Inkblot Authentication

A. Stubblefield, D. Simon,

Microsoft Research Technical Report
MSR-TR-2004-85, 16 pp., August 2004

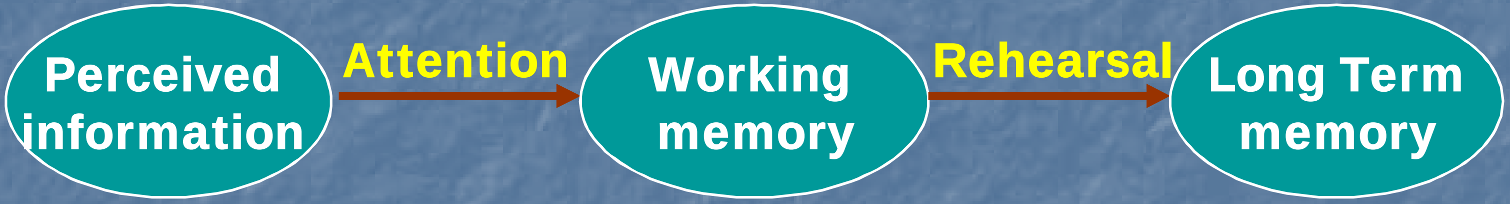
Presented by : Bo Jin

Summary

- Purpose： Help users select, remember, and differentiate robust password.
- Methodology ： Ask a user to form semantic associations with a set of randomly generated inkblot-like images and then authenticate the user based on the image associations
- Theoretical Support： Humans can remember pictorial representations more readily than textual or verbal representation (Recognition VS Recall).
- Benefits： Chosen password high in entropy (more secure) and memorability (Easy to remember).

appreciative comment

- Benefits in combinations of graphical and algorithmic approaches to choosing password
  - Save efforts in memorizing processes



Normal Processes in memory

With the help of the inkblot image, users do not need to go through the normal processes involved in memorizing or retrieving information form our brain (Recall) or other supporting materials. Instead, what we need simply do is to retrieve a semantic association from the currently presented image (Recognition).

appreciative comment (continued)

- Benefits in combinations of graphical and algorithmic approaches to choosing password

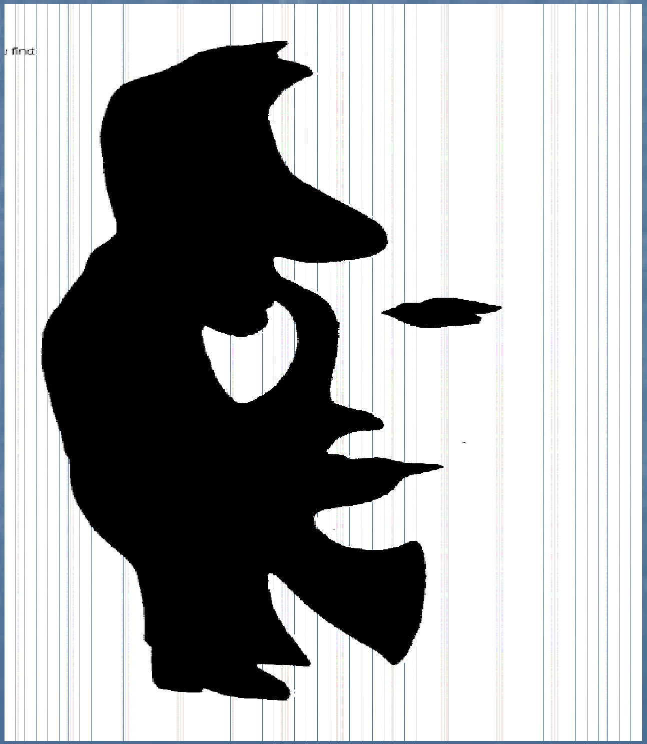
  - ➢ High entropy by employing computable hash function

  This scheme recommends users to hash their association down to a few characters which contain most of the entropy . Since these associations are user-specific, it is definitely much securer than traditional text-based password selection criteria such as user randomly selected password or pass phrase

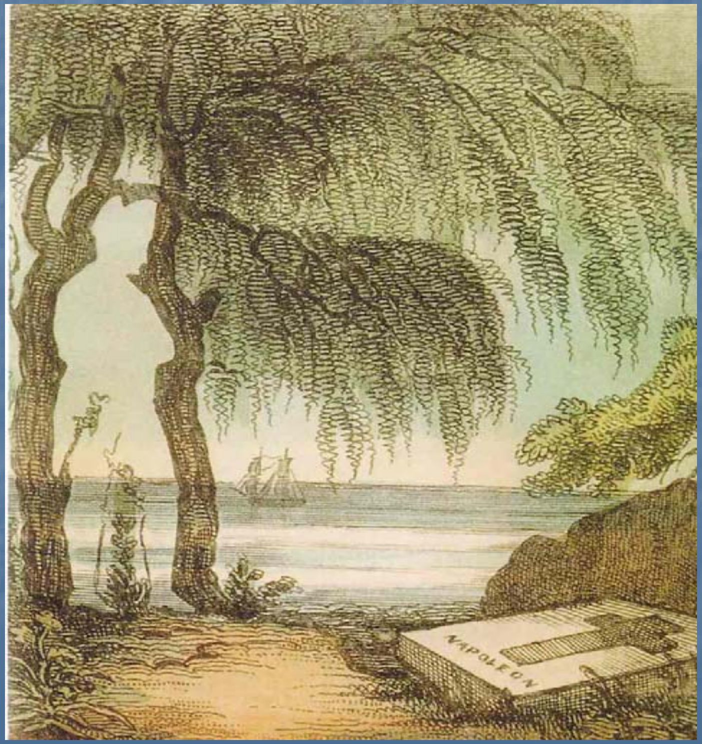
Critical comment 1

- Does it really work ?
  - Can users really generate an unique association?

Perceptual ambiguity



What do you see in this picture ?



How about this ?

Critical comment 1

- Does it really work ?
  - With respect to humans' inherent capacities

Humans are not machines, making mistakes sometime is unavoidable.

Even the authors admit that chances are one out of ten that users will recognize an association incorrectly and have to modify the system to tolerate the inevitable mistake

By allowing that, it might leave a backdoor for attackers.

Critical comment 2

- Are their claimed experimental results statistically significant ?

Although their data set is extensive “a group of self-selected users drawn from researchers, programmers, testers, administrative assistants, and secretaries”, it is not sufficient enough to represent the real population (Sample VS. Real population).

It is important to give evidence that the sample is statistically valid

My recommendation : Statistical hypothesis test such as Student's T-test

Discussion

Memoryfree and authors proposed high secure password

Conventional text-based password with Well-known selection criteria

Which side do you want to choose?

Thank you for your attention