Towards reliable storage of 56-bit secrets in *human* memory

Joseph Bonneau
Princeton University

Stuart Schechter
Microsoft Research

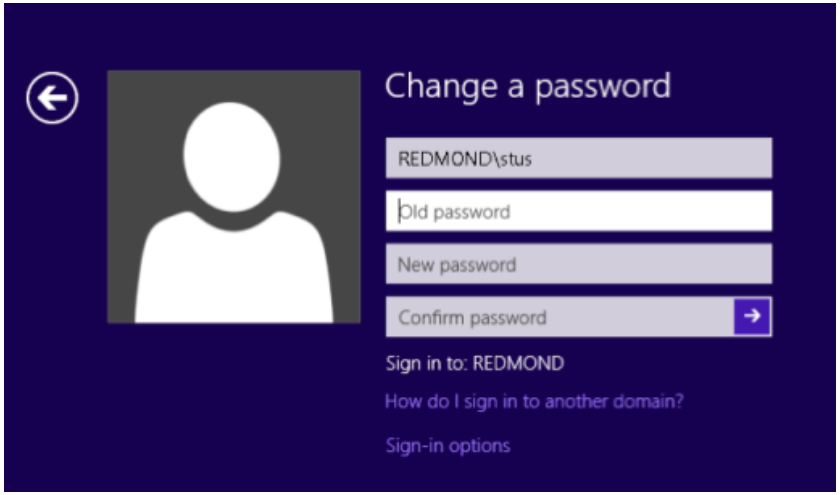
SOUPS 2014 lightning talk (to appear at Usenix Security)

Sometimes, a really strong secret is actually worth some effort

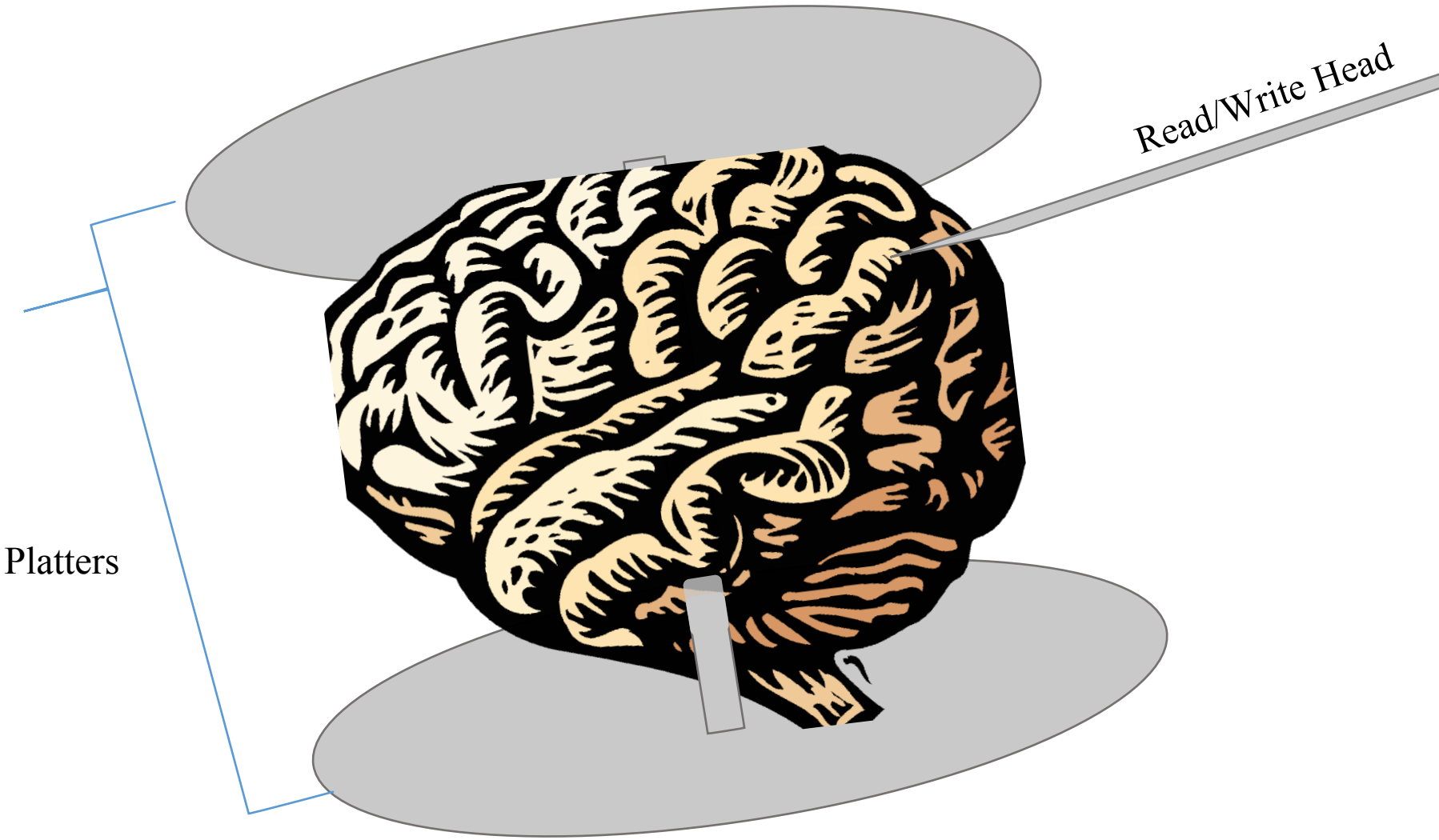
LastPass ****

iCloud Keychain

1Password



How to store secrets in humans?



Modeling human memory as a disk

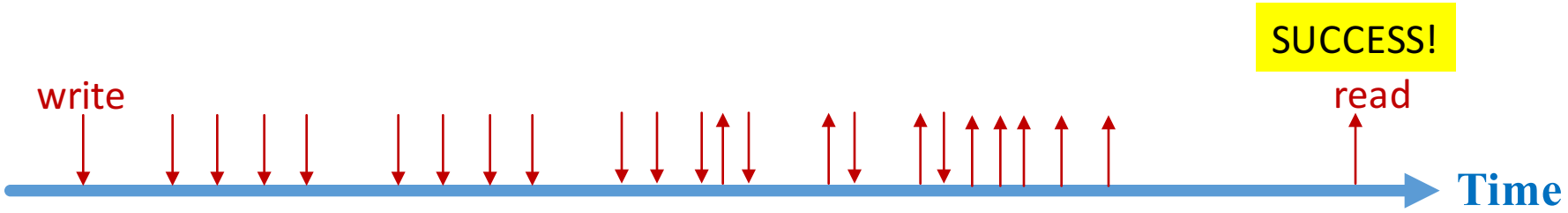
Humans are incapable of securely storing high-quality cryptographic keys… they are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.

Kaufman, Perlman and Speciner
Network Security: Private Communication in a Public World
2002

A more accurate model for human memory

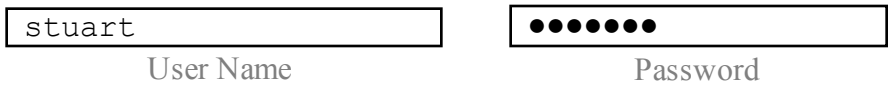
http://en.wikipedia.org/wiki/File:Wavecut_platform_southerndown_pano.jpg

Learning through spaced repetition



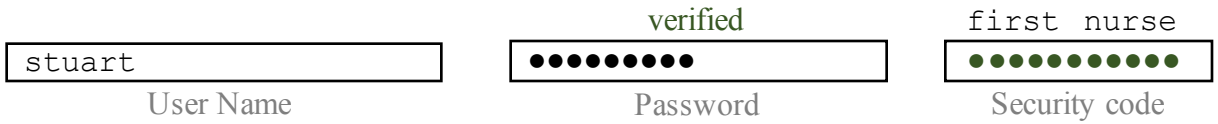
Spaced repetition for passwords

Step 1: Type user-chosen password



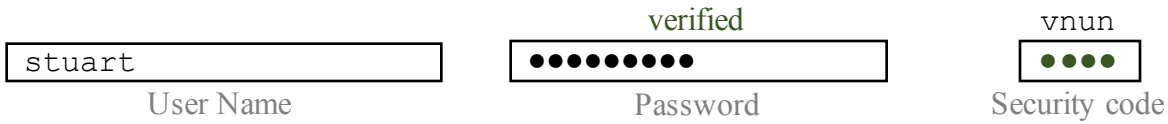
Spaced repetition for passwords

Step 2a: Type the random words as displayed



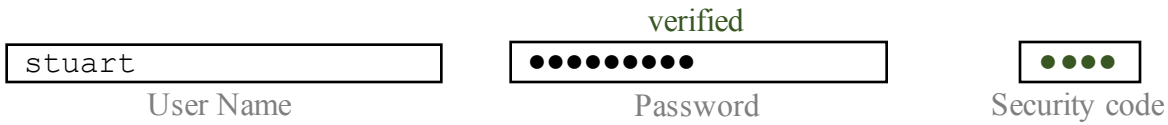
Spaced repetition for passwords

Step 2b: Type the random characters as displayed



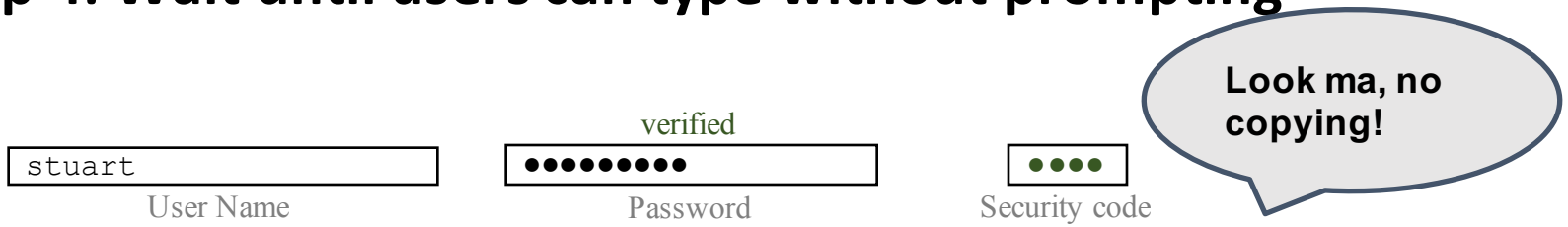
Spaced repetition for passwords

Step 3: Add increasing delays before showing the hint



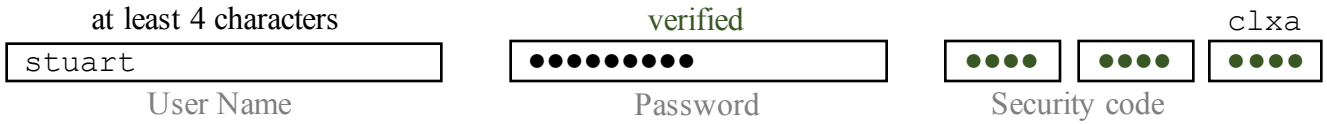
Spaced repetition for passwords

Step 4: Wait until users can type without prompting



Spaced repetition for passwords

Step 5: add more codes and repeat



https://experiment.research.microsoft.com/

29:52 until next Attention Ex...

Microsoft Research Attention Study

Instructions

Watch for a word to appear in one of the two boxes below.

If the word "left" appears in either box, type 'f'.
If the word "right" appears in either box, type 'j'.

Lower scores are better. Keep your score low by responding as quickly and as accurately as possible.

You have now completed 6 of the 60 attention tests required by Tuesday February 4 at 08:47AM.

Time remaining until you may perform your next attention test:

29:52

Time remaining (seconds):	0	Total response time (ms):	12662
Number of incorrect responses:	0	Penalty for incorrect responses (1000 each):	0
Number of correct responses:	9	**Your score** (total response time + penalty):	12662

If you have any questions or problems with this experiment, please contact the researchers at msrstudy@microsoft.com.

But will it work?

	Control		*Letters*		*Words*		*Total*	
Signed up for the 'attention' study	41		92		90		223	
Quit after 2 or 3 games	0/41	0%	9/92	10%	12/90	13%	21/223	9%
Otherwise failed to finish	6/41	15%	14/92	15%	12/90	13%	32/223	14%
Completed the 'attention' study	35/41	85%	69/92	75%	66/90	73%	170/223	76%
Received full security code	—		63/68	93%	64/65	98%	127/133	95%
Typed entire code from memory	—		62/63	99%	64/64	100%	126/127	99%

(after 3+ days)

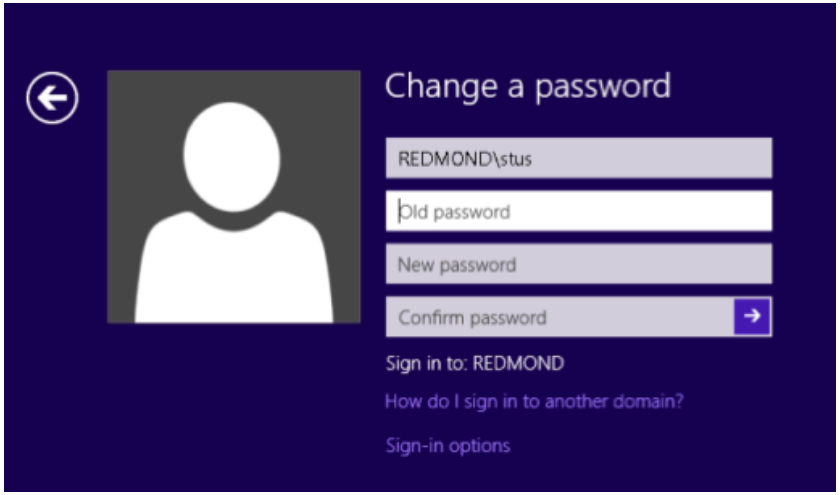
(after 17+ days)

Some passwords are worth 5-10 aggregate minutes of training

LastPass ****

iCloud Keychain

1Password



Lots of memory training effects!

- **Generation effect**
  - Make users fill in the blanks
- **Depth of processing effect**
  - Make users convert the password
- **Dual coding effects**
  - Show multiple versions

Try it yourself!

experiment.research.microsoft.com

"It was surprising that you did this follow up, because I did not expect it. After having to enter the codes so many times, the words are branded into my brain."