Towards Implicit Visual Memory-Based Authentication

Claude Castelluccia, Inria Grenoble
Markus Dürmuth and Maximilian Golla, Ruhr-University Bochum
Fatma Deniz, University of California, Berkeley

Types of Authentication

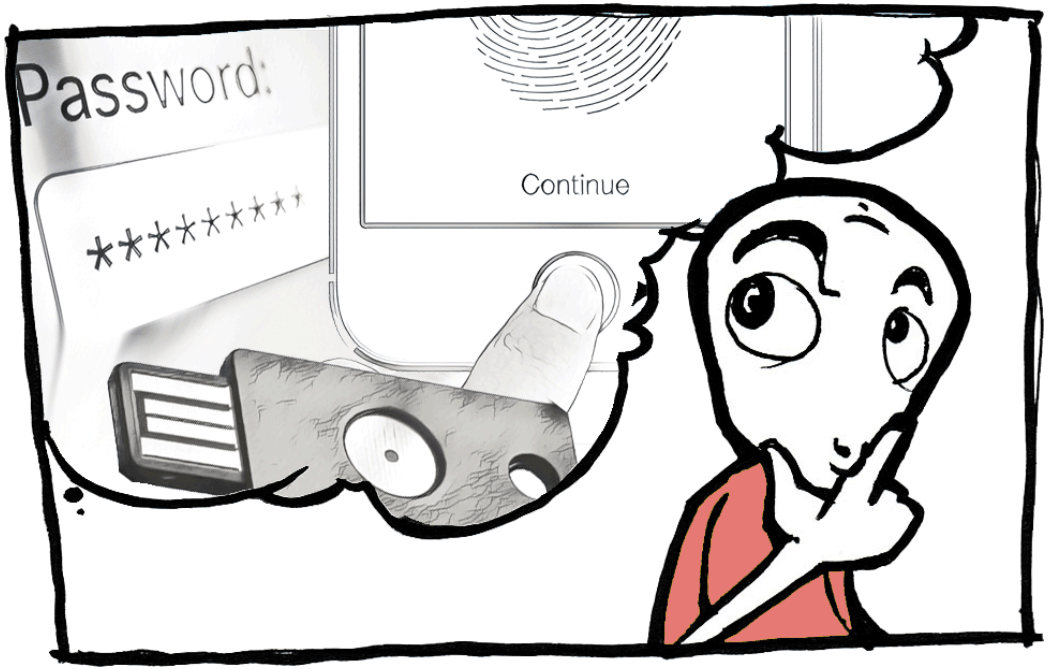
Competing requirements of **security** and **usability**. [1]

Common Factors:

1) Knowledge (Password, PIN)
2) Biometrics (Fingerprint, Face)
3) Possession (Token)

Reinforced by:

- 2-Factor Authentication
- Risk-based Authentication
- Continuous Authentication



[Ref. 1] Joseph Bonneau et al.: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. (SP '12)

Knowledge-based Authentication

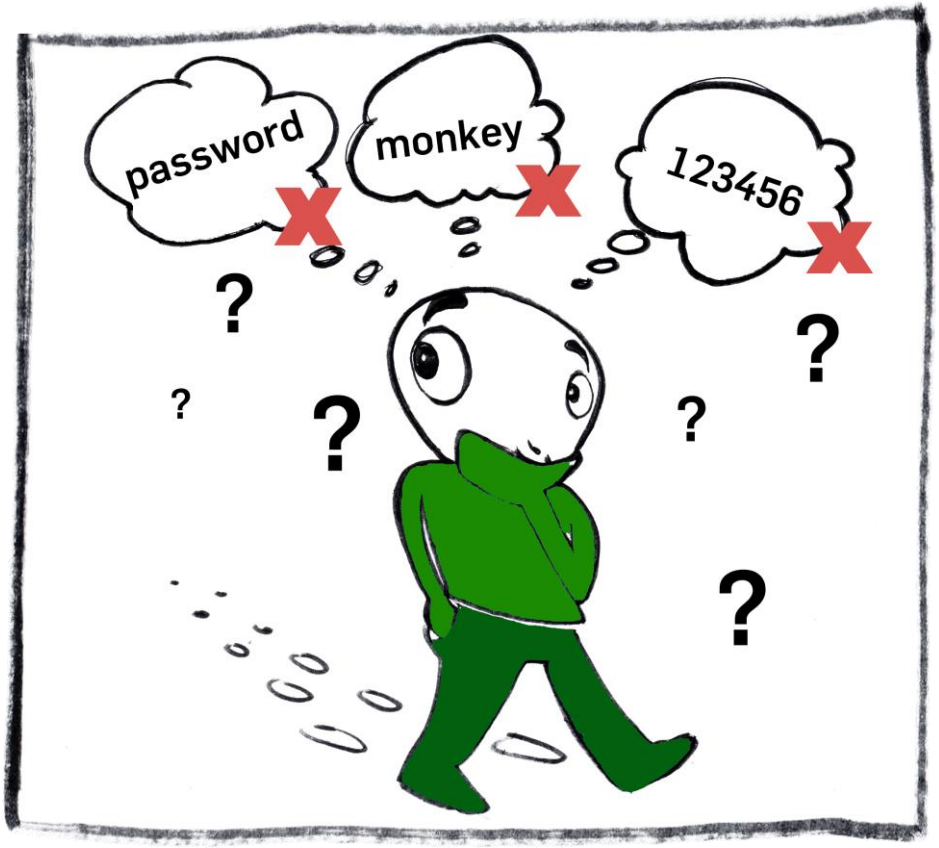
Example: Passwords

1) Create a secure password
2) **Remember the password**
3) Provide at time of authentication

All steps involved are hard for users.

→ High cognitive burden

→ Password reuse
→ Password resets



Fallback Authentication

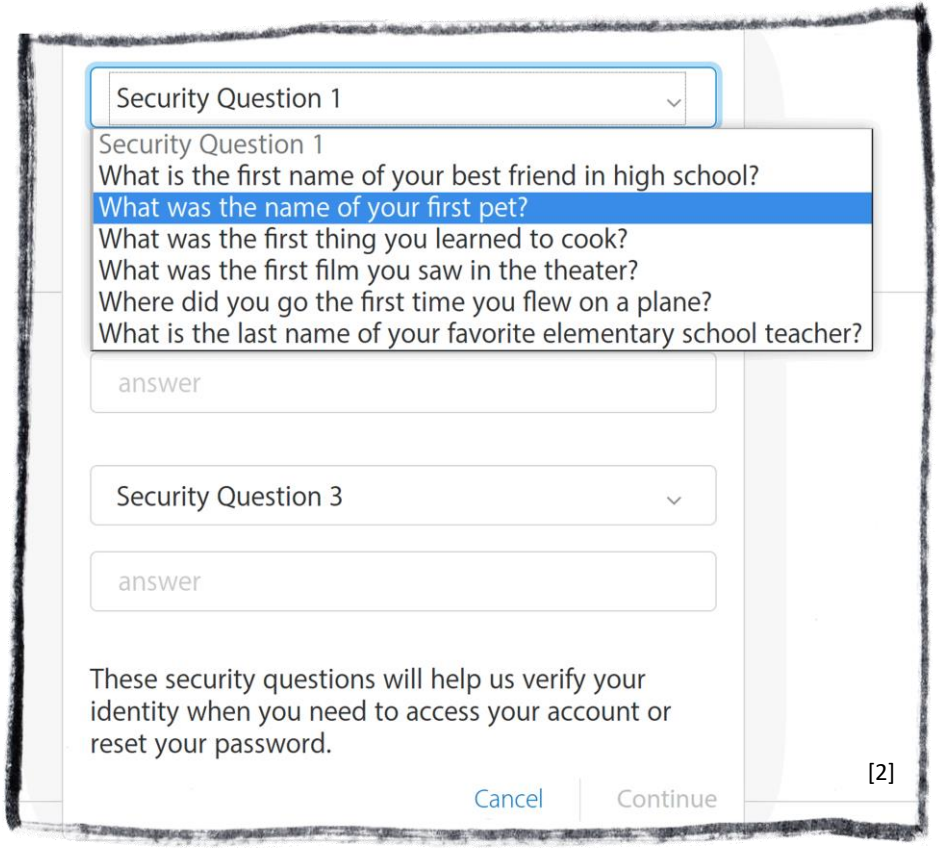
Used to regain access if the primary means of authentication is lost!

Different:

- Memorability
- Rate limiting
- Time required to authenticate

→ Often the weakest link in the chain (Sarah Palin, Mat Honan, …)

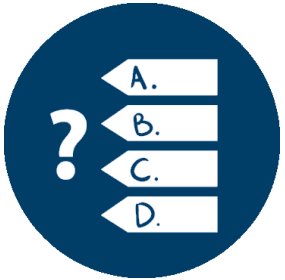
→ We need to design better systems!



[2]

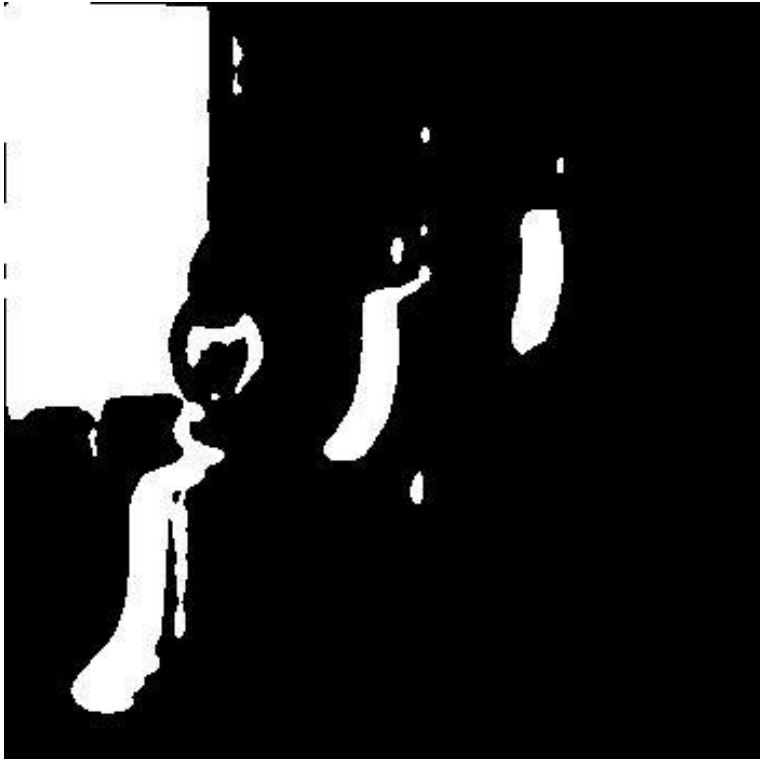
[Ref. 2] Joseph Bonneau et al.: Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. (WWW '15)

Let’s Play



Before we start, a short game.

Priming



Priming

Priming

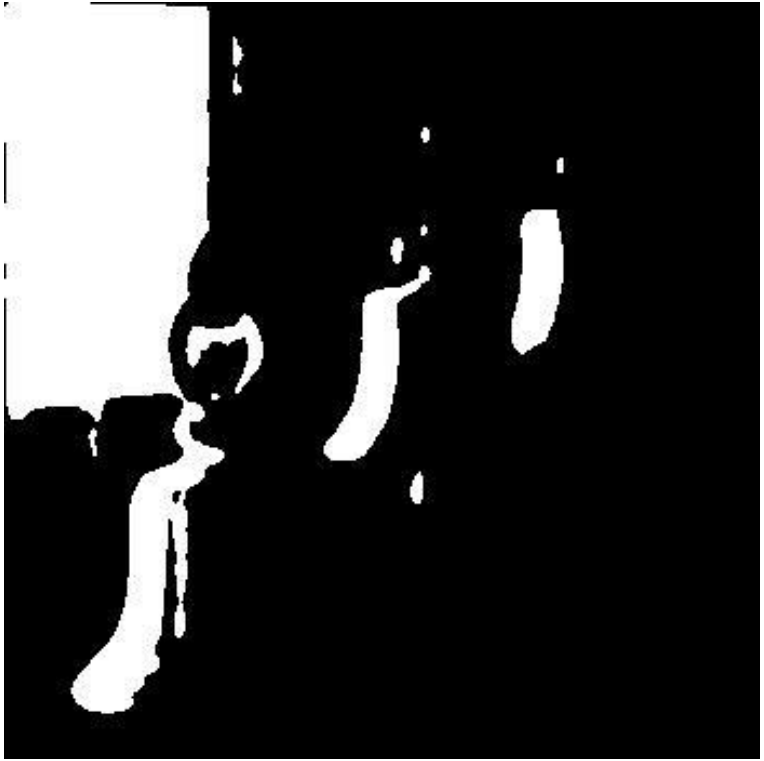
Bells

Priming

Bells

Priming

Bells



Priming

Priming

Priming

Cows

Priming

Cows

Priming

Cows

Mooney Images

Thresholded two-tone images showing a single object.

Recognition:

- Hard to recognize at first sight
- Sudden recognition (aha! / Eureka-effect)
- Intrinsically / By marking the contour of object / Showing the original image

Value for Authentication?

- Trigger brain processes involved in **implicit memory**.

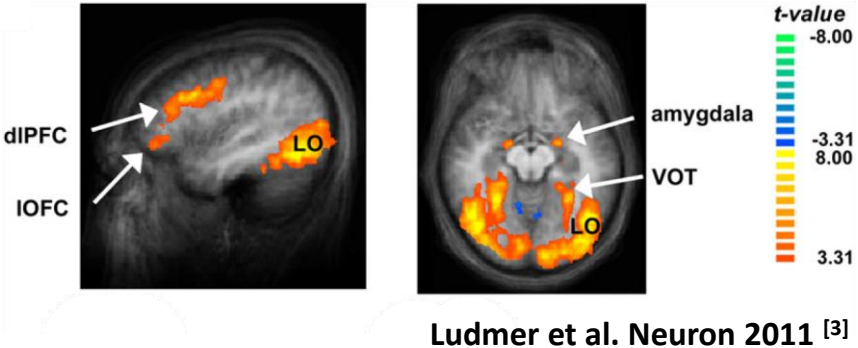
Implicit Memory

Unintentional recollection of information.

Can be observed in *habitual* behavior, i.e., riding a bike, playing an instrument.

We are not aware of the information stored in our memory.

We can trigger the implicit memory by a process called *priming*.

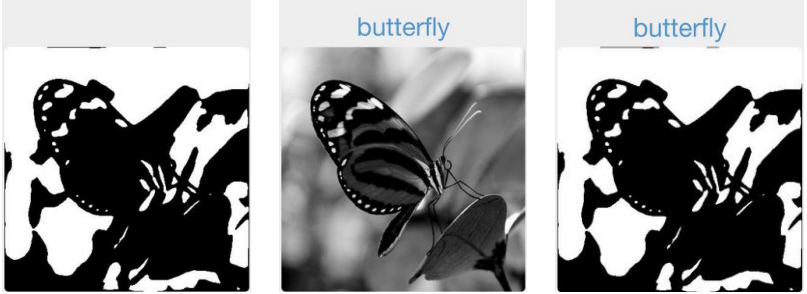


Ludmer et al. Neuron 2011 [3]

[Ref. 3] Rachel Ludmer et al.: Uncovering Camouflage: Amygdala Activation Predicts Long-Term Memory of Induced Perceptual Insight. (Neuron '11)

MooneyAuth

Relieves users of the cognitive burden of remembering an explicit password.

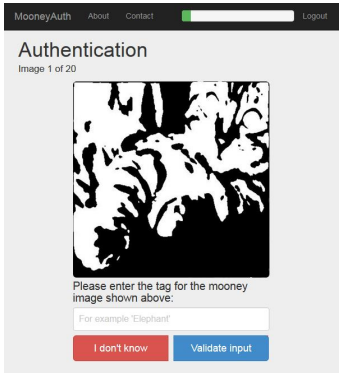


1) Enrollment / Priming:

- Prime on set of random Mooney images.
- We show every image twice.

2) Authentication:

- Primed + non-primed Mooney images are presented to the user.
- User is requested to label the images.
- Scoring algorithm based on surprisal of observed events.
- User authenticated: score > threshold.

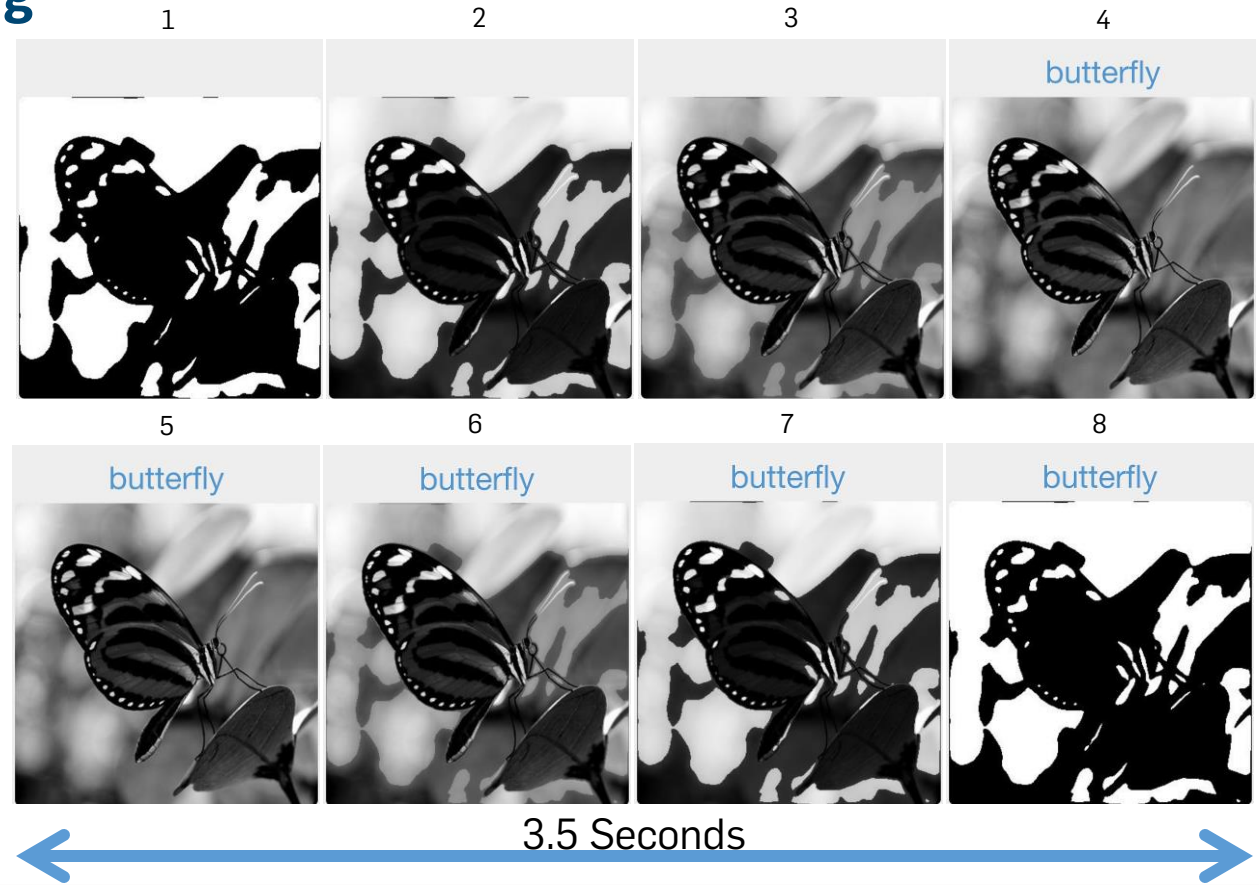


Enrollment / Priming

- Smooth transition

- Takes 3.5 seconds per image.

- In a user study we primed 10 images



Authentication

Primed + non-primed images are presented.

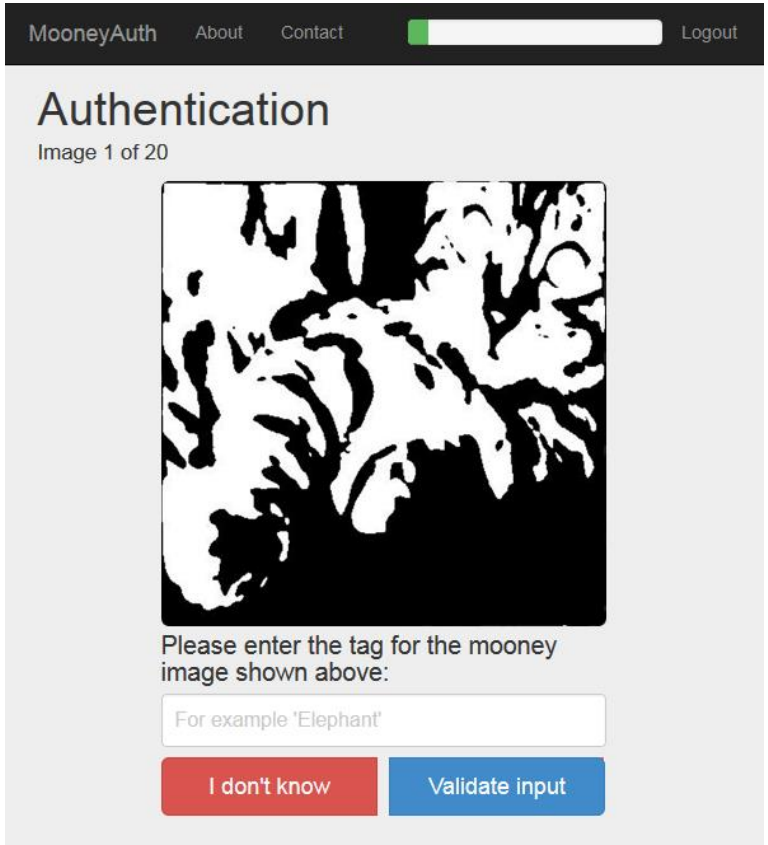
Task:

User has to **label** the image

or

skip by pressing the I don't know button.

Assumption:
User labels primed images more often correctly (and faster).



Scoring

- Score derived from the self-information (surprisal) of the observed events.
- There are four events that can occur:

	Correct Label	Incorrect Label
Primed	p_i	$1-p_i$
Non-Primed	n_i	$1-n_i$

$$I(E_{primed,correct}) = -\log_2 P(correct \mid primed)$$

→ **A "good" Mooney image has a high p_i, but low n_i value.**

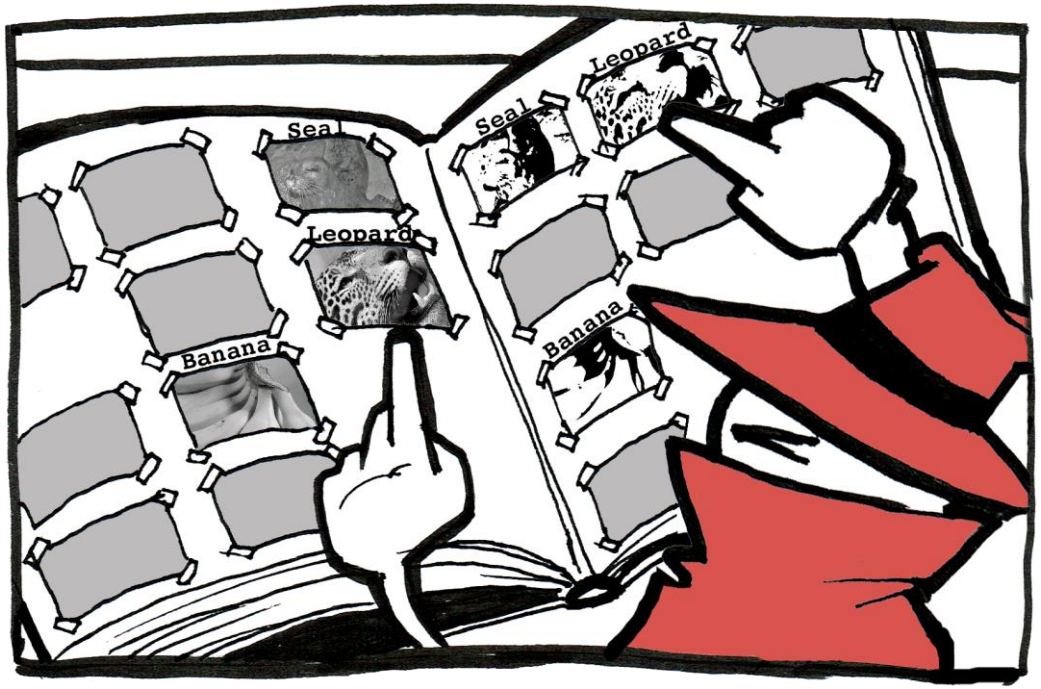
Attacker Model

The security does not rely on secrecy of the hidden object.

We provide the attacker with the solution for every Mooney image:

- Mooney image
- Original grayscale image
- Correct label

The scheme can not be broken by computer vision algorithms!

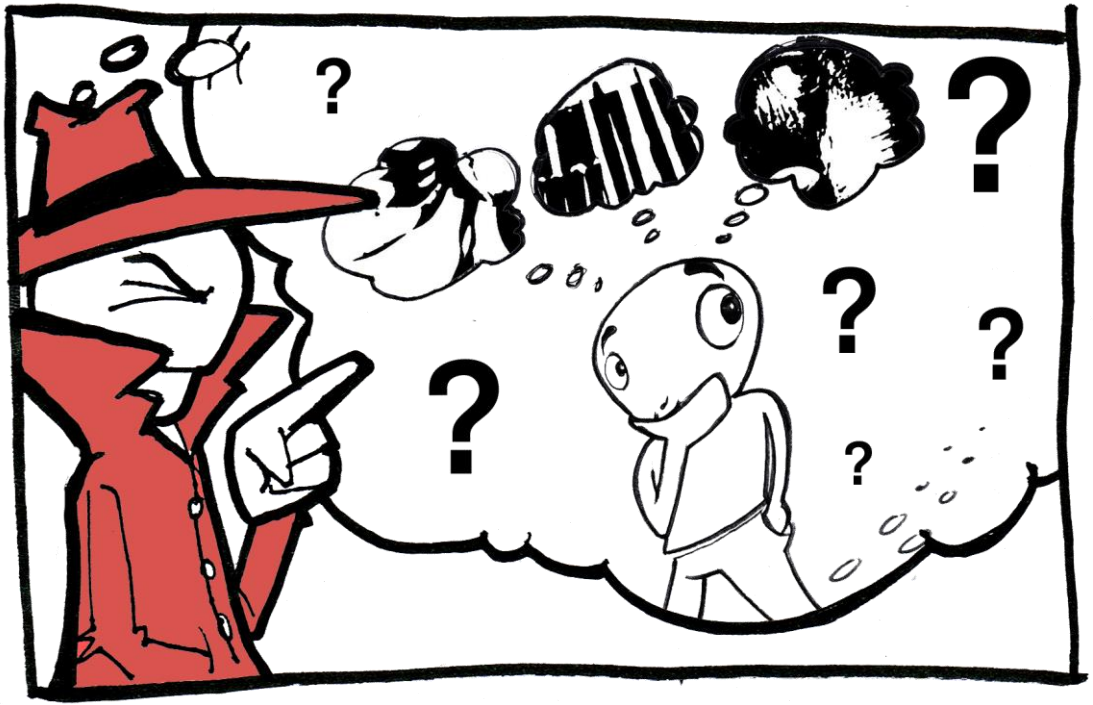


Attacker Model

Secret: Knowing which images the user was primed on.

During enrollment images are selected by the server:

- No user selection bias
- Random guessing
- Rate limit guessing attempts



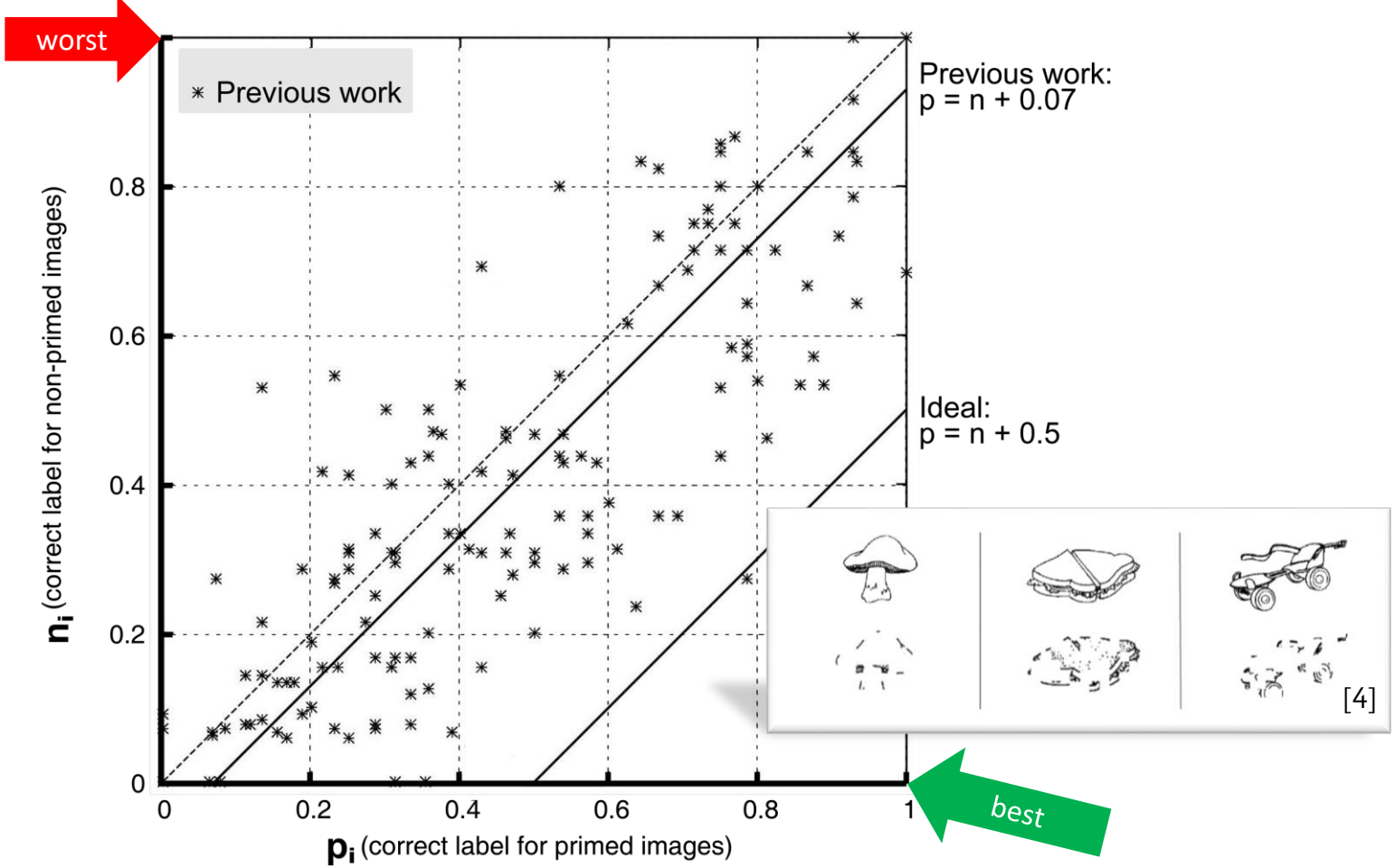
Main Results

Does implicit memory-based authentication work?

User Studies

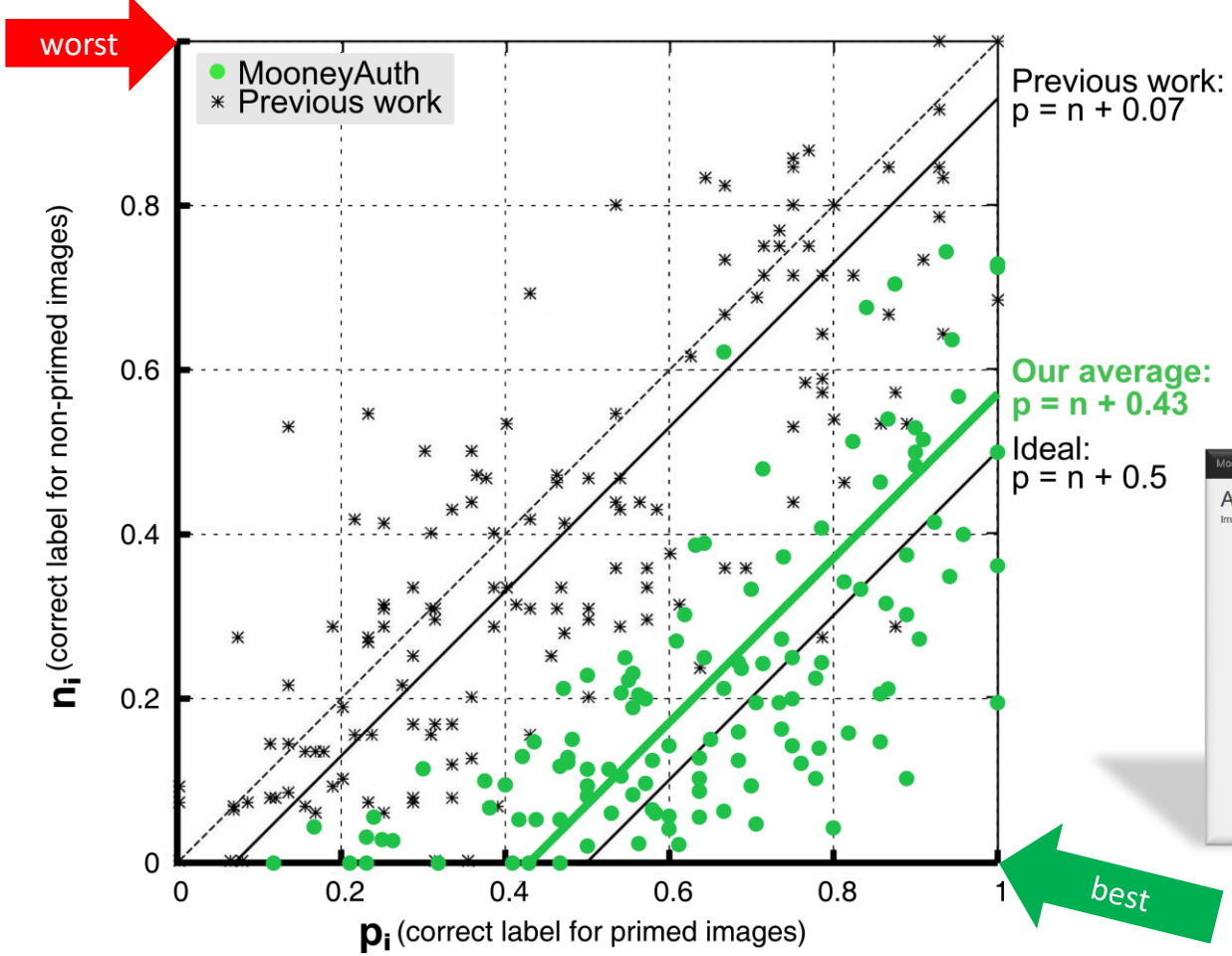
Pre Study	Long-Term Study	Main Study
230 participants 20 days	~130 participants 8.5 moths	70 participants 21 days
Goals: - Get p_i, n_i for Scoring - Test Label Matching	**Goals**: - Long-Term Effects	**Goals**: - Performance Measure

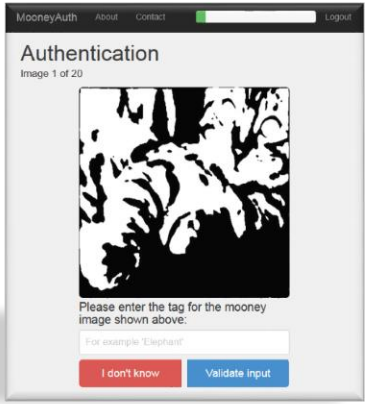
Previous Work



[Ref. 4] Tamara Denning, Kevin D. Bowers, Marten van Dijk, and Ari Juels: Exploring Implicit Memory for Painless Password Recovery. (CHI '11)

Our Result

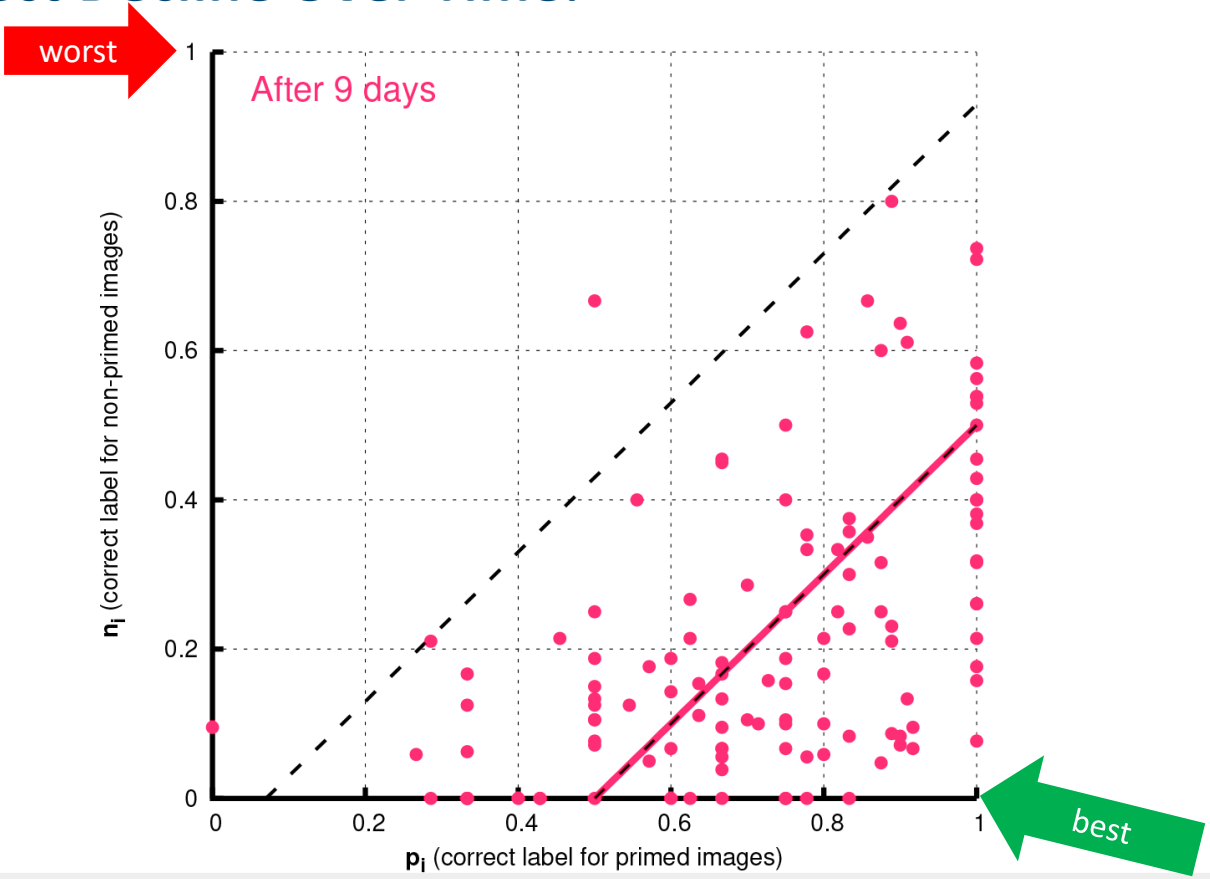

worst
MooneyAuth
Previous work
Previous work:
p = n + 0.07
Our average:
p = n + 0.43
Ideal:
p = n + 0.5
best
n_i (correct label for non-primed images)
p_i (correct label for primed images)
0
0.2
0.4
0.6
0.8
1


MooneyAuth
About
Contact
Logout
Authentication
Image 1 of 20
Please enter the tag for the mooney image shown above:
I don't know
Validate input

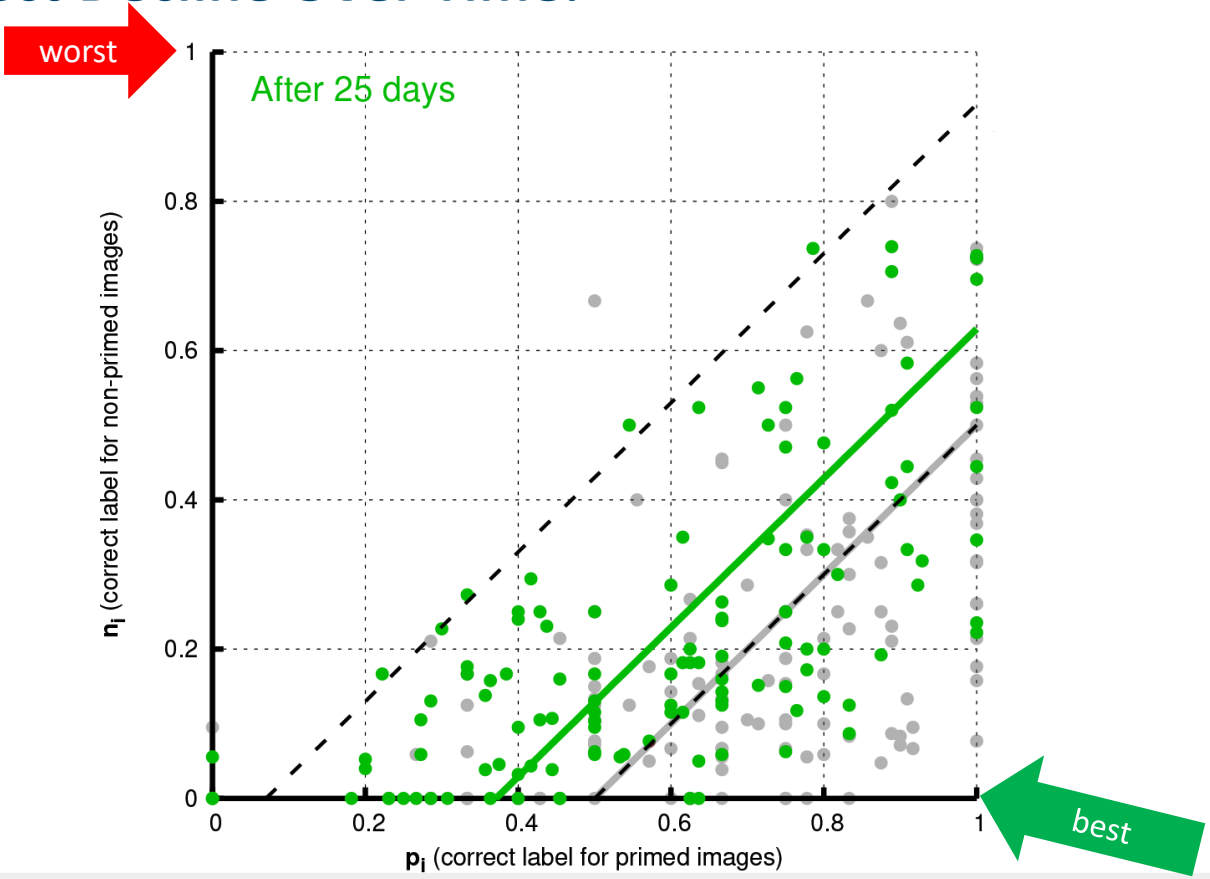
Long-Term Results

How long does the priming last?

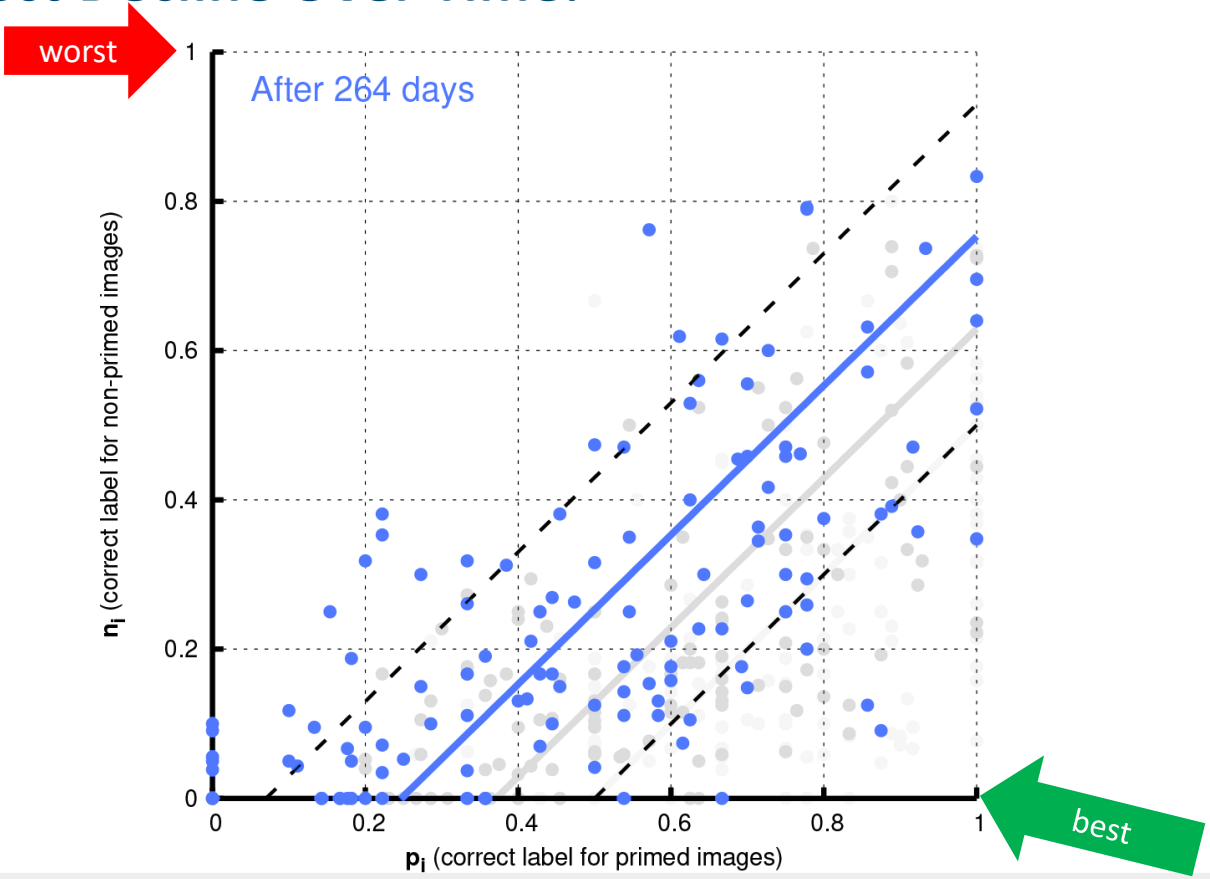
Priming Effect Decline Over Time:



Priming Effect Decline Over Time:



Priming Effect Decline Over Time:



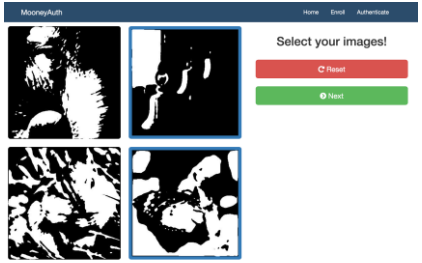
Benefits and Limitations

Benefits:

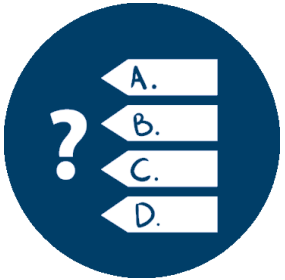
- High memorability
- Server selected secret (no user bias)

Limitations:

- Cumbersome to label (software keyboard, time required)
- Unexplored: Interference effects (use for multiple services)
- Phishing
- Shoulder surfing
- Secure storage of secret



Let’s Play Again!



Back to the game.

Authentication

?

Authentication

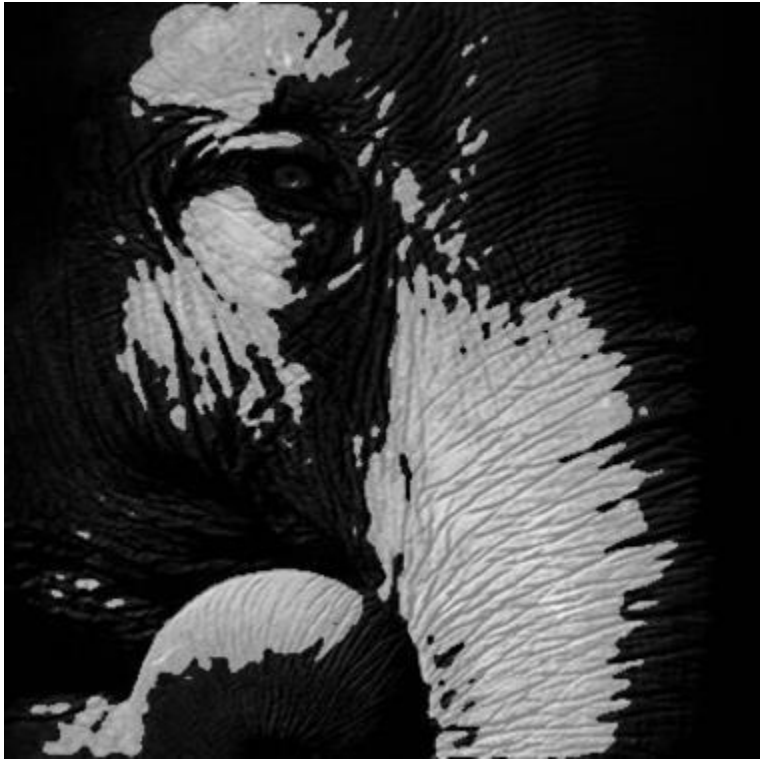
Authentication

Cows

Authentication

?

Authentication

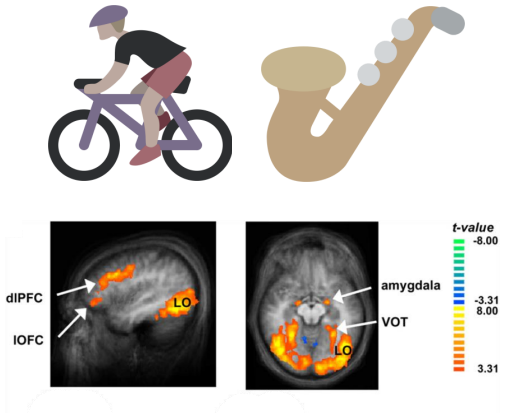


Authentication

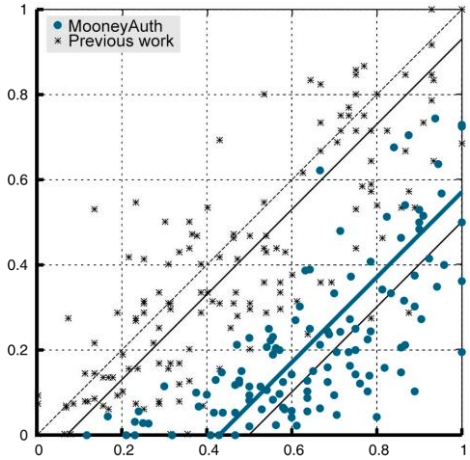
Elephant

Takeaway

Mooney Images



Implicit Memory



Implicit Memory-Based Authentication

Demo? mooneyauth.org

Mooney Image Generation

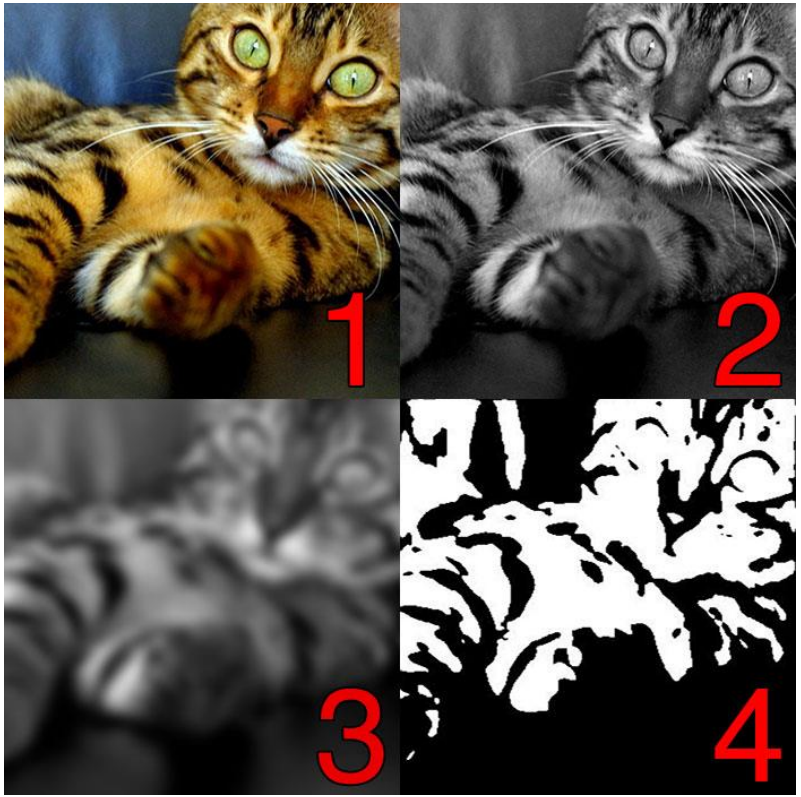
1) Image search with nouns from "MRC Psycholinguistic Database".

2) Convert images to gray-scale.

3) Smoothing via Gaussian filter.

4) Otsu's histogram based thresholding algorithm.

5) Filter for mean recognition rate of 5 sec. and longer. [5]



[Ref. 5] Fatma Imamoglu et al.: Changes in Functional Connectivity Support Conscious Object Recognition. (NeuroImage '12)