A Random Cursor Matrix to Hide Graphical Password Input

Alice Boit Thomas Geimer
Hochschule Bremen (University of Applied Sciences)

Jörn Loviscach*
Fachhochschule Bielefeld (University of Applied Sciences)

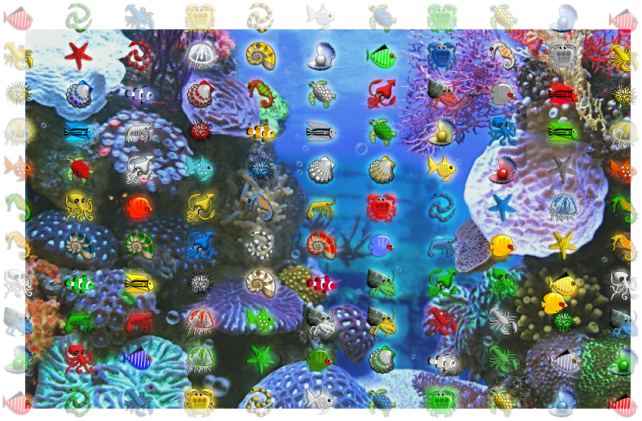

Figure 1: *The position of the matrix of cursor icons is coupled to the computer mouse. Icons moving past a boundary reappear on the opposite side, as indicated by the shapes outside of the frame.*

1 Introduction

Graphical passwords [Suo et al. 2005] address vital problems of textual passwords: Users pick from a limited vocabulary; machine-generated passwords are hard to memorize. Graphical input, however, faces "shoulder surfing," as bystanders can watch the screen. Current solutions to this problem tend to impose high cognitive loads. We propose an easy-to-handle approach.

First, the user selects a "home base" point on an image; this point serves as a login name. Then he or she clicks on a secret sequence of further secret points. These clicks are hidden from shoulder surfers because there is not only a single cursor on the screen, but a matrix of many different decoy cursors that move in parallel. To prohibit edge effects, a cursor that moves past the right border reappears one the left side, etc. To offer many memorable click spots, our prototype employs a detailed picture of a coral reef, see Figure 1. The cursor matrix is formed by 10×10 unique icons that depict various marine animals. These icons and the background image are customizable to cater for user-specific mnemonic strategies.

Each pair of cursor icon and secret point represents one step of the login sequence. For increased security, the user has to accomplish three rounds of selecting secret points. A shoulder surfer gains almost no information because the positions of the decoy cursors are shuffled randomly for every login. To break this scheme, an attacker has to record the position of each and every cursor for at least two login attempts of the same user: The cursor that is valid for a given step of the login sequence reveals itself as the only one that is positioned over the same spot in both login attempts.

2 User Tests

We conducted an Web-based test of the system. 54 participants took part actively; 31 completed the final survey. We recorded 936 login attempts, of which 76 percent were successful. The median of the time required was 29 seconds. Note that this number results from the time needed to find the specific icon in the randomized cursor matrix plus the time for dragging the icons to their destination location on the background image. Over the seven or more days that the test lasted per user, the median login time decreased by about a quarter, indicating a learning effect. 15 percent of the successful logins took less than 15 seconds, which demonstrates the feasibility of quick logins with our method.

58 % percent of the participants agreed that the method is a viable idea to replace normal logins. There was a split opinion on whether the graphical password is easier to remember than a textual one. The time needed to log in was an issue for most participants (52 %), but a majority (65 %) affirmed to have had fun using the system.

29 subjects who took part in a special treasure hunt (log in at least five times on the first day, five times on the second day, and five times after one week or later) were examined concerning the memorability of passwords. Only 12 were able to remember their first chosen password throughout the entire course of the experiment. Most forgot their first password on the same day they had chosen it, but nobody ever forgot his or her second password. This indicates that it is possible to remember a graphical password for a longer time. However, it takes some time to get used to the procedure. This is a general issue of graphical passwords and does not so much concern the specific should surfing problem we address here.

A basic parameter that influences the success rate is the tolerance with which the system accepts mouse clicks. Based on preliminary experiments, we chose a tolerance radius of 20 pixels on the image of 800×500 pixels. In the final test, 84 % of all clicks fell into that range. The radius allows a best-case estimate on the security: The probability to click three times correctly just by chance amounts to three in one billion. This naïve argument, however, only applies to blind clicking: The spots chosen by the users cluster around "hot spots," reducing the uncertainty from 8.3 to 6.0 bits per click.

3 Conclusion and Outlook

We have presented a graphical authentication method that requires only little mental effort from the user but is theoretically safe against one-time shoulder surfing, even when done with full recording. Since the hundred or more cursors overtax the memory of a human observer, shoulder surfing with the naked eye is hardly possible even if several logins of a single user can be overseen.

To better convey the idea of unlimited cursor motion, we want to conduct future tests with a trackball instead of a mouse. On top of that, the conspicuousness of the cursor icons can be improved so that are more memorable and can be discovered faster in the random matrix. Nor surprisingly, users in our tests preferred icons in strong primary colors and remembered them better. Future versions of the system should suppress the appearance of hot spots in the password choices. One part of the solution to this problem may be to capitalize on the fact that our system does not rely on selecting spots in an image alone, but builds on the associative value between an icon and a point in an image.

References

SUO, X., ZHU, Y., AND OWEN, G. S. 2005. Graphical passwords: A survey. In *Proc. ACSAC '05*, 463–472.

*e-mail: joern.loviscach@fh-bielefeld.de