Virtual Fingerprint - Image-Based Authentication Increases Privacy for Users of Mouse-Replacement Interfaces

Viktoria Grindle[1], Syed Kamran Haider[2], John Magee[1(✉)], and Marten van Dijk[2]

[1] Math and Computer Science Department, Clark University, 950 Main St,Worcester, MA 01610, USA
{vgrindle,jmagee}@clarku.edu
[2] Department of Electrical Engineering and Computer Science, University of Connecticut, Storrs, CT 06269, USA
syed.haider@uconn.edu, vandijk@engr.uconn.edu

Abstract. Current secondary user authentication methods are imperfect. They either rely heavily on a user's ability to remember key preferences and phrases or they involve providing authentication on multiple devices. However, malicious attacks that compromise a user's device or discover personal information about the user are becoming more sophisticated and increasing in number. Users who rely on mouse-replacement interfaces face additional privacy concerns when monitored or assisted by caregivers. Our authentication method proposes a way of quantifying a user's personality traits by observing his selection of images. This method would not be as vulnerable to malicious attacks as current methods are because the method is based on psychological observations that can not be replicated by anyone other than the correct user. As a preliminary evaluation, we created a survey consisting of slides of images and asked participants to click through them. The results indicated our proposed authentication method has clear potential to address these issues.

Keywords: Human-Computer Interaction · Mouse-replacement interfaces · Security · Privacy · Behavioral biometric · Authentication · Camera Mouse · Virtual Fingerprint

1 Introduction

We investigate privacy implications of users with severe motion impairments that use mouse replacement interfaces. Users of such interfaces interact with a computer via an on-screen pointer that is always visible to anybody who is also able to see the screen. This creates privacy concerns, for example, when such an interface is used with an on-screen keyboard to enter a password. We propose to use a "virtual fingerprint" to authenticate such users in a way that maintains privacy despite observation yet can be accomplished entirely on-screen with mouse-replacement interfaces.

M. Antona and C. Stephanidis (Eds.): UAHCI 2015, Part IV, LNCS 9178, pp. 182–191, 2015.
DOI: 10.1007/978-3-319-20687-5_18

We work with people who use the Camera Mouse [4] – a mouse replacement interface that tracks head motion to move a mouse pointer on the screen. Users of other pointer-manipulation interfaces such as trackballs, accessible joysticks, or head and mouth actuated controllers face similar issues. Previous investigations of this interface modality revealed that users were concerned about their privacy while using a variety of software programs [10].

Online social networks can be used to address loneliness and isolation issues that people with disabilities sometimes face. However, some challenges include lack of privacy (the caregiver is always present), lack of autonomy, and inadequate computer literacy of caregivers [2,5,9].

Users of the Camera Mouse typically use the software with a caregiver. It can be difficult to maintain privacy and security while authenticating (i.e., "logging in") to various services. Beyond social networks, users may need to authenticate to email, file or photo sharing, online banking, or health care-related services. Users are faced with a choice of letting a caregiver observe the password as it is entered in an on-screen keyboard, allowing the caregiver to know the password and enter it themselves, or trust them to look away as it is entered.

A "virtual fingerprint" is a behavioural biometric way to authenticate users of mouse-replacement interfaces that is tolerant to observation. It involves authentication through the selection of images. An initial investigation of this approach for secondary user authentication (e.g., replacement of security questions) was conducted.

2 Related Work

2.1 Graphical Passwords

Using images to authenticate a user has been studied in the past. One such common area of study is on the use of graphical passwords. Graphical passwords are intended to replace regular passwords [7]. These passwords are easier for the user to remember and are also more difficult to brute force since there are no weak passwords. A couple early studies tested how well graphical passwords could be used to authenticate users.

One early pioneering study, called "Deja Vu" [7], had participants select images they liked and then had them find the images later on among a large assembly of other random images. A second early study, "Hash Visualization" [11], also had users select previously seen images. However, these images used "random art" [11] (a randomly generated image) to generate an image for the user to memorize rather than having the user pick their own images. Both studies as well as others concluded using images for authentication is easier for users as well as just as secure as regular textual and numeric based passwords against brute force [8]. Numerous other studies have also been conducted in the area of graphical passwords. The glaring problem with these authentication techniques is that they are intended to provide the user with an easier time with passwords rather than to specifically prevent certain kinds of attacks. If the user's device is compromised or if a malicious attacker is observing the communication between a user and the

service provider they could still easily observe what images the user is clicking on (similar to observing what textual password a user is typing in) and use those images to log into the user's account in the future.

2.2 Biometrics

Recent research in the category of behavioral and physiological biometrics as authentication techniques [1] also has shown a lot of promise. Physiological biometrics are traits that can be used to distinguish one person from another such as a physical fingerprint, DNA sample, retina scan, and many others. Behavioral biometrics on the other hand focus more on behavioral traits and tendencies that define an individual. For example, observing how a user types or how they phrase sentences is a behavioral biometric. Other commonly studied behavioral biometrics to use for authentication purposes include observing "keystroke dynamics" and "mouse dynamics" [1].

One particular study tested out the effectiveness of using keystroke and mouse dynamics to detect "computer intrusions" [1]. The implementation they proposed and experiments conducted were shown to be extremely effective in detecting intrusion and identifying users. However, these biometrics still present issues. First of all, a lot of individual key and mouse habit data is needed to form a profile for the user. This tends to take time to gather and is not entirely feasible or convenient for a company to do for each of their users. Secondly, in order to record this data, special software usually needs to be installed on the client's machine. Lastly, although it would be significantly more difficult than with graphical passwords, if a malicious attacker is observing the user's mouse and/or key strokes they could potentially gather enough data to replicate the user's style in the future. This study intended for the implementation to be used to detect general computer intrusions rather than for a service provider to authenticate a user.

3 Methodology

A virtual fingerprint of a user is a measure of their personality and behavior. The fingerprint is created by a user upon account creation and stored in the system. Each subsequent time the user logs in they would go through a short series of slides which generates a fingerprint and compares it to the one currently stored for him to determine if its a close enough match. The slides contain images that correspond to previously determined personality categories. The categories and images are randomly selected with each generated slide. The categories are also unknown to the user or any other observer, making it difficult for a malicious attacker to replicate a user's personality pattern. A user is instructed to click on images he likes which are then used to form his personal image selection pattern, what we call his virtual fingerprint. The slides are generated based on an algorithm to test for particular features used to categorize users and derive correlation (Fig. 1).

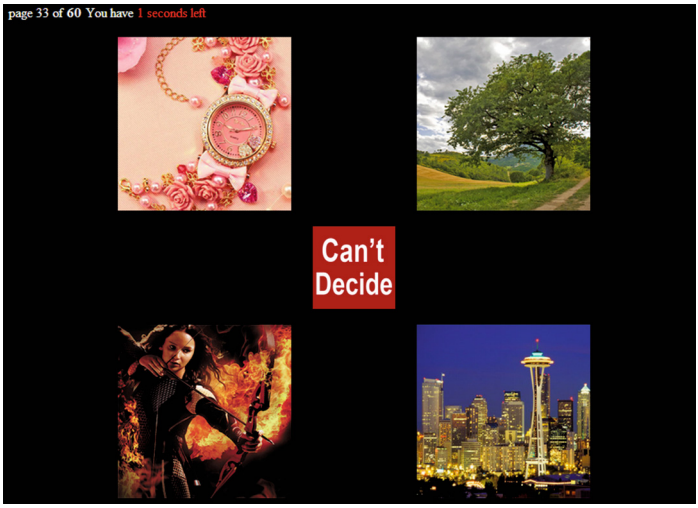

Fig. 1. Sample slide displaying 4 randomly selected images.

3.1 Design

In order to test out the potential effectiveness of using personality based images to authenticate a user we conducted a study that enrolled approximately 160 participants. This study was conducted using two online surveys. The first survey recorded responses from approximately 100 participants and the second from approximately 60 participants. Our participants were mostly volunteers from Amazon Mechanical Turk, which is an online service that allows users to take surveys and perform small tasks in exchange for compensation. The participants were required to be 18 years of age or older and be living in the USA. We created an online survey that consisted of 60 slides. Each slide contained 4 randomly selected images and each image corresponded to a particular personality category. No category was repeated on the same page and we developed an algorithm to make sure each category was seen an equal number of times. This prevented any unnecessary polluting of the results from a participant seeing some categories more than others. The image database consisted of a total of 224 images and 28 personality categories. Each category consisted of 8 images. Before deploying the second survey the image database was doubled. Each category then contained 16 images instead of 8 in order to see if having a larger number of images and less image repeats would affect the results. We also implemented a 5 s timer on each slide which refreshed the page if an image was not clicked. The timer was included in the survey design to promote an initial reaction from participants and prevent long periods of decision making from adding bias to the results. Each participant was instructed to simply select images they liked. Additionally, a'can't decide' button was added to each slide in case the participant had no immediate preference for any of the images.

Users of mouse-replacement interfaces would be able to complete this survey simply by moving the mouse pointer over the image they wish to choose. We hypothesized that the two features we tested for would be significantly different if a participant was looking at their own slides versus if they were looking at another participant's slides (Fig. 2).

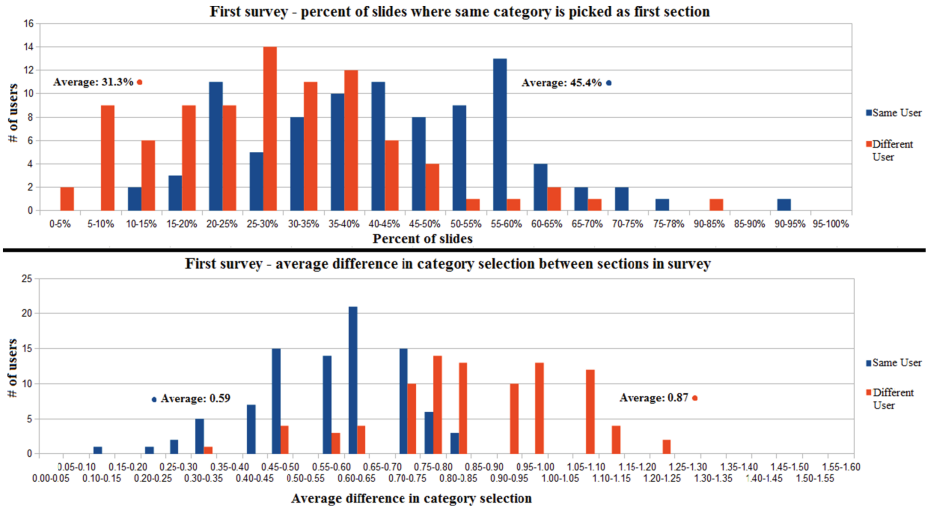

Fig. 2. Results of category selection from preliminary authentication experiment.

3.2 Feature Testing

After a user went through the first 20 slides, these 20 slides were selected again at random and shown to the same user. Each slide of this set of 20 contained the same 4 categories as a slide from the first set of 20. However, a different image was randomly selected from each category so neither an attacker nor a participant would be aware what slide or category he was being shown. This second set of 20 slides tested for one of two features. Firstly, it tested to see what percent of the time a participant would select the same category from a set of 4 categories as they did previously. This, we believed would be a much higher percentage than if the participant selected categories from another participant's set of first 20 slides. The second feature we tested for was overall variance in category selection. Each of the 28 categories was selected a certain number of times in a participant's first 20 slides. We compared that number to the number of times each category was selected in the next 20 slides and computed an average difference in same category selection. This, we believed would be a much smaller difference between category selection if a participant was looking at their own slides than if he was looking at another participant's slides. The third and final set of 20 slides randomly selected slides from a different randomly selected participant's first 20

slides. The purpose of this third set of 20 slides was to compare the features we tested for in the participant's first 20 slides with a different participant's first 20 slides. We hypothesized that the two features (mentioned above) we tested for would be significantly different if a participant was looking at their own slides versus if they were looking at another participant's slides. To determine how correct this assumption is, we performed linear regression analysis on the first half of the data set from the second survey (30 participants) and tested that model on the second half of the data set from the same survey as well as all of the data from the first survey (100 participants). The linear regression model quantified the correlation between the two features. It output a predicted value which was then compared to the actual value for each user. If the actual value was higher than the predicted, the authentication would be approved. If it was lower, the authentication would be rejected. This model had a correct positive and correct negative prediction rate which will be discussed in the next section.

4 Results

4.1 Distribution of Data

The second feature we tested for showed more weight in authenticating a user than the first feature. This can be seen in the normal distribution graphs for both features (Fig. 2). Participants on average selected the same categories on the same slides as they had previously 45.4 % (first survey) and 41 % (second survey) of the time. On the other hand participants only selected the same categories of another participant's slides as that participant had selected an average of 31.3 % (first survey) and 29.5 % (second survey) of the time. As for the second feature, participants on average had an average difference between overall category selection on their own slides of 0.59 (first survey) and 0.62 (second survey). They also on average had an average difference between overall category selection on another participant's slides of 0.87 (first survey) and 0.89 (second survey). It is obvious from the normal distribution that neither feature can solely be used to predict if a user is who they say they are or not. This is apparent from the overlap between a true user and a 'hacker' present in both normal distribution curves.

4.2 Regression Analysis

As mentioned previously both features were plotted against one another and analyzed using a linear regression model. After performing linear regression analysis on the first half of the data from the second survey, we came up with the following regression model: $Y = 45.596X\text{-}2.238$ where Y represents the percent of same categories picked and X represents the average difference in category selection. After running the rest of the data from the second survey through the regression equation, our model correctly predicted that a user was truly who he claimed to be (correct positive rate) 75 % of the time and correctly predicted that a user

Regression Model: Y = 45.596*X – 2.238 **Y** = percent of same categories picked as on previous slides **X** = average difference in category selection for each category	**First Survey** **Correct positive rate:** 78% **Correct negative rate:** 68% **Second Survey** **Correct positive rate:** 75% **Correct negative rate:** 75%
If actual user's Y > predicted Y **approve authentication** **else, reject authentication.**	

Fig. 3. Summary of linear regression statistics

was not who he claimed to be (correct negative rate) 75 % of the time as well. This created an overall accuracy rate of 75 %. In the first survey the correct positive rate was 78 % and the correct negative rate was 68 % which makes for an overall accuracy of 73 % (Fig. 3).

On a quick side note, as mentioned previously the second survey was designed the same as the first but with twice as many images to determine if authentication was affected by a participant seeing repeated images. From our results we concluded that doubled image database size had little effect on the accuracy (73 % is close to 75 %). The second survey also added a third set of 20 slides which tested for the same two features on the same random participant picked from the second set of 20 slides. This was designed to determine if a participant would have consistent results for both of their features if given another participants 20 slides twice. Our accuracy statistics above point to yes since there was about the same level of accuracy for each survey, one with the additional 20 slides and one without. Overall, it is clear that there is promising probability that our theory of using personality based images to authenticate a user could be a viable option (Fig. 4).

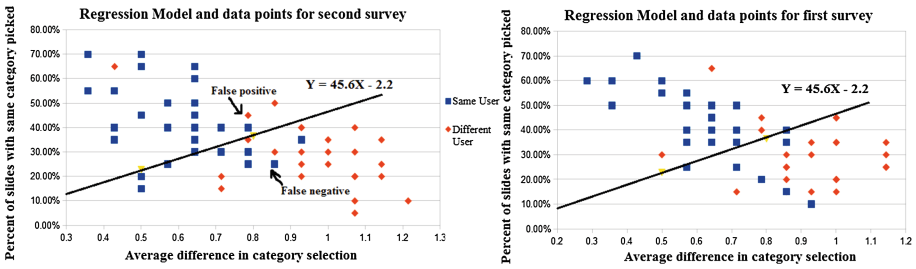

Fig. 4. Linear regression model.

5 Conclusion and Future Work

Although our regression model shows high potential for further implementation, there are a few weaknesses and concerns we noticed in the overall system. Firstly,

motivating users to be active participants that pay attention to their image selection can be difficult. Any amount of randomness to their selection technique will quickly lead to a false negative. Some users may find it inconvenient to go through 20 slides of images after providing their user name and passwords. For implementation in the real world, this technique might serve better as an optional authentication method, unless a service provider is able to turn the authentication into a type of game or reward system that will provide incentive for the user. The second issue is a vulnerability in dealing with a particular type of malicious attack. The proposed virtual fingerprint method is theoretically secure from a brute force attack. There are many possible answers to a set of N slides which grows exponentially in N. Finding the exact desired answer is therefore hard to find. Of course, the authentication procedure is threshold based and large subsets of possible answers will lead to authentication: in the study a malicious attacker has 25 % probability (for N=20) to be successful in correctly guessing a member of such a larger subset. This probability corresponds to being able to guess a set of answers whose"distance" to the exact desired answer is within some threshold. As N grows larger, a malicious attacker will have a much lower probability of achieving a successful guess. From the user perspective, a large N is user unfriendly. For this reason we will investigate techniques that allow to capture more authentication content per slide. The Virtual Fingerprint is also theoretically secure from device compromising, and observation of communication between a client and server, since the images are random and unpredictable and also only have significance to the user. However, the one point of vulnerability is if the attacker personally knows the user very well and could potentially predict what images the user will select. We consider it to be a low risk for an attacker to personally know the user that well. However, it is still worth testing out.

The accuracy of our regression model is high enough to be promising but low enough to indicate that much more research is needed to bring up the accuracy before this authentication method can be implemented in a real world setting. We plan on adding dimensions to our survey and re deploying it to test for further correlations and reduce overlap between 'true users' and 'hackers'. In this study we only tested for two features. However, adding an additional one or two features would create for a more accurate regression model and overall prediction. Additionally, we also plan to test to see if increasing the number of initial slides (which for this experiment was 20) will increase accuracy of the regression model. Also, more research is needed to better determine potential personality categories as well as what images are proper representatives of each personality trait. Lastly, after raising the accuracy for this study we plan on doing a time based analysis where we have participants do the survey twice with a certain amount of time (at least one month) in between. This will determine how well our method can authenticate a user repeatedly and over time.

Using the "virtual fingerprint" with mouse-replacement interfaces is a promising approach to providing privacy and security for users with disabilities. Improvements to the accuracy of the system via additional research is ongoing,

and user studies with people with disabilities are planned. We believe that this approach could be implemented as part of a password manager (software that stores user's passwords and fills them in automatically) or a strategy in an accessible authentication framework [3]. Such a password manager with virtual fingerprint authentication would provide a good level of usability and some level of privacy for our users.

Acknowledgments. The authors would like to thank their participants. We would also like to thank John Chandy for his extensive guidance and the University of Connecticut for hosting the Research Experience for Undergraduates where much of the study discussed in this paper was conducted. Lastly we would like to thank the NSF for providing funding through the CNS-1359329 grant.

References

1. Ahmed, A.A.E., Traore, I.: Detecting computer intrusions using behavioral biometrics. In: PST (2005)
2. Ballin, L., Baladin, S.: An exploration of loneliness: communication and the social networks of older people with cerebral palsy. J. Intellect. Dev. Disabil. **32**(4), 315–327 (2007)
3. Barbosa, N.: Strategies: an inclusive authentication framework. In: Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility (ASSETS 2014), pp. 335–336. ACM (2014)
4. Betke, M., Gips, J., Fleming, P.: The camera mouse: visual tracking of body features to provide computer access for people with severe disabilities. IEEE Trans. Neural Syst. Rehabil. Eng. **10**(1), 1–10 (2002). IEEE
5. Cooper, L., Baladin, S., Trembath, D.: The loneliness experiences of young adults with cerebral palsy who use alternative and augmentative communication. Augment. Altern. Commun. **25**(3), 154–164 (2009)
6. Denning, T., Bowers, K., van Dijk, M., Juels, A.: Exploring implicit memory for painless password recovery. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2011), pp. 2615–2618. ACM (2011)
7. Dhamija, R. Perrig, A.: Deja vu: a user study using images for authentication. In: Proceedings of the 9th Conference on USENIX Security Symposium, SSYM 2000, vol. 9. USENIX Association (2000)
8. Jermyn, I., Mayer, A.J., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: Usenix Security (1999)
9. Lewis, M.: Cerebral palsy and online social networks. In: The 12th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 2010). ACM, October 2010
10. Magee, J.J., Betke, M.: Automatically generating online social network messages to combat social isolation of people with disabilities. In: Stephanidis, C., Antona, M. (eds.) UAHCI 2013, Part II. LNCS, vol. 8010, pp. 684–693. Springer, Heidelberg (2013)
11. Perrig, A., Song, D.: Hash visualization: a new technique to improve real-world security. In: International Workshop on Cryptographic Techniques and E-Commerce, pp. 131–138 (1999)

12. Schmidt, A-D., Bye, R, Schmidt, H-G., Clausenm J., Kiraz, O., Yuksel, K.A., Camtepe, S.A., Albayrak, S.: Static analysis of executables for collaborative malware detection on android. In: IEEE International Conference on Communications, ICC 2009, pp. 1–5. IEEE (2009)