Poster: Using Avatars to Safeguard Privacy during Online Registrations

Gaurav Misra
UNSW Canberra Cyber
School of Engineering and Information Technology
University of New South Wales
Canberra, Australia
g.misra@unsw.edu.au

Nicholas Micallef
UNSW Canberra Cyber
School of Engineering and Information Technology
University of New South Wales
Canberra, Australia
n.micallef@unsw.edu.au

***Index Terms*—usable privacy, obfuscation, avatars**

I. Introduction

People often have to go through a registration process to avail different types of services, such as email accounts, loyalty memberships and even accessing public Wi-Fi hotspots. Most of the forms used for such registrations, ask for a lot of personal information about the individual which are often beyond what is required to deliver the particular service [1]. More pertinently, users are often aware that their personal information is at risk and have been repeatedly found to be cynical about how it is used by organizations that collect it [2].

Obfuscation has been proposed as a privacy protection mechanism to safeguard users' personal information [3]. Such mechanisms intercept the user's personal information before it is processed by the service provider, including social networks, and obfuscate it by either encrypting the data [4] or substituting it with randomly generated fake data [5]. Most obfuscation mechanisms, however, function "under-the-hood" and therefore do not enhance users' understanding of how their information is protected. Users have to blindly trust that the obfuscation mechanism can effectively safeguard their personal information and have no control over how it actually works. Consequently, such mechanisms have not been widely adopted, possibly due to the so called "privacy paradox", which suggests that users often refrain from using privacy protection mechanisms, even if they are aware of the risks of disclosing personal information [6]. Therefore, new techniques need to be investigated to improve the usability of privacy protection mechanisms to make them more engaging for users, to encourage adoption, as well as provide them with greater control and flexibility when safeguarding their privacy.

II. Using Avatars for Privacy Protection

With the objective of providing users with more control when protecting their personal information, and make this process more transparent and engaging, in this research, we propose the use of "avatars", which are digital representations for human users used for communicating online [7], [8], in a privacy protection mechanism. The mechanism would allow users to create "avatars" and then use the "fake" information of the avatar to register for online services. Hence, the users would replace their personal information, thereby safeguarding their privacy, and still complete the forms using the information from the avatar profiles. In this way, the use of avatars as a privacy protection mechanism addresses the issues of lack of control and transparency that are currently exhibited by privacy protection techniques that use obfuscation.

Avatars have been previously used in numerous application areas [9], to enhance users' intrinsic motivation through self-determination theory [10], for the purpose of playing games [11], [12] or to adhere to self-improvement programs [13]. The self-determination theory states that people's intrinsic motivation to conduct a task could be satisfied by fulfilling the following three psychological needs when interacting with an application: **competence** - the need of experiencing control over the outcome of a challenge; **autonomy** - the need to engage in a challenge under one's own choice; and **relatedness** - the universal need of feeling connected to others. For privacy protection, the use of avatars would satisfy the self-determination needs of users as they would: (1) create avatars they feel connected to (**relatedness**); (2) feel in control of which information they want to use from the avatar, and what personal information they want to safeguard (**competence**); and (3) be creative in generating the avatars of their choice (**autonomy**). To the best of our knowledge, avatars have not been used for privacy protection and as highlighted in the discussion above, we hypothesize that using avatars would be an engaging and flexible privacy protection mechanism.

III. A Practical Case Study

Figure 1 illustrates an example of how a user may use an avatar to generate fictitious information to represent themselves when registering for online services. The figure shows how Bruce Banner, a physicist born in December 1969, creates an avatar of himself called *"The Hulk"*. He then uses the fictitious information, highlighted in green (name, ZIP code, email and birthday), to register for a *Starbucks Rewards*[1] membership. In this way, Bruce can register for Starbucks Rewards program and still safeguard his personal information.

[1]https://www.starbucks.com/starbucks-rewards

Fig. 1. Using an avatar to register for online services

In the given example (Figure 1, when Bruce Banner registers for the Starbucks Rewards program, he would need to use a legitimate Starbucks card number. He can, however, use fictitious information (obtained from the avatar) to represent himself, as shown in the example. This illustrates how using avatars provides users with the desired flexibility of combining fictitious and real information when providing it to service providers, thereby controlling what personal information (in addition to the mandatory requirements) they provide.

There may be instances in which fictitious information cannot be used when registering for services as certain details about the user cannot be "faked". For example, when purchasing products online, the user would need to provide a genuine credit card number to ensure the successful completion of a transaction. Moreover, if the product requires delivery, a genuine address would need to be provided. Therefore, if Bruce would want to use the delivery service, he would need to use his correct ZIP code (01451) and not the fictitious one (90028). Thus, using avatars can only safeguard privacy of personal information which is not essential for the transaction to be completed. It is also important to note that the information referred to as essential is different from mandatory (typically indicated with a '*' symbol), which may be "faked" if it does not affect the legitimacy of the transaction.

IV. Future Work

The next steps of this research can be summarized as the following tasks:

- A systematic analysis of online registration forms, to identify the most common personal information requested from users, which will determine the biographical information to be included in the avatars.
- A user-centered approach (i.e. workshops and focus groups) to identify the key features required by such a system to make it engaging (e.g. how could the system be designed to motivate users to engage with it in a regular manner?) and to satisfy users' usability requirements (e.g. what features should be provided to improve users interaction with the system?).
- On completion of design and development, the mechanism will be evaluated through a longitudinal field study to determine whether it fulfills the privacy-protection, control and engagement objectives.

References

[1] O. Starov, P. Gill, and N. Nikiforakis, "Are You Sure You Want to Contact Us? Quantifying the Leakage of PII via Website Contact Forms," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 1, pp. 20–33, jan 2016.

[2] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, ""My Data Just Goes Everywhere" User Mental Models of the Internet and Implications for Privacy and Security," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS) 2015*, 2015.

[3] F. Beato, M. Kohlweiss, and K. Wouters, "Scramble! Your Social Network Data," in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, Berlin, Heidelberg, 2011, pp. 211–225.

[4] E. D. Cristofaro, C. Soriente, G. Tsudik, and A. Williams, "Hummingbird: Privacy at the Time of Twitter," in *2012 IEEE Symposium on Security and Privacy*. IEEE, may 2012, pp. 285–299.

[5] W. Luo, Q. Xie, and U. Hengartner, "FaceCloak: An Architecture for User Privacy on Social Networking Sites," in *2009 International Conference on Computational Science and Engineering*. IEEE, 2009, pp. 26–33.

[6] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[7] K. L. Nowak and J. Fox, "Avatars and computer-mediated communication: a review of the definitions, uses, and effects of digital representations," *Review of Communication Research*, vol. 6, pp. 30–53, 2018.

[8] N. Micallef and M. Just, "Using Avatars for Improved Authentication with Challenge Questions," in *The Fifth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2011*, 2011.

[9] N. Micallef and N. A. G. Arachchilage, "A gamified approach to improve users' memorability of fall-back authentication," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, 2017.

[10] R. M. Ryan, C. S. Rigby, and A. Przybylski, "The Motivational Pull of Video Games: A Self-Determination Theory Approach," *Motivation and Emotion*, vol. 30, no. 4, pp. 344–360, dec 2006.

[11] M. V. Birk, C. Atkins, J. T. Bowey, and R. L. Mandryk, "Fostering Intrinsic Motivation through Avatar Identification in Digital Games," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*. New York, New York, USA: ACM Press, 2016, pp. 2982–2995.

[12] R. Carrasco, S. Baker, J. Waycott, and F. Vetere, "Negotiating stereotypes of older adults through avatars," in *Proceedings of the 29th Australian Conference on Computer-Human Interaction - OZCHI '17*. ACM Press, 2017, pp. 218–227.

[13] M. V. Birk and R. L. Mandryk, "Combating Attrition in Digital Self-Improvement Programs using Avatar Customization," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. New York, New York, USA: ACM Press, 2018.