EMBARGOED until June 24th 2014: 7 am EDT; 12 midday UK time

PeerJ
Your Peers, Your Science
Academic Publishing is Evolving

Facelock: a new password alternative which plays to the strengths of human memory

Forgotten passwords are a serious problem for both IT managers and users. The root of the problem is a trade-off between memorability and security: simple passwords are easy to remember but easy to crack; complex passwords are hard to crack but hard to remember. A newly proposed alternative based on the psychology of face recognition was announced today. Dubbed 'Facelock', it could put an end to forgotten passwords, and protect users from prying eyes.

Decades of psychological research has revealed a fundamental difference in the recognition of familiar and unfamiliar faces. Humans can recognize familiar faces across a wide range of images, even when their image quality is poor. In contrast, recognition of unfamiliar faces is tied to a specific image—so much so that different photos of the same unfamiliar face are often thought to be different people. Facelock exploits this psychological effect to create a new type of authentication system whose details were published today in the open-access journal PeerJ (http://PeerJ.com).

Familiarity with a particular face determines a person's ability to identify it across different photographs and as a result a set of faces that are known only to a single individual can be used to create a personalized 'lock'. Access is then granted to anyone who demonstrates recognition of the faces across images, and denied to anyone who does not.

To register with the system, users nominate a set of faces that are well known to them, but are not well known to other people. The researchers found that it was surprisingly easy to generate faces that have this property. For example, a favorite jazz trombonist, or a revered poker player are more than suitable — effectively one person's idol is another person's stranger. By combining faces from across a user's domains of familiarity—say, music and sports— the researchers were able to create a set of faces that were known to that user only. To know all of those faces is then the key to Facelock.

The 'lock' consists of a series of face grids and each grid is constructed so that one face is familiar to the user, whilst all other faces are unfamiliar. Authentication is a matter of simply touching the familiar face in each grid. For the legitimate user, this is a trivial task, as the familiar face stands out from the others. However, a fraudster looking at the same grid hits a problem—none of the faces stand out.

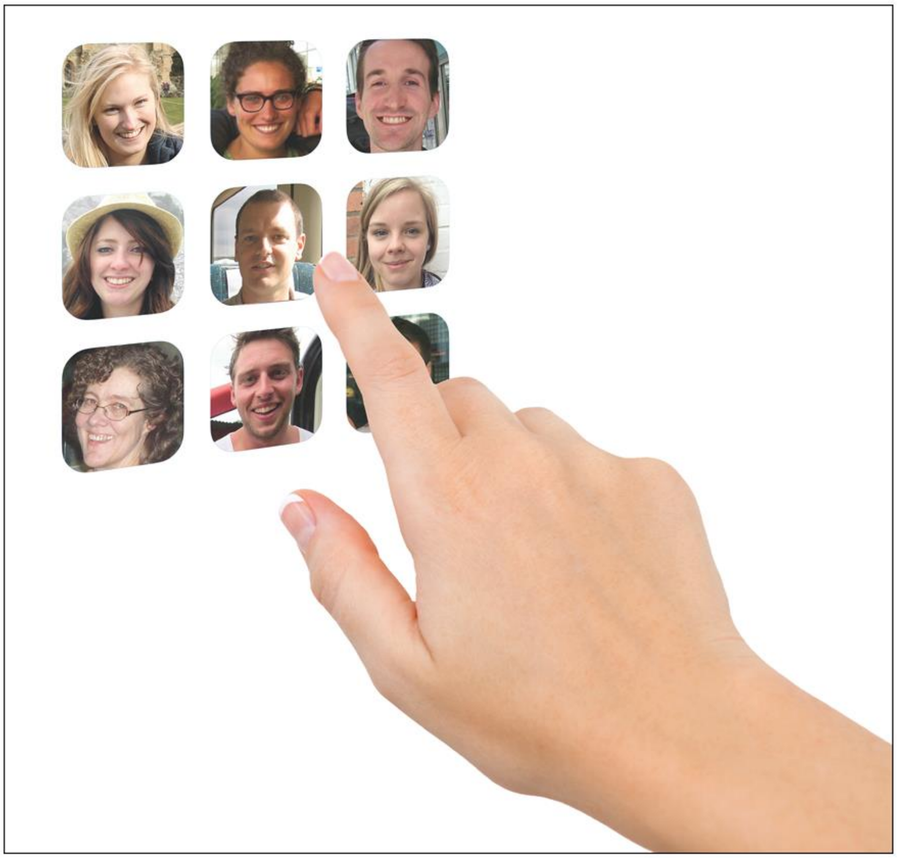
Building authentication around familiarity has several advantages. Unlike password or PIN-based systems, a familiarity-based approach never requires users to commit anything to memory. Nor does it require them to name the faces in order to authenticate. The only requirement is to indicate which face looks familiar. Psychological research has shown that familiarity with a face is virtually impossible to lose and so this system is naturally robust. In the current study, users authenticated easily even after a one-year interval. In contrast, disused passwords can be forgotten within days.

As well as being extremely durable, familiarity is very hard to fake. This makes the system difficult for fraudsters to crack. In the current study, the researchers asked volunteer attackers to watch a successful authentication sequence based on four target faces, so that they could pick out the same four faces from similar test grids. These attacks could be defeated simply by using different photos of the same faces in the test grids. For the user, who is familiar with the target faces, it is easy to recognize the faces across a range of images. For the attacker, who is unfamiliar with the target faces, generalizing across images is difficult.

Lead author, Dr Rob Jenkins of the University of York in the UK, said that “pretending to know a face that you don’t know is like pretending to know a language that you don’t know—it just doesn’t work. The only system that can reliably recognize faces is a human who is familiar with the faces concerned.”

The initial study elegantly combines the cognitive science of face perception and the computer science of secure authentication to work in sympathy with the strengths and limitations of human memory. It is hoped that software developers will now take this framework and turn it into a polished app, whilst other experts optimize the usability of the system. If those two things happen, you could see this system on your device in the next product cycle.

Image:



Text: Example of how Facelock could be implemented in practice.
Image Credit: Rob Jenkins – CC BY SA

###

EMBARGOED until June 24th 2014: 7 am EST; 12 midday UK time (i.e. the date of publication)

Link to the PDF of this Press Release: http://bit.ly/JenkinsPeerJRelease

Link to the Press Preview of the Original Article (this link should only be used **BEFORE** the embargo ends): http://static.peerj.com/press/previews/2014/06/444.pdf (note: this is a low-resolution author proof and so may change slightly before publication)

Link to the Published Version of the article (quote this link in your story – the link will ONLY work **after** the embargo lifts): https://peerj.com/articles/444 - your readers will be able to **freely** access this article at this URL.

Citation to the article: Jenkins et al. (2014), Facelock: familiarity-based graphical authentication. **PeerJ 2:e444; DOI 10.7717/peerj.444**

###

About PeerJ

PeerJ is an Open Access publisher of peer reviewed articles, which offers researchers a lifetime publication plan, for a single low price, providing them with the ability to openly publish all future articles for free. PeerJ is based in San Francisco, CA and London, UK and can be accessed at https://peerj.com/. PeerJ's mission is to help the world efficiently publish its knowledge.

All works published in PeerJ are Open Access and published using a Creative Commons license (CC-BY 4.0). Everything is immediately available—to read, download, redistribute, include in databases and otherwise use—without cost to anyone, anywhere, subject only to the condition that the original authors and source are properly attributed.

PeerJ Media Resources (including logos) can be found at: https://peerj.com/about/press/

###

Media Contacts

Note: If you would like to join the PeerJ Press Release list, visit: http://bit.ly/PressList

For the authors: David Garner (david.garner@york.ac.uk, +44 (0) 1904 322153), and Rob Jenkins (rob.jenkins@york.ac.uk)

For PeerJ: email: press@peerj.com , https://peerj.com/about/press/

###

Abstract (from the article):

Authentication codes such as passwords and PIN numbers are widely used to control access to resources. One major drawback of these codes is that they are difficult to remember. Account holders are often faced with a choice between forgetting a code, which can be inconvenient, or writing it down, which compromises security. In two studies, we test a new knowledge-based authentication method that does not impose memory load on the user. Psychological research on face recognition has revealed an important distinction between familiar and unfamiliar face perception: When a face is familiar to the observer, it can be identified across a wide range of images. However, when the face is unfamiliar, generalisation across images is poor. This contrast can be used as the basis for a personalised ‘facelock’, in which authentication succeeds or fails based on image-invariant recognition of faces that are familiar to the account holder. In Study 1, account holders authenticated easily by detecting familiar targets among other faces (97.5% success rate), even after a one-year delay (86.1% success rate). Zero-acquaintance attackers were reduced to guessing (<1% success rate). Even personal attackers who knew the account holder well were rarely able to authenticate (6.6% success rate). In Study 2, we found that shoulder-surfing attacks by strangers could be defeated by presenting different photos of the same target faces in observed and attacked grids (1.9% success rate). Our findings suggest that the contrast between familiar and unfamiliar face recognition may be useful for developers of graphical authentication systems.