Images and codes could provide secure alternative to multiple device password systems

December 23 2015

Credit: George Hodan/Public Domain

A system using images and a one-time numerical code could provide a secure and easy to use alternative to multi-factor methods dependent on hardware or software and one-time passwords, a study by Plymouth University suggests.

Researchers from the Centre for Security Communication and Network Research (CSCAN) believe their new multi-level authentication system GOTPass could be effective in protecting personal online information from hackers.

It could also be easier for users to remember, and be less expensive for providers to implement since it would not require the deployment of potentially costly hardware systems.

Writing in *Information Security Journal: A Global Perspective*, researchers say the system would be applicable for online banking and other such services, where users with several accounts would struggle to carry around multiple devices, to gain access.

They also publish the results of a series of security tests, demonstrating that out of 690 hacking attempts - using a range of guesswork and more targeted methods - there were just 23 successful break-ins.

PhD student Hussain Alsaiari, who led the study, said: "Traditional passwords are undoubtedly very usable but regardless of how safe people might feel their information is, the password's vulnerability is well known. There are alternative systems out there, but they are either very costly or have deployment constraints which mean they can be difficult to integrate with existing systems while maintaining user consensus. The GOTPass system is easy to use and implement, while at the same time offering users confidence that their information is being held securely."

To set up the GOTPass system, users would have to choose a unique username and draw any shape on a 4x4 unlock pattern, similar to that already used on mobile devices. They will then be assigned four random themes, being prompted to select one image from 30 in each.

When they subsequently log in to their account, the user would enter

their username and draw the pattern lock, with the next screen containing a series of 16 images, among which are two of their selected images, six associated distractors and eight random decoys.

Correctly identifying the two images would lead to the generated eight-digit random code located on the top or left edges of the login panel which the user would then need to type in to gain access to their information.

Initial tests have shown the system to be easy to remember for users, while security analysis showed just eight of the 690 attempted hackings were genuinely successful, with a further 15 achieved through coincidence.

Dr Maria Papadaki, Lecturer in Network Security at Plymouth University and director of the PhD research study, said: "In order for online security to be strong it needs to be difficult to hack, and we have demonstrated that using a combination of graphics and one-time password can achieve that. This also provides a low cost alternative to existing token-based multi-factor systems, which require the development and distribution of expensive hardware devices. We are now planning further tests to assess the long-term effectiveness of the GOTPass system, and more detailed aspects of usability."

More information: H. Alsaiari et al. Secure Graphical One Time Password (GOTPass): An Empirical Study, *Information Security Journal: A Global Perspective* (2015). DOI: 10.1080/19393555.2015.1115927

Provided by University of Plymouth