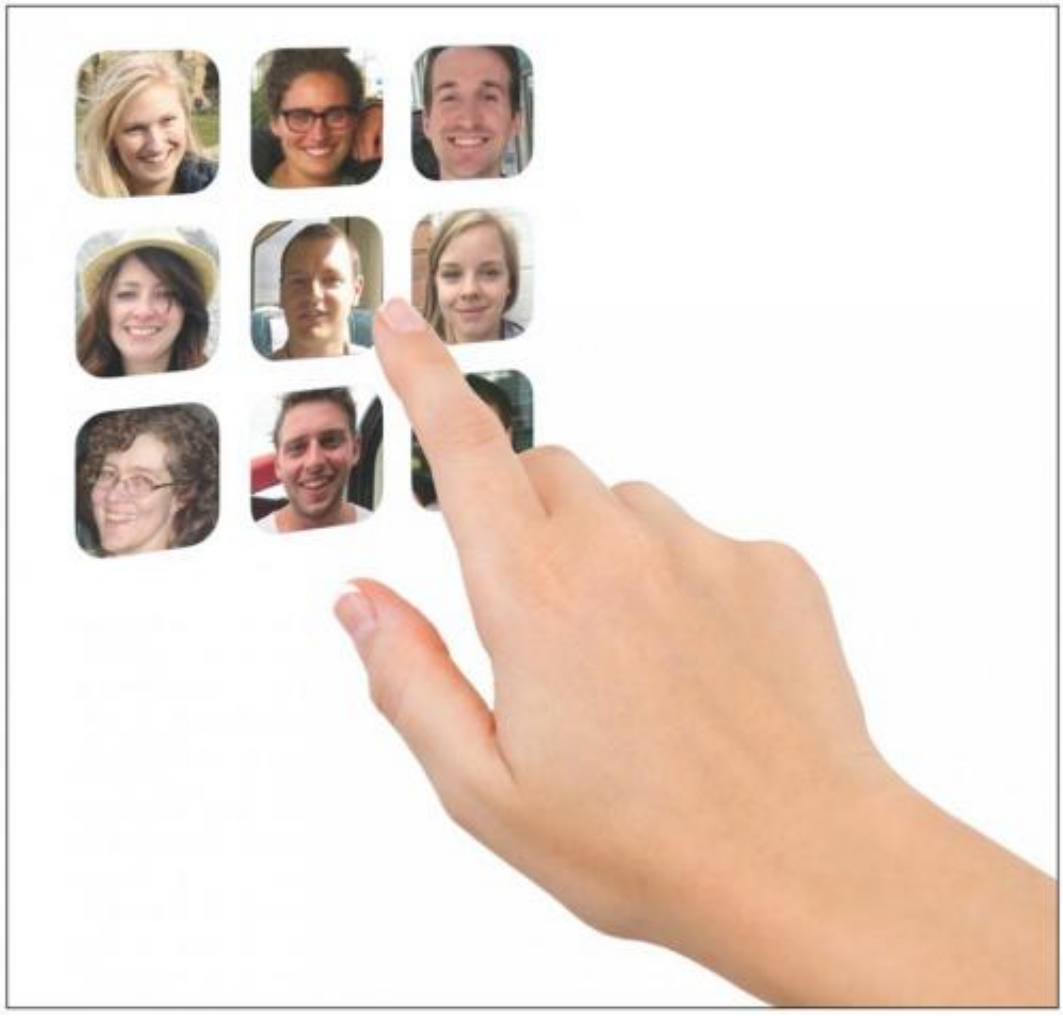
Facelock: A new password alternative which plays to the strengths of human memory

June 24 2014



An example of how Facelock could be implemented in practice. Credit: Rob Jenkins

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*.

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.

More information: *PeerJ*, peerj.com/articles/444

Provided by PeerJ

Citation: Facelock: A new password alternative which plays to the strengths of human memory (2014, June 24) retrieved 28 April 2024 from https://phys.org/news/2014-06-facelock-password-alternative-strengths-human.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.