradox" [2][14]. Despite the studies that reveal evidence of this thesis [8], complementary research judges the non-holistic approach of the applied methods in these findings

[1] https://www.facebook.com/help/405183566203254/ (last access: 22/01/2016)

[5]. Nevertheless, we believe that, whether the privacy paradox exists or not, users' on-line behavior has to be empowered with a recommendation system that can assist them in the identification of potentially sensitive information in real time.

3.3 Defining sensitiveness in Social Media

Several gaps and dilemmas have been identified when trying to define what sensitive information is [15]. Moreover, it is a matter of discussion in the legislation of many countries and politico-economic unions [1][6]. The European Parliament for instance has defined some "personal data" categories (e.g. racial or ethnic origin) that are protected against public disclosure. It also makes use of the term "sensitive information", however it does not define it [6]. The Canadian Personal Information Protection and Electronic Documents Act 2000 state that: "Although some information (e.g. medical records) is almost always considered to be sensitive, any information can be sensitive depending on the context" [6]. This last one is an interesting approach towards the definition of "sensitive information" since it highlights the influence that the context has over it. Nevertheless, this reveals the need for considering and understanding the context where the information is placed.

A SNS is a complex environment where multiple factors converge and (in many cases) are the ones that define the rules of interaction and contributions for the users. For instance, a post that can look trivial on Facebook can be totally inappropriate in another SNS like LinkedIn (e.g. a photo of you in a party might not look very professional). In other words, here the context affects the degree of sensitiveness of the content. In this case the targeted audience of the SNS is a conditioning dimension of the context.

3.4 Towards a MAPE-K-based approach

An awareness system like the one proposed in this work has a self-adaptive nature. Its purpose is to perform a constant monitoring over the user sharing activities and notify when a self-disclosure behavior is detected. This notification can be seen as an interaction with the user, where he or she will have the last word and control over the sharing act. In other words, the user should have the chance to accept or reject the recommendation of not to share potentially sensitive information. This sequence of detection-notification-acceptance defines a feedback loop between the user and the awareness system.

As we have discussed in the previous sections, classifying information into categories of sensitiveness does not have a straightforward solution. However, as several legislations agree, it is possible to build categories of "personal" or "sensitive" data. Since the user's perception is also a determinant on the final classification, it seems logical to perform a classification of the users based on their interpretation of particular pieces of information. Then, by combining these two approaches together with attributes of the SNS (e.g. the targeted audience

Fig. 2. Elements for the analysis of sensitive information

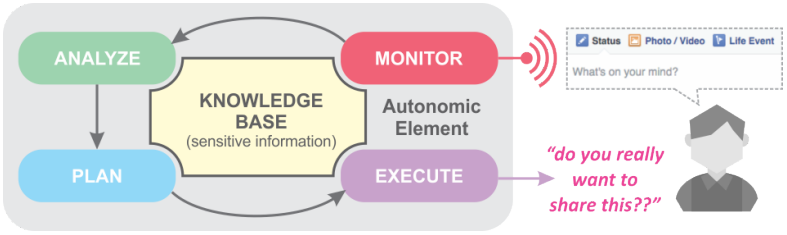

Fig. 3. Adapted MAPE-K Loop

and activity levels of the users), a better classification of the information can be performed (Fig. 2).

In Fig. 3 an adapted version of the MAPE-K loop is described. In this case, the *Managed element* corresponds to the representation of the user in a SNS, this is, the user's account. In this approach, the *Monitor* is sensing the activity of the user and responses when an information-sharing event takes place. As was previously mentioned, the goal of this system is to provide recommendations to the user when it attempts to publish content of sensitive nature. Therefore, what the *Analysis* unit should do is to analyze the information collected by the Monitor's *sensors* and classify it into sensitive or not sensitive. Here, the *Knowledge base* has a main role because it contains all what has been learned about sensitiveness and its influencing factors. After this is done, the *Plan* will elaborate a recommendation for the user, and then the *Execute* module will proceed to deliver it to the user.

A privacy protection recommendation system must be able to adapt on users individual self-disclosing behavior without destructing the interactive nature of SNSs. Our approach takes this statement into account by asking the user "do you really want to share this?" instead of forbidding it to continue. By this, the autonomy of the user is ensured and its final decision contributes to the feedback loop of the system.

Nevertheless, self-adaptation brings into account a fundamental reasoning problem: decide which is the best course of action to follow based on the perceived

stimuli from the environment. In Artificial Intelligence this type of reasoning is usually called *planning*, where the condition to achieve is called *goal* and the sequence of actions that will make the goal true is called a *plan* [4]. Because such Autonomic Element must exhibit an intelligent behavior, *planning* is a central discipline in our study. According to [4] Situation Calculus based on First Order Logic (FOL) is an adequate candidate to support *planning* due to its appropriateness for representing dynamically changing worlds. Furthermore, it provides a framework for defining a set of actions, states and changes in the environment, and entails a reasoning mechanism to make inferences. Adapting Situation Calculus to our problem domain is one of the major challenges of our research.

4 Discussion

Many privacy breaches in SNSs have been identified and addressed through different types of privacy-preserving software architectures (e.g. P2P). Many researchers advocate particularly for decentralized architecture schemas unlike predominant centralized approaches[13]. Some of the benefits of this are end-to-end encryption, hidden activity from 3rd parties, and hidden social graph among others. Although decentralized schemas improve privacy protection for the users, they demand a major development effort and cannot provide the same functionality as centralized ones [13]. This is one of the major reasons why users are reluctant to migrate to privacy-preserving SNSs [13].

While these approaches focus mainly on the architectural elements that a privacy-preserving SNS must have, the solution presented in this work propose to contribute to privacy on the application level. This is, even with a centralized and non-privacy-preserving SNS architecture, it should be possible to arise user's awareness and hence prevent extensive self-disclosure. In this way, empowered users will take better control over their on-line acts and in consequence over their private data. This can be achieved since SNSs like Facebook provide APIs and extension points for including 3rd party applications, which would allow us to integrate our solution without forcing users to change into another SNS.

5 Conclusions

In off-line situations people's communication about sensitive topics take place behind closed doors; whereas in SNSs users do not seem to lock their metaphorical doors when they address sensitive topics [3]. Moreover, the range of the audience that can access to personal information is perceived differently in on-line and off-line contexts. In an off-line context a person usually recognizes his or her audience, whereas in on-line contexts people are not able to sufficiently estimate the size of such audiences [17]. Due to the difficulty in estimating the number of receivers of what in many cases can be sensitive information, it is important to support the users in analyzing the sensitivities of their contributions.

It is true that some users are not much concerned about the consequences that self-disclosure in SNSs could bring to them, and are not willing to modify their behavior. However, this does not neglect the fact that it is necessary to support and empower them through better control and awareness systems. Instead, this raises the necessity of developing instruments that take into consideration users' distinctive characteristics that make them more or less adverse to the risks of over-exposition.

Self-disclosure and information sensitiveness analysis propose a number of challenges and opportunities for self-adaptive systems. This work has analyzed and summarized the requirements that a self-adaptive solution must cover for addressing self-disclosure in SNSs. Now this vision has to be put into practice and undoubtedly new challenges and research questions will arise. This is matter of our future work, together with an analysis of acceptance of such awareness system among the social network's community.

Acknowledgments. This work was supported by the Deutsche Forschungsgemeinschaft (DFG) under grant No. GRK 2167, Research Training Group "User-Centred Social Media".

References

1. Australian Law Reform Commission, et al.: For your information: Australian privacy law and practice (alrc report 108). Sydney: Commonwealth of Australia (2008)
2. Barnes, S.B.: A privacy paradox: Social networking in the United States. First Monday 11(9) (2006)
3. Bartsch, M., Dienlin, T.: Control your facebook: An analysis of online privacy literacy. Computers in Human Behavior 56, 147–154 (2016)
4. Brachman, R.J., Levesque, H.J.: Knowledge representation and reasoning, vol. 9. Morgan Kaufmann Publishers, Massachusetts, US (2004)
5. Dienlin, T., Trepte, S.: Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology 45(3), 285–297 (2015)
6. Directive, E.: 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EC 23(6) (1995)
7. Gol Mohammadi, N., Bandyszak, T., Moffie, M., Chen, X., Weyer, T., Kalogiros, C., Nasser, B.I., Surridge, M.: Maintaining trustworthiness of socio-technical systems at run-time. In: Trust, Privacy, and Security in Digital Business - 11th International Conference, TrustBus 2014, Munich, Germany, September 2-3, 2014. Proceedings. pp. 1–12 (2014), http://dx.doi.org/10.1007/978-3-319-09770-1_1
8. Hughes-Roberts, T.: Privacy and social networks: Is concern a valid indicator of intention and behaviour? In: SocialCom 2013: International Conference on Social Computing. pp. 909–912. IEEE (2013)
9. Kephart, J., Kephart, J., Chess, D., Boutilier, C., Das, R., Kephart, J.O., Walsh, W.E.: An architectural blueprint for autonomic computing. IBM White paper (2003)

10. Kephart, J.O., Chess, D.M.: The vision of autonomic computing. Computer 36(1), 41–50 (2003)
11. McCown, F., Nelson, M.L.: What happens when Facebook is gone? In: Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries. pp. 251–254. ACM (2009)
12. Nguyen, M., Bin, Y.S., Campbell, A.: Comparing online and offline self-disclosure: A systematic review. Cyberpsychology, Behavior, and Social Networking 15(2), 103–111 (2012)
13. Schwittmann, L., Wander, M., Boelmann, C., Weis, T.: Privacy preservation in decentralized online social networks. IEEE Internet Computing (2), 16–23 (2014)
14. Taddicken, M.: The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication 19(2), 248–273 (2014)
15. Thompson, E.D., Kaarst-Brown, M.L.: Sensitive information: A review and research agenda. Journal of the American Society for Information Science and Technology 56(3), 245–257 (2005)
16. Vilić, V., Radenković, I.: Privacy protection on Facebook, Twitter and LinkedIn. Syntesis: International Scientific Conference of IT and Business-Rlated Research (2015)
17. Vitak, J.: Balancing privacy concerns and impression management strategies on Facebook. In: Symposium on Usable Privacy and Security (SOUPS) (2015)
18. Zheleva, E., Terzi, E., Getoor, L.: Privacy in Social Networks. Synthesis Lectures on Data Mining and Knowledge Discovery, Morgan & Claypool Publishers (2013), `https://books.google.de/books?id=5YpiAQAAQBAJ`