Selected for the Royal Society's SUMMER SCIENCE EXHIBITION 08

Graphical passwords: will your doodle keep the hackers away?

Dr Jeff Yan, Mr Paul Dunphy, Mr Ahmad El Ahmad, and Mr David Griffiths,
School of Computing Science, Newcastle University

Secure and usable authentication

Background

Today, the use of passwords is commonplace in everything from mobile phones to cash machines and computers. Many people have lost money or sensitive personal information because their password was cracked. Most of us have forgotten a password at least once.

The boom in Internet use means that people have to manage more passwords than ever before. For each online account, users are told they must follow stringent password management rules. These rules increase the cognitive load on the users, and increase the likelihood that they will adopt insecure practices. Recurring examples include writing down passwords, using the same password for multiple accounts, choosing guessable passwords and the list continues.

Many of the deficiencies of passwords arise from the limitations of human memory.

Numerous cognitive and psychological studies have revealed that people perform far better when remembering pictures rather than words: as the saying goes, a picture is worth a thousand words. This has inspired fast growing research into the design of graphical password systems in research communities. A graphical password is typically a pictorial secret that people can use to authenticate themselves to computer systems, and that are usually input to a computer with the aid of graphical devices such as mouse and stylus. Graphical passwords offer the possibility of addressing known weaknesses in text passwords, and therefore are usually considered a promising alternative in many contexts.

The science behind the research

Background Draw a Secret (BDAS) is a novel graphical password scheme we have developed at Newcastle University, England. Extending the Draw a Secret (DAS) scheme developed by researchers from New York University, Bell Labs and AT&T Labs, BDAS delivers much enhanced usability and security. It is the first graphical password scheme that shows promise to outperform text passwords in terms of security and usability.

In BDAS, a password is a free-form drawing that a user creates on a grid underlaid with a background image of their choice (see Figure 1). This scheme records the grid cells the user enters whilst creating their drawing. The drawing does not have to be re-created exactly. It is recognised as identical if the encoding is the same (ie the same cells are crossed in the same order), not the drawing itself. This allows for some margin of error, making the system more flexible.

Figure 1: BDAS on a Personal Digital Assistant. (PDA) (copyright © Newcastle University).

We tested a selection of background images for people to draw on, such as a playing card, a crowd or a flower. But most everyday pictures as the one in Figure 2, are also suitable as background in the BDAS system.

Those who took part in testing this new system created passwords that were much more secure than the state of the art, and most testers also found them easy to remember. The background image is key to this technique's success - it encourages people to make their drawing passwords more complicated and less predictable, and aid people to re-create them in the correct locations on the drawing grid. Potentially, BDAS is also very good for people with dyslexia or who can't read or write well.

Our experimental studies compared DAS and BDAS use. The BDAS passwords recalled in a one-week memorability test were, on average, more complicated

than their DAS counterparts by a factor of more than 1024. This means that the memorable BDAS passwords improved security by a factor of more than 1024. They were also more secure than text passwords by an even larger factor.

In particular, we observed that user drawings in the BDAS group show:

- increased complexity as users are able to add more components to drawings with a reduced cognitive burden over DAS
- reduced reliance on global symmetry to create memorable drawings
- reduced reliance on centring drawings for memorable placement

That is, with the aid of a background image, people tended to construct significantly more complex passwords, and other predictable characteristics such as global symmetry and centering within the drawing grid that leads to weak passwords were also reduced.

In the meantime, participants found BDAS passwords just as easy to remember as their DAS counterparts. 95% BDAS users were able to re-recreate their passwords within three attempts one week later.

The most exciting feature of BDAS is that, with a simple enhancement, it provides significantly enhanced usability and security simultaneously.

The future

Our BDAS system potentially provides a secure and usable authentication solution for handheld devices such as the PDAs and phones of tomorrow, and it could soon be expanded to other areas.

A key step to evolve the BDAS system is to move our experiment out of the laboratory setting - we are exploring a number of interrelated usability and security issues that are crucial to the real world uptake of the BDAS system, for example:

- What will make good background images? In other words, what images will not introduce a negative security bias or reduce memorability?
- Can people remember *multiple* strong BDAS passwords, and what can improve that memorability?
- *Shoulder surfing* is a threat in which attackers steal passwords by simply looking over the victim's shoulder. But, how serious a threat shoulder surfing would be for BDAS? If necessary, what is the most effective mechanism for defending against such a threat?

Figure 2: An everyday picture can be used as background in BDAS. (copyright @ LC)

Acknowledgement

This exhibit is sponsored by Microsoft Research and the Engineering and Physical Sciences Research Council (EPSRC). EPSRC is a member of Research Councils UK, the strategic partnership of the seven UK Research Councils.

Further information

Website of the BDAS Project http://homepages.cs.ncl.ac.uk/jeff.yan/bdas.htm
Research Team's website http://homepages.cs.ncl.ac.uk/jeff.yan/lab.html
School of Computing Science, University of Newcastle http://www.cs.ncl.ac.uk/
University of Newcastle http://www.ncl.ac.uk/