Secure graphical password system for high traffic public areas

Bogdan Hoanca
Computer Information Systems, University of Alaska Anchorage, afbh@uaa.alaska.edu

Kenrick Mock
Computer Science, University of Alaska Anchorage, afkjm@uaa.alaska.edu

Graphical passwords are expected to be easier to recall, less likely to be written down and have the potential to provide a richer symbol space than text based passwords. For example, a user might authenticate by clicking a series of points on an image, selecting a series of tiles, or by drawing a series of lines on the screen [Davis et al. 2004]. An example of the tiled approach is the Real User Corporation's PassFaces™ system [Real User, 2005] illustrated in Figure 1. For both text and graphical password entry systems the user needs to carefully enter the password in case a malicious user is observing the session via "shoulder surfing." Although some authors assume that graphical passwords will be entered on a small screen with a reduced observation angle [Jansen 2004], and thus dismiss the likelihood of shoulder surfing, this assumption is not always true.

We propose to use a camera-based eye tracking system that operates as a gaze-based mouse. The user simply looks at an object on the screen and selects it via fixation or by pressing a button. To reduce the danger of shoulder surfing, no on-screen feedback is provided as to which image or location was selected. Due to the lack of on-screen feedback, calibration error, and the uncertainty in remembering an image location down to a specific pixel, our experiments indicate a reasonable cell size is 10x10 pixels. For a 600x400 display, a 10x10 pixel cell yields 2,400 selectable locations. If the user must select n=5 locations in sequence to authenticate, then the password space is 7.9×10^{16}, an order of magnitude stronger than an 8 character text password using any of 95 printable characters. In practice, many of these 2400 locations will be non-distinguishable. Users are more likely to select key points of interest along the edges of objects. We posit that each image has 30-50 distinguishable locations. This reduces the size of the password space to 30^n. Alternatively, for tiled images, each different tile would be a point of interest. A 6x6 grid of tiled images on a 400x400 pixel screen allows 66x66 pixel icons, much larger than the likely margin of error and with cryptographic complexity of the order 36^n.

We further refine the authentication algorithm to deal with both random errors (due to limitations in sampling) and systematic errors (due to improper calibration or because the user's head moved). To include the effects of random errors, we model the errors as randomly and uniformly distributed, with a high probability that the estimate gaze point corresponds to the actual gaze point, and with lower probability that the estimate is spatially close to but different from the actual gaze point (Figure 2). For simplicity, we consider a rectangular grid although a circular geometry would more accurately describe the situation. For authentication that requires selecting S successive points or tiles, the probability of k exact matches between the estimated and the fixated tile is given by a binomial distribution. Using conditional probabilities, we develop a "soft reject" model that relaxes the authentication requirements to account for the more likely failures due to random errors. The process could be further optimized by combining the conditional probabilities across immediately consecutive authentication attempts. The impact of the proposed soft reject is to relax the authentication rules and increase the likelihood that a legitimate user will authenticate successfully even in the presence of errors. The undesired effect of increasing false positives is much less pronounced.

We also present a scheme that accounts for systematic errors. This type of error is when the estimated gaze position and the actual gaze position differ by a constant translation vector. For example, the estimate could always be to the lower left of the actual. The cryptographic complexity of this scheme for a session that requires S screens to select data is equivalent to a session of S-1 screens with no tolerance for systematic errors.

Figure 1. PassFaces™ idea. Using images of faces for tiles, the user selects a face out of a series of faces for their password.

p_2	p_2	p_2
p_2	p_1	p_2
p_2	p_2	p_2

Figure 2. PDF for the estimated gaze point when the user is fixating the center (grey) tile. The probability is zero for remote tiles.

The system we are using to investigate eye-tracking based authentication is the Eye Response Technologies ERICA system and a notebook PC with 1 cm screen resolution. With a screen tiled in an 8x8 array and a session requiring three screens for authentication, the probability that a user authenticates successfully with the basic technique is approximately 0.73. In contrast, if using the eye tracking aware approach described here, the probability increases to 0.81. The cryptographic complexity is reduced by a similar amount, 0.81/0.73 = 1.11 (less than 0.15 bits of equivalent complexity).

REFERENCES

Davis, D., Monrose, F. and Reiter, M. 2004. On User Choice in Graphical Password Schemes. In *Proc. 13th USENIX Security Symposium*, San Diego, CA, USA.

Jansen, W. 2004. Authenticating Mobile Device Users through Image Selection. In *The Internet Society: Advances in Learning, Commerce and Security*, K. Morgan & M. J. Spector (Editors), v30, p 10.

Real User. 2005. Retrieved 12/21/05 from www.realuser.com.